Sécurité de l'ordinateur

Sécurité de l'ordinateur

Pour comprendre la notion de sécurité informatique, il faut déjà commencer par comprendre les différents types de menaces dont vous pouvez être victime. Ensuite, nous parlerons des différentes habitudes. Les différentes habitudes à prendre et celles qui sont à perdre. Nous parlerons des moyens de protection, puis de quelques détails sur la navigation sur Internet.

Certaines personnes trouveront peut-être triviales les différentes explications fournies. De même, certaines explications sont volontairement simplifiées afin d'être compréhensibles par le plus grand nombre. En ce qui concerne le système d'exploitation, ce didacticiel concerne (au moins pour la partie des logiciels de protection, quoiqu'il existe une version de Avast pour Linux, même si nous utiliserons AntiVir sous Windows) essentiellement Windows, mais la partie sur les explications et les bonnes habitudes à prendre sont universelles.

Ne soyez pas inquiétés par le nombre de pages. De nombreuses pages comportent des illustrations, ce qui augmente fortement le nombre de pages.

Autre chose, parmi les 285 pages, il y a environ :

- 30 pages de choses à lire et comprendre et mémoriser une seule fois.
- 15 pages de téléchargement de logiciels
- 100 pages d'installations (choses que vous n'aurez bien sûr pas à faire tous les jours) et de choses à ne faire qu'une fois
- 10 pages d'instructions pour analyser son PC régulièrement
- 50 pages d'instructions pour le cas où vous auriez un problème de sécurité

Sommaire

Un sommaire un peu plus complet est disponible à la fin du document.

I) Les différentes menaces

Comme vous avez pu voir dans le sommaire à la page précédente (sauf si vous n'avez pas lu le plan, je ne vous en voudrai pas, ça m'arrive régulièrement aussi de ne pas lire les sommaires), les menaces sont nombreuses en types.

Vous avez certainement déjà entendu parler des virus, mais le mot de « spyware » (ou logiciel espion en français), de « trojan » (cheval de Troie, comme dans la mythologie) ou encore « rootkit » vous semblera peut-être un peu chinois si vous ne lisez pas les quelques lignes en-dessous. C'est pour ça que, pour qu'on se comprenne bien, nous allons parler de toutes ces joyeusetés qui circulent sur le net, et d'autres joyeusetés dont je n'ai pas encore mentionné le nom.

Chacune de ces menaces peut avoir de très nombreux effets tous plus indésirables les uns que les autres.

Il existe un mot permettant de désigner la plupart des menaces : le mot malware. Ce mot désigne un logiciel espion, ou un cheval de Troie, ou un rogue, ou un virus, ...

Bref, le mot malware désigne toute cochonnerie pouvant s'incruster dans votre ordinateur. Ce terme sera donc de temps en temps utilisé dans ces quelques pages afin d'éviter d'écrire toute la liste des cochonneries pouvant infester votre ordinateur.

I.1) Quelques effets

Commençons par parler des différents effets des différentes menaces que vous pourriez trouver sur Internet.

Certains malwares sont totalement inoffensifs (très rares), d'autres peuvent détruire irrémédiablement l'ordinateur (heureusement très rares aussi). Ce ne sont bien évidemment pas les seuls effets des malwares. Voici une liste d'effets visibles ou même invisibles qui peuvent de produire si votre ordinateur attrape un malware :

- ralentissement global du PC
- l'ordinateur qui se met à écrire tout seul
- des millions de spams envoyés au monde entier à votre nom (ou pas) via votre ordinateur pour que des gens achètent du viagra ou se fassent allonger le pénis (les femmes reçoivent aussi ce genre de messages, des virus ne sont pas particulièrement intelligents).
- Des fichiers que vous ne connaissez pas qui se retrouvent à des endroits auxquels ils n'ont rien à faire (des fichiers bizarres qui se retrouveraient dans vos photos par exemple / attention : certains programmes légitimes créent parfois des fichiers tout à fait légitimes dans vos documents, ne donc pas y voir tout de suite l'intervention d'un virus)
- Destruction complète de certains fichiers
- Infection de certains fichiers légitimes par des virus (afin de se répliquer pour quand vous ouvrirez ce fichier sur un autre PC)
- Impossibilité de lancer certains logiciels (qui marchaient très bien avant et qui ne marchent plus sans raisons apparentes)
- Disparition de l'antivirus
- Impossibilité de lancer le gestionnaire des tâches (Ctrl + Alt + Suppr) ou un éditeur de registre
- Impossibilité de démarrer l'ordinateur
- Page d'accueil de votre navigateur changée (avec impossibilité de revenir à l'ancienne page d'accueil)
- affichage de fenêtres non désirées (et souvent publicitaires)
- vol d'informations
- …

Impossible de faire une liste exhaustive des effets d'un malware, car il y aurait sans

doute plusieurs dizaines de pages. De plus, les virus et les chevaux de Troie sont très nombreux : F-Secure (une entreprise connue dans le domaine de la sécurité informatique) annonce que leur nombre pourrait dépasser le million à la fin de l'année 2008.

I.2) Les malwares et les autres menaces

I.2.a) Le menaces actives

I.2.a.i) Les virus

Un virus est un programme informatique écrit dans le but de se propager à d'autres ordinateurs en infectant un programme légitime.

Les virus se répliquent en infectant des logiciels particuliers, mais il existe des variantes qui peuvent se multiplier par leurs propres moyens, sans infecter de logiciel hôte. Ce sont des vers.

I.2.a.ii) Les chevaux de Troie

Un cheval de Troie est un type de logiciel malveillant. Le plus souvent, un tel programme exécute des actions nuisibles à l'utilisateur. Ce n'est pas un virus car il ne se réplique pas lui même. Cependant, il peut être apparu en même temps qu'un virus qui aurait installé lui même le cheval de Troie.

Le plus souvent, un cheval de Troie ouvre une porte dérobée dans votre ordinateur. De ce fait, un pirate informatique peut à tout moment prendre le contrôle de l'ordinateur à distance et en faire ce qu'il veut.

Les effets d'un cheval sont nombreux et similaires à ceux des virus.

I.2.a.iii) Les logiciels espions

Appelé en anglais spyware, ou en français espiologiciel, ou plus rarement espiongiciel, un logiciel espion a pour but de collecter des informations contenues dans votre ordinateur (sites sur lesquels vous allez, et toutes autres informations que les concepteurs jugeraient intéressantes). Les logiciels espions accompagnent souvent les logiciels gratuits et sont souvent installés à l'insu des utilisateurs.

Parfois, certains logiciels espions se font passer pour des logiciels anti-logiciels espions, tentent d'effrayer l'utilisateur et poussent à l'achat de la version complète du logiciel espion.

Il n'est pas rare aussi que certains logiciels espions soient livrés gratuitement avec des virus et autres chevaux de Troie.

I.2.a.iv) Les keyloggers

Derrière ce nom se cachent des malwares dont la fonction est d'enregistrer exactement ce que vous tapez au clavier. Y compris bien entendu le numéro de votre carte bancaire lors d'un achat en ligne, ou encore vos identifiants et mots de passe de Paypal, ou votre adresse e-mail et le mot de passe qui va avec.

Certains sites utilisent maintenant un système visuel pour entrer son code (comme certaines banques), mais les keyloggers ont maintenant la possibilité d'enregistrer aussi l'écran en faisant des captures d'écran.

I.2.a.v) Les rootkits

Les rootkit modifient le comportement de votre système d'exploitation (Windows, Linux, ...) afin de cacher les opérations malveillantes effectuées par les chevaux de Troie et les autres cochonneries du Web qui seraient dans votre ordinateur. Ce qui les rend indétectables par des méthodes classiques et difficilement supprimables.

Il y a eu des affaires tristement célèbres sur les rootkits. De nombreux CD musicaux de Sony-BMG ont pendant un temps installé un rootkit qui rendait certains dossiers invisibles aux yeux des utilisateurs. Ce qui a permis à des virus de se mettre dans ces dossiers cachés et les

antivirus ont eu du mal à les y enlever.

I.2.b) Des vecteurs de menaces

Les différentes choses expliquées ici ne sont pas directement des menaces mais peuvent apporter des malwares à votre ordinateur.

I.2.b.i) Les scripts Javascript

Pour pouvoir correctement expliquer ce que sont les scripts Javascript, il va falloir que j'explique ce que sont les pages Internet. Les pages Internet sont presque tout le temps conçues en HTML (ou ses dérivés).

Le HTML, c'est un langage qui est en quelque sorte un plan. C'est au navigateur d'afficher tout les éléments du plan correctement à l'écran. Comme vous vous en doutez surement, le HTML tout seul est quand même limité.

Les scripts Javascript sont de petits programmes inclus à l'intérieur des pages qui permettent d'améliorer la navigation sur Internet.

Ils permettent par exemple de changer la couleur d'une page, de faire apparaître du texte dans une page sans changer de page, ...

Ils sont donc agréables, mais sont parfois malicieux car en faisant planter le navigateur (via des failles de sécurité), ils permettent la propagation de malwares.

I.2.b.ii) Les failles de sécurité

Ce ne sont pas à proprement parler des menaces directes. Une faille de sécurité est un défaut de fonction dans un logiciel qui permet à des virus ou des personnes physiques de corrompre le système, de voler des données et dans tout les cas, d'effectuer des actions non désirées.

Très nombreux (pour ne pas dire tous) sont les logiciels ayant des failles de sécurité. La plupart sont corrigées, d'autres ne sont pas encore découvertes.

C'est du fait des failles de sécurité qu'il faut mettre à jour ses logiciels, et donc éviter les logiciels piratés.

I.2.b.iii) Les macros

Comme le nom ne l'indique pas, ce ne sont pas de petits poissons qui seraient cachés dans votre ordinateur. Ce sont de petits programmes qui sont inclus dans des documents. Il n'est pas rare d'avoir des macros dans des documents de traitement de texte, de tableur, ou d'autres types de documents.

Certaines macros sont agréables, elles permettent par exemple à ma mère d'envoyer des documents de son boulot facilement à ses employeurs. Mais il en existe de nombreuses qui ne le sont pas, et qui permettent la propagation de virus et autres cochonneries.

I.2.c) Les menaces par e-mail

I.2.c.i) Les chaines de messages

Vous avez très certainement reçu au moins une fois un mail vous donnant une information soit disant sérieuse, mail où il était préconisé de le transférer au plus de gens possible afin que tout le monde entier soit au courant.

On appelle ça une chaine de message. Chaine car si vous le transférez aussi, d'autres personnes à qui vous avez envoyé le message le transmettront à leur tour.

Nous en reparlerons plus en détails à la section II.6.b page 25.

I.2.c.ii) Le spam

Le SPAM en majuscule désigne une marque jambon épicé en boite de conserve utilisé souvent pour faire des sandwiches. Pourquoi je vous parle de ça ? Parce qu'il existe le même mot, mais en minuscules. Parfois traduit en pourriel, rarement en polluriel, ce mot désigne les e-mails indésirés qui ont été expédiés en masse à but publicitaire voire malhonnête.

Le spam peut être trouvé sous ces formes :

- Le spam contient généralement de la publicité. Les produits les plus vantés sont les services pornographiques, les médicaments (le plus fréquemment les produits de « dopage sexuel » ou, des hormones utilisées dans la lutte contre le vieillissement), le crédit financier, les casinos en ligne, les montres de contrefaçon, les diplômes falsifiés et les logiciels craqués.
- Des escrocs envoient également des propositions prétendant pouvoir vous enrichir rapidement : travail à domicile, conseil d'achat de petites actions (penny stock).
- Les chaines de messages ne sont pas réellement du spam, mais ce sont quand même des e-mails indésirables.
- Parfois aussi, mais de plus en plus rarement, il s'agit de messages d'entreprises ignorantes des règles du bon comportement sur Internet qui y voient un moyen peu couteux d'assurer leur promotion.
- Certains messages indiquant qu'un mail n'est pas arrivé à destination peuvent également être qualifiés de spam lorsque le message d'origine n'a pas été envoyé par vous même mais par exemple par un virus se faisant passer pour vous.
- Enfin la dernière forme de spam, le phishing

I.2.c.iii) Le spit

SPIT, pour Spam over Ip Telephony.

Ce qui en français signifie spam par téléphonie IP.

Depuis l'avènement de la téléphonie IP (avant, la téléphonie passait directement par les lignes téléphoniques et était analogique. Maintenant, la téléphonie passe de plus en plus par Internet et est numérique, ce qui permet une réduction importante des couts), il y a eut quelques tentatives de spam par téléphone.

Les experts en sécurité annoncent que dans quelques temps, on peut s'attendre à des déluges d'appels vers des serveurs téléphoniques afin de les saturer et de pénaliser une entreprise, de faire perdre du temps, ou tenter de faire passer leur message publicitaire afin de vendre des produits douteux.

I.2.c.iv) Le spim

Dans le même registre, il existe aussi le spim (pour Spam over Instant Messaging), c'est à dire le spam par messagerie instantanée.

Par exemple des messages proposant de faire agrandir son pénis en plein milieu d'une discussion romantique avec votre aimé(e) (cette situation ne m'est pas arrivée, contrairement à d'autres situations évoquées dans ces quelques pages), ou encore des demandes régulières de nouveaux contacts, contacts qui veulent absolument vous faire aller sur des sites cochons, en vous parlant tout en anglais.

I.2.c.v) Le phishing

Vous êtes à la caisse d'épargne et vous recevez un mail qui semble tout ce qu'il y a de plus officiel vous demandant de rentrer pour des raisons de maintenance toutes vos coordonnées bancaires sur le site après avoir cliqué dans le lien donné dans le message ? C'est très certainement un faux, et vous risquez si vous le faite de voir s'envoler ailleurs tout votre argent.

C'est ce qu'on appelle le phishing, ou hameçonnage en français. Cette technique est utilisée par les fraudeurs afin de vous soutirer des informations personnelles (identifiants, mots de passe, numéro de carte de crédit, date de naissance, ...) dans le but de se faire passer pour vous. Cela consiste à se faire passer pour un organisme de confiance (sa propre banque, Paypal, ...) afin de vous soutirer ces informations. Le phishing existe sous deux formes : par mail et sur des sites Internet. Et bien souvent, c'est un mail qui vous fait aller sur un site Internet frauduleux.

Les sites où il est demandé d' aller dans ces messages ressemblent souvent

énormément aux originaux. Mais il arrive très souvent qu'il y ait de nombreuses fautes de français.

I.2.c.vi) Le pharming

Le pharming est une variante de phishing, mais encore plus poussée.

Pour expliquer le pharming, il va falloir expliquer une partie du fonctionnement d'Internet.

Le réseau Internet ne voit pas les adresses des sites Internet (comme www.google.fr par exemple). Chaque site possède une (ou plusieurs) adresse IP (une succession de quatre nombres compris entre 0 et 255 séparés par des points, par exemple : 209.85.129.104). Et les fournisseurs d'accès fournissent un service qui permet d'associer une adresse IP à une adresse de site. C'est ce qu'on appelle les DNS.

Lorsque vous êtes victime d'une attaque de pharming, les fraudeurs ont au préalable réussi à modifier les DNS de façon à vous rediriger automatiquement vers le site frauduleux même en tapant à la main l'adresse du site dans la barre d'adresse. L'adresse apparaissant dans la barre d'adresse de votre navigateur sera bien l'adresse normale du site. Cependant, vous serez sur un site frauduleux.

Ensuite, l'arnaque est la même qu'avec le phishing. Si l'internaute entre des informations confidentielles, c'est à ses risques et périls.

Ce type d'attaque est quand même relativement rare.

I.2.c.vii) Le vishing

Toujours dans le domaine du phishing, voici le vishing (le v est pour « voix »).

La méthode est la même que le phishing, sauf que le moyen utilisé est différent. Cette fois, c'est au téléphone que tout se passe. Une voix de synthèse vous demande donc vos identifiants et mots de passe.

Donc toujours pareil : ne donnez pas ces informations à une voix de synthèse.

Ce type de menace est pour le moment encore peu répandu.

I.2.c.viii) Ingénierie sociale

L'ingénierie sociale est assez proche du vishing sur le principe. Tout se passe par téléphone, sauf que c'est une personne réelle à l'autre bout du fil.

Certaines personnes, dans le but de s'attaquer à une entreprise, ciblent parfois les employés de cette même entreprise.

I.2.d) Autres types de menaces

I.2.d.i) Les faux logiciels de protection et les faux codecs

Il se peut que vous en rencontriez lors de vos navigations sur Internet.

Si vous avez une page vous disant quelque chose du genre « Votre ordinateur est infecté, téléchargez gratuitement WinAntivirus pour le désinfecter », ne le faites surtout pas. Bon nombre de ces soit-disant outils de désinfection sont en fait des outils d'infection, ou des outils totalement inefficaces.

De même si une page vous dit que vous n'avez pas le bon codec pour lire une vidéo ou une musique. Il existe de nombreux sites qui vous proposeront d'installer pour vous des codecs ainsi qu'une quantité de cochonneries non désirées.

Dans le cas ou vous verriez ce genre d'alertes, utilisez votre antivirus et votre antispyware pour vous désinfecter.

Et si vous voulez vraiment installer un pack de codecs, il y a plusieurs choses à prendre en compte :

• La multiplication des packs risque de ralentir votre ordinateur ou de le faire bugger.

• Téléchargez le pack de codecs sur un site de confiance (pour éviter les risques d'infection par ce qui pourrait vous être proposé par un site peu sûr).

I.2.d.ii) Les cookies

Tout comme les macros, les cookies ne sont pas de petits gâteaux secs avec des pépites de chocolat lorsqu'on est dans le domaine de la navigation sur Internet. Voici une définition tirée de Wikipédia légèrement retouchée par mes soins :

> Les cookies sont de petits fichiers textes stockés par le navigateur Internet (Internet Explorer, Mozilla Firefox, ...) sur le disque dur du visiteur d'un site Web et qui servent (entre autres) à enregistrer des informations sur le visiteur ou encore sur son parcours dans le site.
>
> Le concepteur du site peut ainsi reconnaitre les habitudes d'un visiteur et personnaliser la présentation de son site pour chaque visiteur ; les cookies permettent alors de garder en mémoire combien d'articles il faut afficher en page d'accueil ou encore de retenir les identifiants de connexion à une éventuelle partie privée : lorsque le visiteur revient sur le site, il ne lui est plus nécessaire de taper son nom et son mot de passe pour se faire reconnaitre, puisqu'ils sont automatiquement envoyés par le cookie.
>
> Un cookie a une durée de vie limitée, fixée par le concepteur du site. Ils peuvent aussi expirer à la fin de la session sur le site, ce qui correspond à la fermeture du navigateur.
>
> Les cookies sont largement utilisés pour simplifier la vie des visiteurs et lui présenter des informations plus pertinentes. Mais une technique particulière permet aussi de suivre un visiteur sur plusieurs sites et ainsi de collecter et recouper des informations très étendues sur ses habitudes. Cette technique a donné à l'usage des cookies une réputation de technique de surveillance violant la sphère privée des visiteurs.

Comme vous avez donc pu le lire, les cookies ne sont pas tous à but malveillant. Le fait de vouloir à tout prix tous les supprimer est inutile et même gênant. Nous verrons ça plus en détail à la fin de ces quelques pages.

II) Quelques conseils théoriques

Face à son ordinateur, chacun a ses habitudes de fonctionnement. Mais face à Internet, il ne faut pas avoir la même attitude que face à son traitement de texte ! Il y a de bonnes habitudes à prendre, et de mauvaises habitudes à perdre. Cette section donnera quelques conseils préventifs pour éviter les problèmes, ou quelques conseils pour résoudre certains problèmes.

Nous parlerons d'abord de quelques conseils théoriques dans une première partie, puis nous passerons à la pratique après. Cela permettra aux gens ayant déjà les bons paramètres de lire la théorie en une seule fois (ou en plusieurs pour les moins courageux).

II.1) Quelques conseils avec les logiciels

Dans cette partie, nous parlerons des habitudes à prendre par rapport aux logiciels en général. Nous parlerons donc de piratage de logiciels, de téléchargement et de mises à jour de logiciels.

II.1.a) Télécharger sur des sites connus – Ne pas payer des logiciels gratuits

Il y a une grande mode en ce moment sur Internet : les sites qui vous font payer des logiciels tout ce qu'il y a de plus gratuits.

Exemple avec Avast.

Souvent, dans les liens commerciaux de Google pour les logiciels censés être gratuits, il y a un site qui vous proposera de les télécharger gratuitement à condition d'appeler un numéro surtaxé qui vous coutera très très cher (ce qu'ils ne vous disent pas bien entendu).

En plus, rien ne vous assure qu'il s'agira bien de la version officielle et pas d'une version modifiée de Avast.

Bref, quand vous téléchargez des logiciels, faites le de préférence sur des sites fiables. Et si vous tombez sur un site moins connu, ne sortez pas votre téléphone portable ni votre carte de crédit si le logiciel est censé être gratuit. Changez simplement de site.

Il existe de très nombreuses façons de télécharger des logiciels. Pour des raisons évidentes de sécurité, je ne vous recommande pas de télécharger des logiciels piratés (les utilisateurs les plus expérimentés sauront éviter les problèmes, mais les débutants devraient éviter). Cependant, télécharger des logiciels gratuits (ou même des versions de démonstration afin d'acheter ultérieurement les logiciels) peut s'avérer risqué car ces logiciels pourraient contenir des spywares, virus ou autres joyeusetés. De même, certains sites ne sont de base pas sûrs et vous proposeront même de vous faire payer un service gratuit.

C'est pour cette raison que je vous recommande de télécharger des logiciels à partir de sites connus. Ça permet aussi d'avoir un avis sur les utilisateurs de ces logiciels, et peut-être de savoir comment ne pas installer le/les spywares qui seraient inclus avec certains logiciels (comme pour Messenger Plus, refuser le sponsor permet de ne pas être embêté). Vous pourrez ensuite, à partir de ces sites, accéder à la version la plus récente du logiciel : la plupart de ces sites proposent un lien vers le site de l'éditeur, ce qui vous permet de télécharger une version parfois plus récente sans soucis.

Liste non exhaustive de sites vous permettant de télécharger des logiciels :

- Téléchargement de tout types de logiciels :
  - http://www.clubic.com
  - http://www.telecharger.com
  - http://telechargement.journaldunet.com
- Extensions Firefox et Thunderbird :
  - https://addons.mozilla.org/fr/
  - http://www.geckozone.org/

Dans les sections suivantes, je vous indiquerai comment télécharger certains logiciels de protection. J'ai volontairement choisit de donner les liens des sites des éditeurs, afin de montrer que certains sites (le site de Microsoft par exemple) ne sont pas très faciles à manipuler, ainsi que pour vous donner les dernières versions de ces logiciels.

II.1.b) Éviter de cliquer systématiquement sur Suivant

Certains logiciels abritent d'autres logiciels quand vous les installez. Et parfois même tout un tas de cochonneries qui sont désactivables.

Encore faut-il ne pas cliquer trop vite sur « Suivant ».

Souvent, ce sont des barres d'outils qui s'installent alors que vous ne les attendiez pas.

N'hésitez pas à effectuer des installations personnalisées qui vous permettront de mieux comprendre ce qui sera installé sur votre ordinateur.

II.1.c) Mettre à jour ses logiciels

Des failles de sécurité sont régulièrement découvertes dans les logiciels que vous utilisez tous les jours (en commençant par Windows lui même). Il faut donc mettre à jour ses logiciels.

L'un des inconvénients de Windows, c'est qu'il n'y a aucune gestion centralisée des logiciels installés. Du coup, il n'y a pas non plus de centralisation des mises à jour. Chaque logiciel gère ses mises à jour comme il souhaite.

Quelques petites règles de base tout de même :

- Mettre à jour par le logiciel lui même
- Ne pas installer de mises à jour fournies par mail
- Dans le cas de logiciels qui ne se mettent pas à jour par eux-mêmes, téléchargez les versions les plus récentes sur des sites connus.

II.1.d) Éviter d'utiliser Internet Explorer et Outlook Express

Si vous avez un Windows piraté ou ancien (Windows 2000, NT4, 98, Me, 95 (ne cherchez pas plus loin, si vous avez Windows 3.1 ou des versions antérieures, songez à acheter un autre PC ou éventuellement à mettre Linux, quoique les PC avec du Windows 3.1 ne supporteront peut-être pas non plus Linux)), vous devez donc avoir certainement de très vieilles versions de ces deux logiciels, avec tous les bugs et toutes les failles de sécurité connues. Je vous recommande donc de passer à Mozilla Firefox (pour la navigation sur Internet, à la place d'Internet Explorer) et Mozilla Thunderbird (pour lire vos mails, à la place d'Outlook Express).

Commençons par le (commencement me dirons certains) cas Outlook Express (eh bah non, je vous ai eu).

- Outlook Express :

Outlook Express ne possède pas d'anti-spam. Donc si vous recevez régulièrement des e-mails vous proposant d'élargir votre pénis ou d'acheter du viagra, Outlook Express ne fera pas le tri et mettra tout dans votre boite de réception comme un grand. Et si vous ne recevez que deux mails réels pour 10 spams, vous en aurez vite marre d'Outlook Express.

Je me rappelle aussi beaucoup de l'époque ou ma mère avait Outlook Express. Parfois plusieurs fois par semaines, celle-ci m'appelait pour que je lui relance son Outlook Express car cet idiot avait planté et était impossible à relancer, ou pour d'autres bugs divers et variés.

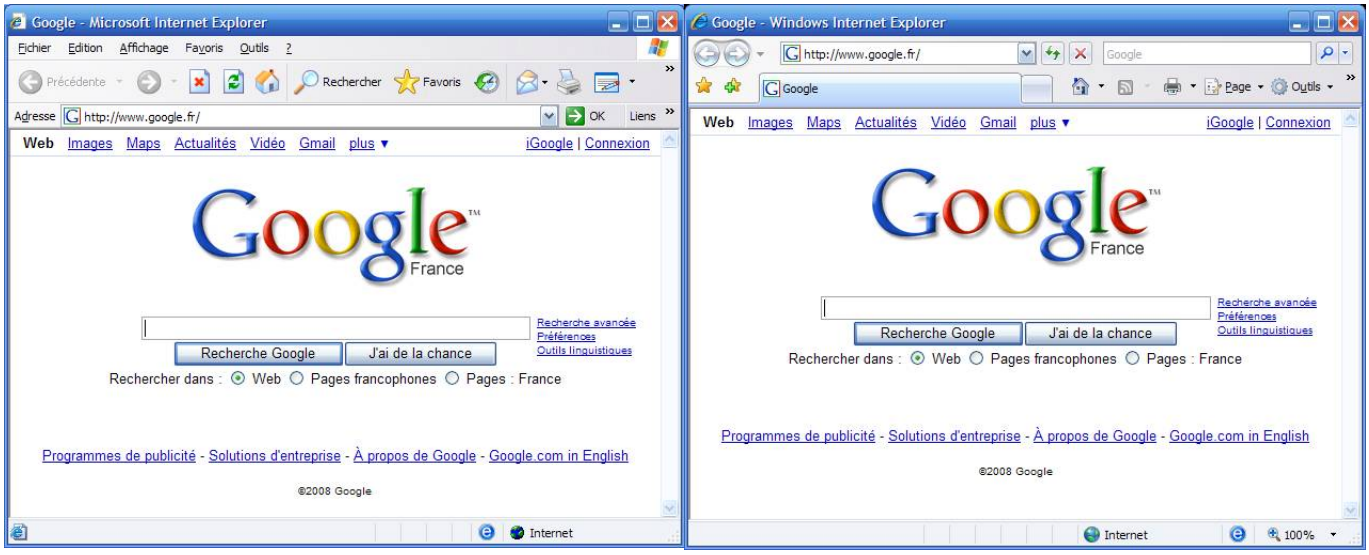
Comme vous l'aurez sans doute compris en lisant les quelques lignes ci-dessus, je n'aime pas Outlook Express. Je lui préfère grandement Mozilla Thunderbird qui est un logiciel libre beaucoup moins buggé et plus complet que Outlook Express.

Sous Windows Vista, Outlook Express n'existe plus (ce qui n'est pas plus mal), c'est Windows Mail qui le remplace. Sachant que c'est le successeur d'Outlook Express, je redoute le pire concernant ce programme. Sincèrement, ne l'ayant jamais testé, je ne peux pas dire s'il est le digne successeur d'Outlook Express ou si celui-ci a relevé le niveau. Je sais que celui-ci dispose enfin d'un anti-spams. Mais c'est à peu près tout ce que je sais.

- Internet Explorer :

Là encore, si vous avez un Windows piraté, évitez Internet Explorer. Si vous avez Internet Explorer 6, passez à la version 7 ou même 8 qui est plus sécurisée et respecte mieux les standards des pages Internet.

Si vous ne savez pas quelle version vous avez, voici la capture d'écran des deux versions :



Internet Explorer 6 *Internet Explorer 7*

Si vous êtes sous Windows Vista, vous avez obligatoirement la version 7 d'Internet Explorer. Et si vous avez Windows 7, alors vous avez déjà Internet Explorer 8.

Donc si vous êtes sous Windows 95, 98, Me, NT4, 2000, et même XP (si vous n'avez pas le service pack 2, et que vous ne pouvez/voulez pas le mettre, vous ne pourrez pas avoir Internet Explorer 7), je vous recommande grandement de passer à Mozilla Firefox qui sera plus sécurisé, moins buggé et plus respectueux des standards qu'Internet Explorer.

Par respect des standards, je veux dire qu'Internet Explorer n'affiche pas toujours correctement des pages correctement écrites (Firefox non plus, mais il est nettement plus doué qu'Internet Explorer dans le domaine du respect des standards). Imaginez par exemple des gens qui construisent une maison en fonction d'un plan. Avec Internet Explorer, la maison risque de ne pas beaucoup respecter le plan, alors qu'elle sera beaucoup mieux construite avec Mozilla Firefox.

L'un des problèmes d'Internet Explorer, c'est aussi les ActiveX. Ce nom barbare désigne une série de minis programmes incrustés à l'intérieur de nombreuses pages web. Ces petits programmes, une fois exécutés, ont tout pouvoir sur votre machine, ce qui explique que de nombreux sites pas toujours très nets proposent d'installer des ActiveX afin de vous offrir gracieusement des virus, chevaux de Troie ou simplement d'envoyer au monde entier de nombreux mails indésirés proposant d'acheter du viagra via votre ordinateur. Bien qu'au fond, la technologie des ActiveX soit intéressante, le problème est qu'elle est très (trop) souvent utilisée à des fins malhonnêtes.

Mozilla Firefox ne supporte pas la technologie des ActiveX.

Je terminerai ces quelques mots sur Internet Explorer pour dire de Firefox qu'il est bien plus souple qu'Internet Explorer, qu'il est par exemple possible de lui ajouter un bloqueur de publicités (qu'est-ce qu'il peut être énervant de parfois, sur certains sites, avoir une publicité qui prends toute la page, qu'on ne peut pas fermer et dont on est obligés d'attendre quelques secondes avant qu'elle ne s'en aille), d'avoir un navigateur fiable et moins buggé (à l'époque ou j'avais Internet Explorer 6, il me plantait très (trop) souvent à la figure aussi) et plus sécurisé.

Les installations de Firefox et de Thunderbird sont détaillées aux parties Erreur : source de la référence non trouvée et Erreur : source de la référence non trouvée aux pages Erreur : source de la référence non trouvée et Erreur : source de la référence non trouvée.

Si malgré tout ce que j'ai dit, vous souhaitez conserver Internet Explorer, passez au moins à la version 7. Pour ceci, suivez les instructions de la partie Erreur : source de la référence non trouvée page Erreur : source de la référence non trouvée.

II.1.e) Le piratage de logiciels

II.1.e.i) Évitez d'utiliser des logiciels piratés

La raison essentielle (pour la sécurité de votre ordinateur) pour laquelle je vous déconseille d'utiliser des logiciels piratés, c'est que vous ne pourrez pas le mettre à jour du fait de la politique anti-piratage des éditeurs de logiciels (qui interdisent les mises à jours dans le cas de logiciels piratés).

Et comme vous ne pourrez pas les mettre à jour, si vous attrapez un virus qui exploitait la faille de sécurité non mise à jour, vous serez (enfin pas vous, mais votre ordinateur, heureusement que les virus ne se transmettent pas du PC à l'être humain) infecté.

De plus, de nombreux logiciels, du fait d'Internet ou de procédures d'activation de certains logiciels payants, verront que vous les avez piratés (Windows XP et Vista, Nero, Word, Excel, Powerpoint, ...). Certains iront même jusqu'à se désactiver si vous ne payez pas le logiciel au bout d'un certain temps.

Pour éviter le piratage, il existe de nombreuses alternatives gratuites aux logiciels payants. Ces alternatives ne seront peut-être pas aussi complètes, mais en général, les gens n'utilisent pas plus de 10% des fonctions des logiciels payants (sauf peut-être les professionnels avec les logiciels qu'ils utilisent tous les jours au boulot). Donc pourquoi pirater quand aussi bien, voire meilleur existe ? Et gratuit qui plus est ?

Je ne vais pas m'attarder ici à faire la liste des équivalences entre les logiciels payants et les gratuits.

Votre ami Google (ou tout autre moteur de recherche) vous sera d'une grande aide.

J'ai trouvé ce site qui fera un récapitulatif non exhaustif qui résumera bien la situation :
http://www.commentcamarche.net/faq/486-equivalents-gratuits

II.1.e.ii) Évitez de pirater vos logiciels

Les sites vous proposant des cracks (programmes ou procédures de contournement des restrictions de la version de démonstration) ou autres keygens (générateur de numéro de série afin d'obtenir une version complète d'un logiciel) sont parfois agrémentés de spywares ou de virus.

Quand ce ne sont pas les sites qui sont infestés, ce sont parfois les téléchargements de cracks ou keygens qui sont infestés.

Je vous recommande donc de ne pas chercher à pirater vous mêmes vos logiciels. Et sachant qu'au niveau de l'utilisateur particulier, il existe des logiciels gratuits équivalents à presque tout les logiciels payants existants.

Donc il faut éviter de pirater vos logiciels !

II.2) Quelques conseils avec la messagerie instantanée

Tout comme pour les e-mails, il faut faire attention aussi sur les logiciels de messagerie.

De la même façon que pour les e-mails, vos contacts sur Windows Live Messenger peuvent avoir un ou des virus. Certains de ces virus se transmettent aussi tous seuls par messagerie instantanée. Les virus de messagerie instantanée sont en général très bavards. Ils discutent à la place de vos contacts ayant ces virus en anglais (même si la personne ne comprend pas un mot d'anglais), en espagnol, en français, ...

Tout comme pour les e-mails, ne téléchargez pas de fichiers envoyés par vos contacts si vous n'êtes pas sûrs.

Un contact ayant un virus de messagerie instantanée vous parlera souvent de la même chose, en vous demandant par exemple de cliquer sur un lien pour voir les photos de votre sœur (même si vous n'en avez pas), ou de télécharger les photos de Britney Spears nue (oui, certains créateurs de virus sont un peu cochons), ...

De plus, ces virus répètent souvent le même message en boucle, et vous envoient plusieurs fois d'affilée le même lien ou le même fichier.

De même que pour les mails, si votre contact vous parle dans une langue qui n'est pas la sienne, qu'il vous dit des choses incohérentes, qu'il n'écrit pas du tout de la même façon que d'habitude (en SMS au lieu d'un français parfait), et / ou qu'il répète plusieurs fois la même phrase en boucle, alors votre contact a probablement un virus.

Tout comme pour les mails, n'hésitez pas à demander à votre contact qui agit bizarrement s'il n'aurait pas un virus.

Autre petit truc très important pour les possesseurs de Windows Live Messenger et Messenger Plus! : n'activez surtout pas les réponses automatiques aux différentes requêtes car vous risquez par cette occasion d'accepter automatiquement un virus dans votre ordinateur.

Pour voir la procédure pour désactiver les acceptations automatiques, allez à la section III.4.a (Page 49).

II.3) Quelques conseils théoriques à propos des outils bureautique

II.3.a) Les macros

Comme le nom ne l'indique pas, ce ne sont pas de petits poissons qui seraient cachés dans votre ordinateur. Ce sont de petits programmes qui sont inclus dans des documents. Il n'est pas rare d'avoir des macros dans des documents de traitement de texte, de tableur, ou d'autres types de documents.

Le plus souvent, les logiciels de traitement de texte désactivent automatiquement les macros. Si une personne vous envoie régulièrement des messages drôles ou sympathiques (diaporamas, vidéos, ou autres), il est possible qu'un jour, votre logiciel de diaporama (ou de traitement de texte, en fonction du document ouvert) vous demande s'il faut exécuter ou non les macros du document. A moins que vous ne soyez absolument sûr de la provenance du document, n'exécutez pas les macros.

Par défaut, les logiciels désactivent les macros et ne vous demandent rien.

Il est possible de leur faire afficher une boite de dialogue vous permettant d'activer ou de désactiver les macros dans le cas où le document en contiendrait.

Ceci est beaucoup moins sûr que le niveau de sécurité élevé (le niveau qui ne vous

demande rien) car s''il y a d'autres personnes manipulant l'ordinateur, elles pourraient très bien activer les macros d'un document piégé.

Expliquez ce nouveau réglage ainsi que ce que sont les macros aux différentes personnes manipulant régulièrement votre ordinateur. Ne faites donc ce réglage qu'en cas de besoin (si OpenOffice (ou Microsoft Office) vous dit par exemple que les macros d'un document sûr ont été désactivées).

Les instructions pour OpenOffice sont disponibles à la section III.3.a (Page 46). Nous verrons les instructions pour Microsoft Office à la section III.3.b (Page 48).

Sous OpenOffice, il suffit de faire une seule fois le réglage qui est ensuite effectif pour tout les modules (Writer, Calc, ...). Sous Microsoft Office, il faut le faire dans tout les logiciels différents (Word, Excel, ...).

Microsoft Office 2007 a un autre réglage par défaut : il demande automatiquement ce qu'il doit faire pour les macros. Il n'y aura donc rien à changer pour cette version.

II.4) Quelques conseils par rapport à la gestion des fichiers

II.4.a) La contamination par clés USB

Il fut un temps (pas si lointain) ou les disquettes étaient le premier élément de transmission de données (hors Internet). A cette époque, il existait des virus qui se transmettaient sur les disquettes et pouvaient ainsi contaminer d'autres ordinateurs si les utilisateurs ouvraient le mauvais fichier.

Les virus étaient nettement moins répandus à cette époque que maintenant.

Les CD avaient aussi une particularité intéressante à cette époque : si un programme était définit par défaut, il pouvait se lancer dès l'insertion du CD dans le lecteur. Bien entendu, ce programme pouvait très bien être un virus, et donc infecter les ordinateurs.

Vous devez vous demander pourquoi je vous parle de ça ! C'est parce que les clés USB bénéficient aussi de cette fonction qui a été améliorée avec Windows XP :

- si aucun programme n'existe par défaut, Windows XP (et Vista, mais on parlera du cas Vista après) vous affiche une liste de choses que vous pouvez faire avec la clé (pareil pour les cartes mémoires)
- si un programme est défini par défaut, il est lancé

Du coup, si le programme par défaut est un virus, vous serez infecté (à moins que le virus ne soit connu par votre antivirus, mais le risque n'est jamais nul).

Je vous recommande donc plusieurs petites choses :

- désactiver l'exécution automatique
- afficher les fichiers cachés et ceux masqués par le système d'exploitation
- toujours se méfier des ordinateurs sur lesquels vous mettez des périphériques comme vos clés USB ou vos cartes mémoires. Certaines personnes n'ont pas toujours d'antivirus (n'étant pas conscientes des problèmes de sécurité qu'on trouve sur Internet) se font donc infecter très facilement et attrapent des virus qui peuvent se recopier sur clé USB (j'ai vu le cas pendant les vacances de Pâques 2008)

Le cas Windows Vista :

Par défaut, Windows Vista affiche la liste des choses que vous pouvez faire avec la clé USB, le CD ou la carte mémoire. Même s'il y a un programme par défaut. Du coup, le programme par défaut n'est jamais lancé tout seul. Le danger de la copie de virus par clés USB est donc diminué, mais pas nul non plus. Vous n'aurez donc pas besoin de désactiver l'exécution automatique. Mais affichez quand même tout les fichiers, et méfiez vous des autres ordinateurs aussi.

Exemple avec l'image ci-dessus. J'ai créé un programme que j'ai appelé « coucou.exe » que j'ai mit en programme par défaut au lancement de la clef. Sous Vista, celui-ci vous demande s'il doit exécuter le programme de la clef à l'insertion de celle-ci.

Si votre clef USB n'est pas censée contenir de programme par défaut, alors ne cliquez sous aucun prétexte sur une des lignes de la catégorie « Installer or exécuter un programme ». Même s'il s'agit de la même icone que « Ouvrir le dossier et afficher les fichiers » (il y a eu un virus qui avait ce comportement : imiter cette ligne afin que l'utilisateur clique dessus par erreur).

Petite astuce valable sous Windows toute version :

Pour empêcher le chargement de la clef (et donc de son programme par défaut), il est possible d'appuyer une dizaine de secondes sur la touche majuscule ( de gauche ou de droite, peu importe) lors de l'insertion de celle-ci dans l'ordinateur.

II.4.b) Afficher tous les fichiers

Par défaut, Windows n'affiche pas toujours tout les fichiers afin de donner un ordinateur « plus propre » esthétiquement. Ce qui est appréciable (d'avoir un système esthétiquement propre), mais le problème est que les virus et autres cochonneries d'Internet en profitent aussi pour se cacher aux yeux des utilisateurs.

Je vous recommande donc de les afficher, afin que vous puissiez éventuellement détecter vous-même que votre ordinateur a un comportement bizarre. Par exemple, j'ai vu une fois une cochonnerie qui se répliquait automatiquement dans les documents en créant des fichiers install.exe (ou .msi, je ne sais plus) à des endroits où la personne pouvait être sûre qu'ils n'avaient rien à faire.

Le revers de la médaille est que vous verrez apparaitre nettement plus de fichiers dans votre ordinateur. Et de nombreuses personnes sont tentées régulièrement de faire du ménage à la main de fichiers qu'elles ne connaissent pas, et parfois de fichiers indispensables à certains logiciels, voire de fichiers du système d'exploitation (et du coup les supprimer pourrait endommager les programmes de l'ordinateur).

Conclusion, méfiez vous, mais n'hésitez pas à demander de l'aide à un ami ou un membre de votre famille si vous avez un doute.

La procédure pour afficher tous les fichiers est disponible à la section III.1.c (Page 38).

II.4.c) Afficher l'extension de tous les fichiers

Par défaut, Windows n'affiche pas les extensions des fichiers (la fin du nom du fichier, après le dernier « . »), ce qui peut paraitre joli, mais qui est un risque pour votre sécurité aussi.

Si votre fichier s'appelle machin.jpg.exe, c'est un programme (du fait du .exe à la fin du nom), et pas une image. Bref, après affichage des extensions, si un fichier contient deux extensions, méfiez vous car c'est la deuxième qui compte. Par contre, si vous renommez le fichier après affichage des extensions, vous pouvez la modifier (trop) facilement.

Bref, l'affichage des extensions peut permettre aussi de détecter des actions louches qui s'effectueraient dans votre ordinateur. Cependant, le risque de faire une erreur en renommant un fichier à la main n'est pas nul non plus (en cas d'erreur, il suffit de renommer encore le fichier et de remettre l'extension correctement (par exemple, « .jpg » pour une photo)). Le problème, c'est que si on enlève l'extension d'un fichier, à moins de connaitre de mémoire le contenu et l'extension de ce type de contenu, il est difficile de remettre la bonne extension. Je recommanderai donc aux débutants de ne pas afficher les extensions et de suivre les instructions de la section Erreur : source de la référence non trouvée (Page Erreur : source de la référence non trouvée) lorsqu'ils voient un fichier avec uen extension alors qu'elles ne sont pas affichées (du coup, l'extension non affichée peut correspondre à un programme).

Autre dernière petite remarque : lorsque Windows ne connait pas une extension, il l'affiche. Donc il se peut que vous rencontriez un jour un fichier avec une extension, mais ça ne signifie pas non plus obligatoirement qu'il a une extension cachée.

Pour ceux qui se sentent moins débutants, les instructions pour afficher tous les fichiers sont disponibles à la section III.1.a (page 34).

II.4.d) Modifier l'exécution automatique

Section en construction

II.5) Les habitudes sur Internet

De la même façon que pour la gestion de ses fichiers, il faut aussi avoir de bonnes habitudes sur Internet.

II.5.a) Bien choisir ses mots de passe

Il est très important de bien choisir ses mots de passe.

Imaginons que vous choisissiez sur un site un mot de passe composé de cinq chiffres. Un programmeur mal intentionné pourrait tester votre mot de passe en moins de temps qu'il n'en faut pour le dire. Car il lui suffirait au maximum de 99999 essais (5 chiffres tous compris entre 0 et 9, il suffit de commencer à 0, puis d'ajouter 1 à chaque fois pour tomber au bout d'un moment sur le mot de passe) pour l'obtenir. A raison de plusieurs centaines d'essais par secondes (prenons 1000), l'ordinateur de ce programmeur peut trouver votre mot de passe en moins d'une minute et quarante secondes. Le chiffre de 1000 était vraiment loin de la vérité.

Supposons maintenant que votre mot de passe ne soit composé que de lettres toutes en minuscules. Pour un ordinateur de la même puissance pour trouver un mot de passe de cinq lettres, il faudrait 11881376 essais au maximum, soit un calcul de trois heures et vingt minutes pour tester toutes les combinaisons possibles.

Ce qui est déjà beaucoup plus long mais pas impossible.

Le truc à savoir, c'est que très souvent, les gens utilisent toujours par exemple le nom de leur chien, ou un mot existant. Du coup, il existe une autre technique permettant de trouver le mot de passe de quelqu'un : la technique du dictionnaire.

Cette technique consiste à tester le mot de passe avec une liste de mots.

Prenons par exemple une liste de deux millions de mots. Il faudra un peu plus d'une demi heure au maximum pour trouver votre mot de passe.

Tout ceci pour vous dire qu'il ne faut absolument pas choisir de mot de passe simple. Et

surtout pas de mot de passe composé uniquement de chiffres, ni uniquement de lettres.

Il vaut mieux choisir un mot de passe composé de lettres et de chiffres. Et il vaut même mieux qu'il y ait des lettres en minuscules et en majuscules dans votre mot de passe, voir des symboles autres comme un espace, un point (simple, d'interrogation, d'exclamation), un #, une virgule, ou tout autre symbole accessible sur votre clavier. Une taille minimale à respecter pour un mot de passe serait de huit caractères (d'ailleurs, bon nombre de sites imposent ce nombre minimal de caractères pour des mots de passe maintenant).

Il existe une technique simple pour créer un mot de passe sûr et facile à retenir en six étapes :

1*)* Imaginez une phrase que vous pourrez mémoriser. Elle servira de point de départ à l'élaboration de votre mot ou phrase de passe. Choisissez une phrase facile à mémoriser, par exemple : « Mon fils Olivier a trois ans ».

2*)* Vérifiez si votre ordinateur ou votre système en ligne accepte cette phrase. Si vous pouvez effectivement utiliser une phrase de passe (avec des espaces séparant les caractères) sur votre ordinateur ou sur votre système en ligne, n'hésitez pas.

3*)* Dans le cas contraire, transformez la phrase de passe en mot de passe. Prenez la première lettre de chaque mot de cette phrase pour créer un mot, qui n'aura alors plus aucune signification. Avec l'exemple ci-dessus, vous obtenez : « mfoata ».

4*)* Brouillez les pistes en utilisant à la fois des minuscules et des majuscules, ainsi que des chiffres. Vous pouvez également inverser certaines lettres ou intégrer des fautes d'orthographe. Par exemple, dans la phrase ci-dessus, vous pouvez faire en sorte que le nom Olivier comporte une faute d'orthographe, ou bien remplacer le mot « trois » par le chiffre 3. De nombreuses possibilités de substitutions s'offrent à vous ; et n'oubliez pas : plus la phrase de départ est longue, plus le mot de passe pourra être complexe. La phrase peut ainsi devenir « Mon FilS OlivI6R à 3 aNs ». Si votre ordinateur ou votre système en ligne n'accepte pas les phrases de passe, utilisez la même technique sur un mot de passe plus court. Vous pouvez alors obtenir un mot de passe du type « MfOa3a ».

5*)* Enfin, il est conseillé d'avoir recours à des caractères spéciaux. Vous pouvez utiliser des symboles ressemblant à des lettres, accoler des mots (en supprimant les espaces). Pensez à toute autre méthode permettant d'augmenter la complexité du mot de passe. En appliquant ces astuces, on obtient par exemple une phrase de passe comme « Mon€ilS O10R @ 3 An$ » ou un mot de passe (reprenant la première lettre de chaque mot) tel que « M€Oa3A ».

6*)* Testez tout nouveau mot de passe à l'aide d'un testeur de mots de passe.

<u>Stratégies à éviter</u>

Les criminels connaissent la plupart des méthodes de création de mots de passe les plus répandues. Pour éviter les mots de passe de faible niveau de sûreté, faciles à deviner :

- N'utilisez pas de suites ou de répétitions de caractères. « 12345678 », « 222222 », « abcdefg » ou une suite de lettres voisines sur le clavier forment des mots de passe relativement inefficaces.
- Évitez de remplacer des lettres uniquement par le chiffre ou le symbole leur ressemblant le plus. Les criminels et autres personnes mal intentionnées assez expérimentés pour essayer de pirater votre mot de passe ne se laisseront pas leurrés par l'emploi du chiffre« 1 » à la place d'un « i » ou du caractère « @ » à la place d'un « a », comme dans « N1nteñd0 » ou « m0tdep@88e ». Cependant, ce type de substitution peut se révéler utile s'il est associé à d'autres astuces permettant d'améliorer la sûreté du mot de passe, comme le fait de privilégier la longueur, l'ajout de fautes d'orthographe ou les changements de casse.
- N'utilisez pas votre identifiant de connexion. Il est fortement déconseillé de former un mot de passe à partir de tout ou partie de votre nom, de votre date de naissance ou de votre numéro de sécurité sociale, ou d'informations du même type relatives à vos proches. C'est souvent par là que les criminels commencent leurs manœuvres de piratage.
- Évitez d'employer des mots se trouvant dans le dictionnaire, même dans une autre

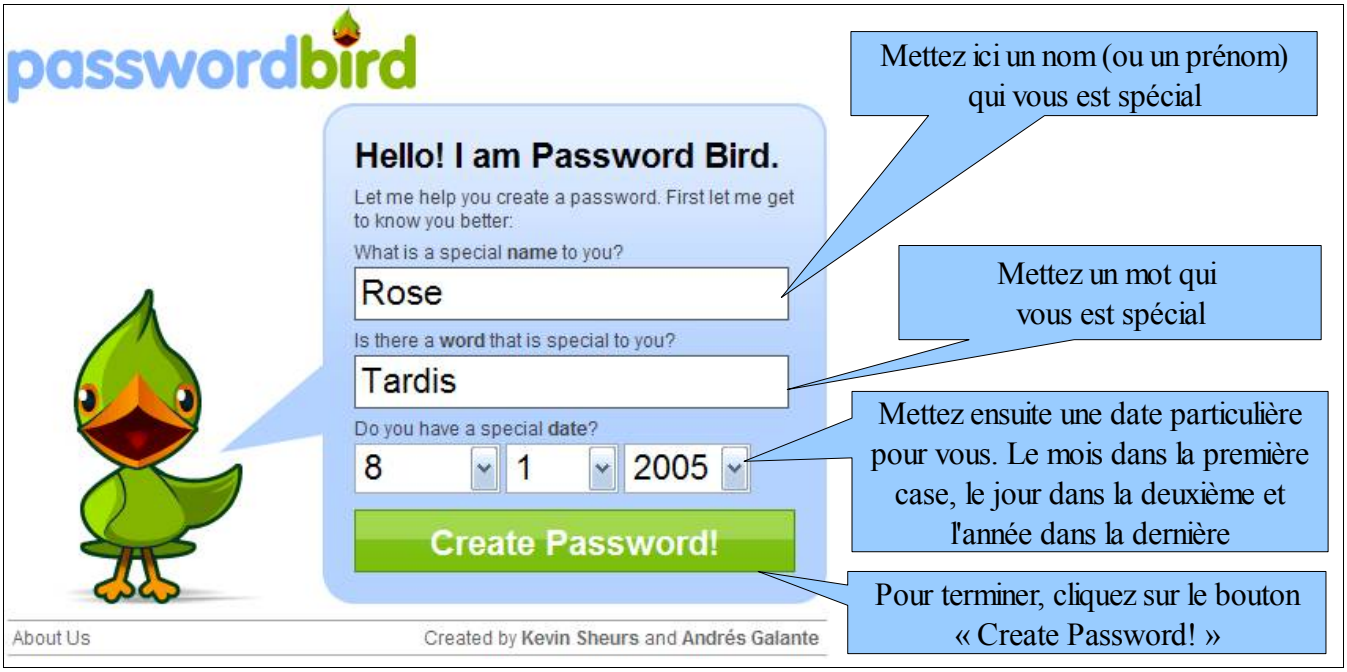
langue. Les criminels utilisent des outils sophistiqués pouvant deviner les mots de passe rapidement en se basant sur le contenu de différents dictionnaires et contourner les astuces consistant à écrire les mots à l'envers, à intégrer des fautes d'orthographe courantes ou à avoir recours à des substitutions de caractères. Sont également à exclure tous les types de jurons imaginables et les mots que vous ne dites jamais en présence de vos enfants.

- N'utilisez pas le même mot de passe partout. Si l'un des ordinateurs ou site Internet protégé par ce mot de passe est compromis, vous pouvez considérer que toutes vos informations personnelles protégées par ce mot de passe sont également compromises. Il est extrêmement important de créer un mot de passe différent pour chaque système.
- Évitez de stocker par écrit votre mot de passe dans votre ordinateur (ou un quelconque ordinateur sur Internet), car une personne piratant un site Internet ou même votre ordinateur pourrait retrouver le mot de passe stocké.

II.5.a.i) Un générateur de mots de passe simples à retenir

Ce générateur simple s'appelle passwordbird. Vous pouvez soit le rechercher avec votre ami Google, soit en recopiant ce lien dans la barre d'adresses de votre navigateur :

http://passwordbird.com/



Une fois sur la page du site, suivez les instructions marquées ci-dessus (j'ai mit un truc assez bidon dans l'image d'exemple).

Ce qui donne :

Si le mot de passe ne vous plait pas, vous pouvez cliquer sur le lien « Click here and I will make a new one! » afin qu'il en génère un nouveau avec les mêmes mots clés. Si vous voulez en générer un autre complètement nouveau, cliquez sur le lien « Click here and tell me different information! » (le deuxième lien).

N'hésitez pas à mettre un caractère spécial (ponctuation ou autre) pour augmenter la sécurité de votre mot de passe.

II.5.a.ii) Mais aussi bien choisir ses questions secrètes !

De nombreux services Internet (Hotmail, Windows Live Messenger, Gmail, ...) vous proposent un moyen de récupérer votre mot de passe. Ce moyen, c'est très souvent la question secrète.

Le concept :

Quand vous vous inscrivez à un service, vous choisissez un mot de passe, et vous choisissez/rédigez une question à laquelle vous donnez la réponse exacte (sinon, ça ne sers à rien).

Trois jours plus tard, vous vous rendez compte que vous ne vous rappelez plus de votre mot de passe car vous avez choisit le mot de passe le plus compliqué au monde. Du coup, vous cliquez sur un lien « Mot de passe oublié », ou tout autre lien ressemblant à ça. Ensuite, une question vous sera posé (la fameuse question secrète que vous avez choisi/rédigé). Vous devrez répondre exactement la même chose que le jour de votre inscription pour pouvoir recréer un mot de passe.

Le problème, c'est que le plus souvent, les gens mettent des réponses évidentes (un personnage de série TV alors que tout le monde sais que la personne est fan de cette série, ...).

Quand vous pouvez choisir la question, ne prenez pas quelque chose à quoi tout le monde vous connaissant (voire tout le monde tout court) pourrait répondre.

Prenez un truc qui sois extrêmement personnel, auquel seul vous pourra répondre, mais aussi un truc dont vous serez sûr de vous souvenir (pas votre personnage de fiction préféré par exemple, car ça peut changer).

Autre raison pour ne pas prendre un truc trop facile :

Si vous avez un blog, il est fort probable que vous parliez par exemple de vos animaux de compagnie. Si le nom de votre animal (ou un animal que vous aviez) apparaît dans votre blog, et que c'est la réponse à la question secrète d'un service sur lequel vous êtes inscrit, le risque de vous faire pirater votre compte est grand.

De même pour les mots de passe, c'est aussi une raison pour laquelle il ne faut pas prendre un simple mot ayant un sens pour vos comme mot de passe.

II.5.b) Ne pas télécharger tout ce qui vous est demandé de télécharger

Il arrive des fois, heureusement assez rarement, que certains sites proposent d'analyser votre ordinateur alors que vous n'avez rien demandé à personne. Ne le faites pas ! Il y a de grandes chances que ça ne soit pas un produit qui analysera votre ordinateur, qui vous dira qu'il y a des cochonneries et qu'il faudra acheter pour retirer les cochonneries qu'il n'y a pas dans votre ordinateur.

Si vous voyez une telle page, fermez votre navigateur. Et surtout, ne téléchargez pas ce qui vous sera proposé. Sous peine d'être infecté !

De même si vous êtes sur un site vous proposant de visionner une vidéo. Si le site vous demande de télécharger un (ou plusieurs) codec, ne le faites pas via ce site. Il est très probable que vous n'installiez aucun codec via ce site, mais tout un tas de cochonneries que vous n'aurez pas demandé.

Ce genre de cochonneries est d'autant plus efficace sur des navigateurs anciens (comme Internet Explorer 6 et antérieurs) qui à cause de mauvais réglages, téléchargent automatiquement la cochonnerie qui infectera votre ordinateur.

II.5.c) Ne pas laisser son adresse e-mail sur les forums ou dans les commentaires

Il est très facile pour une personne malintentionnée de créer un programme qui ira partout sur Internet dans le but de repérer des adresses e-mail, car toutes les adresses ont la même forme.

Il vaut donc mieux éviter de laisser son adresse e-mail en direct sur un forum, ou dans les zones de commentaires de certains sites. Utilisez de préférence les systèmes d'envoi de messages privés si vous souhaitez contacter une personne en particulier sur un blog/forum/zone de commentaire lorsqu'un tel système existe.

Dans le cas ou vous voudriez tout de même laisse une adresse e-mail, il existe plusieurs façons plus ou moins simple pour le faire :

- Créer une image qui contient votre adresse, et poster cette image sur la page désirée
- Ajouter un morceau qu'un humain pourra facilement voir qu'il faut le retirer :
  par exemple : truc.machin(nospam)@gmail(nospam).com
  Un être humain saura qu'il doit virer les « (nospam »
- Ne mettre ni point, ni arobase (le @), ou pas :
  par exemple : truc point machin arobase gmail point com
  en anglais, le « . » se dit « dot », et l'arobase est souvent abrégé en « at » aussi bien en anglais qu'en français

II.6) Quelques conseils pour les e-mails

Beaucoup de personnes reçoivent régulièrement de nombreux e-mails dans leurs boîtes de réception. Tous ne sont pas sans dangers. Voici quelques explications sur quelques types d'e-mails que vous pourriez trouver dans votre courrier.

II.6.a) Faire attention aux e-mails avec pièces jointes

Parmi les mails auxquels il faut faire attention, il y a ceux contenant des pièces jointes.

Première règle de base, n'ouvrez pas une pièce jointe d'un mail dont vous ne connaissez pas l'expéditeur !

Et même si vous connaissez l'expéditeur, il faut aussi se méfier : il existe de nombreux virus qui regardent le carnet d'adresse des gens pour s'envoyer automatiquement en pièce jointe chez les personnes du carnet d'adresse. Du coup, vous pourriez très bien recevoir un mail d'une personne que vous connaissez très bien, mais qui contient un virus.

Il y a plusieurs signes permettant de détecter ça :

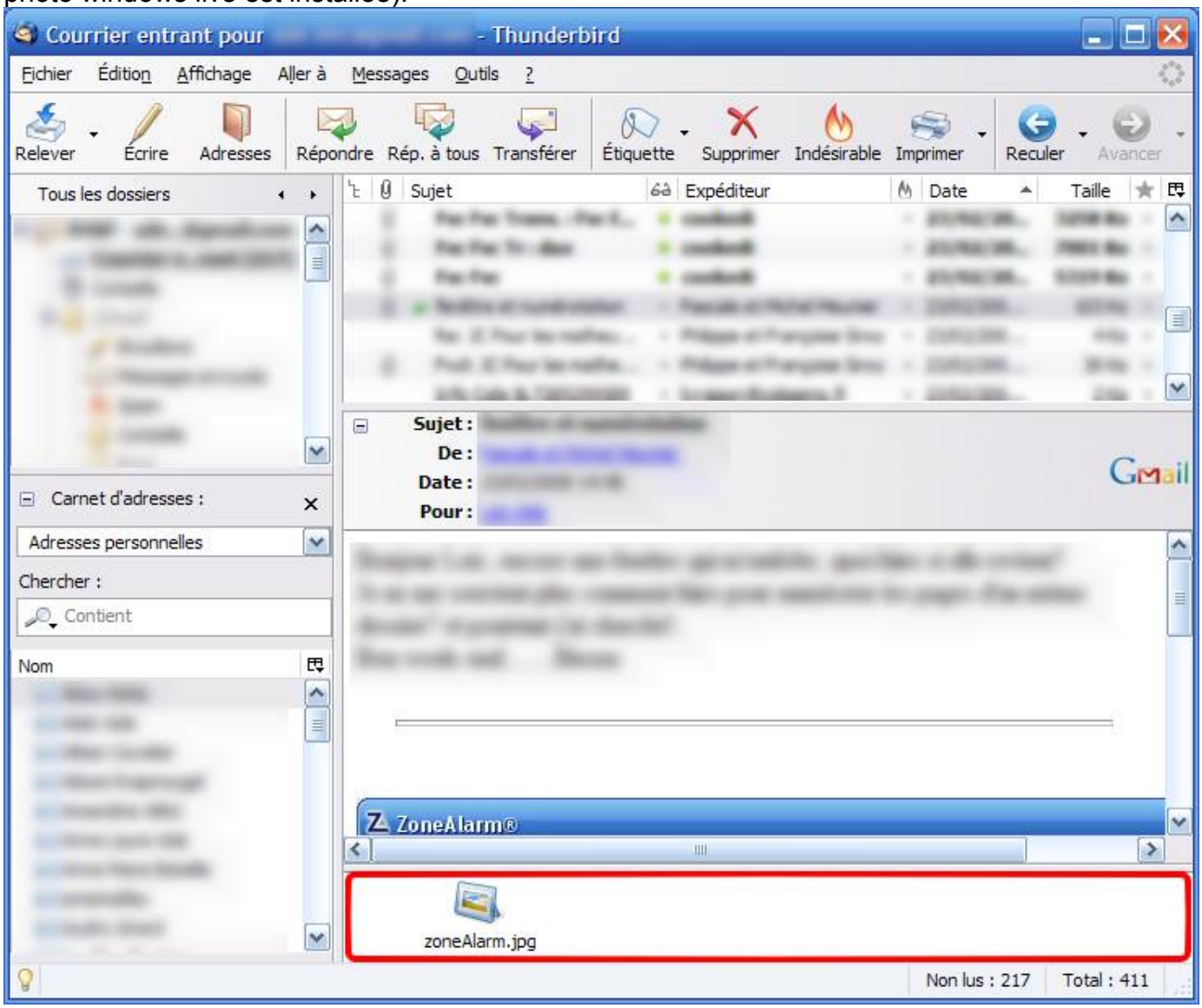
- le mail est écrit en anglais alors que la personne ne comprend pas un mot de cette

langue (valable pour n'importe quelle autre langue que l'anglais)

- le mail est écrit en français parfait alors que la personne écrit toujours ses mails en SMS ou avec un français avec plein de fautes (cette situation est quand même peu probable)
- l'inverse, donc que le mail soit écrit en SMS ou en français très approximatif alors que la personne emploie toujours un français parfait (ce qui peut être plus fréquent)
- vous avez reçu plusieurs fois le même e-mail louche

Autre moyen de faire attention avec les pièces jointes :

Si l'icône ne correspond pas au nom du fichier indiqué. Par exemple, l'icône de la seule pièce jointe du mail ci-dessous correspond bien à l'icône d'une image (lorsque la galerie de photo windows live est installée).



Il y a un autre petit truc auquel on peut faire attention : l'extension d'un fichier.

L'extension d'un fichier, c'est les quelques dernières lettres qui suivent le dernier point dans le nom d'un fichier. Malheureusement, Windows n'affiche pas automatiquement toutes les extensions de tout les fichiers, du coup, vous ne pouvez facilement connaitre l'extension d'un fichier dans l'explorateur Windows (Pour savoir comment afficher les extensions des fichiers, voir la section II.4.c page 19). Cependant, certains logiciels comme les logiciels de messagerie les affichent. C'est aussi à double tranchant : si vous avez un doute sur un fichier, que celui-ci affiche par exemple une extension « .jpg » et que l'icône est correcte, vérifiez sur d'autres mails sûr que le logiciel affiche bien l'extension.

Dans l'image précédente, on peut voir que l'extension du nom du fichier (zonealarm.jpg) est « jpg », ce correspond bien à une image.

Grâce à l'affichage de l'extension, vous pouvez voir si les pièces jointes sont suspectes.
Voici une liste des extensions de pièces jointes suspectes à n'ouvrir sous aucun prétexte :

- .exe
- .com
- .pif
- .cmd
- .bat
- .vbs
- .msi

Il y a quelques exceptions : les fichiers compressés, qui peuvent contenir d'autres fichiers. Dans ce cas là, il faut regarder l'extension de chaque fichier à l'intérieur de ce fichier compressé. Les fichiers compressés les plus répandus ont pour extension :

- .zip
- .rar
- .7z

Il existe d'autres formats de compression, mais il est peu probable que vous les trouviez en pièce jointe de mails.

De plus, le fait que ce soit une extension « .jpg » (extension correspondant à une image, souvent une photo) ne signifie en rien que le fichier soit sûr, car il existe des virus qui exploitent des failles de sécurité dans Windows afin de s'introduire dans votre ordinateur. Ces virus peuvent se cacher dans des images et le simple fait d'afficher / d'ouvrir la photo peut vous infecter ! Il est donc encore une fois très important de mettre à jour son ordinateur par les moyens officiels.
Les images aux formats EMF et WMF sont parfois vecteurs de virus. Donc si vous en recevez par mail, ne les ouvrez surtout pas à moins d'être vraiment sûr. Car très rares sont les personnes susceptibles de générer des images dans ces deux formats.
Bref, n'ouvrez jamais une pièce jointe de quelqu'un que vous ne connaissez pas. Car n'importe quel fichier peut abriter n'importe quel virus.

Si vous avez un doute sur la légitimité d'un message, n'hésitez pas à contacter (uniquement dans le cas ou vous connaissez la personne) l'expéditeur du mail pour savoir si le contenu d'un message est légitime.

II.6.b) Les chaines de messages

Une chaine de message est un mail qu'on vous demandera de transférer vous même afin de faire passer une information ou un message. Les personnes a qui vous enverrez le mail devront elles aussi transmettre le mail.
Le problème est que dans la plupart des cas, l'information du mail est fausse. Quand ce n'est pas une information, c'est souvent un message vous disant qu'il faut le renvoyer à plein de monde pour ne pas avoir tout le reste de votre vie un malheur immense qui s'abattra sur vous.

Nous allons voir les différentes raisons de ne pas les transmettre :

II.6.b.i) Les informations sont presque toujours fausses

Non non et non, Google ne vous enverra pas 100€ pour ses 10 ans si vous envoyer le mail à 15 personnes, Noëlie la petite fille est morte depuis le 1er juin 2004, Sony-Ericson n'enverra pas de téléphone aux gens envoyant le mail à 15 personnes différentes.

Ce ne sont que trois exemples récurrents de messages semblant vrais, mais qui dans les faits sont faux, ou sont devenus faux (le contenu du mail pour Noëlie était plus ou moins vrai au départ).

Commencez par apprendre à discerner le vrai du faux dans les mails :

- Le cas des mails à cadeaux :

Il est techniquement impossible pour une entreprise même aussi puissante que Google de vérifier que chaque personne a envoyé chaque mail autant de fois que désiré. La seule solution envisageable est que dans le mail, il y ait une adresse e-mail d'une personne travaillant dans cette entreprise, ce qui n'est jamais le cas. Et très souvent, dans ce genre de mails, il est demandé de faire du copier coller du contenu du message uniquement, et en plus, vous ne remettez dans les destinataires que les personnes de vos contacts (enfin, je dit ça pour les gens qui ont déjà renvoyé ce genre de mails), ce qui fait que personne chez Google ne peut savoir que le mail a été envoyé, et à qui il a été envoyé.

De plus, supposons qu'on soit 10 millions d'internautes en France. Supposons maintenant que un million de personnes envoient le mail. Croyez vous vraiment que Google va dépenser 100 millions d'euros comme ça ? De même, pensez vous vraiment que Sony-Ericson enverra vraiment un million de téléphones gratuitement à travers la France ? Sachant qu'un téléphone, ça ne coute pas rien, et que les frais d'envoi, comme de traitement des « cadeaux », ne sont pas donnés non plus.

Donc je vous en prie, ne transmettez pas ce genre de messages !

- Le cas des mails à virus :

Le contact truc_bidule_du_92@hotmail.fr n'est pas un virus. Dans le pire des cas, la personne ayant cette adresse à un virus sur son ordinateur, mais vous pouvez sans crainte lui envoyer des mails ou l'ajouter sur MSN. Vous ne risquez rien tant que vous êtes prudent après (voir les parties suivantes sur le comportement à avoir avec MSN et les pièces jointes des messages).

Il y a encore un autre type de « mails à virus », ceux disant de supprimer certains fichiers du disque dur. Ne le faite surtout pas ! Il s'agit souvent de fichiers tout à fait légitimes.

Le dernier type de mails à virus, c'est celui qui dit de ne pas ouvrir tel fichier car il s'agit (par exemple) du virus le plus méchant sur Terre car il détruira tout votre PC à la simple ouverture du fichier, et que ni Norton, ni McAfee n'ont jamais vu ! Ne craignez rien, je suis à peu près sûr que ces fameux virus n'ont jamais existé, ou alors, ça fait des années qu'ils sont reconnus par la plupart des antivirus (c'est surement plutôt ça d'ailleurs car ça fait des années que les mêmes mails trainent dans nos boîtes aux lettres). De plus, toujours avec un peu de prudence, ce genre de mail ne sers à rien, car il ne faut pas ouvrir une pièce jointe d'un mail d'une personne que vous ne connaissez pas.

Conclusion, ce genre de mails ne sers non plus à rien ! Faites lire ces quelques pages à la personne vous ayant envoyé le mail. Et ne transmettez pas ce type d'e-mail.

- Les mails des personnes ayant besoin de votre aide :

Ceux là sont les plus vicieux. Car très souvent, ils arrivent trop tard. Le cas de la petite Noëlie est le plus connu : celle ci est morte depuis plusieurs années maintenant, et de très nombreuses personnes continuent de transmettre les messages de demande de moelle osseuse, ...

Ou encore le cas d'une adolescente ayant fugué un jour. Un membre de sa famille a demandé à tout ses contacts de transmettre le message et donnait toutes les informations nécessaires pour contacter les parents. L'adolescente est rentré le lendemain chez elle, mais 5 ans après, la chaine ne s'arrête pas.

Conclusion : ne transmettez pas les messages de ce type ! Vous les recevez toujours bien après l'incident relaté dans le mail.

- Les pétitions :

Là encore, c'est assez drôle : parfois, dans certains mails, il est demandé d'ajouter au

bout du mail son nom et son prénom (et parfois d'autres informations plus ou moins inutiles) et de renvoyer le message à tout ses contacts. De la même façon que pour les mails cadeaux, les entreprises ou organisations n'ont aucun moyen de vérifier que le mail a été envoyé 5000 fois au total.

Mais dans tout les cas, ne renvoyez pas les mails de type pétition dans lesquels il suffit d'inclure son nom à la fin du message. Car en imaginant que l'entreprise ou l'organisation ayant commencé la chaine réussisse à pister les messages, le problème est que si vous envoyez un mail pétition à 15 personnes, ces 15 personnes ajouteront leur nom sur un seul des 15 mails. Du coup, il n'existera aucun mail comptant l'intégralité des coordonnées des gens. Et même si l'organisation ou l'entreprise pistait l'intégralité de ces messages (par exemple s'il faut ajouter l'adresse mail d'une des personnes de l'organisation/entreprise participant à la pétition), ça leur ferait donc des millions de mails différents contenant des millions de noms différents dont certains peuvent se retrouver au total des milliers de fois parmi tout les mails. Bref, c'est totalement ingérable (d'autant plus que les mails seront pratiquement tous différents à cause des pubs rajoutées par les sites/logiciels de messagerie, ou encore de la mise en page qui peut changer d'un site/logiciel de messagerie à l'autre).

Bref, n'envoyez pas les mails de type pétition.

- Le cas des mails de superstition :

Votre grand amour ne sera pas révélé en envoyant le mail à 142857 personnes différentes. De même, vous ne perdrez pas non plus l'amour de votre vie si vous n'envoyez pas le mail, ou vous n'aurez pas deux cents millions d'année de malheur en n'envoyant pas les mails de chaines !

Une personne de ma fac m'a fait une excellente remarque à propos des chaines de messages. Il a dit a ceux qui lui envoyaient ce genre de conneries (désolé pour ceux que ça choquera de lire ça, mais 100% de ces mails ne sont que destinés à faire chier le monde / voilà, mon coup de gueule est passé) que ce n'était pas être ami avec lui que de lui envoyer ce genre de mails, car en supposant qu'il y crois, ça l'oblige à réexpédier ce genre de mails à tout le monde s'il veut être tranquille.

Alors je vous en prie, arrêtez les chaines de type superstition ! Ces messages sont absurdes et très souvent sans le moindre fondement scientifique !

Si vous avez vraiment un doute sur la véracité du message, avant de casser les pieds aux gens, vérifiez l'information du message via le site hoaxbuster : http://www.hoaxbuster.com

Ce site recense toutes les chaines de messages que vous pouvez recevoir par e-mail. Un moteur de recherche vous permettra de trouver votre chaîne parmi toute la base de données, ainsi qu'une explication sur la chaîne.

Faites lire à vos enfants (à supposer que vous en avez bien entendu) au moins la partie sur les chaines de messages (vous pouvez bien entendu leur demander de tout lire). Car ce sont (par expérience) souvent les plus jeunes qui transmettent le plus ce genre de bêtises.

Et je vous en prie, prenez le temps d'aller sur le site hoaxbuster. Certaines chaines trainent depuis des années sur Internet (et traineront encore surement pendant très/trop longtemps) car les gens ne prennent pas le temps de vérifier la véracité de ce qu'ils envoient !

Pour conclure à propos des chaînes de messages, je dirai que tous ces types de messages (et bien d'autres encore que je n'hésiterai pas à ajouter) sont ce qu'on appelle des canulars, ou hoax en anglais (sauf les mails de type superstition qui ne sont qu'un pur concentré de bêtise humaine). Partez du principe de base que si dans le mail que vous recevez, il est demandé de le transmettre à tout vos contacts, alors ce message est un canular ou une ânerie.

Et ensuite, réfléchissez au contenu du message. S'il fait partie des catégories citées juste au dessus, alors il est inutile de le transmettre. Si vous avez un doute, vérifiez sur HoaxBuster.

II.6.b.ii) Encombrement des réseaux

Si vous envoyez un mail dont la taille fait environ 10 Ko à 10 personnes (ce qui fait 100 Ko sur des ordinateurs quelque part sur Internet), et que chacune de ces personnes envoie à son tour ce mail à 10 personnes (on atteint maintenant 1 Mo).

Ça peut aller vite ! D'autant plus que le message n'a été transmit que deux fois !

Imaginez maintenant qu'il soit transmit 10 fois à 10 personnes différentes à chaque fois.

Ça ferait 10Ko * 10 * 10 * 10 * 10 * 10 * 10 * 10 * 10 * 10 * 10, soit 100 To (Téraoctets) de données. Ce qui représente 69 444 444 disquettes !

Imaginons maintenant un e-mail de 5 Mo transmit autant de fois. On atteint la somme astronomique de 50 000 To de données, soit 34 722 222 222 disquettes.

Bref, évitez de transmettre les chaines de messages.

II.6.b.iii) La désinformation

Plus un fait est entendu, plus il parait vrai sur Internet (l'exemple de la vidéo sur les jeunes qui font du popcorn avec quatre téléphones portables).

Certains particuliers ont vu une partie de leur vie privée exposée au public à cause de chaines de messages. Par exemple, il y a eu le cas d'une jeune fille qui a fait une fugue. Un de ses amis à envoyé un mail à tout son carnet d'adresses. La jeune fille est revenue le lendemain matin, pourtant l'e-mail est toujours en circulation des années après sur Internet.

Certaines entreprises ont aussi une mauvaise réputation à cause de chaines. Par exemple, es célèbres directeurs Andy et John annoncent la fermeture de MSN depuis sa création (Andy et John n'ont bien entendu jamais existé). Mais bon, Microsoft n'a pas une mauvaise réputation qu'à cause de MSN et des chaines qui circulent.

II.6.b.iv) Vous faites de la publicité

De nombreux logiciels de messagerie ou sites de messagerie par e-mail ajoutent au bout des messages une pub pour eux. C'est pour ça que des fois, vous avez une petite image animée envoyée à la fin de messages par des gens qui n'en ont pas la compétence technique. Ou même simplement à chaque mail de ces même personnes.

Bref, vous faites de la pub pour des messageries.

Mais vous faites aussi parfois de la pub involontaire (comme le coup des quatre portables qui font chauffer du popcorn, ce gros canular était en fait une publicité pour une entreprise vendant du matériel audio en Bluetooth). Les cas de ce genres sont assez nombreux.

II.6.b.v) Vous recevrez encore plus de spam et de chaines

Autre raison pour ne pas transmettre les chaines de messages : souvent, les gens se contentent de cliquer sur le bouton « Transférer » de leur logiciel de messagerie et d'ajouter des destinataires, ce qui provoque l'apparition complète dans le message de l'ancien e-mail avec toutes les adresses e-mail contenues dans le message original. Du coup, les spammeurs récupérant ces messages récoltent toutes les adresses e-mail et vous envoient des informations pour que vous puissiez acheter du viagra (donc du SPAM), ou même pour tenter de vous escroquer (phishing et autres arnaques de ce genre).

II.6.c) Que faire pour éviter de recevoir trop de spam

II.6.c.i) Attention aux inscriptions !

Lorsque vous vous inscrivez sur un site Internet pour un concours ou une newsletter, il n'est pas rare qu'il vous soit proposé de recevoir les bons plans des partenaires commerciaux de l'entreprise qui gère le concours ou qui envoie la newsletter.

Faites bien attention à ces cases à cocher (ou à décocher, car les cases sont bien souvent déjà cochées pour vous) car vous pourriez recevoir plus de mails que vous n'en avez

demandé.

II.6.c.ii) Avoir plusieurs adresses e-mail

Avoir plusieurs adresses e-mail permet de préserver certaines du spam.

L'idéal serait d'avoir trois adresses e-mail :

- une pour les amis et la famille
- une pour les sites internet de confiance
- et une dernière adresse poubelle qu'on utilise pour les sites dont on n'est pas sûrs.

Ceci permettrai de pouvoir facilement changer d'adresse e-mail sans risquer d'inonder de spam l'adresse qui vous sers pour vos amis ou votre famille.

Pour les sites auxquels vous auriez donné l'adresse poubelle, rien ne vous empêche d'aller sur le site auquel vous vous êtes inscrit et de fournir l'adresse des sites de confiance si vous ne recevez pas de spam de leur part.

Cette technique est assez efficace mais aussi contraignante car elle suppose la gestion de plusieurs comptes e-mail. Il existe une autre technique moins contraignante : les adresses e-mail jetables. Spamgourmet permet d'avoir autant d'adresses jetables que vous voulez.

II.6.c.iii) Spamgourmet

Spamgourmet permet d'avoir des adresses jetables pour pouvoir vous inscrire sur tous les sites que vous voulez sans avoir de spam dans votre boite e-mail. Spamgourmet fonctionne avec un principe de redirections limitées : l'adresse que vous créerez permettra de rediriger un nombre limités de messages vers votre boîte e-mail réelle.

Avec Spamgourmet, vous pourrez décider de rediriger vers votre boîte e-mail réelle entre 1 et 20 messages. Si quelqu'un tente de vous envoyer un mail avec une adresse jetable spamgourmet et que la limite est dépassée, vous ne recevrez jamais ce mail.

II.6.c.iv) Instruire ses amis

Le problème des gens qui envoient des chaines de messages, c'est qu'ils transmettent parfois des dizaines (voire des centaines) d'adresses e-mail dans leurs messages.

J'ai reçu récemment un e-mail d'un contact qui avait laissé 79 adresses e-mail des personnes ayant précédemment transmit le message. Un autre encore plus récent : 326 adresses e-mail ! Je pensais que je n'aurai pas plus, eh bien non. J'ai reçu un mail qui a été transmis à au moins 505 personnes !

Heureusement pour ces 79, ces 326 et ces 505 personnes que je suis pas un spammeur, sinon, j'aurai pu leur envoyer des e-mails pour acheter du viagra.

Donc quand vous transmettez un message, veillez à bien supprimer les différentes adresses e-mail qui apparaitraient dans le message afin d'éviter de recevoir du spam.

Comme ça, vous serez sûr que d'autres personnes ne recevront pas non plus de spam par votre faute.

Et veillez bien à utiliser aussi le champ Cci (pour Copie Cachée invisible) ou Bcc de votre site ou logiciel de messagerie électronique (voir section II.6.c.v page 29) !

II.6.c.v) Utiliser le champ Cci de votre site/logiciel de messagerie

II.6.c.vi) Ne pas afficher directement son adresse e-mail sur Internet

Les spammeurs ont une technique pour obtenir des adresses e-mail : l'analyse des pages Internet.

Il n'est pas rare que des gens laissent directement leur adresse e-mail sur des blogs ou des forums, ou même sur leur propre site.

Du coup, les spammeurs créent des robots qui parcourent le web à la recherche

d'adresses e-mail complètes. Mais il existe plusieurs techniques qui permettent d'éviter qu'un robot ne récupère votre adresse e-mail :

- écrire son adresse comme on la prononce :
  Par exemple : truc arobase machin point fr
- ajouter un mot (ou plusieurs) entre caractères spéciaux :
  Par exemple : truc(veut-pas-de-spam)@machin.fr
- écrire son adresse dans une image et afficher cette image plutôt que l'adresse en texte

II.6.c.vii) Quelques principes de bases à appliquer pour ne pas se faire avoir

Jamais aucun site ni aucun organisme ne vous demandera par e-mail ou tout autre moyen que ce soit de devoir entrer quelque part vos informations personnelles et/ou bancaires que vous auriez déjà pût entrer une première fois auparavant.

Si vous avez un doute, n'hésitez pas à aller sur le site officiel de la banque / de l'organisation / de l'entreprise concernée (en passant par Google, pas en cliquant sur les liens dans le mail bien entendu). Allez ensuite voir si ce site dispose d'une rubrique avec des actualités afin de voir s'il n'y a pas une vague de tentative d'arnaque par mail. Si le site ne dispose pas d'actualités, n'hésitez pas à les contacter (toujours en passant par le site officiel, un numéro donné dans un mail de ce type peut aussi être frauduleux) afin d'obtenir plus de renseignements, ou pour demander si le mail reçu est légitime.

Autre chose : si le message reçu est dans un français très approximatif, avec parfois des mots dans n'importe quelle langue autre que le français, méfiez vous ! Il s'agit sans doutes d'un faux.

En voici un très bel exemple :

Déjà, ce mail a quelques problème avec les lettres accentuées (il n'y en a aucune comme vous pourrez le remarquer). De plus, la traduction depuis l'anglais est imparfaite (voir cadre orange de l'image ci-dessus). Enfin, si vous passez la souris au dessus des liens qui sont dans ces mails, vous verrez dans votre logiciel de messagerie (ou sur le site sur lequel vous êtes pour lire vos e-mails) que l'adresse du site est très louche (voir cadre bleu). Par exemple dans ce mail, l'adresse réelle du site (ce qu'il y a entre le « http:// » et le premier slash (le symbole « / »)) est « womum.co.nz », ce qui ne ressemble absolument pas à PayPal. Ce qui suit « womum.co.nz » (« www.PayPal.fr ») ressemble beaucoup plus à PayPal, mais ce n'est absolument pas l'adresse réelle du site, et il ne faut donc pas y faire attention.

Un autre moyen est de regarder l'adresse e-mail de l'expéditeur. Si vous recevez un message qui semble venir de PayPal mais que l'adresse de l'expéditeur se termine en « @yahoo.com », alors il est très probable que vous ayez reçu une tentative de phishing.

II.6.d) Que faire une fois qu'on en reçoit des e-mails indésirables ?

II.6.d.i) Se désinscrire

Vous recevez toujours les mêmes messages que vous n'avez jamais demandé de la même entreprise et un lien de désinscription est présent dans les messages ?

Réfléchissez-y à deux fois avant de vous désinscrire. Car dans la plupart des cas, lorsque vous vous désinscrivez, vous confirmez votre adresse e-mail. Et vous confirmez donc que votre adresse existe, et qu'elle est donc apte à recevoir encore plus de messages.

La plupart des grandes entreprises envoyant des mails proposent un moyen de se

désinscrire, mais vous pourriez très bien avoir reçu un message se faisant passer pour un message d'une grande entreprise.

Quand c'est possible, passez plutôt par le site lui même pour vous désinscrire.

Si le site officiel ne vous propose pas de vous désinscrire, vous pouvez effectuer une recherche sur Internet afin de savoir s'il y a un risque à se désinscrire, ou si vous êtes tombé sur une tentative de spam.

Si le message est un spam, ne vous désinscrivez surtout pas. Il s'agit à coup sûr d'une technique qui permettra au spammeur de vous envoyer encore plus de spam.

II.6.d.ii) Changer de gestionnaire de courrier

Certains logiciels de messagerie assez anciens ne proposent pas de fonction antispam. Ce qui devient très vite handicapant si vous recevez plus de spams que de messages légitimes.

Outlook Express est un bon exemple de logiciel de messagerie sans antispam.

Si vous n'utilisez pas de logiciel de messagerie mais que vous allez directement sur Internet pour lire vos messages, et que le site ne propose pas non plus d'antispam, je vous recommande grandement l'usage d'un logiciel de messagerie comme Thunderbird, qui affichera mieux vos messages et qui vous permettra de mieux le gérer que sur certains sites de messagerie.

II.6.d.iii) Ou changer d'adresse e-mail

Si vous ne désirez pas changer de logiciel de messagerie et que votre site de messagerie ne propose pas d'antispam, vous pouvez opter pour une nouvelle boîte e-mail.

GMail est un très bon site de messagerie par e-mail qui propose un très bon antispam.

Il arrive aussi que même les meilleurs antispams ne parviennent pas à se débarrasser de tout le spam qui pourrait être dans vos messages. Il y a des personnes qui reçoivent parfois plusieurs dizaines de spams par jour, voire plus encore.

Il est donc parfois nécessaire de changer d'adresse afin d'être tranquille et de repartir sur de bonnes bases.

II.6.d.iv) Instruire vos amis (ou en changer)

Voir ici : section II.6.c.iv page 29

II.6.d.v) Appliquer un filtre pour les chaines

Si vos amis continuent d'envoyer des chaines de messages après que vous leur ayez demandé de ne plus le faire le font toujours, vous pouvez créer un ou plusieurs filtres pour supprimer automatiquement ces messages.

Vous vous demanderez surement comment reconnaître des chaines de messages. Eh bien la réponse est simple. L'objet d'une chaine de message commence à peu près toujours de la même manière :

- Fwd:
- [Fwd:
- Fw:
- Tr:

On peut donc demander à un logiciel de messagerie d'automatiquement supprimer un message écrit par une personne particulière dont l'objet commence par un des éléments que j'ai donné.

La plupart des logiciels de messagerie proposent ce genre d'options. De même pour quelques sites de messagerie.

Étant donné la quantité de logiciels de messageries différents et de sites de messagerie différents, nous ne verrons que la procédure pour Mozilla Thunderbird.

II.6.e) Conclusion des conseils sur les e-mails et arnaques similaires

Il y a donc plusieurs règles simples à respecter :

- Tout mail censé être sérieux (banque, site de vente/achat, fournisseur d'accès à Internet…) n'étant pas écrit dans un français parfait (ou presque parfait) est probablement un faux. Même chose pour un mail d'une connaissance qui contiendrai des mots d'une langue qu'il ne parle pas.
- Tout mail soit disant d'une grande entreprise X provenant d'une adresse gmail, yahoo ou d'un fournisseur d'adresse e-mail connu est un faux (par exemple, si free perdait vos identifiants de connexion, ils n'enverraient pas de mail à partir d'une adresse hotmail)
- Tout mail vous demandant vos coordonnées bancaires ou vos identifiants et mots de passe est un faux
- Toute personne qui se prétendra du service informatique de l'entreprise, qui vous demandera par mail ou par téléphone vos identifiants et mots de passe est probablement un arnaqueur
- Quand vous envoyez un mail à plusieurs personnes, n'hésitez pas à être discret, en masquant à chaque personne les autres destinataires

III) Quelques conseils – la pratique

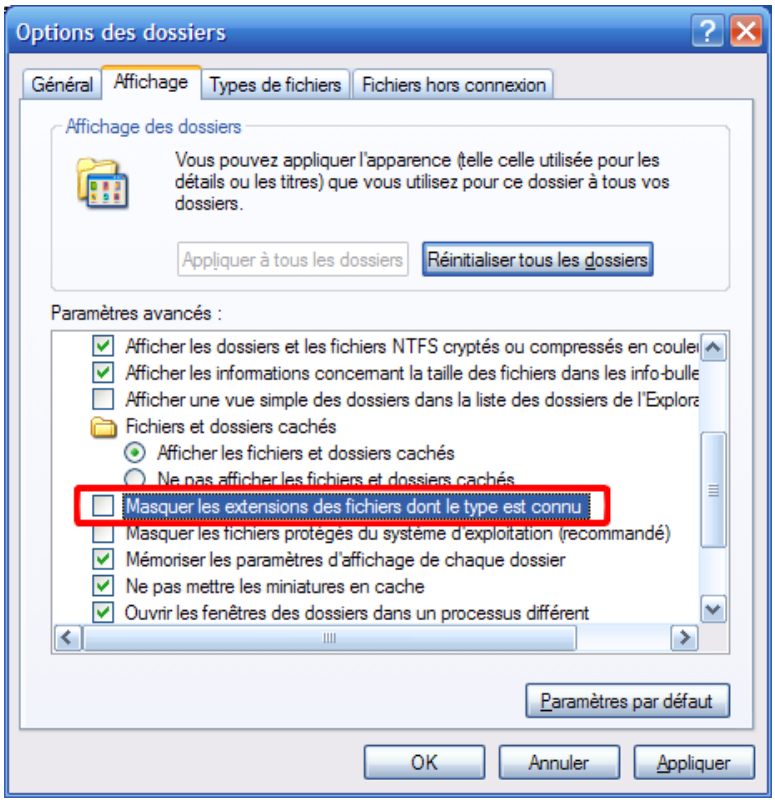
Maintenant que vous avez toutes les explications en main sur ce qu'il faut faire et ne pas faire, voyons certaines procédures afin d'appliquer ce que vous venez d'apprendre (ou que vous saviez peut-être déjà) :

III.1) La gestion des fichiers

III.1.a) Afficher l'extension de tous les fichiers - Procédure

Pour activer l'affichage des extensions de tous les fichiers, allez dans le « Panneau de configuration », puis dans « Options des dossiers » (voir la section précédente pour y accéder).

Allez ensuite dans l'onglet « Affichage » et décochez la case « Masquer les extensions des fichiers dont le type est connu » :

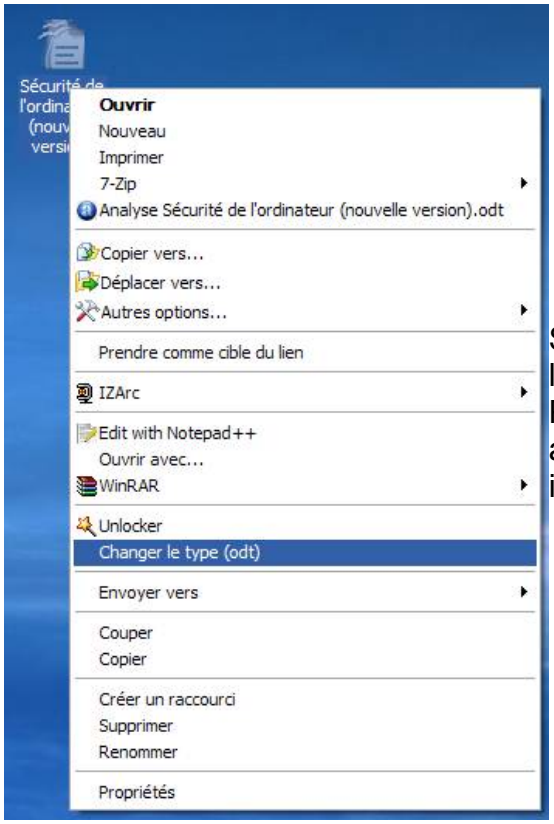


Cliquez sur le bouton OK.

III.1.b) Change Extension

Personnellement, je n'aime pas trop l'affichage des extensions, je trouve ça assez moche en plus du risque non négligeable de supprimer l'extension. J'ai opté pour une situation intermédiaire qui me permet d'afficher l'extension uniquement quand j'en ait envie, et qui me retire le risque de changer l'extension en renommant le fichier. Cette solution s'appelle Change Extension :

Il s'agit d'un petit logiciel qui apparait dans le menu contextuel (le fait de faire un clic droit sur le fichier dans l'explorateur Windows ou sur le bureau fait apparaitre un menu : le menu contextuel), qui affiche l'extension d'un fichier, et qui permet de la changer.



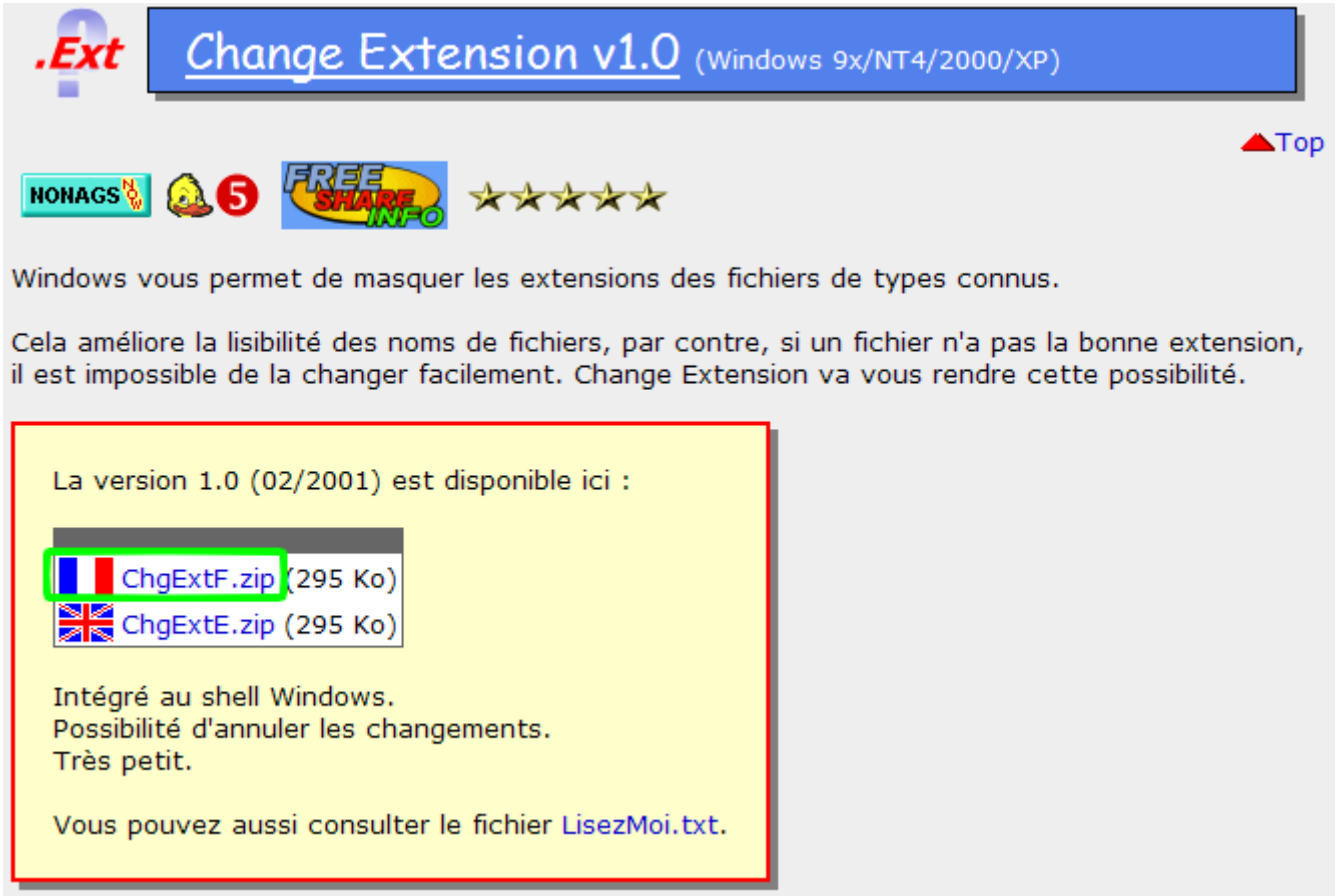
Si vous faites un clic droit, vous pouvez regarder si l'extension concorde au type du fichier.
Par exemple, si l'extension est « .exe » (le . n'est pas affiché par le logiciel) alors que l'icône correspond à une image, méfiez vous.

Installons Change Extension :
Recopiez cette adresse dans la barre d'adresses de votre navigateur Internet :
http://home.nordnet.fr/~pmdevigne/programmes.html#ChangeExtension

Ou alors, utilisez votre moteur de recherche préféré pour trouver ce résultat :

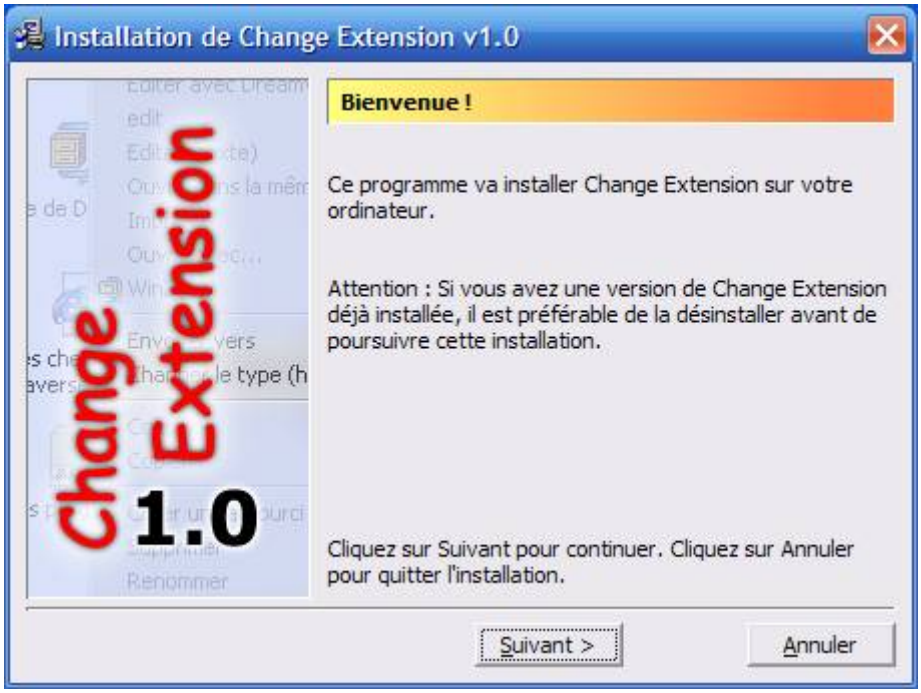
Mes logiciels
Cela améliore la lisibilité des noms de fichiers, par contre, si un fichier n'a pas la bonne **extension**, il est impossible de la **changer** facilement. **...**
home.nordnet.fr/~pmdevigne/programmes.html - 101k - En cache - Pages similaires

Dans la page sur laquelle vous arriverez, cliquez sur le lien « ChgExt.zip » (voir cadre vert de l'image ci-dessous) :

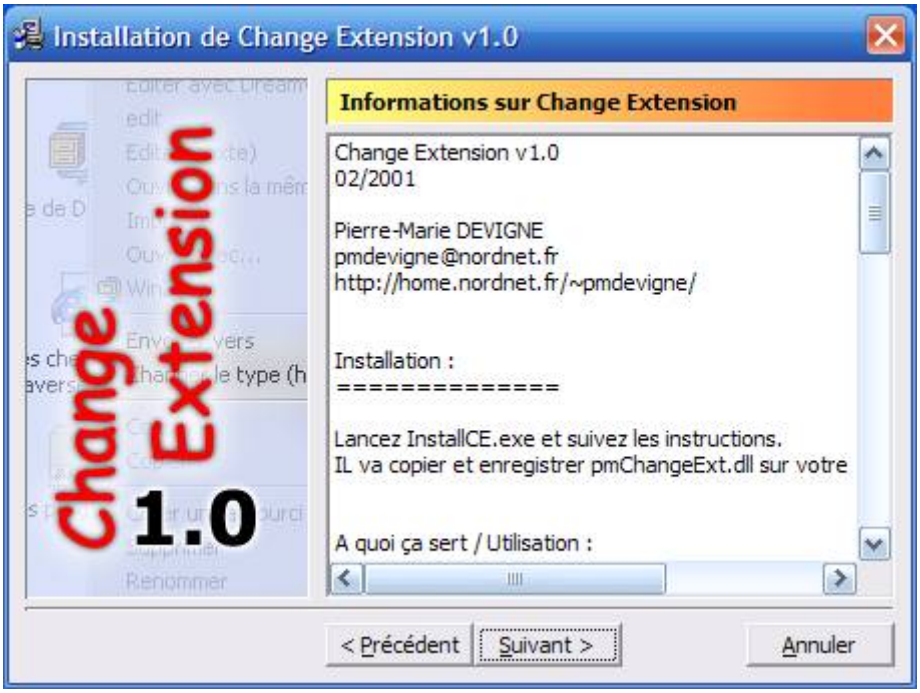


Téléchargez le fichier proposé.

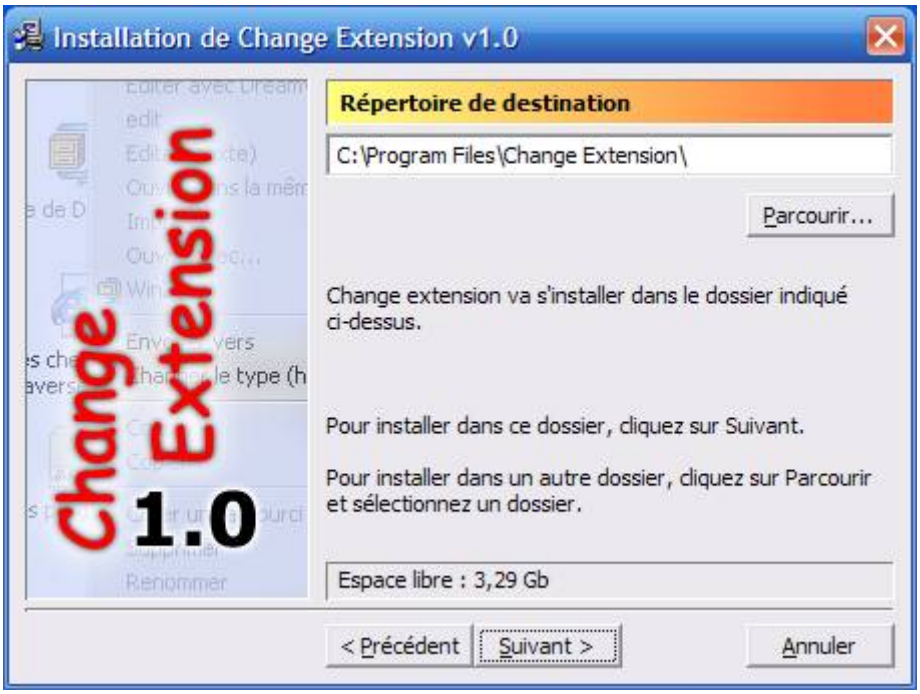
Ouvrez le, puis ouvrez ensuite le fichier « InstallCE » ou « InstallCE.exe ».



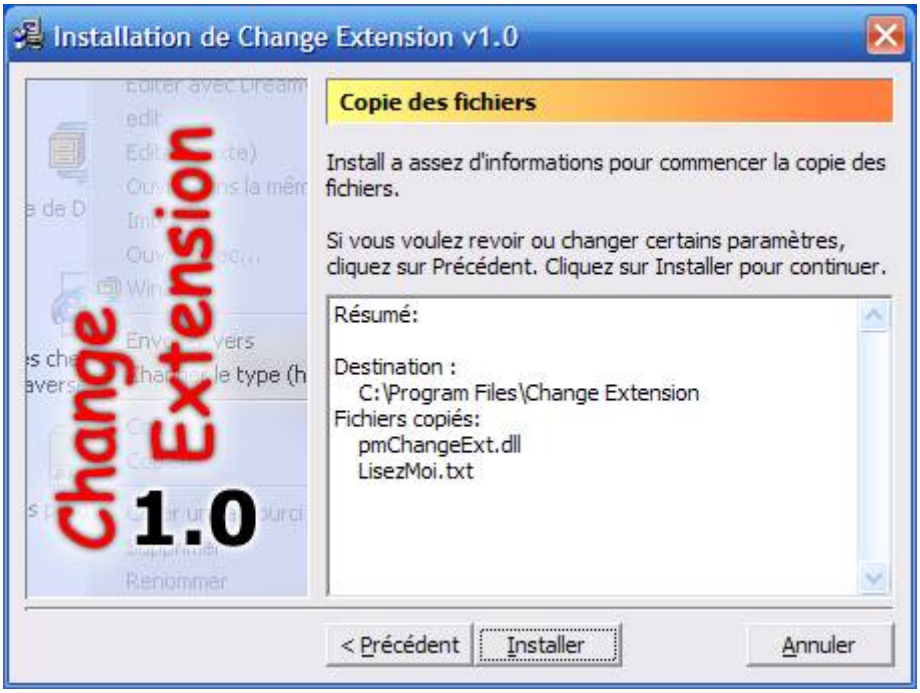
Cliquez sur le bouton « Suivant ».



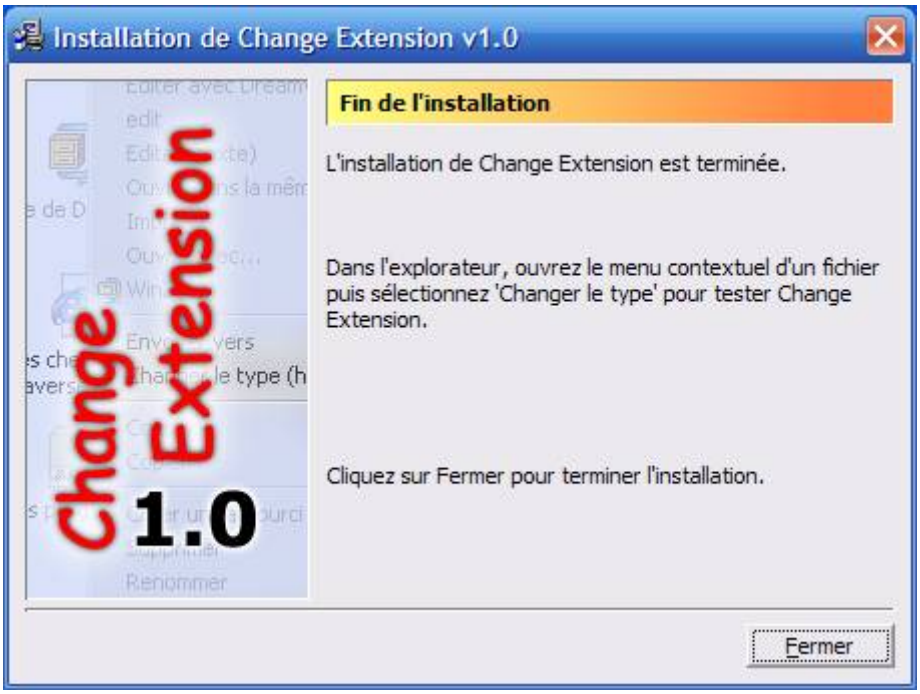
Cliquez encore sur le bouton « Suivant ».



Cliquez de nouveau sur le bouton « Suivant ».



Cliquez sur le bouton « Installer ».

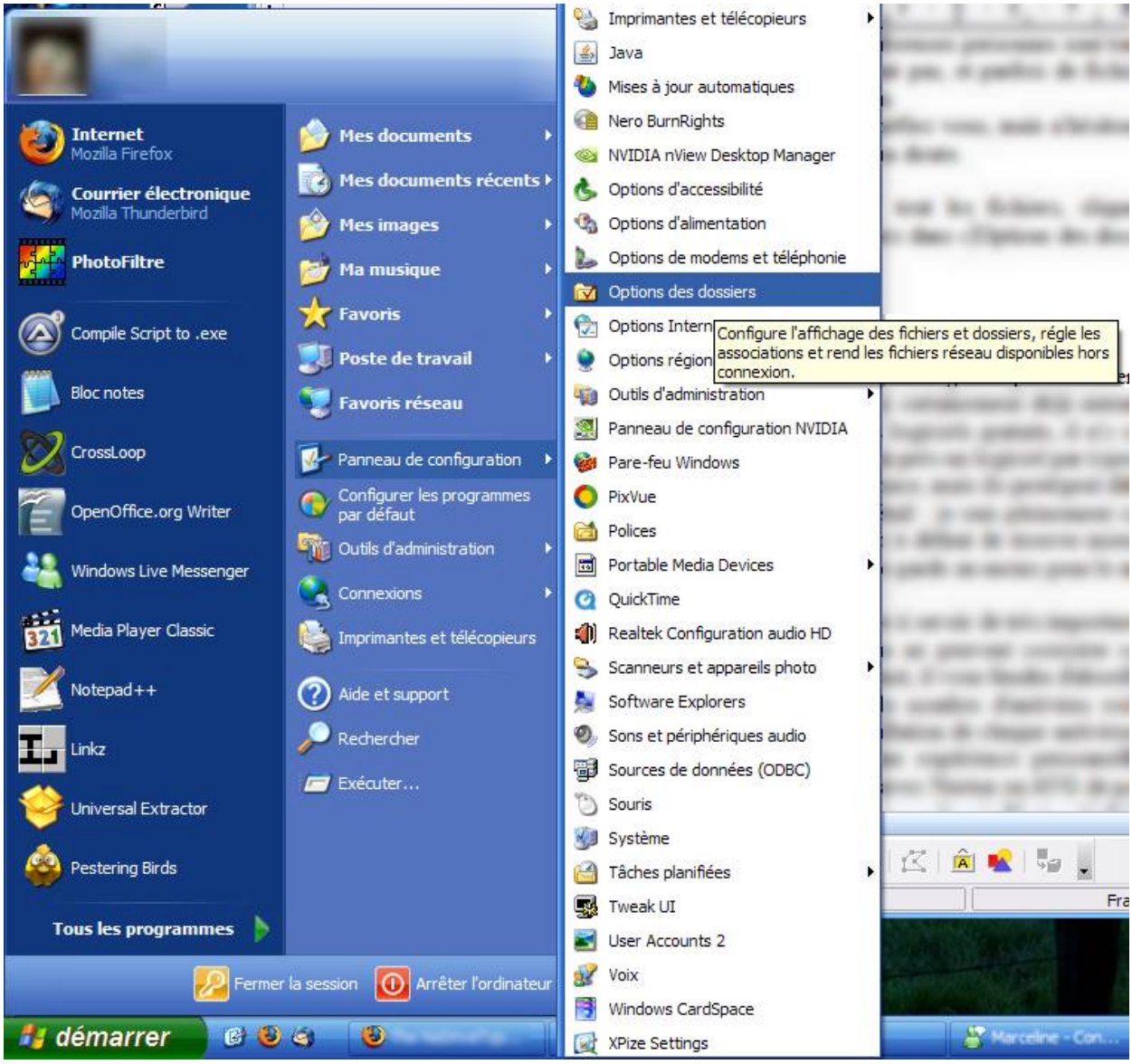


Cliquez maintenant sur le bouton « Fermer ».

Change Extension est maintenant installé.

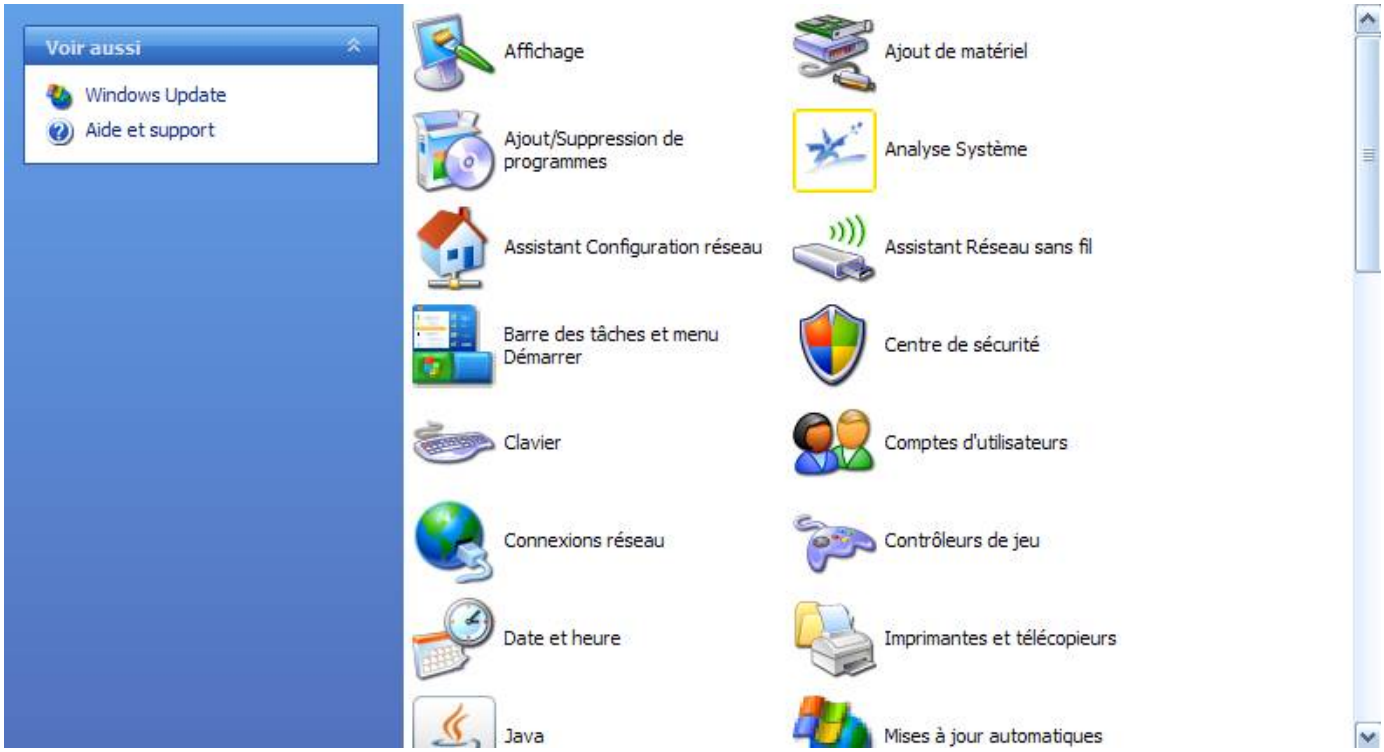
III.1.c) Afficher tous les fichiers – Procédure et remarques

Pour afficher tout les fichiers, cliquez sur le bouton « Démarrer », allez dans Panneau de configuration puis allez dans « Options des dossiers » :



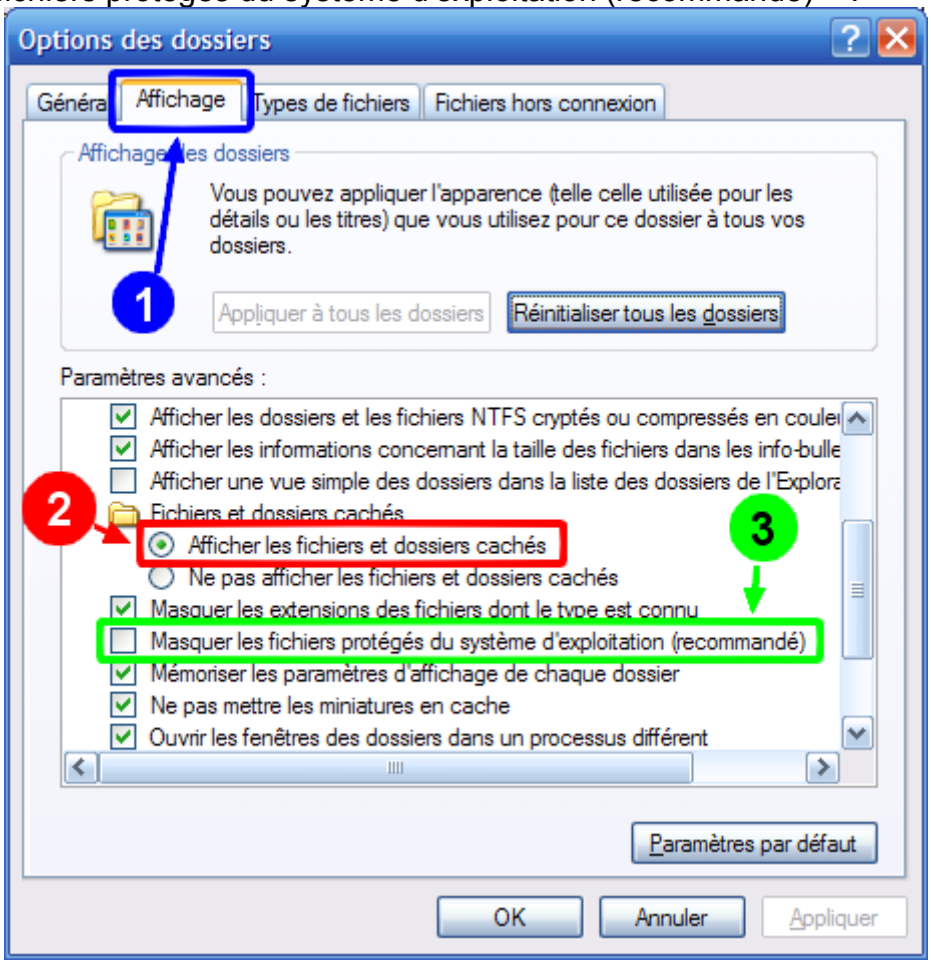
Si le panneau de configuration ne s'affiche pas en menu comme dans l'image ci-dessus, cliquez sur Panneau de configuration.

Si Options des dossiers n'apparait pas dans la partie droite de la fenêtre, cliquez sur « Basculer vers l'affichage classique » (dans la barre à gauche) :

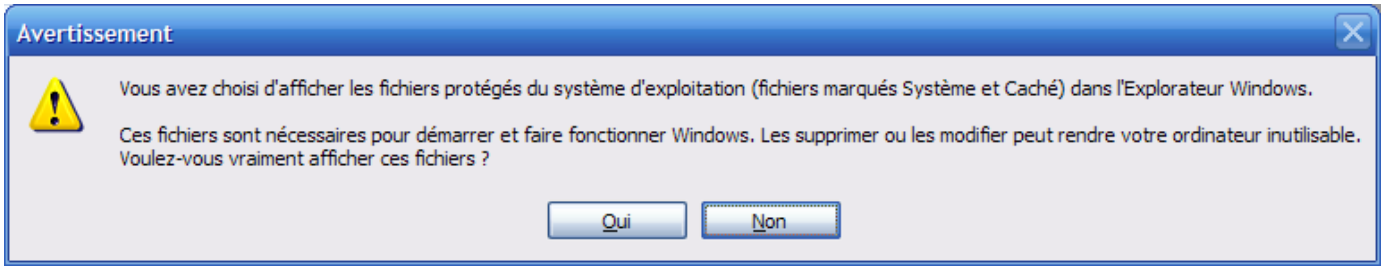


Ensuite, double cliquez sur « Options des dossiers ».

Cliquez sur l'onglet « Affichage » (voir cadre bleu de l'image ci-dessous), puis cochez la case « Afficher les fichiers et dossiers cachés » (voir cadre rouge), puis décochez la case « Masquer les fichiers protégés du système d'exploitation (recommandé) » :



Si la fenêtre suivante apparaît, cliquez sur « Oui »



Cliquez sur OK pour fermer la fenêtre « Options des dossiers » et valider les réglages.

Le cas de Windows Vista :

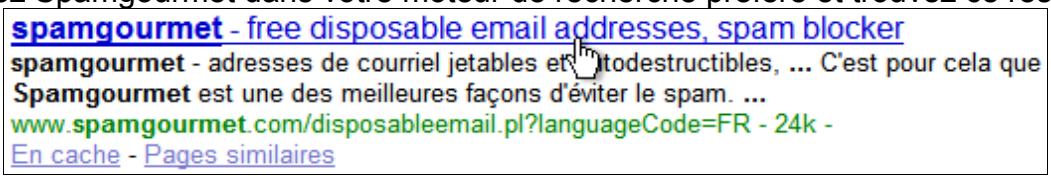
Par défaut, ce système d'exploitation crée de nombreux fichiers « desktop.ini » partout dans le système d'exploitation. Ceci permet à Windows Vista de cacher le vrai nom de certains dossiers. Par exemple, dans C:\, vous avez le dossier « Programmes ». Ce dossier est « un faux » dossier « Programmes », si vous supprimez le fichier « desktop.ini » de ce dossier, vous vous rendrez compte que celui-ci s'appelle en réalité « Program files » (comme avant sous Windows XP).

Les plus inutiles sont ceux qui apparaissent sur le bureau. Vous pouvez sans crainte supprimer ces deux fichiers. De même, quand vous gravez un CD avec Vista, il y a un fichier « desktop.ini » créé automatiquement (ou même seulement si vous mettez un CD sans rien graver). Supprimez le aussi sans soucis.

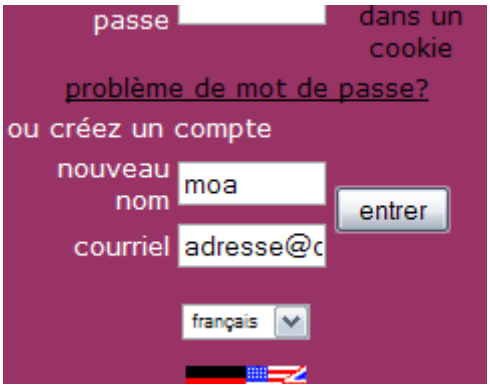
III.2) Les e-mails

III.2.a) Spamgourmet - Inscription

Tapez Spamgourmet dans votre moteur de recherche préféré et trouvez ce résultat :



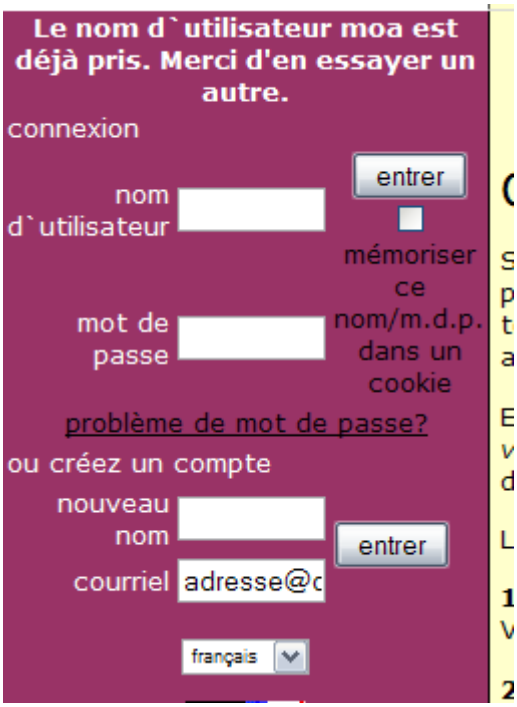
Dans la partie gauche de ce site, il est possible de se connecter pour régler quelques paramètres, mais il est aussi possible de s'inscrire maintenant :



Dans la zone « nouveau nom », mettez le nom d'utilisateur que vous désirez (sans lettres accentuées, ni espaces ou caractères spéciaux) et dans la zone « courriel », mettez votre adresse e-mail.

Cliquez ensuite sur le bouton « entrer ».

Si le nom d'utilisateur que vous avez entré est déjà pris par quelqu'un, un message vous avertira :



Dans ce cas recommencez l'opération.

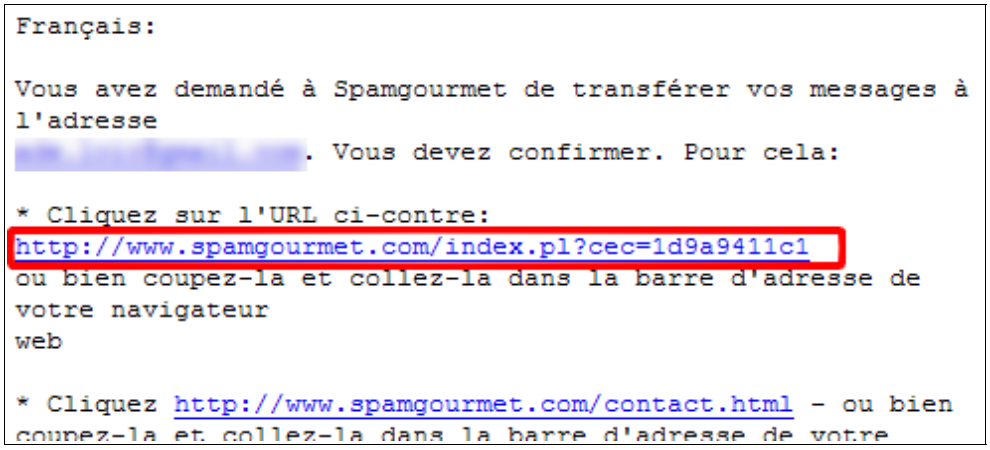
Si le nom d'utilisateur que vous avez choisi n'a pas déjà été pris par quelqu'un d'autre, alors la page devrait ressembler à ceci :

Dans la zone de texte « entrez le contenu dans l'image », tapez les lettres et chiffres dans le même ordre que ceux qui sont dans l'image.

Dans la zone de texte « nouveau m.d.p », tapez un mot de passe (n'hésitez pas à suivre les recommandations données à la section II.5.a page 19 pour créer un bon mot de passe) et retapez le dans la zone du texte juste en dessous.

Cliquez ensuite sur le bouton « entrer ».

Un message de validation a été envoyé dans votre boîte e-mail (n'hésitez pas à regarder dasn les spams car ce message a été considéré comme un spam par Gmail). Cliquez sur le lien pour valider l'inscription :



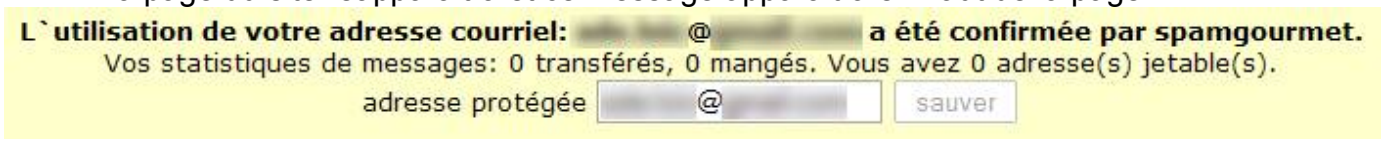
Français:

Vous avez demandé à Spamgourmet de transférer vos messages à l'adresse
. Vous devez confirmer. Pour cela:

* Cliquez sur l'URL ci-contre:
http://www.spamgourmet.com/index.pl?cec=1d9a9411c1
ou bien coupez-la et collez-la dans la barre d'adresse de votre navigateur
web

* Cliquez http://www.spamgourmet.com/contact.html - ou bien coupez-la et collez-la dans la barre d'adresse de votre

La page du site réapparaitra et ce message apparaitra en haut de la page :



L`utilisation de votre adresse courriel: @ a été confirmée par spamgourmet.
Vos statistiques de messages: 0 transférés, 0 mangés. Vous avez 0 adresse(s) jetable(s).
adresse protégée @ sauver

Vous pouvez utiliser Spamgourmet dès maintenant !

III.2.b) Spamgourmet - Utilisation

Spamgourmet est très simple à utiliser. Il n'y a qu'une seule chose à se rappeler :
unmot.x.utilisateur@spamgourmet.com

Vous remplacez « unmot » par ce que vous voulez (que des lettres et/ou des chiffres), x par un nombre compris entre 1 et 20, et vous remplacez « utilisateur » par votre nom d'utilisateur.

Par exemple, si vous vous êtes inscrit avec le nom d'utilisateur « moi » et que vous voulez que le site « siteaconcours » (totalement fictif comme exemple) ne puisse vous envoyer que 5 messages maximum, voici un exemple d'adresse que vous pouvez utiliser :
siteaconcours.5.moi@spamgourmet.com

Il ne faudra plus utiliser ce mot dans une nouvelle adresse. Pour augmenter le nombre d'adresses possibles avec un mot donné, vous pouvez ajouter la date à la fin du mot que vous avez choisi avant le premier point, comme ceci par rapport à l'exemple précédent :
siteaconcours310109.5.moi@spamgourmet.com

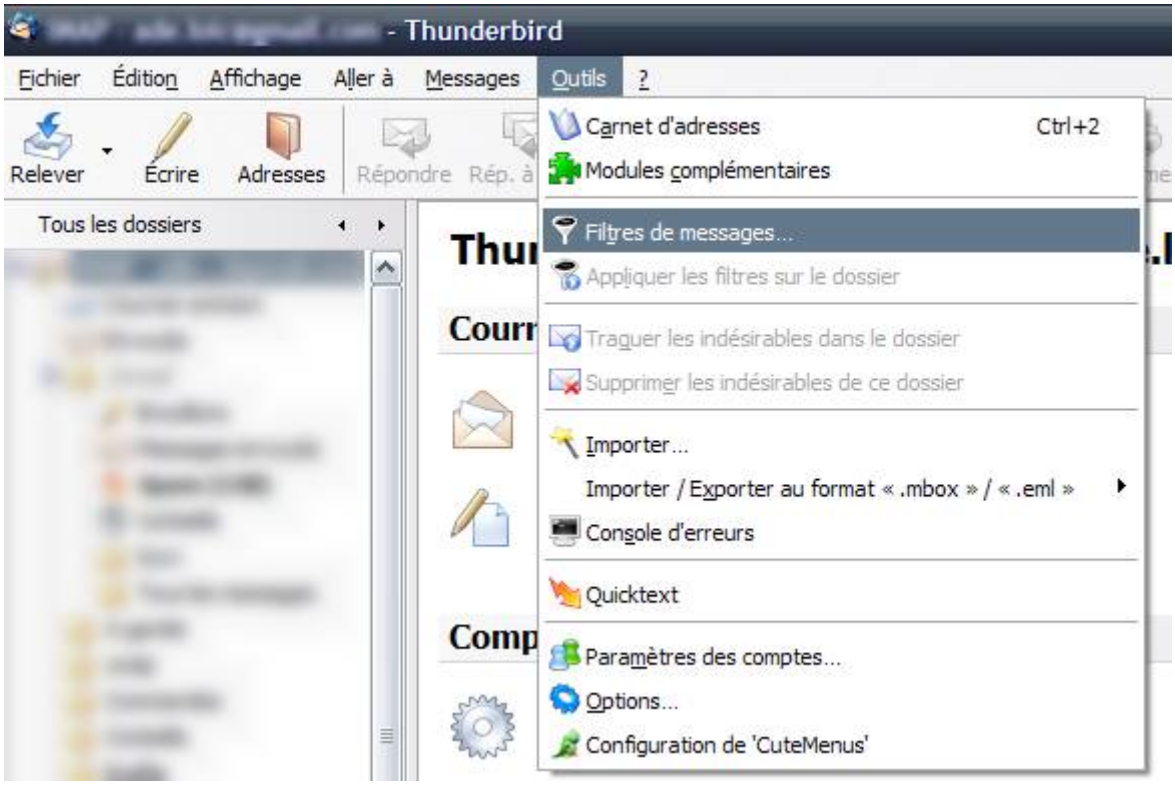
Spamgourmet est fonctionnel 24h/24 sans aucune configuration particulière. Normalement, vous ne devriez jamais avoir besoin de retourner sur leur site.

Les e-mails qui seront envoyés aux adresses jetables arriveront dans votre boîte aux lettres avec un changement dans l'objet des messages. Ce changement indique le nombre de messages envoyés ainsi que le nombre de messages qui peuvent être envoyés sur l'adresse jetable.

III.2.c) Chaines de messages – Appliquer un filtre

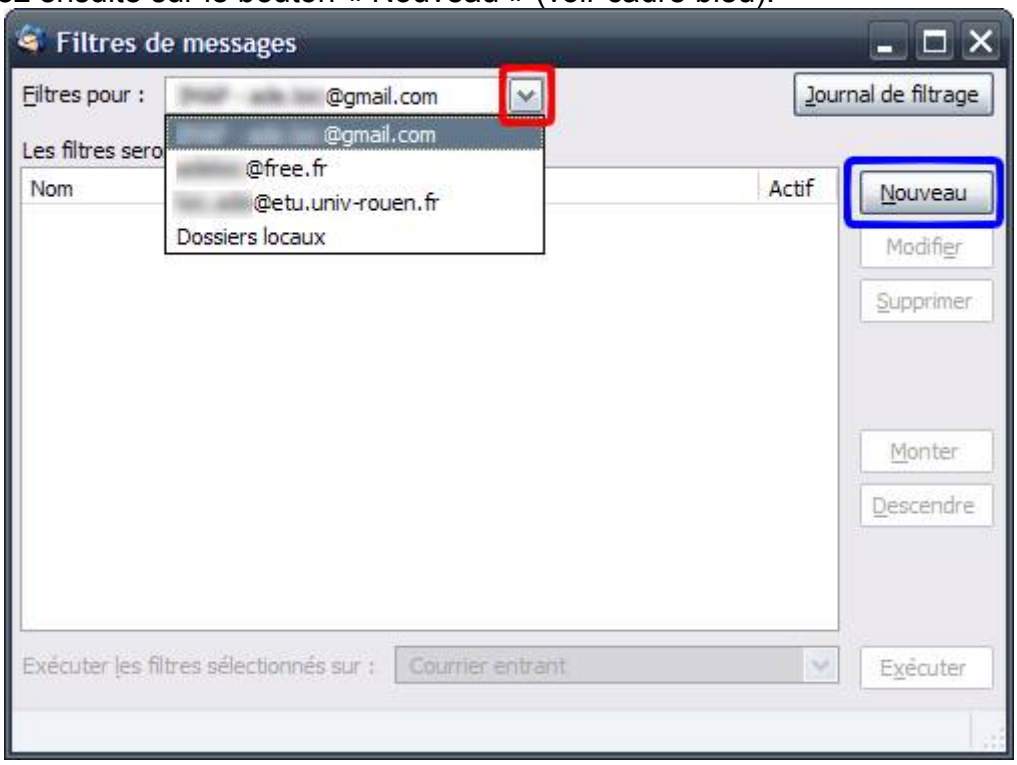
Ouvrez Mozilla Thunderbird.

Allez dans le menu « Outils », et cliquez sur « Filtres de messages... ».



Si vous avez plusieurs adresses e-mail, cliquez sur la petite flèche de la zone déroulante « Filtres pour : » (voir cadre rouge de l'image ci-dessous), et cliquez sur l'adresse où appliquer le filtre.

Cliquez ensuite sur le bouton « Nouveau » (voir cadre bleu).



Changez le nom de votre filtre (voir cadre magenta de l'image ci-dessous / il s'appelle par défaut « Filtre sans titre », ce qui est très moche et peu explicite). Vous pouvez copier sur mon exemple de nom, je ne vous en voudrait pas.

Cochez ensuite la case « valident toutes les conditions suivantes » (voir cadre bleu).

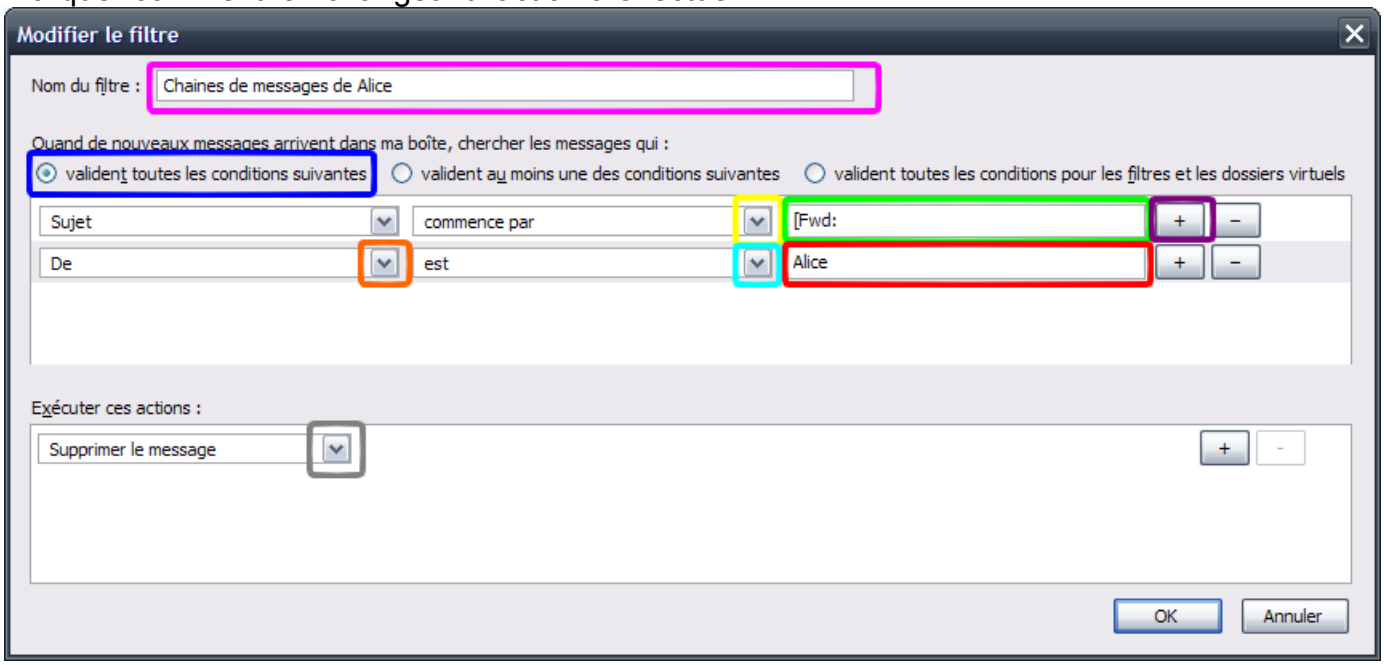
Ouvrez la deuxième liste déroulante pour remplacer « contient » par « commence par » (voir cadre jaune). Dans la deuxième zone de texte (voir cadre vert), tapez par exemple « [Fwd: ».

Si vous souhaitez bloquer les chaines d'une personne uniquement, cliquez sur le bouton « + » et suivez les instructions du prochain paragraphe. Sinon, passez directement au paragraphe d'après.

Une deuxième ligne pour une deuxième condition de filtre apparaitra. Changez le « Sujet » par « De » en utilisant la première boîte déroulante de la deuxième ligne (voir cadre orange). Changez ensuite le contenu de la deuxième boite déroulante de la deuxième ligne par « est » (voir cadre bleu clair). Dans la zone de texte de cette même ligne, tapez le nom de l'expéditeur. Faites attention au nom de l'expéditeur : certaines personnes utilisent parfois une adresse qui n'est pas la leur (cela arrive souvent que des couples n'utilisent qu'une seule adresse par exemple). Il faudra donc taper dans la zone de texte le nom qui est affiché quand ces personnes vous envoient un message (si vous tapez autre chose, ça risque de ne pas marcher).

Une fois la deuxième remplie (ou pas si vous désirez bloquer les chaines de tout le monde), changez l'action par « Supprimer le message » (voir cadre gris foncé).

Vous pouvez aussi décider de déplacer le message dans un autre dossier, ou encore le marquer comme lu en changeant l'action à effectuer.

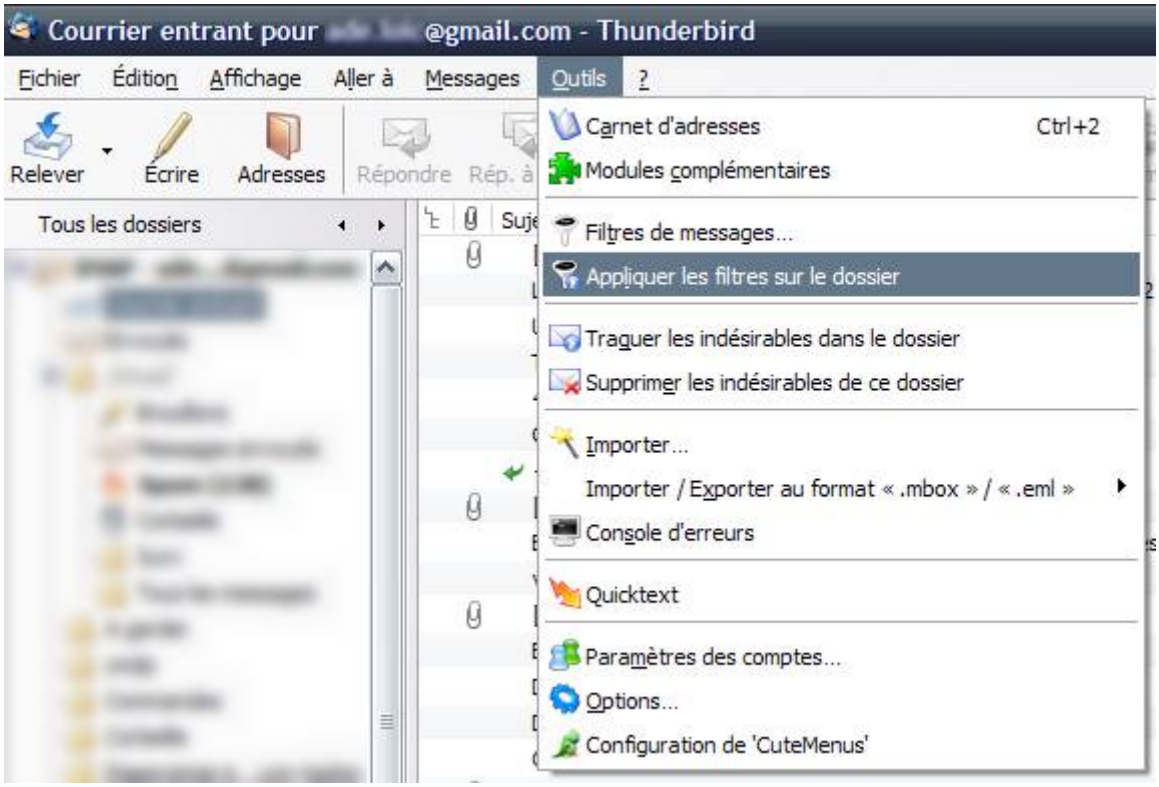


Une fois ceci fait, cliquez sur le bouton « OK ».

Cliquez sur le bouton « Nouveau » pour créer autant de filtres qu'il y a de débuts d'objets à filtrer (« Fwd: », « [Fwd: », « Fw: », « Tr: », ...).

Fermez ensuite la fenêtre des filtres.

Par défaut, le filtre ne s'activera que pour les messages déjà reçus. Si vous voulez trier les messages déjà reçus, placez vous dans le dossier à trier et allez dans le menu « Outils », puis cliquez sur « Appliquer les filtres sur le dossier ».

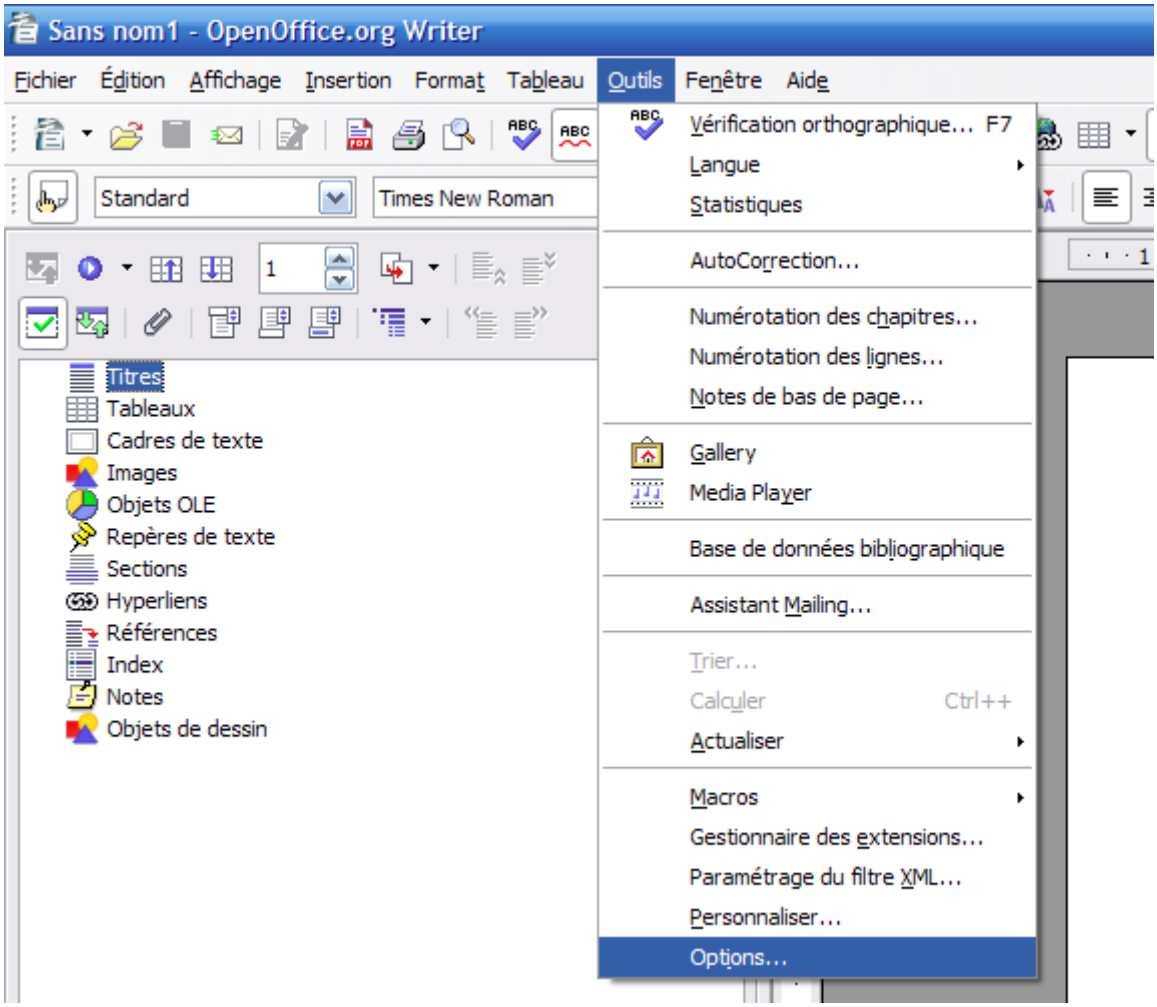


III.3) Les outils de bureautique

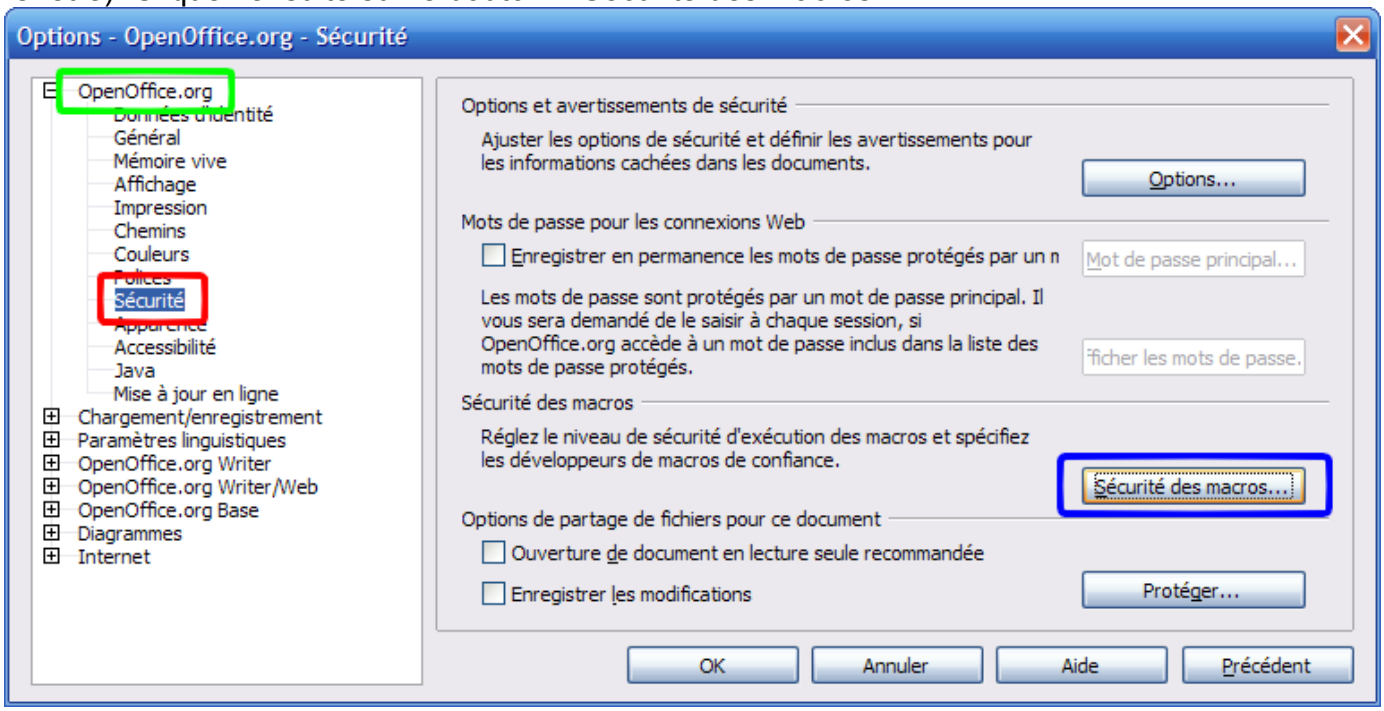
III.3.a) Macros à la demande sous OpenOffice

Ouvrez le module Writer de OpenOffice (ou n'importe quel autre module en fait, mais pour l'exemple, on fera avec Writer).

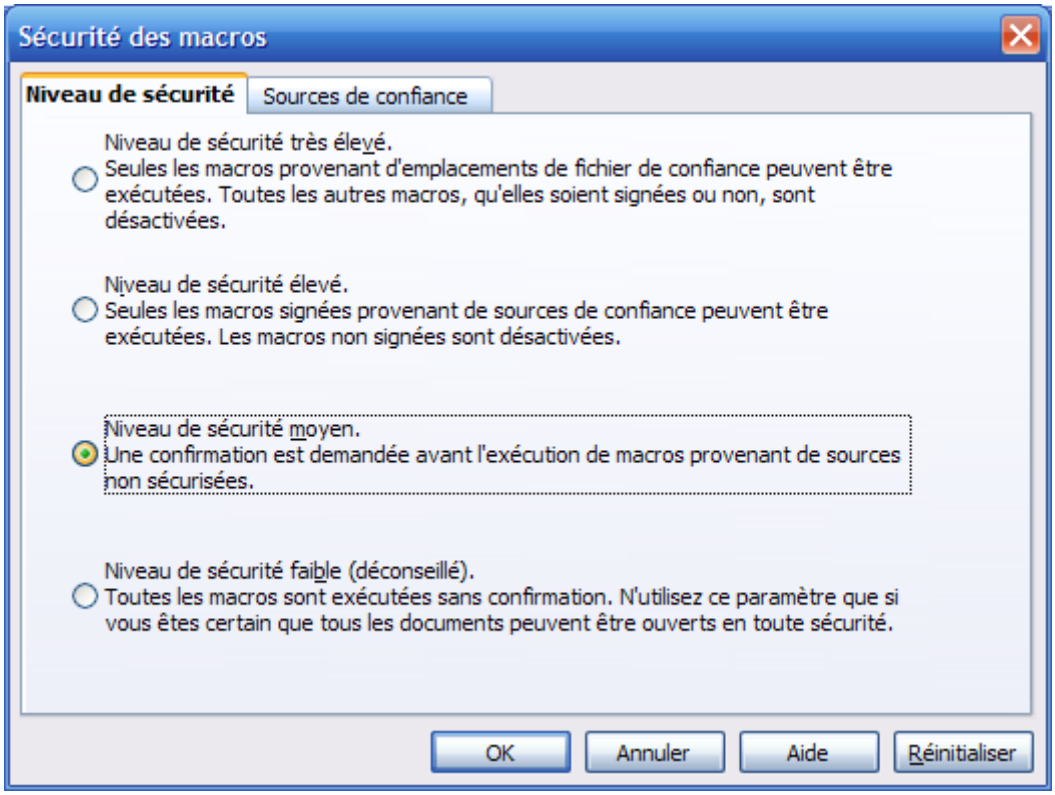
Allez ensuite dans le menu « Outils », puis cliquez sur « Options » :



Allez ensuite dans « Sécurité » de l'élément « OpenOffice.org » (à gauche dans la fenêtre). Cliquez ensuite sur le bouton « Sécurité des macros » :



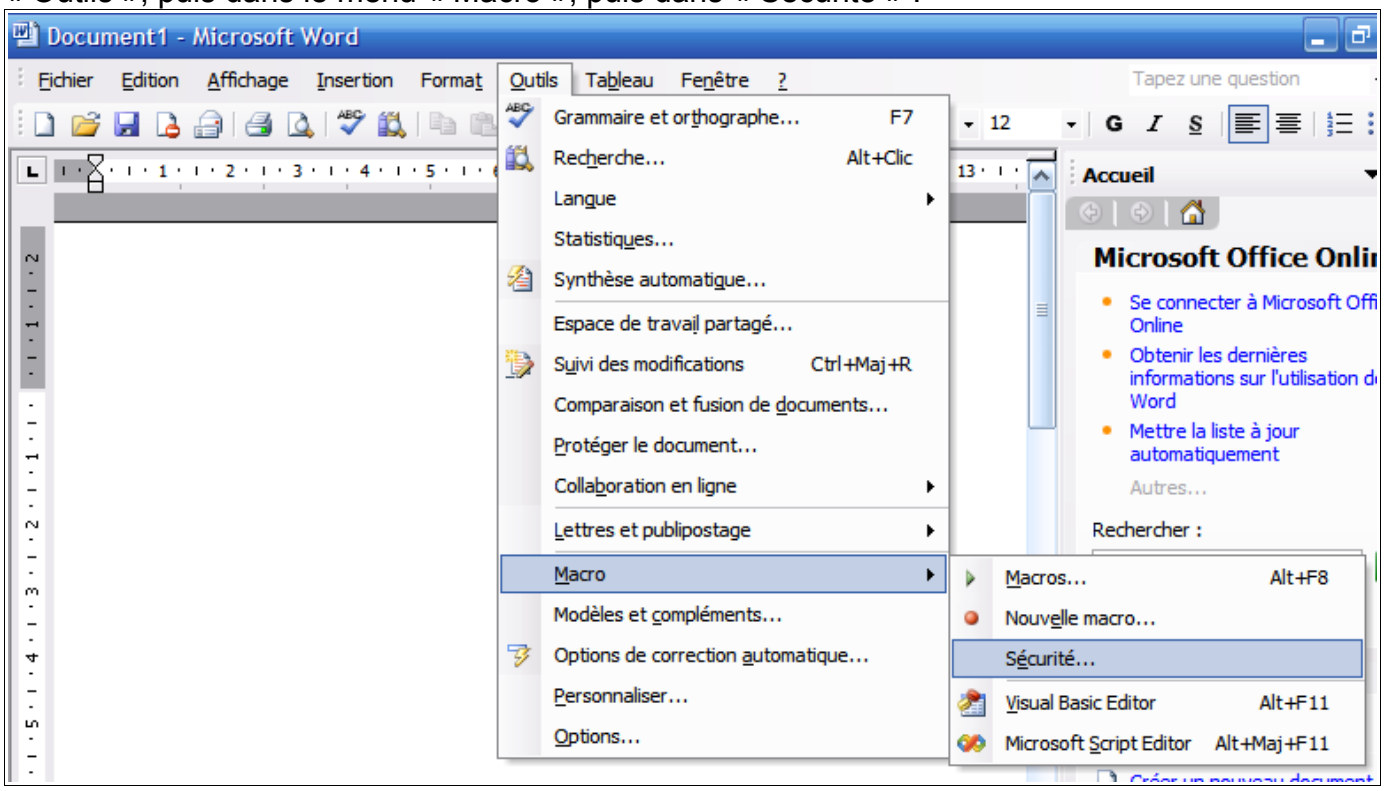
Cochez ensuite la case « Niveau de sécurité moyen », puis cliquez sur le bouton « OK ». Cliquez ensuite sur le bouton OK de la fenêtre précédente.



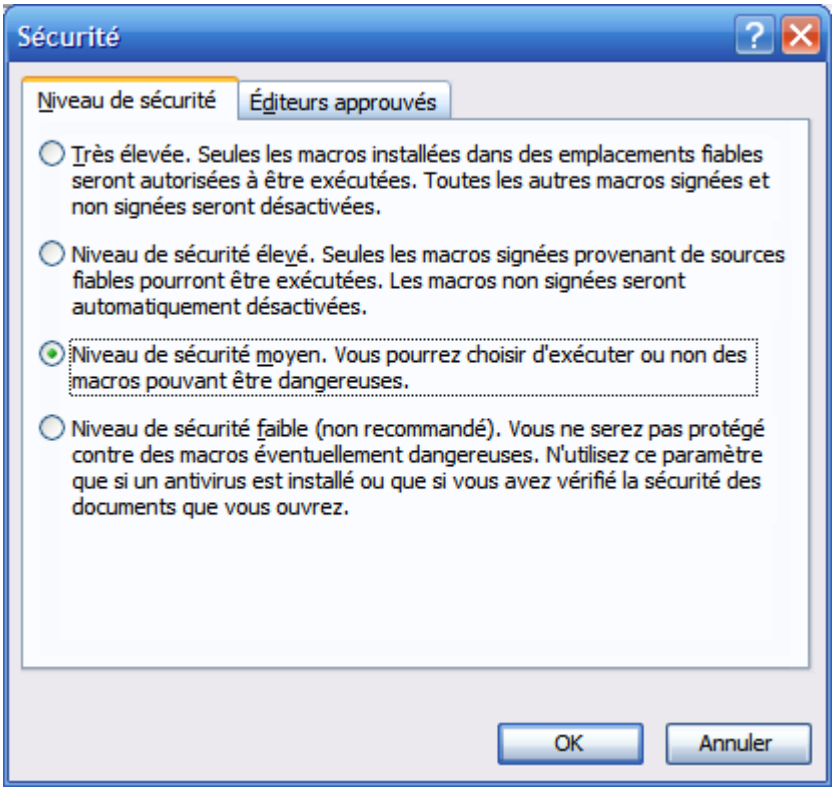
III.3.b) Macros à la demande sous Microsoft Office 2003 et antérieurs

La procédure décrite ci-dessous fonctionne avec Word, Excel, PowerPoint, Publisher et Outlook (et probablement avec tout les autres composants de Microsoft Office).

Dans le logiciel dont il faut changer le mode d'activation des macros, allez dans le menu « Outils », puis dans le menu « Macro », puis dans « Sécurité » :



Cochez ensuite la case « Niveau de sécurité moyen » (comme dans l'image ci-dessous) :



Cliquez ensuite sur OK.

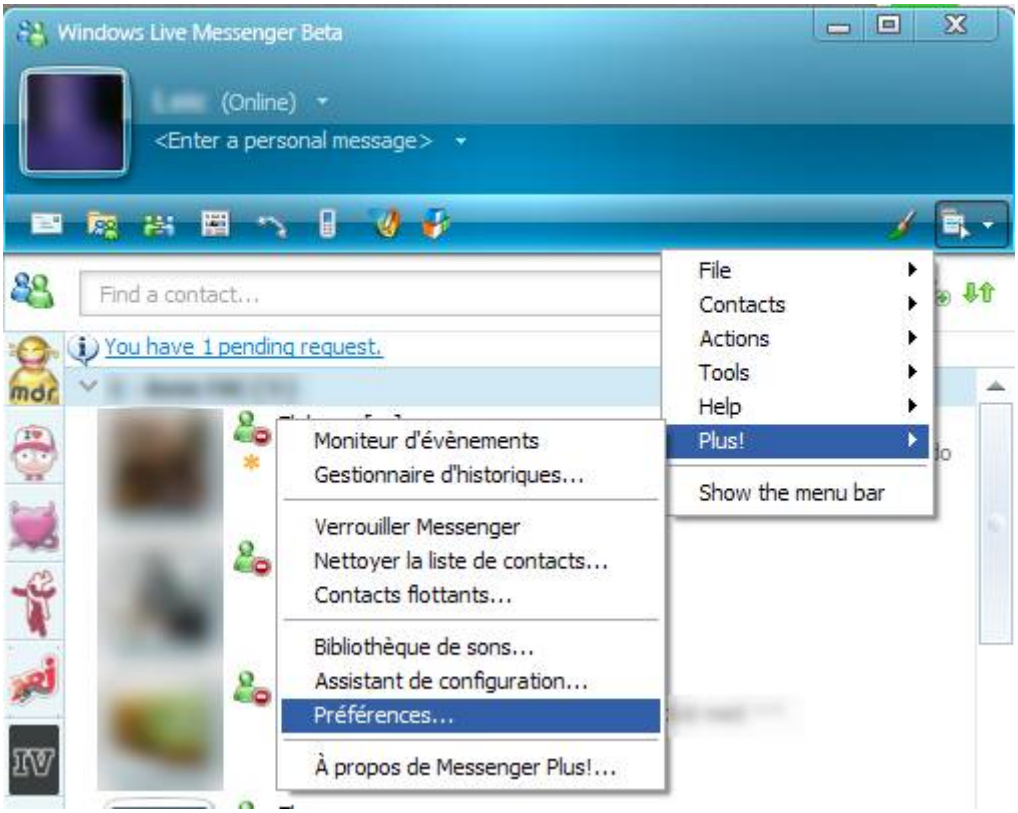
III.4) Les outils de messagerie instantanée

III.4.a) Désactiver les réponses automatiques aux requêtes avec Messenger Plus!

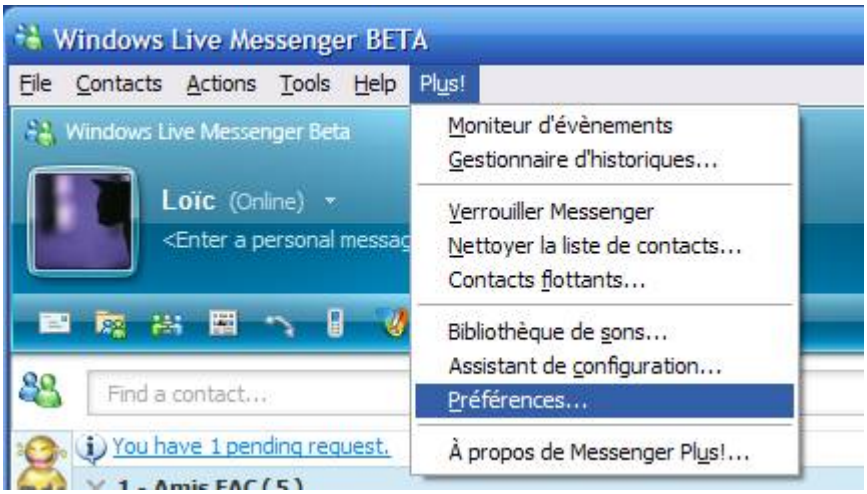
Voici donc la procédure pour désactiver les acceptations automatiques aux requêtes (valide pour Windows Live Messenger et Messenger Plus!, la procédure pour les versions MSN Messenger est légèrement différente et je n'ai pas l'occasion de réinstaller une vieille version de ces deux logiciels) :

Vous remarquerez que certains menus sont en anglais, c'est lié au fait que je teste une version non officiellement sortie de Windows Live Messenger, mais ne vous inquiétez pas, les menus intéressants sont en français chez moi et chez vous.

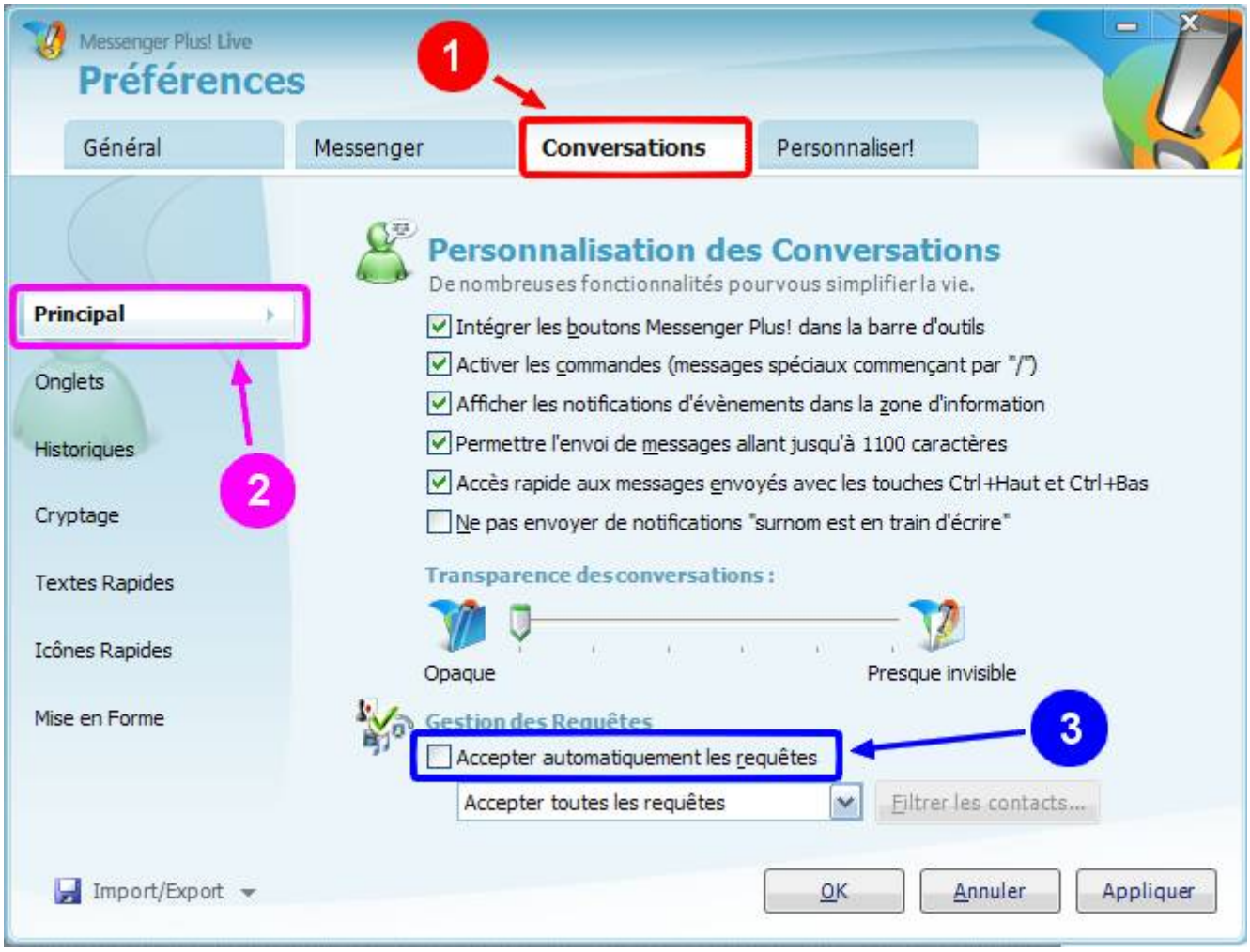
Allez dans la fenêtre principale de Windows Live Messenger (la fenêtre contenant la liste de vos contacts) puis cliquez sur  (en haut à droite), allez ensuite dans « Plus! » puis dans « Préférences » :



Pour des versions plus anciennes de Windows Live Messenger ne disposant pas du bouton  , les menus sont affichés directement :



Allez ensuite dans l'onglet « Conversations » (voir cadre rouge de l'image ci-dessous), cliquez ensuite sur « Général » (voir cadre violet) puis décochez ensuite la case « Accepter automatiquement les requêtes » (voir cadre bleu) :



Cliquez enfin sur le bouton « OK ».

IV) Les défenses de Windows et de ses logiciels

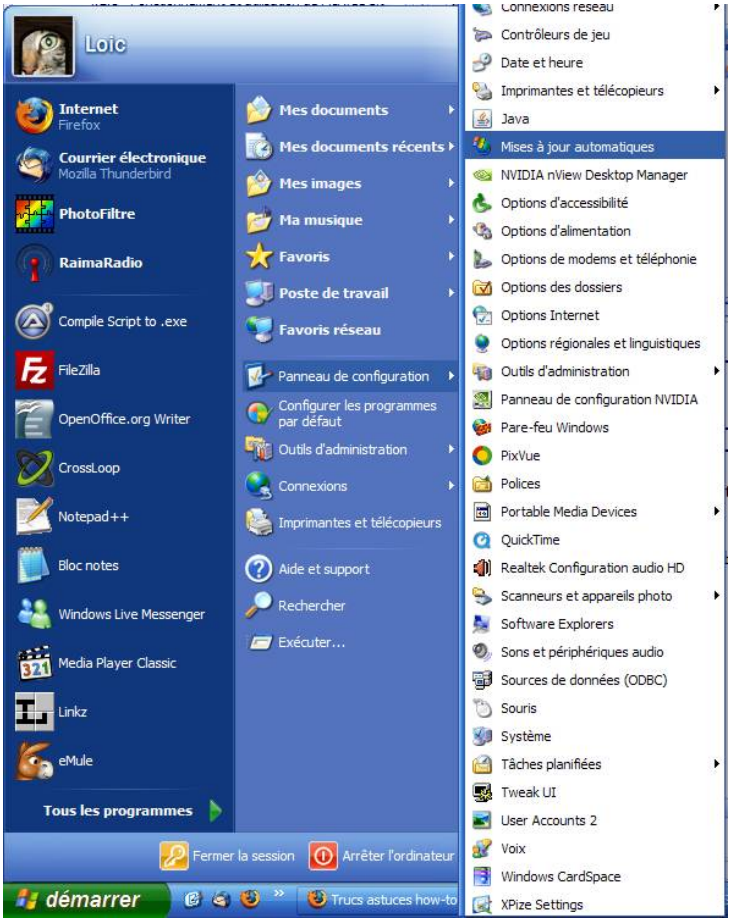
IV.1) Activer les mises à jour automatiques

IV.1.a) Sous Windows XP et antérieurs

Comme nous l'avons vu et expliqué précédemment, l'installation des mises à jour des programmes est importante. Windows a une fonction qui lui permet de se mettre à jour automatiquement. Cependant, selon les ordinateurs, il se peut qu'elles ne soient pas activées.

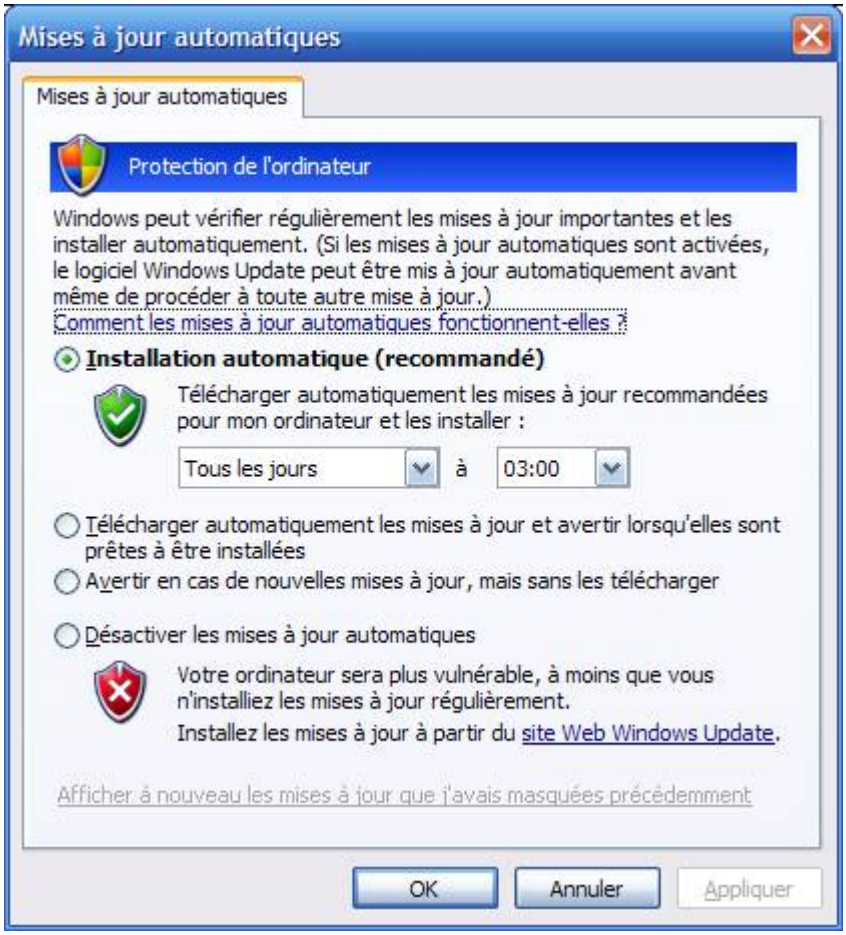
Dans le cas d'un ordinateur piraté, pour votre confort, je vous recommande de soit passer à Linux pour les gens ne désirant pas acheter Vista à prix d'or sur un ordinateur qui pourrait être ancien (ou XP, mais plus pour très longtemps car il sera retiré de la vente dans quelques mois), soit de ne pas activer les mises à jour automatiques afin de ne pas installer sans le vouloir le « Windows Genuine Advantage Validation Tool » qui vous préviendra régulièrement que votre Windows n'est pas légal.

Vérifions que les mises à jour de Windows s'installeront automatiquement (uniquement les mises à jour prioritaires, les mises à jour facultatives seront à aller chercher via Windows Update).



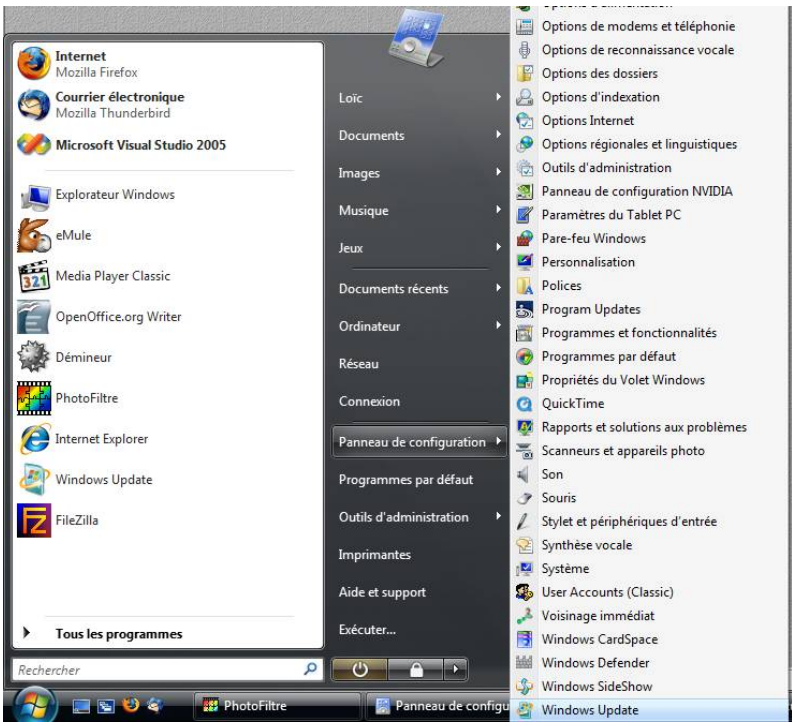
Cliquez sur le bouton « Démarrer », puis allez dans le « Panneau de configuration » et allez enfin dans « Mises à jour automatiques ».

Il se peut que le panneau de configuration n'apparaisse pas en menu, dans ce cas, cliquez dessus.
Si vous n'avez pas l'élément « Mises à jour automatiques », cliquez sur « Basculer vers l'affichage classique » dans la partie gauche de la fenêtre.



Si ce n'est pas déjà le cas, cochez la case « Installation automatique (recommandé) » et cliquez sur le bouton OK.

IV.1.b) Sous Windows Vista

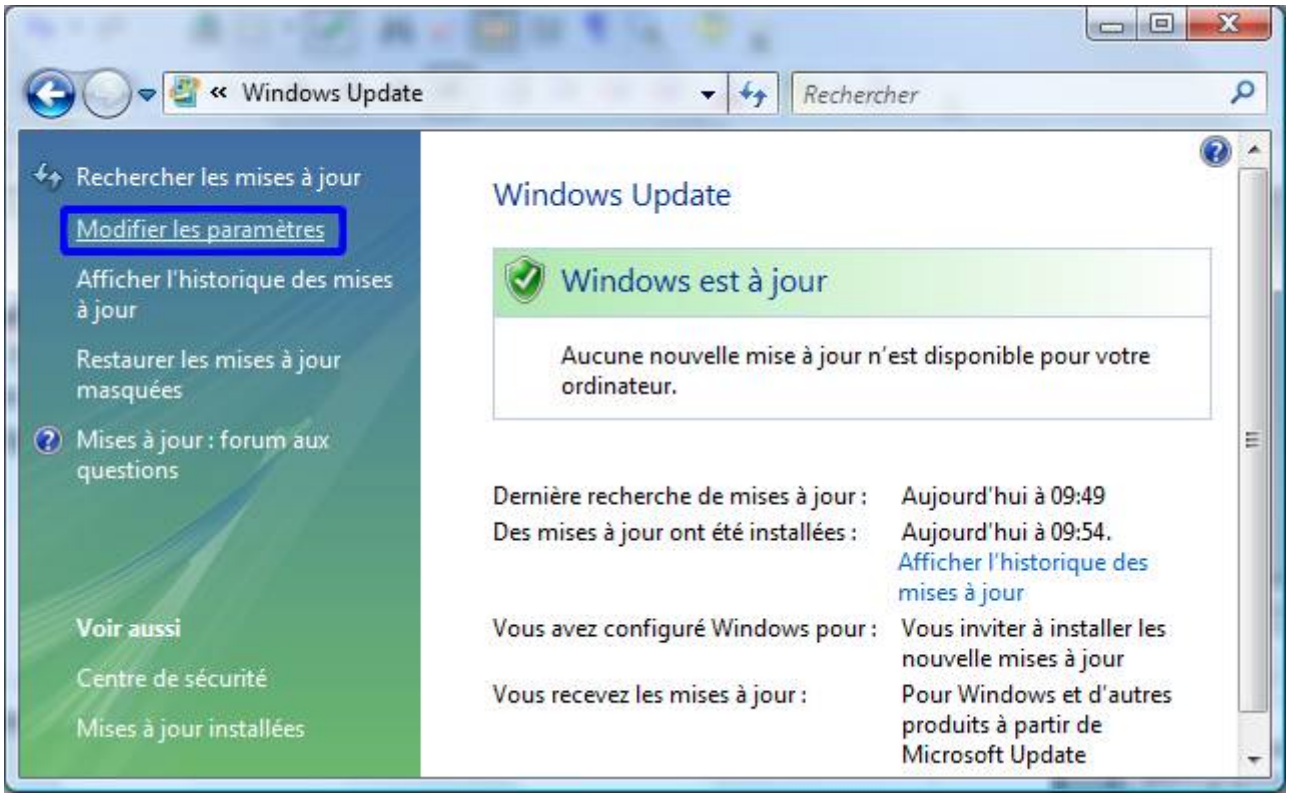


Cliquez sur votre bouton Windows 

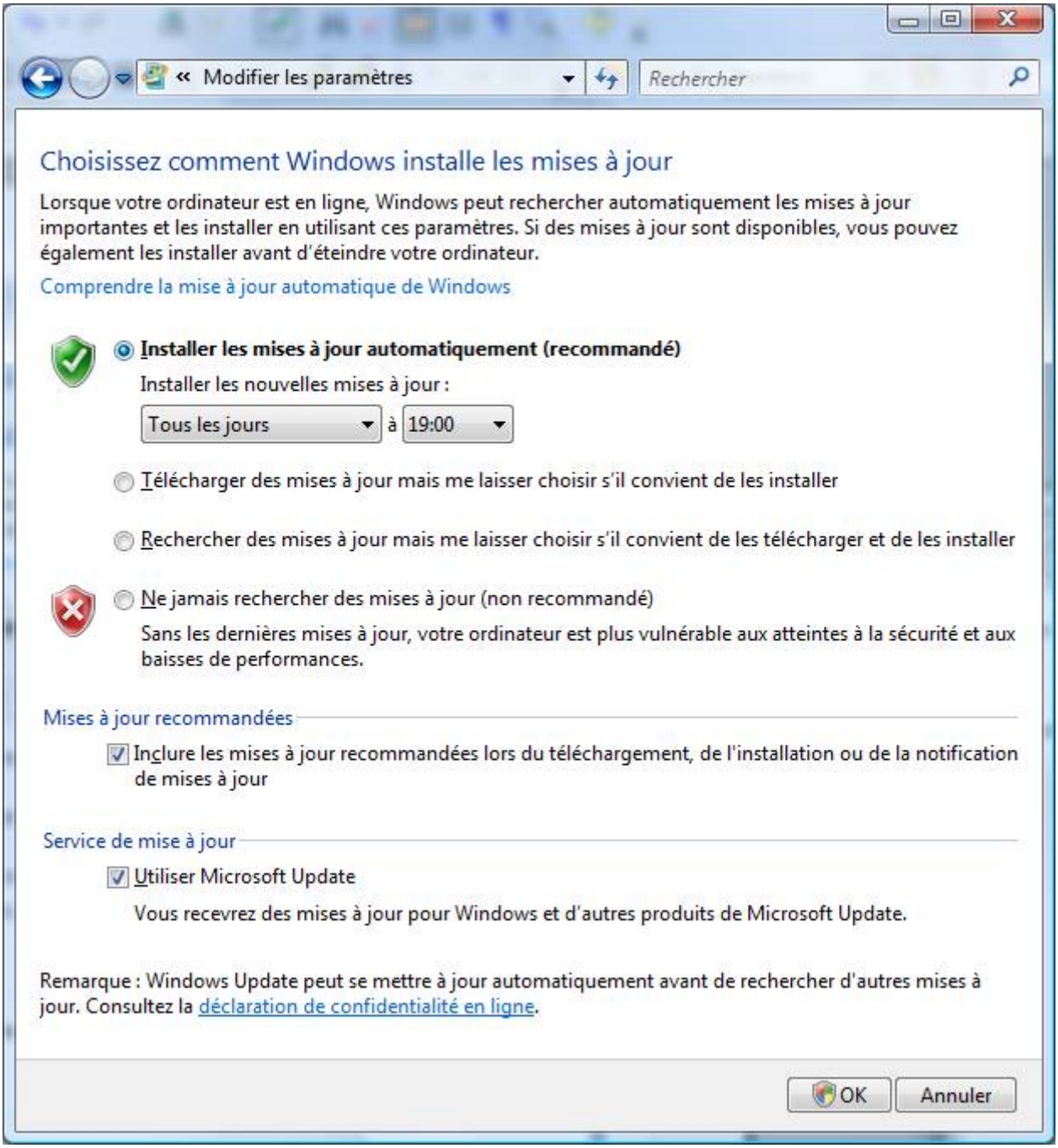
Allez ensuite dans le « Panneau de configuration », puis allez dans Windows Update.

Il se peut que le panneau de configuration ne s'ouvre pas en menu ainsi. Dans ce cas, cliquez sur « Panneau de configuration », et double cliquez sur l'icône de « Windows Update ».

Si l'icône n'apparaît pas, cliquez sur « Affichage classique » et double cliquez ensuite sur l'icône de « Windows Update »



Cliquez ensuite sur le lien « Modifier les paramètres » (voir cadre bleu de l'image ci-dessus).



Cochez les cases « Installer les mises à jour automatiquement », « Inclure les mises à jour recommandées lors du téléchargement de l'installation ou de la notification de mises à jour » et « Utiliser Microsoft Update » et cliquez sur OK.

Il vous sera ensuite demandé de cliquer sur le bouton « Continuer » pour valider. Cliquez sur ce bouton « Continuer ».

Vous pouvez ensuite fermer Windows Update.

IV.2) Le contrôle des comptes utilisateurs (UAC)

Le contrôle des comptes utilisateurs est un mécanisme de sécurité introduit par Windows Vista qui contrôle les faits et gestes de l'utilisateur et des programmes de votre ordinateur.

Il a souvent été reproché à Windows d'être assez laxiste au niveau sécurité et de permettre facilement la propagation des virus et autres malwares. Ceci étant dû au fait que par défaut, l'utilisateur a tout les droits avant Windows Vista.

Avec Windows Vista, l'utilisateur a beaucoup moins de droits par défaut. Et dès que celui-ci tente d'accéder à une fonction importante de Windows, un message d'alerte apparaît alors. Ce message permet à l'utilisateur d'accéder quand même à la fonction désirée. Donc si

un programme tente d'accéder à une fonction importante de Windows, ou à un emplacement important (comme le dossier Program Files par exemple), celui-ci sera suspendu tant que l'utilisateur n'aura pas répondu au message qui viens de lui apparaître. Le programme accédera à la fonction désirée seulement si l'utilisateur aura répondu favorablement au message affiché par Windows.

D'anciens programmes étant conçus avant Vista ne feront pas apparaître le contrôle des comptes utilisateurs. Mais ceux-ci n'ont pas pour autant accès aux fonctions importantes de Windows pour autant.

Ce qui fait au final que certains virus et autres cochonneries seront bloquées par le contrôle des comptes utilisateurs (j'utiliserai dorénavant l'abréviation UAC qui correspond à l'acronyme anglais désignant cette fonction de Windows Vista) du fait qu'ils ne sont pas conçus pour l'afficher. Et même s'ils affichaient l'UAC, l'utilisateur pourrait s'interroger sur le bien fondé de la requête et refuser au virus l'accès aux fonctions importantes de Windows.

Il existe une technique simple pour savoir quand le contrôle des comptes va apparaître. Chaque fois que vous cliquerez sur un bouton ou un lien qui présente un logo avec un petit bouclier multicolore (), alors une alerte du contrôle des comptes utilisateurs apparaîtra.

Il arrivera des fois ou le contrôle des comptes utilisateurs fait apparaître certaines alertes alors que vous ne les attendiez pas. Ceci peut intervenir lorsque certains logiciels cherchent à se mettre à jour. Mais ceci pourrait aussi intervenir lorsqu'un malware tenterai d'accéder à certaines fonctions de votre ordinateur.

IV.2.a) Comment réagir face aux alertes

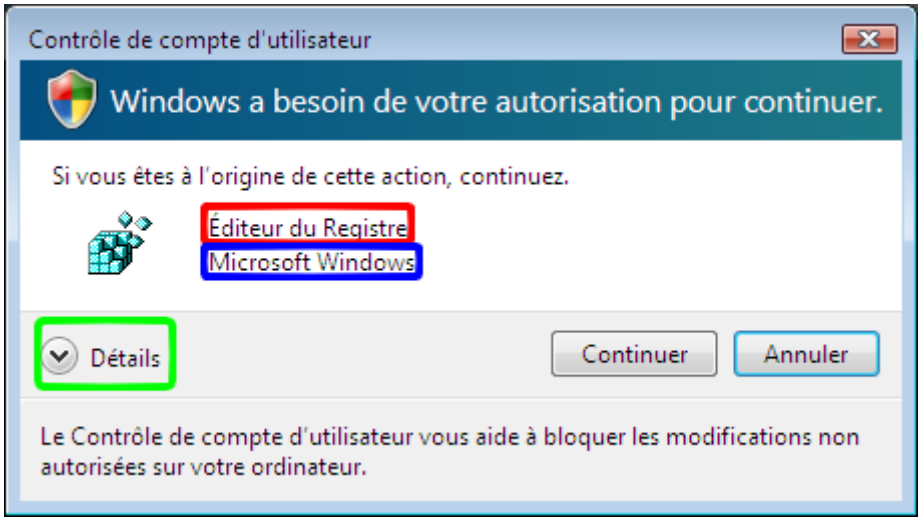
La première chose à faire est de ne pas cliquer sur « Continuer ». Sinon, l'alerte n'aura servi à rien.

La première chose à faire est de vous poser des questions à peu près dans cet ordre :

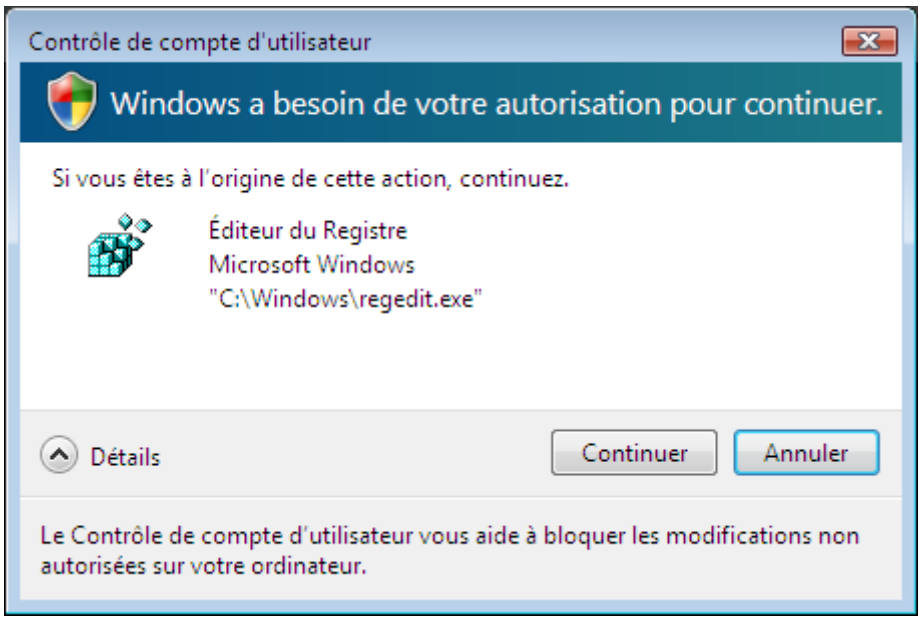
- Qu'est-ce que je faisais juste avant l'alerte ?
- Est-ce normal qu'une alerte apparaisse ?
    - ► Ai-je cliqué sur un bouton ou un lien avec un ?
    - ► Ou ai-je demandé à un programme de s'ouvrir en mode administrateur ?
- Si je ne sais pas pourquoi l'alerte apparaît, quel est le programme qui demande l'autorisation ?
- Si je ne connais pas le programme qui demande, est-ce que je connais au moins l'éditeur de ce programme ?
- Si je ne connais ni le nom du programme, ni l'éditeur, est-ce que je connais au moins l'emplacement de ce programme ?
- Si je connais tout du programme, a-t-il besoin d'un accès à une fonction importante de Windows ?
- Si je ne connais presque pas le programme, est-il connu par quelqu'un d'autre que moi ?
- Si je ne connais presque pas le programme, mais que je sais qu'il n'a pas besoin d'accéder à des fonctions importantes de Windows, dois-je cliquer sur « Continuer » ?

La plupart de ces questions ont des réponses simples. Pour répondre à la plupart des questions données ci-dessus, il suffit de bien regarder une alerte.

Le nom du logiciel est une des premières choses marquées (voir cadre rouge de l'image ci-dessous). Juste en dessous apparaît de nom du créateur du programme demandant l'autorisation (voir cadre bleu / Il se peut que le nom n'apparaisse, ou apparaisse comme « Editeur inconnu », ça ne veut pas dire que le programme est louche pour autant car assez nombreux sont les programmes dont l'UAC n'est pas capable d'afficher l'éditeur).



Si vous cliquez sur « Détails », l'UAC affichera l'emplacement du programme demandant l'autorisation.



Parfois, le fait de savoir où se trouve le programme appelant peut vous aider à reconnaître le programme. Cela pourrait aussi vous permettre de savoir si le programme est louche ou non (par exemple, si le programme viens du dossier de documents, il y a de quoi se poser des questions).

Vous savez dorénavant comment bien connaître le programme appelant.

Il faut aussi savoir une chose : lorsque vous installez un programme, le programme d'installation modifiera obligatoirement des emplacements protégés par Windows (en l'occurrence le dossier Program Files). Il est donc fortement probable que vous ayez une alerte qui apparaîtra.

De même pour certains programmes qui voudraient se mettre à jour automatiquement, il y a parfois une fenêtre de l'UAC qui demande une autorisation pour continuer.

Par exemple : Adobe Updater.

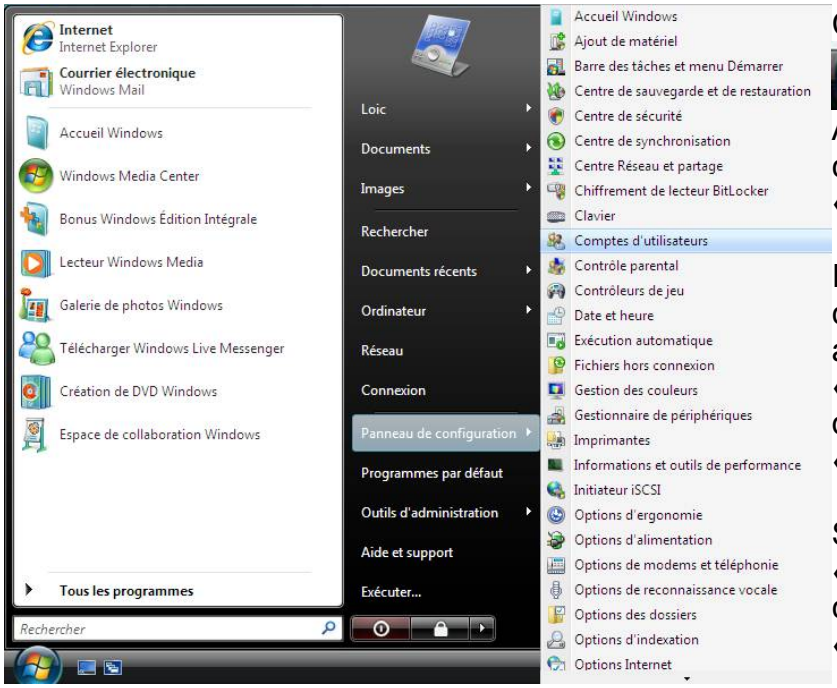
IV.2.b) Activer le contrôle des comptes utilisateurs

L'UAC peut se révéler vite agaçant pour des utilisateurs qui modifieraient souvent leur PC en profondeur, mais il est quand même important pour les néophytes afin qu'ils se soucient un peu plus de ce qui se passe dans leur ordinateur.

Il vaut mieux le laisser activé.

Mais certaines personnes le jugeant un peu trop vite le désactivent sans réfléchir. Nous

allons donc voir comment l'activer (cette méthode sera aussi valable pour le désactiver, ce que je ne vous recommande pas).

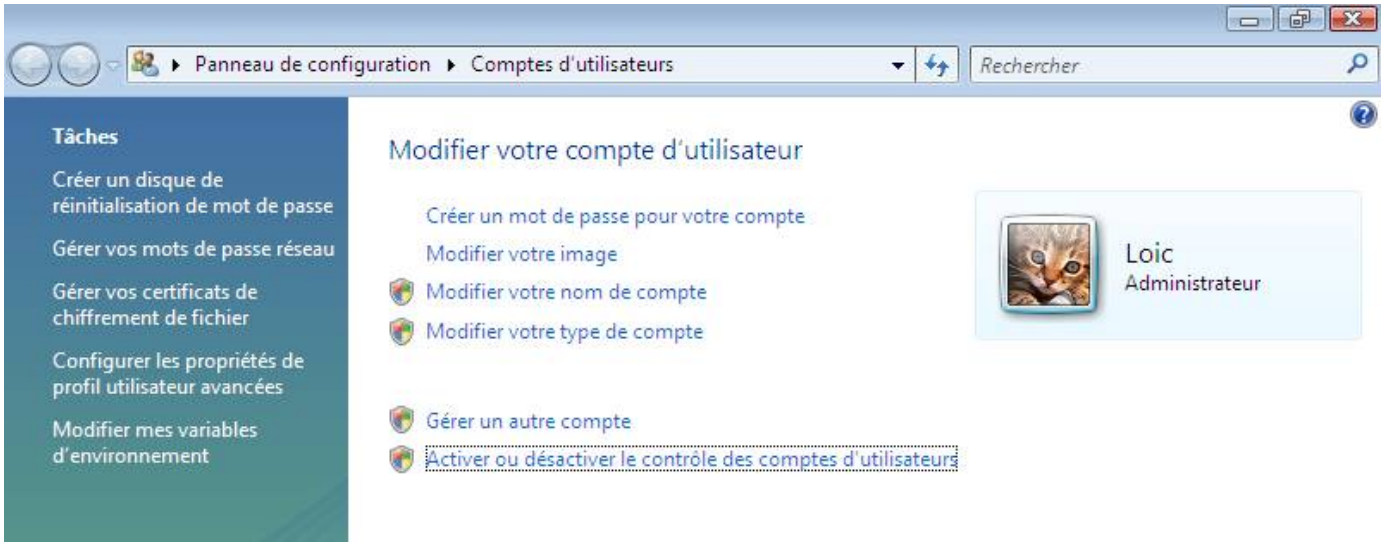


Cliquez sur votre bouton Windows 

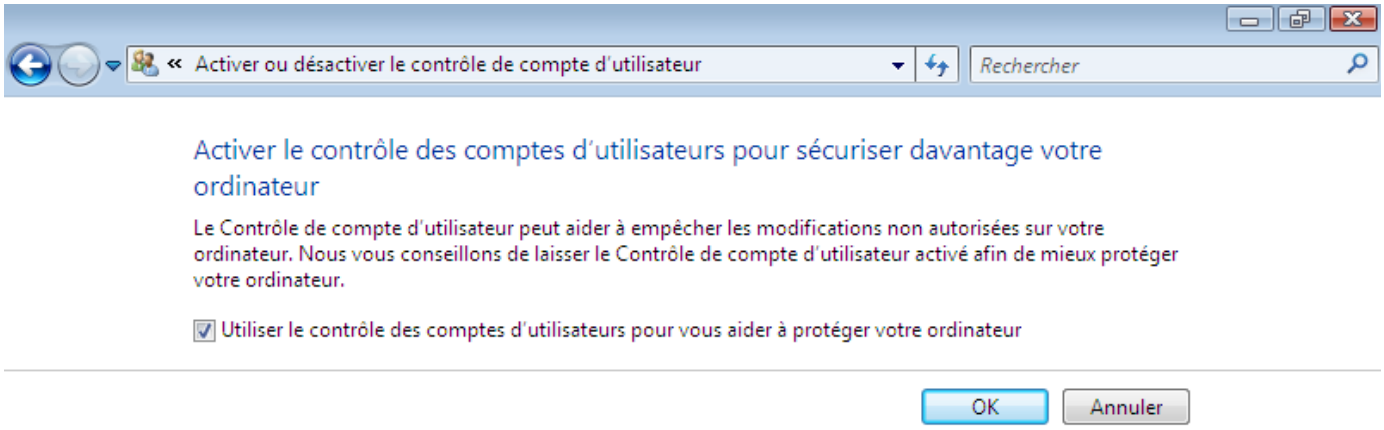
Allez ensuite dans le « Panneau de configuration », puis allez dans « Comptes d'utilisateurs ».

Il se peut que le panneau de configuration ne s'ouvre pas en menu ainsi. Dans ce cas, cliquez sur « Panneau de configuration », et double cliquez sur l'icône de « Comptes d'utilisateurs ».

Si l'icône n'apparaît pas, cliquez sur « Affichage classique » et double cliquez ensuite sur l'icône de « Comptes d'utilisateurs »



Cliquez sur « Activer ou désactiver le contrôle des comptes d'utilisateurs ».



Cochez la case « Utiliser le contrôle des comptes d'utilisateurs pour vous aider à protéger votre ordinateur » et cliquez sur le bouton « OK ».

IV.3) Le pare feu de Windows

Un pare-feu empêche les pirates qui sont sur Internet d'accéder à votre ordinateur par des portes qui seraient ouvertes. Autant dire qu'il est assez important d'avoir un tel logiciel.

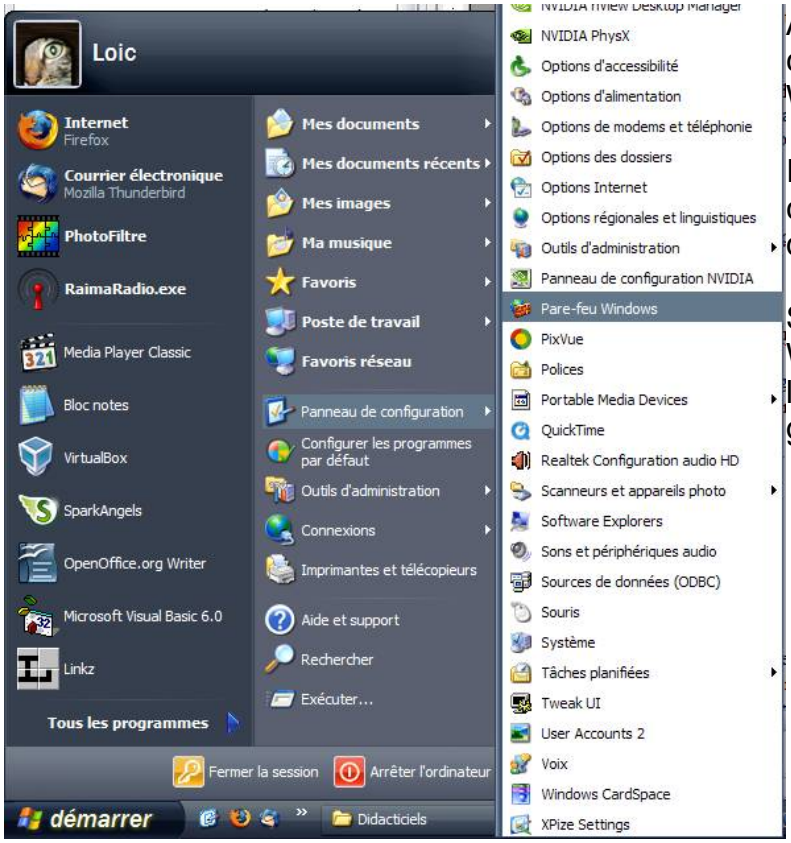
Windows XP en possède un par défaut, tout comme Windows Vista. Cependant, un pare-feu permet aussi de repérer les éventuels programmes de votre ordinateur tentant d'accéder à Internet sans votre autorisation. Il permet donc de détecter si un virus (ou un logiciel espion) qui aurait réussi à s'introduire sur votre ordinateur tente d'accéder à Internet pour appeler tout ses petits copains. Mais mieux que ça, il permet aussi d'empêcher ces virus d'accéder à Internet.

Par défaut, le pare-feu de Windows XP ne filtre que les données entrant vers votre ordinateur. Alors que le pare-feu de Windows Vista filtre les entrées entrantes et sortantes.
Celui de Windows XP est assez pauvre, tandis que celui de Windows Vista est plus complet.

Nous verrons l'utilisation d'un autre pare-feu en lieu et place de celui de Windows. Mais cet autre pare-feu pose un peu plus de questions et peu se révéler agaçant pour les débutants.
Les personnes qui souhaiteraient installer Comodo Internet Security (l'autre pare-feu que nous verrons à la section V.3 page 108) peuvent désactiver celui de Windows car il risque de faire doublon avec Comodo Internet Security.

IV.3.a) Activer-Désactiver

IV.3.a.i) Sous Windows XP

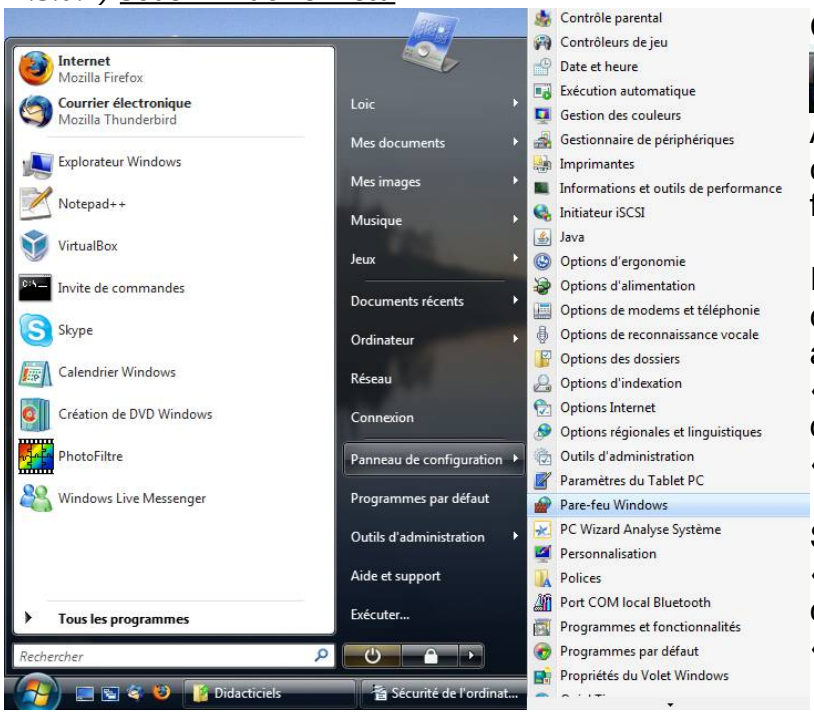


Allez dans le « Panneau de configuration », et allez dans « Pare-feu Windows ».

Il se peut que le panneau de configuration n'apparaisse pas en menu, dans ce cas, cliquez dessus.

Si vous n'avez pas l'élément « Pare-feu Windows », cliquez sur « Basculer vers l'affichage classique » dans la partie gauche de la fenêtre.

IV.3.a.ii) <u>Sous Windows Vista</u>

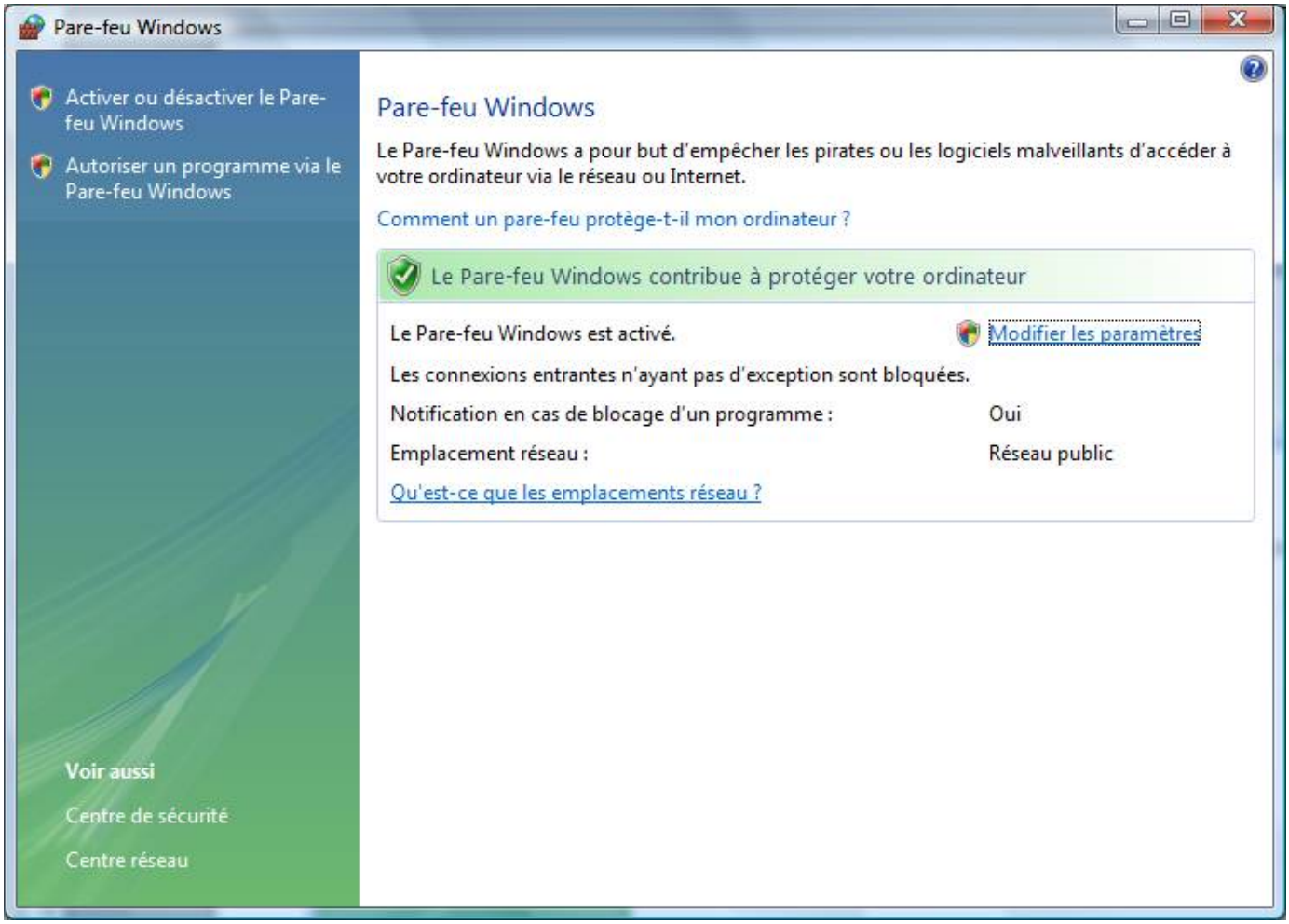


Cliquez sur votre bouton Windows 

Allez ensuite dans le « Panneau de configuration », puis allez dans « Pare-feu Windows ».

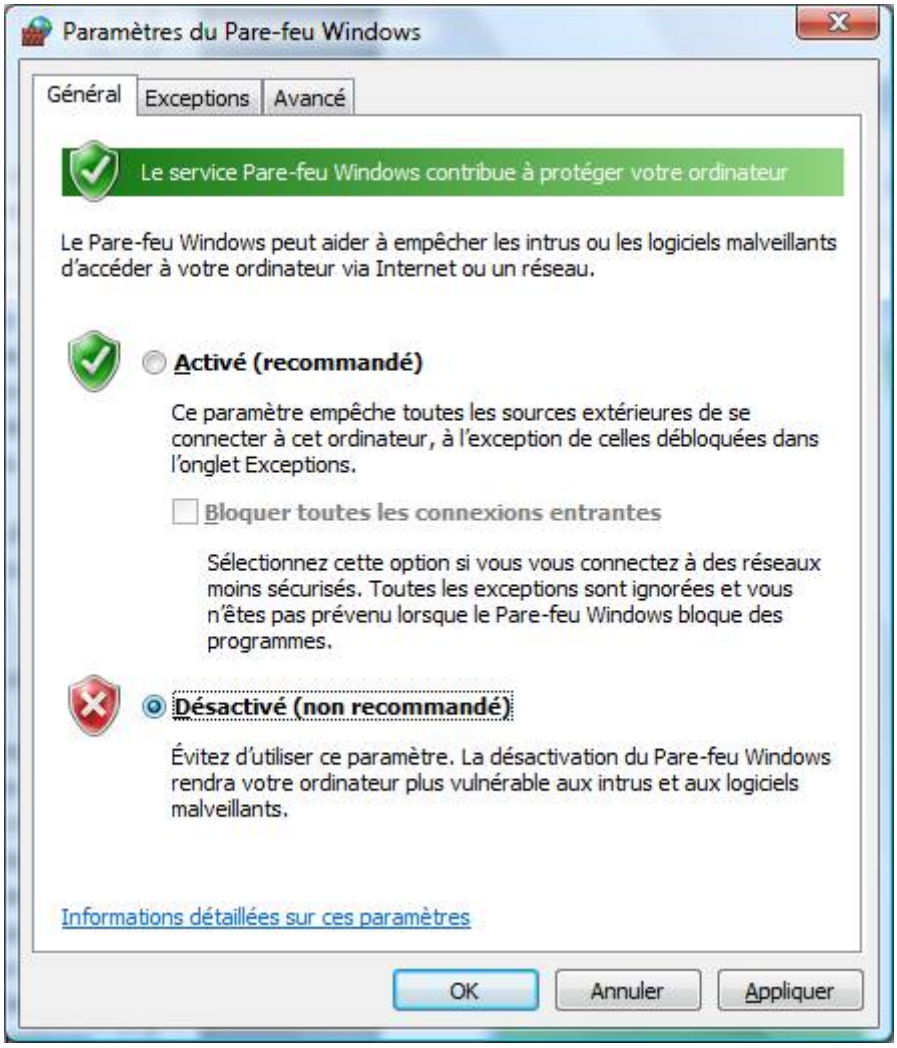
Il se peut que le panneau de configuration ne s'ouvre pas en menu ainsi. Dans ce cas, cliquez sur « Panneau de configuration », et double cliquez sur l'icône de « Comptes d'utilisateurs ».

Si l'icône n'apparaît pas, cliquez sur « Affichage classique » et double cliquez ensuite sur l'icône de « Comptes d'utilisateurs »



Cliquez ensuite sur « Modifier les paramètres ».

Une demande d'autorisation apparaîtra. Cliquez sur « Continuer ».



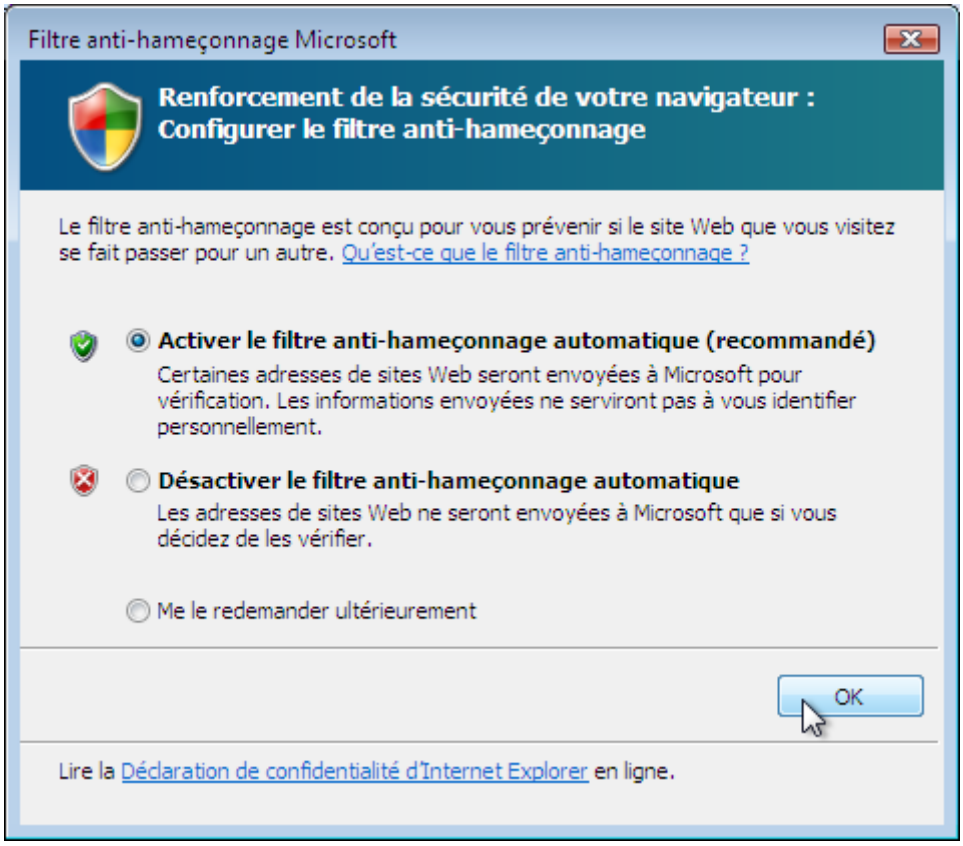
Cochez la case « Désactivé (non recommandé) » et cliquez sur le bouton « OK ».

IV.4) Le centre de sécurité pour vérifier que tout va bien

IV.5) Les défenses de Internet Explorer 7/8

IV.5.a) Le filtre anti-phishing

Internet Explorer dispose d'un filtre anti-phishing. Lorsque vous le lancez pour la première fois, cette fenêtre peut apparaître :



Dans ce cas, cochez la case « Activer le filtre anti-hameçonnage automatique (recommandé) » et cliquez sur « OK ».

V) Les logiciels de protection

Il existe différents logiciels pour différents types d'attaques.

Vous avez très certainement déjà entendu parler d'antivirus, avec le très connu Norton Antivirus. Dans le domaine des logiciels gratuits, il n'y a pas qu'un seul et unique logiciel qui s'occupe de toute la protection. Il y a à peu près un logiciel par type de menace (à peu près il y a parfois plusieurs logiciels pour un même type de menace, mais ils protègent différemment).

Dernière chose à savoir de très importante :

Deux antivirus ne peuvent coexister sans conflits. Si vous avez un autre antivirus et que vous souhaitez passer à Antivir, il vous faudra d'abord désinstaller cet antivirus avant d'installer Antivir.

Étant donné le nombre d'antivirus existant, vous comprendrez que je ne peux pas détailler la procédure de désinstallation de chaque antivirus.

Ce n'est qu'une expérience personnelle qui s'est trouvée vérifiée plusieurs fois, mais je vous recommande si vous avez Norton de passer à un autre antivirus :

Il fut un temps ou j'avais Norton (à l'époque, il était très lourd et ralentissait tout le PC). Je suis ensuite passé sur certains PC à AVG. AVG m'a détecté toute une série de virus que Norton n'avais jamais vu. Je suis ensuite passé à Avast. Celui-ci m'a détecté toute une série de virus qu'AVG n'avais pas vu. Depuis quelques temps, AVG semble, d'après les différents forums que j'ai pu lire sur Internet, s'être grandement amélioré, alors que Avast a perdu en qualité (en fait son gros problème c'est que les mises à jour se font longtemps après l'apparition de nouvelles menaces). Antivir semble très efficace d'après de nombreux forums qui conseillent de passer de Avast à Antivir. Nous parlerons donc de Antivir.

V.1) Antivirus

V.1.a) Antivirus à installer dans votre ordinateur : Antivir

Maintenant que Antivir version 9 est en français, nous allons utiliser cet antivirus. Nous verrons comment le télécharger, comment l'installer et comment l'utiliser.

V.1.a.i) Téléchargement

Utilisez votre moteur de recherche préféré pour aller sur le site de Antivir. Vous devrez trouver ce résultat :

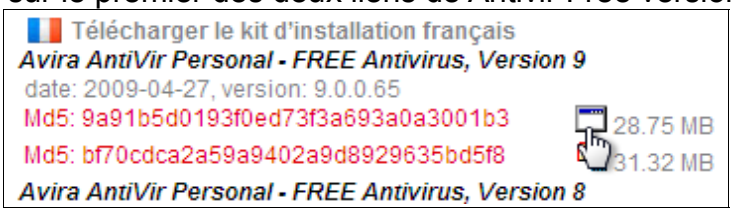
Cliquez sur « Download » :

Cliquez ensuite sur le drapeau français :

Cliquez ensuite sur le bouton « Télécharger » :

Cliquez sur le lien « ici » :

Cliquez ensuite sur le premier des deux liens de Antivir Free version 9 :

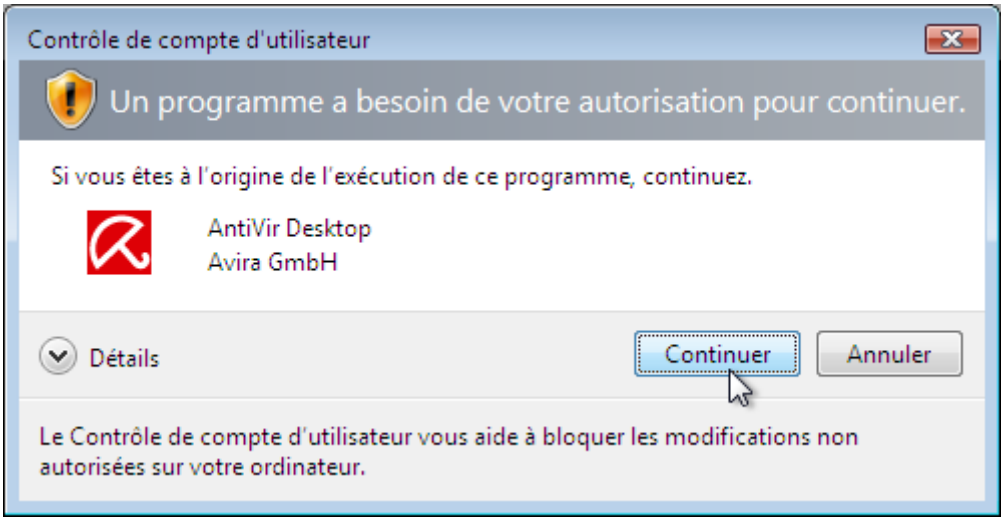


La procédure de téléchargement est ensuite la procédure standard de votre navigateur.

V.1.a.ii) *Installation*

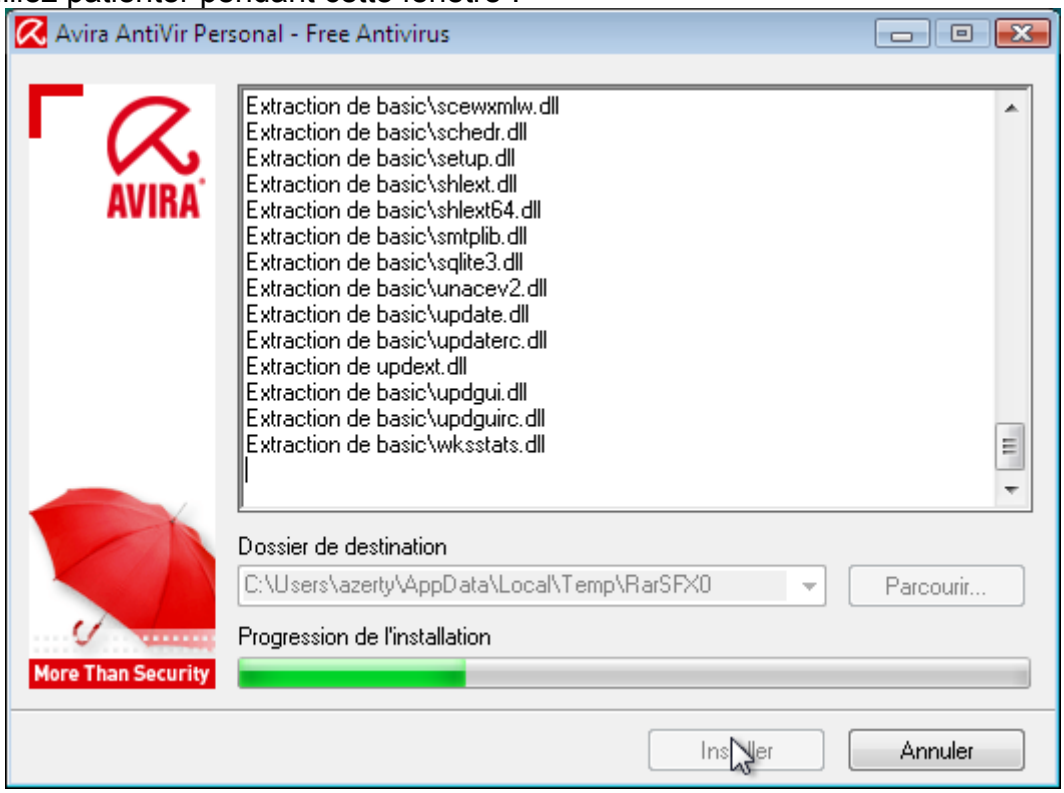
Ouvrez le fichier précédemment téléchargé.

Lorsque le « Contrôle de compte d'utilisateur » apparaitra (sous Windows Vista ou 7), cliquez sur « Continuer » :

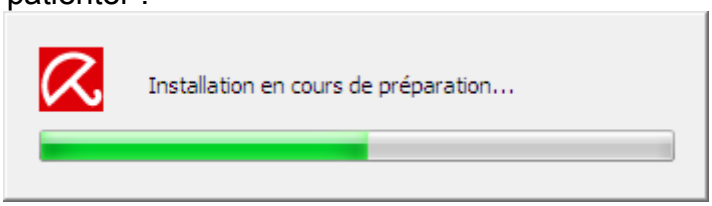


Cliquez ensuite sur « Accepter » :

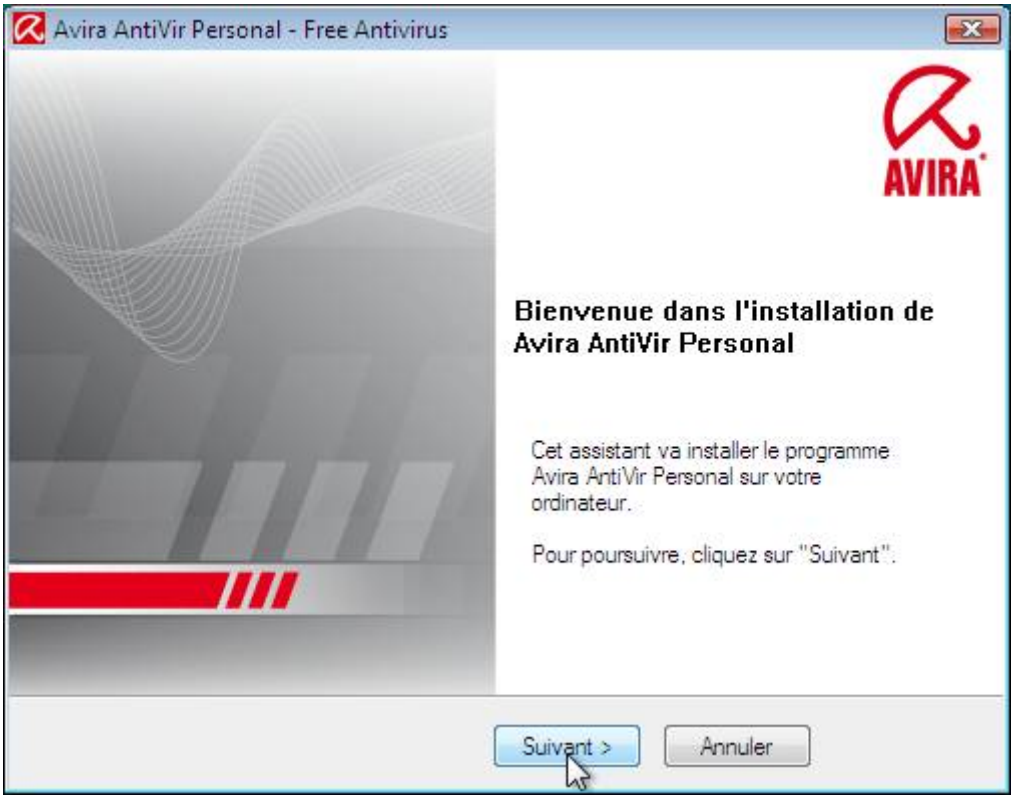
Veuillez patienter pendant cette fenêtre :



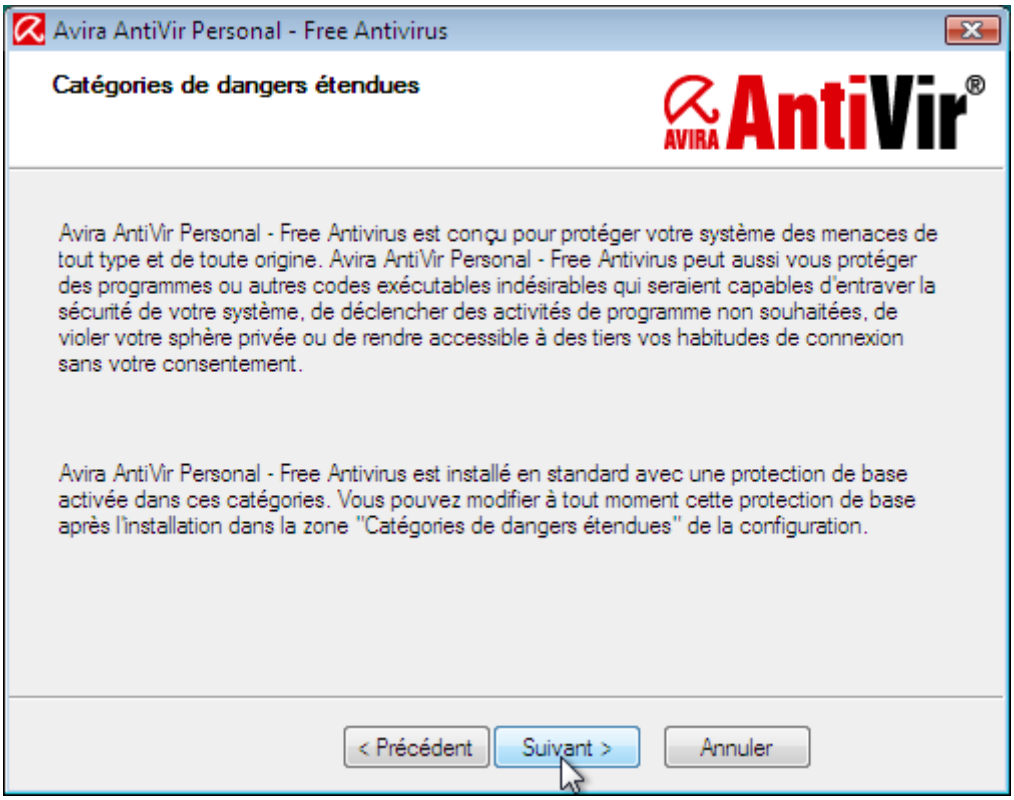
Là encore il faut patienter :



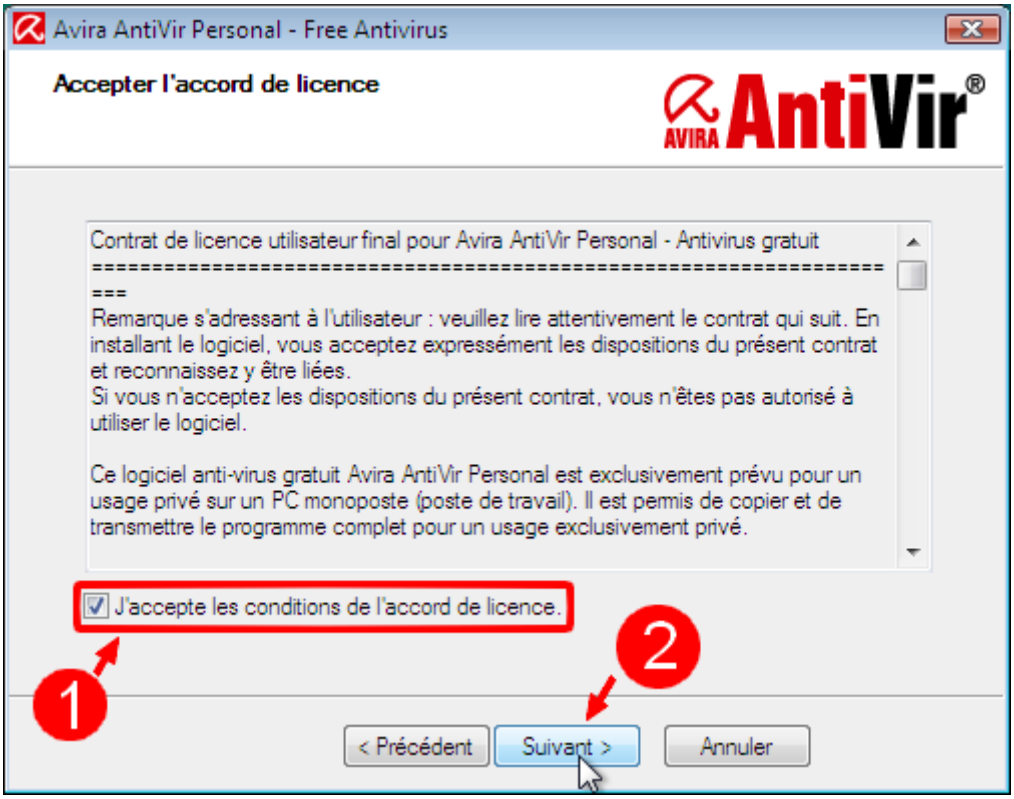
Cliquez sur le bouton « Suivant » :



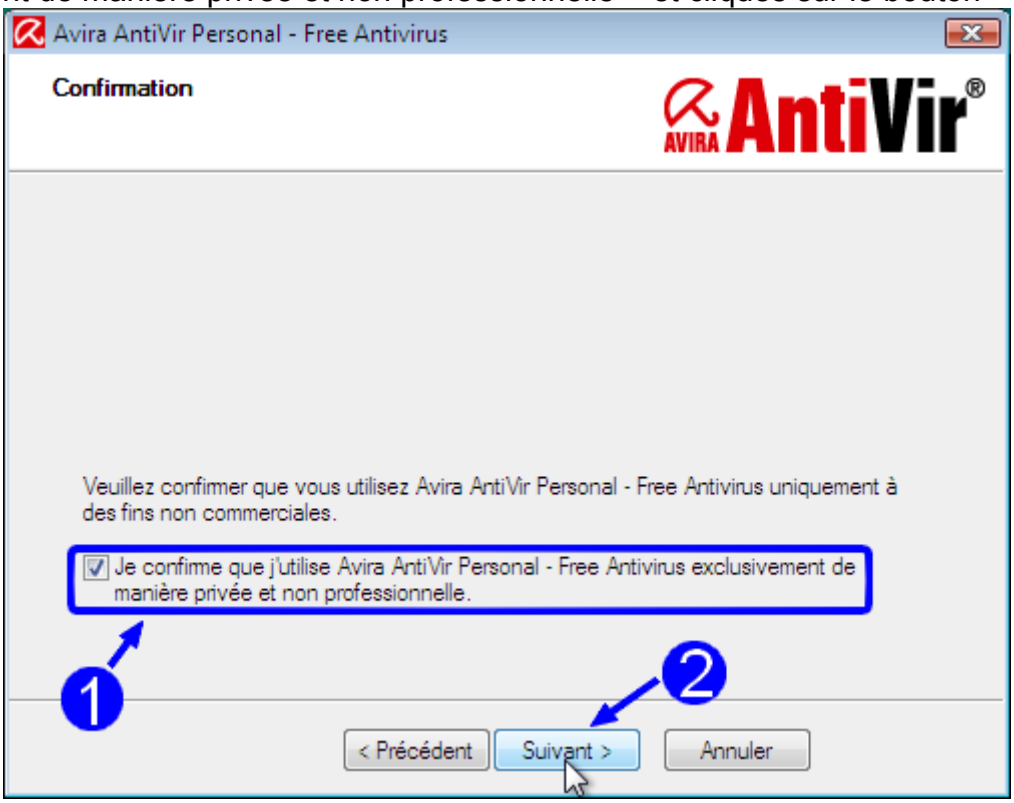
Cliquez de nouveau sur le bouton « Suivant » :



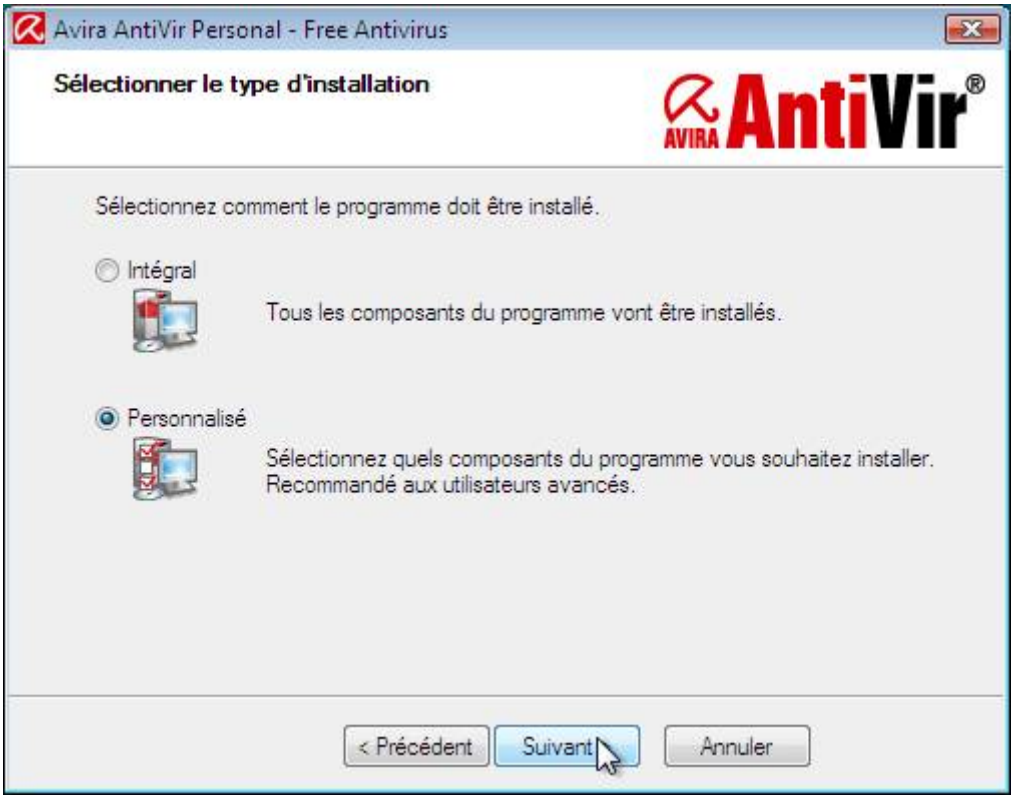
Cochez la case « J'accepte les conditions de l'accord de licence » et cliquez sur le bouton « Suivant » :



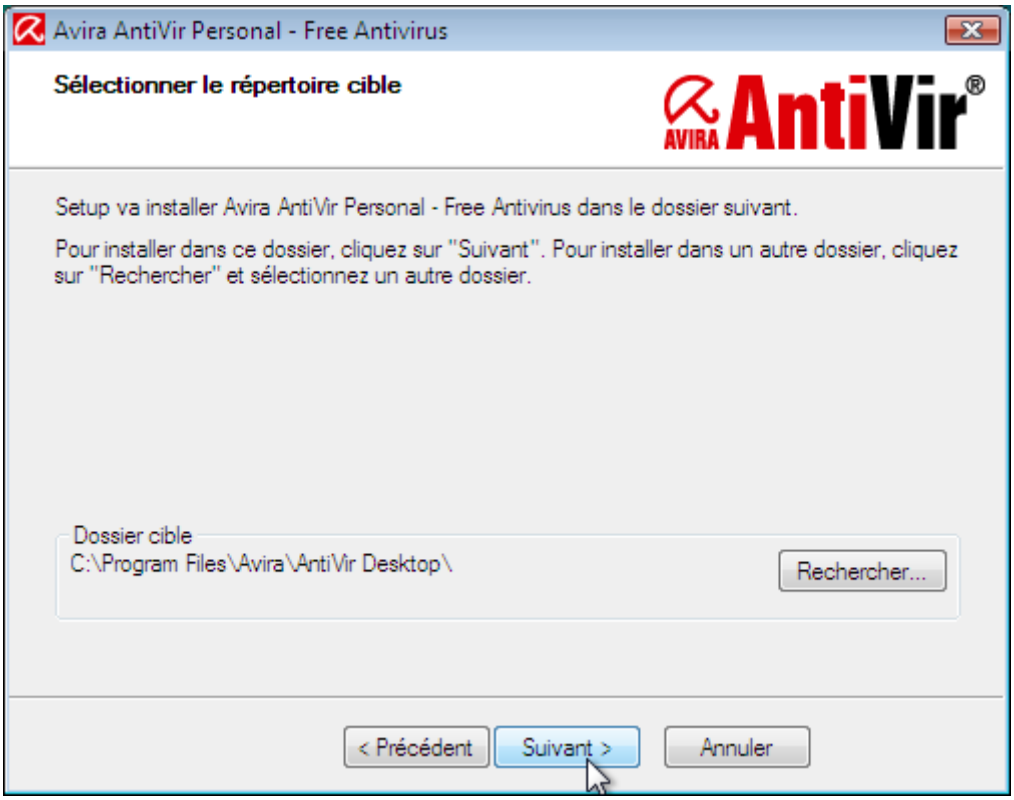
Cochez la case « Je confirme que j'utilise Avira AntiVir Personal – Free Antivirus exclusivement de manière privée et non professionnelle » et cliques sur le bouton « Suivant » :



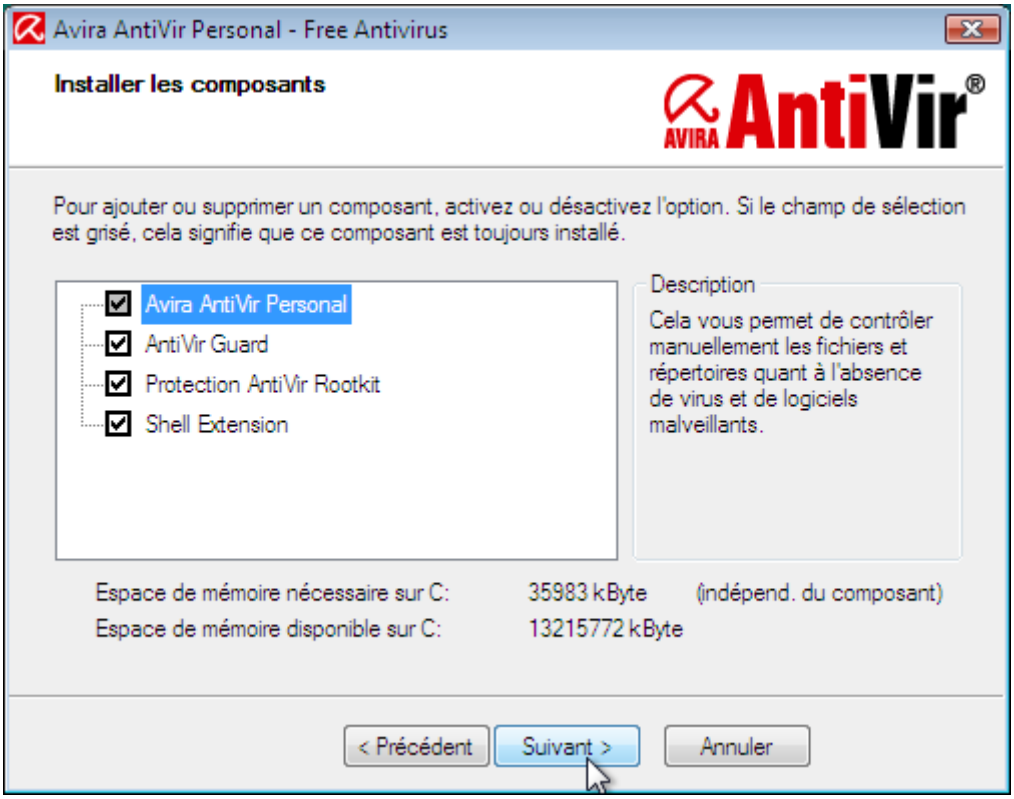
Cochez la case « Personnalisé » et cliquez sur « Suivant » :



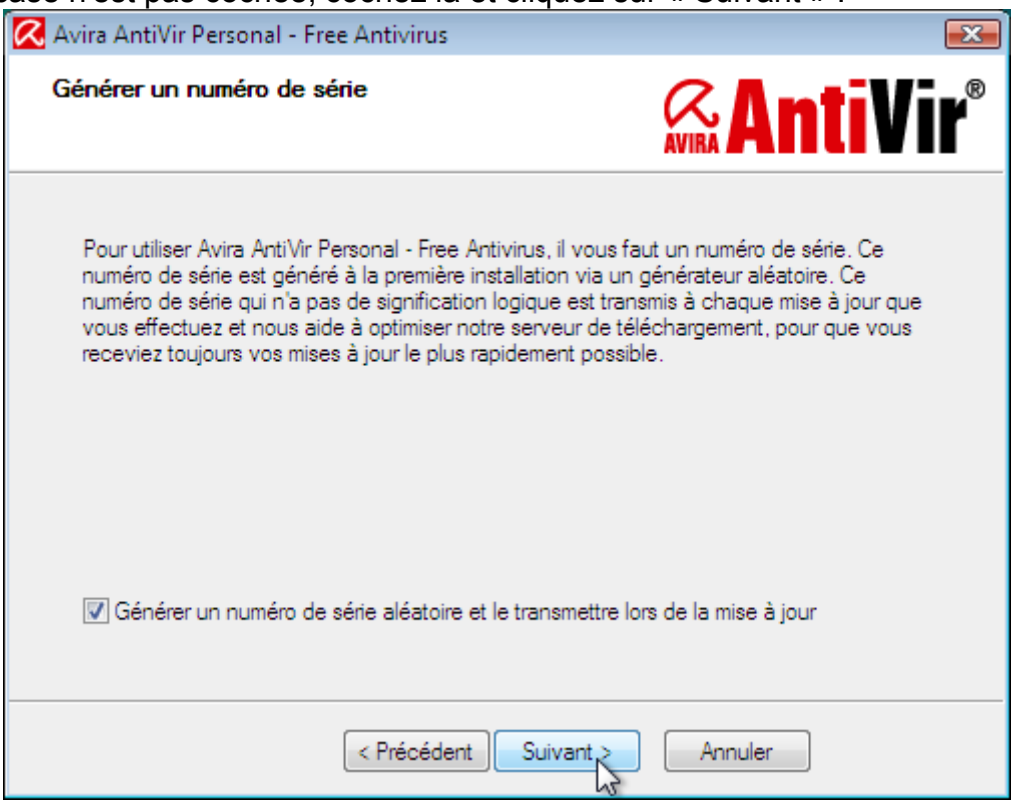
Cliquez sur le bouton « Suivant » :



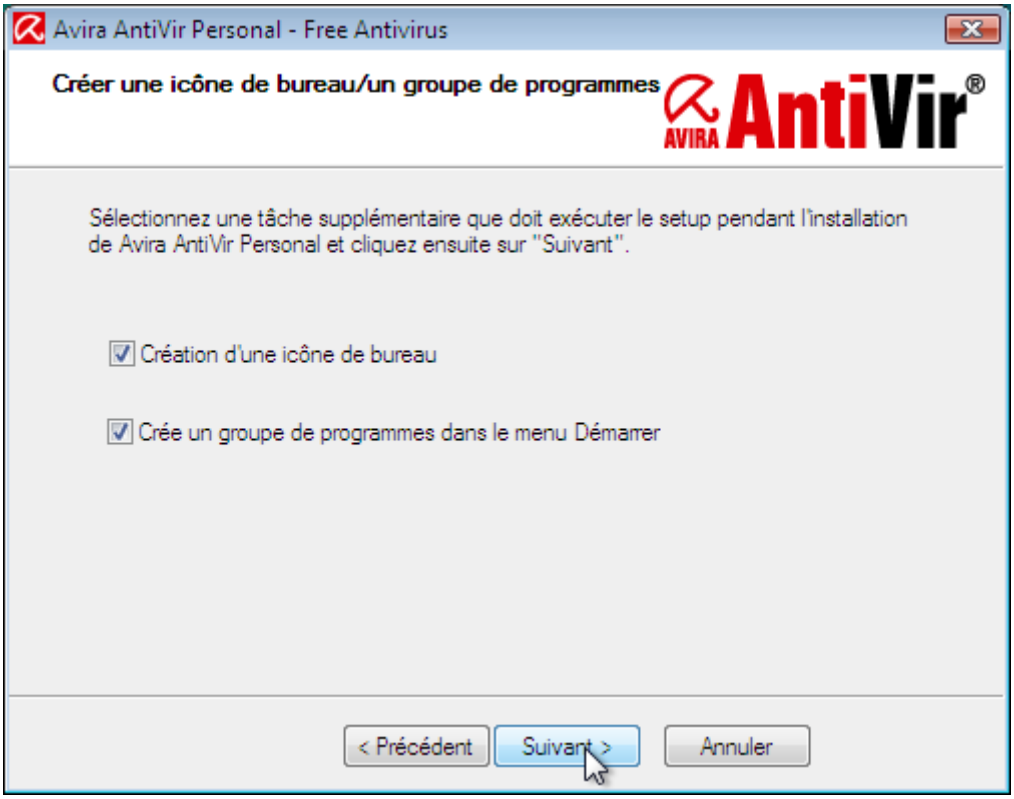
Cliquez sur le bouton « Suivant » :



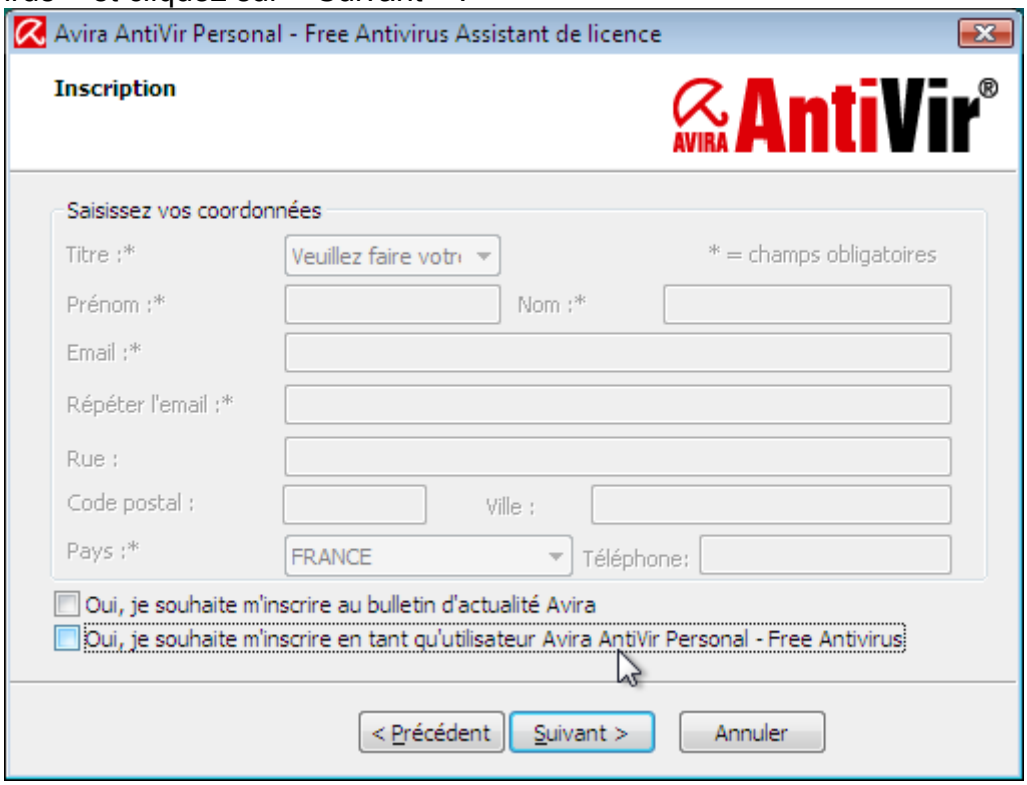
Si la case n'est pas cochée, cochez la et cliquez sur « Suivant » :



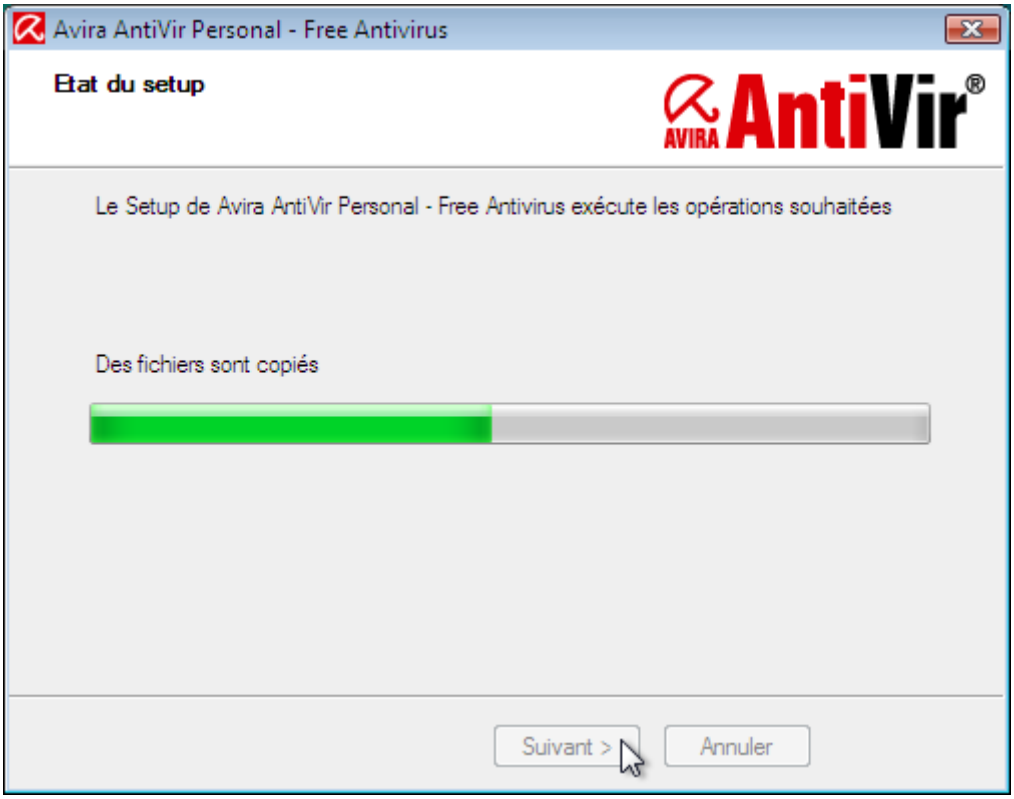
Cochez les deux cases (si elles ne sont pas déjà cochées) et cliquez sur le bouton « Suivant » :



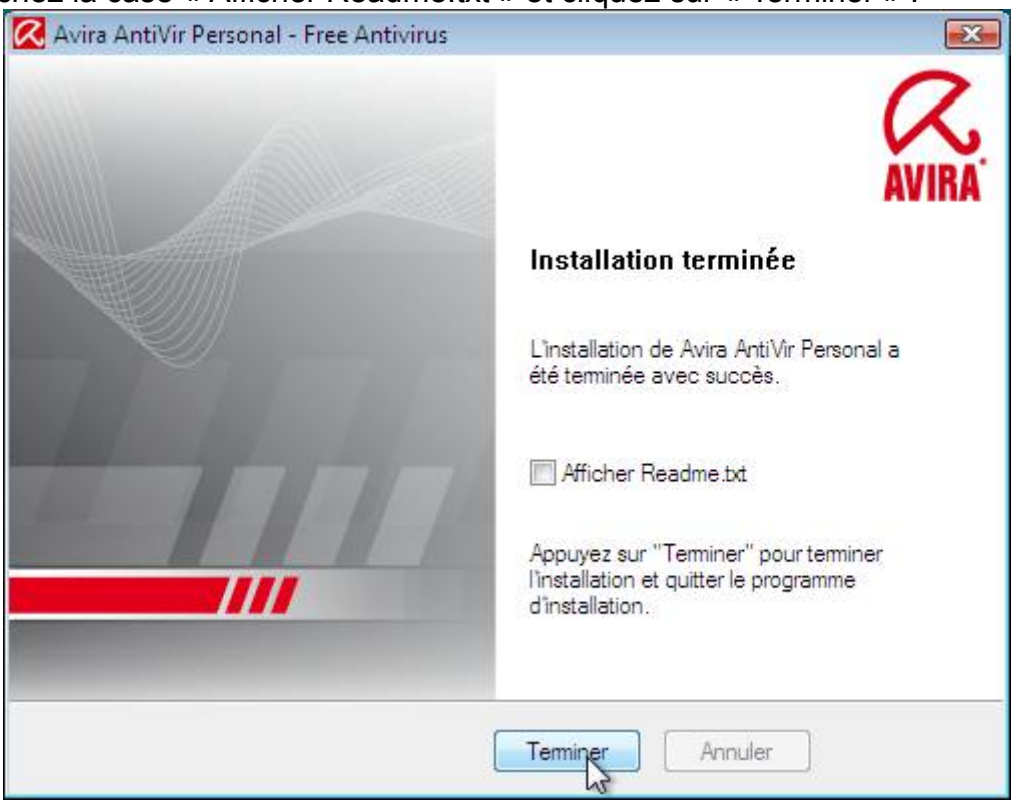
Décochez la case « Oui, je souhaite m'inscrire en tant qu'utilisateur Avira AntiVir Personal – Free Antivirus » et cliquez sur « Suivant » :



Veuillez patienter durant l'installation de AntiVir :



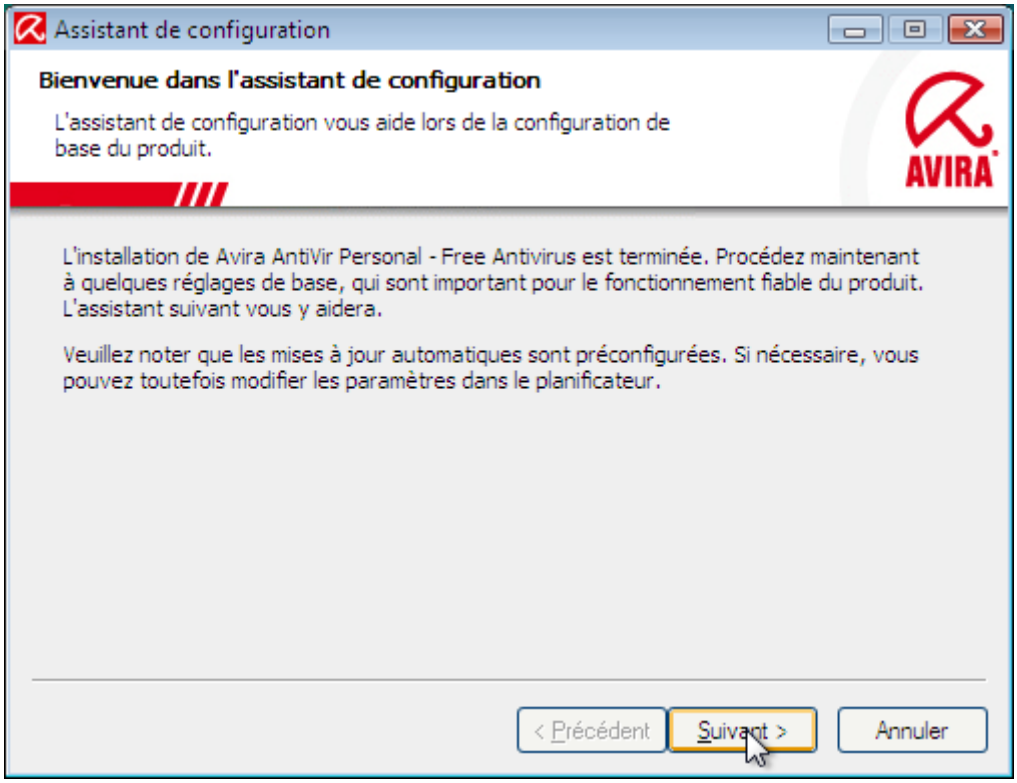
Décochez la case « Afficher Readme.txt » et cliquez sur « Terminer » :



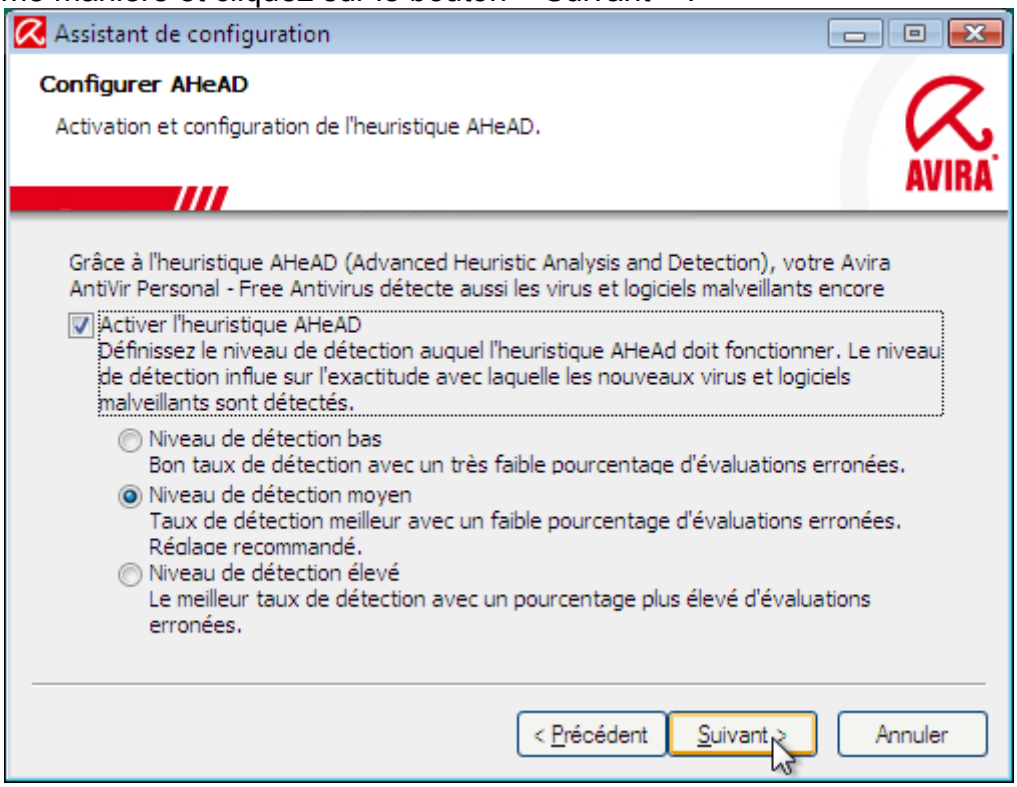
Une fois l'installation terminée, un assistant de configuration apparaitra. Veuillez suivre les instructions de la partie ci-dessous :

V.1.a.iii) <u>Assistant de configuration</u>

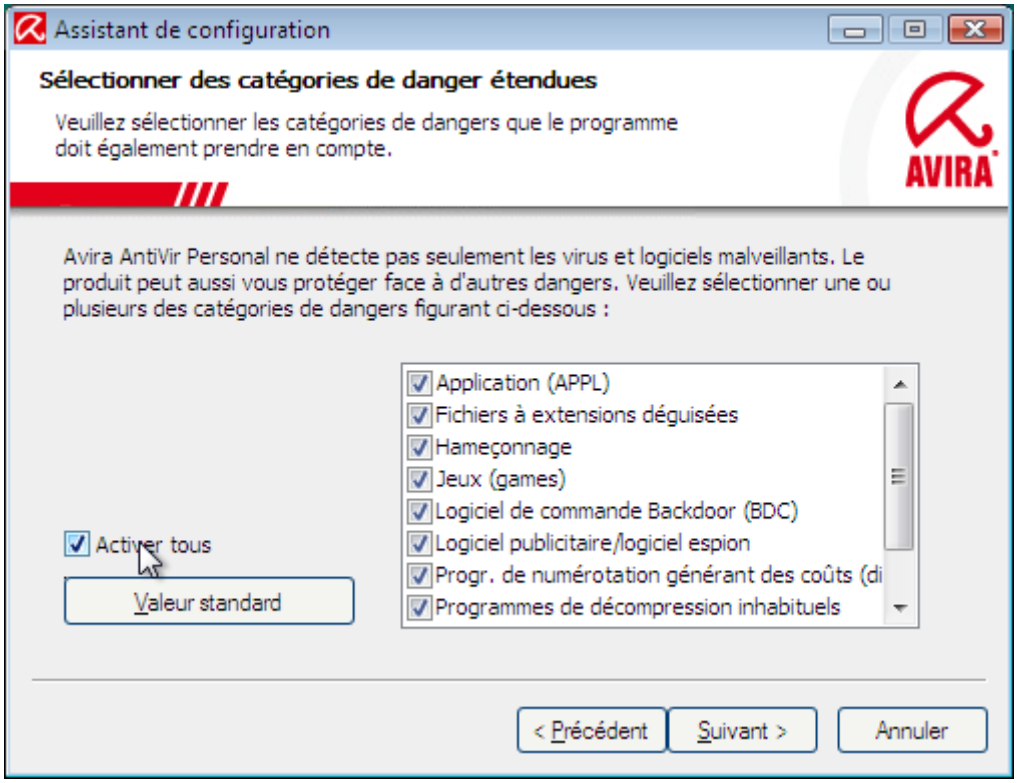
Première page, petite introduction qui explique qu'on va configurer AntiVir pour qu'il fonctionne correctement sur votre ordinateur. Cliquez sur « Suivant » :



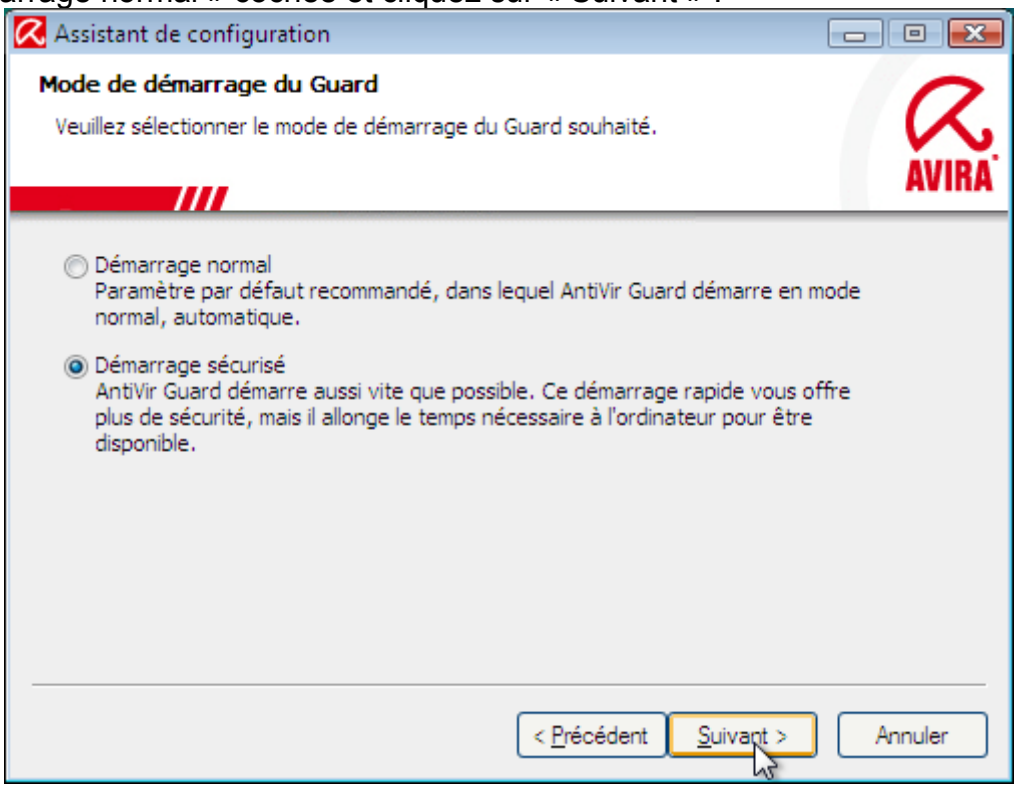
Si sur votre écran les cases sont cochées différemment de l'image ci-dessous, cochez les de la même manière et cliquez sur le bouton « Suivant » :



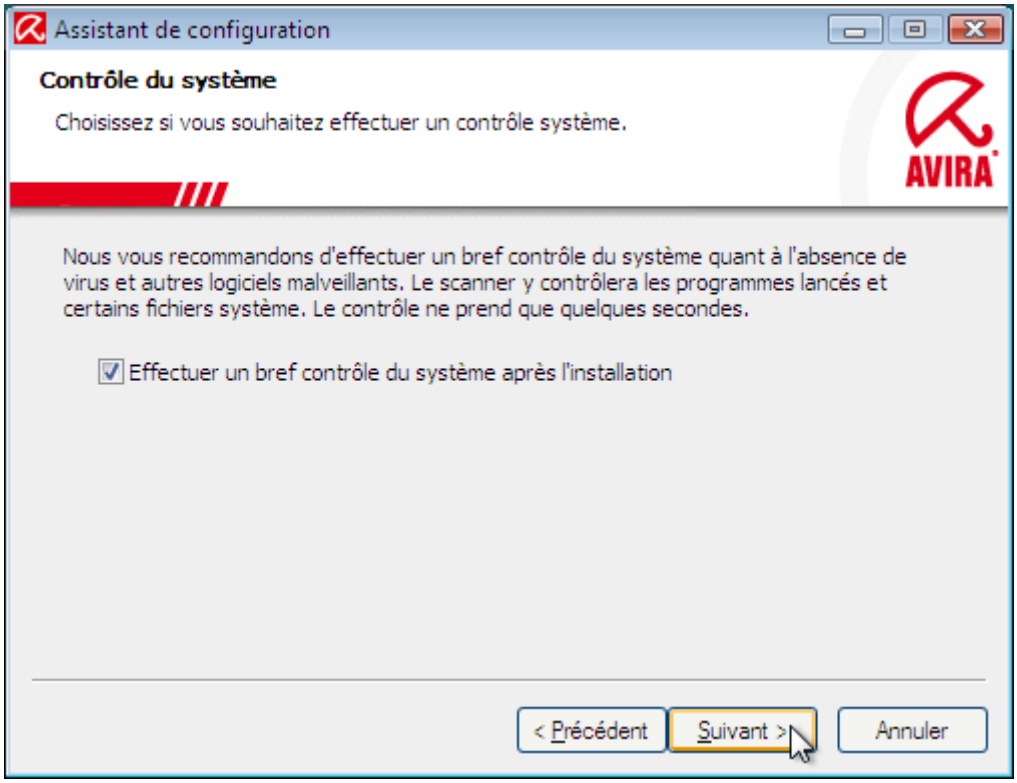
Cochez la case « Activer tous » et cliquez sur « Suivant » :



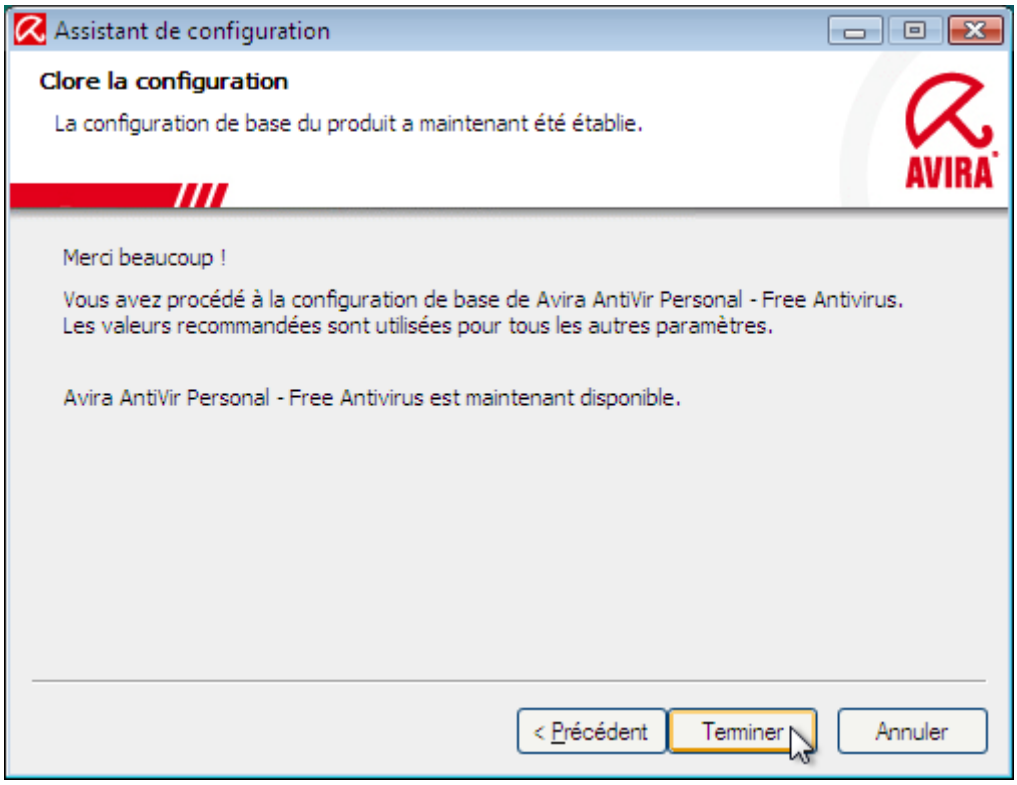
Si votre ordinateur est assez récent (deux ou trois ans au maximum), cochez la case « Démarrage sécurisé » et cliquez sur le bouton « Suivant ». Dans le cas contraire, laissez la case « Démarrage normal » cochée et cliquez sur « Suivant » :



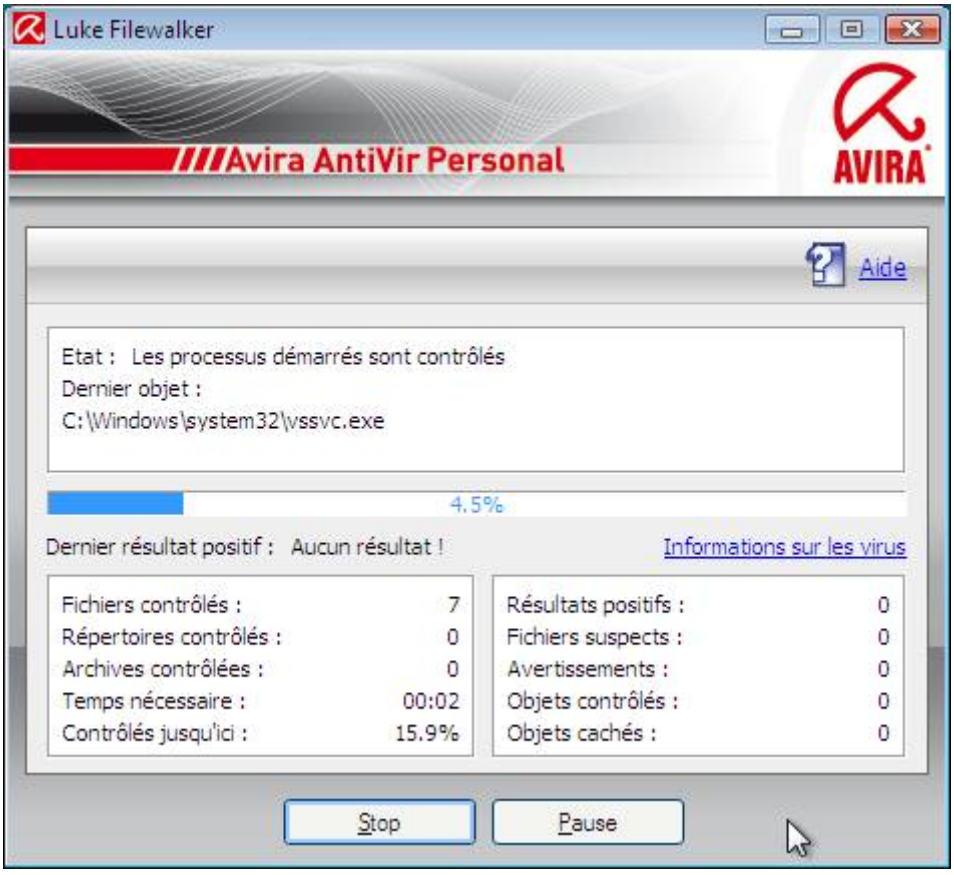
Cliquez sur « Suivant » :



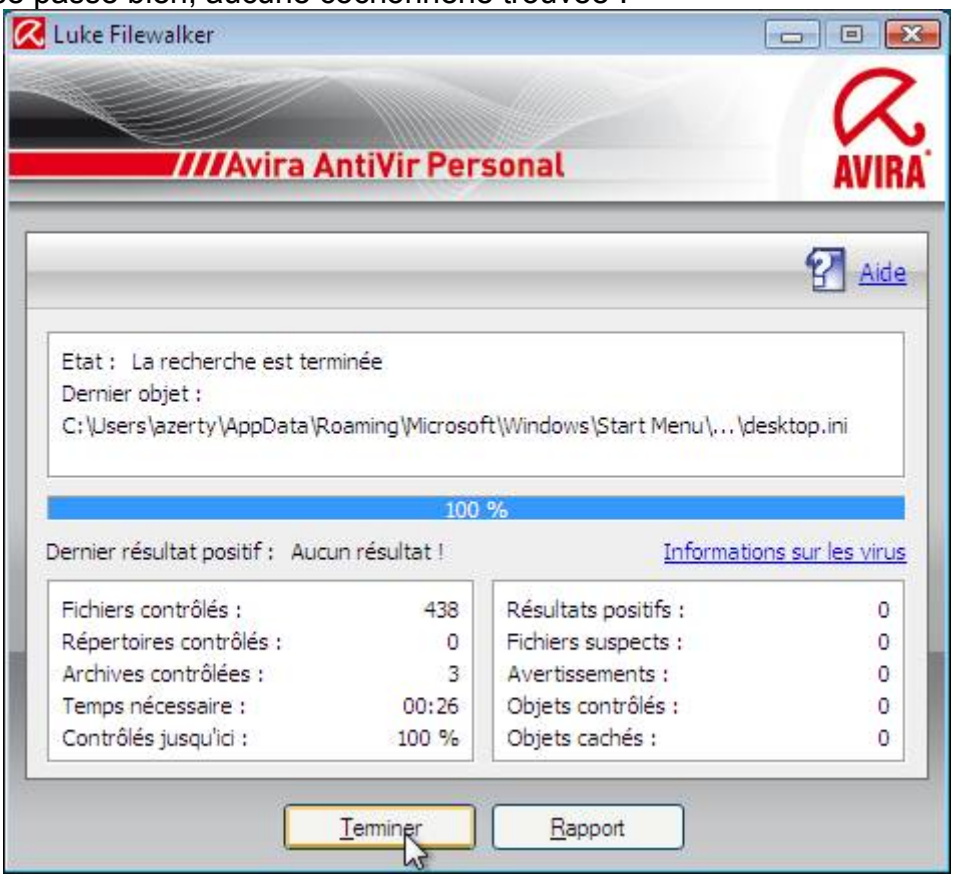
Cliquez sur le bouton « Terminer » :



Et voici l'analyse rapide dont ils parlaient :



Si tout se passe bien, aucune cochonnerie trouvée :



N'oubliez pas que ce n'était qu'un contrôle rapide. N'hésitez pas à faire une recherche plus approfondie pour être sûr.

V.1.a.iv) Mise à jour et publicité

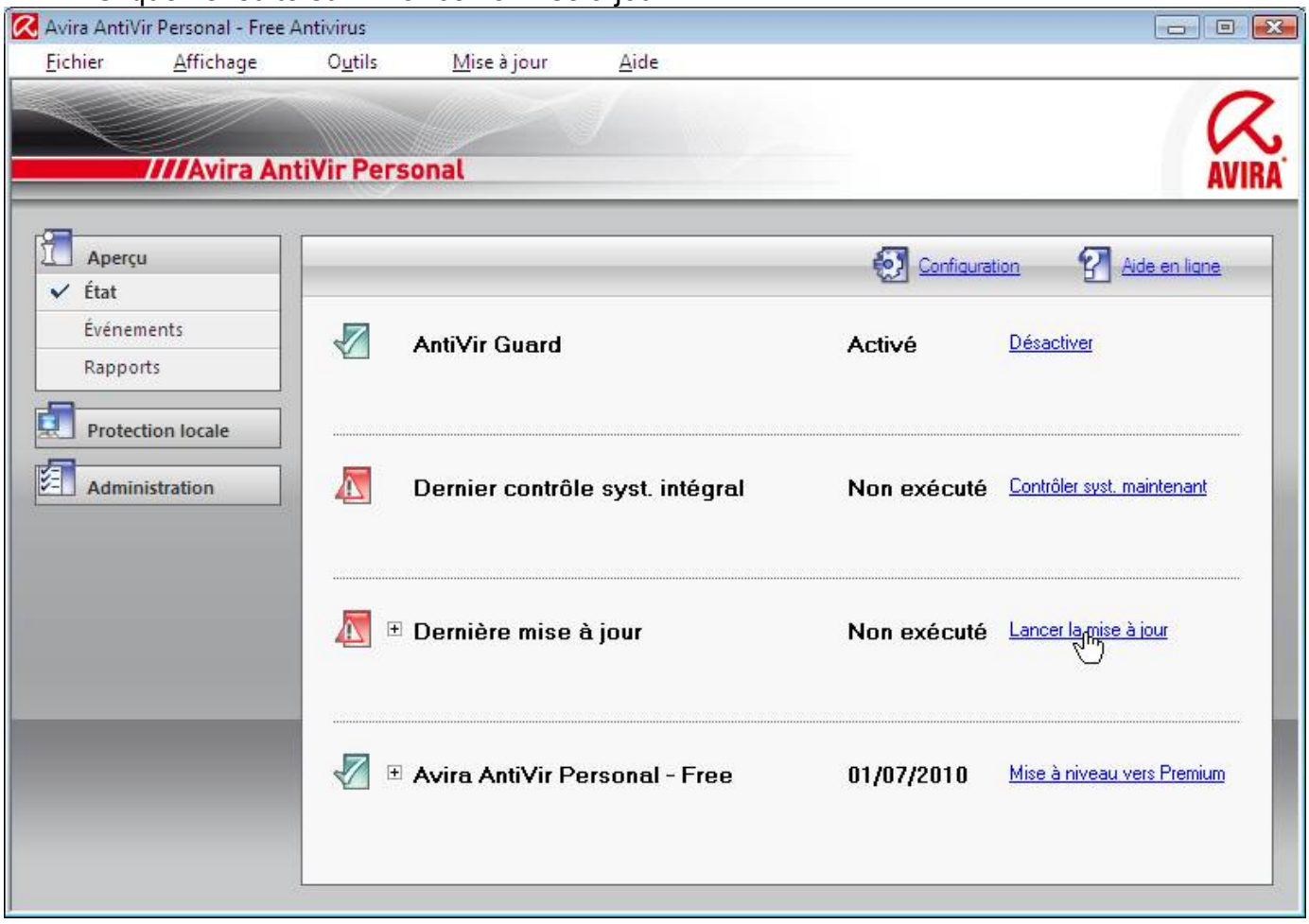
La mise à jour est automatique. Vous pourrez forcer la mise à jour si vous le souhaitez.

Une fenêtre de publicité pourra apparaître parfois. Il vous sera proposé d'acheter la version payante de AntiVir. Cliquez simplement sur OK.

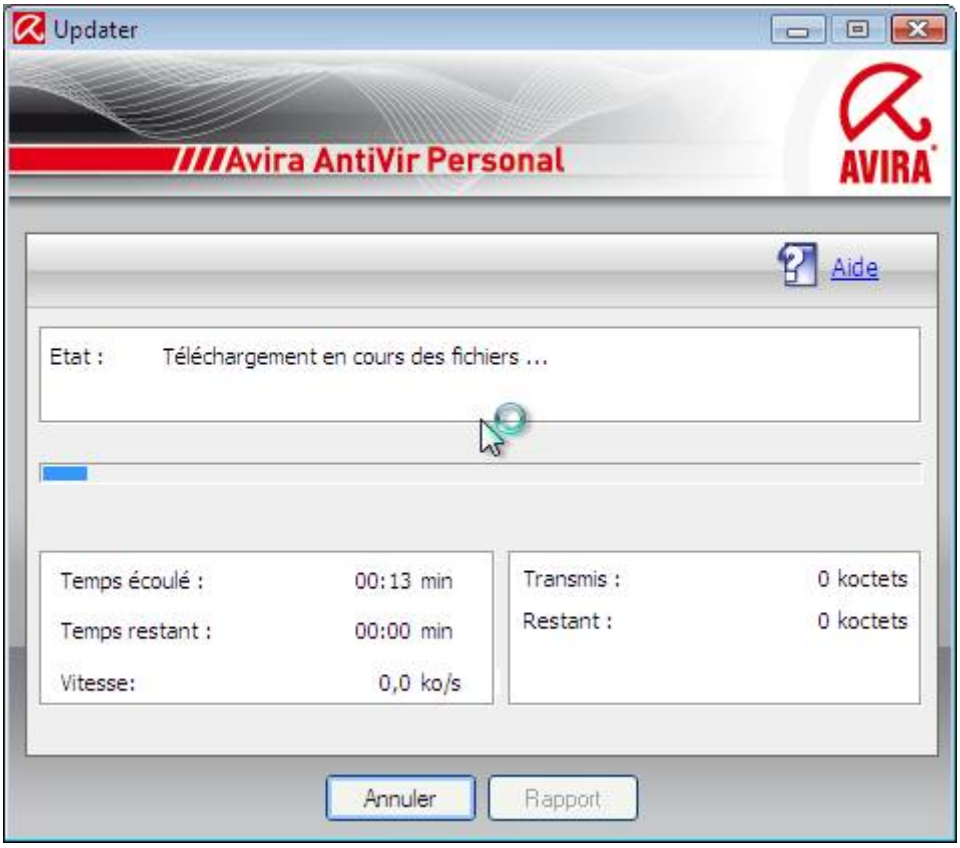
V.1.a.v) Forcer la mise à jour

Pour effectuer une analyse de votre ordinateur, double cliquez sur l'icône « Avira AntiVir Control Cetner » de votre bureau :

Cliquez ensuite sur « Lancer la mise à jour » :



Cette petite fenêtre indiquera la progression de la mise à jour. Elle disparaitra quand la mise à jour sera terminée :

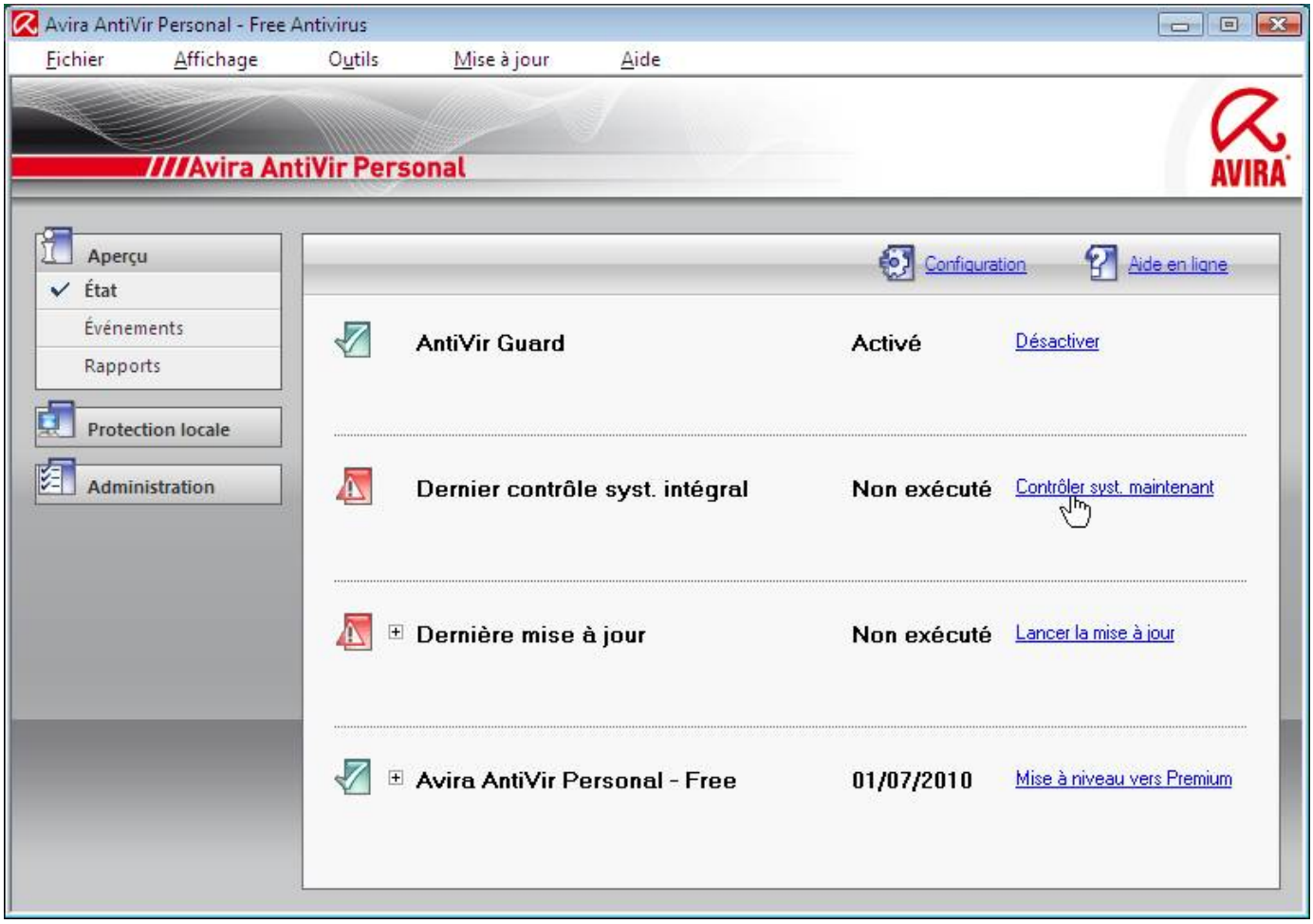


Cette autre fenêtre moins petite est une publicité pour la version payante de AntiVir. Cliquez simplement sur OK pour la faire disparaître :

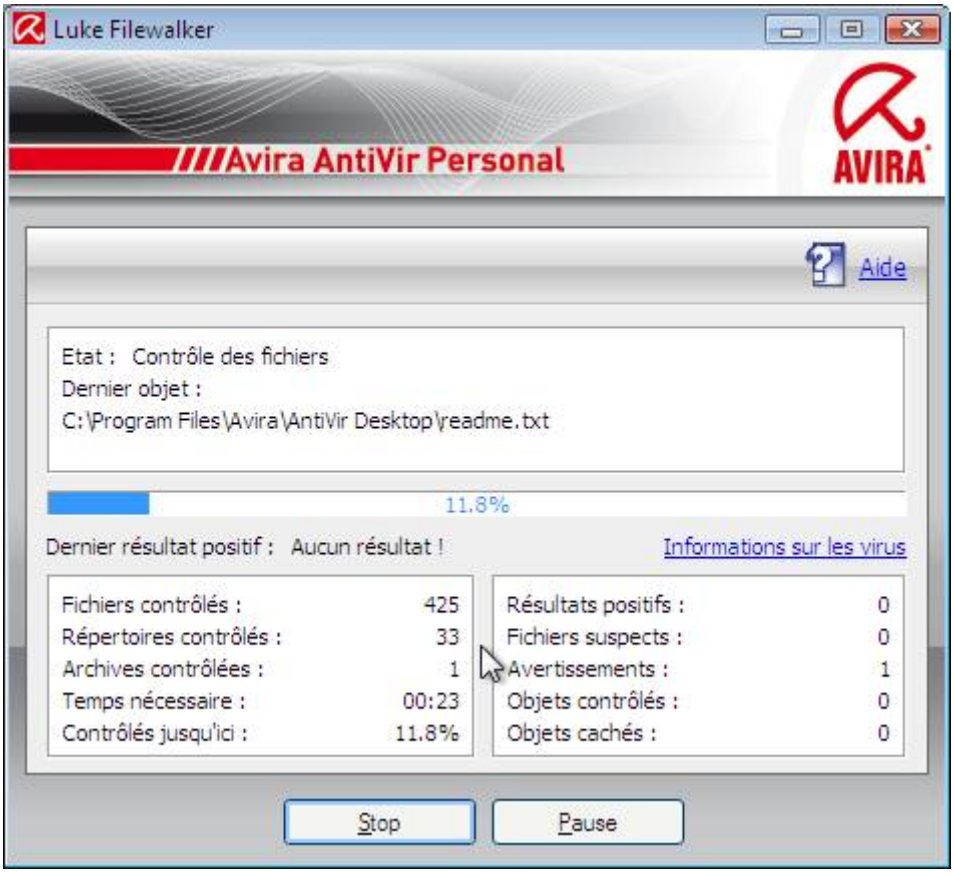
V.1.a.vi) <u>Effectuer une analyse de son ordinateur</u>

Pour effectuer une analyse de votre ordinateur, double cliquez sur l'icône « Avira AntiVir Control Cetner » de votre bureau :

Cliquez ensuite sur « Contrôler syst. maintenant » :

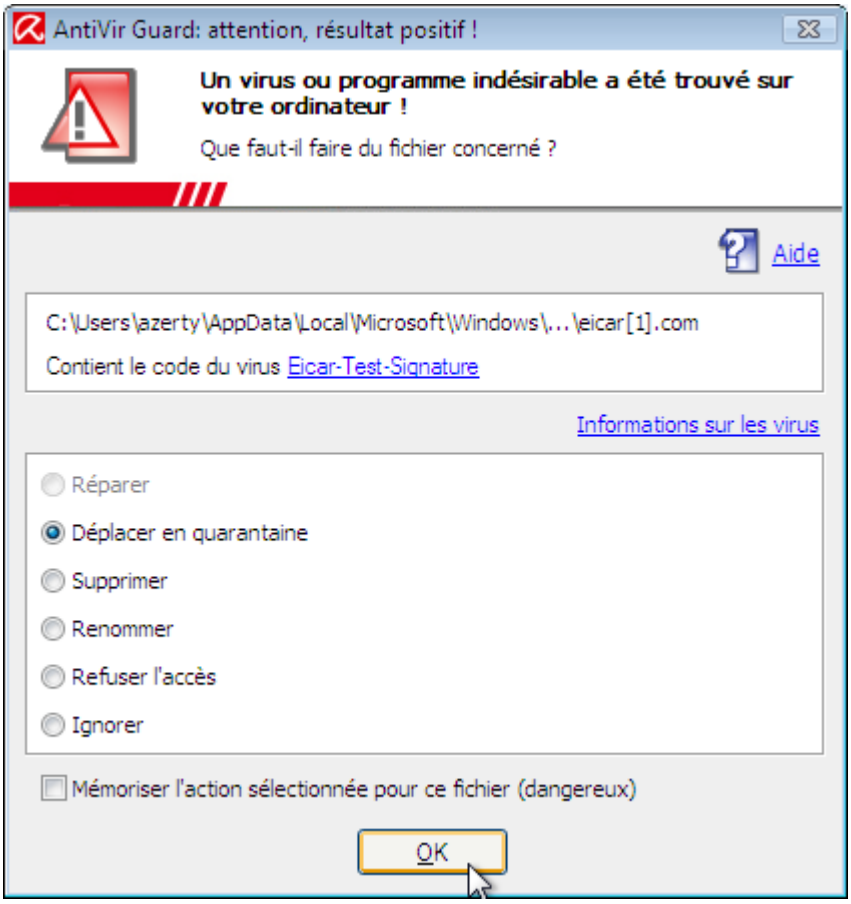


L'analyse sera ensuite lancée :



V.1.a.vii) <u>Répondre à une alerte</u>

Voici la fenêtre qui apparaît lorsque vous avez un virus dans votre ordinateur :



Plusieurs choix sont possibles :

• Réparer : Cela réparera le fichier si une sauvegarde non infectée de ce fichier existe

• Déplacer en quarantaine : Cela déplacera le fichier dans un dossier spécial de AntiVir d'une telle façon que le fichier ne sera pas exécuté (et donc le virus qui serait dans votre fichier ne sera pas lancé)

• Supprimer : Cela supprime le fichier

• Renommer : Cela permet de changer le nom du fichier (je ne vois pas l'intérêt d'une telle option)

• Refuser l'accès : Cela permettra de bloquer le fichier. Il sera toujours là, mais vous ne pourrez pas l'utiliser.

• Ignorer : Cela permet dans le cas d'un faux positif d'ignorer le fichier.

Dans la majeure partie des cas, il sera plus sûr de déplacer en quarantaine. En effet, il arrive régulièrement à certains antivirus de détecter des virus dans des fichiers n'en contenant pas. Cela leur arrive aussi de détecter des virus dans les fichiers indispensables au bon fonctionnement de l'ordinateur, et du coup, si vous supprimez le fichier vous aurez des problèmes de fonctionnement sur votre ordinateur.

La mise en quarantaine permet de récupérer le fichier si jamais il s'agissait d'un faux positif.

V.1.b) Tester un fichier en ligne

Il se peut que de temps en temps, votre antivirus détecte certains fichiers comme contenant un malware. Et parfois même, il s'agit de fichiers tout à fait légitimes.

En cas de doute avant de détruire définitivement un fichier ne contenant pas de virus, vous pouvez l'analyser sur Internet via un site qui le permet.

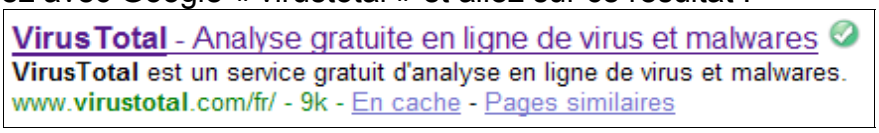
Vous pouvez faire ceci avec par exemple VirusTotal. Il permet d'analyser les fichiers que vous lui envoyez. VirusTotal analyse les fichiers avec une bonne trentaine de moteurs différents (en fait, ça fait comme si une trentaine d'antivirus donnaient leur avis sur votre fichier). Il se peut donc que votre antivirus y soit. Et il se peut aussi que peu d'antivirus détectent quelque chose de suspect dans votre fichier. Mais dans le cas où ils détectent tous quelque chose, votre fichier

est probablement bon à supprimer.

V.1.b.i) Avec Virustotal

Allez à l'adresse http://www.virustotal.com

Ou cherchez avec Google « virustotal » et allez sur ce résultat :

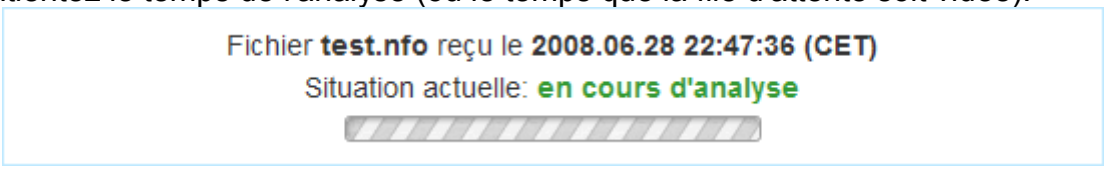


L'interface du site est en fait assez simple :

Pour commencer, cliquez sur le bouton « Parcourir ». Une boîte de dialogue vous permettra de rechercher le fichier suspect dans votre ordinateur. Sélectionnez votre fichier et cliquez sur le bouton « Ouvrir » de la boîte de dialogue.

Ceci fait, cliquez sur le bouton « Envoyer le fichier ».

Patientez le temps de l'analyse (ou le temps que la file d'attente soit vidée).



L'analyse est terminée lorsque ce même cadre indique quelque chose de ce genre :

Le résultat indique le nombre d'antivirus ayant déclaré votre fichier comme contaminé. En dessous de ce cadre, vous avez les résultats par antivirus (et les noms que donnent les antivirus à votre virus) :

Fichier **test.nfo** reçu le **2008.06.28 22:47:36 (CET)**
Situation actuelle: **terminé**
Résultat: **33/33 (100%)**

Formaté | Impression des résultats

Antivirus	Version	Dernière mise à jour	Résultat
AhnLab-V3	2008.6.27.1	2008.06.27	EICAR_Test_File
AntiVir	7.8.0.59	2008.06.28	Eicar-Test-Signature
Authentium	5.1.0.4	2008.06.28	EICAR_Test_File
Avast	4.8.1195.0	2008.06.28	EICAR Test-NOT virus!!
AVG	7.5.0.516	2008.06.28	EICAR_Test (+1)
BitDefender	7.2	2008.06.28	EICAR-Test-File (not a virus)
CAT-QuickHeal	9.50	2008.06.28	EICAR Test File
ClamAV	0.93.1	2008.06.28	Eicar-Test-Signature
DrWeb	4.44.0.09170	2008.06.28	EICAR Test File (NOT a Virus!)
eSafe	7.0.17.0	2008.06.26	EICAR Test File
eTrust-Vet	31.6.5911	2008.06.27	the EICAR test string

(image coupée exprès car elle prenait beaucoup de place pour pas grand chose)

Lorsque l'un des antivirus détecte que le fichier est saint, un petit trait apparaît :

Antivirus	Version	Dernière mise à jour	Résultat
ClamAV	0.93.1	2008.06.28	-
F-Secure	7.60.13501.0	2008.06.26	-
Microsoft	1.3704	2008.06.28	-
Norman	5.80.02	2008.06.27	-
Panda	9.0.0.4	2008.06.28	-
Prevx1	V2	2008.06.28	-
Webwasher-Gateway	6.6.2	2008.06.28	-

Il ne vous reste plus qu'à espérer que votre fichier apparaisse sain pour la majorité des antivirus.

V.1.b.ii) Autres adresses

Nom de la page	URL	Limitations
Online malware scan	http://virusscan.jotti.org/	10 Mo / fichier
Virus.Org :: Malware Scanning Service	http://scanner.virus.org/	5 Mo / fichier

V.1.c) Analyser tout son ordinateur avec un antivirus en ligne

Il se pourrait aussi que votre antivirus soit infecté / désinstallé (par un virus, ou par le fait que vous ne l'ayez pas renouvelé). Bref, votre ordinateur pourrait être compromis et votre

antivirus pourrait ne pas pouvoir vous aider.

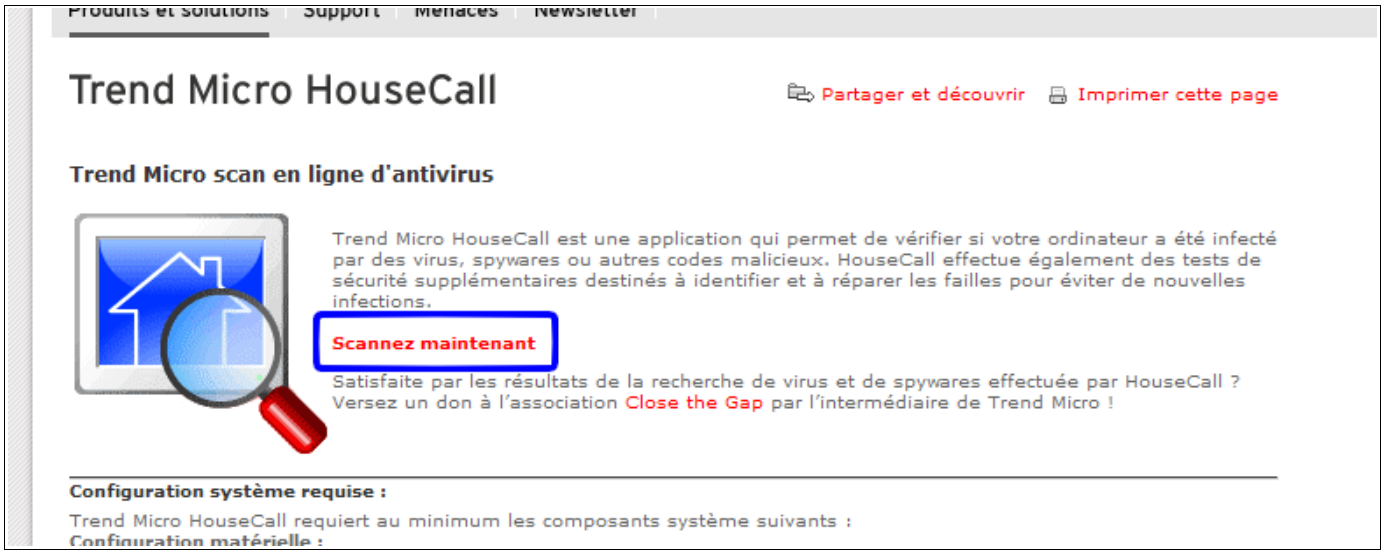
Il y a donc encore une autre solution : l'antivirus en ligne.

Un antivirus de ce type ne s'installe que temporairement dans votre ordinateur et la plupart permettent de supprimer les malware qui seraient présents dans votre ordinateur. Je dis la plupart car il y en existe certains qui ne sont qu'une publicité de leurs équivalents payants (et donc ne proposent pas toujours la suppression des malwares).

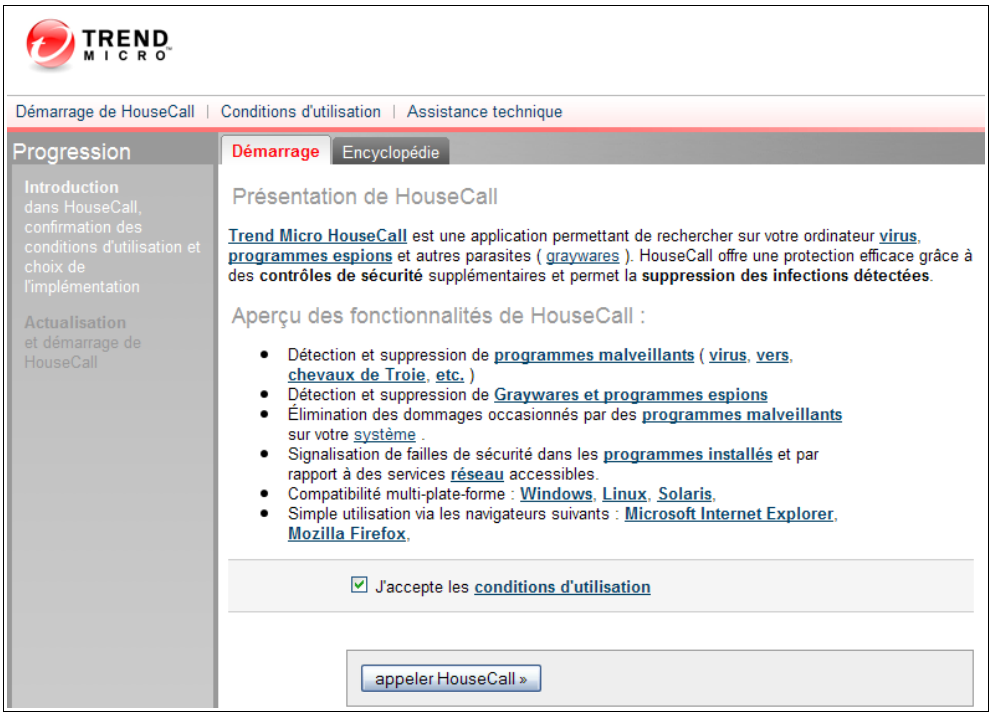
V.1.c.i) Avec Trend Micro HouseCall

Tapez « House call » sur Google et cherchez ce résultat :

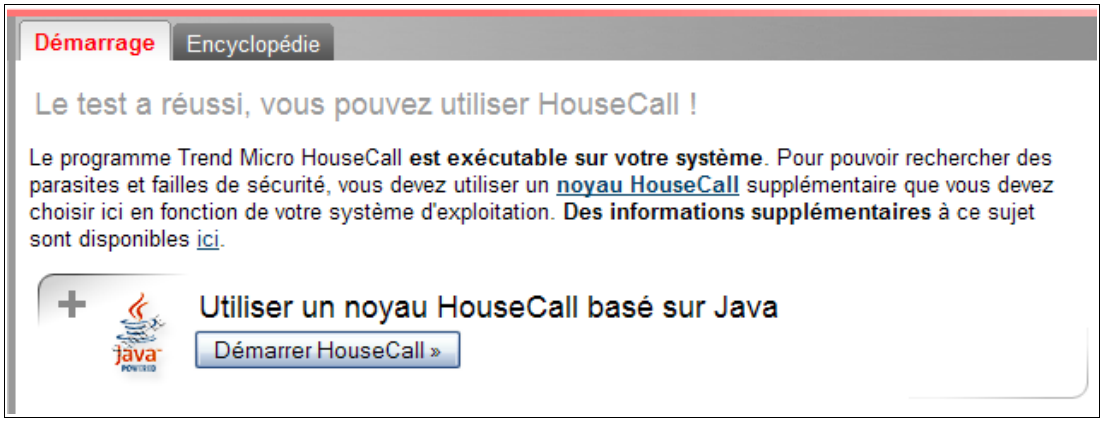
Allez sur la page.



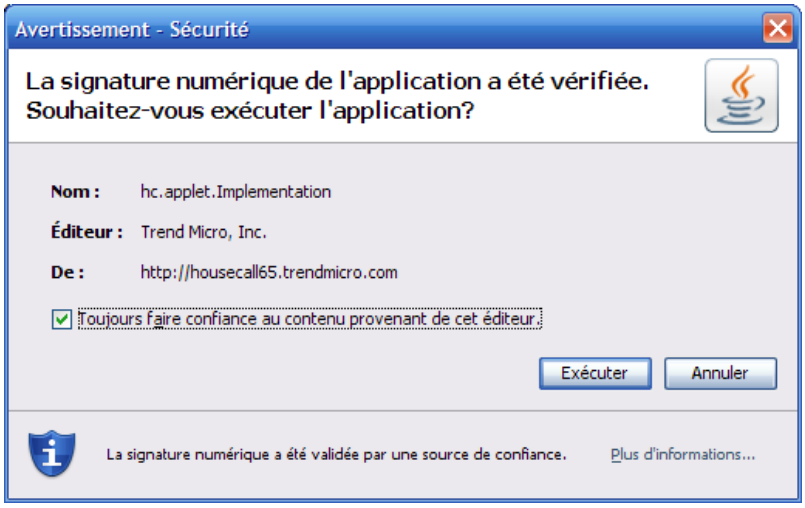
Cliquez ensuite sur le lien « Scannez maintenant ».



Si la case « J'accepte les conditions d'utilisation » n'est pas déjà cochée, cochez la.
Cliquez ensuite sur le bouton « appeler HouseCall ».

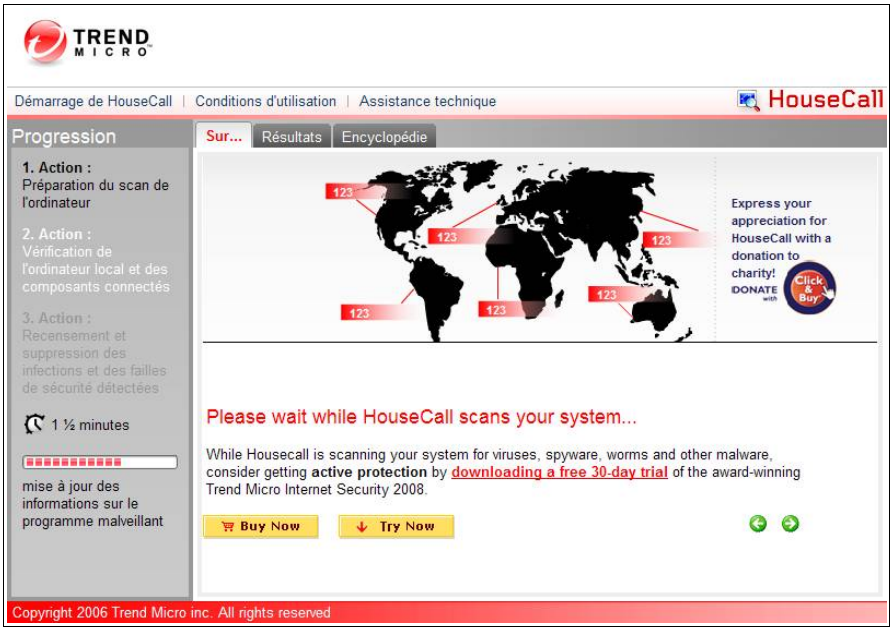


Un test pour savoir si votre ordinateur est compatible est effectué. Une fois le test terminé, cliquez sur le bouton « Démarrer HouseCall » en dessous du texte « Utiliser un noyau HouseCall basé sur Java ».

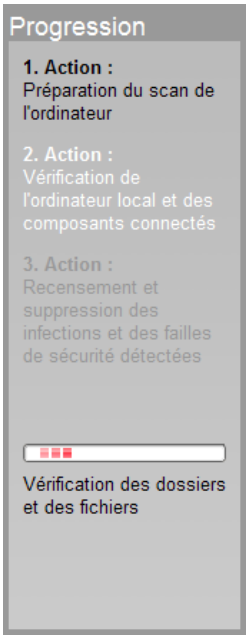


Cliquez sur le bouton « Exécuter ».

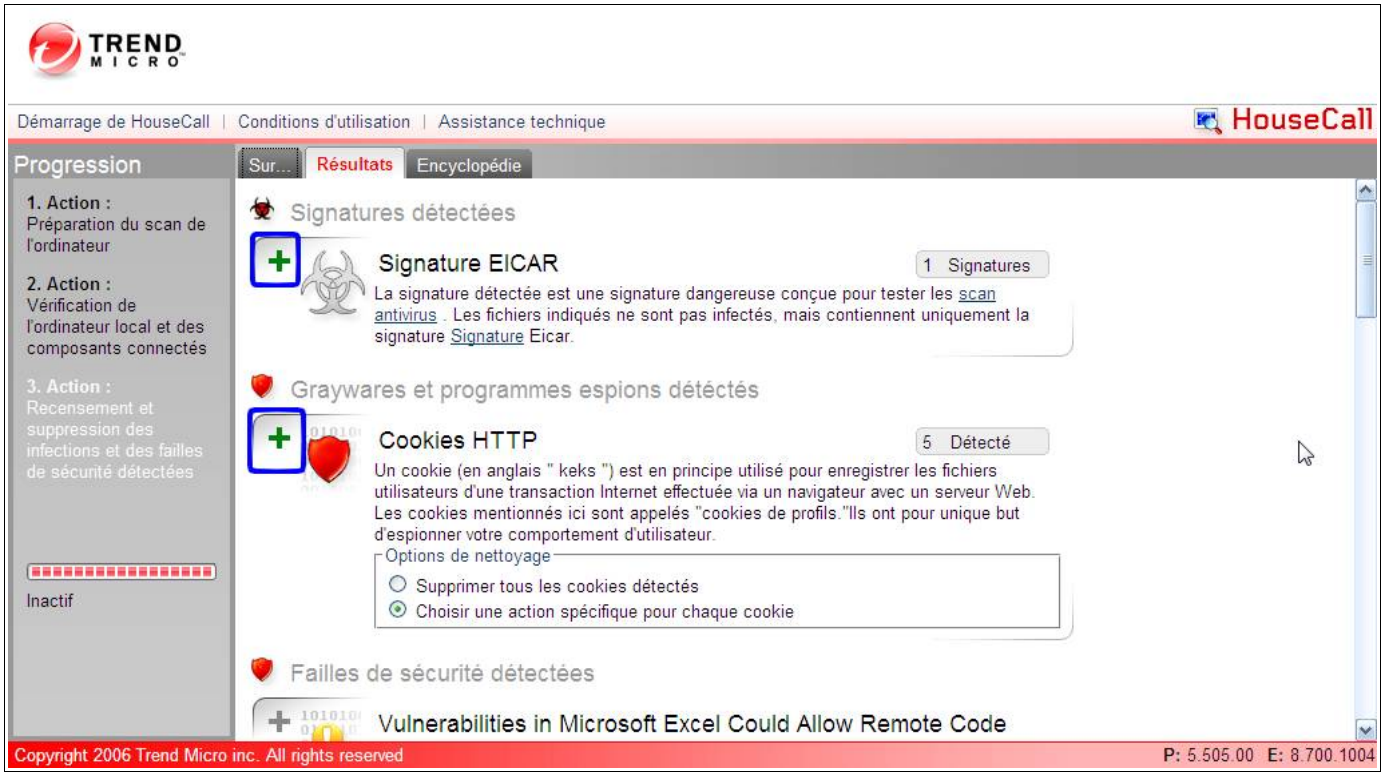
On va effectuer une recherche sur l'intégralité de votre ordinateur. Pour ceci, cliquez sur le bouton « Continuer ».



Pendant la mise à jour de l'antivirus en ligne, une petite pub pour la version complète l'antivirus de TrendMicro apparaitra.

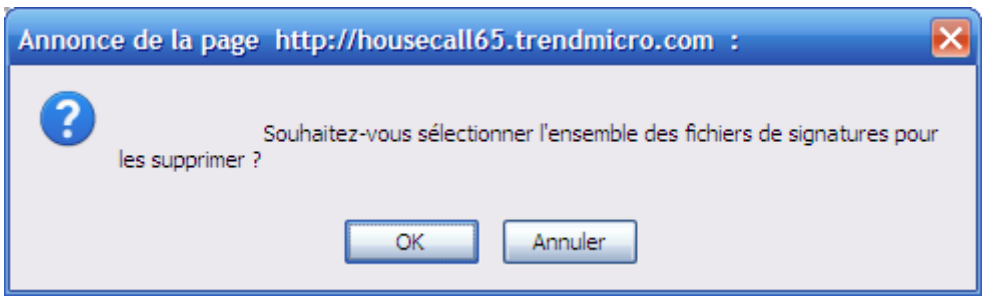


La progression est affichée dans la partie gauche du site.



Lorsque la page de résultats apparaît toute seule (elle était déjà disponible pendant le scan), c'est que le scan est terminé. Cliquez sur chaque plus vert (voir cadres bleus de l'image ci-dessus).

Cliquez ensuite sur la croix rouge (voir carré rouge de l'image ci-dessus) de chaque tableau.



Un message de confirmation apparaîtra. Cliquez sur OK pour supprimer la menace.

V.1.c.ii) Autres adresses

Ces antivirus en lignes sont compatibles avec Internet Explorer et Firefox :

Nom	Url
Panda ActiveScan	http://www.pandasecurity.com/activescan/

C'est malheureusement le seul autre antivirus en ligne qui existe (ne pas comprendre ça dans le sens que ça soit dommage que ce soit Panda, je n'ai rien contre Panda). Il en existe de nombreux autres antivirus en ligne, mais il vous faudra obligatoirement utiliser Internet Explorer.

Antivirus en ligne compatibles avec Internet Explorer uniquement :

Nom	Url
Windows Live Onecare	http://onecare.live.com/site/fr-be/
Symantec Security Check	http://security.symantec.com/sscv6/
Kaspersky Online-Scanner	http://webscanner.kaspersky.fr/
F-Secure Online Virus Scanner	http://support.f-secure.fr/fra/home/ols.shtml
et plein d'autres encore ...	

V.1.d) Conflit Antivirus en ligne et hors ligne

Si vous avez installé un antivirus dans votre ordinateur (ce que je vous recommande bien entendu) et que vous avez déjà rencontré un virus qui a été placé en quarantaine, il est très probable que si vous faites une analyse en ligne, l'antivirus en ligne trouve ce même virus dans la quarantaine de celui installé dans votre ordinateur.

Ce comportement est tout à fait normal et il se peut donc que votre ordinateur n'ait pas de virus en activité.

Pour être sûr d'une analyse en ligne, effectuez d'abord un vidage de la quarantaine de l'antivirus installé sur votre ordinateur avant de lancer l'analyse.

V.2) Antispyware

Nous utiliserons deux logiciels pour se protéger contre les spywares.

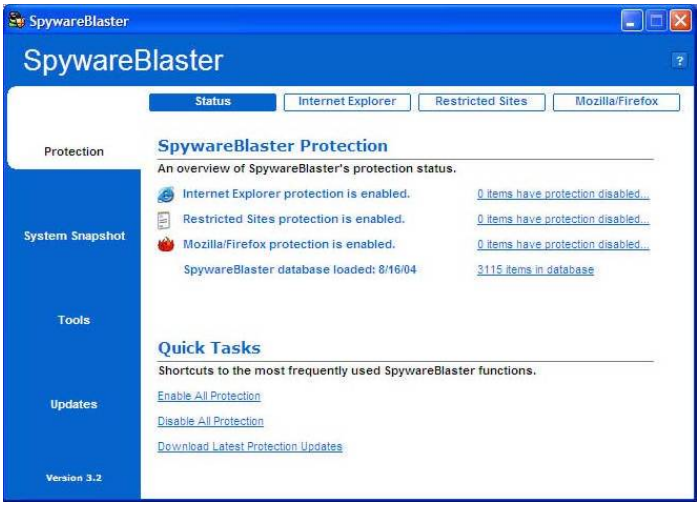
Ces deux logiciels ont une façon différente de protéger. SpywareBlaster empêchera l'installation de certains logiciels espions en interdisant l'accès à certains sites dangereux, et MalwareBytes permettra d'analyser votre ordinateur.

V.2.a) SpywareBlaster

Ce logiciel permet une protection passive en interdisant l'installation une sélection de logiciels espions.

Les différentes étapes expliquées dans cette partie seront plus découpées car certaines feront appel à d'autres. Commençons par le téléchargement du logiciel.

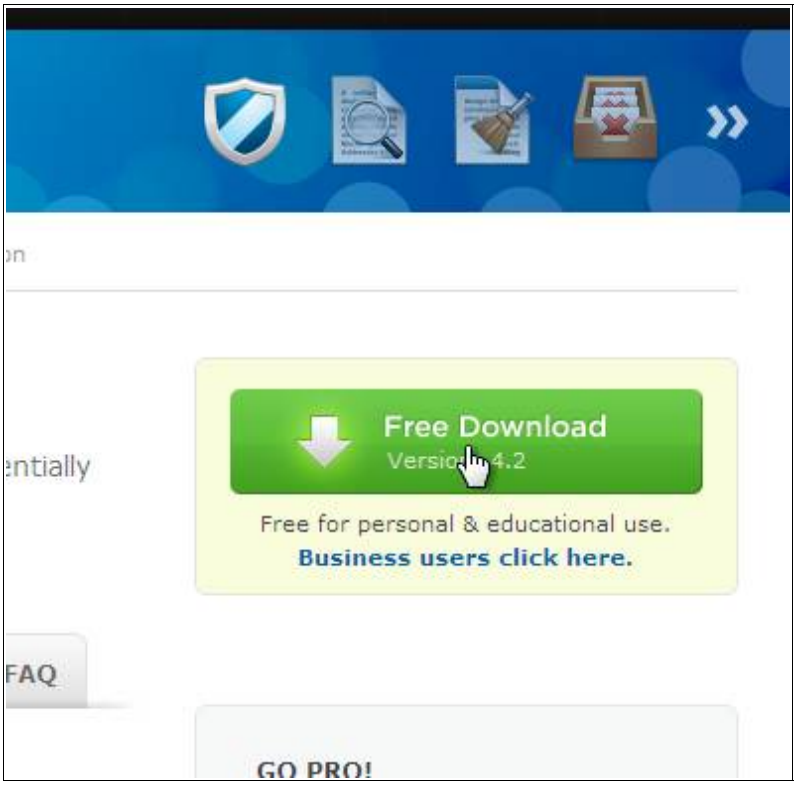
Si vous avez déjà SpywareBlaster d'installé sur votre ordinateur, et si la fenêtre principale du logiciel ressemble à l'image ci-dessous, pour installer le logiciel, passez à l'étape Erreur : source de la référence non trouvée à la page Erreur : source de la référence non trouvée.



V.2.a.i) Téléchargement du logiciel

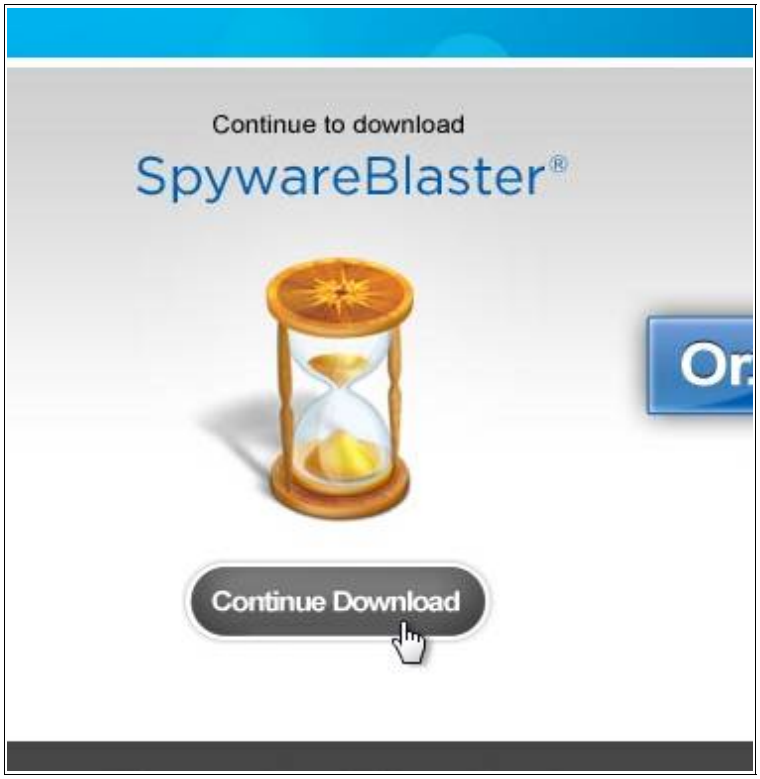
Utilisez votre moteur de recherche préféré pour aller sur le site officiel de SpywareBlaster (voici la page qu'il faut trouver : [http://www.javacoolsoftware.com/spywareblaster.html)](http://www.javacoolsoftware.com/spywareblaster.html)

Cliquez ensuite sur « Free Download » :



Cliquez ensuite sur le premier des trois liens (voir le cadre vert de l'image ci-dessous :

Cliquez ensuite sur « Continue Download » :

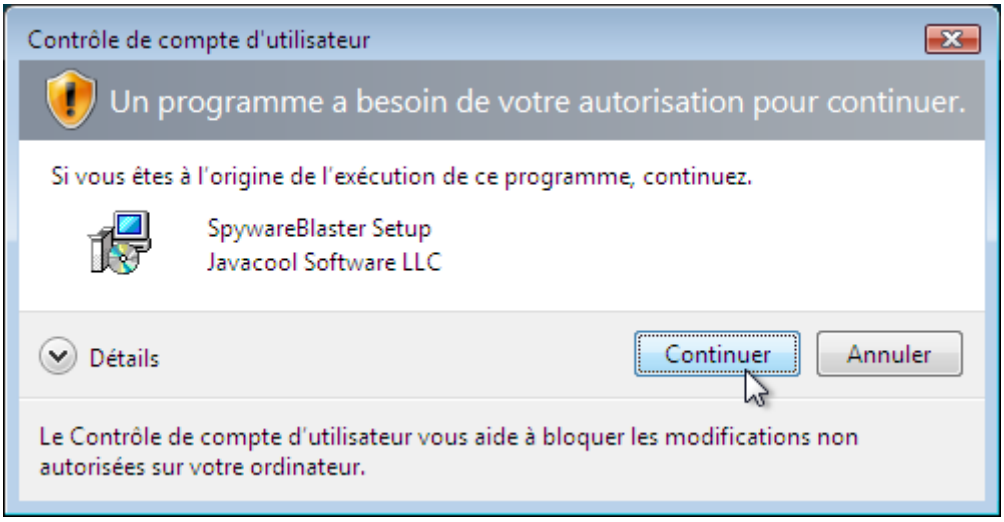


Cliquez ensuite sur le troisième lien. La procédure est ensuite la procédure habituelle de téléchargement de votre navigateur.

V.2.a.ii) Installation du logiciel

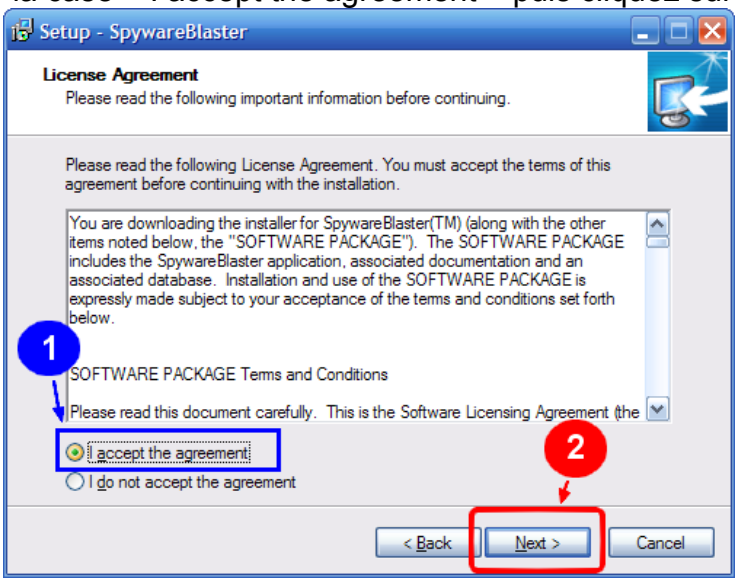
Ouvrez le fichier précédemment téléchargé.

Sous Windows Vista ou Windows 7, le « Contrôle de compte d'utilisateur » apparaitra. Cliquez sur « Continuer » :

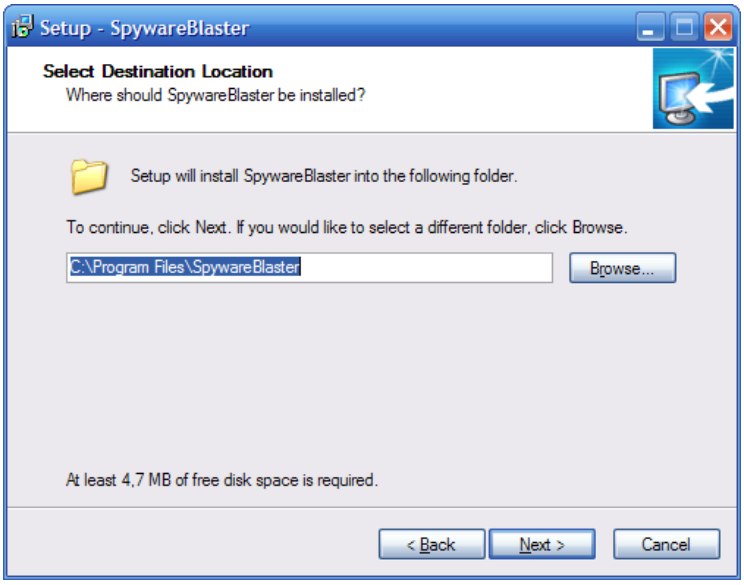


Lorsque vous aurez cette fenêtre, cliquez sur « Next » :

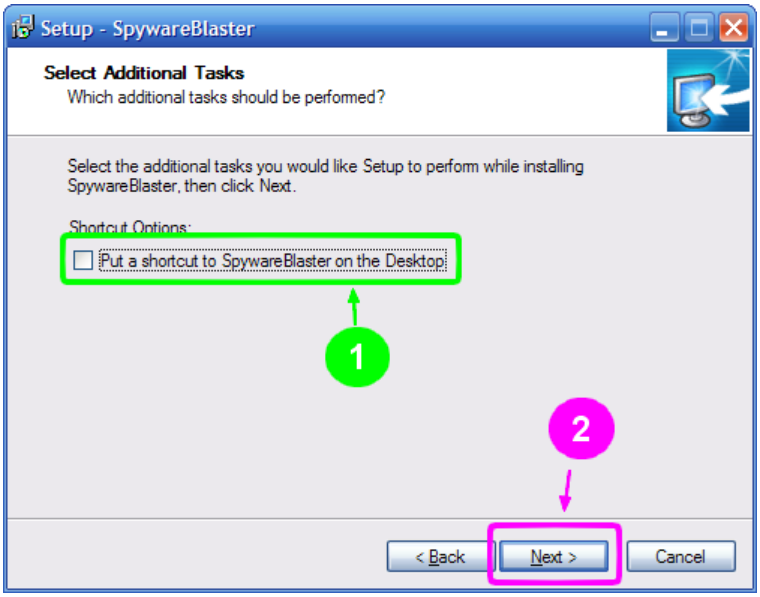
Cochez ensuite la case « I accept the agreement » puis cliquez sur « Next ».



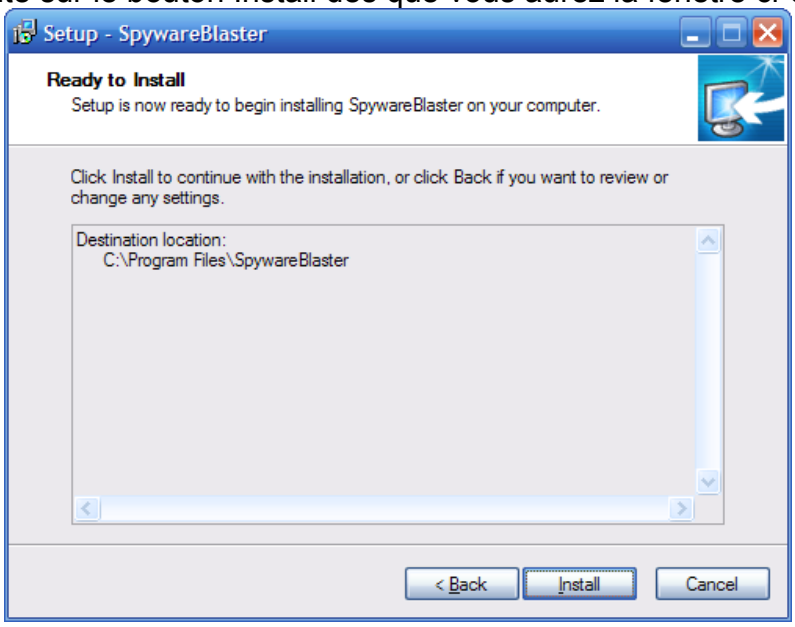
Cliquez ensuite sur « Next » :



Cochez ensuite la case « Put a shortcut to SpywareBlaster on my Desktop », puis cliquez sur Next :



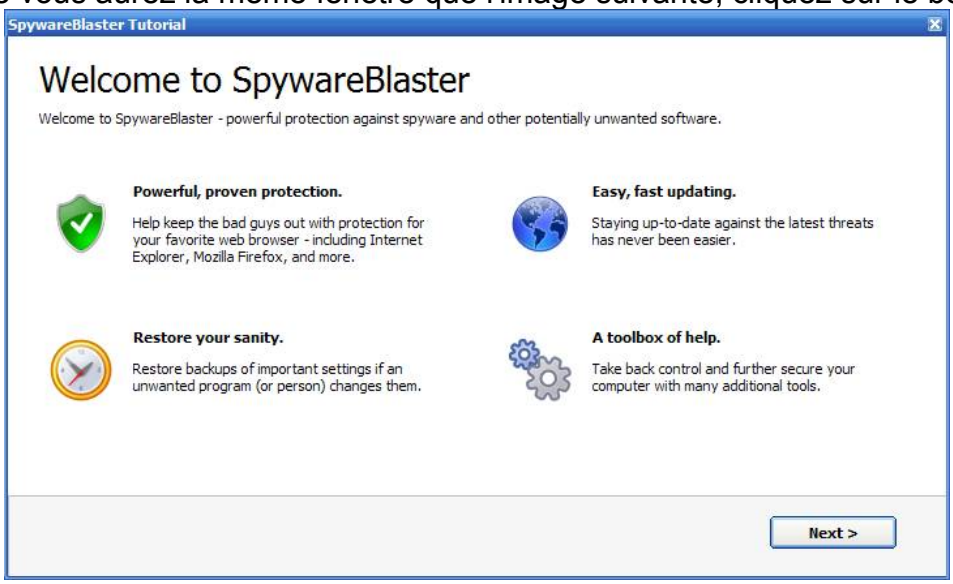
Cliquez ensuite sur le bouton Install dès que vous aurez la fenêtre ci-dessous :



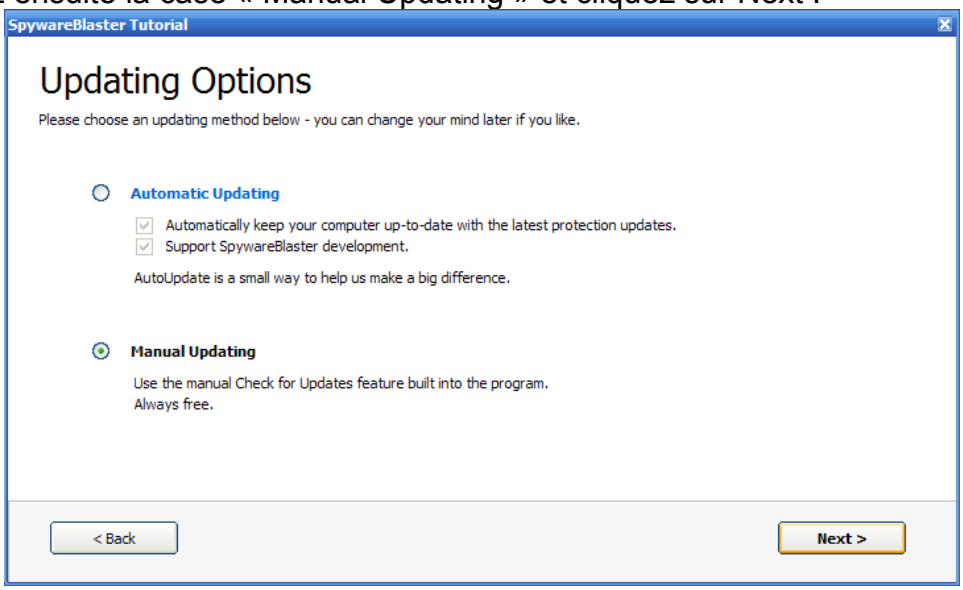
Peu de temps après, vous aurez cette fenêtre, cliquez sur Finish (et laissez la case cochée) :

V.2.a.iii) *<u>Assistant de premier lancement</u>*

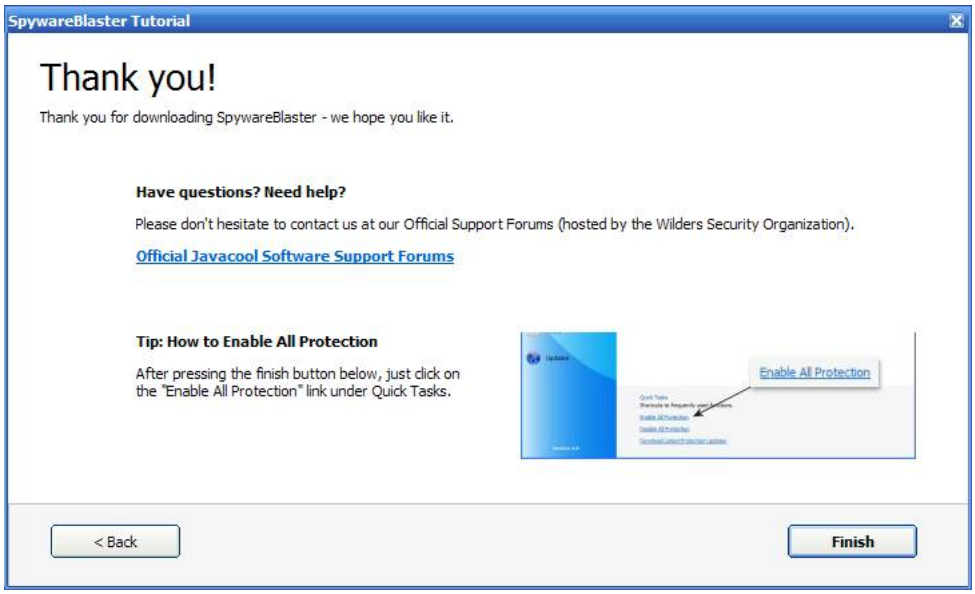
Au premier démarrage de SpywareBlaster, vous aurez un petit assistant de départ.
Dès que vous aurez la même fenêtre que l'image suivante, cliquez sur le bouton Next :



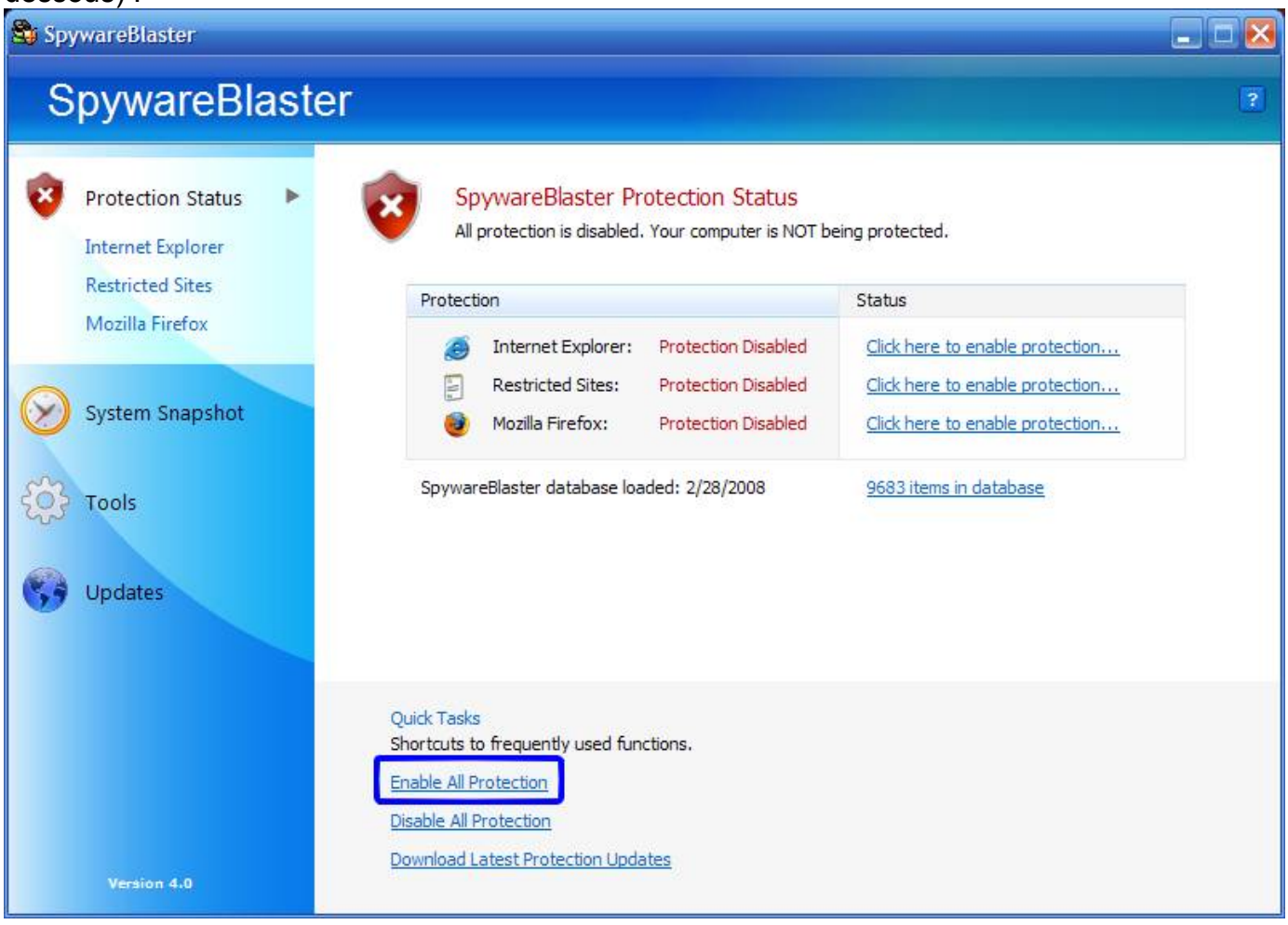
Cochez ensuite la case « Manual Updating » et cliquez sur Next :



Cliquez ensuite sur Finish :

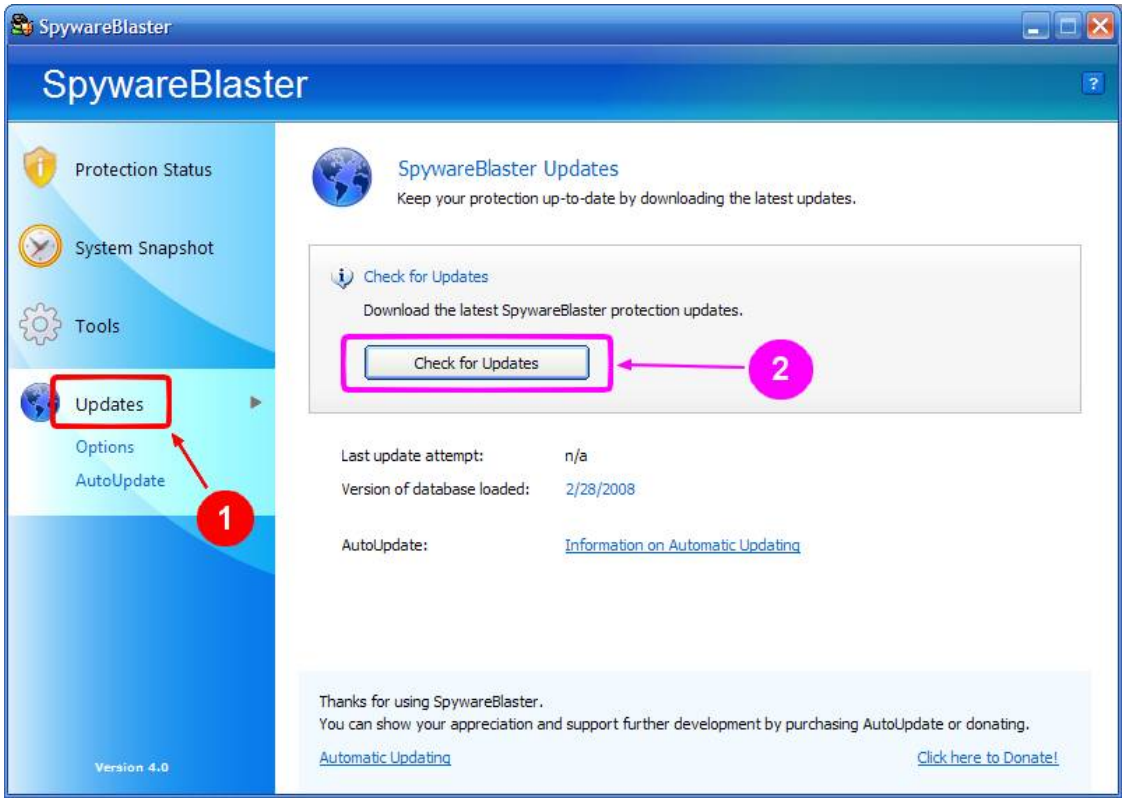


Ensuite, cliquez sur le lien « Enable All Protection » (voir cadre bleu de l'image ci-dessous) :



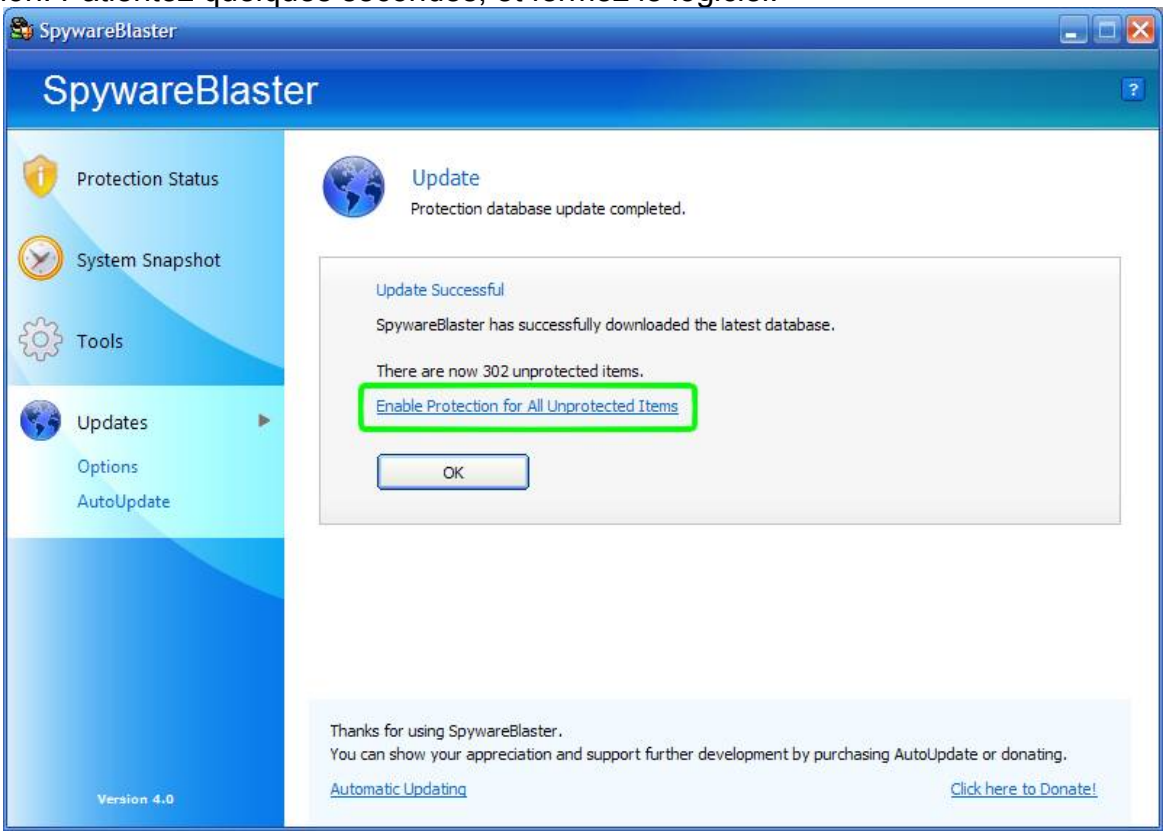
V.2.a.iv) <u>Mise à jour de la protection</u>

Maintenant, vaccinons votre ordinateur des quelques menaces dont SpywareBlaster peut vous prémunir. Commençons par mettre à jour le logiciel. Cliquez sur « Updates » (voir cadre rouge de l'image ci-dessous), puis cliquez sur le bouton « Check for Updates » (voir cadre violet) :



Votre pare-feu va sans doute vous alerter que SpywareBlaster tente d'accéder à Internet, autorisez le définitivement.

Cliquez maintenant sur « Enable Protection for All Unprotected Items » pour activer la protection. Patientez quelques secondes, et fermez le logiciel.

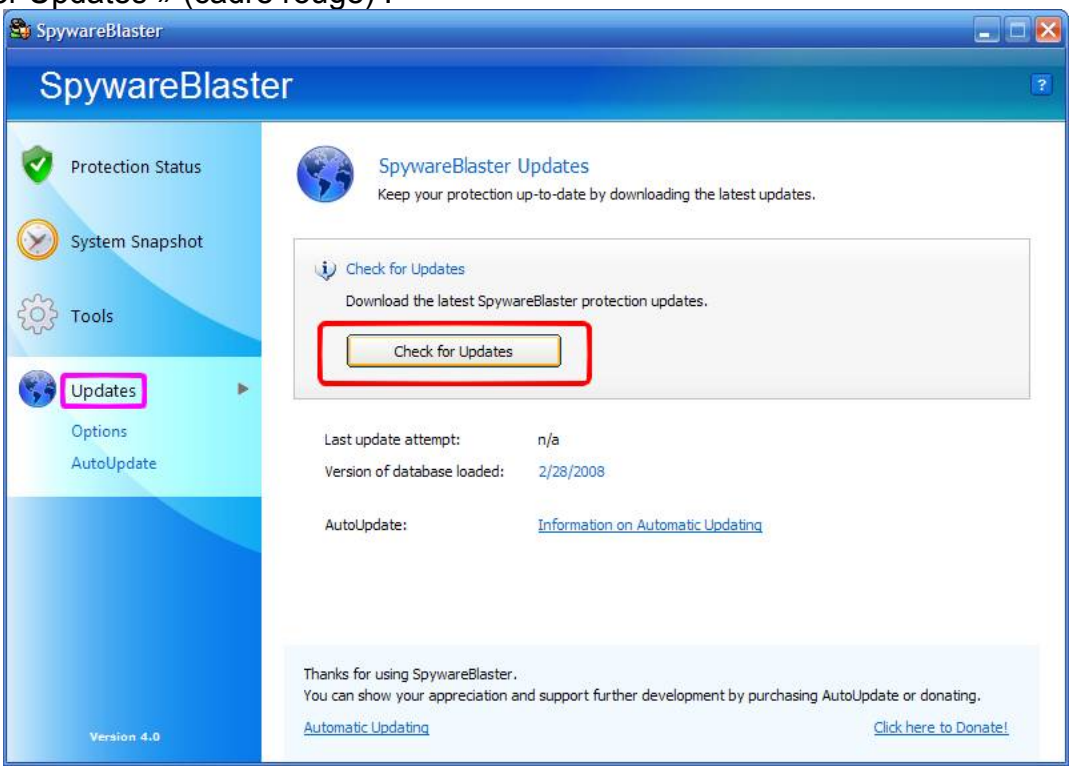


V.2.a.v) *<u>Mise à jour du logiciel</u>*

La procédure de mise à jour du logiciel commence de la même manière que la mise à jour de la protection.

Cliquez sur « Updates » (voir cadre violet de l'image ci-dessous) puis cliquez sur

« Check for Updates » (cadre rouge) :

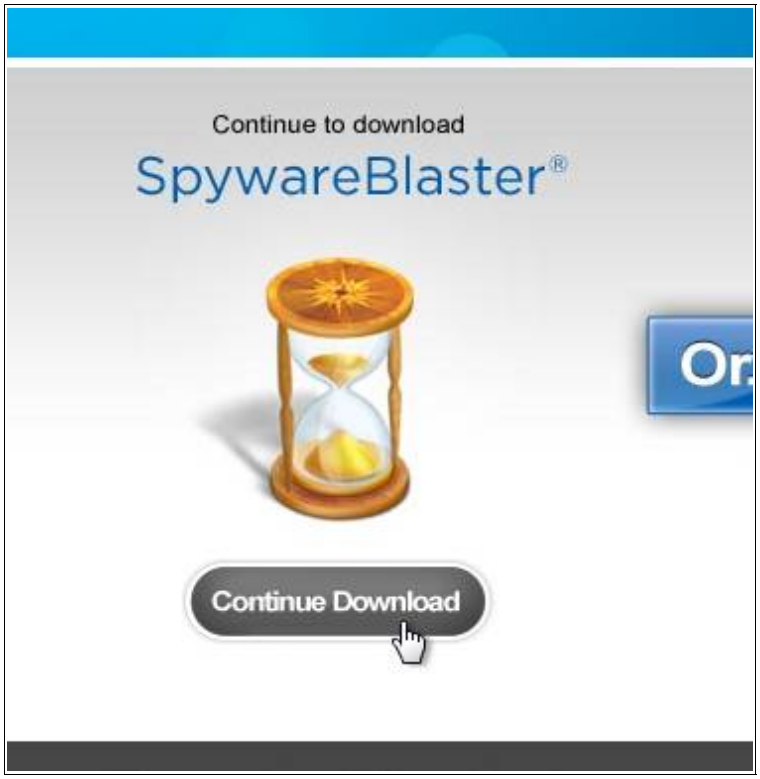


Cliquez sur le bouton « OK » :

Cliquez ensuite sur le lien « http://www.javacoolsoftware.com/sbdownload.html ».

Cliquez ensuite sur le bouton « Download » :

Cliquez ensuite sur « Continue Download » :



Cliquez ensuite sur le troisième lien. La procédure est ensuite la procédure habituelle de téléchargement de votre navigateur.

Téléchargez le fichier, ouvrez le et passez à l'étape Erreur : source de la référence non trouvée.

V.2.b) Malwarebytes' Anti-Malware

Malwarebytes' Anti-Malware (j'écrirais MBAM pour aller plus vite) est un anti-spywares assez récent et très efficace d'après les commentaires qu'on peut lire sur Internet. Nous allons donc l'utiliser.

V.2.b.i) Téléchargement

Utilisez votre moteur de recherche préféré pour trouver le site officiel de Malwarebytes' Anti-Malware. Allez sur la page correspondant à ce résultat :

Ensuite, cliquez sur « Download free version » :

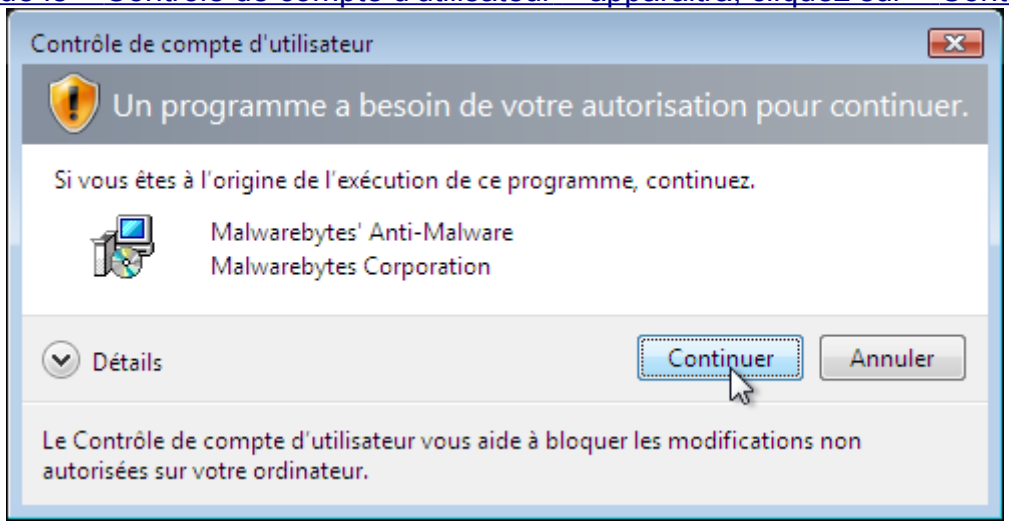
Cliquez ensuite sur « Download now » :

Après cinq secondes d'attente, la procédure habituelle de téléchargement débute.

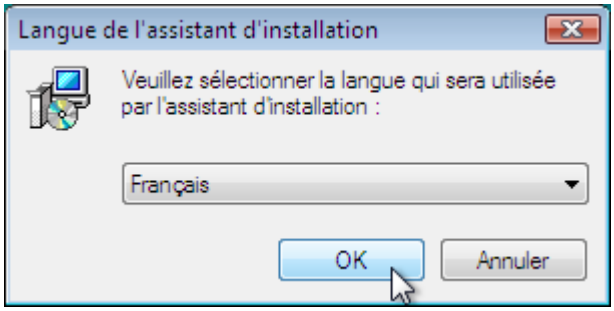
V.2.b.ii) Installation

Ouvrez le fichier précédemment téléchargé.

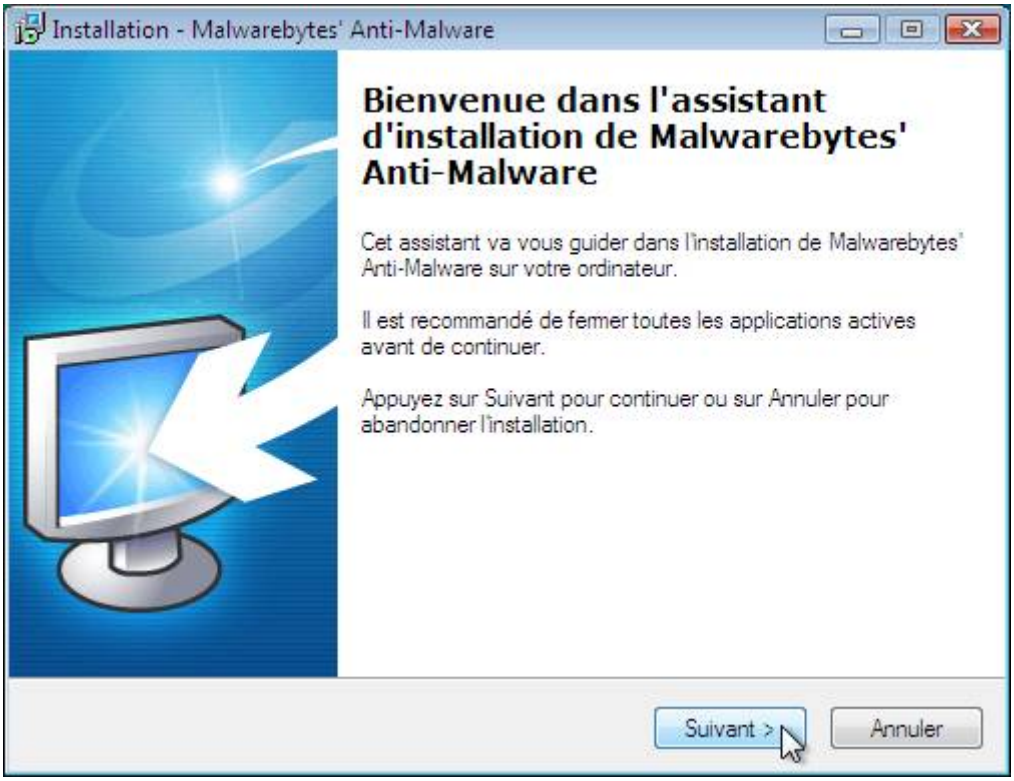
Lorsque le « Contrôle de compte d'utilisateur » apparaitra, cliquez sur « Continuer » :



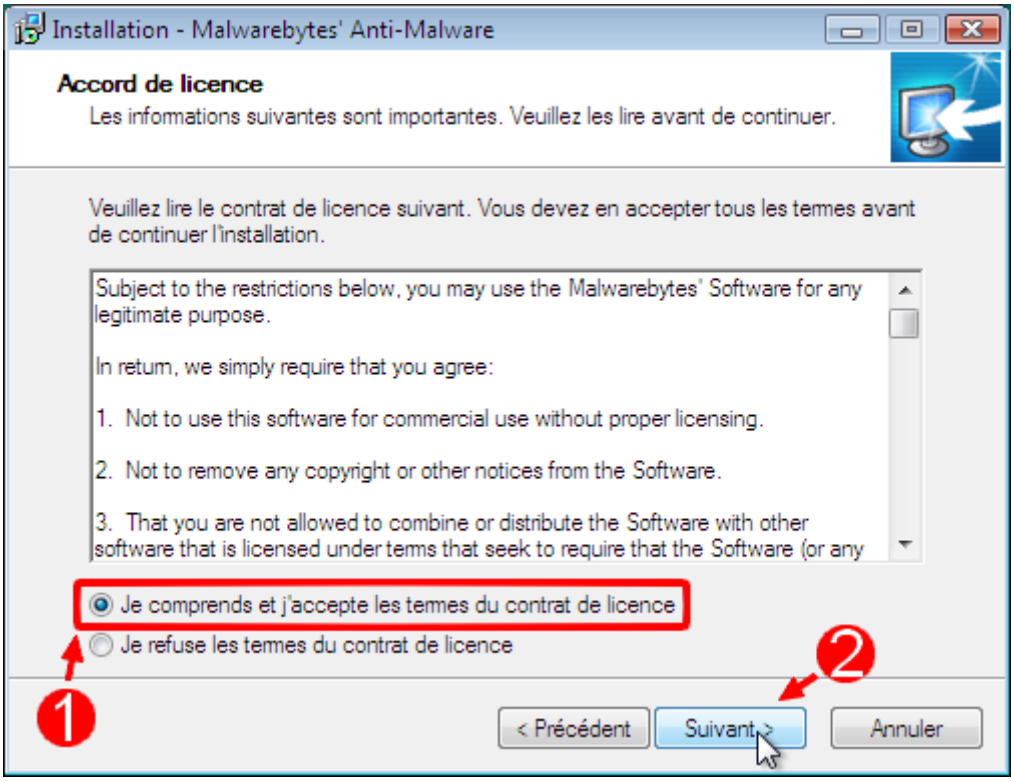
Cliquez sur « OK » :



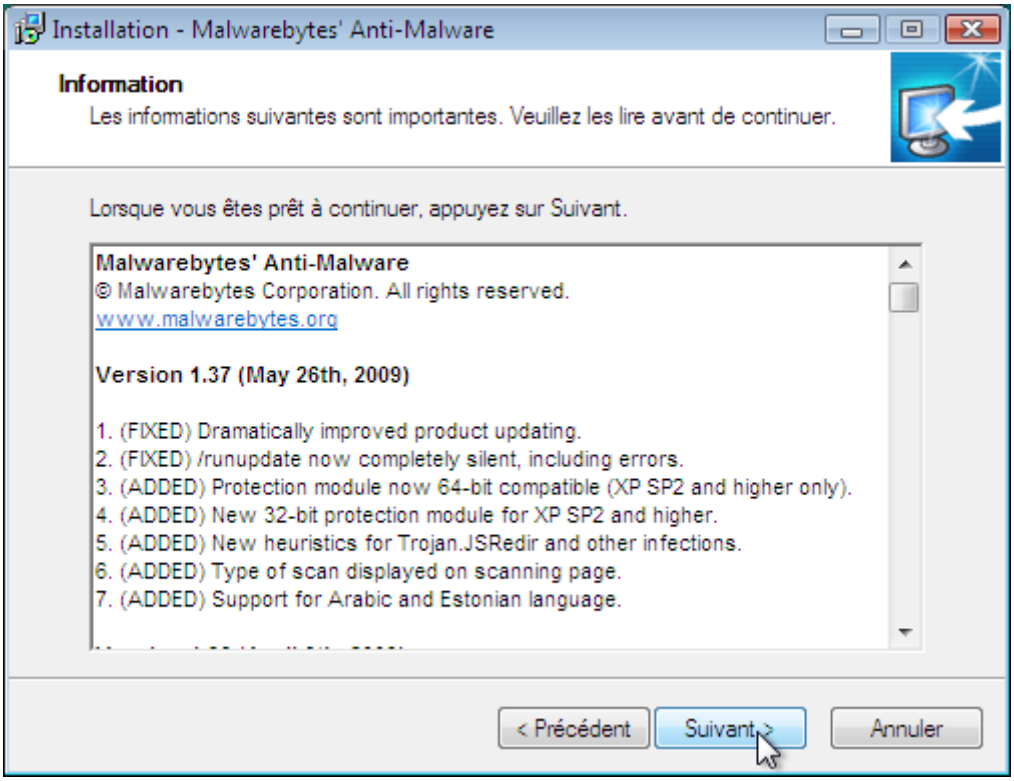
Cliquez sur le bouton « Suivant » :



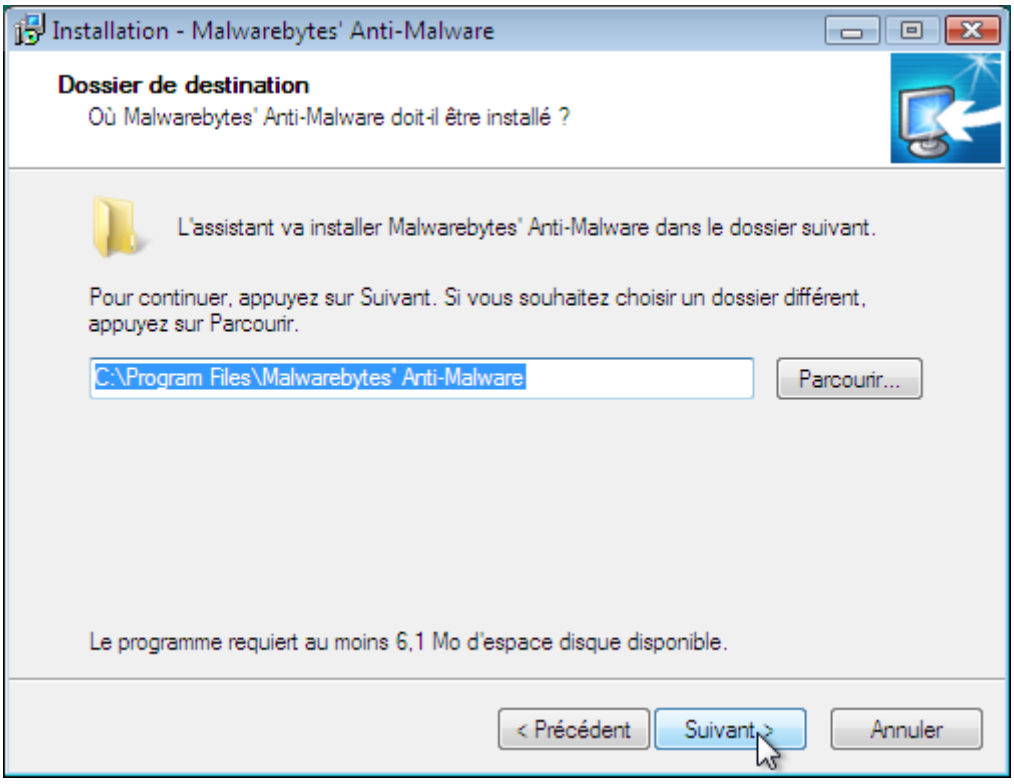
Cochez la case « Je comprends et j'accepte les termes du contrat de licence » et cliquez sur « Suivant » :



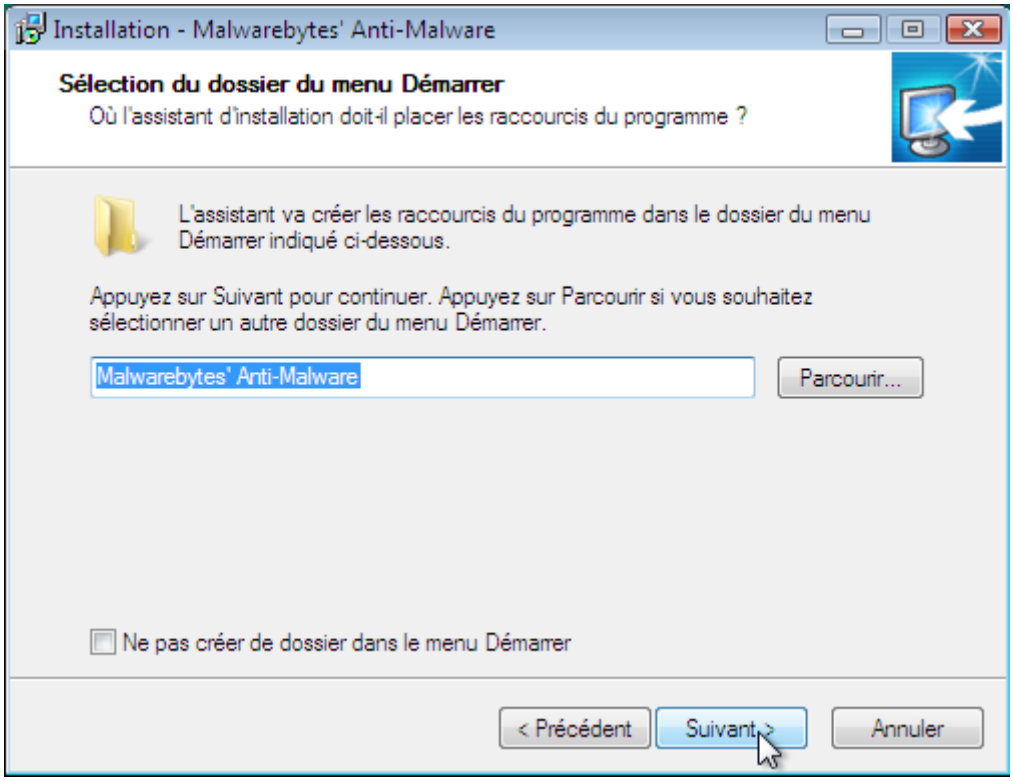
Cliquez sur le bouton « Suivant » :



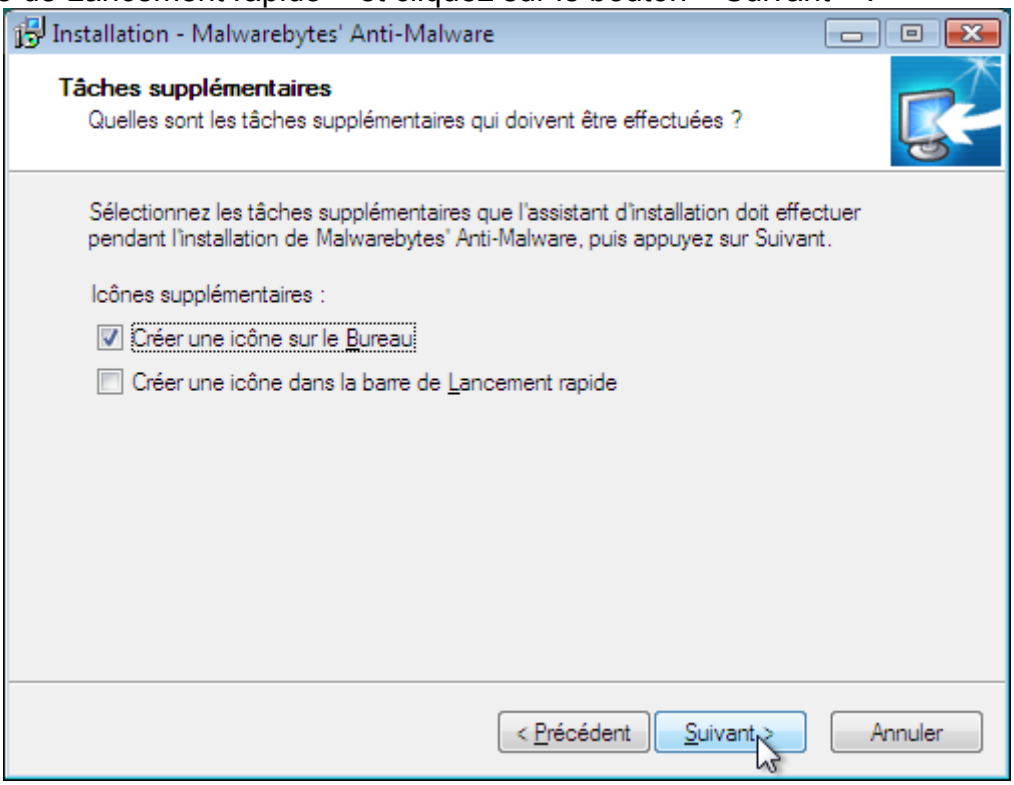
Cliquez encore sur le bouton « Suivant » :



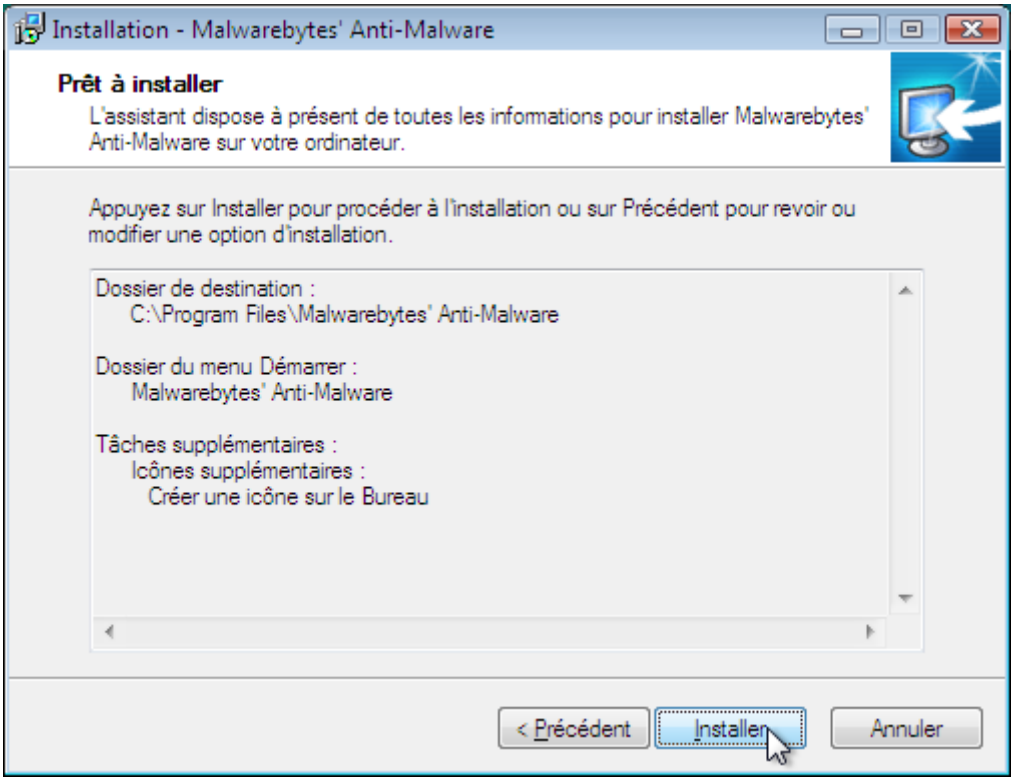
Cliquez sur le bouton « Suivant » :



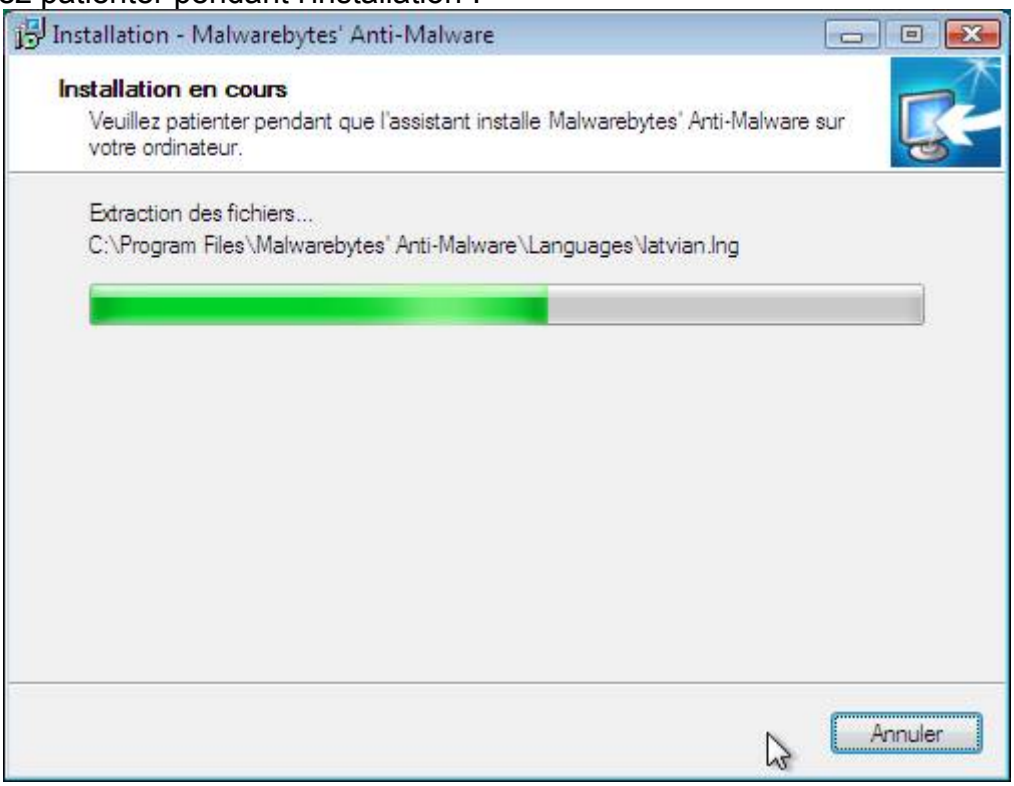
Cochez l'icône « Créer une icône sur le Bureau » et décochez l'icône « Créer une icône dans la barre de Lancement rapide » et cliquez sur le bouton « Suivant » :



Cliquez sur le bouton « Installer » :



Veuillez patienter pendant l'installation :

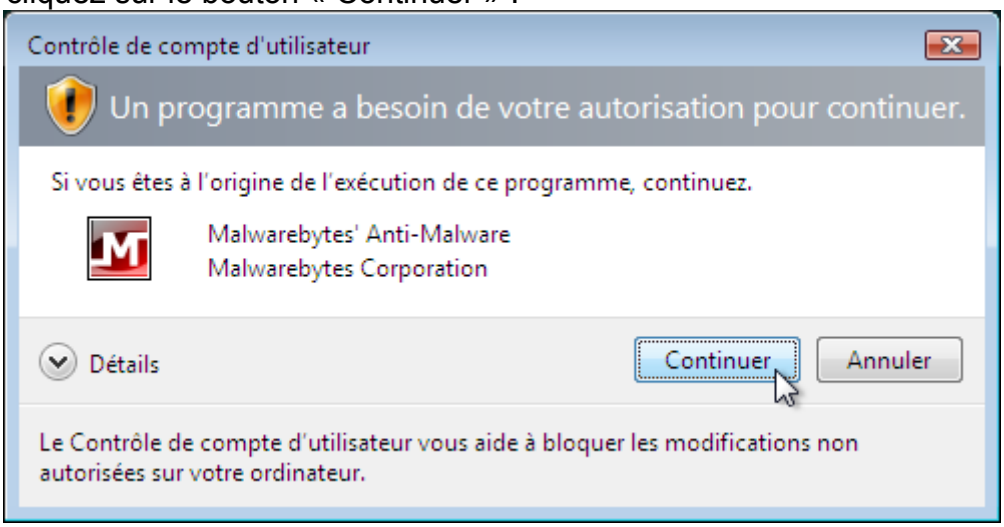


Décochez les deux cases et cliquez sur « Terminer » (on mettra à jour en ouvrant directement MBAM juste après) :

V.2.b.iii) *Mise à jour de la base de signatures*

Pour effectuer une mise à jour de la base de signatures, ouvrez MBAM en double cliquant sur l'icône du bureau :

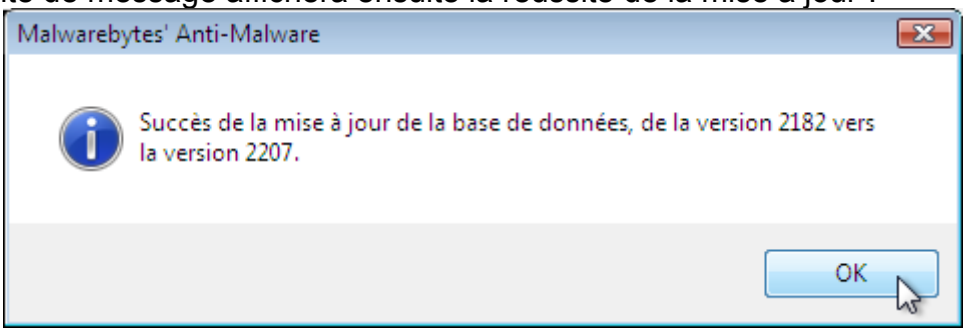
Lorsque le « Contrôle de compte d'utilisateur » apparaitra (sous Windows Vista ou Windows 7), cliquez sur le bouton « Continuer » :



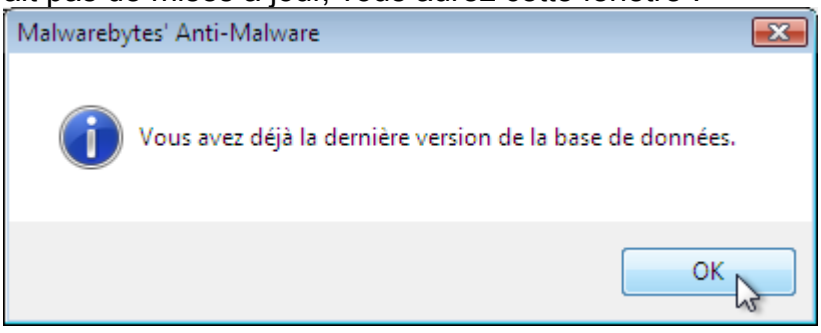
Cliquez ensuite sur l'onglet « Mise à jour » (voir cadre rouge de l'image ci-dessous) et cliquez sur el bouton « Recherche de mise à jour » :

Une petite fenêtre montrera la progression du téléchargement :

Une boite de message affichera ensuite la réussite de la mise à jour :



Ou s'il n'y avait pas de mises à jour, vous aurez cette fenêtre :



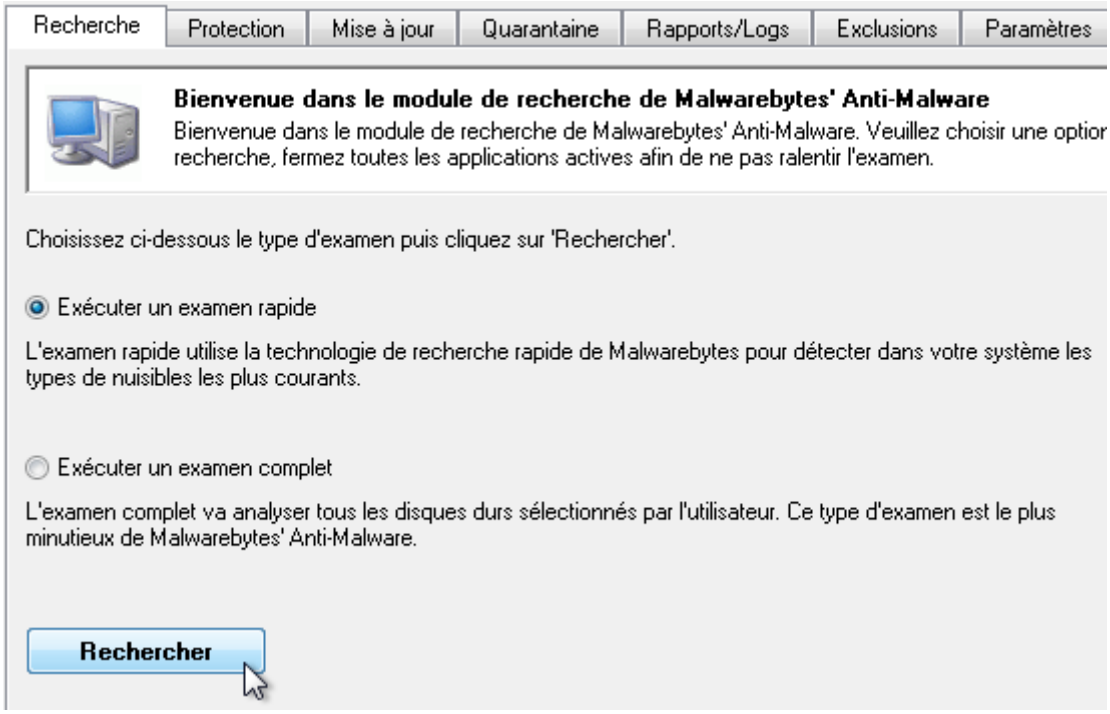
V.2.b.iv) Mise à jour du programme

V.2.b.v) Analyse

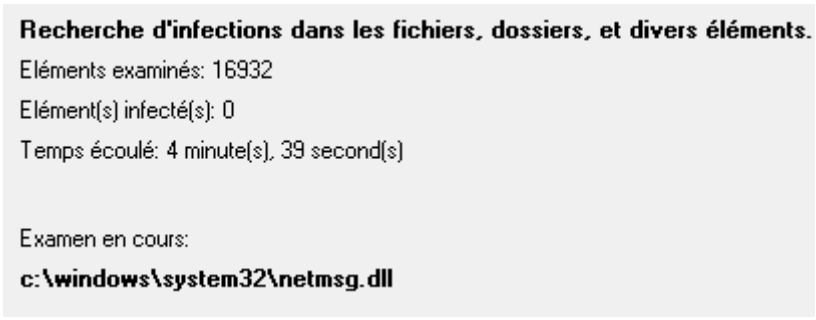
Pour effectuer une analyse de votre ordinateur, ouvrez MBAM en double cliquant sur l'icône du bureau :

Faites la mise à jour de la base de signatures.

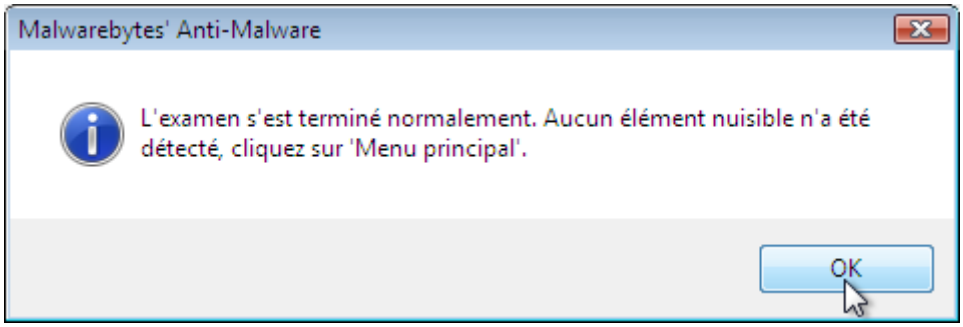
Ensuite, dans l'onglet « Recherche », cochez soit la case « Examen rapide », soit la case « Examen complet » en fonction du type d'examen que vous désirez et cliquez sur le bouton « Rechercher » :



Examen en cours...



Si tout se passe correctement, vous aurez cette fenêtre :



Vous pourrez donc fermer MBAM ainsi que le rapport qui apparaît après.

Dans le cas contraire, …

V.3) Pare-feu

Pour rappel, un pare-feu empêche les pirates qui sont sur Internet d'accéder à votre ordinateur par des portes qui seraient ouvertes dans votre ordinateur. Autant dire qu'il est assez important d'avoir un tel logiciel.

Windows XP en possède un par défaut, tout comme Windows Vista. Cependant, un pare-feu permet aussi de repérer les éventuels programmes de votre ordinateur tentant d'accéder à Internet sans votre autorisation. Il permet donc de détecter si un virus (ou un logiciel espion) qui aurait réussi à s'introduire sur votre ordinateur tente d'accéder à Internet pour appeler tout ses petits copains. Mais mieux que ça, il permet aussi d'empêcher ces virus d'accéder à Internet.

Nous utiliserons Comodo Internet Security comme pare-feu.

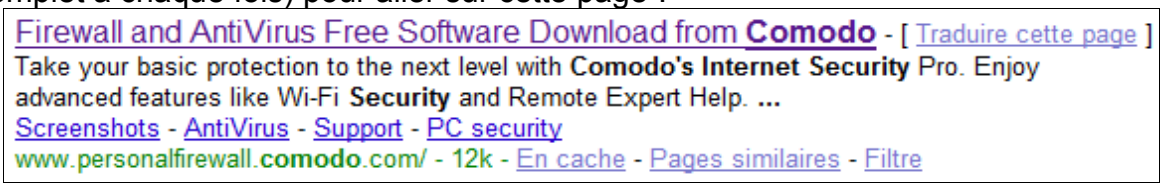
V.3.a) Comodo Internet Security

Il faut déjà savoir une chose : Comodo Internet Security intègre trois types de protection. Il y a le pare-feu, l'antivirus et un module HIPS (un module qui permet de vérifier la légitimité des actions des logiciels).

Nous n'utiliserons pas l'antivirus intégré à Comodo Internet Security, mais nous utiliserons le pare-feu et le module HIPS.

V.3.a.i) Téléchargement

Utilisez votre moteur de recherche préféré pour aller sur le site officiel de Comodo Internet Security (que j'appellerai probablement CIS à plusieurs reprises pour éviter d'écrire le nom complet à chaque fois) pour aller sur cette page :



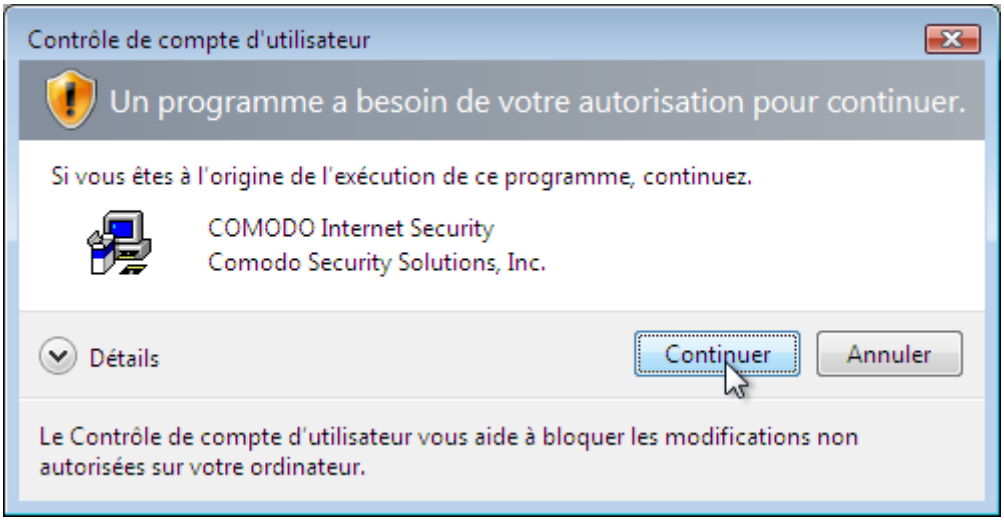
Cliquez ensuite sur le bouton « Free download » :

Cliquez ensuite sur le bouton « Click to download » :

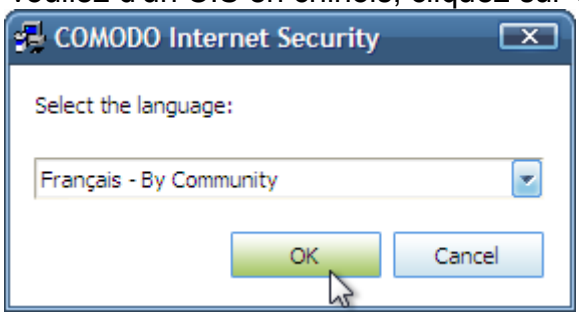
La procédure de téléchargement est ensuite la procédure standard de votre navigateur.

V.3.a.ii) *<u>Installation</u>*

Ouvrez le fichier précédemment téléchargé.
Lorsque le « Contrôle de compte d'utilisateur » apparaitra, cliquez sur « Continuer » :

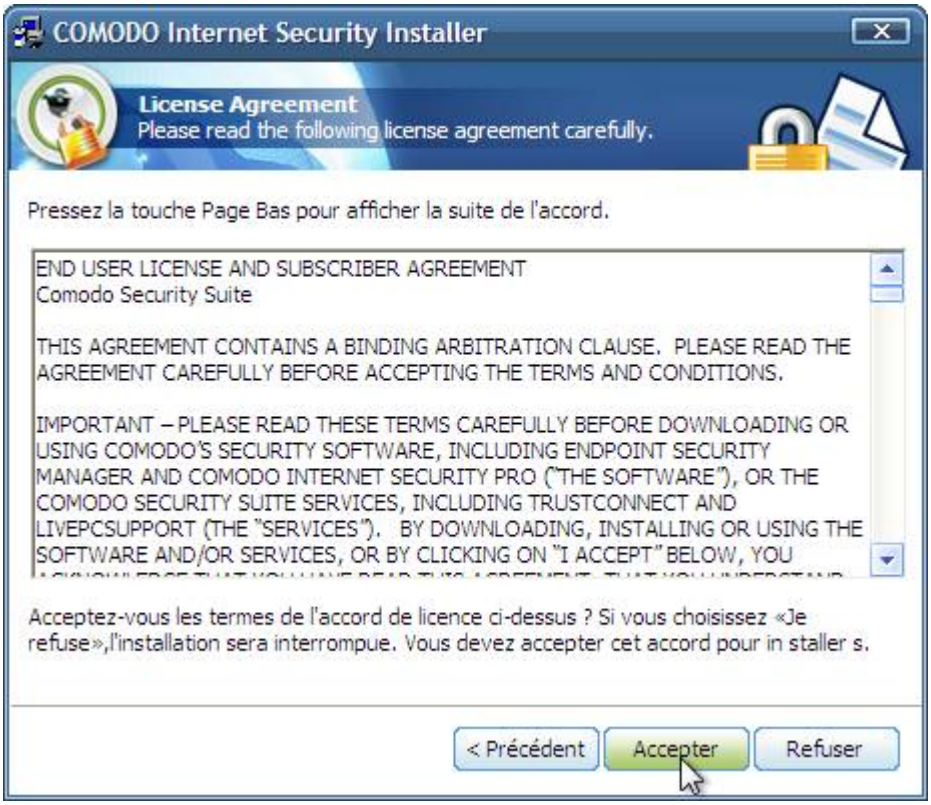


A moins que vous ne vouliez d'un CIS en chinois, cliquez sur « OK » :

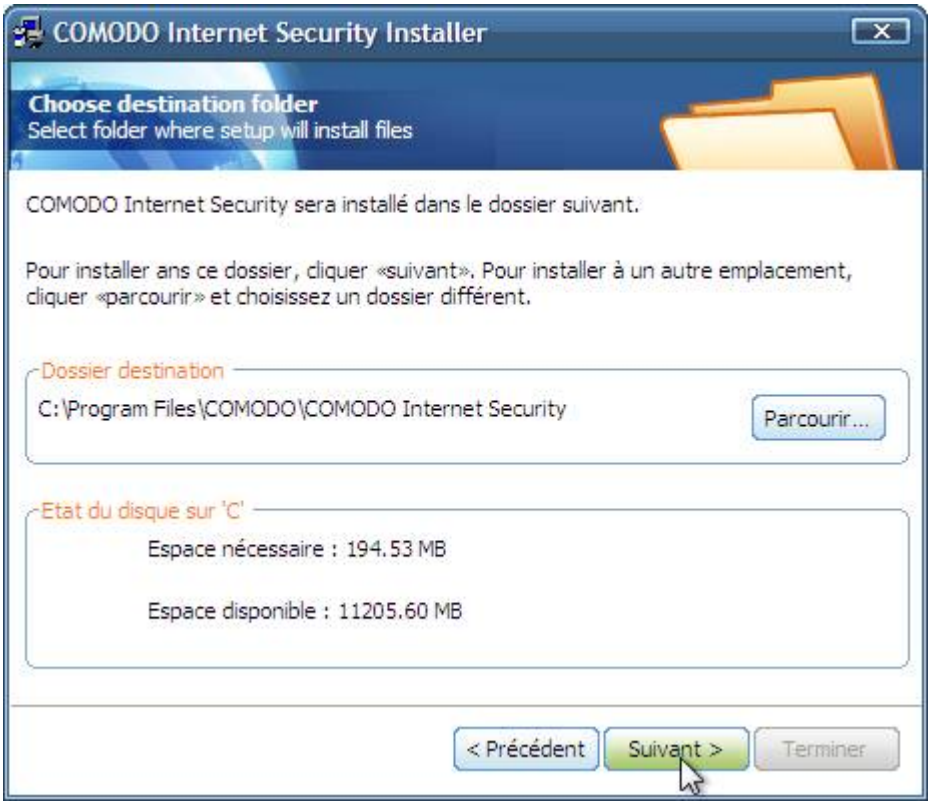


Cliquez sur le bouton « Suivant » :

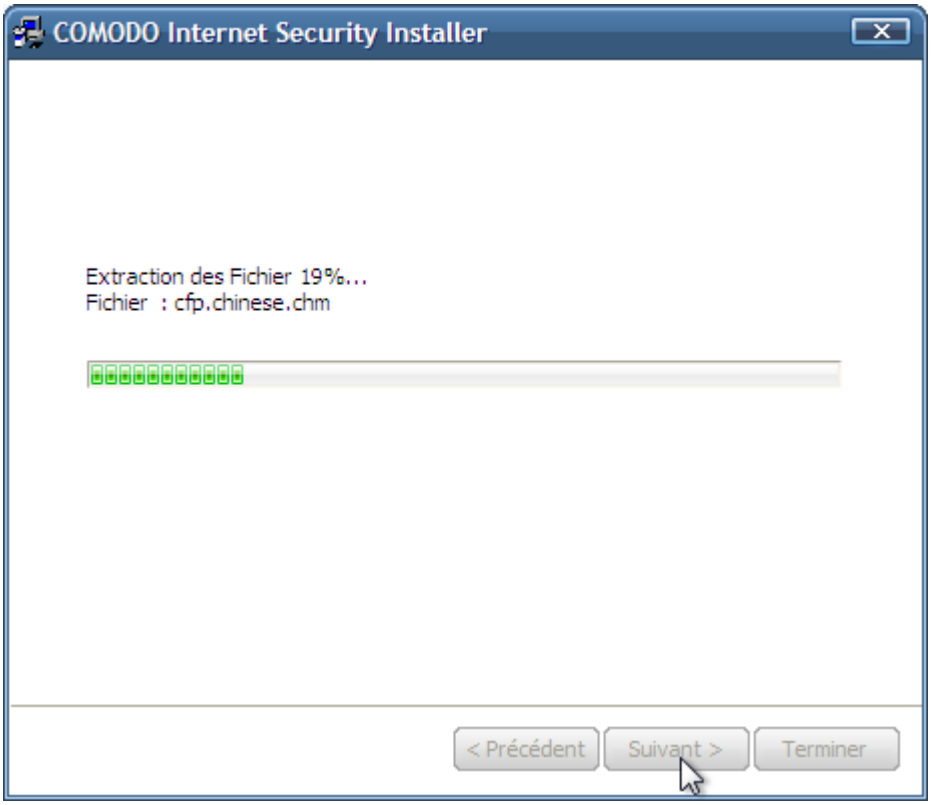
Cliquez ensuite sur « Accepter » :



Cliquez ensuite sur le bouton « Suivant » :



Veuillez patienter pendant l'installation de CIS :



Une fois l'installation terminée, il reste encore quelques réglages à faire. Si vous souhaitez recevoir des informations sur CIS, alors vous pouvez inscrire votre adresse. Dans tous les cas, cliquez sur « Suivant » :

Ensuite, décochez la case « Installer l'antivirus COMODO (recommandé) » cochez la case « Installer le pare-feu COMODO (recommandé) » si elle n'est pas déjà cochée, et cliquez sur « Suivant » :

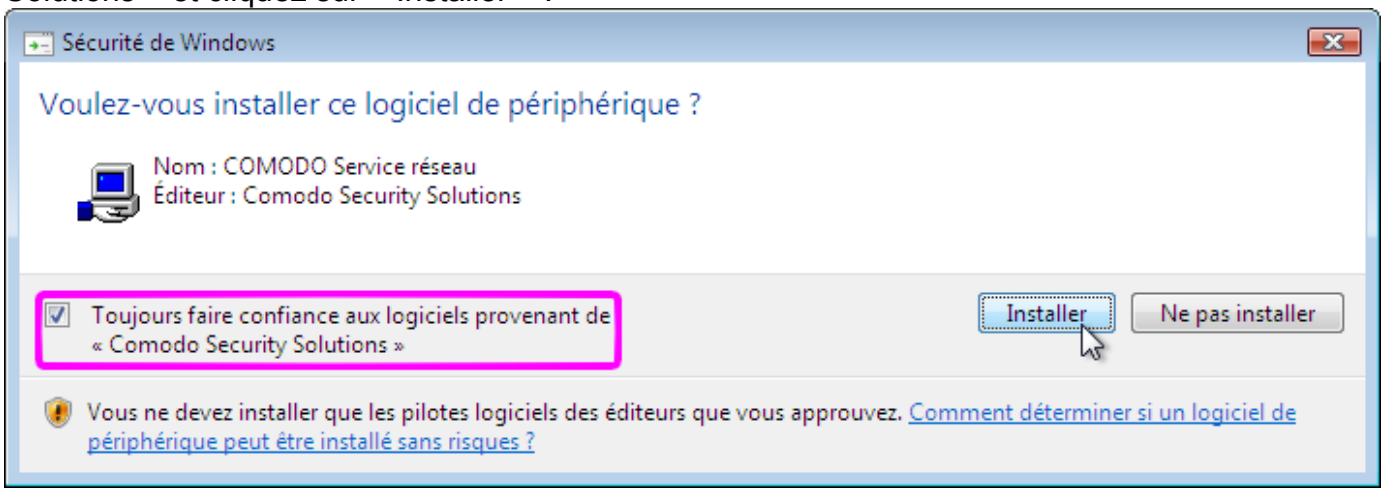
Cliquez ensuite sur « Suivant » :

Si elle n'est pas déjà cochée, cochez la case « Je désire participer à la communauté Threatcast » car cela vous permettra d'avoir des indications sur ce que vous devriez faire lorsque vous aurez une alerte. Cliquez ensuite sur le bouton « Suivant » :

Décochez les trois cases et cliquez sur « Suivant » :

Veuillez patienter pendant la suite de l'installation de CIS :

Cochez la case « Toujours faire confiance aux logiciels provenant de « Comodo Security Solutions » et cliquez sur « Installer » :

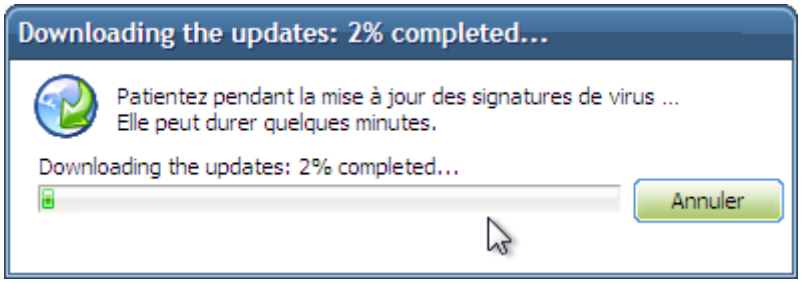


Encore quelques réglages et c'est bientôt terminé. Cliquez sur « Suivant » :

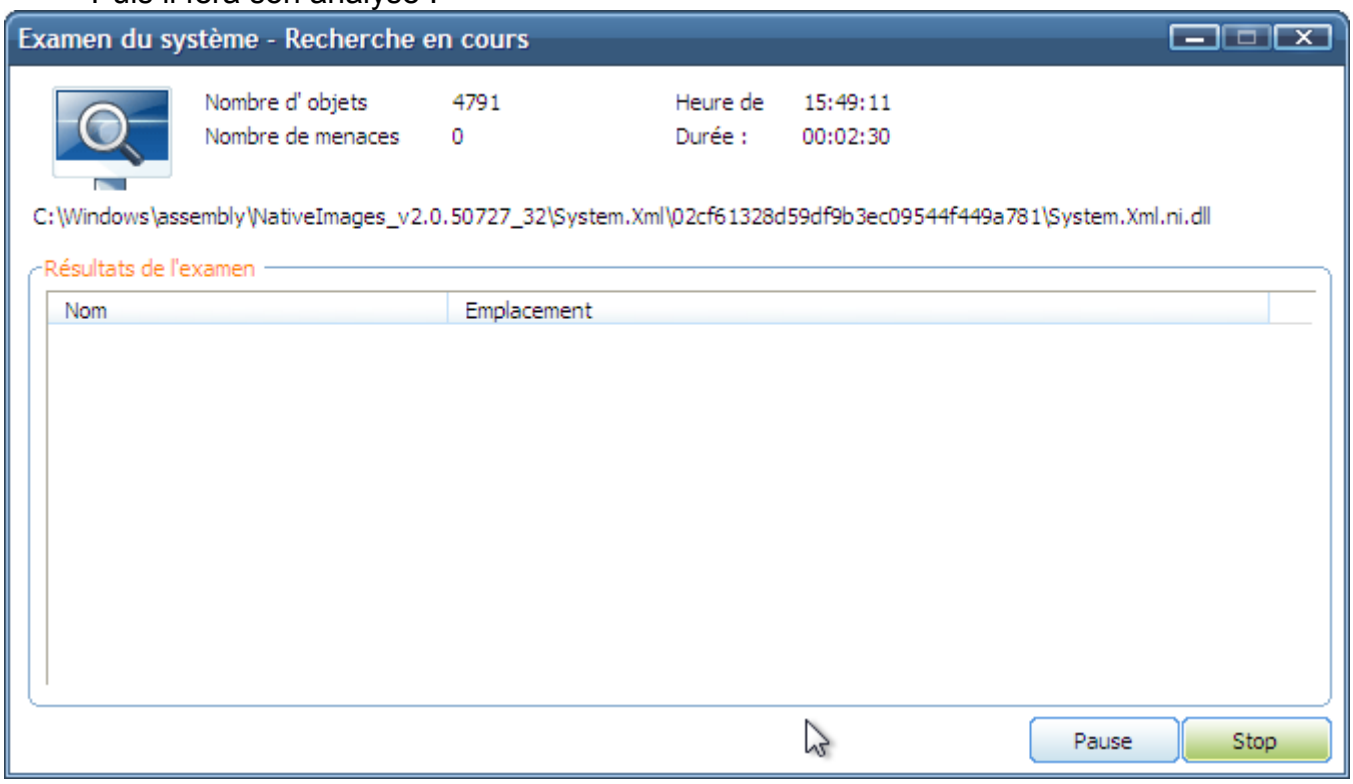
CIS veut rechercher s'il y a des virus dans l'ordinateur.

Bref, si vous venez juste de faire une analyse avec AntiVir, décochez la case. Dans le cas contraire, laissez la case cochée. Dans tous les cas cliquez sur « Terminer ».

Si vous avez demandé l'analyse, CIS téléchargera d'abord les mises à jour de son antivirus (vous avez largement le temps de prendre un café ou de faire tout ce que vous voulez car ça prend en effet plusieurs minutes) :



Puis il fera son analyse :

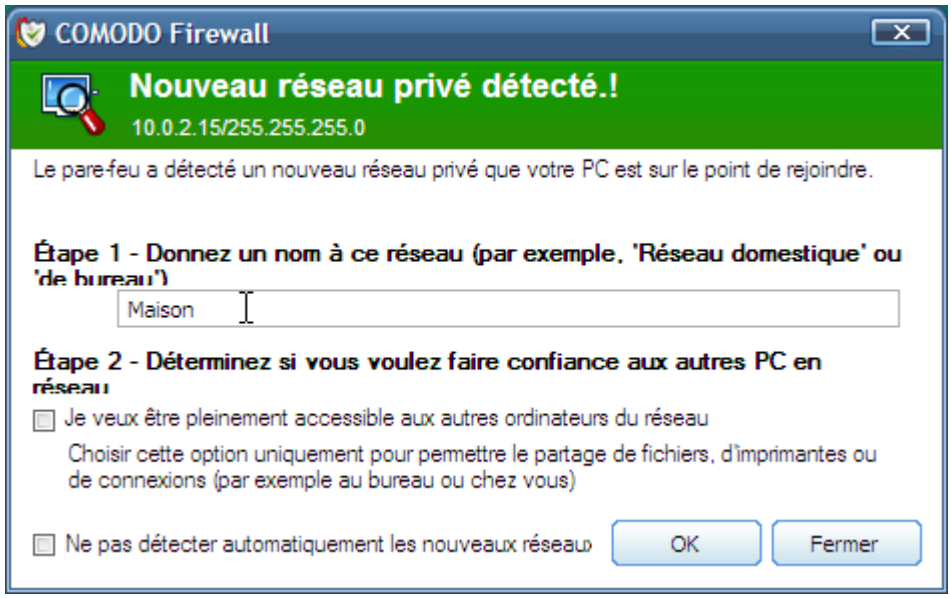


Une fois l'analyse terminée, la fenêtre disparaît s'il n'y a aucune menace détectée.

Vous serez invité à redémarrer votre ordinateur. Sauvegardez le travail en cours et cliquez sur « Terminer » :

V.3.a.iii) <u>Nouveau réseau</u>

A chaque fois que vous vous connecterez pour la première fois sur un nouveau réseau, CIS vous demandera ceci :



CIS veut que vous donniez un nom à ce réseau et vous demande si vous voulez que votre ordinateur soit visible aux autres ordinateurs du réseau. Si vous avez plusieurs ordinateurs chez vous, cochez la case « Je veux être pleinement accessible aux autres ordinateurs du réseau ». Dans tous les cas, donnez un nom à ce réseau (ici « Maison »). Ensuite, cliquez sur le bouton « OK ».

V.3.a.iv) <u>Étude d'une alerte</u>

V.3.a.v) <u>Répondre en fonction du logiciel</u>

Votre ordinateur est rempli de logiciels (sinon, vous ne ferez pas grand chose avec votre ordinateur). Certains n'ont pas du tout besoin d'Internet, d'autres de temps en temps, et d'autres

en permanence.

• Les logiciels de protection :

Les logiciels de protection, tels votre antivirus, vos logiciels antispywares ou votre pare-feu ont toujours besoin d'accès à Internet. Ne serais-ce que pour les mises à jours.

Dans ce cas, cochez la case « Conserver ce paramètre » et cliquez sur Autoriser.

Avast avec CIS vous paraitra certainement très casse pieds. Ceci s'explique par le fait qu'Avast est décomposé en plusieurs modules qui agissent alternativement. Antivir avec CIS pose moins de questions.

• Les logiciels d'utilisation d'Internet

De nombreux logiciels nécessitent un accès permanent à Internet. Il faudra donc cocher la case « Conserver ce paramètre » et cliquer sur Autoriser. Par exemple, votre navigateur Internet (Firefox, Internet Explorer, ...), votre logiciel de messagerie (Thunderbird, Outlook Express, ...), votre logiciel de messagerie instantanée (Windows Live Messenger, Yahoo Messenger, ...), votre logiciel de photos satellites (Google Earth, Nasa World Wind, ...), ...

Tout ces logiciels et d'autres que je n'ai pas cité nécessitent un accès permanent à Internet, sinon, ils ne fonctionneront tout simplement pas.

• Logiciels a utilisation temporaire

Il existe un certain nombre de logiciels n'ayant pas besoin d'un accès permanent à Internet. Les traitements de textes (OpenOffice, Word, ...) et autres logiciels de suites bureautiques ont par exemple besoin d'un accès lors d'un copier coller. Les logiciels de vision de vidéo ou pour écouter sa musique ont parfois besoin d'Internet lorsque le fichier à écouter/voir se situe sur Internet, ...

Ces logiciels ont besoin d'un accès temporaire à Internet. Cliquez uniquement sur Autoriser.

• Programmes d'installation

Les programmes d'installation n'ont pas besoin de base d'un accès à Internet. Certains en ont besoin pour télécharger des mises à jours, d'autres pour télécharger les fichiers à installer, mais c'est assez rare.

Vous pouvez les autoriser temporairement (sauf si vous avez un doute, certains programmes n'étant pas liés à Internet ont leur programme d'installation demandant l'accès à Internet), mais ne conservez pas l'autorisation. Car on pourrait imaginer un virus infectant un programme d'installation, et si vous autorisez l'accès, je vous laisse imaginer le cirque.

• Les programmes liés à votre système d'exploitation

Là, la réponse à fournir dépend beaucoup. Certains comme le Generic Host Process demandent régulièrement un accès. La réponse n'étant pas triviale, j'essaierai de faire une liste exhaustive des programmes à conserver l'autorisation.

• Les liens dans les programmes :

Certains programmes comportent parfois des liens vers des sites Internet. Du coup, quand vous cliquerez sur le lien, vous aurez une alerte de Comodo disant que le programme tente d'accéder à Internet. Dans ces cas là, il vaut mieux ne faire qu'autoriser, sans conserver le paramètre.

Bref, il faut réfléchir en fonction du programme demandant l'accès, du besoin que ce programme pourrait avoir d'accéder à Internet, et s'il faut répondre en autorisant ou en refusant.

Il faut donc se poser les questions suivantes à peu près dans le même ordre lorsqu'une alerte de Comodo apparaît :

• Pourquoi il me demande ça ?

• Quel est le programme qui fait la demande d'accès ?

• A-t-il raison de me demander ça ?
• Que dois-je répondre ?

Il est le plus souvent facile de répondre à ces questions (à condition de bien connaître les logiciels installés sur son propre ordinateur), mais ce n'est pas toujours le cas, c'est pourquoi la section suivante contient une liste de certains programmes et des réponses à fournir.

V.3.a.vi) Résoudre une erreur de réponse avec Comodo Internet Security

VI) Si tout ceci échouait

Les logiciels de protection ne sont pas fiables à 100%. Et la faille de sécurité principale de l'ordinateur est souvent ce qui se trouve entre la chaise et le clavier. Même avec les différentes choses expliquées précédemment, personne n'est à l'abri d'une erreur et il se peut qu'un jour votre ordinateur attrape un logiciel espion qui se met à afficher de la pub sur votre écran.

Les logiciels de protection sont plus efficaces à titre préventif que curatif : il existe déjà des millions de virus et cochonneries sur Internet pouvant infecter votre ordinateur, et il existe presque autant de moyens d'infection différents (quels fichiers corrompre, à quel endroit se placer pour télécharger les morceaux de virus qui auraient été enlevés, ...).

Dans cette section, nous allons voir deux ou trois trucs qui vous permettront de vous faire aider par un expert si jamais vous demandez par exemple de l'aide par Internet, ou encore par téléphone à un ami que vous connaissez.

Nous verrons d'abord comment redémarrer son ordinateur en mode sans échec (de deux façons différentes) puis nous parlerons d'un ou plusieurs logiciels souvent utilisés pour désinfecter les ordinateurs. La façon de désinfecter ne sera pas entièrement traitée car elle implique de très bien connaître son ordinateur et les différents logiciels qu'on trouve dans le monde. Ces logiciels de désinfection montrent en fait une certaine quantité de points sensibles de l'ordinateur dans lesquels se trouvent des traces de certains logiciels. Ces traces peuvent être légitimes ou non, et ces logiciels ne font pas la distinction. C'est à l'utilisateur de savoir quelles sont les traces légitimes ou non.

Nous verrons donc comment utiliser ces logiciels, mais nous n'aborderons pas l'analyse des rapports (sinon, il faudrait de nombreuses pages de plus).

VI.1) Redémarrer son ordinateur en mode sans échecs

Tout d'abord, il faut savoir que le mode sans échecs est un mode qui permet à l'ordinateur de démarrer le moins de choses possibles (et donc de peut-être ne pas démarrer le ou les virus / logiciels espions qui seraient présents dans votre ordinateur) afin de dépanner un ordinateur.

Ce mode de fonctionnement vous sera peut-être demandé par un expert afin d'éradiquer un logiciel espion avec les logiciels que nous verront dans cette section.

VI.1.a) 1ère méthode

VI.1.a.i) Sous Windows XP et 2000 et 2003

Cette méthode consiste en fait à appuyer sur la touche F8 juste avant l'apparition du logo de Windows au démarrage de votre ordinateur. Le problème, c'est que ce logo apparaît très vite.

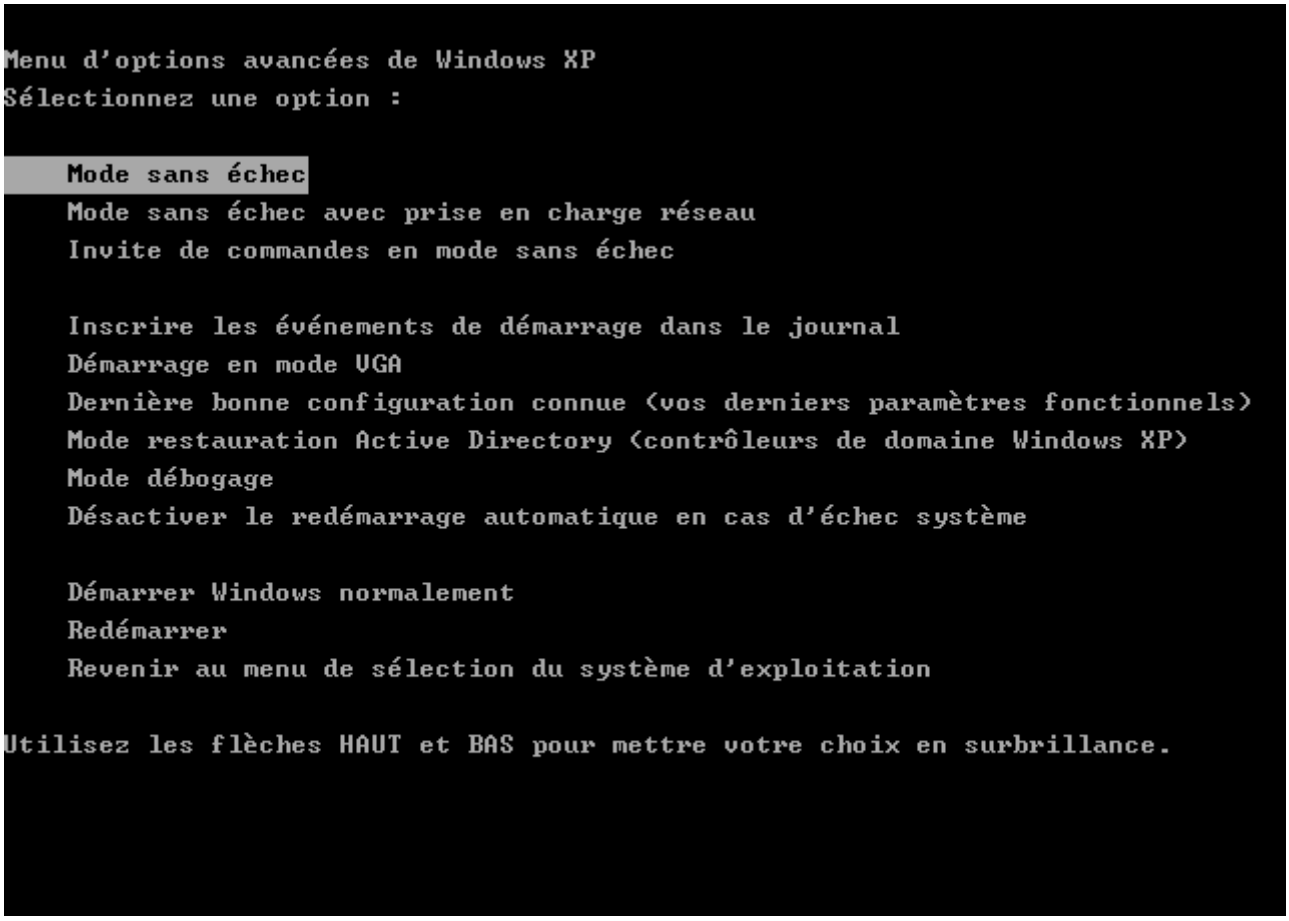
Commencez donc par redémarrer votre ordinateur.

Il faudra appuyer sur F8 juste avant l'apparition du logo Windows :

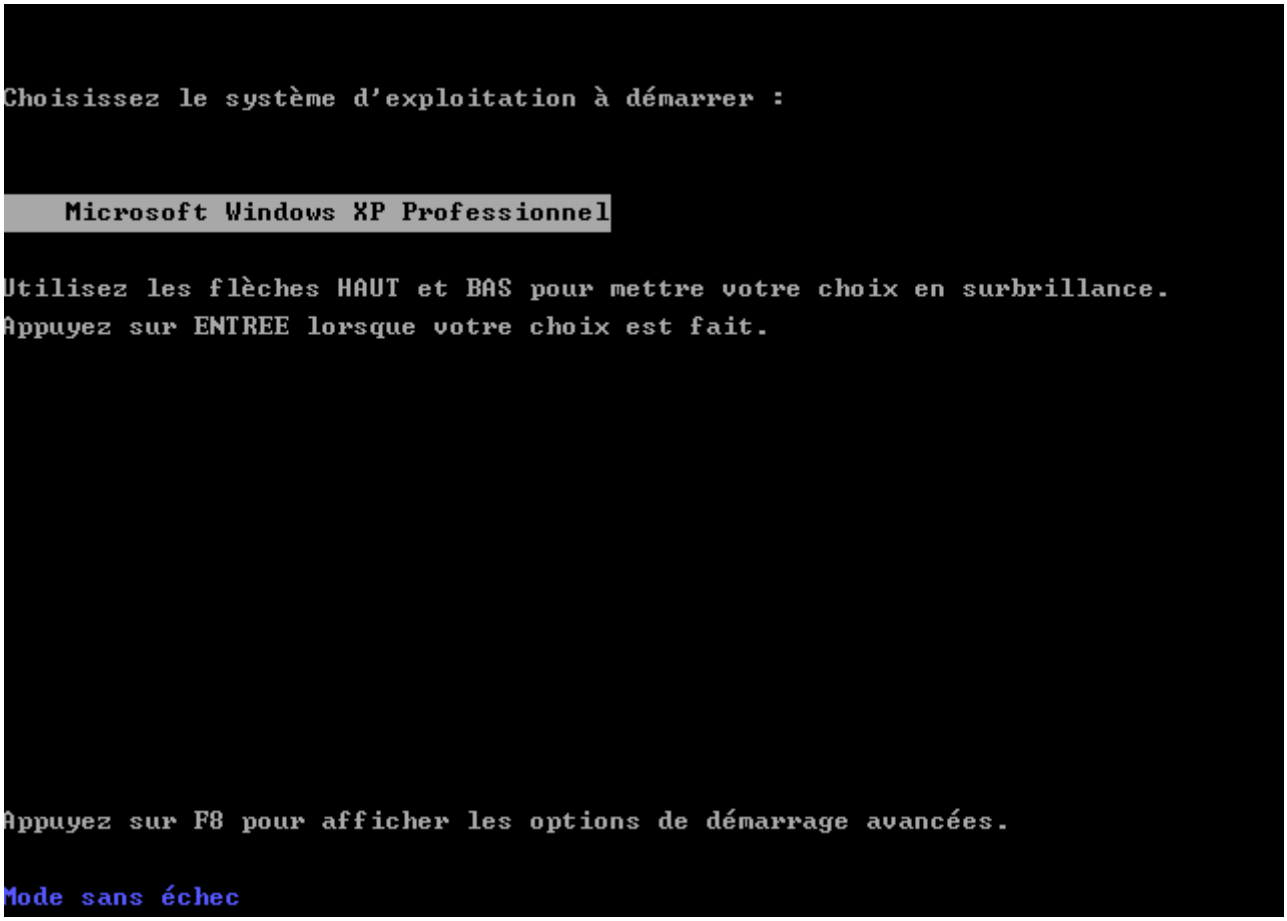
Pour Windows XP

Pour Windows 2000

Utilisez les flèches de votre clavier afin que « Mode sans échec » (ou « Mode sans échec avec prise en charge réseau » en fonction de ce qui vous sera demandé de faire) soit mit en surbrillance :



Appuyez ensuite sur la touche « Entrée » de votre clavier deux fois ce suite pour valider l'écran ci-dessus et celui ci-dessous.



VI.1.a.ii) Sous Windows Vista et 2008

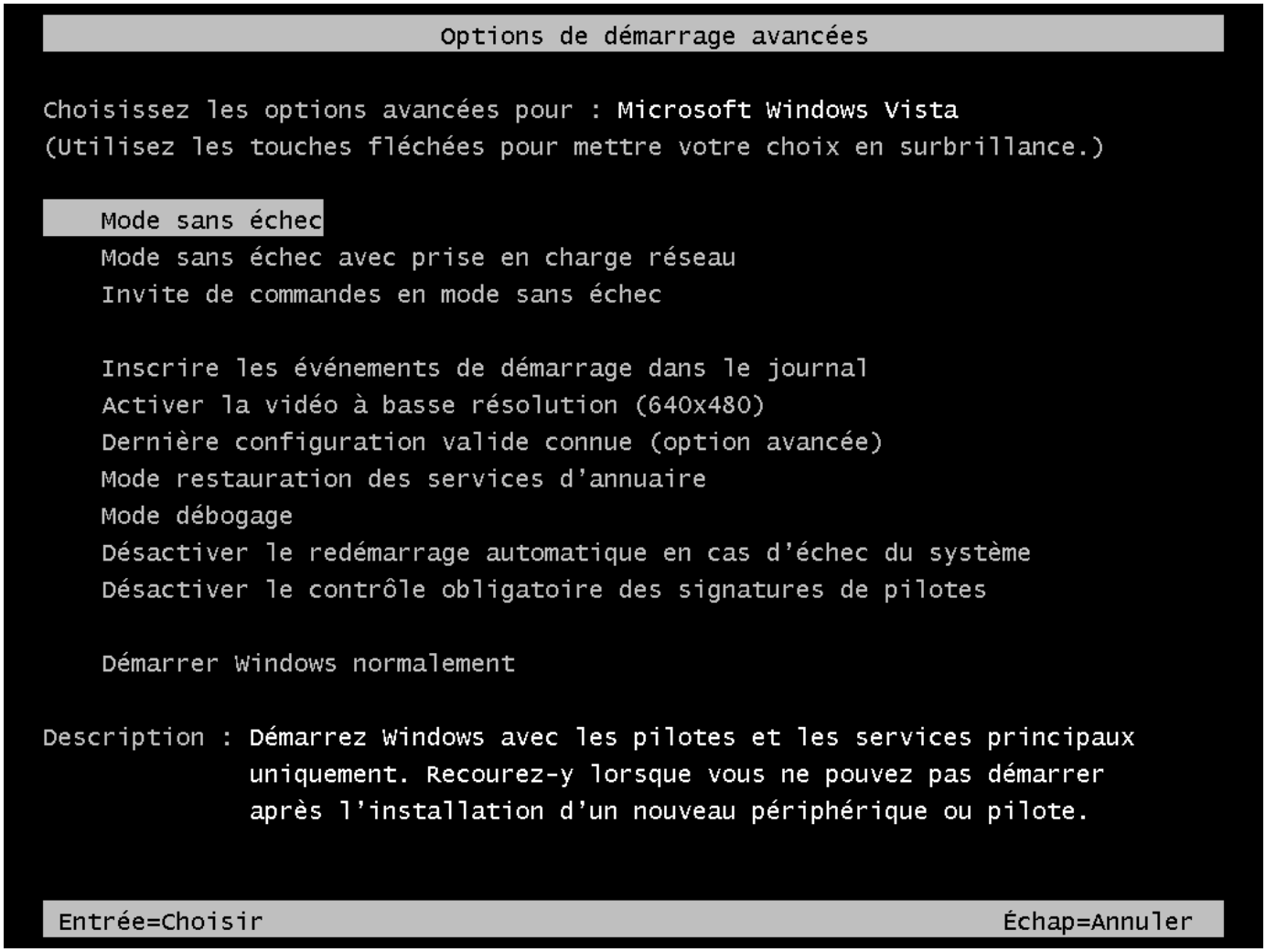
Cette méthode consiste en fait à appuyer sur la touche F8 juste avant l'apparition du logo de Windows au démarrage de votre ordinateur. Le problème, c'est que ce logo apparaît très vite.

Commencez donc par redémarrer votre ordinateur.

Il faudra appuyer sur F8 juste avant l'apparition de cet écran :

Si l'écran si dessus apparaît, c'est trop tard, vous n'arriverez pas au mode sans échec.

Si par contre, vous avez l'écran ci-dessous, utilisez les flèches de votre clavier afin que « Mode sans échec » (ou « Mode sans échec avec prise en charge réseau » selon ce qui vous sera demandé de faire) soit mit en surbrillance :



Ensuite, appuyez sur la touche « Entrée » de votre clavier. Windows se lancera ainsi en mode sans échec.

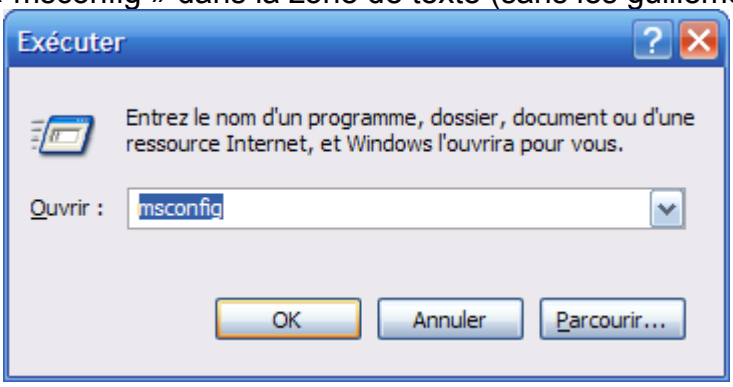
VI.1.b) 2ème méthode

VI.1.b.i) Sous Windows XP, 2000 et 2003

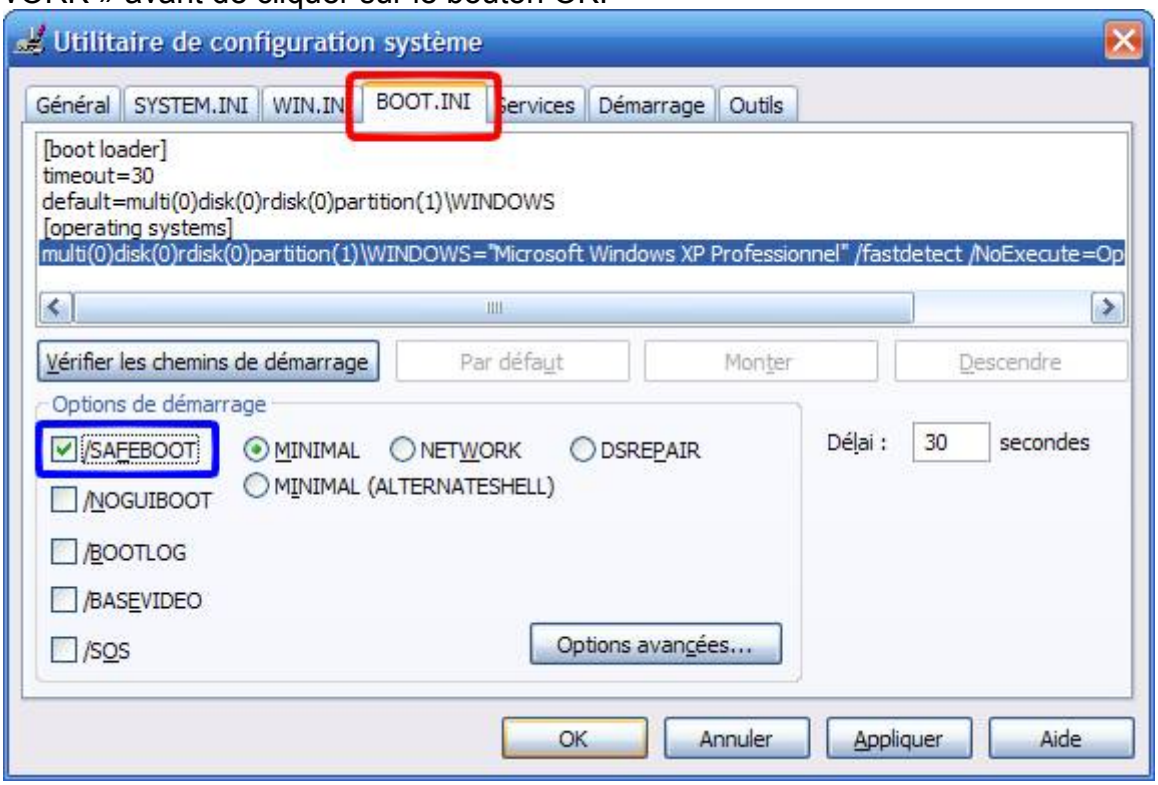
Il va falloir ouvrir l'« Utilitaire de configuration système ».

Pour ceci, sous Windows XP, cliquez sur votre bouton « démarrer », puis cliquez sur « Exécuter » :

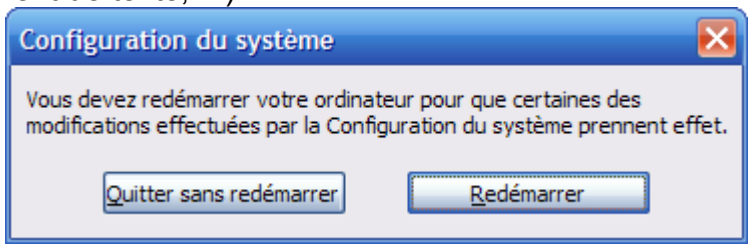
Tapez ensuite « msconfig » dans la zone de texte (sans les guillemets) :



Ensuite, allez dans l'onglet « BOOT.INI » cochez la case « /SAFEBOOT » et cliquez sur le bouton OK. Si on vous demande un démarrage en mode sans échec, cochez la case « NETWORK » avant de cliquer sur le bouton OK.



Une petite fenêtre vous proposera de redémarrer. Si vous êtes en train de lire ces quelques lignes dans le but de redémarrer en mode sans échec, vous pourrez cliquer sur le bouton « Redémarrer », mais pensez quand même à sauvegarder votre travail en cours (documents de traitement de texte, ...).



Cette procédure fait qu'à chaque fois que vous démarrerez votre ordinateur, ça se fera en mode sans échec. Pour pouvoir de nouveau démarrer en mode normal, il faut faire l'opération inverse (donc décocher la case « /SAFEBOOT »).

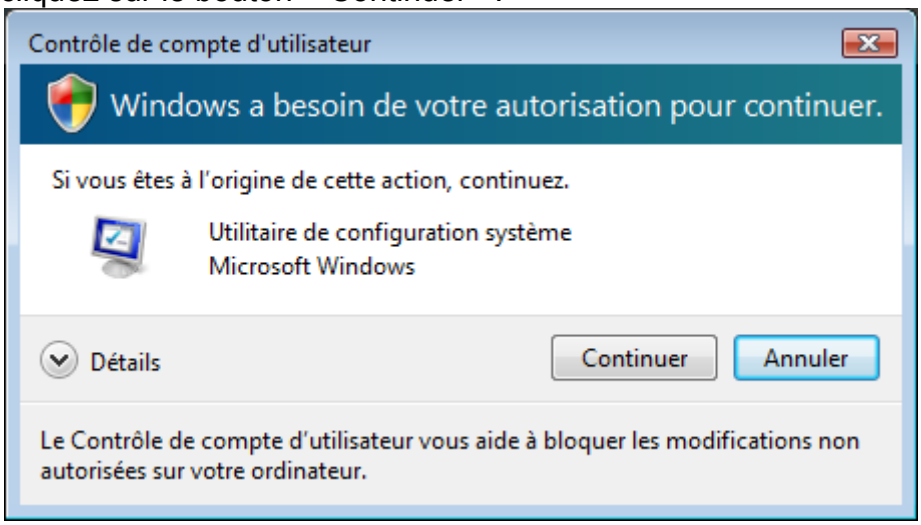
VI.1.b.ii) Sous Windows Vista et probablement Windows Server 2008

Je n'ai pas personnellement testé Windows Server 2008 mais il y a de grandes chances

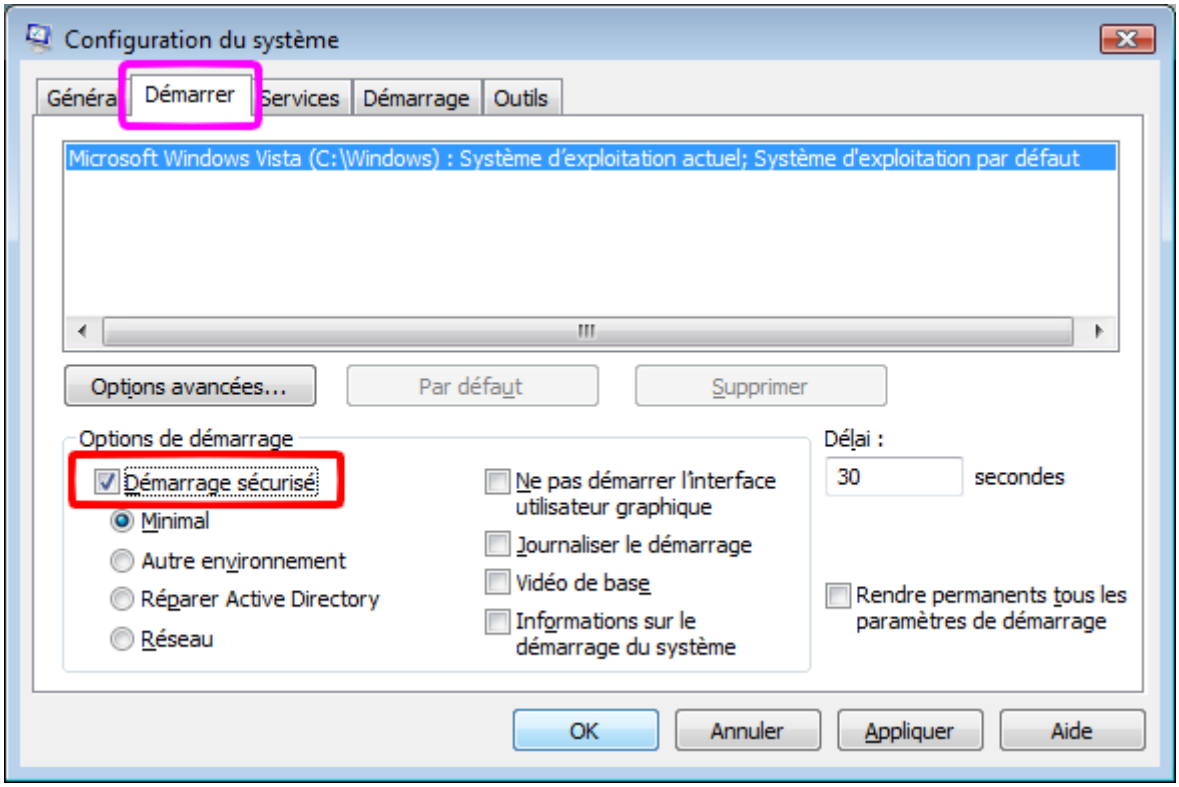
que la procédure soit la même que pour Windows Vista.

Sous Windows Vista, ouvrez votre menu de démarrage et tapez « msconfig » dans le champ de recherche. Appuyez directement sur la touche « Entrée » de votre clavier sans attendre la fin de la recherche.

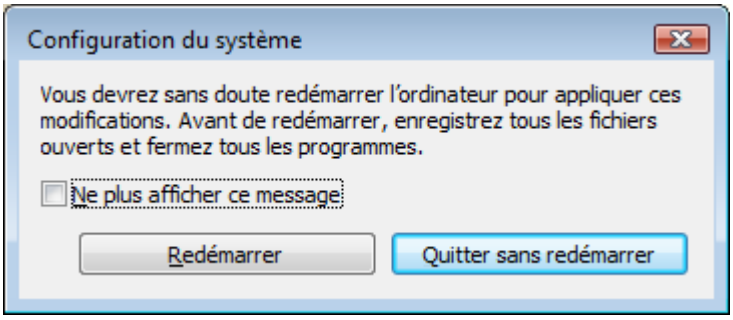
Ensuite, cliquez sur le bouton « Continuer ».



Cliquez sur l'onglet « Démarrer » (voir cadre violet de l'image ci-dessous) et cochez la case « Démarrage sécurisé » (voir cadre rouge). Si on vous demande de redémarrer en mode sans échec avec prise en charge du réseau, cochez la case « Réseau ». Cliquez ensuite sur le bouton « OK ».



Une petite fenêtre vous demandera s'il faut redémarrer. Si c'est votre souhait, cliquez sur le bouton « Redémarrer ». Dans le cas contraire, cliquez sur le bouton « Quitter sans redémarrer » :



Cette manipulation permet de redémarrer en mode sans échecs. Cependant, chaque démarrage se fera désormais en mode sans échec. Pour pouvoir redémarrer en mode normal, il faut faire l'opération inverse de ce qui a été fait (il faut donc retourner dans msconfig, puis dans l'onglet « Démarrer » et il faudra décocher la case « Démarrage sécurisé »).

VI.2) Désactiver la restauration du système

VI.2.a) La restauration du système, qu'est-ce que c'est ?

La restauration du système est un mécanisme qui sauvegarde régulièrement une partie de votre système d'exploitation importante au fonctionnement de votre ordinateur. Ceci permet en cas de bêtise de votre part, ou en cas d'un programme nouvellement installé qui serait défaillant, de revenir en arrière avant que le programme ne soit installé, ou avant que la bêtise ne soit faite.

Ce mécanisme intervient automatiquement à intervalle régulier et très souvent avant que vous n'installiez un logiciel.

Vous vous doutez bien que tout le contenu de l'ordinateur ne peut être sauvegardé, car ceci prendrait un espace de stockage trop important et demanderait beaucoup de temps à chaque sauvegarde. Ça ne permet donc pas de récupérer un document de traitement de texte effacé par accident après avoir vidé la corbeille. Mais ça peut quand même dépanner sans être obligé de demander de l'aide à un ami.

Le problème, c'est que si votre ordinateur est infecté, de nombreux virus et autres cochonneries aiment bien aussi infecter les fichiers de sauvegarde. Du coup, si vous tentez une restauration du système, vous serez toujours infecté.

Il peut donc être utile de désactiver la restauration du système sur un ordinateur infecté afin de pouvoir supprimer tout les fichiers de sauvegarde. Ne le faites que dans le cas ou votre ordinateur serait infecté et qu'on vous demande de le faire.

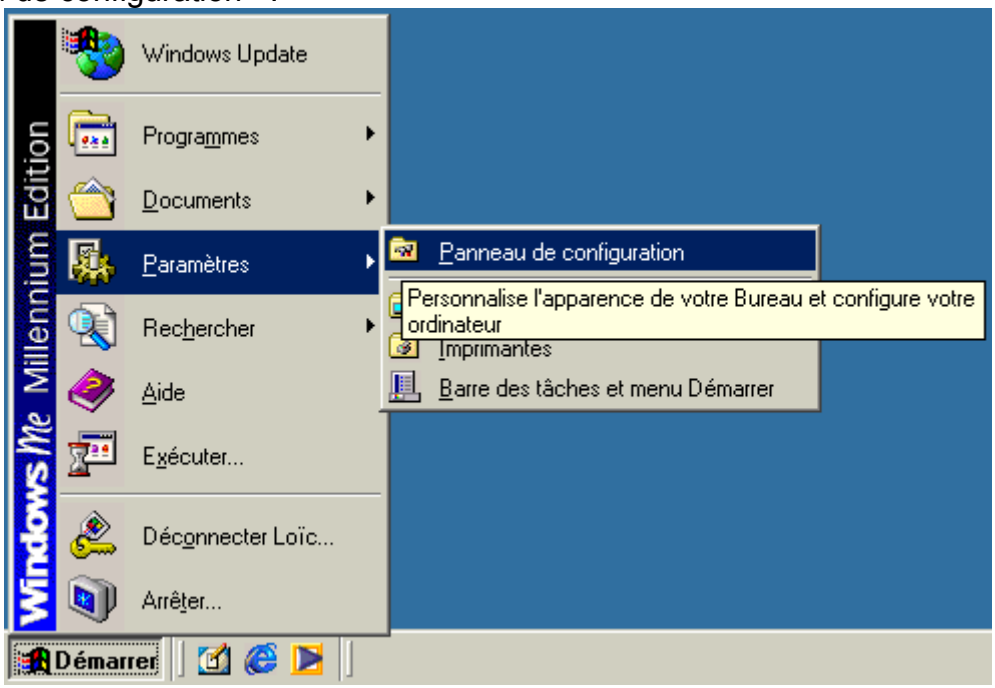
VI.2.b) Comment la désactiver

Nous allons donc voir comment désactiver la restauration du système sous Windows Millenium, 2000, XP et Vista.

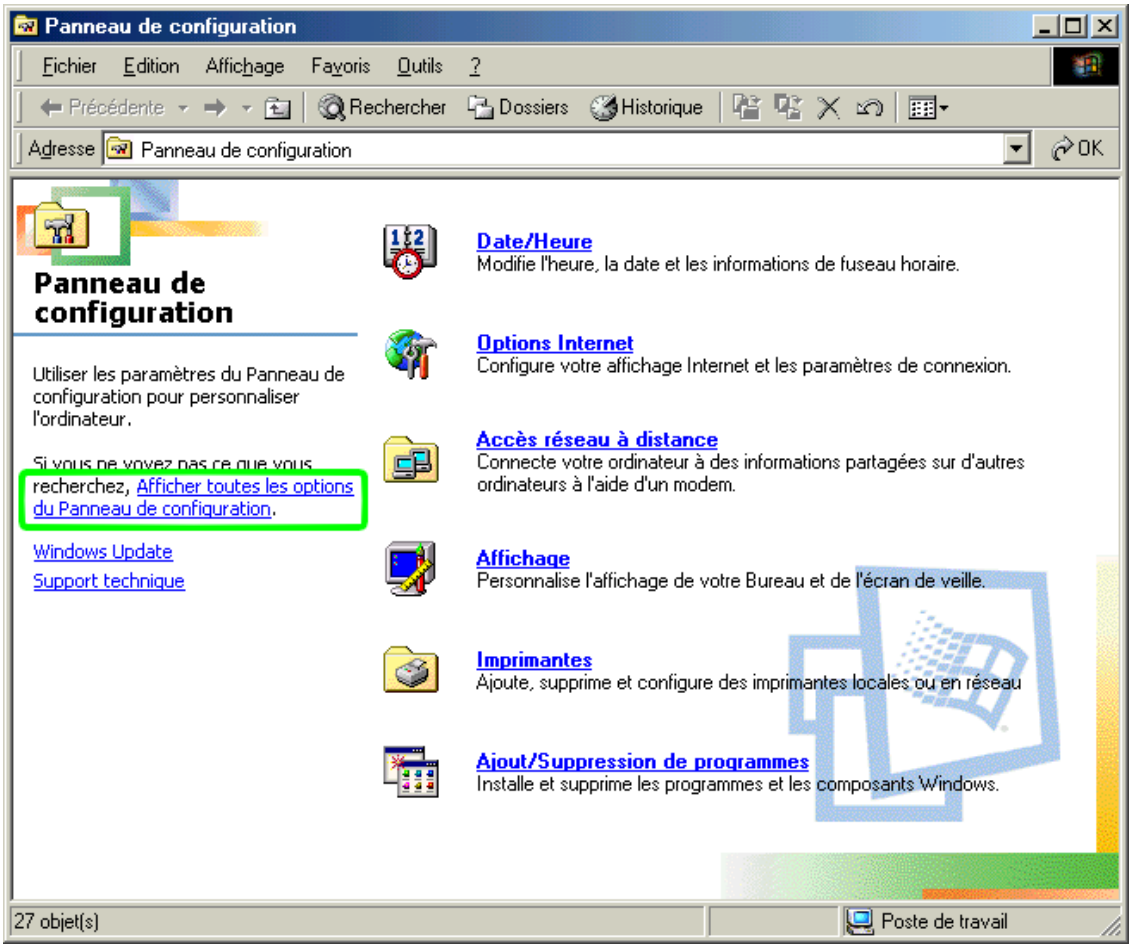
La restauration du système n'existe pas sous Windows 2000, 98 et 95.

VI.2.b.i) Sous Windows Me

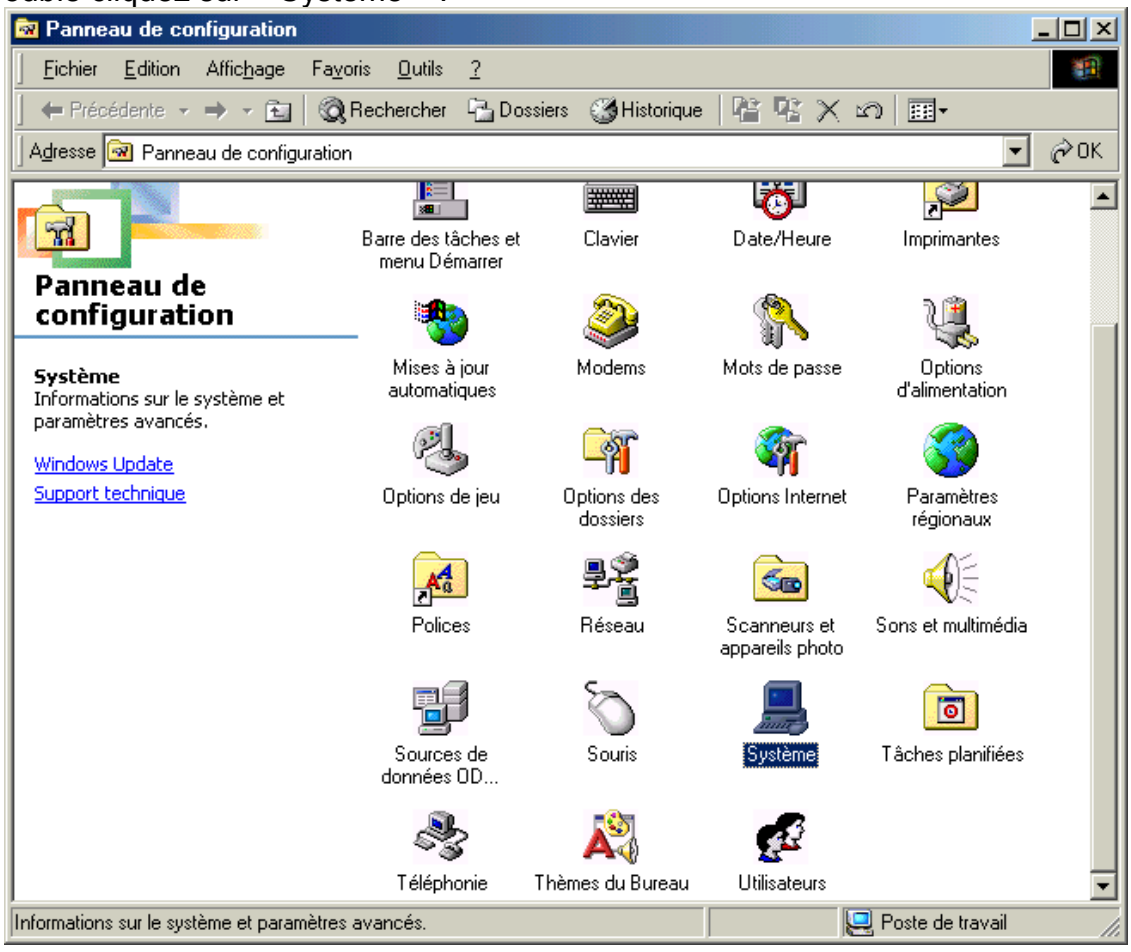
Cliquez sur votre bouton « Démarrer », allez dans le menu « Paramètres » et cliquez sur le « Panneau de configuration ».

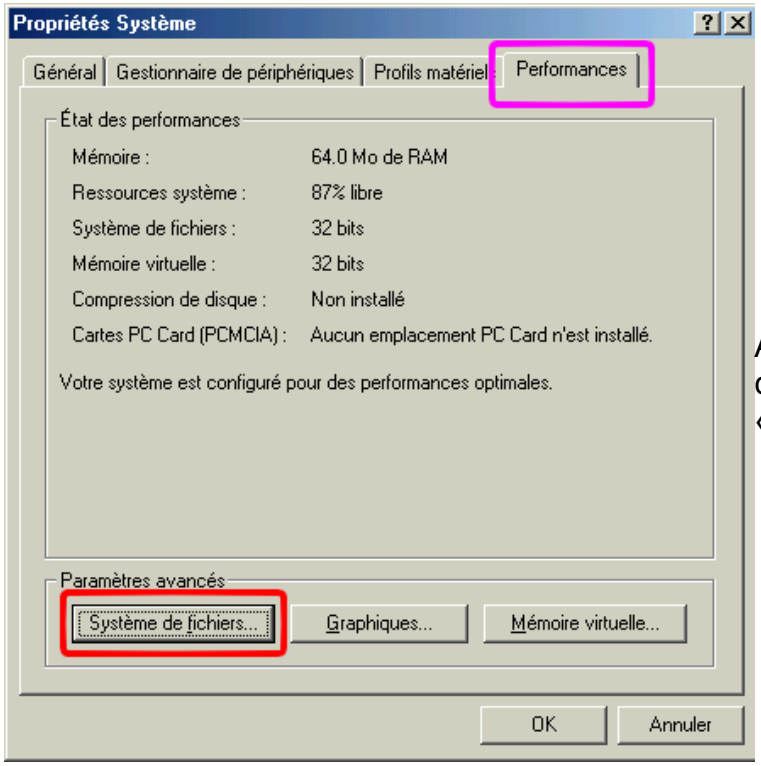


Si vous avez la fenêtre ci-dessous, cliquez sur le lien « Afficher toutes les options du panneau de configuration » (voir cadre vert de l'image ci-dessous) :



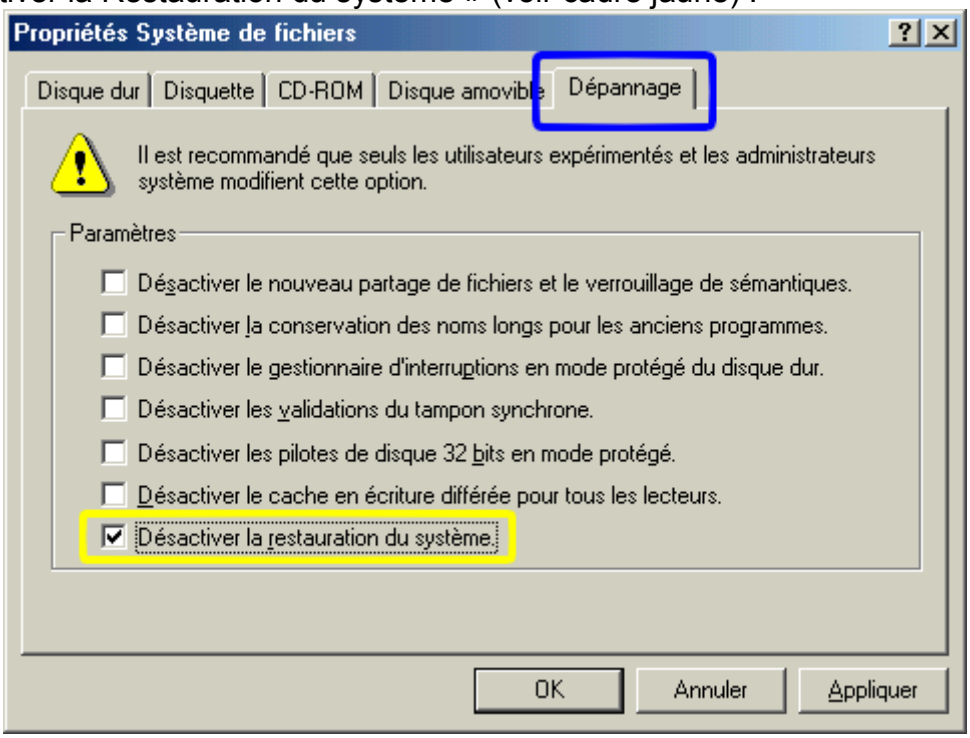
Double cliquez sur « Système » :





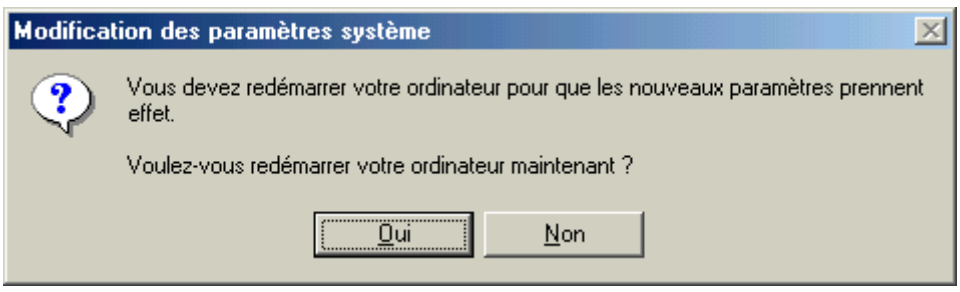
Allez dans l'onglet « Performances » (voir cadre violet), puis cliquez sur le bouton « Système de fichiers » (voir cadre rouge).

Allez dans l'onglet « Dépannage » (voir cadre bleu de l'image ci-dessous), et cochez la case « Désactiver la Restauration du système » (voir cadre jaune) :



Puis cliquez sur le bouton « OK ».

Cliquez sur le bouton « Fermer » de la fenêtre « Propriétés Système ».

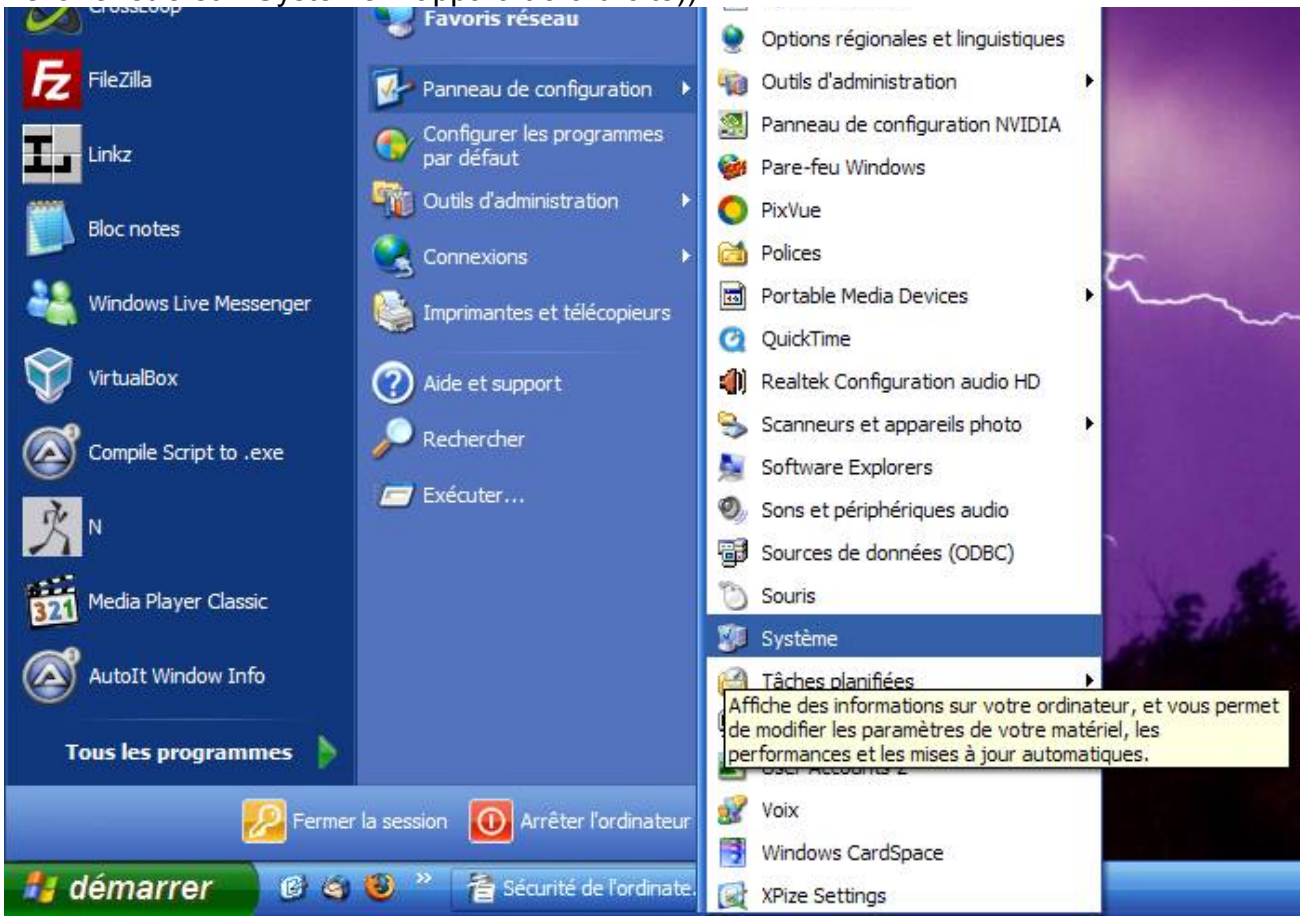


Sauvegardez votre travail en cours et cliquez sur le bouton « Oui ».

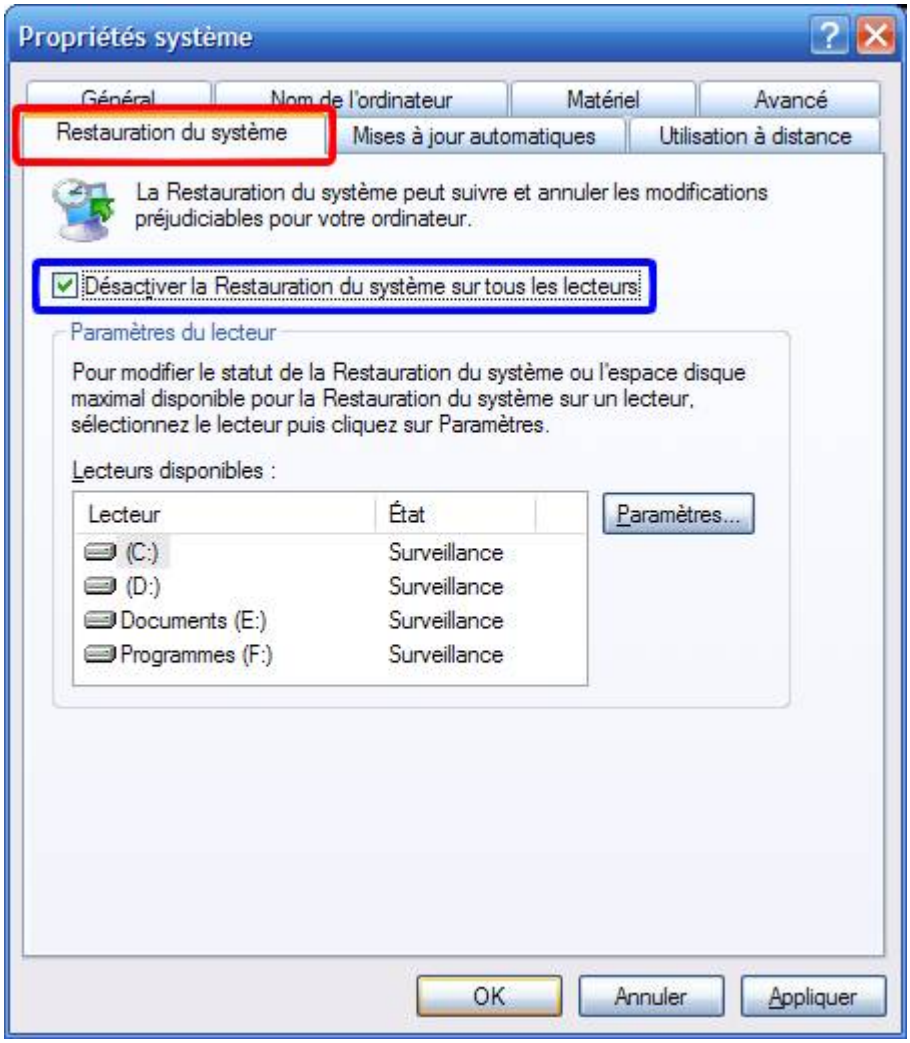
Pour réactiver la restauration du système, il faudra refaire l'opération mais en décochant la case « Désactiver la restauration du système ».

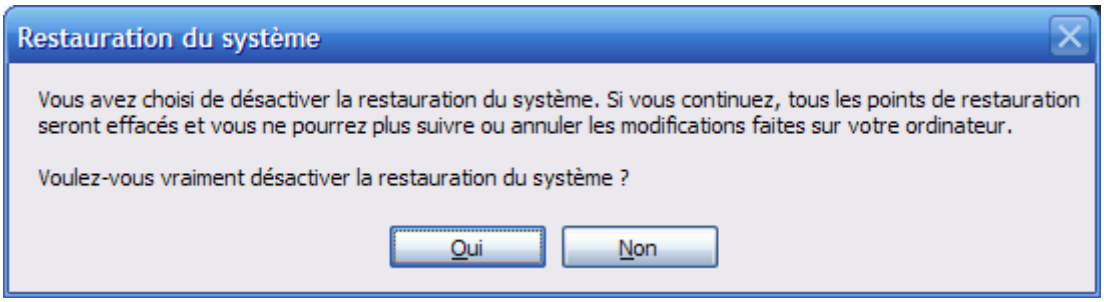
VI.2.b.ii) Sous Windows XP

Allez dans le panneau de configuration, puis allez ensuite dans « Système » (il se peut que vous n'ayez pas le panneau de configuration en menu comme ci-dessous, dans ce cas, cliquez sur Panneau de configuration, puis ensuite, double cliquez dans « Système » (si vous n'avez pas non plus « Système », cliquez sur « Basculer vers l'affichage classique » à gauche dans la fenêtre et « Système » apparaîtra à droite)) :



Allez ensuite dans l'onglet « Restauration du système » (voir cadre rouge de l'image ci-dessous) puis cochez la case « Désactiver la restauration du système sur tous les lecteurs » (cadre bleu), puis cliquez ensuite sur le bouton « OK » :



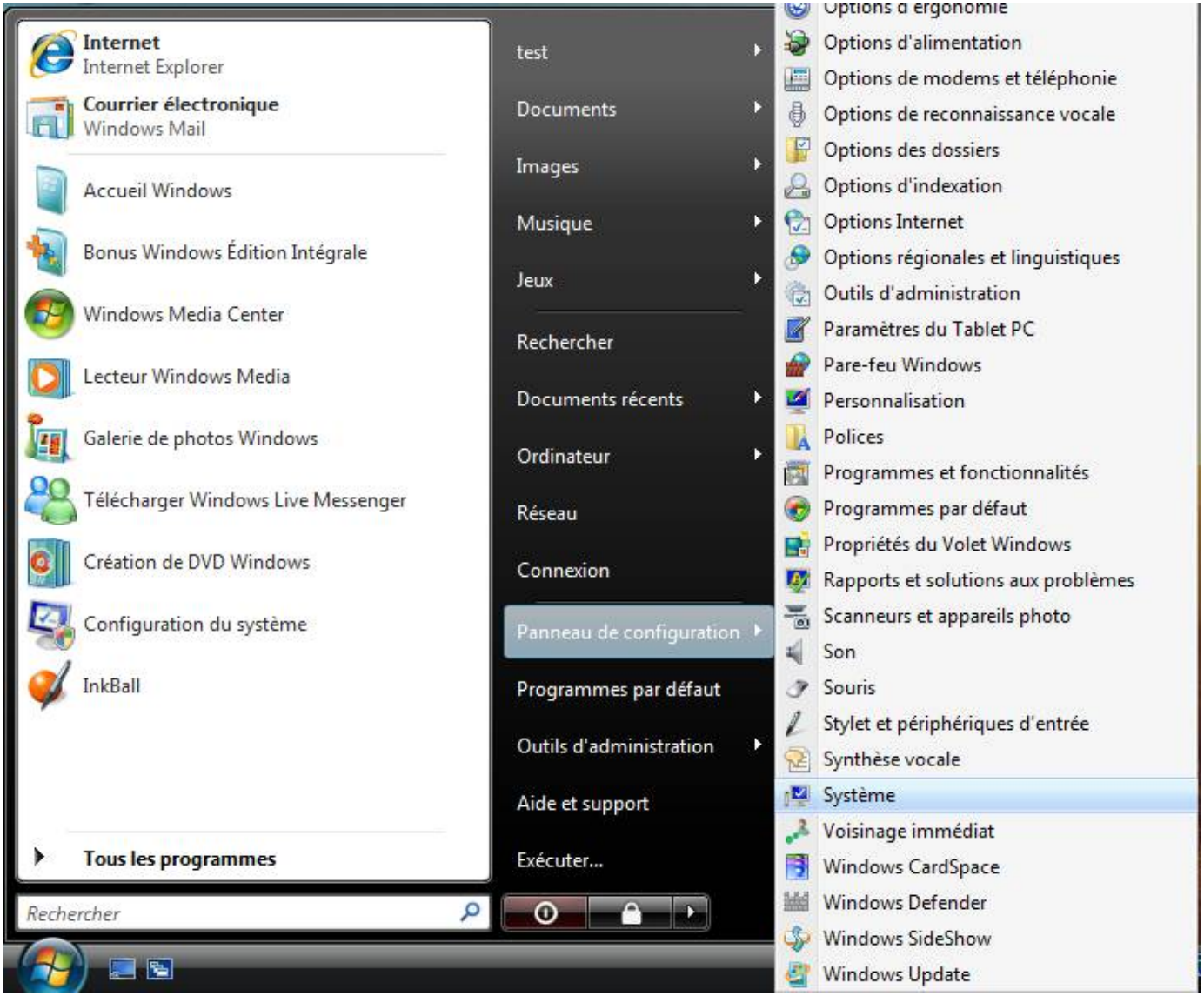


Cliquez sur le bouton « Oui ».

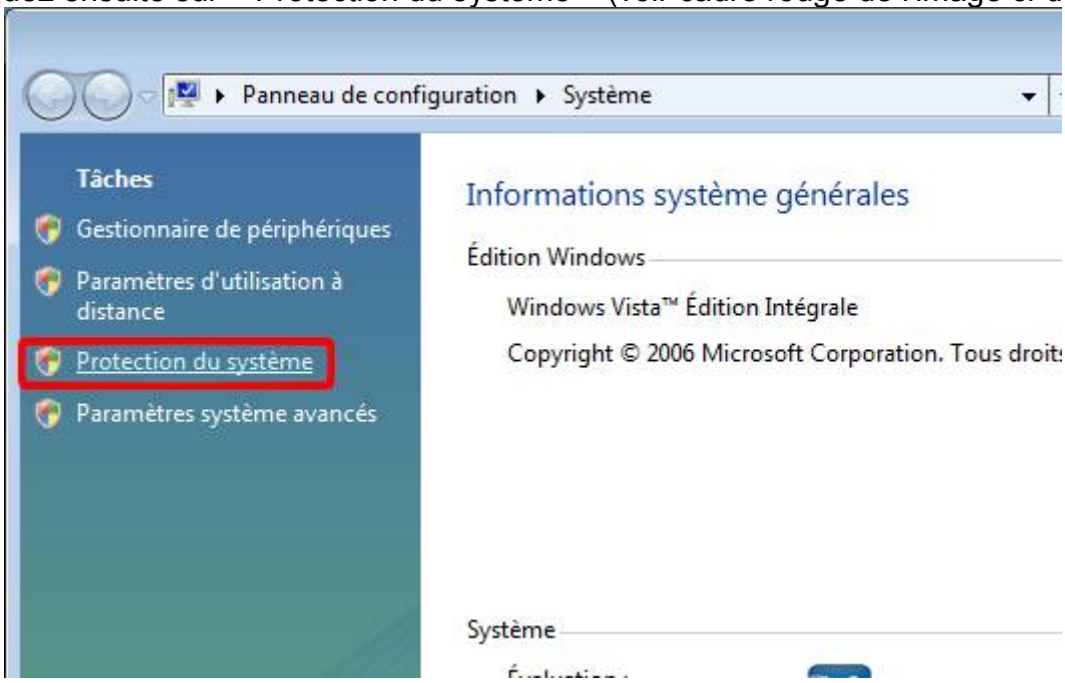
Si vous souhaitez réactiver la restauration du système, il suffira de faire l'opération inverse (donc décocher la case « Désactiver la restauration du système sur tous les lecteurs »).

VI.2.b.iii) Sous Windows Vista

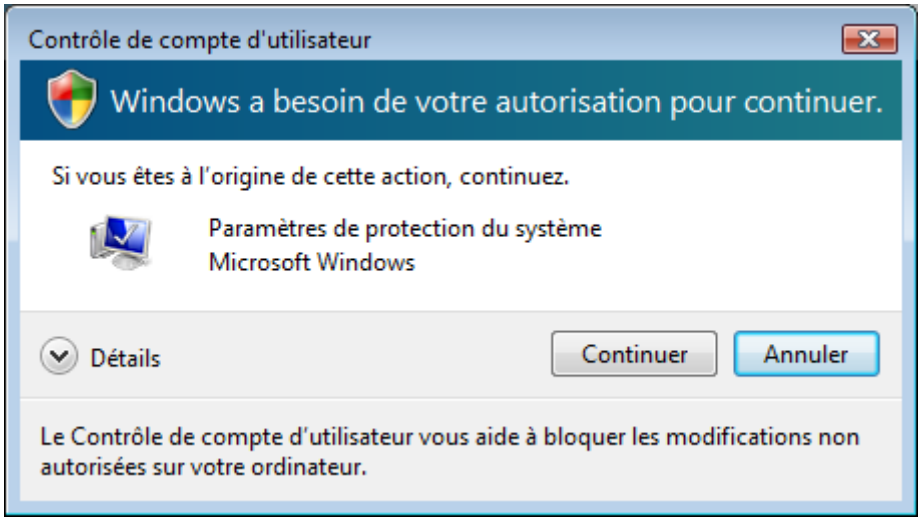
Allez dans le panneau de configuration, puis allez ensuite dans « Système » (il se peut que vous n'ayez pas le panneau de configuration en menu comme ci-dessous, dans ce cas, cliquez sur Panneau de configuration, puis ensuite, double cliquez dans « Système » (si vous n'avez pas non plus « Système », cliquez sur « Affichage classique » à gauche dans la fenêtre et « Système » apparaîtra à droite)) :



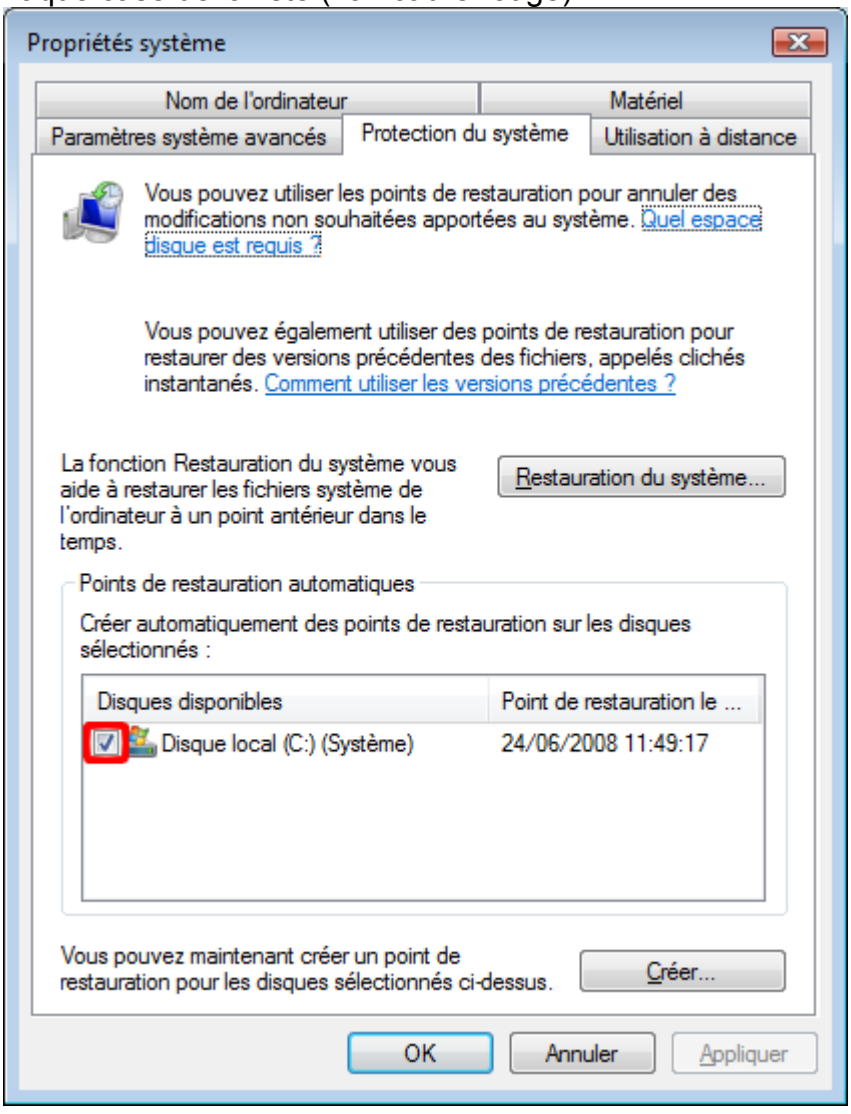
Cliquez ensuite sur « Protection du système » (voir cadre rouge de l'image ci-dessous) :



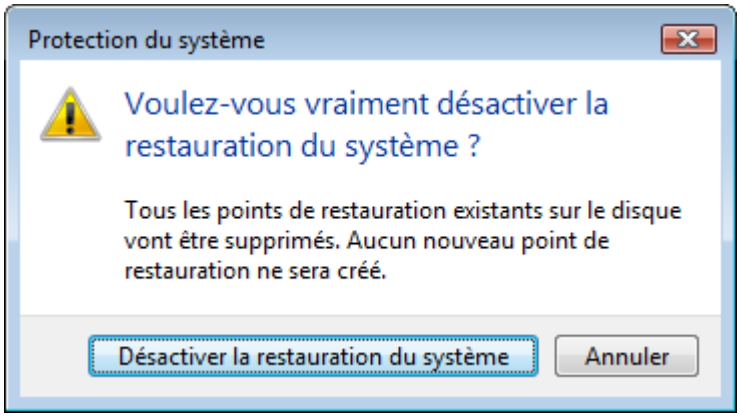
Cliquez ensuite sur le bouton « Continuer » :



Décocher chaque case de la liste (voir cadre rouge) :



Pour chaque case décochée, une petite fenêtre apparaîtra :



Cliquez sur le bouton « Désactiver la restauration du système ».

VI.3) HijackThis

C'est de ce logiciel dont je parlais dans la petite introduction de cette partie qui fait des analyses qui permettront à des gens compétents de vous débarrasser de vos virus/logiciels espions/cochonneries qui seraient dans votre ordinateur.

Ce logiciel n'est pas le seul dans son domaine. Je traiterai ultérieurement le cas d'un autre logiciel.

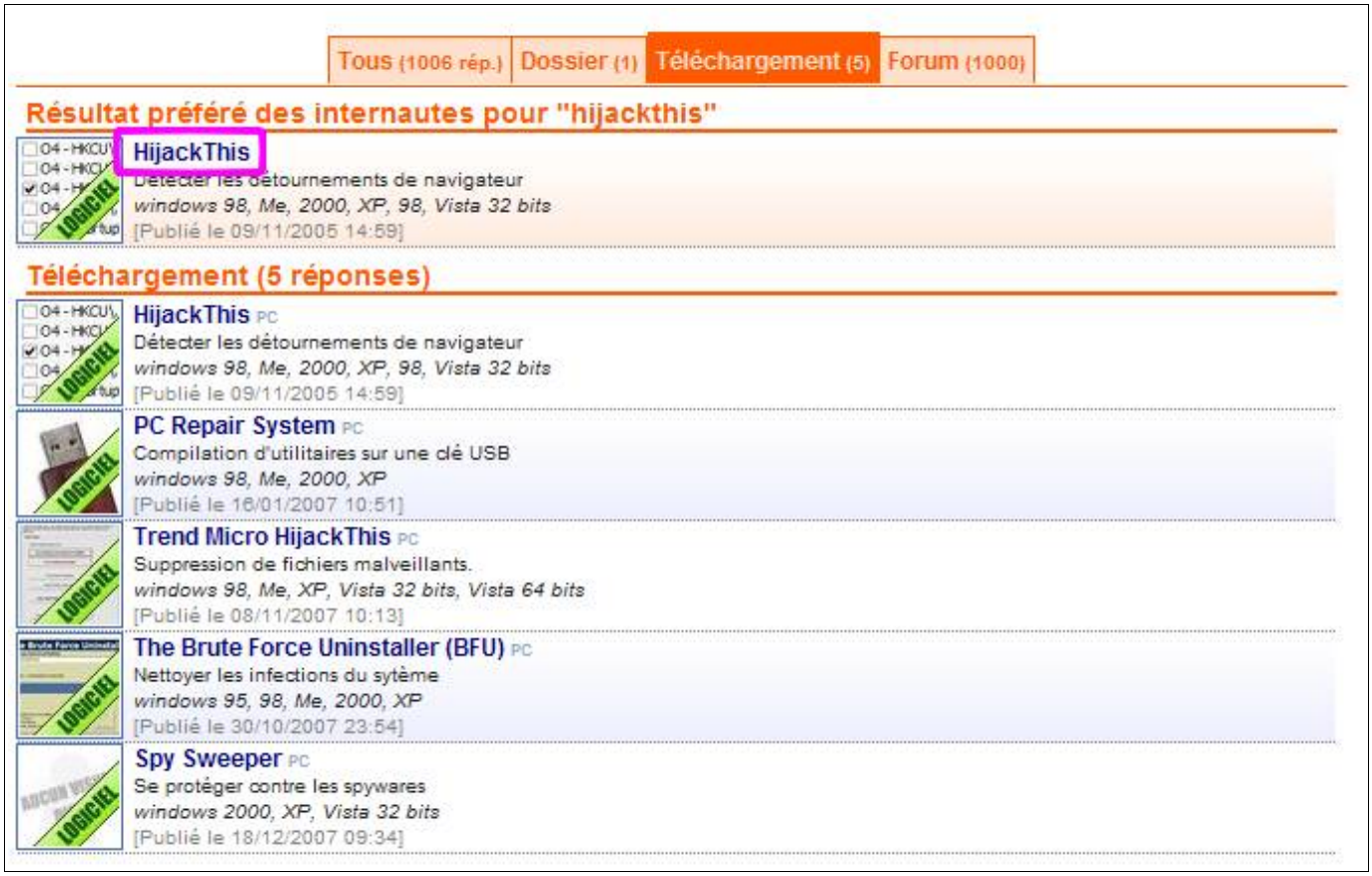
VI.3.a) Téléchargement et installation de HijackThis

Nous allons utiliser le site Clubic pour télécharger ce logiciel (ce qui illustrera en même temps ce que je disais à propos de télécharger sur des sites connus).

Il va falloir aller sur le site de Clubic. Pour cela, vous pouvez taper l'adresse de ce site (www.clubic.com) dans la barre d'adresses, ou encore le rechercher via Google.

Cliquez sur le bouton « Télécharger » (en haut de la page d'accueil de Clubic).

Dans le moteur de recherche en haut de la page, tapez « HijackThis » et appuyez sur le bouton « Rechercher ».



Cliquez sur le « résultat préféré des internautes pour "hijackthis" » (voir cadre violet de l'image ci-dessus).

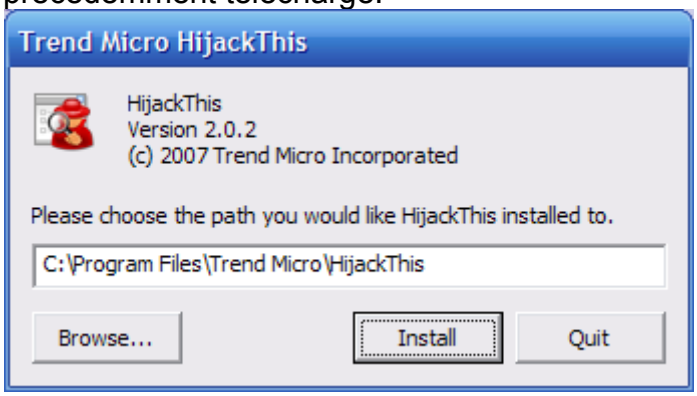
Cliquez ensuite sur le bouton « TÉLÉCHARGER gratuitement » (voir cadre bleu de l'image ci-dessous) :

Cliquez ensuite sur le lien « Lancer le téléchargement » (voir cadre vert de l'image ci-dessous) :

Téléchargez le fichier à un emplacement ou vous pourrez le retrouver facilement.

VI.3.b) Installer HijackThis

Ouvrez le fichier précédemment téléchargé.



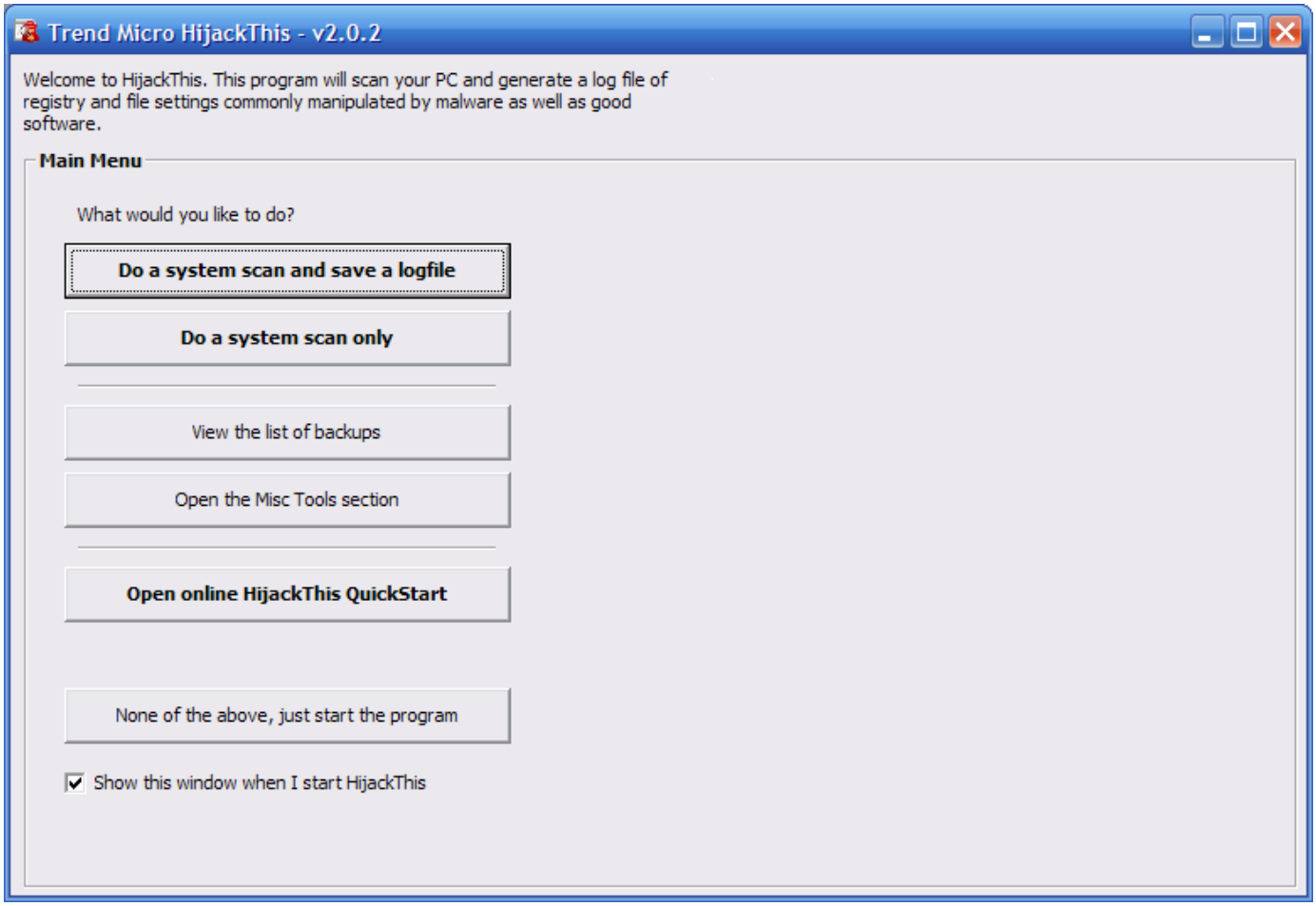
Cliquez sur le bouton « Install ».

C'est tout pour ce qui est de l'installation. Une icône sera créée pour lancer le logiciel. D'ailleurs, celui-ci se lancera automatiquement juste après avoir cliqué sur le bouton « Install ».

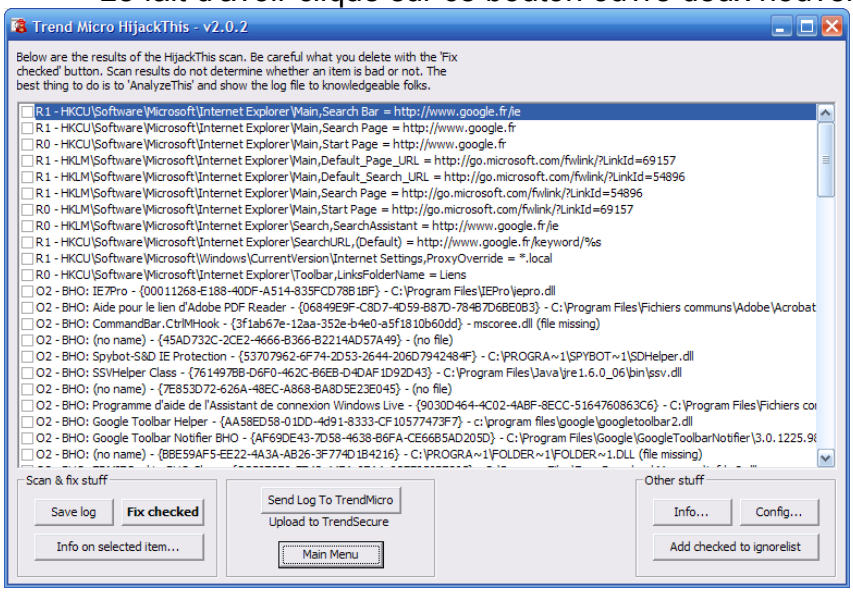
VI.3.c) Analyser son ordinateur

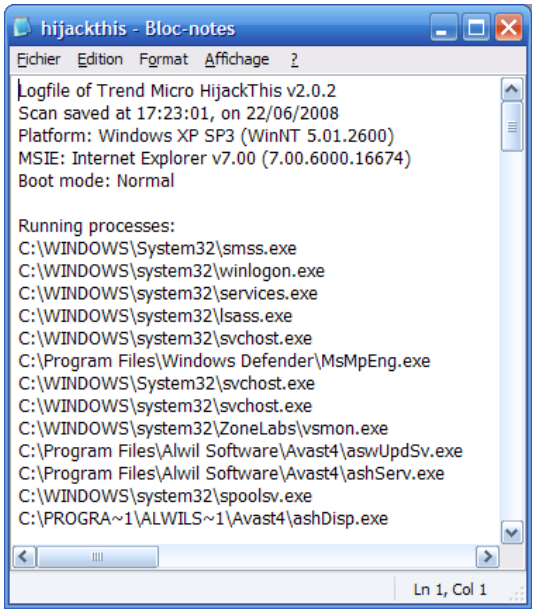
S'il n'a pas déjà été ouvert par l'installation que vous venez peut-être d'effectuer, lancez HijackThis via l'icône qui a été créée sur le bureau.

Cliquez sur le bouton « Do a system scan and save logfile » (ce qui signifie : Effectuer une analyse du système et sauvegarder le rapport) :



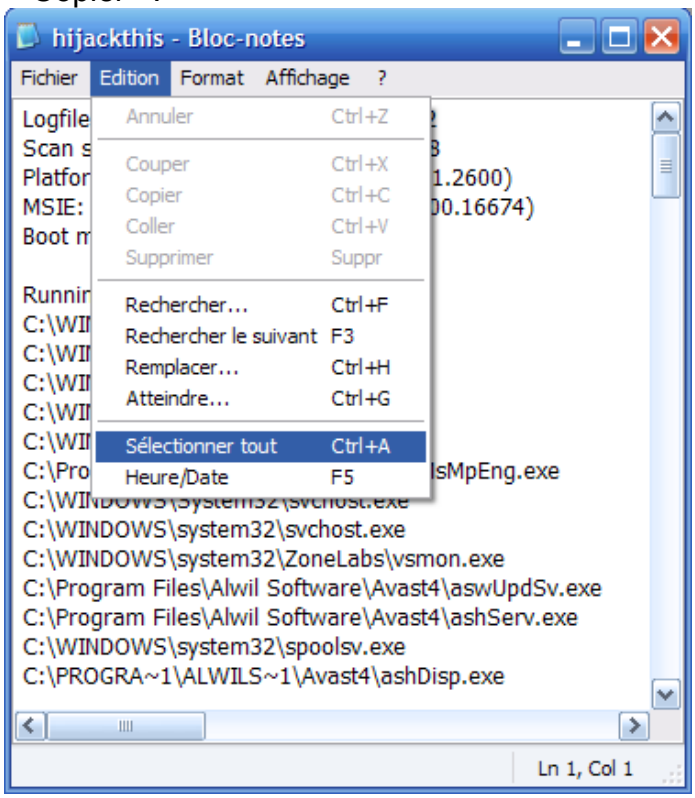
Le fait d'avoir cliqué sur ce bouton ouvre deux nouvelles fenêtres et ferme la première :

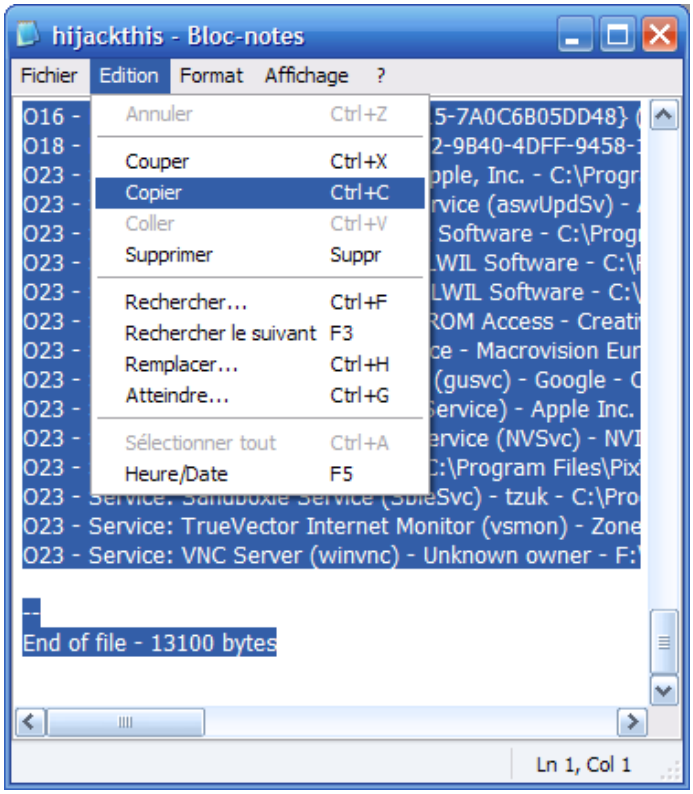




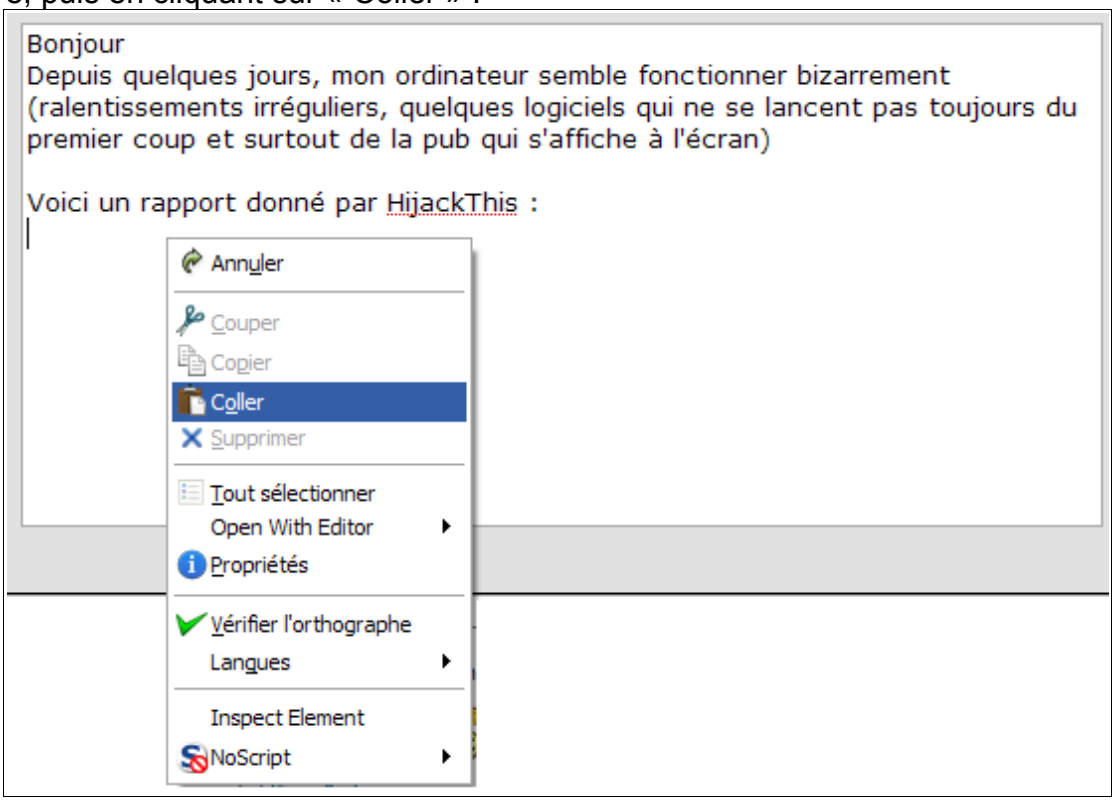
Celle de gauche permettra de résoudre le ou les problèmes contenus dans votre ordinateur tandis que celle de droite contient un rapport que vous pourrez transmettre.

Si vous vous faites aider par un forum, il vous sera demander de faire un copier coller du rapport. Pour ceci, dans la fenêtre du « Bloc notes », allez dans le menu « Edition » puis cliquez sur « Sélectionner tout ». Retournez dans le menu « Edition » et cliquez cette fois sur « Copier ».



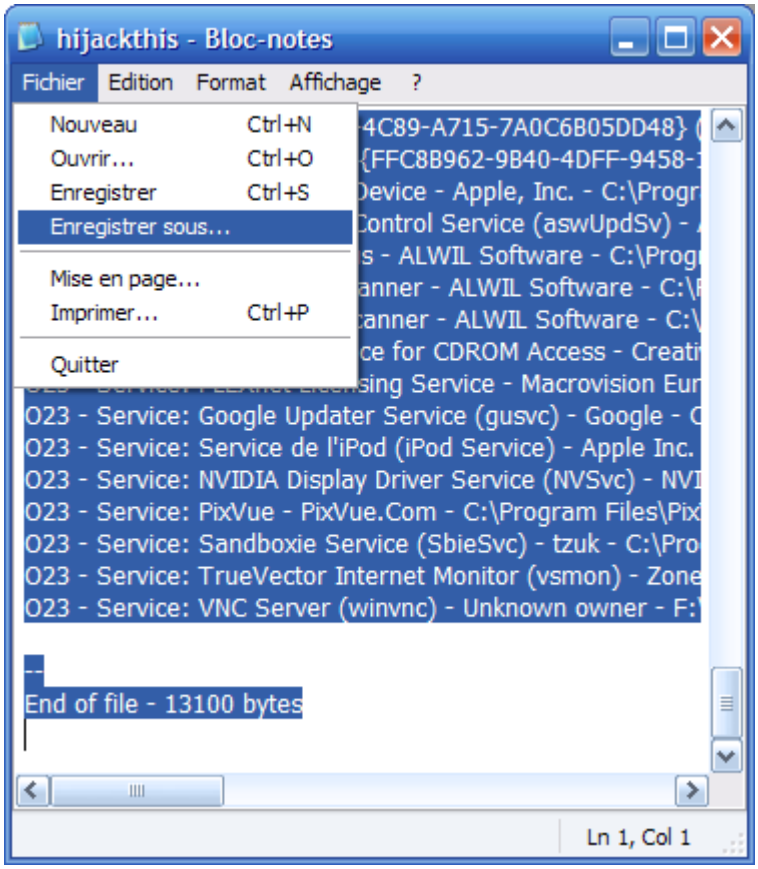


Ainsi, vous pourrez coller votre rapport sur un forum avec un simple clic droit là où il doit apparaître, puis en cliquant sur « Coller » :



Si vous vous faites assister par messagerie instantanée (Windows Live Messenger, Yahoo Messenger, ...), un copier coller ne marchera pas car ces logiciels ont presque tous (pour ne pas dire tous) une limite en nombre de lettres lorsque vous envoyez un message.

Il faudra donc enregistrer le rapport sous forme de fichier pour pouvoir l'envoyer. Pour ceci, il vous suffira dans la fenêtre du Bloc notes d'aller dans le menu « Fichier » puis dans « Enregistrer sous » et d'enregistrer le fichier (si possible à un emplacement ou il vous sera facile de le retrouver, sur le bureau par exemple).



VI.3.d) Réparer un problème

Cette partie est la plus dangereuse. Pour rappel, ce logiciel ne fait qu'analyser un certain nombre de points sensibles de votre ordinateur et montre tout ce qu'il y trouve. Il y a donc des logiciels légitimes et parfois des logiciels qui n'ont rien à faire là.

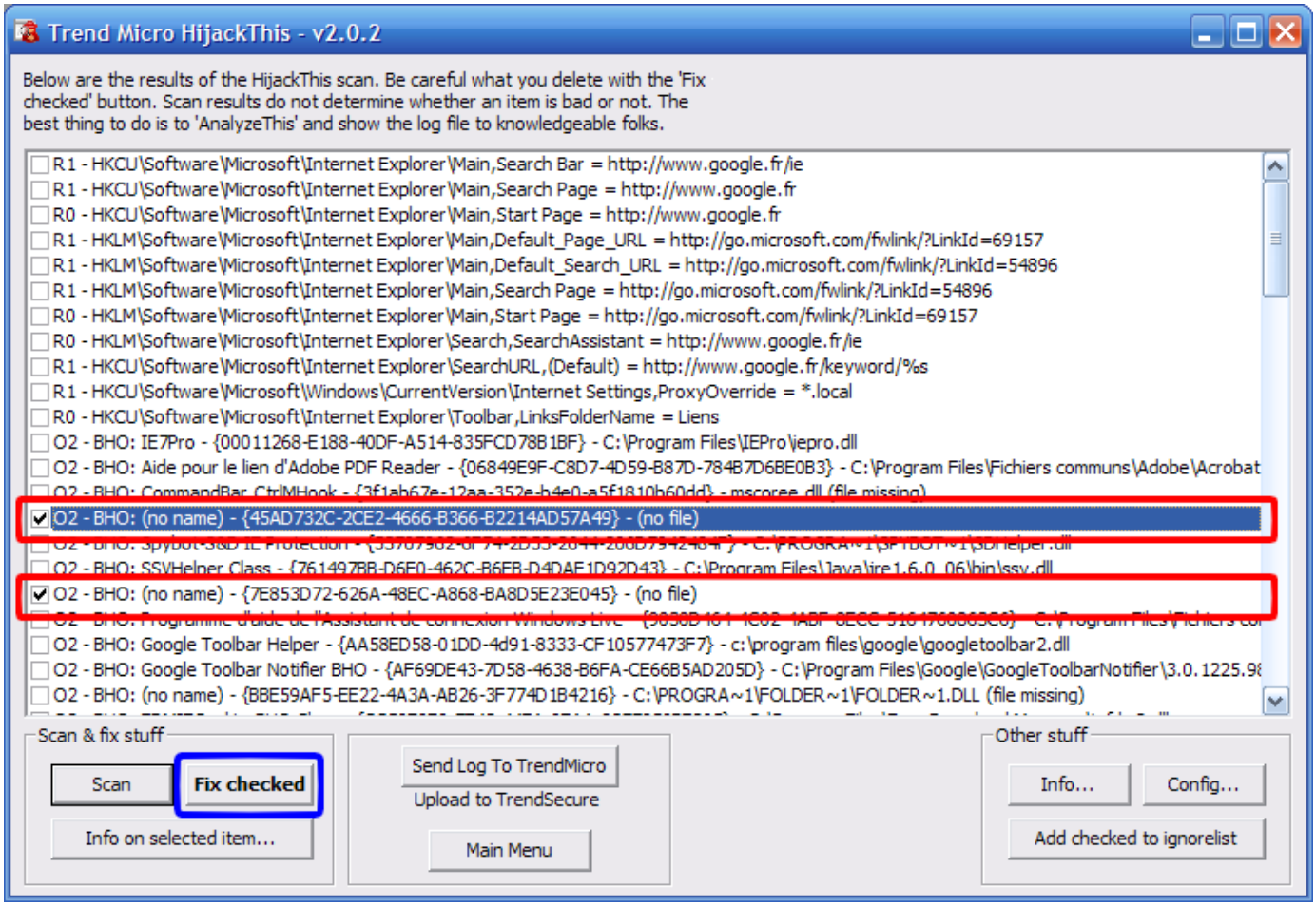
Il ne faut donc réparer que si vous êtes sûr de ce que vous faites, ou que l'interlocuteur est fiable.

Revenons en au fonctionnement de ce logiciel :

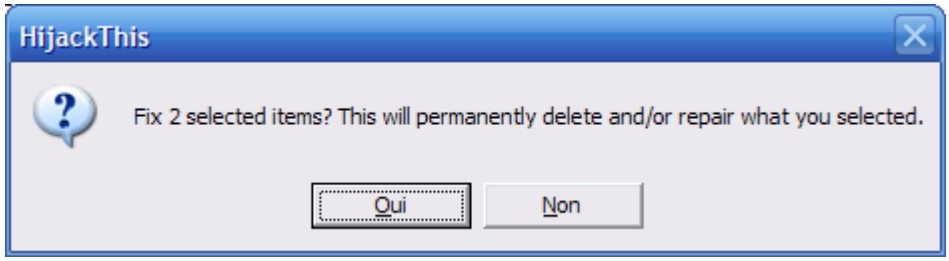
Si par exemple un expert vous dit de « fixer » les lignes suivantes :

O2 - BHO: (no name) - {45AD732C-2CE2-4666-B366-B2214AD57A49} - (no file)
O2 - BHO: (no name) - {7E853D72-626A-48EC-A868-BA8D5E23E045} - (no file)

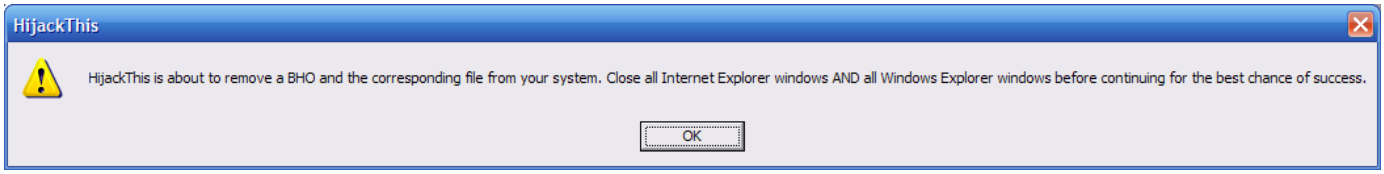
Il faudra que vous les retrouviez dans la même fenêtre que ci-dessous, et que vous cochiez les cases au début de ces lignes :



Il faudra ensuite cliquer sur le bouton « Fix checked ».



Hijackthis vous demandera ensuite confirmation. Cliquez sur « Oui ».



Si cette fenêtre apparaît, fermez toutes les fenêtres de dossiers qui seraient ouvertes ainsi que toutes les fenêtres de Internet Explorer, et cliquez sur le bouton « OK ».

VI.4) Unlocker

Ce petit logiciel bien sympathique permet d'effectuer des opérations sur un fichier même si Windows ne veut pas le faire. Il permet entre autres la suppression de fichiers.

VI.4.a) Télécharger Unlocker

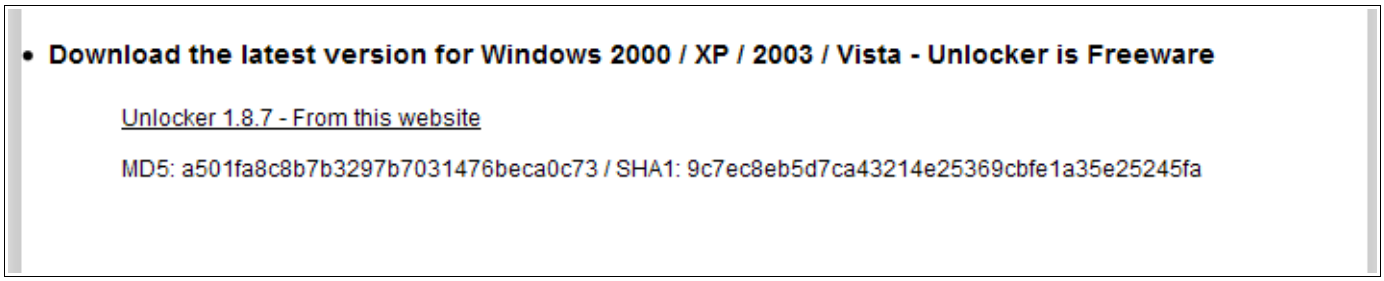
Cherchons le site officiel de ce logiciel par Google (ou n'importe lequel de vos moteurs de recherche favoris).

Tapez « unlocker » dans la zone de texte de recherche et appuyez sur le bouton pour rechercher.

Recherchez dans la liste ce résultat :

Cliquez dessus parmi la liste des résultats.

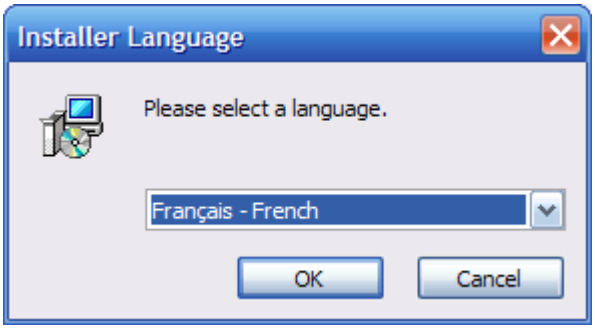
Cliquez ensuite sur le lien « Download » (voir cadre rouge de l'image ci-dessus).



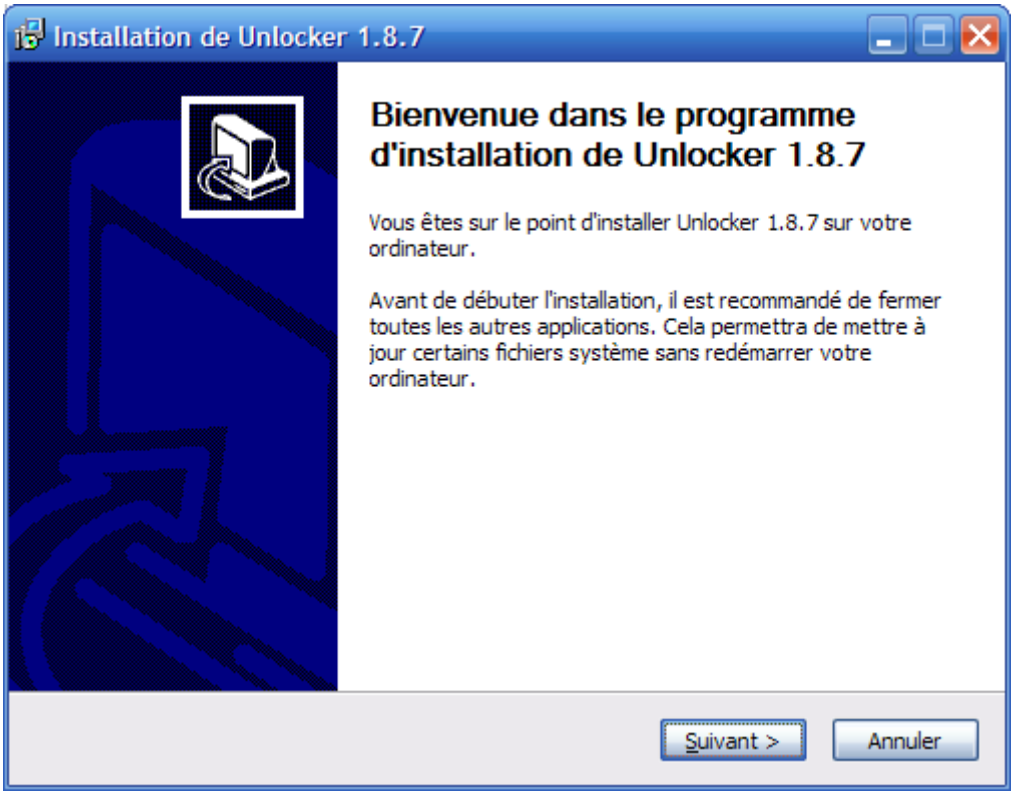
Cliquez ensuite sur le lien « Unlocker 1.8.7 – From this website » et enregistrez le fichier proposé dans votre ordinateur.

VI.4.b) Installer Unlocker

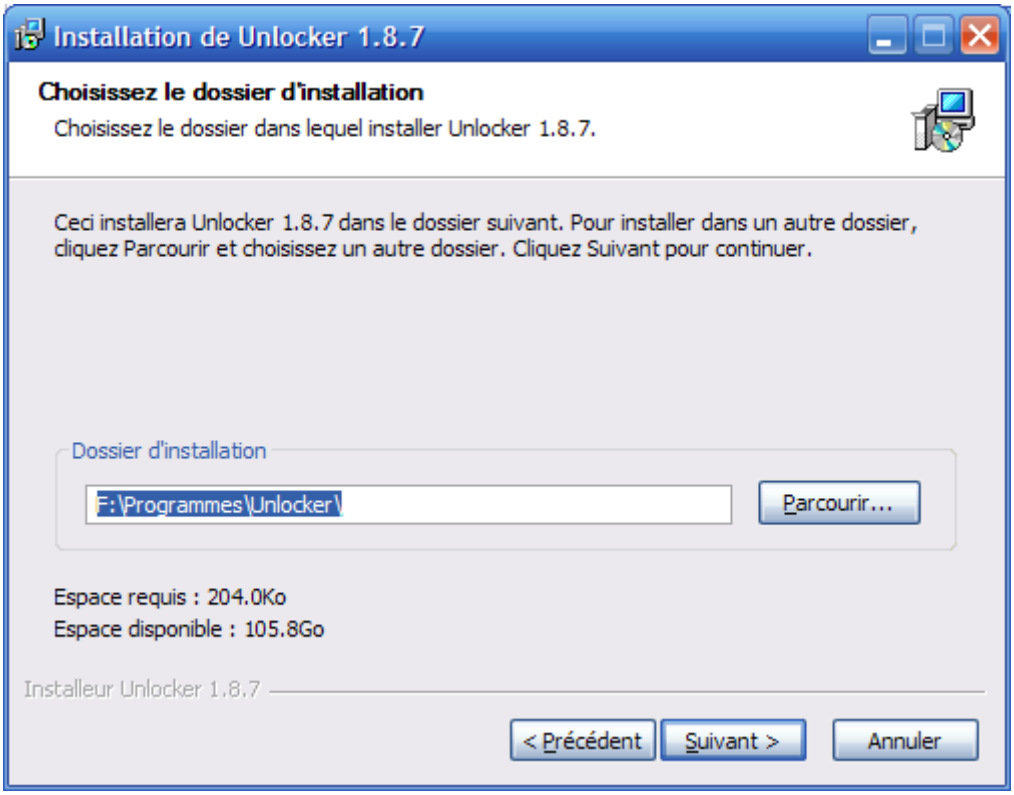
Ouvrez le fichier précédemment téléchargé.



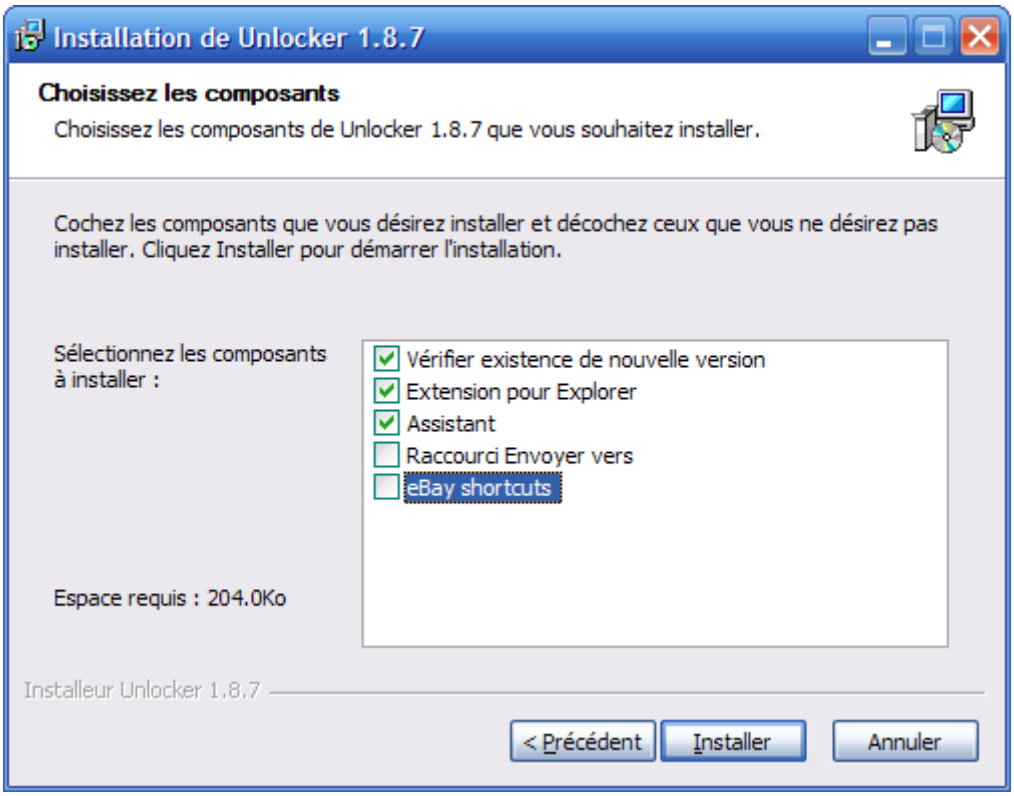
Cliquez sur le bouton « OK ».



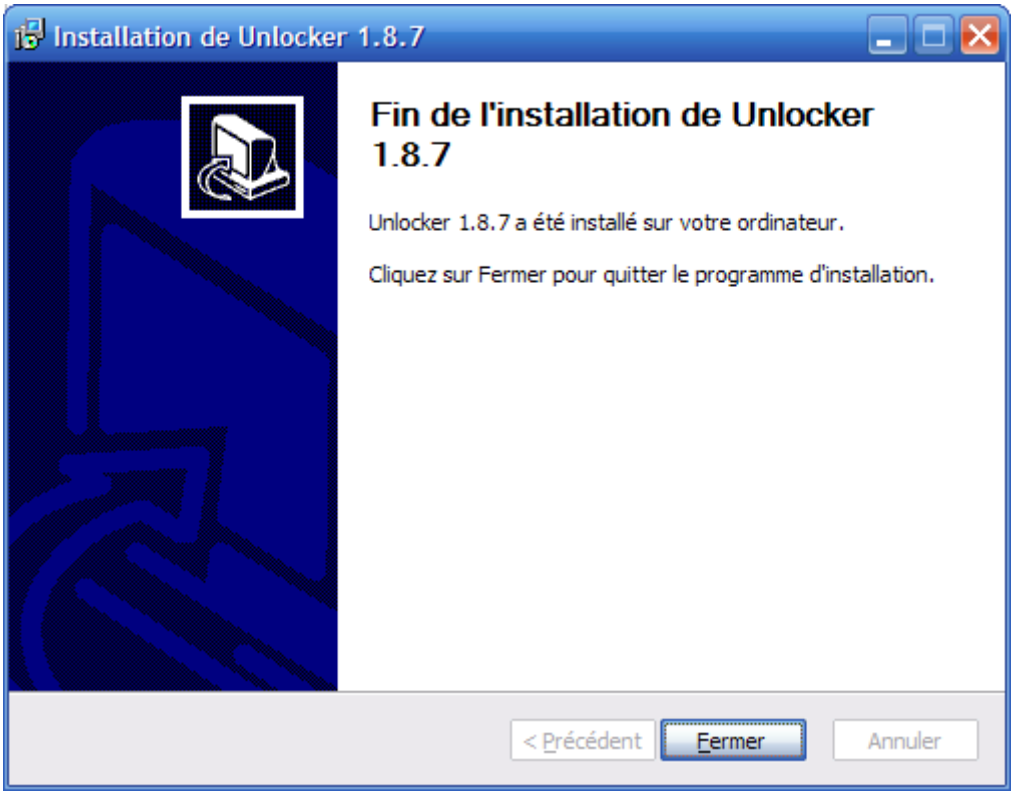
Cliquez sur le bouton « Suivant ».



Cliquez sur le bouton « Suivant ».



Cochez les trois premières cases et décochez les deux dernières.

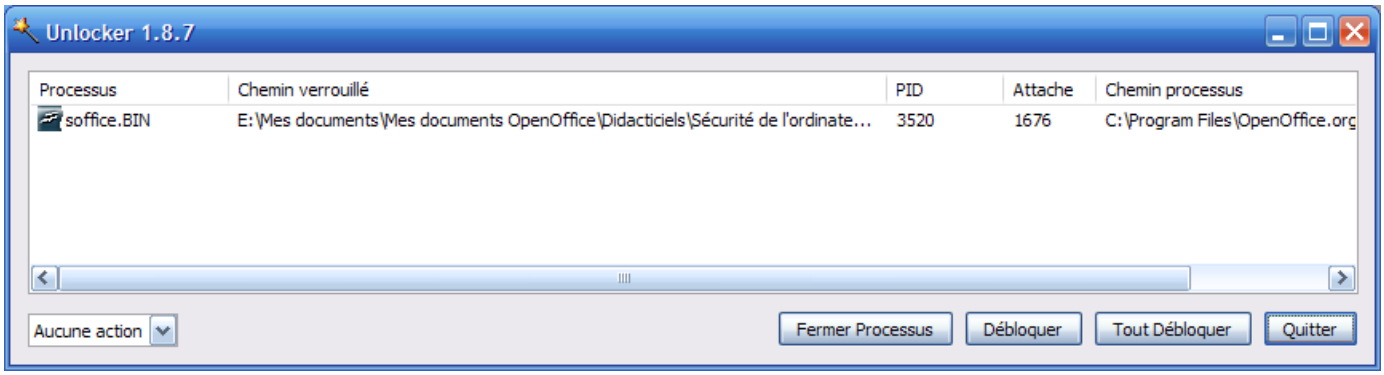


Patientez quelques secondes le temps de l'installation du logiciel et cliquez sur le bouton « Fermer ».

VI.4.c) Utiliser Unlocker

Lorsque vous voulez supprimer un fichier qui ne veut pas être supprimé par Windows, Unclocker apparaît et vous demande ce que vous voulez faire avec le fichier.

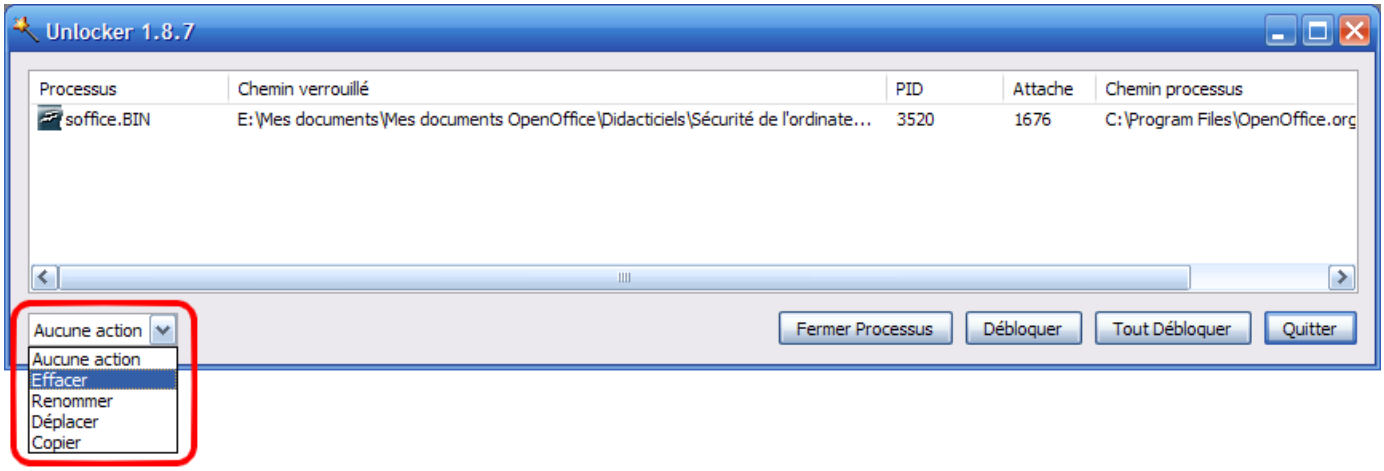
La fenêtre ressemble à ceci :



Chaque ligne indique un ou plusieurs processus bloquant le fichier. Dans ce cas, il y a plusieurs solutions : désassocier le fichier du programme qui le bloque ou fermer le programme qui bloque le fichier (ce qui débloque le fichier).

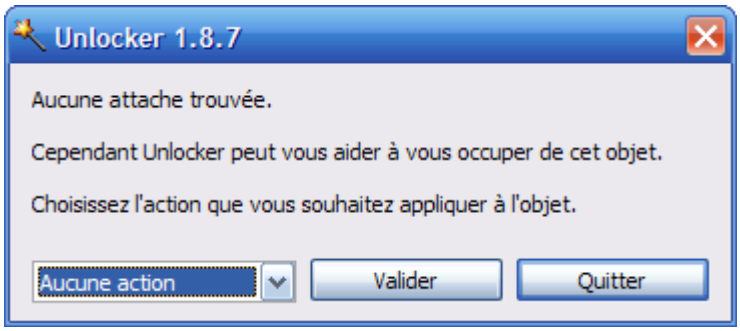
Il faut d'abord choisir l'action à effectuer en bas à gauche de la fenêtre (en déroulant la liste) en cliquant soit sur « Effacer », soit « Renommer », soit « Déplacer » ou soit « Copier ».

Ensuite, si vous voulez effectuer une action sur votre fichier sans quitter le ou les programmes qui gênent, cliquez sur le bouton « Tout débloquer ». Si le fait de fermer le programme bloquant le fichier ne pose pas de problème, vous pouvez cliquer sur « Fermer Processus ».



Soit une fenêtre vous informera de la réussite de l'opération, soit une fenêtre vous proposera d'effectuer l'action après un redémarrage. Dans ce dernier cas, il faudra redémarrer l'ordinateur pour que le fichier soit peut-être supprimé/renommé/déplacé/copié.

Il se peut aussi qu'aucun programme ne bloque le fichier sur lequel vous voulez agir, ou qu'Unlocker ne trouve pas de programme bloquant le fichier. Dans ce cas, Unlocker apparaît comme ceci :



Le fonctionnement est presque identique :

Choisissez une action en bas à gauche dans la fenêtre et cliquez ensuite sur le bouton « Valider ».

VI.4.d) Conclusion sur Unlocker

Je vous recommande d'installer ce petit logiciel car il peut être bien pratique quand Windows décide d'être casse pieds. Je vous le recommande aussi car il m'a permit une fois d'aider un ami à se débarrasser d'un fichier récalcitrant, fichier qui était très certainement un morceau d'un logiciel espion.

VI.5) Teamviewer

VII) Quelques mises à jour de quelques programmes

Comme nous l'avons vu précédemment, il est important de mettre à jour ses programmes afin d'éviter les problèmes de virus exploitant des failles de sécurité.

Dans cette section, nous verrons comment mettre à jour Windows (XP et Vista), Firefox et Thunderbird (la procédure étant identique pour les deux, il n'y aura qu'une seule section traitant de ce sujet) ainsi que de quelques autres logiciels (Java, Adobe Reader ou encore OpenOffice). Étant donné qu'il existe des millions de logiciels différents, vous vous doutez sans doute qu'on ne traitera pas le cas pour chaque logiciels.

VII.1) Mise à jour de Windows

Windows propose régulièrement d'installer des mises à jour (en fait je devrais dire impose car il les installera de toute façon à l'extinction du PC). Windows propose aussi d'autres mises à jour comme les service pack. Par exemple, le service pack 3 de Windows XP est disponible, mais il faut en faire la demande auprès de Windows Update, celui-ci ne le téléchargera pas automatiquement pour vous.

Voici la procédure pour forcer les mises à jour de Windows.

Nous verrons aussi comment activer les mises à jour automatiques.

VII.1.a) Windows XP et antérieurs

Sous Windows XP, trois cas peuvent se présenter à vous lors de l'installation des mises à jour par Windows Update lorsque vous les demandez vous-même.

- Vous aviez le service pack 2 et il vous sera proposé d'installer le service pack 3.
- Vous n'aviez pas le composant Windows Genuine Advantage Validation Tool
- Aucun des deux cas ci-dessus, les mises à jour s'installeront sans poser ces deux questions.

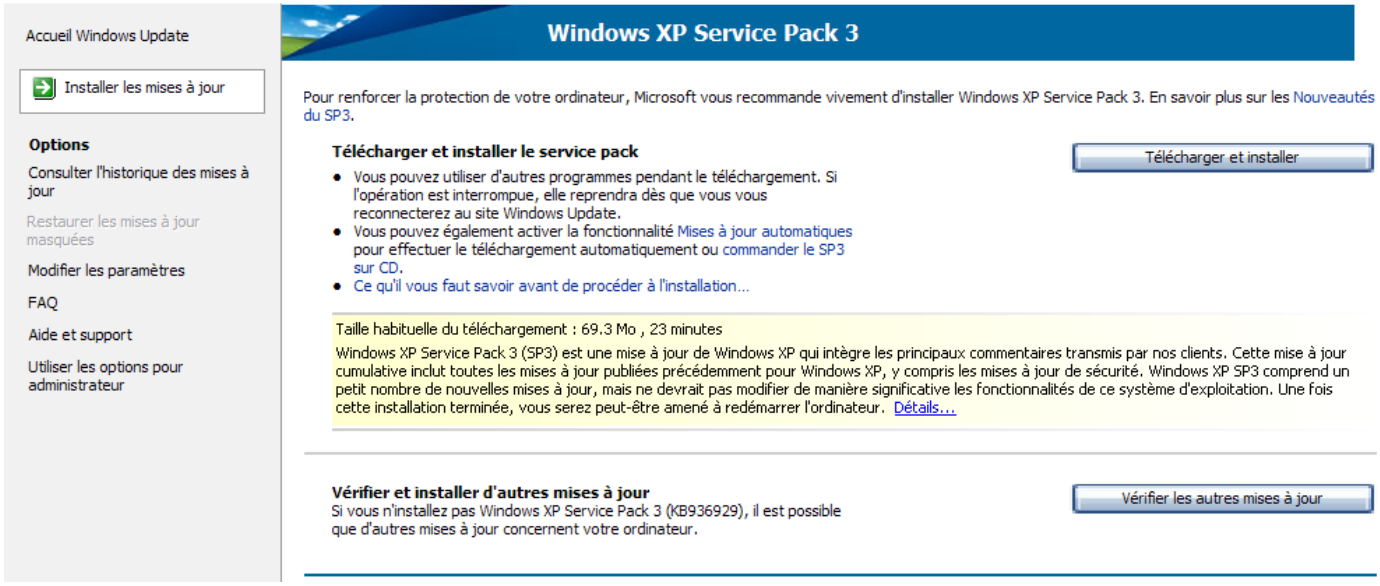
Nous verrons donc les trois cas.

Tout d'abord, il faut ouvrir Windows Update. Pour ceci, allez dans le menu Démarrer, puis allez dans « Tout les programmes », et allez ensuite dans « Windows Update ».

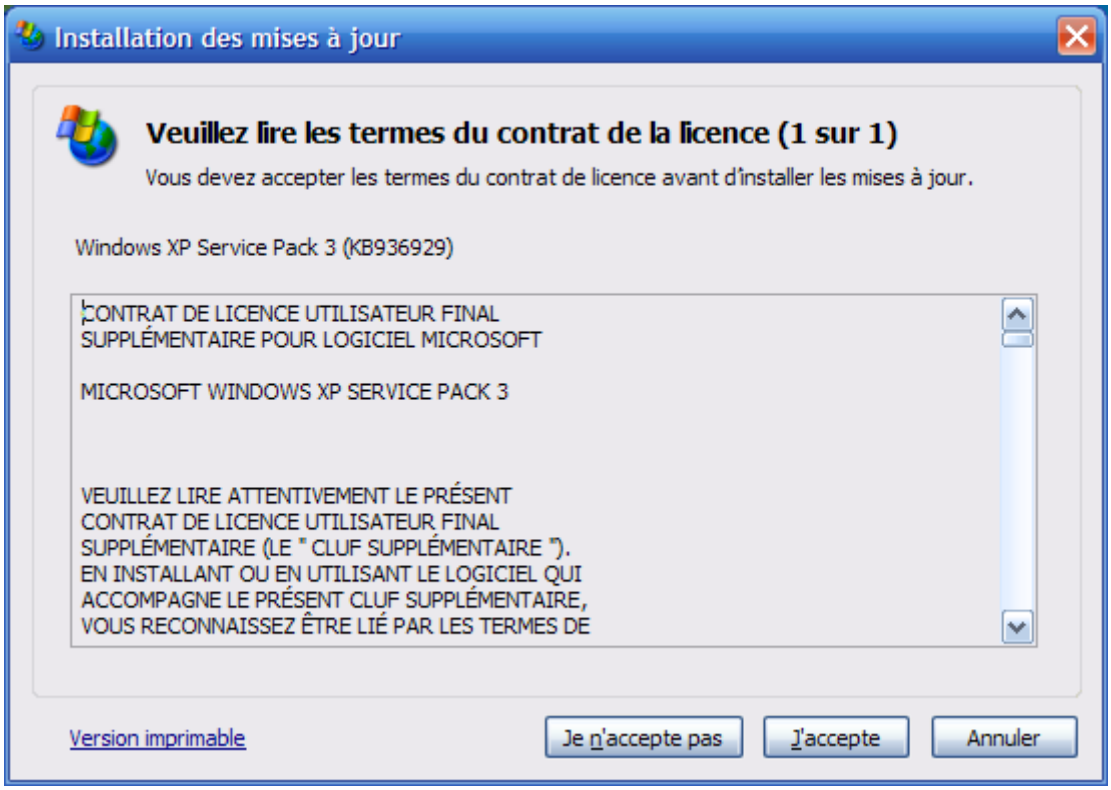
Cliquez ensuite sur le bouton « Personnalisée ».

VII.1.a.i) <u>Installation du SP3 de Windows XP</u>

Si vous n'avez pas encore le service pack 3 de Windows XP, il se peut que la fenêtre de Windows Update ressemble donc à ceci :

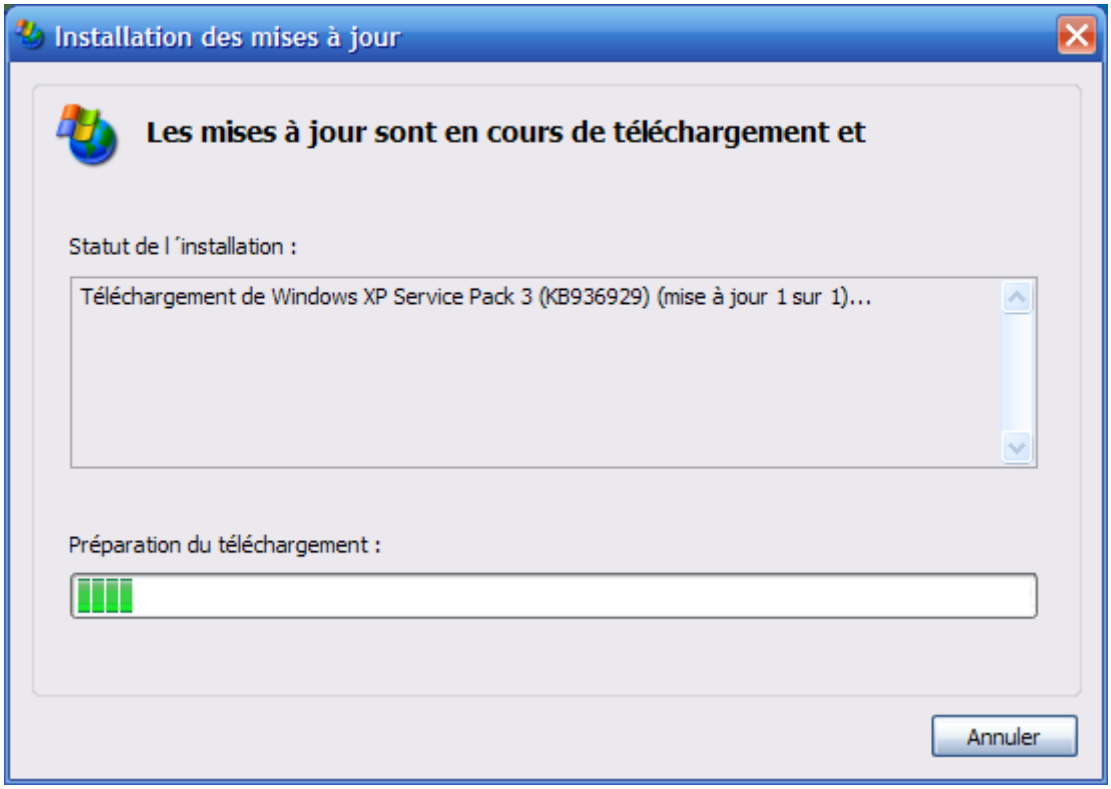


Cliquez donc sur le bouton « Télécharger et installer ».

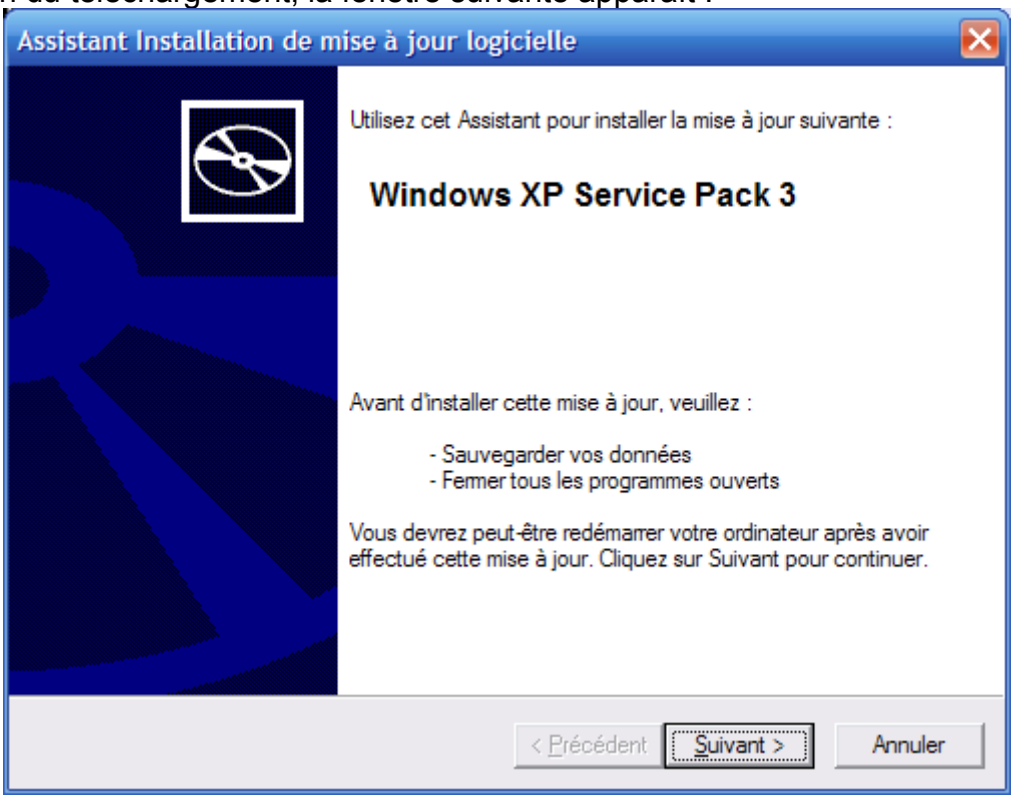


Cliquez sur le bouton « J'accepte ».

Pendant le téléchargement du service pack et l'installation, patientez.

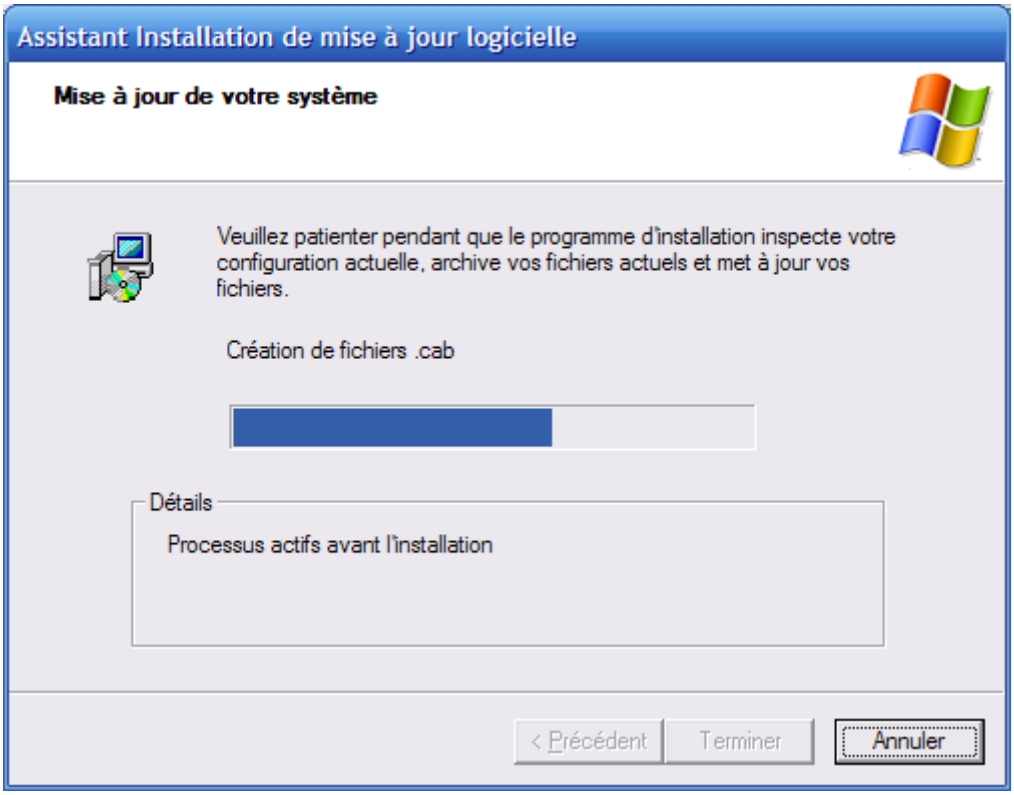


A la fin du téléchargement, la fenêtre suivante apparaît :

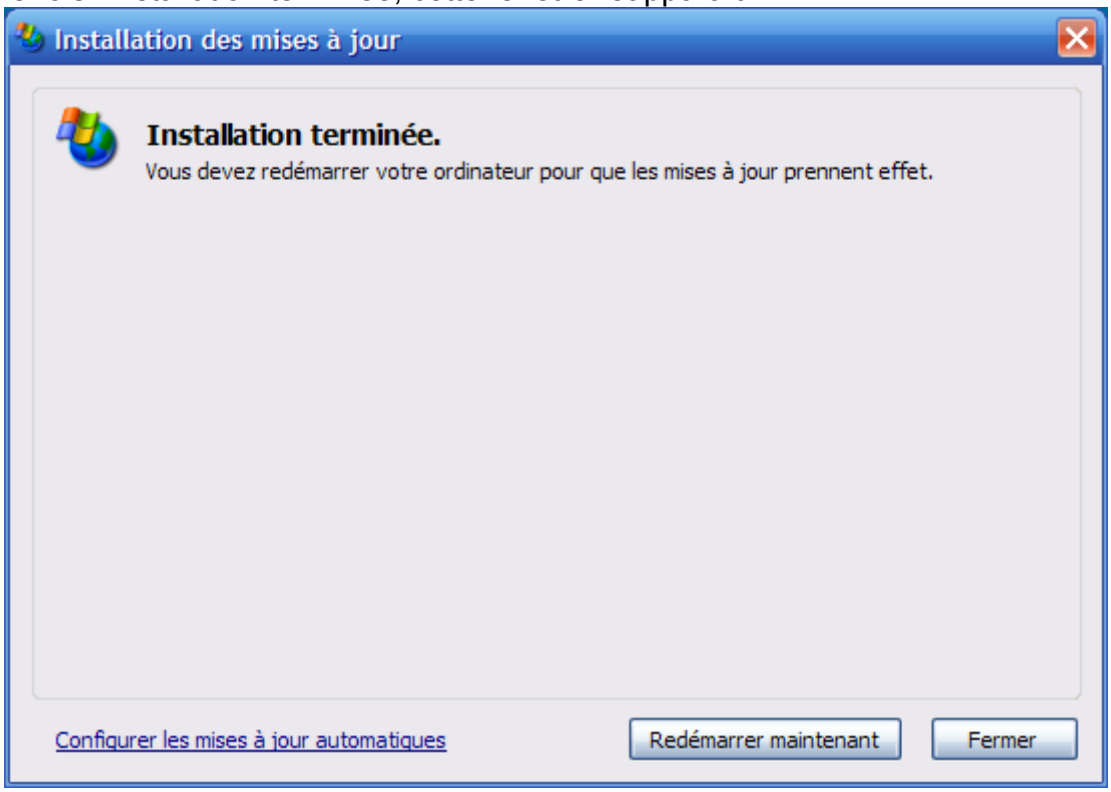


Cliquez sur le bouton « Suivant ».

Pendant que la fenêtre ressemble à ceci, patientez :



Une fois l'installation terminée, cette fenêtre réapparaît :



Cliquez sur le bouton « Redémarrer maintenant ».

Voilà, le service pack 3 de Windows XP est installé !

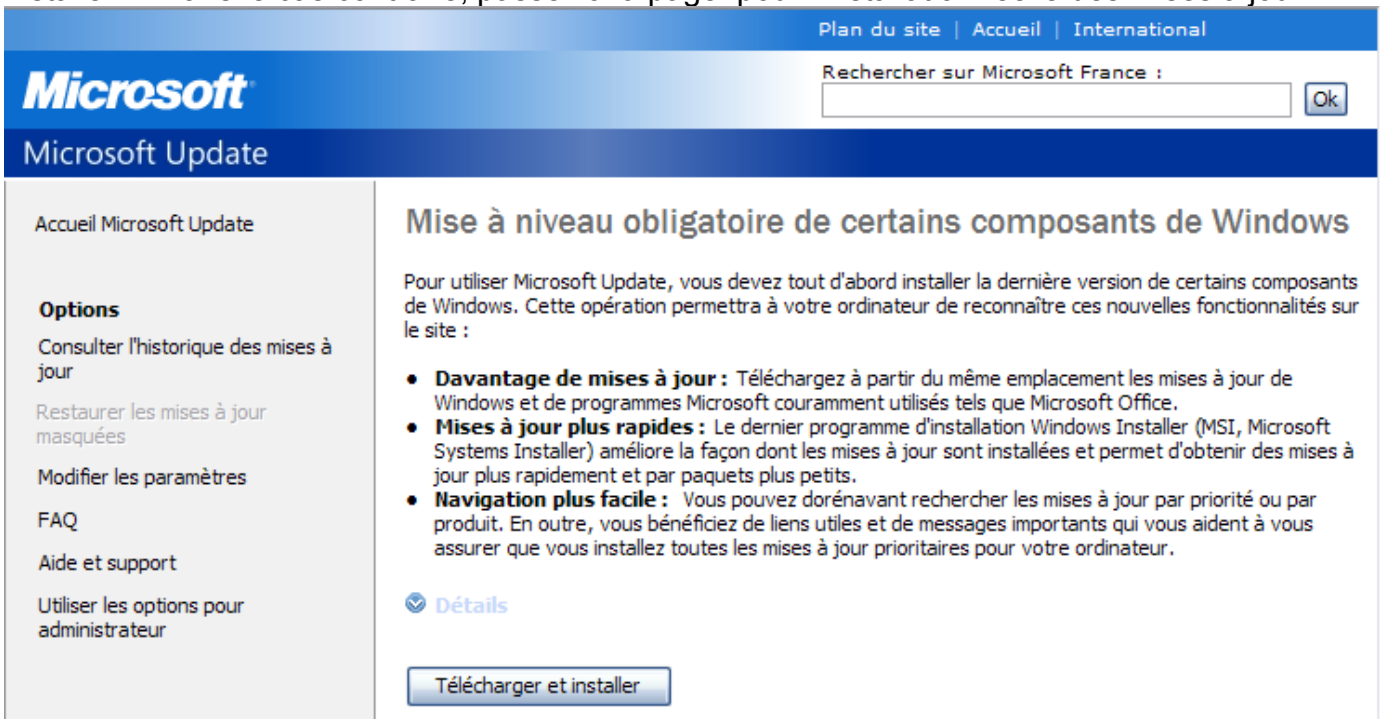
Au redémarrage, recommencez la procédure de Windows Update pour télécharger les mises à jour parues après le service pack 3.

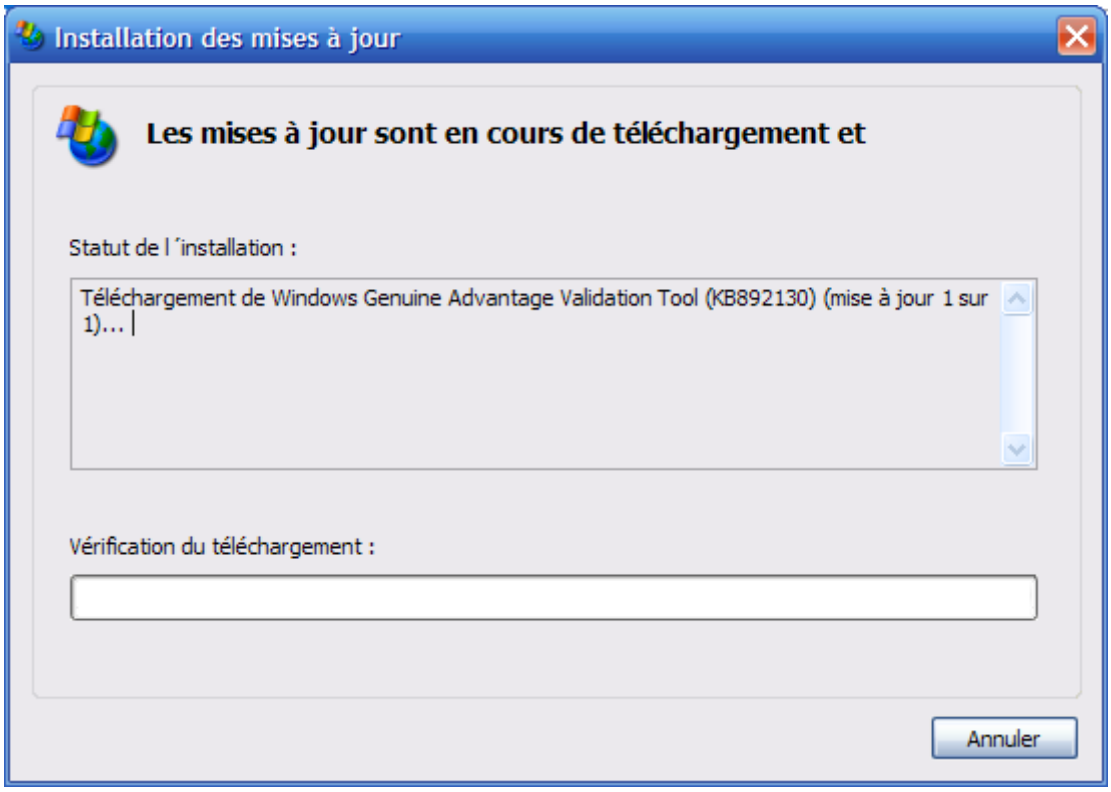
VII.1.a.ii) Installation de « Windows Genuine Advantage Validation Tool »

Cet outil est en fait destiné à vérifier que votre Windows est bien légal. Si votre Windows est illégal et que vous le savez parfaitement, ne faites pas les mises à jour de Windows car

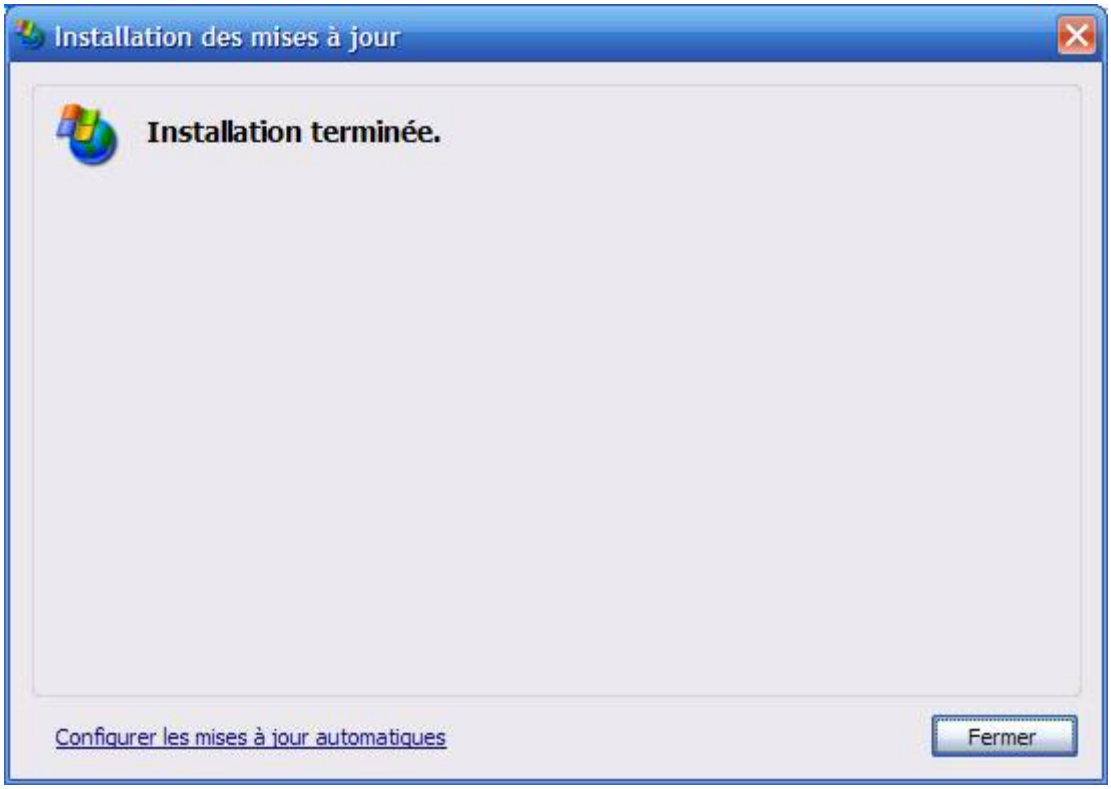
celui-ci risque de devenir très ennuyeux.

Il se peut que Windows Update vous demande d'installer ce composant. Dans ce cas, la fenêtre ressemblera à l'image suivante. Si c'est le cas, cliquez sur le bouton « Télécharger et installer ». Dans le cas contraire, passez à la page pour l'installation réelle des mises à jour.





Lorsque cette fenêtre apparaît, patientez.



Cliquez sur le bouton « Fermer ».

VII.1.a.iii) Installation des mises à jour

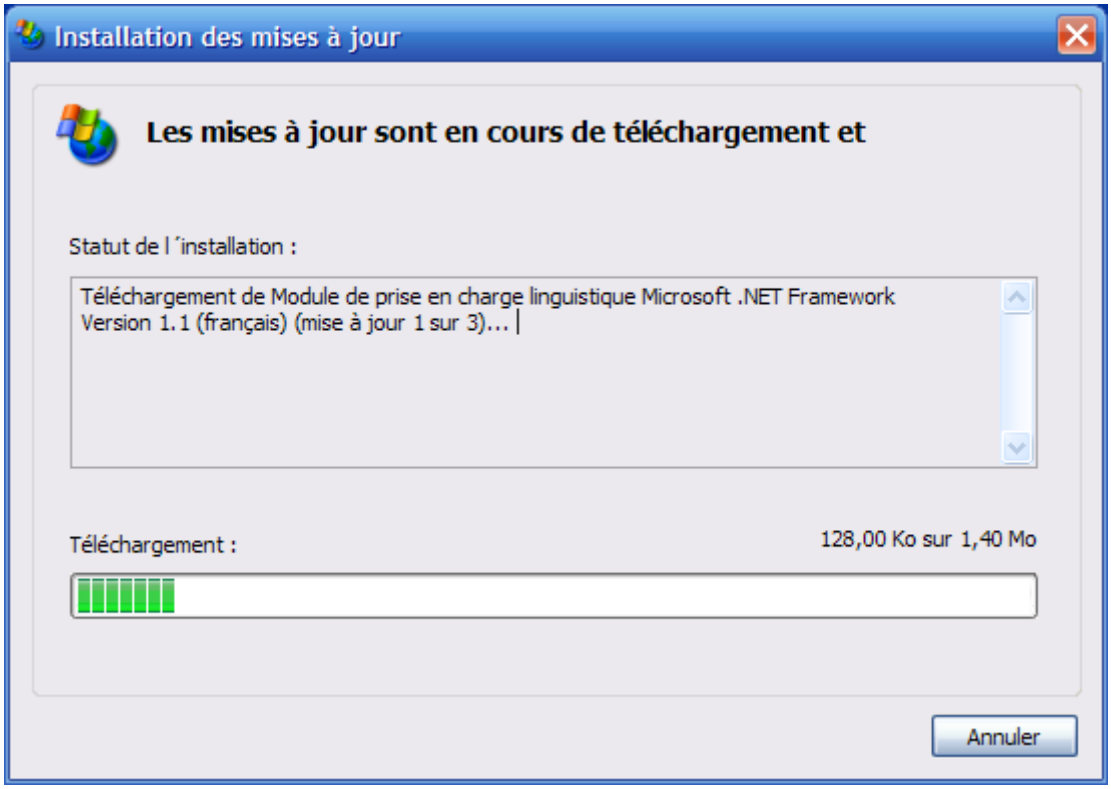
Cliquez sur « Prioritaires » dans la partie gauche de la page, et vérifiez que toutes les cases en face de chaque mise à jour soit bien cochées (voir cadre rouge de l'image ci-dessous) :

Même chose en cliquant sur « Logicielles, facultatives » (toujours à gauche de la page).

Vous pouvez aussi le faire pour « Matérielles, facultatives » mais c'est moins utile.

Une fois ceci fait, cliquez sur le bouton « Installer les mises à jour » (voir cadre bleu de l'image précédente).

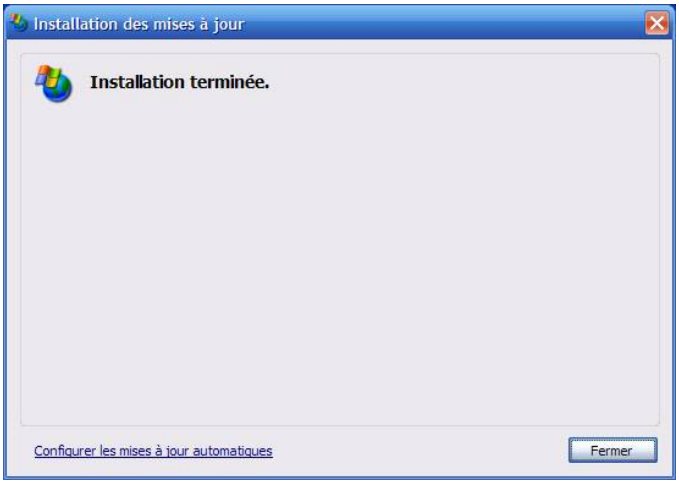
Cliquez ensuite sur le bouton « Installer les mises à jour » (voir cadre vert de l'image ci-dessous) :

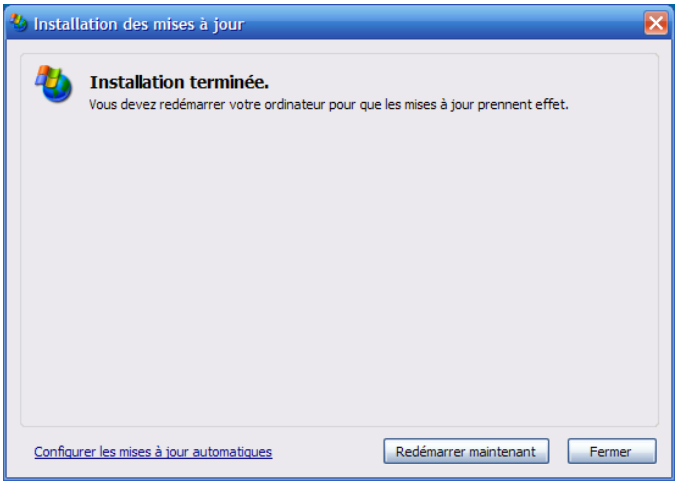


Lorsque cette fenêtre apparaîtra, patientez jusqu'à la fin de l'installation des mises à jour.

Une fois l'installation terminée, vous aurez au choix la fenêtre suivante, ou alors une fenêtre vous proposant de redémarrer le PC afin de terminer l'installation des mises à jour.

Si vous avez la fenêtre de gauche, cliquez sur le bouton « Fermer ». Si vous avez la fenêtre de droite, celle de redémarrage, sauvegardez votre travail en cours (documents OpenOfice ouverts, ...) et cliquez sur le bouton pour redémarrer.





Si vous choisissez de ne pas redémarrer, vous aurez un message d'avertissement vous demandant de redémarrer. Si l'ordinateur détecte que vous n'êtes pas devant le PC (il regarde ça en comptant le temps depuis lequel vous n'avez pas bougé la souris), le message d'avertissement se transformera en compte à rebours de cinq minutes, temps au bout duquel votre ordinateur redémarrera quand même (prenez soin donc de sauvegarder régulièrement votre travail en cours si vous voyez l'avertissement au cas ou vous absenteriez plus de cinq minutes).

Bref, si vous avez un avertissement comme quoi l'ordinateur veut redémarrer, je vous conseille de faire le redémarrage.

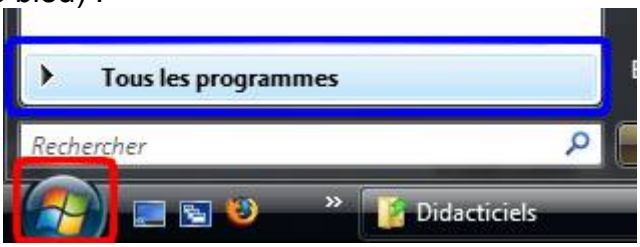
VII.1.b) Windows Vista et ultérieurs

VII.1.b.i) Via Windows Update

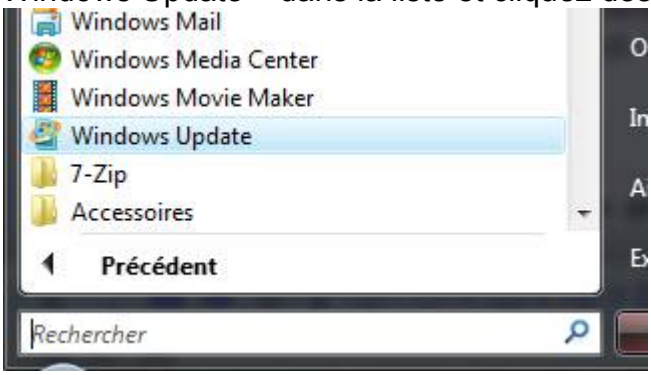
A l'heure ou j'écris ces quelques lignes, il n'existe pas encore de successeur terminé de Windows Vista, il se peut donc que la procédure soit différente sous le futur successeur.

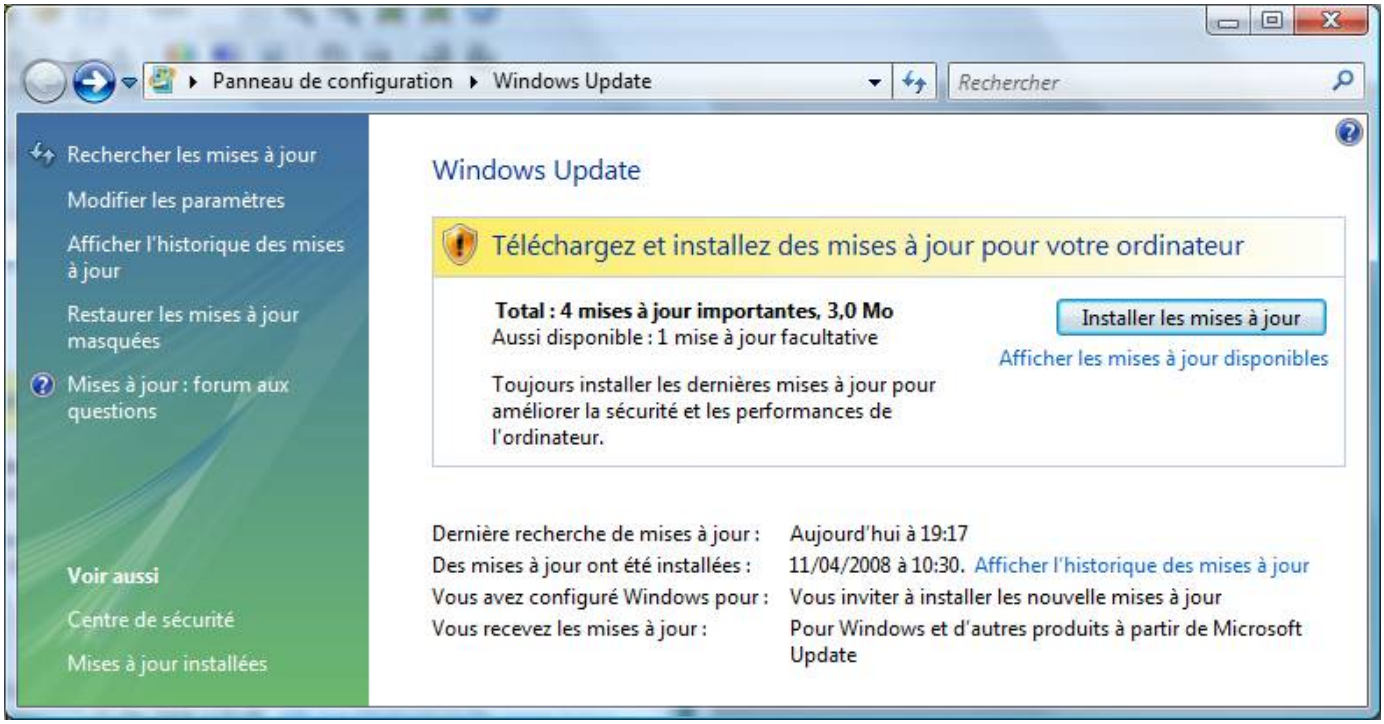
Commençons déjà par accéder à Windows Update.

Cliquez sur le bouton Démarrer (voir cadre rouge) puis cliquez sur « Tout les programmes » (voir cadre bleu) :

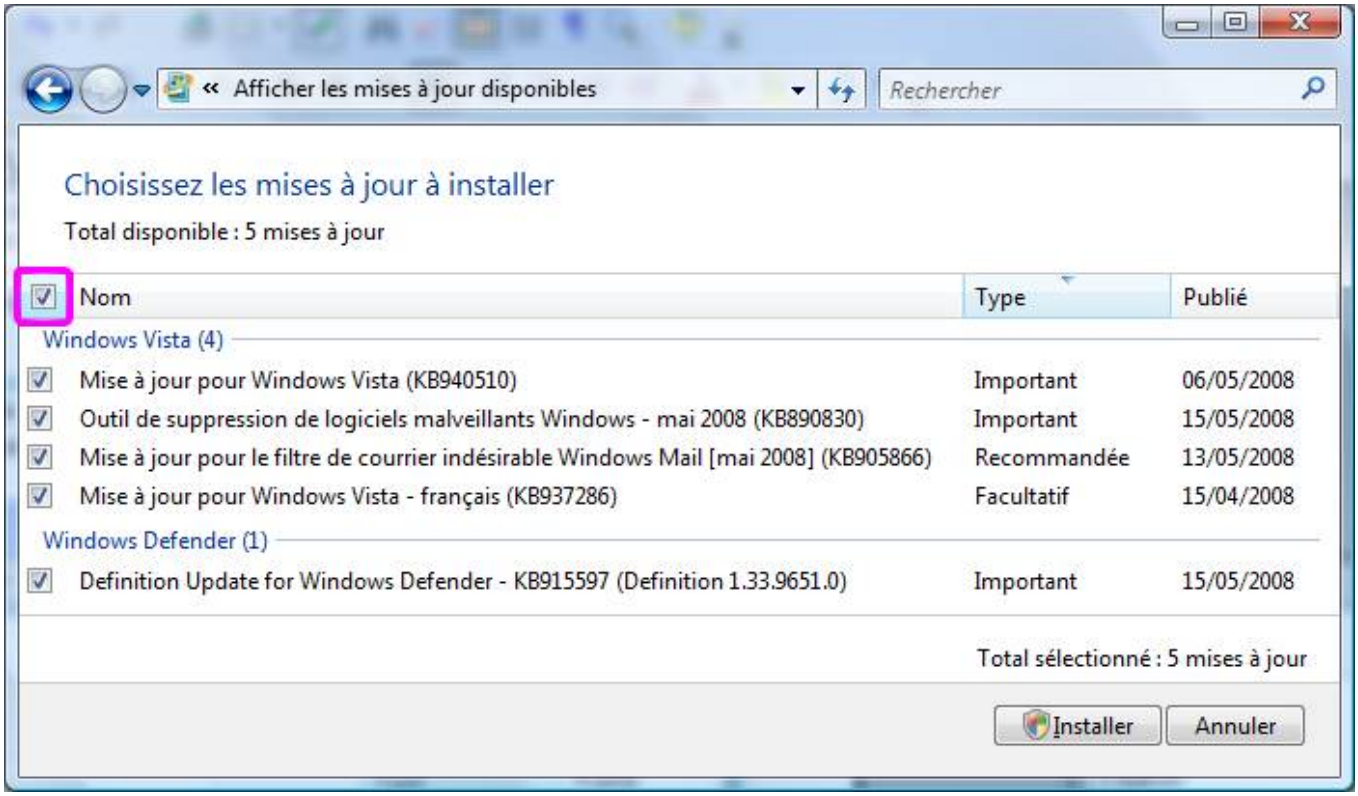


Trouvez ensuite « Windows Update » dans la liste et cliquez dessus :



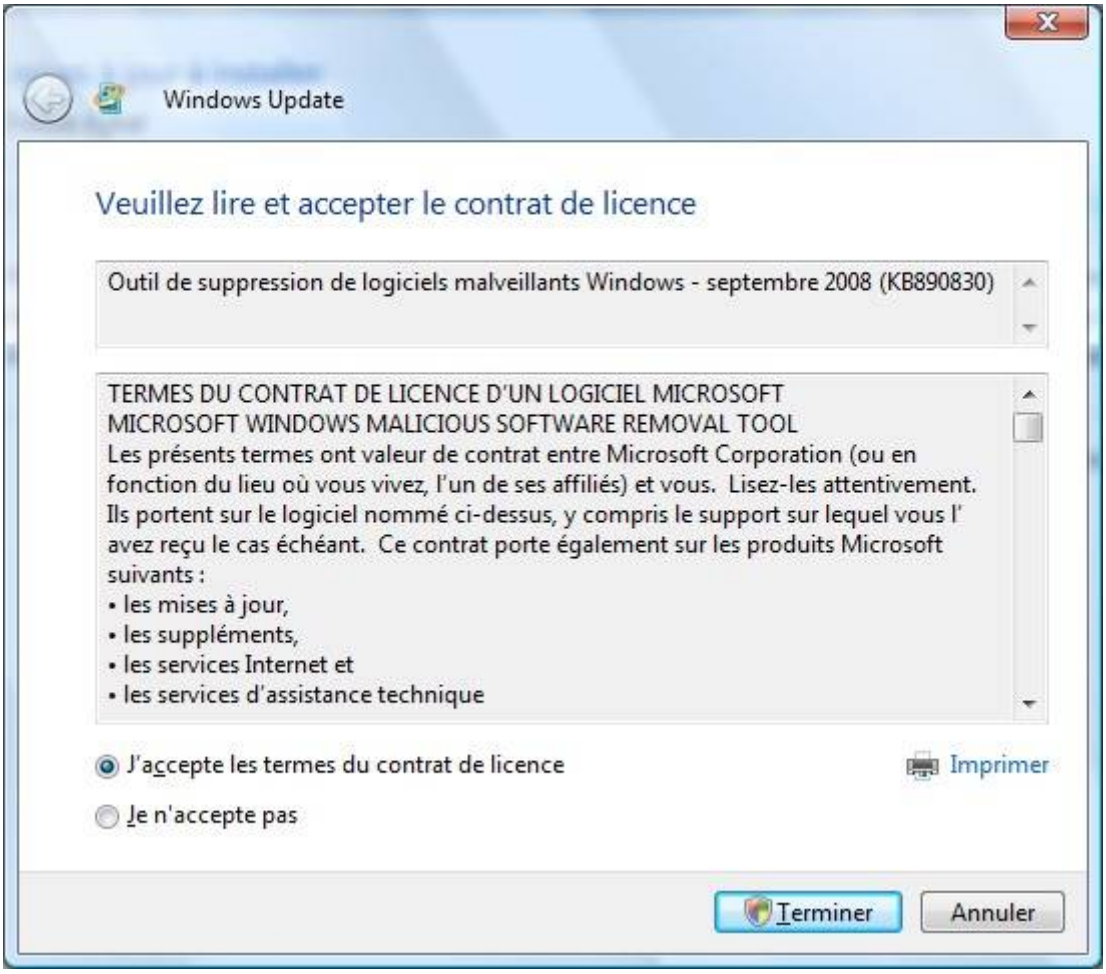


Si Windows Vista vous propose tout de suite des mises à jour, cliquez sur le lien « Afficher les mises à jour disponibles ».

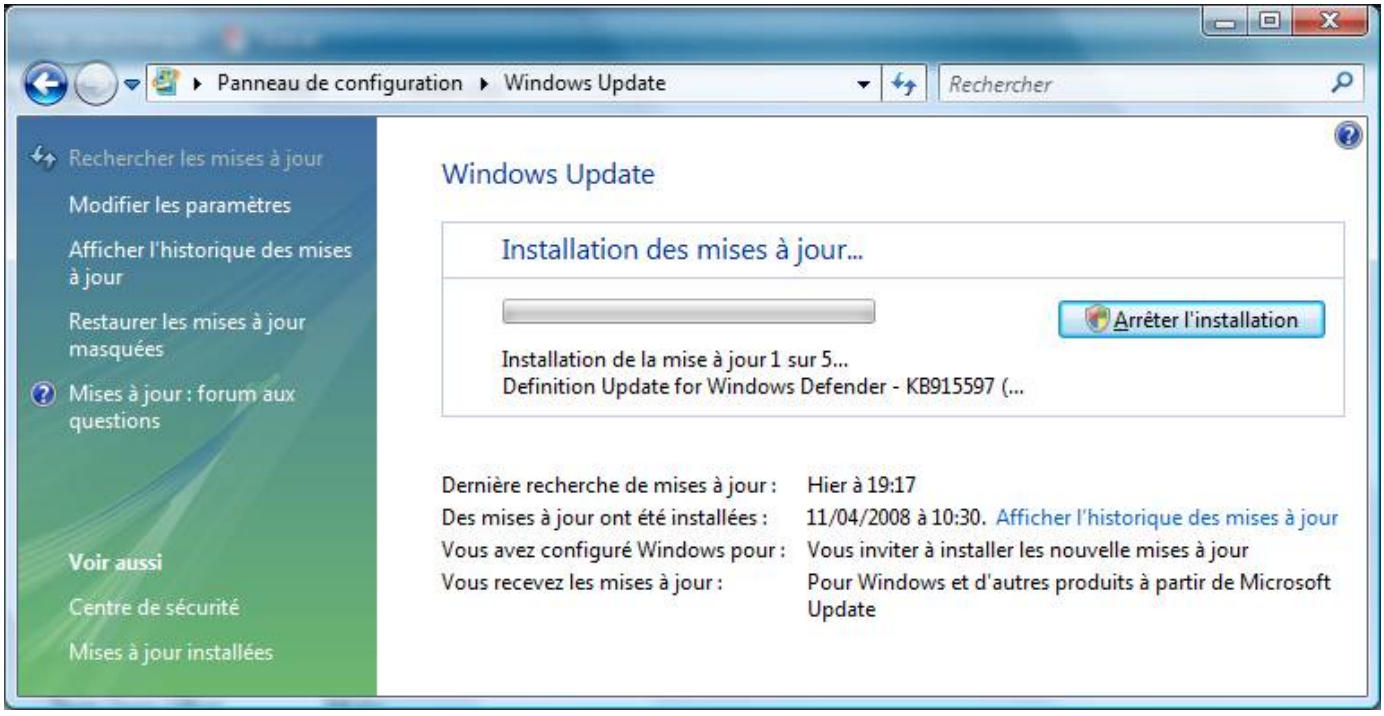


Cochez ensuite la case juste à côté de « Nom » (voir cadre violet de l'image ci-dessus) afin que toutes les cases soient cochées. Cliquez ensuite sur le bouton « Installer ».

Une confirmation vous sera demandé. Cliquez sur Continuer.



Il faudra peut-être aussi valider l'accord de licence pour l'outil de suppression des logiciels malveillants en cochant la case « J'accepte les termes du contrat de licence », puis en cliquant sur « Terminer ».

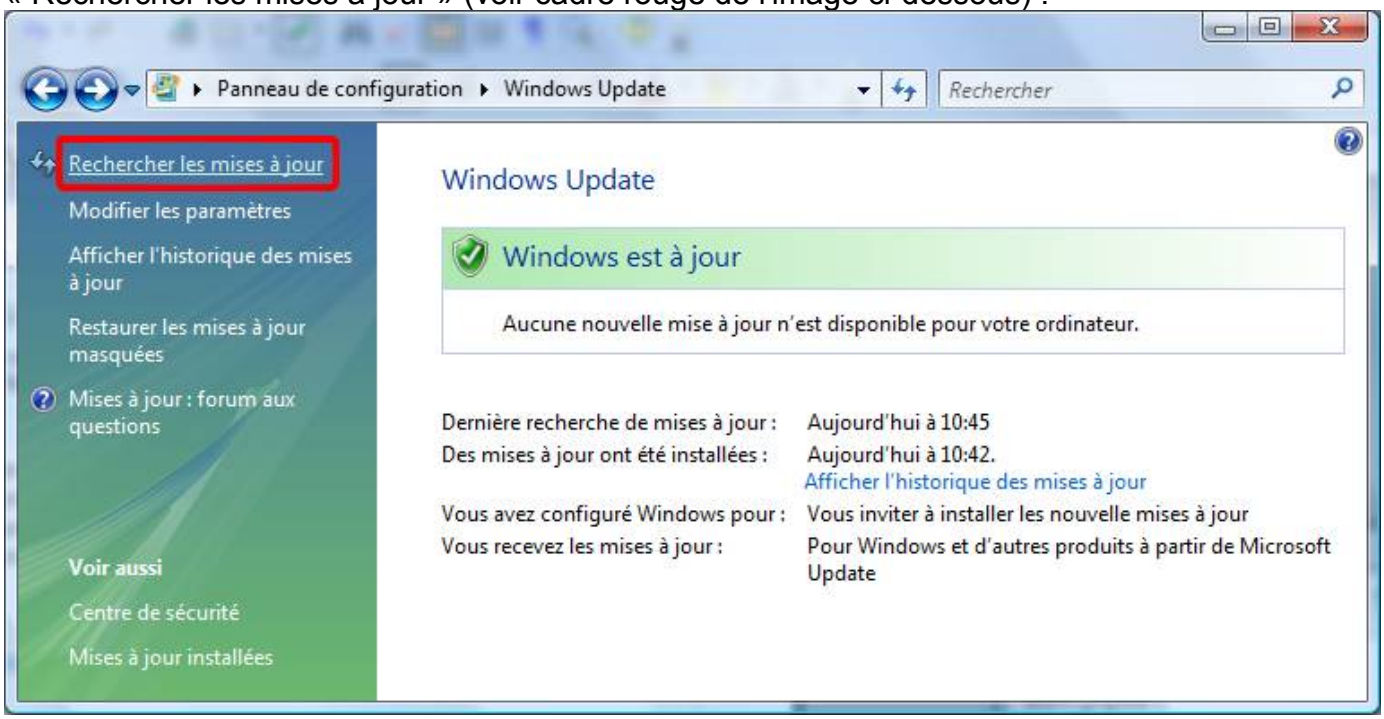


L'installation débutera.

Il est possible qu'il vous soit demandé de redémarrer votre ordinateur. Dans ce cas, enregistrez votre travail en cours et redémarrez votre ordinateur.

Une fois redémarré, recommencez la mise à jour de Windows via Windows Update. Car Windows Update ne vous proposera pas tout de suite d'un seul coup toutes les mises à jour. C'est à vous de lui demander.

Pour chercher s'il y a de nouvelles mises à jour, il suffit de cliquer sur le lien « Rechercher les mises à jour » (voir cadre rouge de l'image ci-dessous) :



Si des mises à jour sont proposées, suivre de nouveau les instructions précédentes.

Le service pack 1 de Windows Vista vous sera proposé à la fin d'un long cycle de mises à jour / redémarrages. S'il vous est proposé, vérifiez bien que vous n'aurez pas besoin dans l'heure de votre ordinateur car celui-ci peut mettre entre une demi heure et une heure à s'installer.

VII.1.b.ii) Installation des mises à jour automatiques

VII.2) Mozilla Firefox et Mozilla Thunderbird

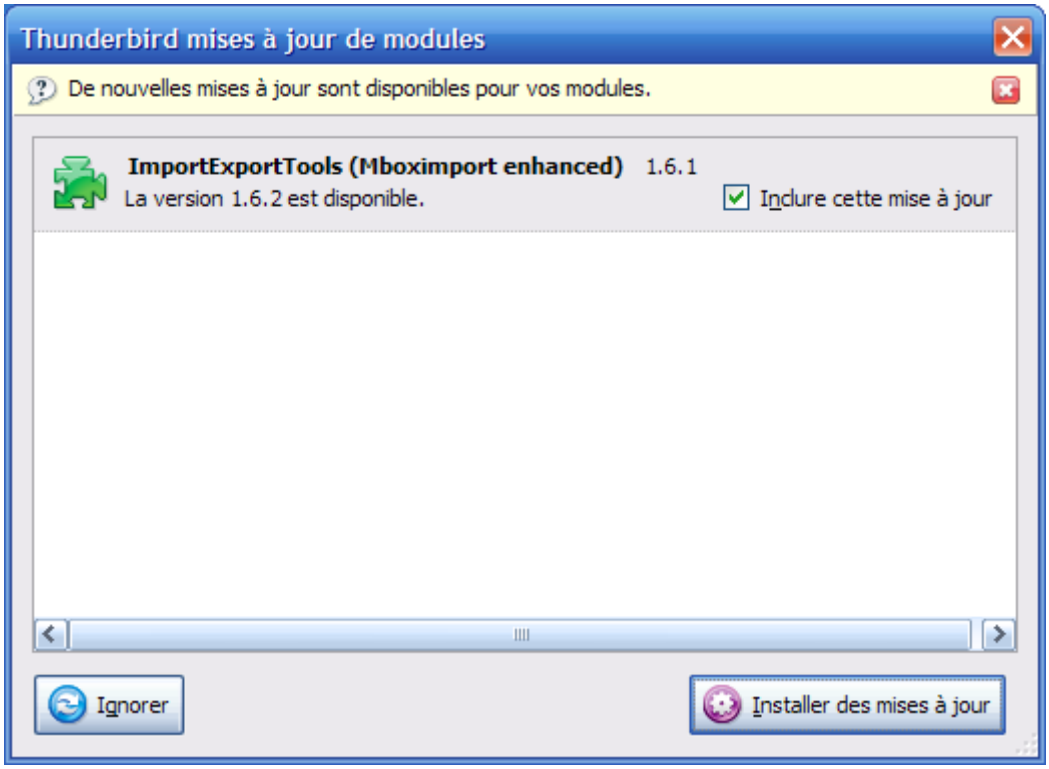
Il arrive de temps en temps deux types de mises à jour pour ces deux logiciels. Sachant qu'ils sont construits à peu près de la même manière, je ferai des explications communes à ces deux logiciels (et en même temps, ça fera moins de pages à imprimer pour les gens qui voudraient imprimer tout ceci).

Il y a :

- les mises à jour des extensions
- les mises à jour du programme

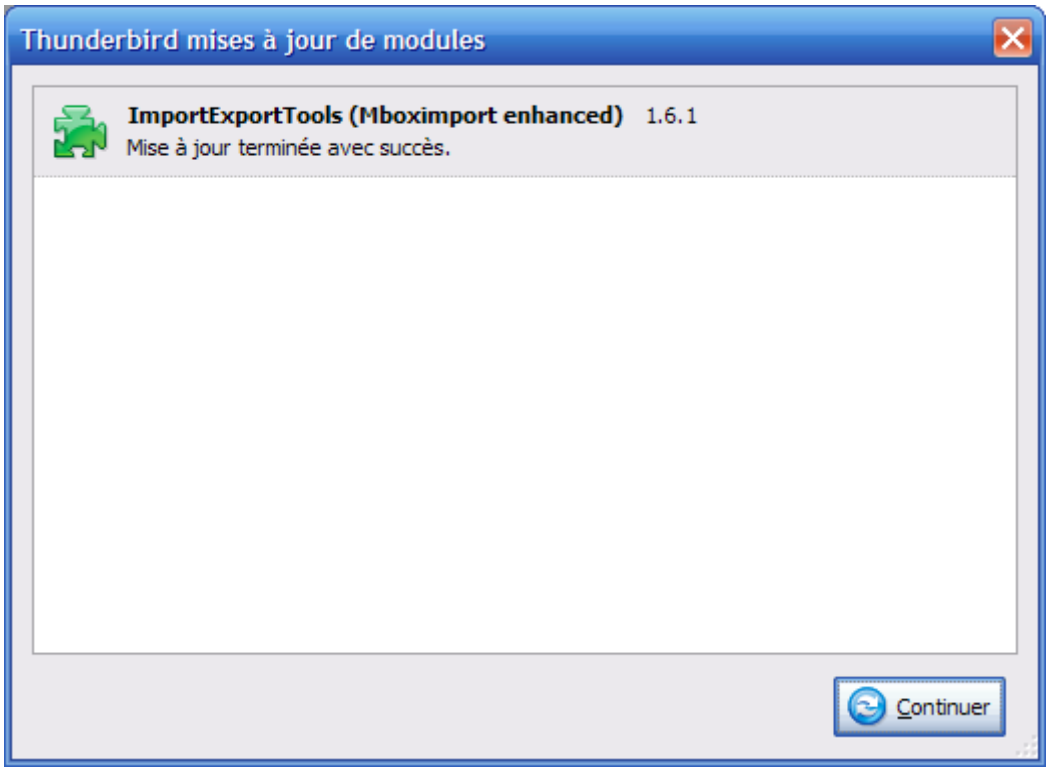
VII.2.a) La mise à jour des extensions

Au démarrage de Thunderbird et de Firefox, il arrive régulièrement qu'une fenêtre ressemblant à ceci apparaisse. Cette fenêtre vous permettra de mettre à jour les différentes extensions qui sont installées dans Thunderbird/Firefox.



Dans ce cas, cliquez sur le bouton « Installer des mises à jour ».

Patientez quelques secondes le temps du téléchargement des extensions puis cliquez sur le bouton « Continuer » :

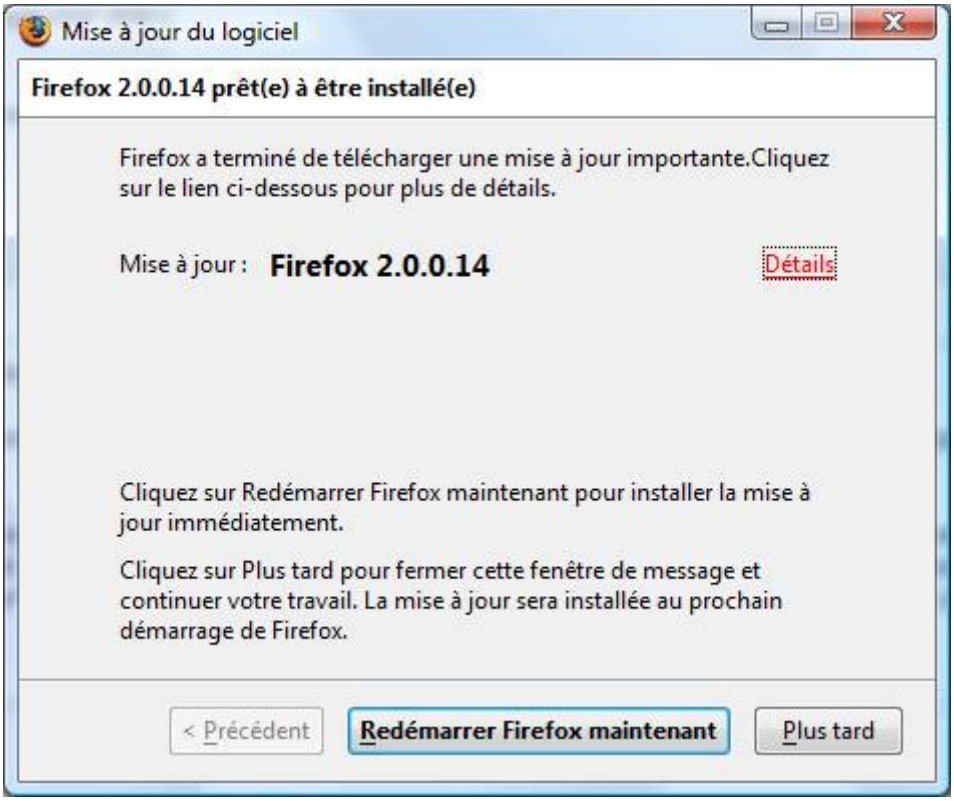


Voilà, vos extensions sont mises à jour.

VII.2.b) La mise à jour du programme

La mise à jour du programme peut arriver à n'importe quel moment lors de l'utilisation d'un de ces deux logiciels (le plus souvent au mauvais moment quand vous faites votre Prizee quotidien en plein milieu d'une partie qui aurait pu vous faire gagner le gros lot).

La fenêtre de mise à jour ressemble à ceci :



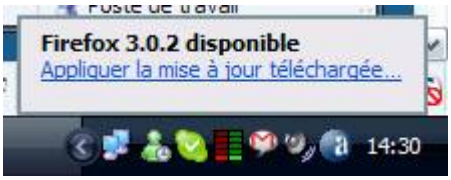
Dans ce cas, cliquez sur le bouton « Redémarrer Firefox maintenant » (ou Redémarrer Thunderbird maintenant).

Si Firefox vous demande de fermer des onglets, ou Thunderbird d'enregistrer votre brouillon en cours de rédaction, acceptez.

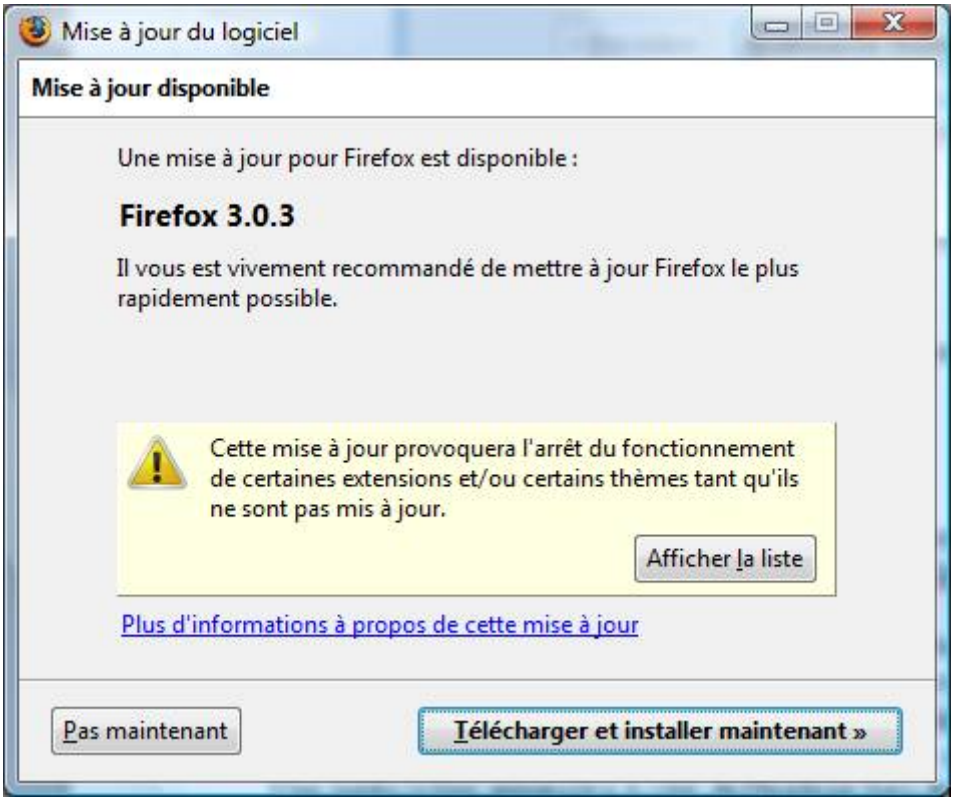
Si tout se passe bien, Firefox/Thunderbird redémarrera tout seul.

VII.2.b.i) Firefox 3

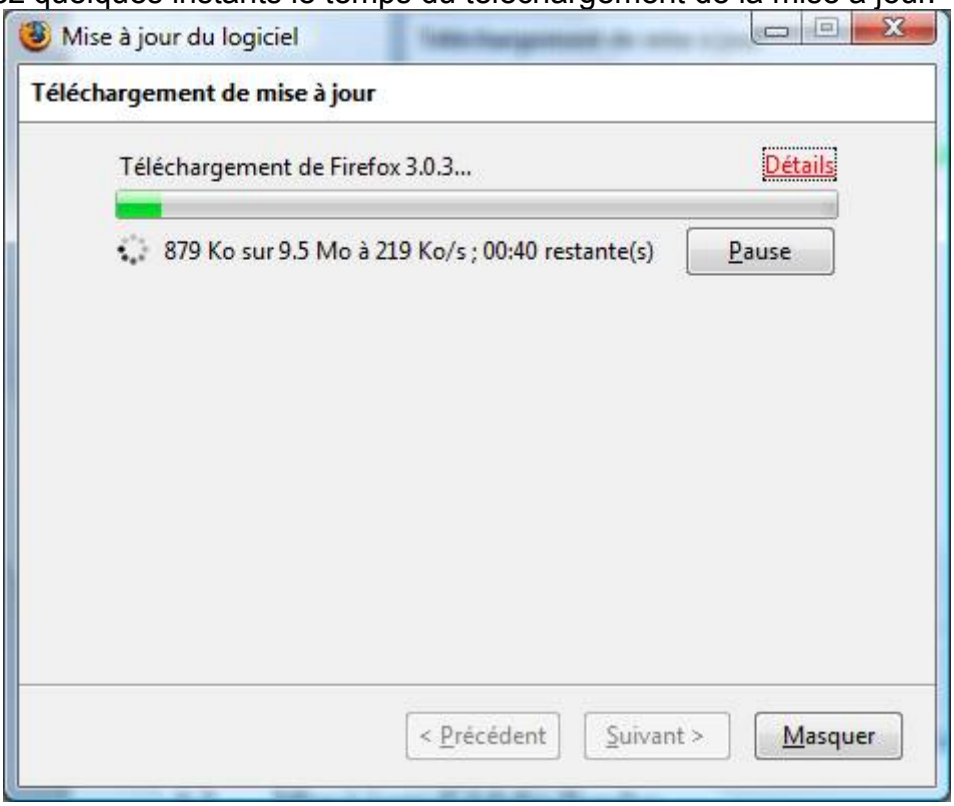
Ce petit message prévient qu'il existe une mise à jour de Firefox. Cliquez sur « Appliquer la mise à jour téléchargée ».



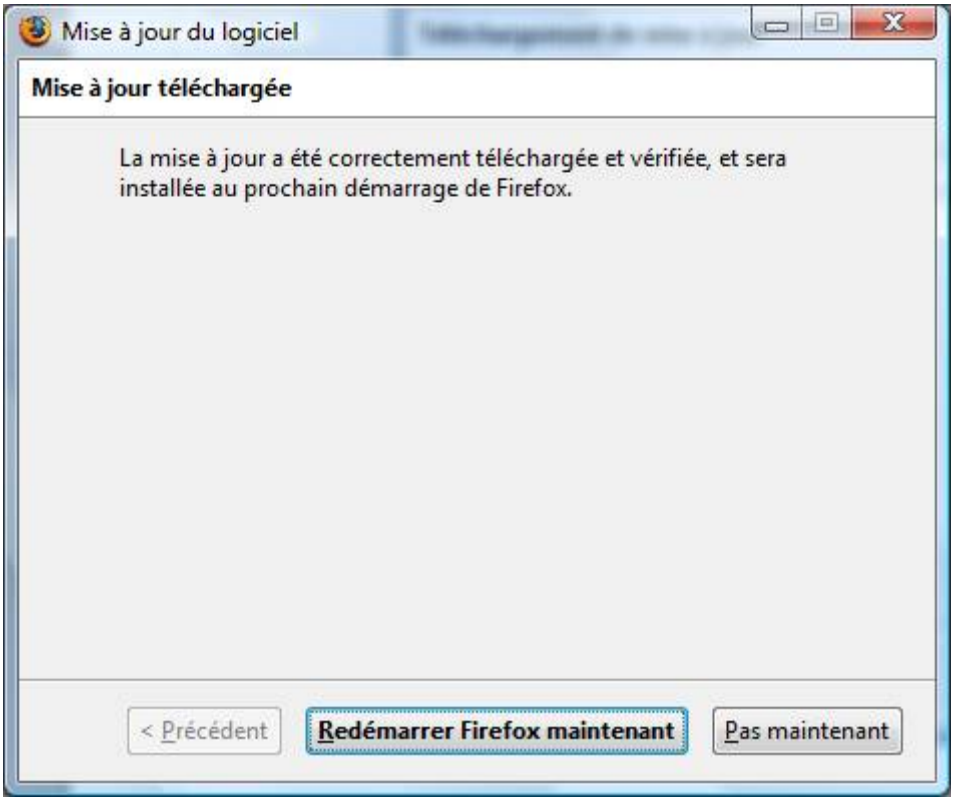
Cliquez sur « Télécharger et installer maintenant ».



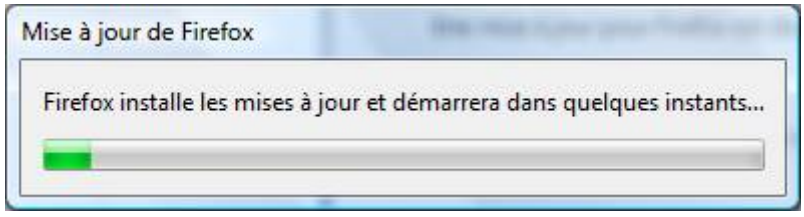
Patientez quelques instants le temps du téléchargement de la mise à jour.



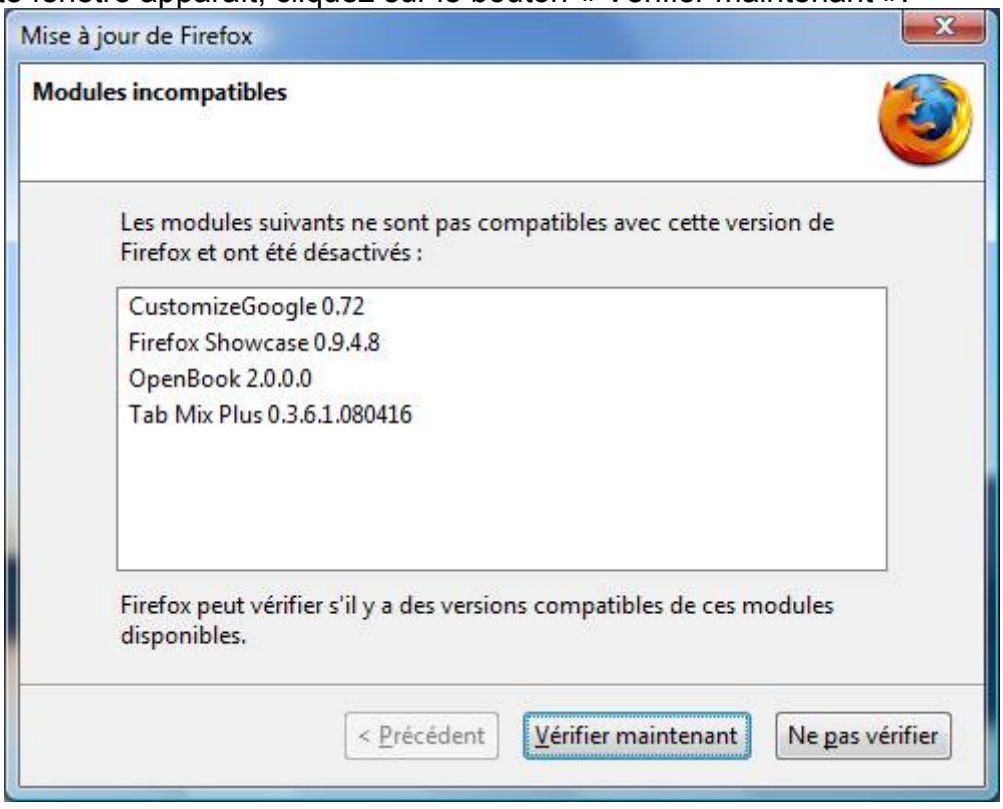
Dès que la mise à jour sera téléchargée, la fenêtre ci-dessous apparaitra. Cliquez sur le bouton « Redémarrer Firefox maintenant ».



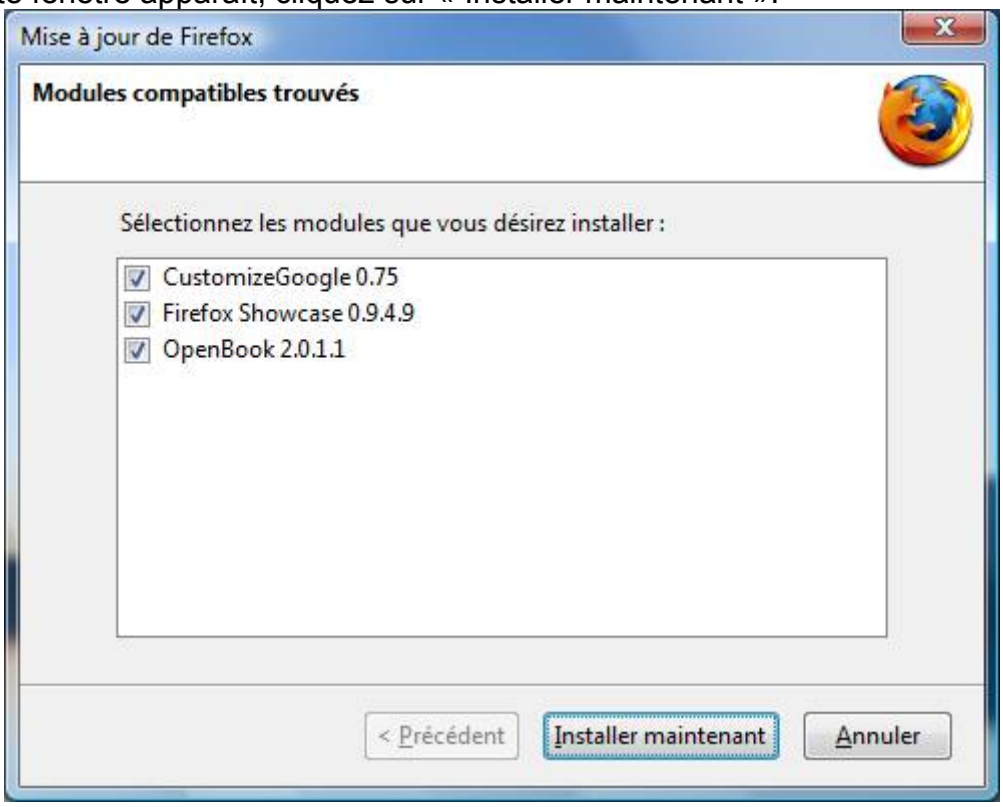
Au redémarrage de Firefox, la fenêtre ci-dessous apparaîtra. Patientez quelques instants.



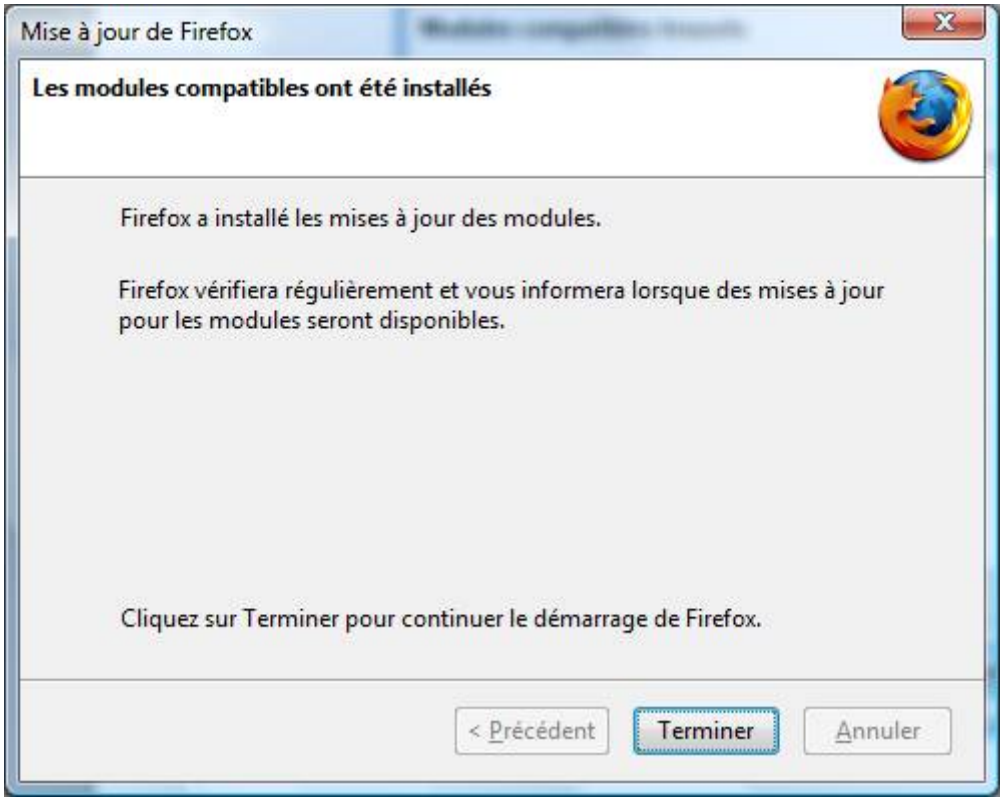
Si cette fenêtre apparaît, cliquez sur le bouton « Vérifier maintenant ».



Si cette fenêtre apparaît, cliquez sur « Installer maintenant ».



Cliquez ensuite sur le bouton « Terminer ».



VII.3) Mise à jour d'Adobe Reader

Sous Windows Vista, il se peut que régulièrement, une fenêtre du « Contrôle des comptes utilisateurs » apparaisse en vous demandant si « Adobe Update Manager » peut continuer son exécution. Dans ce cas, cliquez sur le bouton « Continuer ».

Ce programme permet en fait de mettre à jour Adobe Reader qui est très certainement installé dans votre ordinateur (c'est le logiciel qui vous permet de lire ces quelques pages sur votre ordinateur, ce logiciel s'incruste dans Firefox afin de permettre la lecture des fichiers PDF

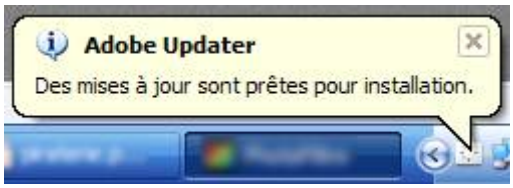
directement dans Firefox).

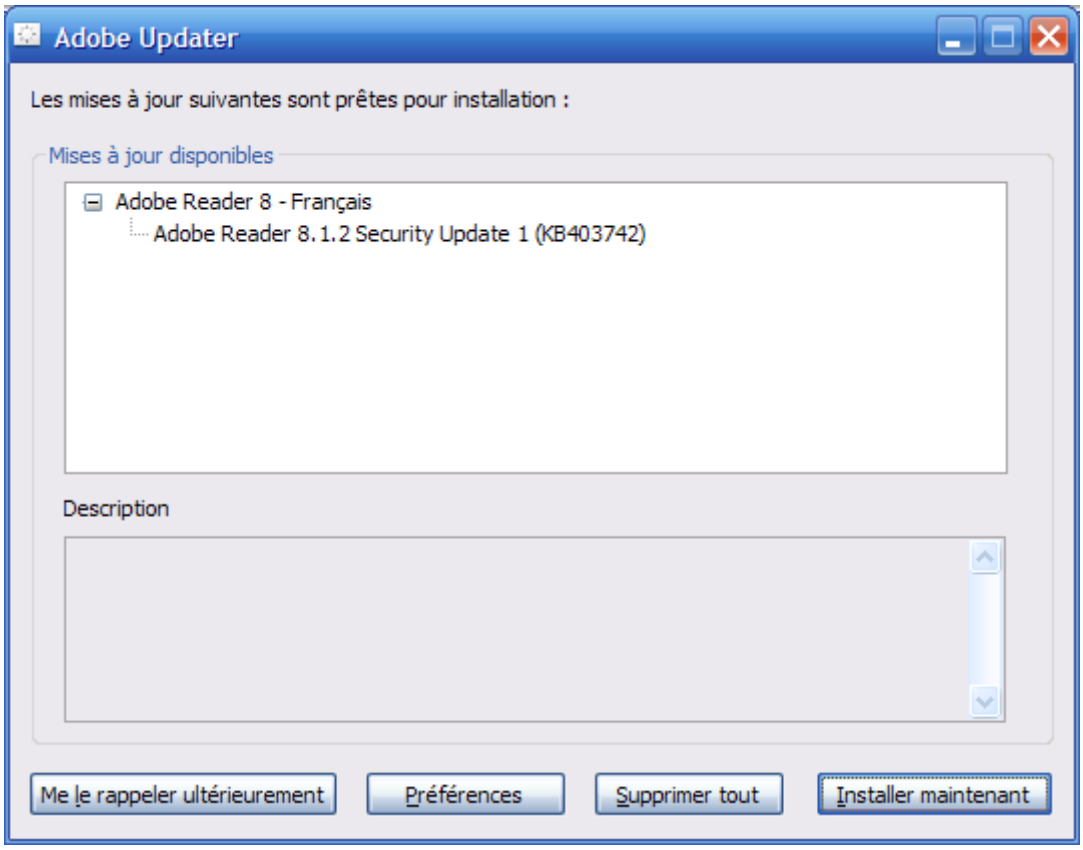
Il vous faudra donc mettre à jour ce logiciel si votre ordinateur en fait la demande.

Une petite icône apparaitra à côté de l'horloge lors du téléchargement des mises à jour :

Dès que le téléchargement est terminé, votre ordinateur vous préviendra en affichant une petite bulle au dessus de l'icône précédente.

Double cliquez sur cette icône :





Cliquez sur le bouton « Installer maintenant ».

L'installation de la mise à jour se fera silencieusement (sans poser aucune question).

Dès que l'installation se termine, cette petite bulle d'aide apparaît, cliquez sur la croix en haut à droite de cette bulle pour la fermer.

Il se peut qu'Adobe Reader s'ouvre aussi. Vous pouvez fermer la fenêtre de Adobe Reader.

Il se peut que vous ayez supprimé l'icône de Adobe Reader de votre bureau lorsque vous l'avez installé la première fois (ou quelqu'un l'a fait pour vous), si c'est le cas, il est possible que

cette icône réapparaisse de nouveau. Vous pouvez donc la supprimer (en effet, l'icône sur le bureau n'a aucun intérêt car Adobe Reader s'ouvrira toujours de lui même quand vous en aurez besoin).

VII.4) Mise à jour de Messenger Plus!

De temps en temps aussi apparaît une autre fenêtre : celle de la mise à jour de Messenger Plus!

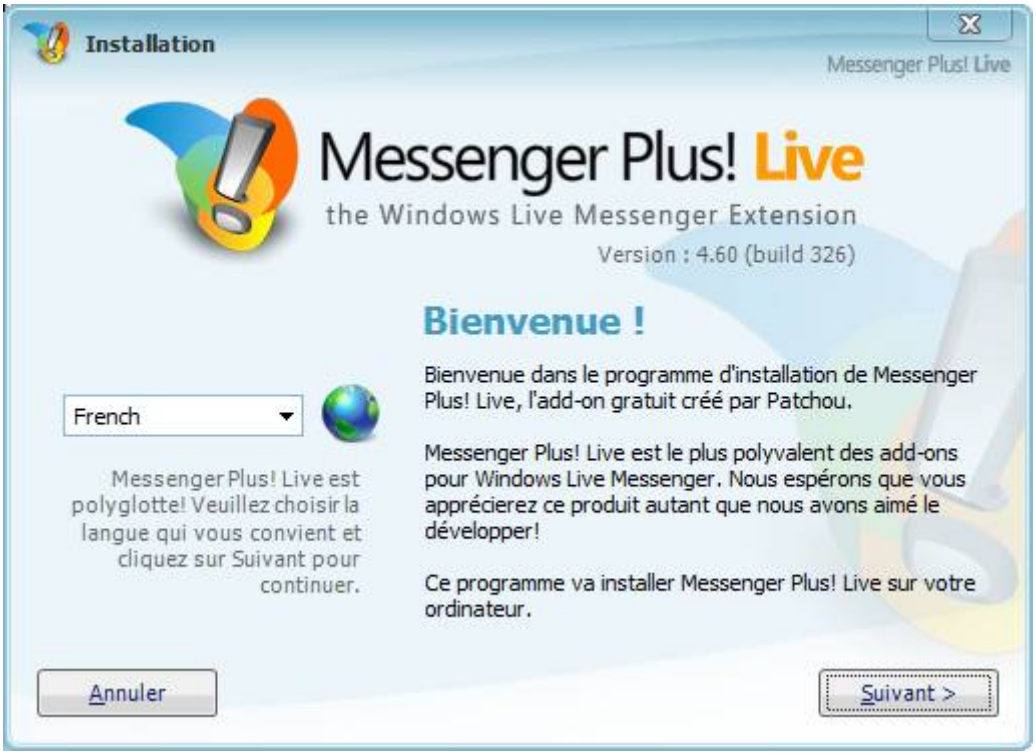
Pour rappel, ce petit programme permet d'améliorer l'utilisation de Windows Live Messenger. Cependant, ce petit programme intègre à l'installation un sponsor (qui est en fait un petit programme publicitaire qui affiche régulièrement des publicités sur l'écran de votre ordinateur).

Lorsque vous avez la fenêtre ci-dessus, cliquez sur le bouton « Télécharger & Installer ».

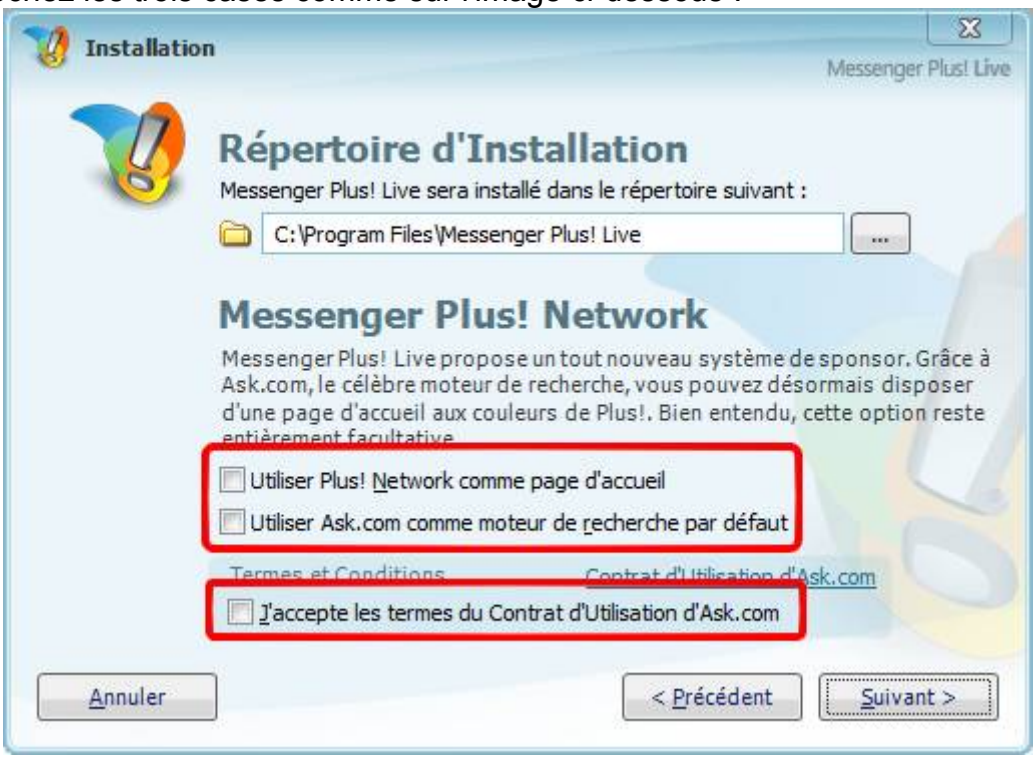
Lorsque cette fenêtre apparaît, patientez.

Si vous avez Windows Vista, une fenêtre de demande de confirmation apparaitra. Cliquez sur le bouton « Continuer ».

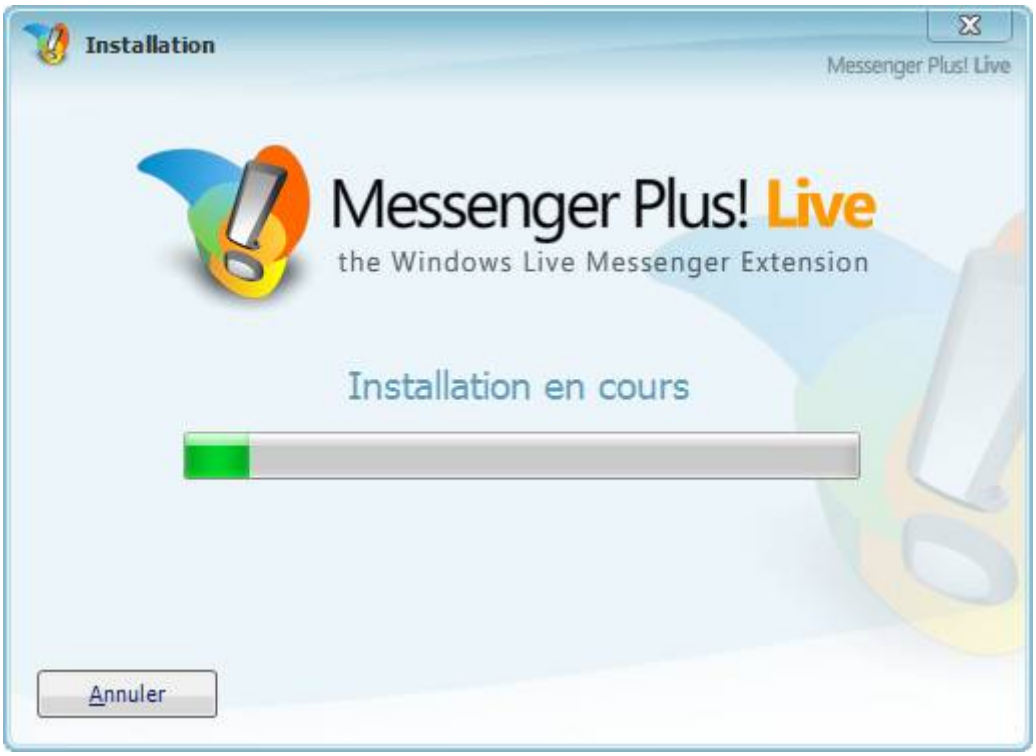
A moins que vous ne vouliez d'un Messenger Plus! en chinois, cliquez sure le bouton « Suivant » :



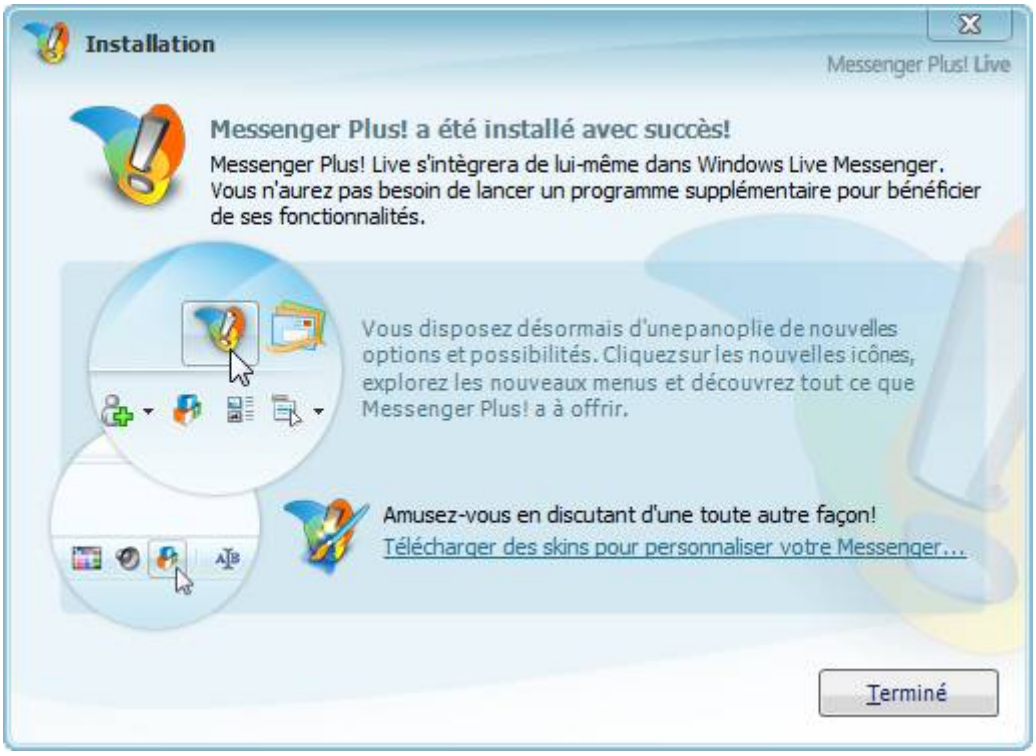
Décochez les trois cases comme sur l'image ci-dessous :



Cochez la case « J'accepte les termes du Contrat d'Utilisation, installer Messenger Plus! Live » et cliquez sur le bouton « Suivant ».



Pendant que vous avez la fenêtre ci-dessus, patientez jusqu'à l'apparition de la fenêtre suivante :

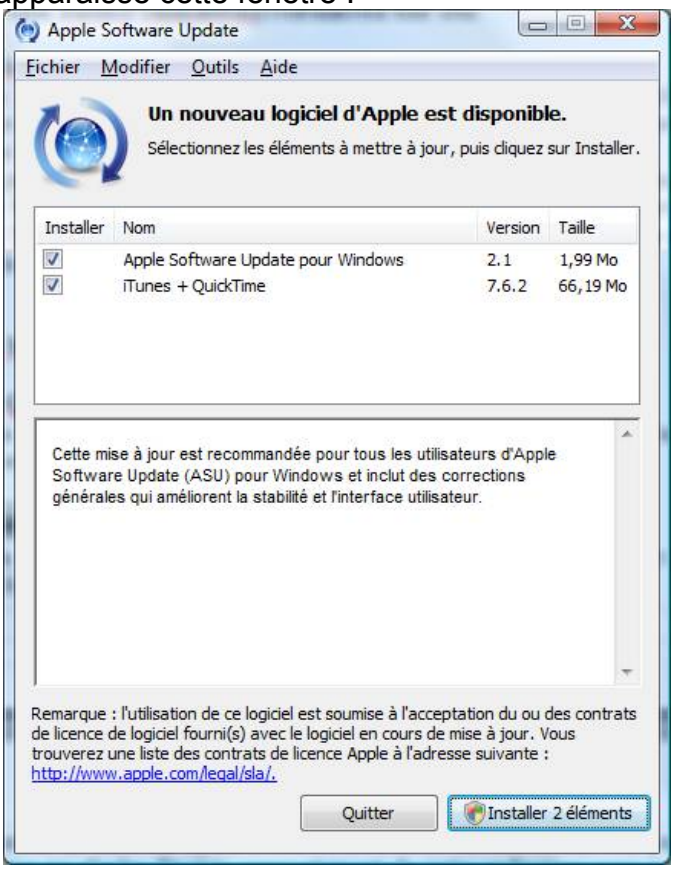


Cliquez sur « Terminé ».

Si Windows Live Messenger ne se relance pas, rouvrez le.

VII.5) Mise à jour de Quicktime, iTunes et Safari

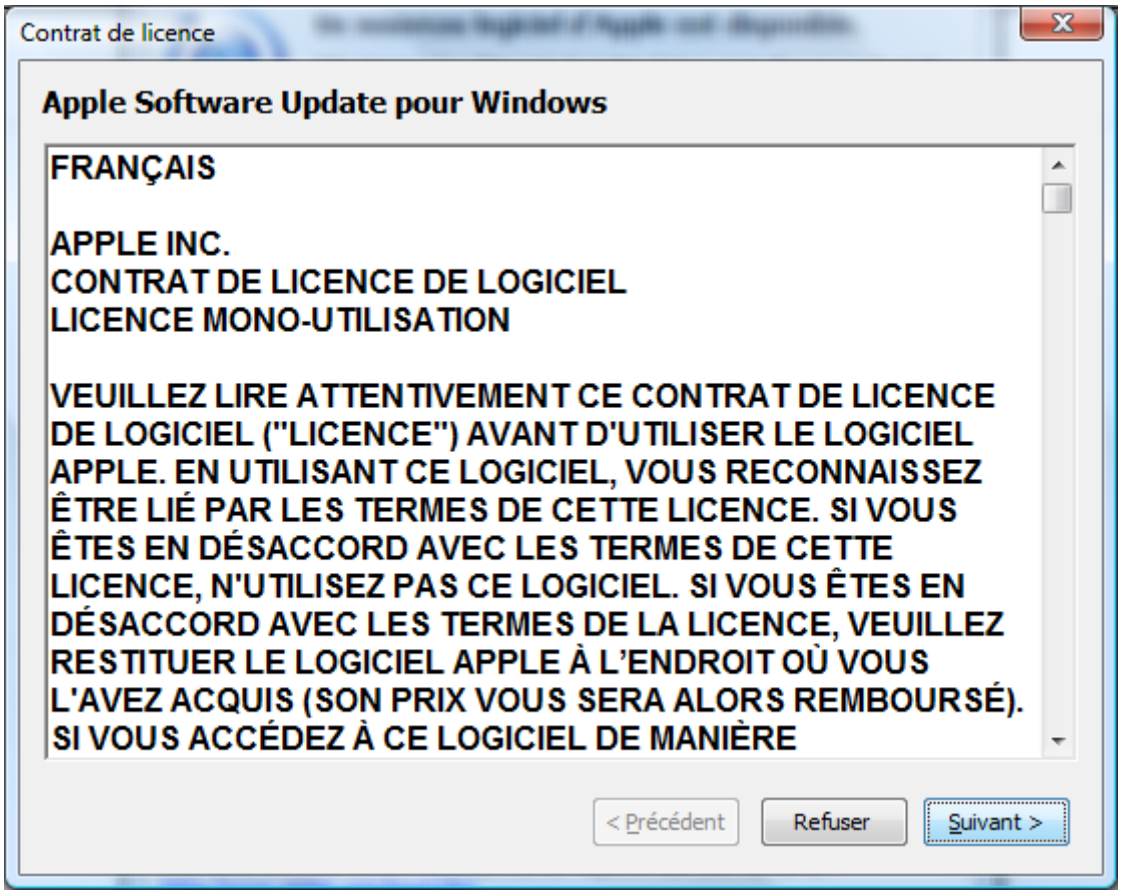
Si vous avez un seul (ou plusieurs) de ces logiciels installés dans votre ordinateur, il se peut que régulièrement apparaisse cette fenêtre :



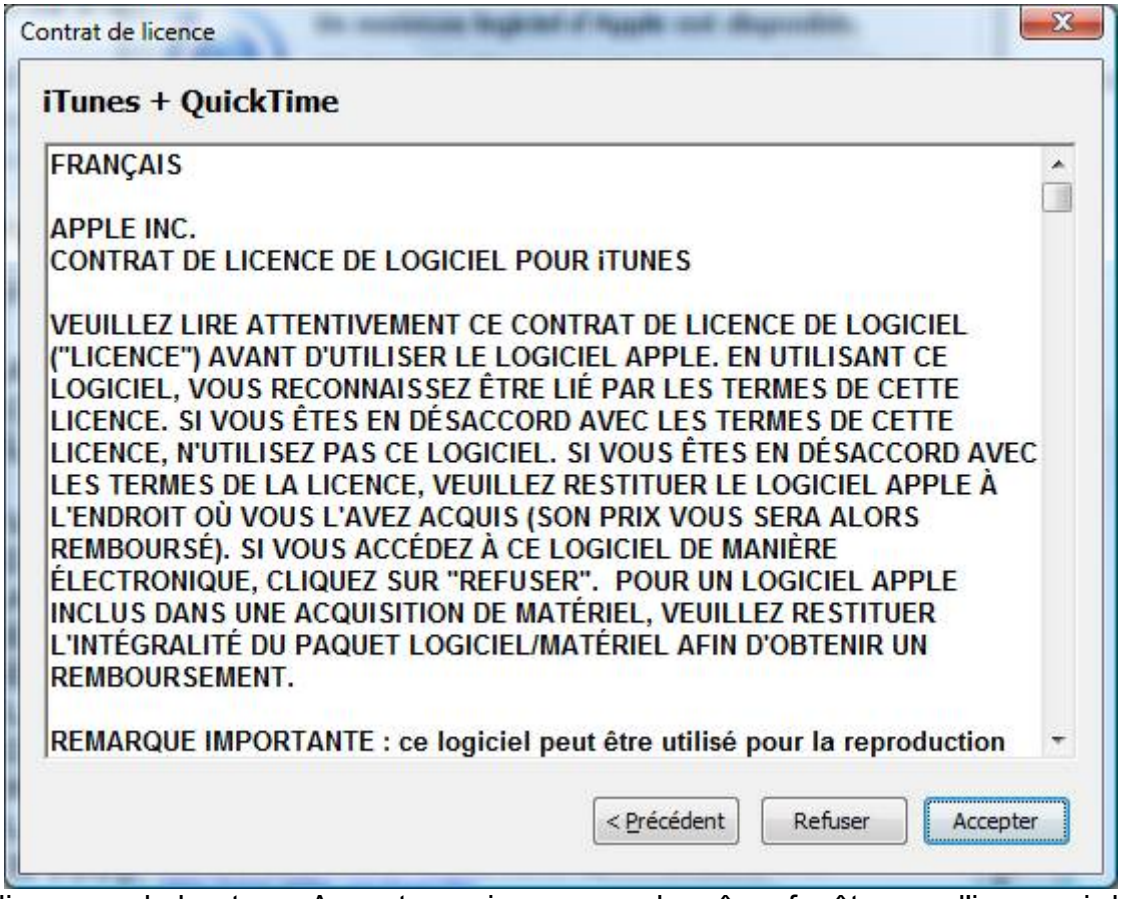
Cliquer sur le bouton « Installer x éléments ».

Tout d'abord, il vous faudra valider les différents contrats de licence des différents

logiciels souhaitant s'installer.



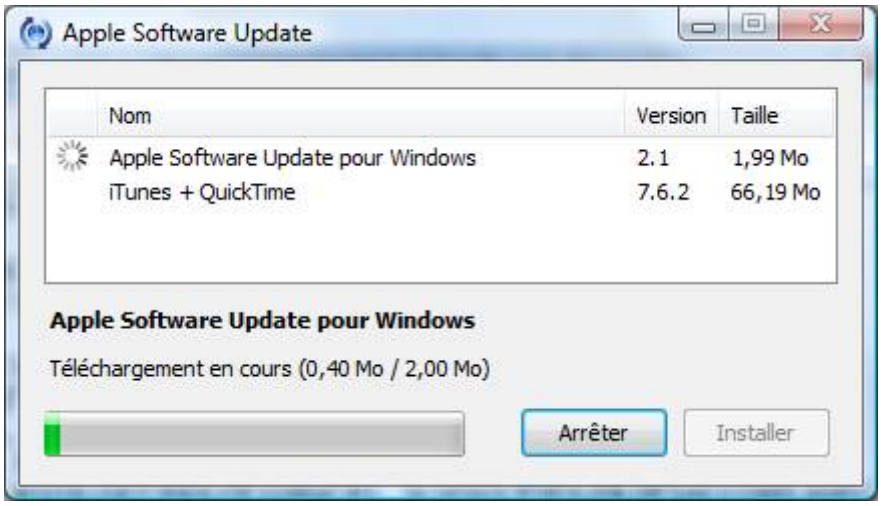
Cliquez sur le bouton « Suivant » si vous avez la même fenêtre que l'image ci-dessus.



Cliquez sur le bouton « Accepter » si vous avez la même fenêtre que l'image ci-dessus.

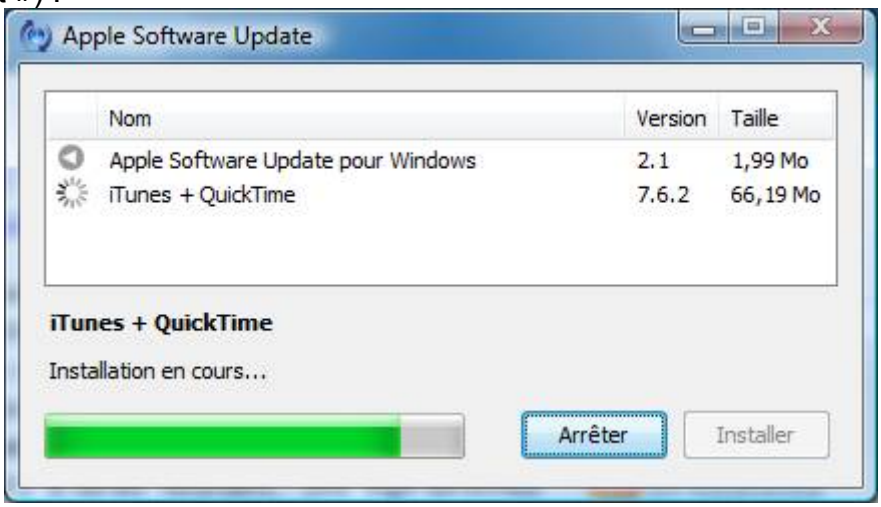
Si vous avez Windows Vista, une demande de confirmation sera ainsi affichée par

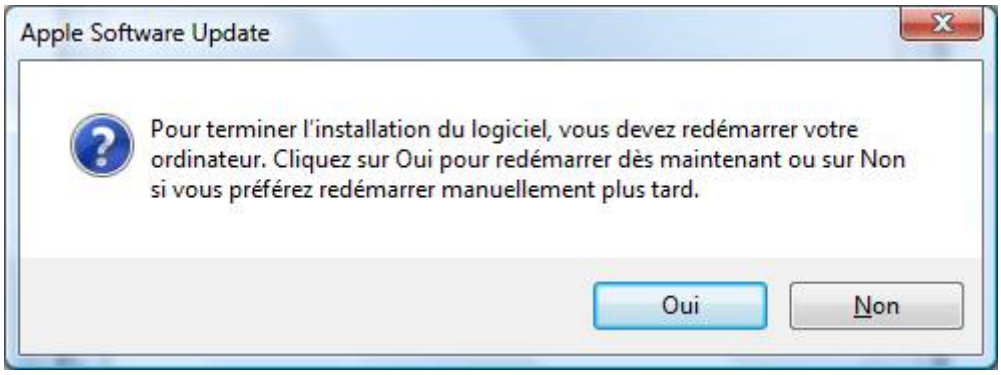
l'ordinateur. Cliquez sur le bouton « Continuer ».



Patientez pendant le téléchargement des différents logiciels.

L'installation se fait ensuite de manière silencieuse (sans vous demander de cliquer 25 fois sur « Suivant ») :





S'il vous est demandé de redémarrer, sauvegardez votre travail en cours et cliquez sur le bouton « Oui ».

VII.6) Mise à jour de Java

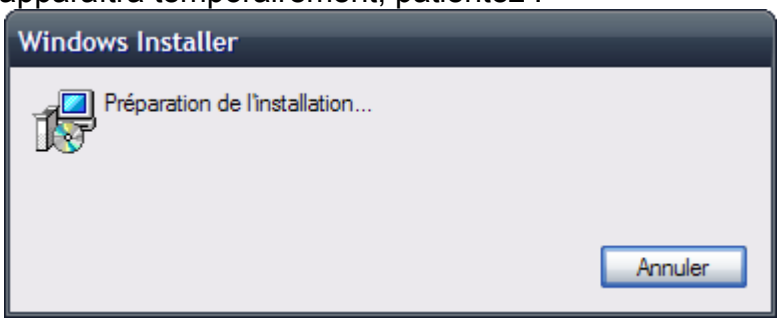
De temps en temps, votre ordinateur vous propose une mise à jour de Java (non, pas pour faire la java). L'ordinateur vous préviens en affichant cette icône à côté de l'horloge avec une petite bulle d'explication :  .

Cliquez dessus.

Cliquez ensuite sur le bouton « Installer ».

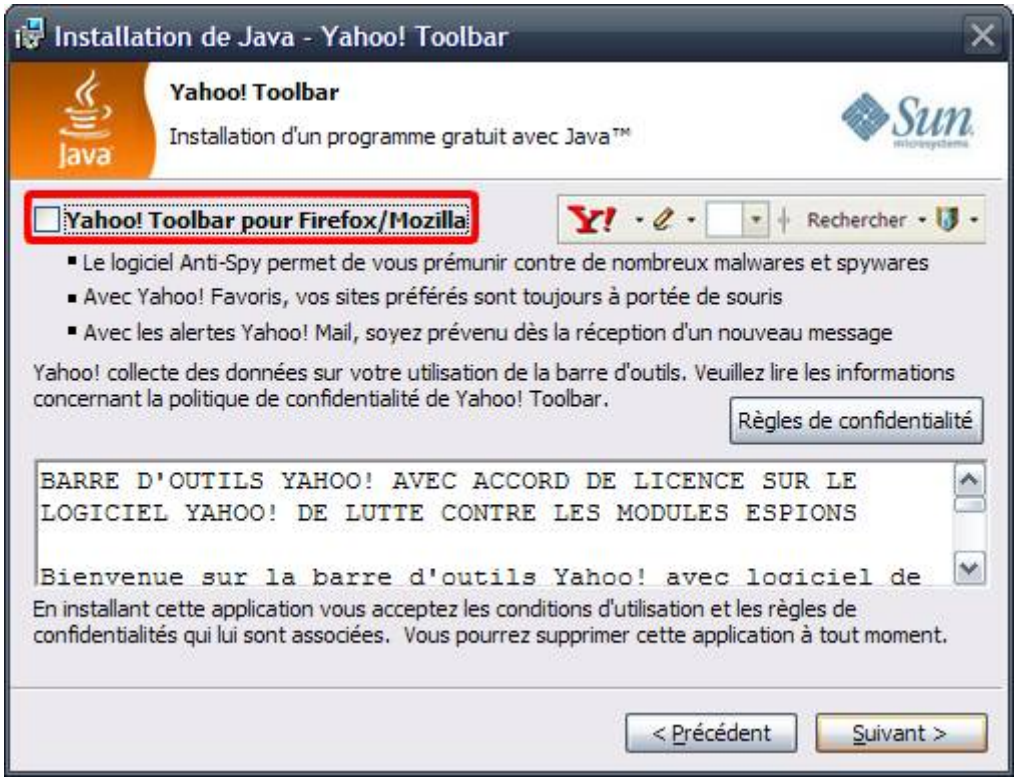
Votre pare-feu vous préviendra d'une tentative d'accès pour ces deux programmes : Java (TM) Update Checker et ZoneAlarm : Java (TM) Plateform SE binary. Autorisez l'accès temporairement (sous ZoneAlarm, cliquez sur Autoriser, sans cocher la case « Conserver »).

Cette fenêtre apparaîtra temporairement, patientez :



Peu de temps après, cette fenêtre apparaît. Cliquez sur le bouton « Accepter » :

Décochez la case « Yahoo Toolbar pour Firefox/Mozilla » et cliquez sur le bouton « Suivant » :

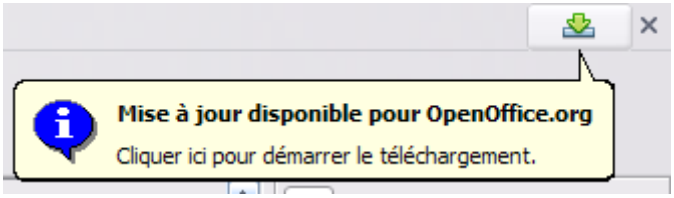


Lorsque la fenêtre prend cette apparence, patientez :

Peu de temps après, la fenêtre prend cette apparence. Cliquez sur le bouton « Terminer » :

VII.7) Mise à jour d'OpenOffice

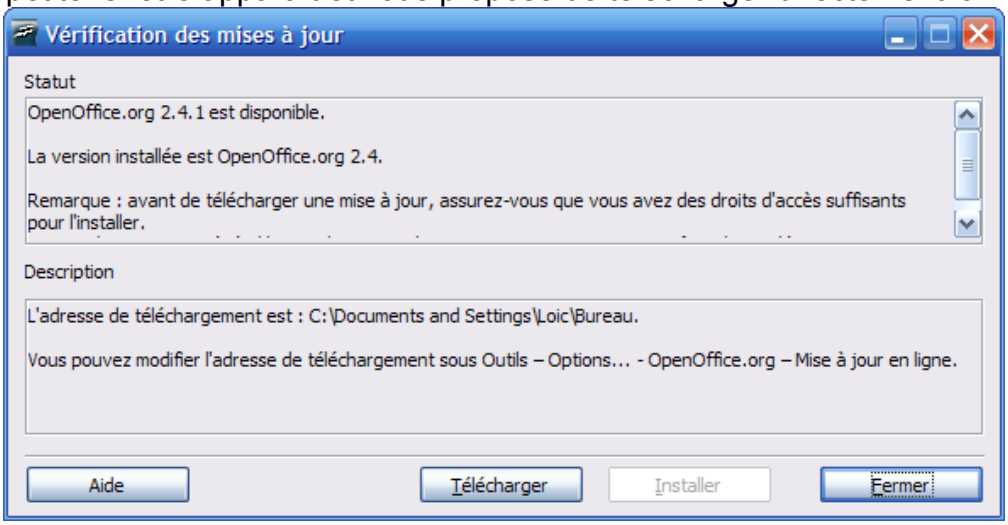
Lorsque vous travaillez sous OpenOffice, sauf si vous avez désactivé l'avertissement des mises à jour automatiques, une petite icône apparaît de temps en temps en haut à droite de la fenêtre :



Cela signifie qu'il y a une mise à jour d'OpenOffice. Sauvegardez votre travail en cours et cliquez sur l'icone.

En fonction de la version que vous avez actuellement, plusieurs choses peuvent se passer :

• Une petite fenêtre apparaît et vous propose de télécharger directement la mise à jour :



Cliquez sur le bouton « Télécharger ».

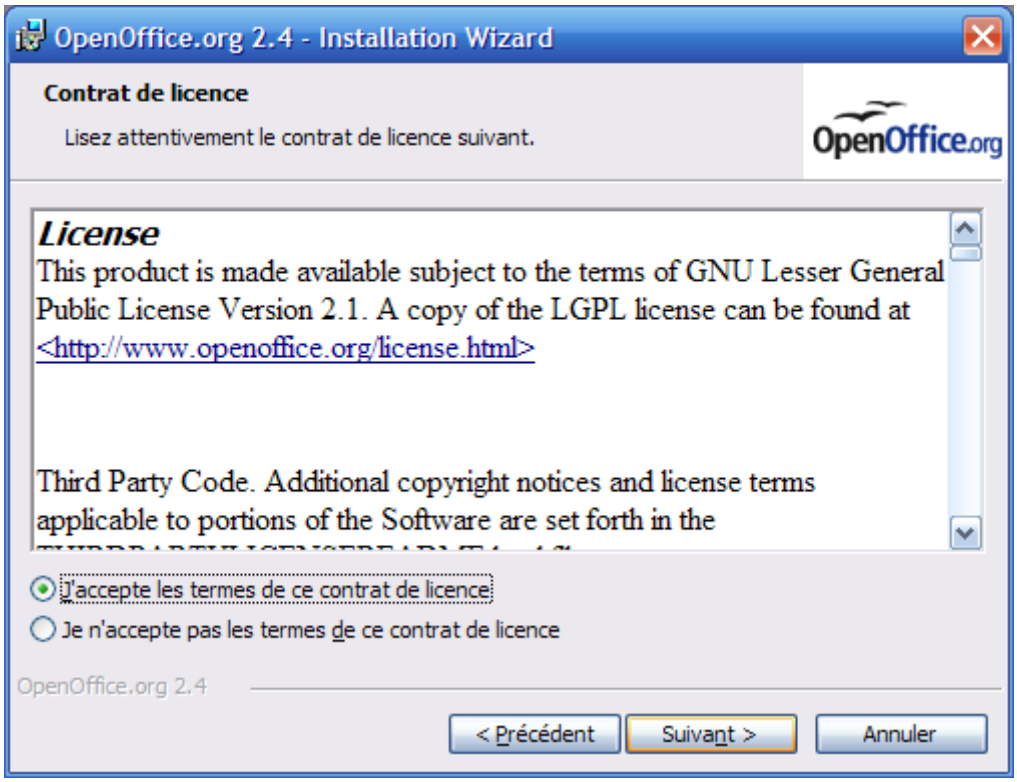
VII.7.a) Installation d'OpenOffice

Cliquez sur le bouton « Suivant ».

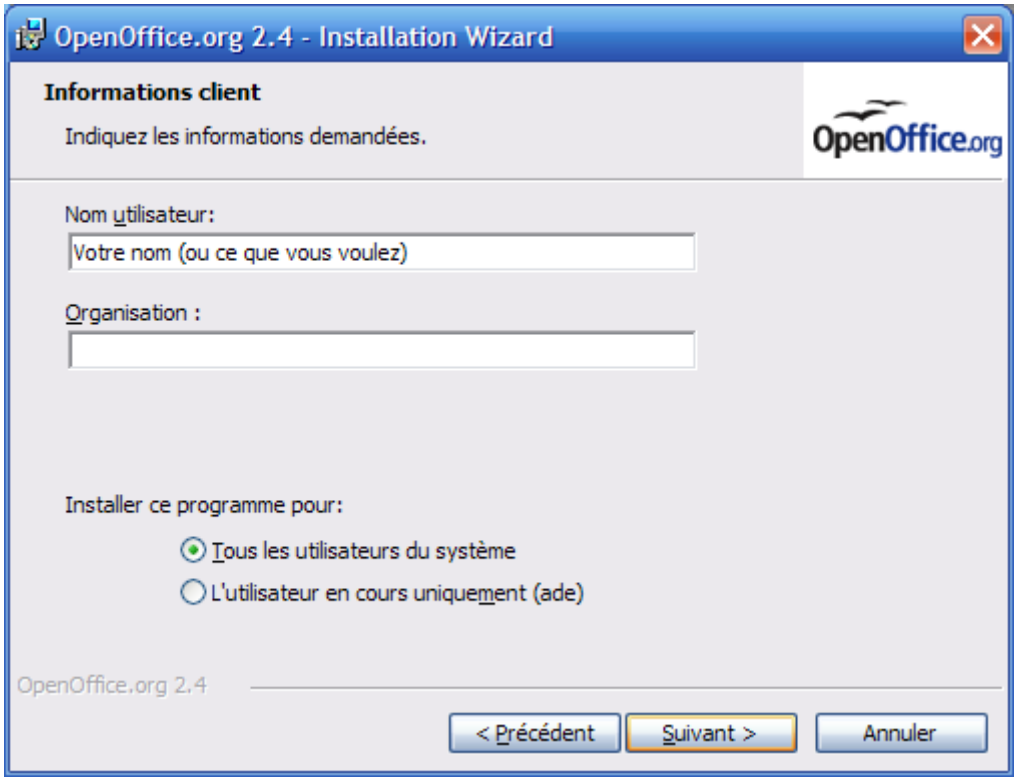
Cliquez sur le bouton « Décompresser ».

Patientez quelques instants.

Patientez encore quelques instants et cliquez sur le bouton « Suivant ».

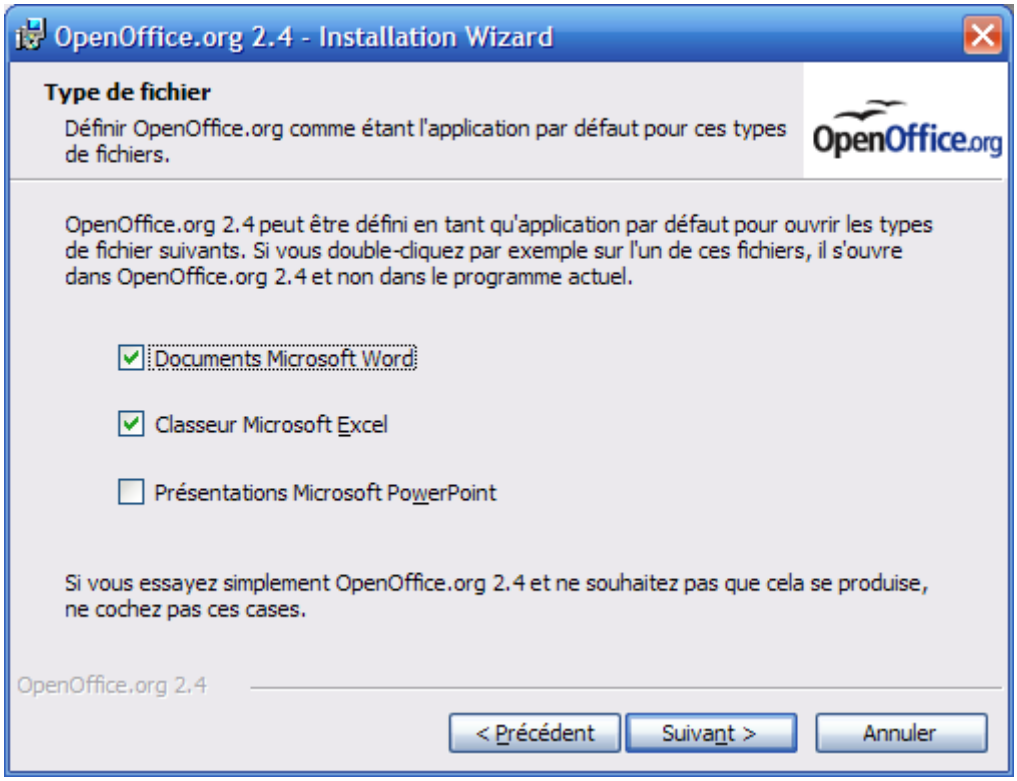


Cochez la case « J'accepte les termes de ce contrat de licence » et cliquez sur le bouton « Suivant ».

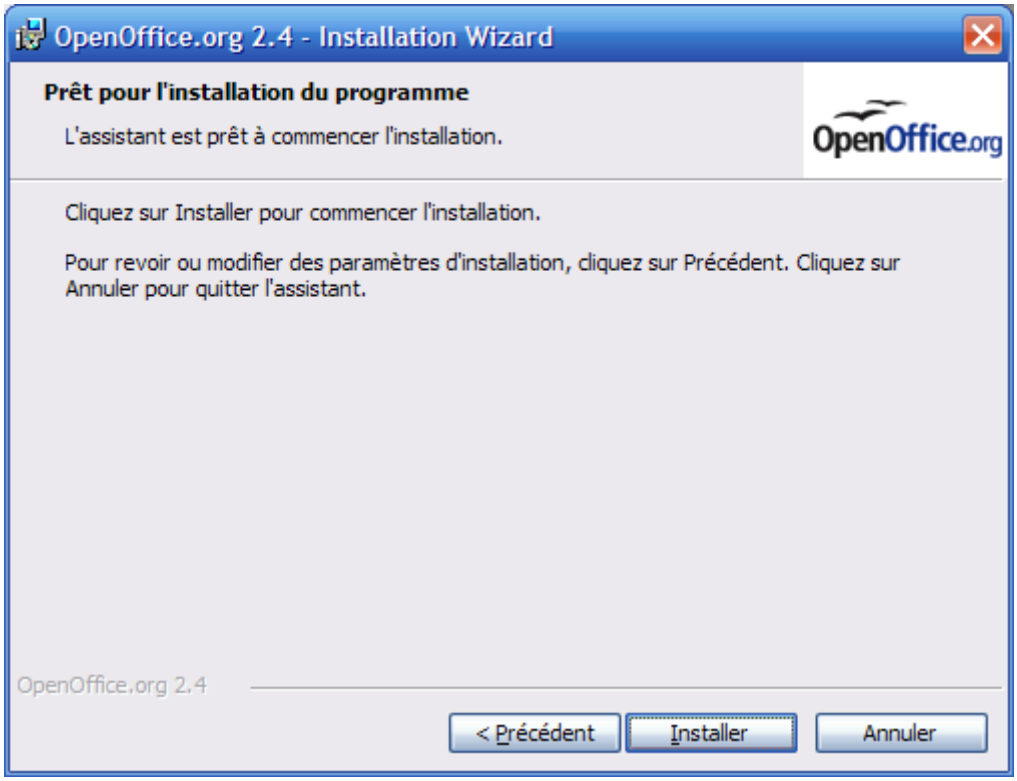


Dans la case « Nom d'utilisateur », tapez votre nom (ou ce que vous voulez, il n'est pas obligatoire de mettre votre nom). Cochez la case 'Tous les utilisateurs de ce système » et cliquez sur le bouton « Suivant ».

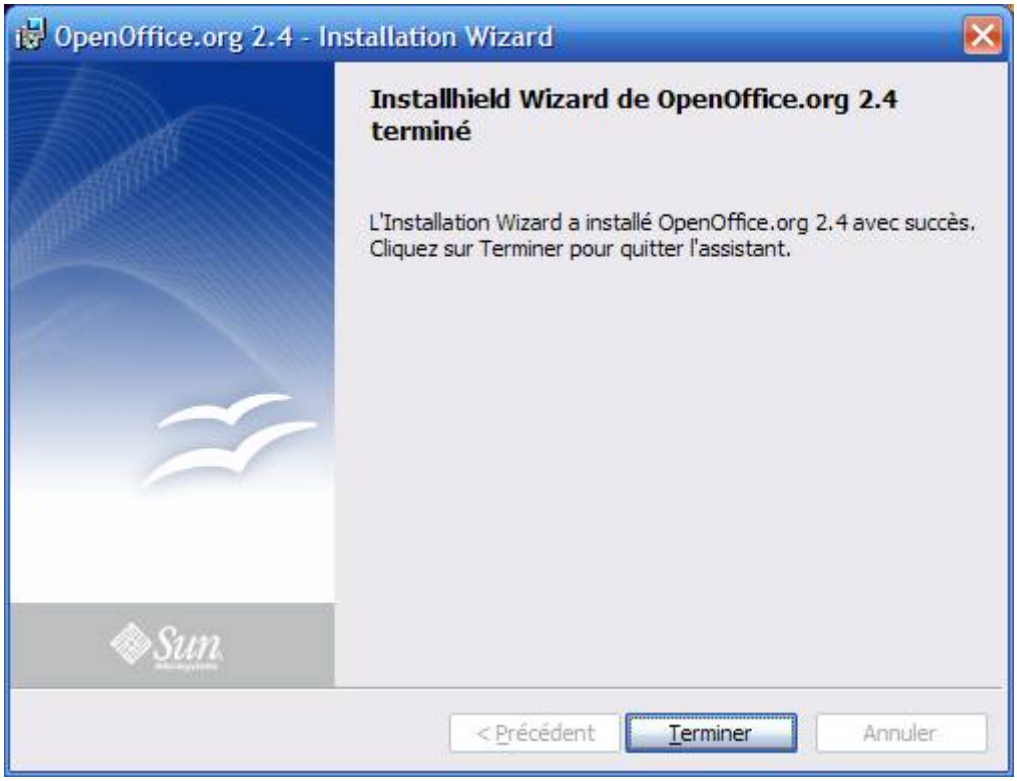
Cochez la case « Installation standard » et cliquez sur le bouton « Suivant ».



Si vous avez Microsoft Office et que vous ne l'utilisez pas, ou que vous ne l'avez pas, cochez les deux premières cases et décochez la dernière (on décoche « Présentations Microsoft PowerPoint » car on utilisera plutôt la visionneuse fournie par Microsoft pour ouvrir ce type de fichiers). Si vous avez Microsoft Office et que vous l'utilisez, décochez les trois cases. Cliquez ensuite sur le bouton « Suivant ».



Cliquez ensuite sur le bouton « Installer ».



Patientez quelques instants le temps de l'installation et cliquez sur Terminer

VII.8) Mise à jour de Flash Player

Adobe Flash Player est un outil qui permet d'afficher les animations Flash. Ces animations Flash, ce sont les encarts publicitaires ou encore les jeux en lignes auxquels vous jouez peut-être (par exemple, Prizee).

Le lecteur d'animations Flash n'est pas un programme parfait (comme les autres) et des failles de sécurité sont aussi régulièrement découvertes. Il est donc important d'effectuer la mise à jour.

Quand il y a une mise à jour disponible, vous verrez cette fenêtre apparaître au démarrage de votre ordinateur :

Cliquez sur « Installer maintenant ».

Si vous avez Windows Vista, le contrôle des comptes utilisateurs apparaîtra et vous demandera l'autorisation de continuer. Cliquez sur le bouton « Continuer ».

Le téléchargement s'effectuera. Patientez pendant cette étape.

Un message d'avertissement vous préviendra que la mise à jour s'est correctement installée. Enregistrez le travail que vous aviez commencé et redémarrez l'ordinateur.

VIII) Quelques installations de quelques logiciels

VIII.1) Internet Explorer 7

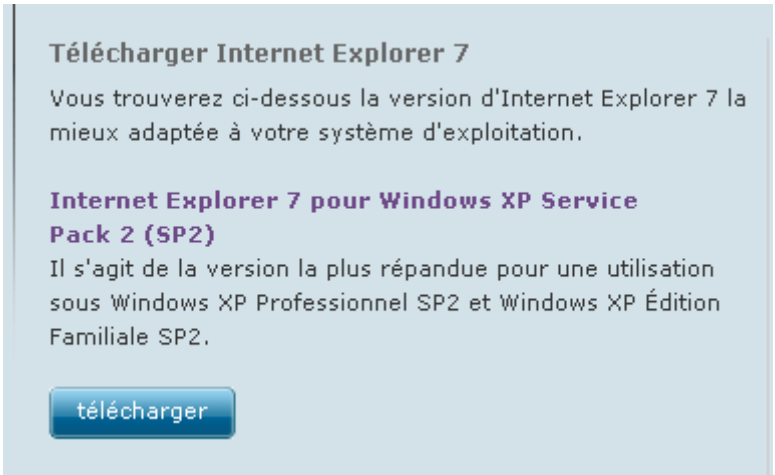
VIII.1.a) Téléchargement

Entrez « Internet Explorer 7 » dans votre moteur de recherche préféré et trouvez ce résultat :

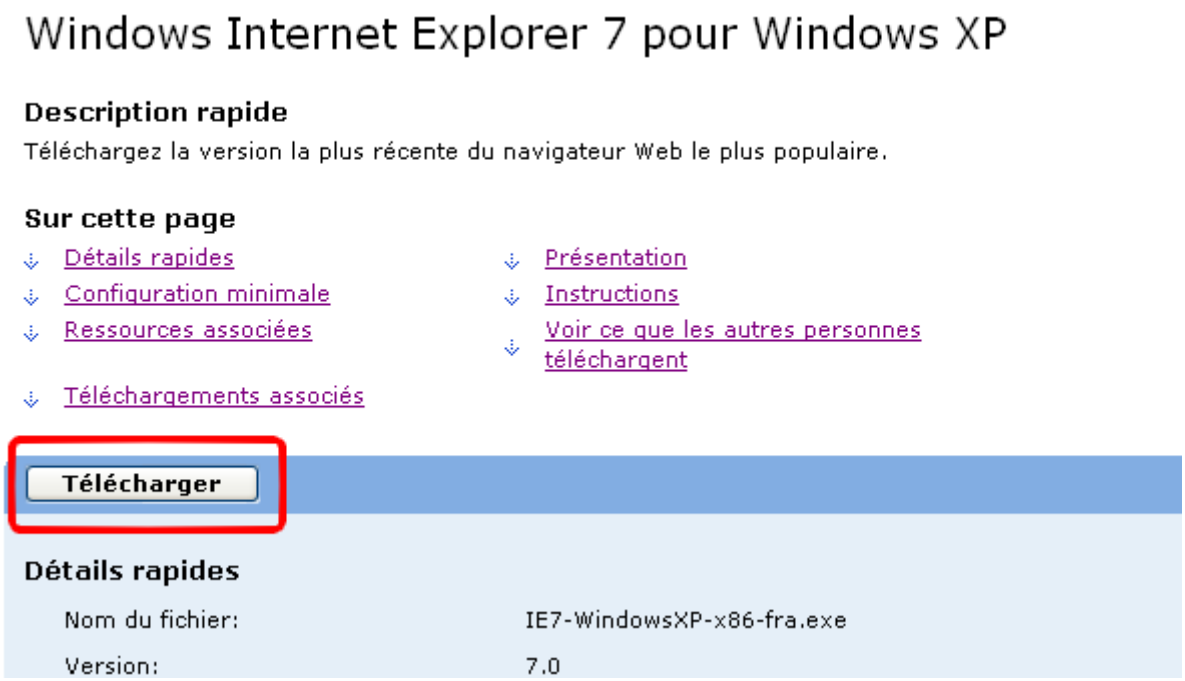
Internet Explorer : Page d'accueil
Téléchargez **Internet Explorer 7**, le navigateur gratuit de Microsoft, ou explorez ses fonctions. Découvrez la façon dont vous pouvez tirer parti de ses ...
www.microsoft.com/france/windows/**ie**/ - 106k - En cache - Pages similaires

Allez dans la page trouvée.

Cliquez ensuite sur le lien « télécharger » (voir cadre bleu de l'image ci-dessus).



Cliquez sur le bouton « télécharger ».



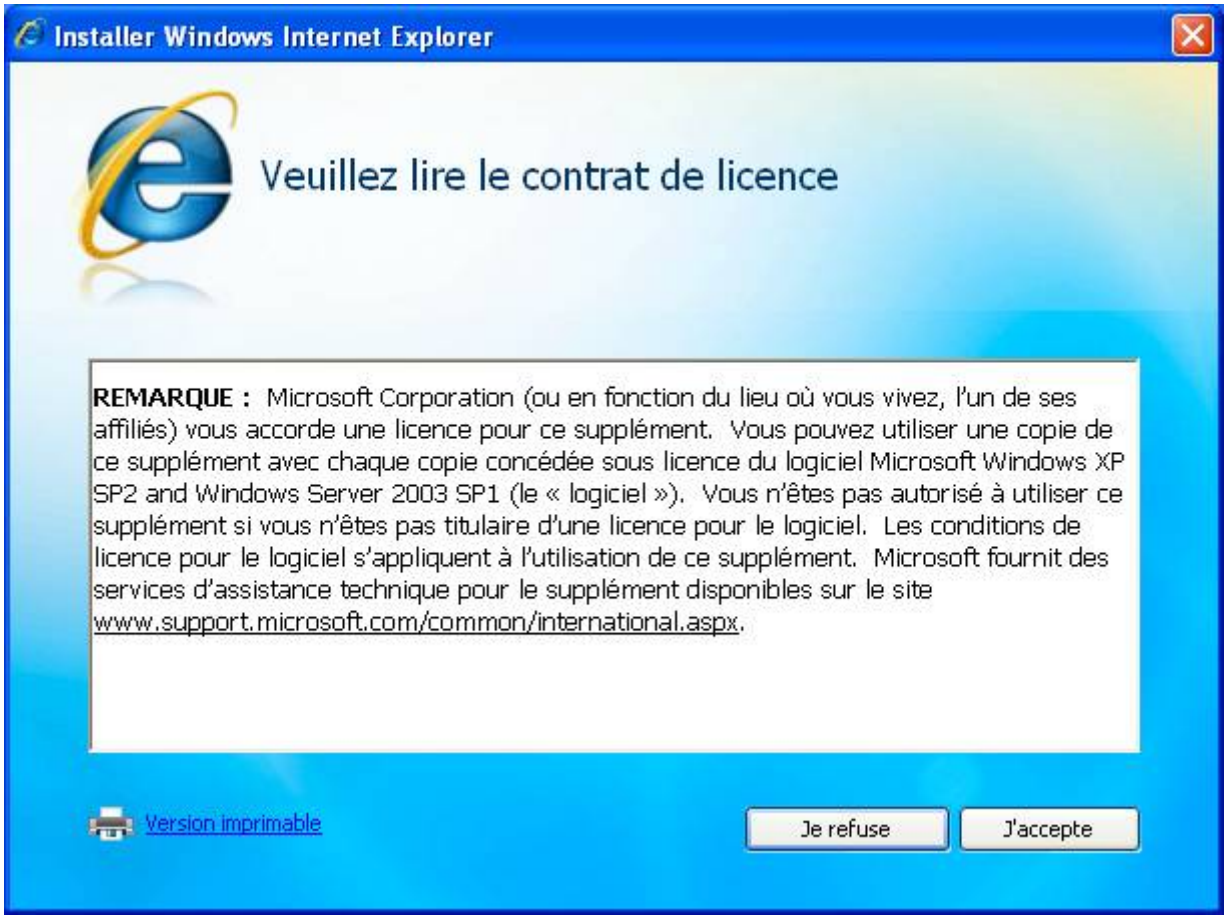
Cliquez sur le bouton « Télécharger ».

Enregistrez le fichier proposé.

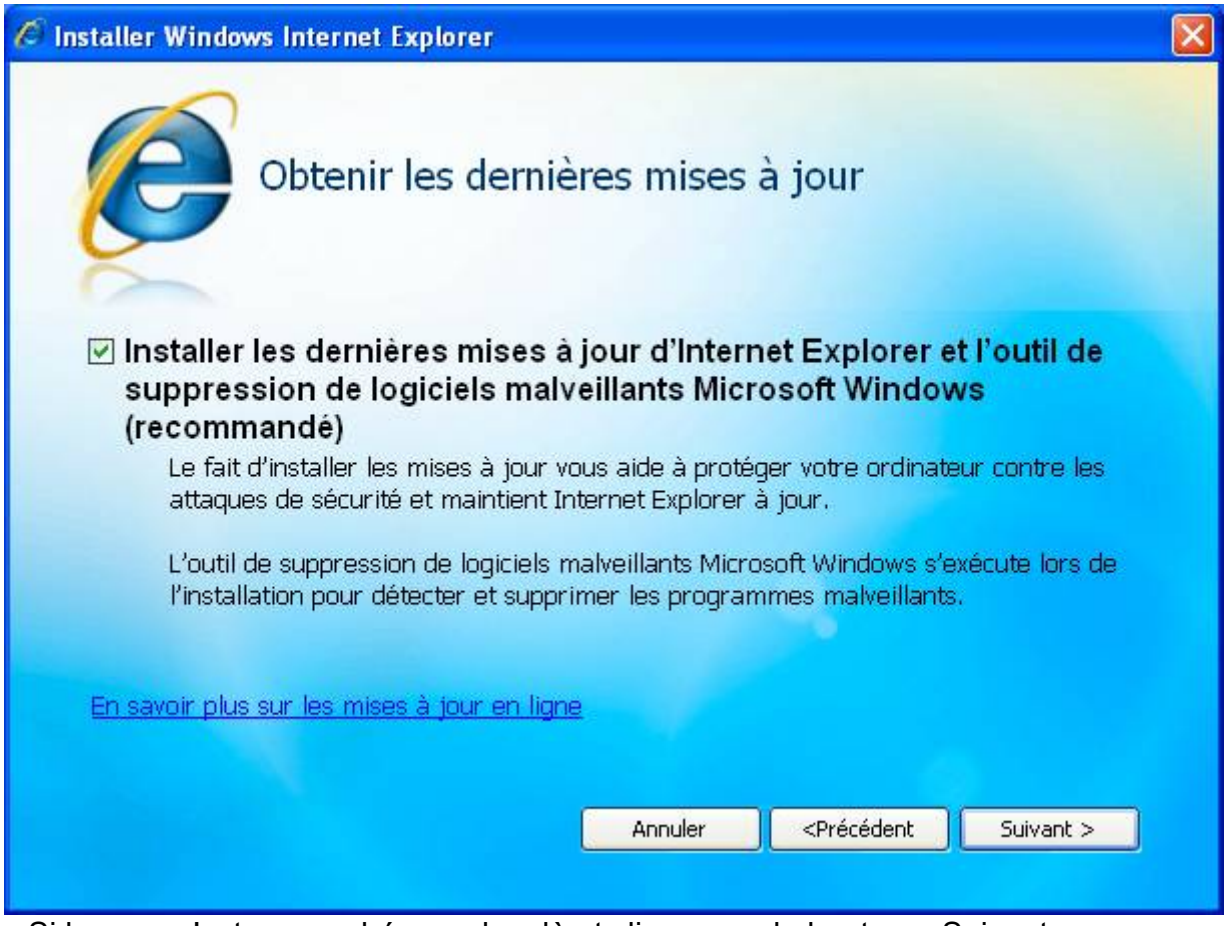
VIII.1.b) Installation

Ouvrez le fichier précédemment téléchargé.

Cliquez sur le bouton « Suivant ».

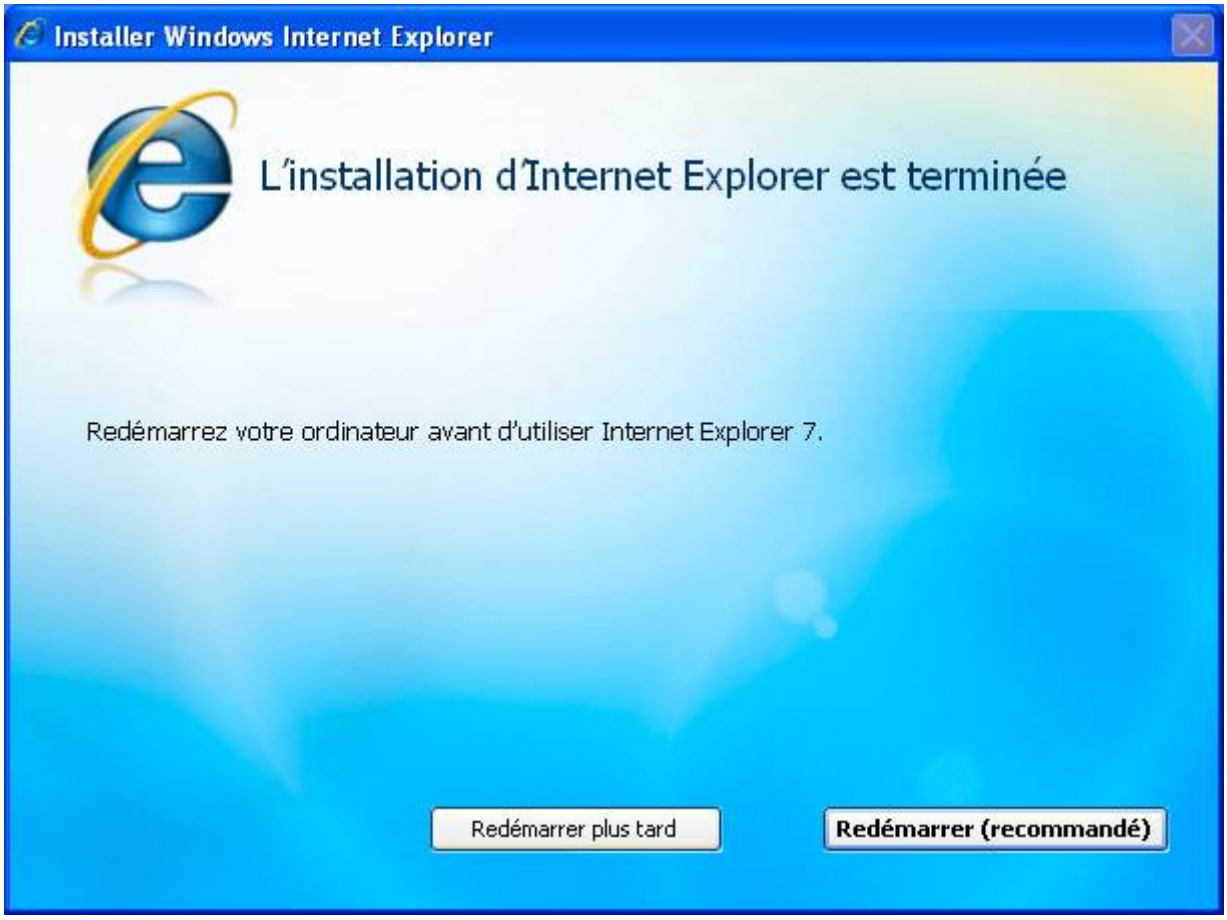


Cliquez sur le bouton « J'accepte ».



Si la case n'est pas cochée, cochez là et cliquez sur le bouton « Suivant ».

Patientez. Le programme d'installation téléchargera les mises à jour et l'outil de suppression de quelques logiciels malveillants. Internet Explorer sera ensuite installé ainsi que les mises à jour.



Sauvegardez votre travail en cours et cliquez sur le bouton « Redémarrer ».

VIII.2) Mozilla Firefox 3

VIII.2.a) Téléchargement

Utilisez votre moteur de recherche préféré pour aller sur el site officiel de Mozilla Firefox et trouvez ce résultat :

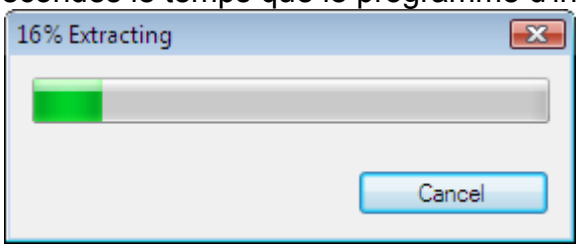
Cliquez ensuite sur « Téléchargement gratuit » :

Ensuite, la procédure de téléchargement est la procédure habituelle de votre navigateur Internet.

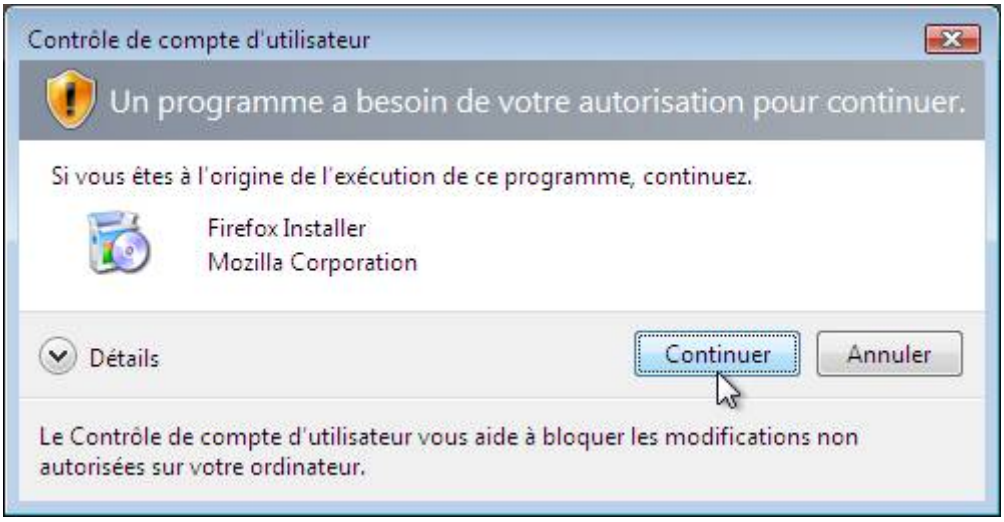
VIII.2.b) Installation

Ouvrez le fichier précédemment téléchargé.

Patientez quelques secondes le temps que le programme d'installation soit extrait :

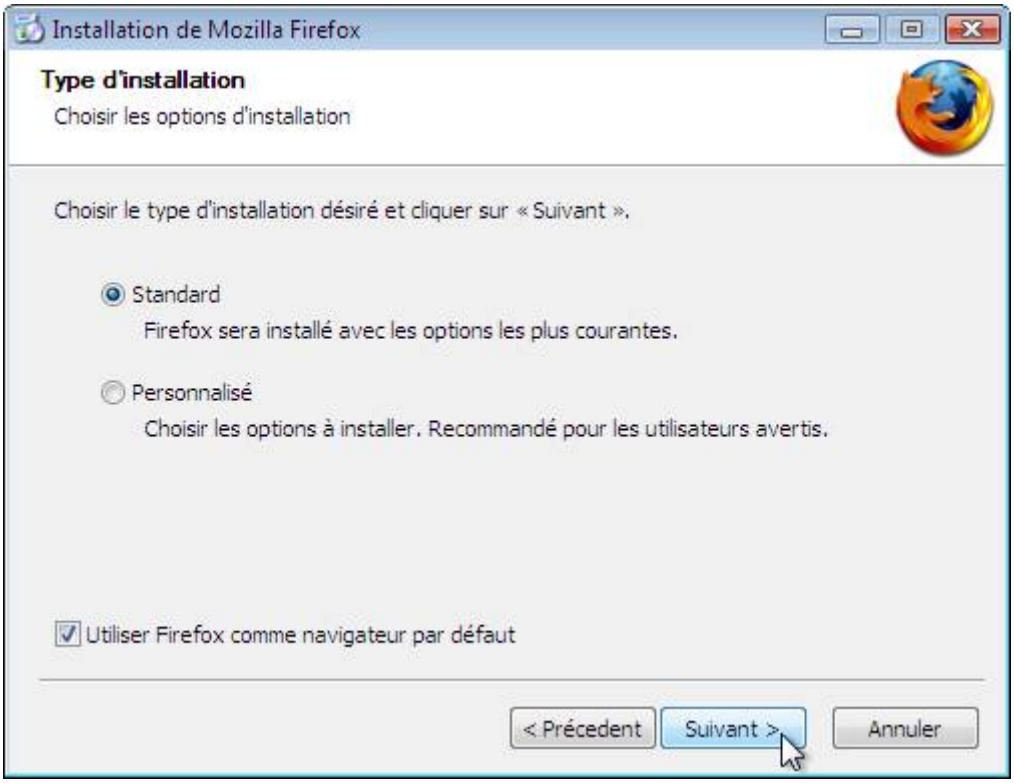


Si le « Contrôle de compte d'utilisateur » apparaît, cliquez sur « Continuer » :

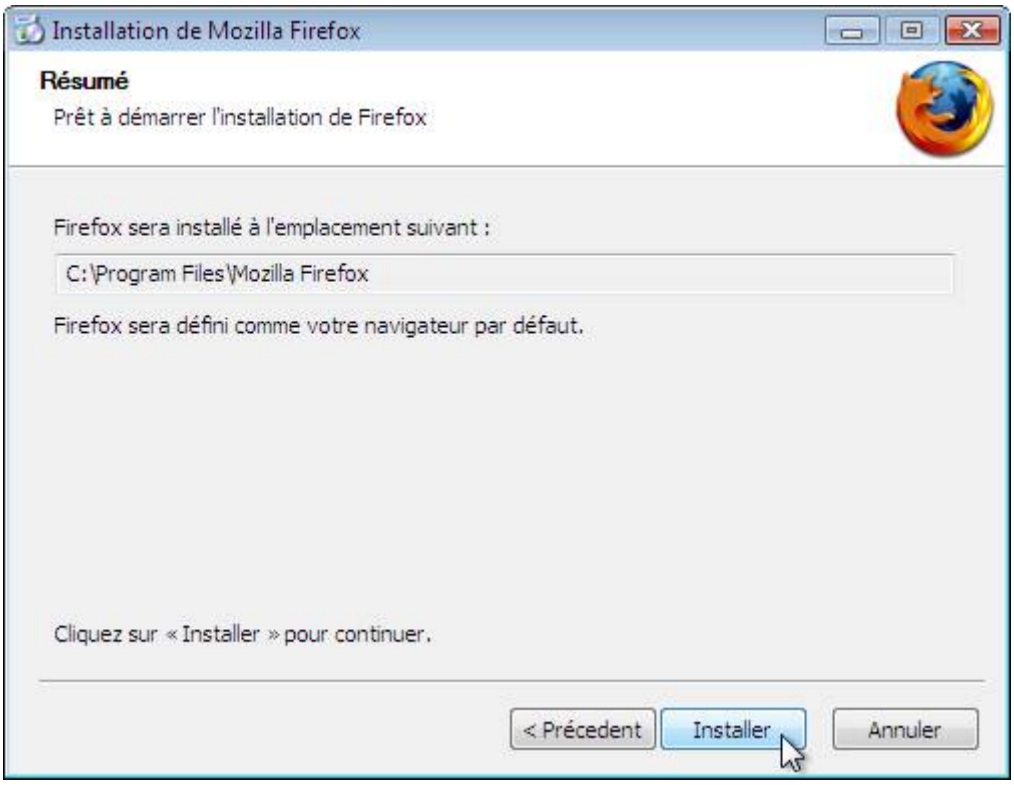


Cliquez ensuite sur le bouton « Suivant » :

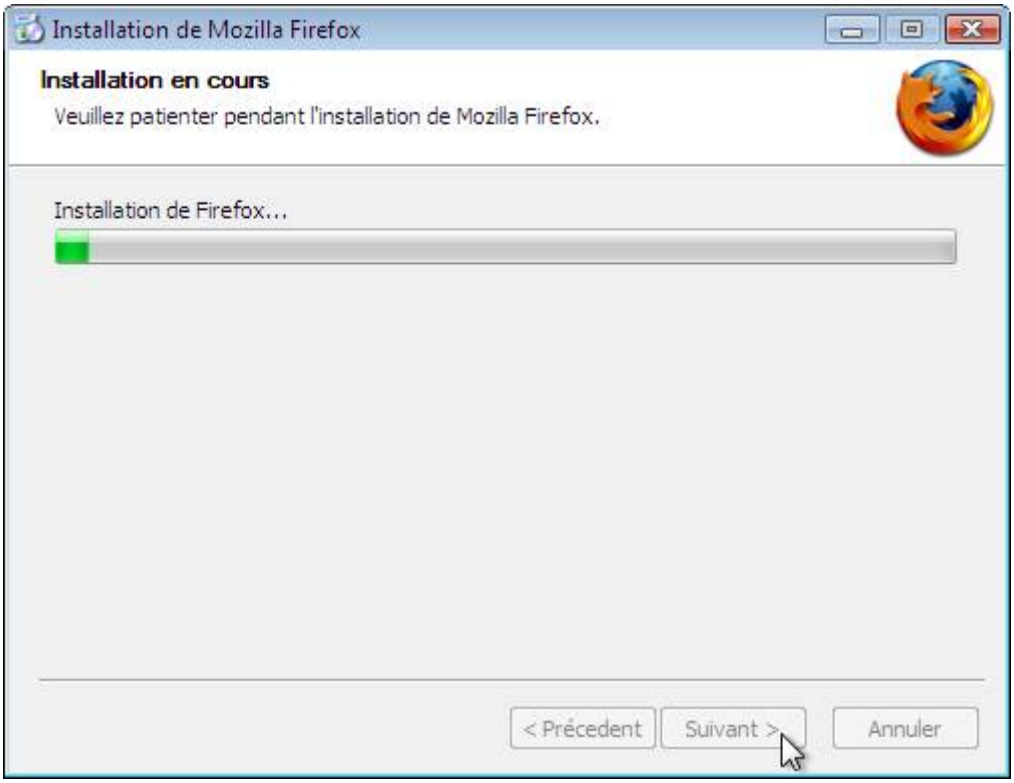
Cochez la case « Standard » ainsi que la case « Utiliser Firefox comme navigateur par défaut » (non obligatoire, mais je vous le recommande fortement). Cliquez ensuite sur le bouton « Suivant » :



Cliquez ensuite sur le bouton « Installer » :



Veuillez patienter pendant l'installation de Firefox :



Décochez la case « Lancer Firefox maintenant » et cliquez sur Terminer :

Maintenant, créons un profil :

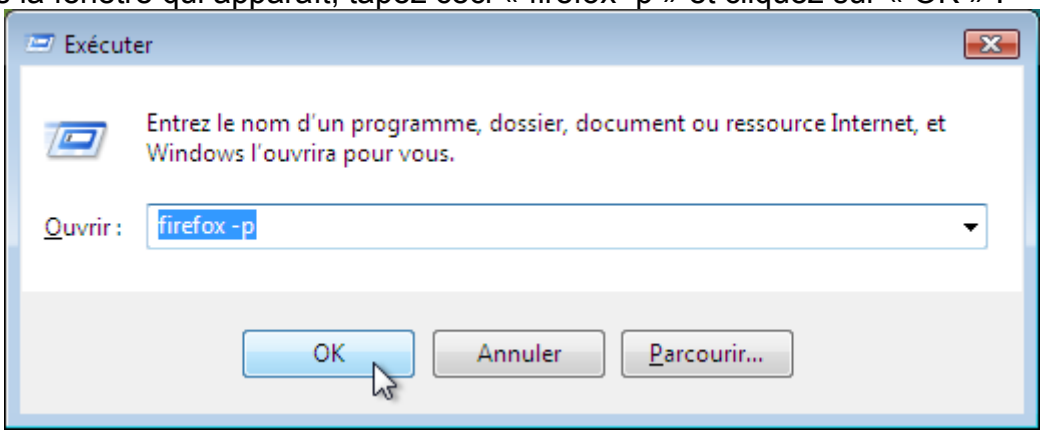
VIII.2.c) Création d'un profil

Par défaut, vos marques pages (les favoris sous Internet Explorer) et tous vos réglages sont enregistrés dans un dossier bien caché de l'ordinateur. Ces réglages et marques pages sont donc régulièrement oubliés lors de sauvegardes de l'ordinateur. Cette procédure permettra de mettre les fichiers de votre profil de Firefox dans votre dossier de documents.

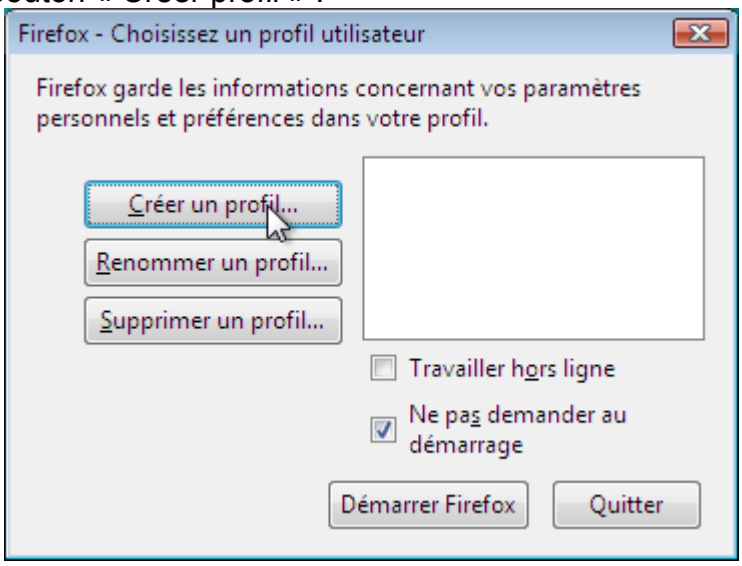
Cliquez sur votre bouton Démarrer, et cliquez sur « Exécuter ». Si vous n'avez pas

« Exécuter », appuyez sur la touche  et en même temps sur la touche  de votre clavier.

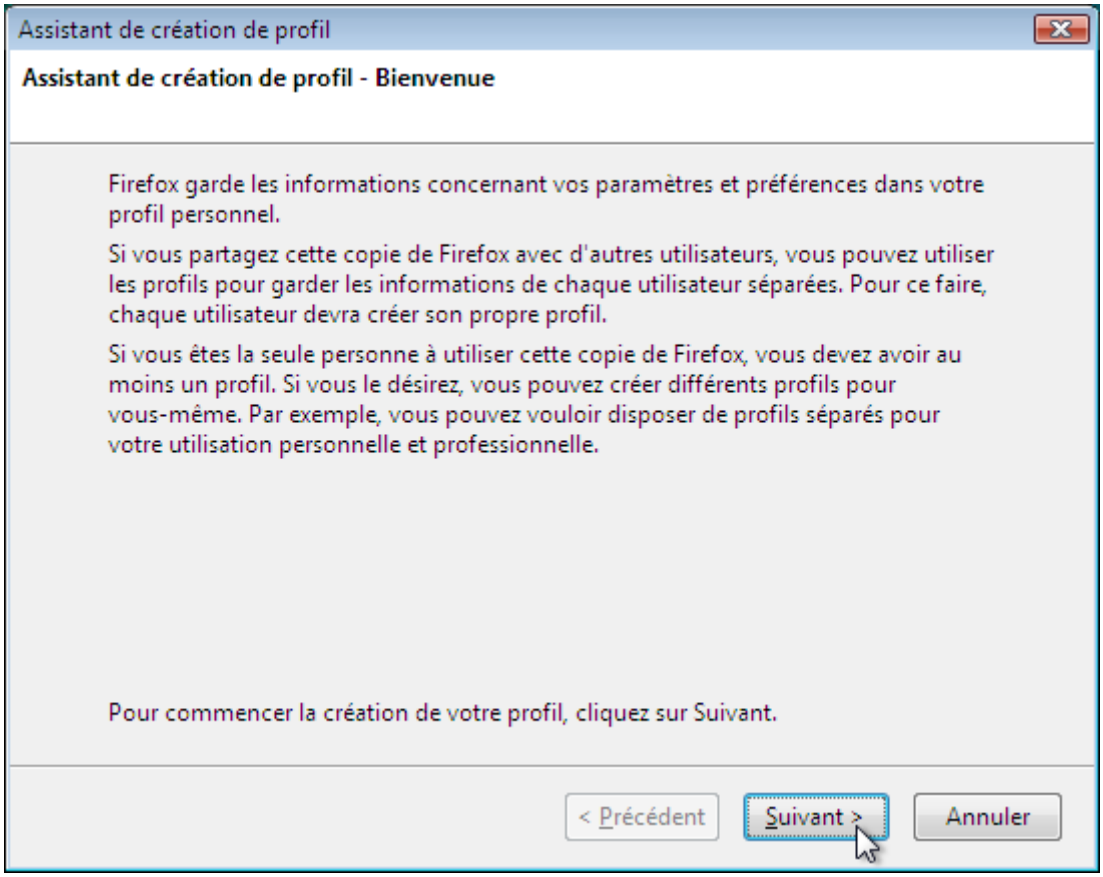
Dans la fenêtre qui apparaît, tapez ceci « firefox -p » et cliquez sur « OK » :



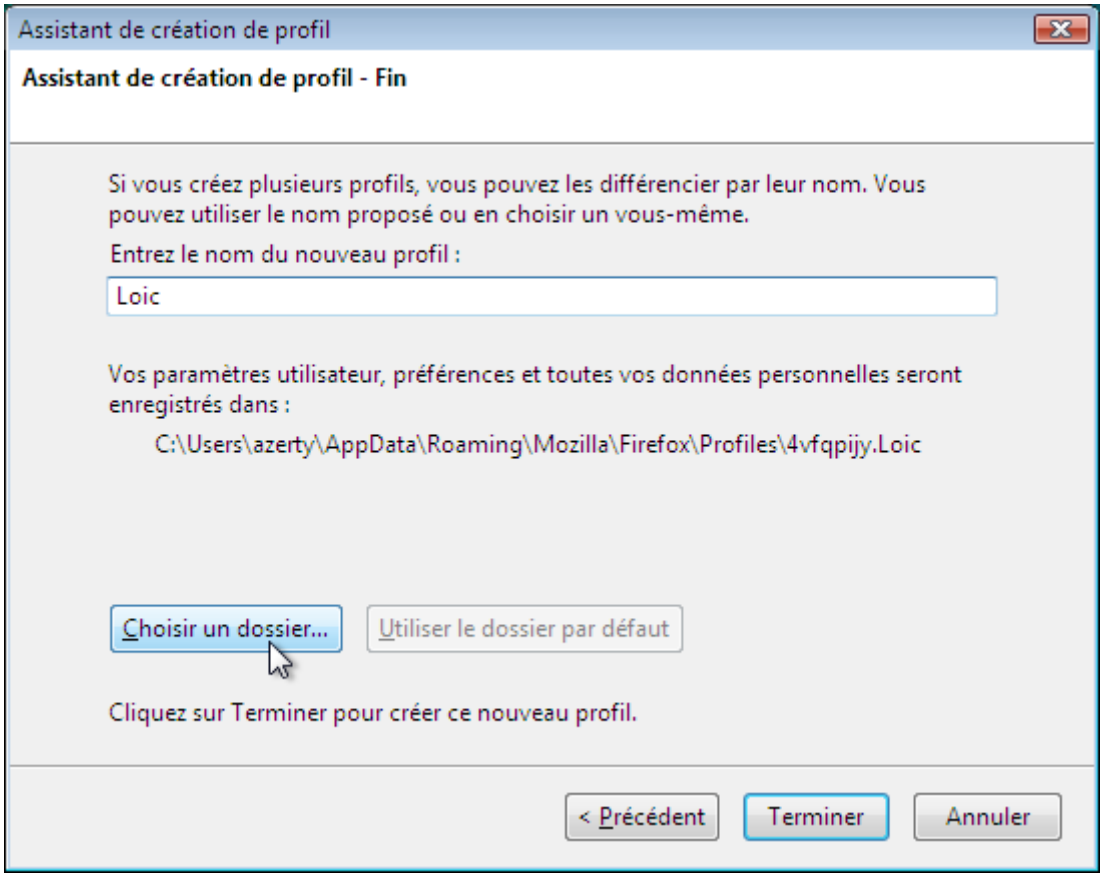
Cliquez sur le bouton « Créer profil » :



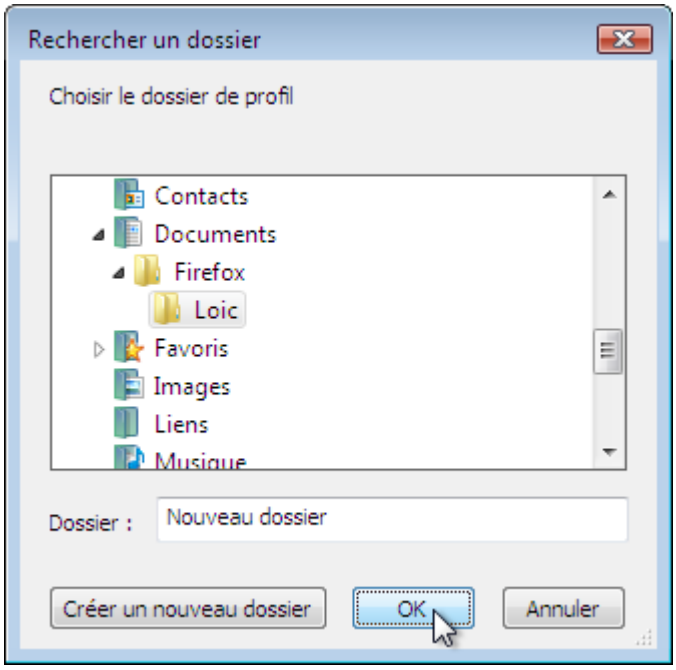
Cliquez sur le bouton « Suivant » :



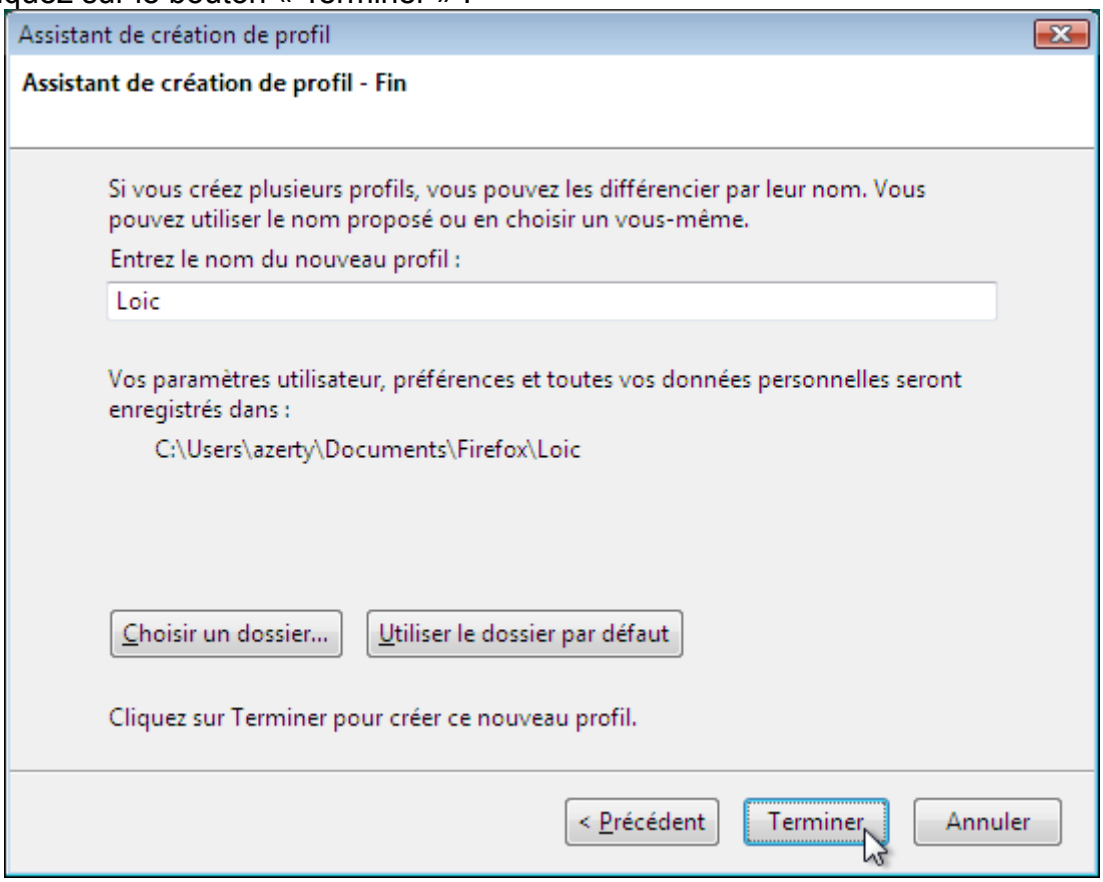
Choisissez un nom pour votre profil (en évitant les lettres accentuées) et cliquez sur le bouton « Choisir un dossier » :



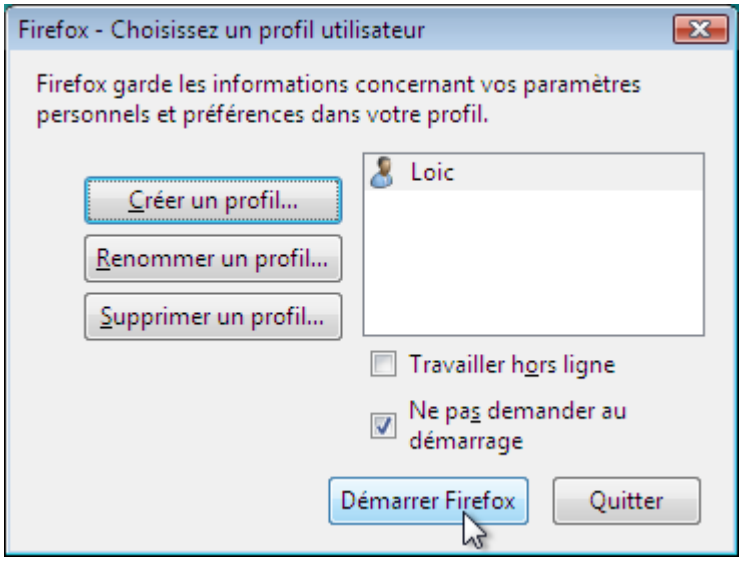
Cherchez votre dossier de documents, et cliquez sur le bouton « Créer un nouveau dossier » afin de créer un dossier « Firefox ». Cliquez sur ce dossier « Firefox » et créez un nouveau dossier avec le nom de votre profil. Cliquez ensuite sur le bouton « OK » :



Cliquez sur le bouton « Terminer » :

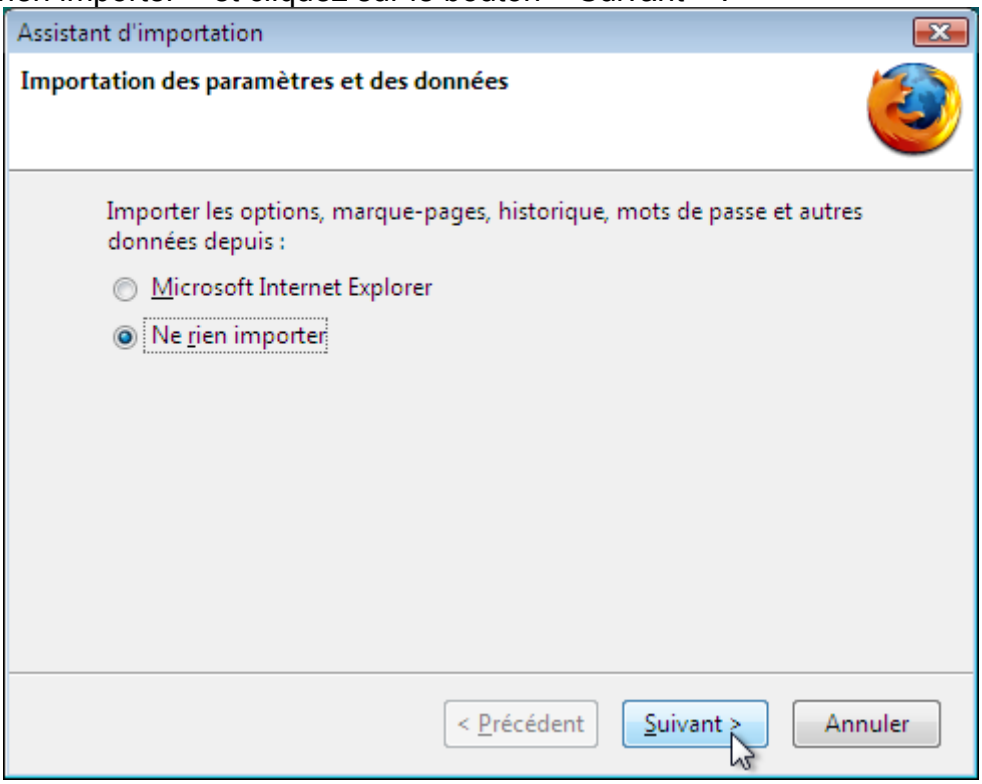


Cliquez sur « Démarrer Firefox » afin de poursuivre sa mise en place :



VIII.2.d) Premier lancement

Au premier lancement de Firefox, vous aurez l'assistant d'importation qui arrive. Cochez la case « Ne rien importer » et cliquez sur le bouton « Suivant » :



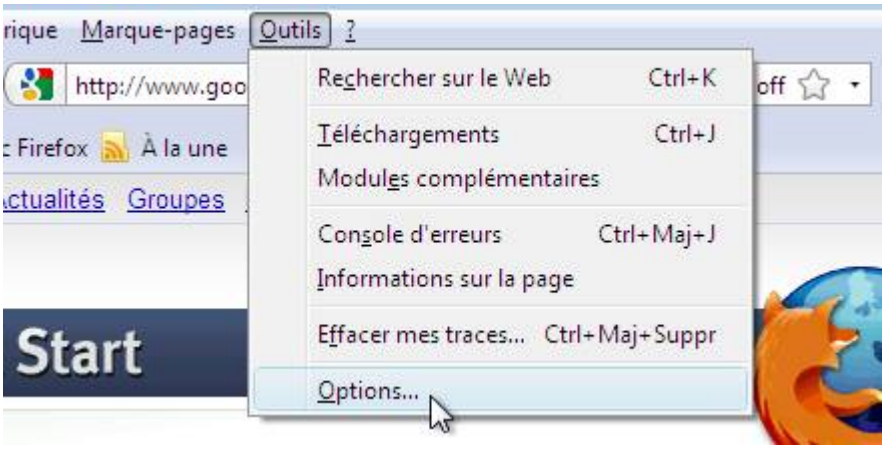
Vous pourrez importer vos favoris ultérieurement (voir section VIII.2.h page 208).

VIII.2.e) Quelques réglages de Firefox

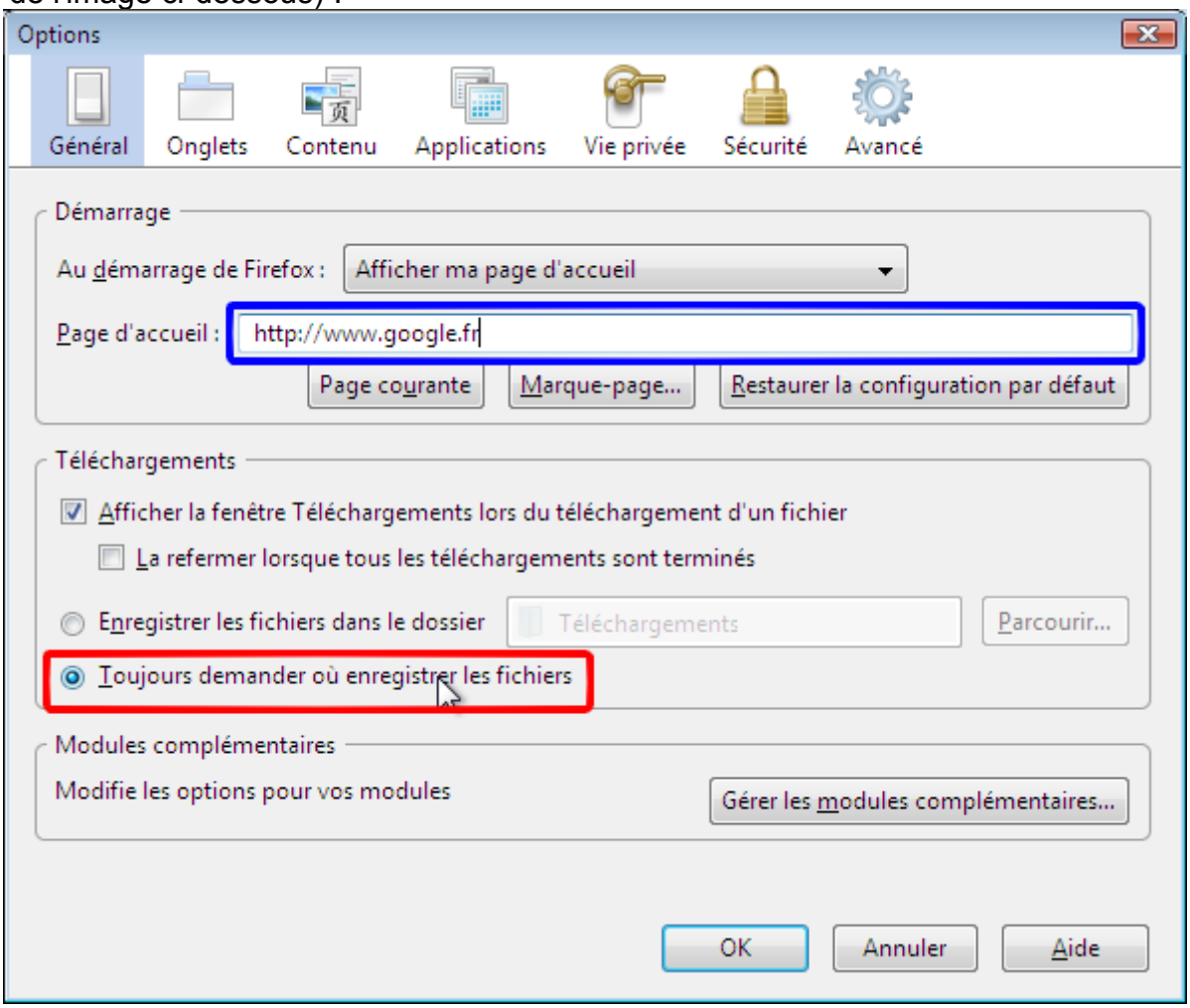
Avant d'installer des extensions pour améliorer Firefox, il faut que nous changions quelques réglages de Firefox qui ne sont pas des plus agréables dans l'état par défaut.

Commençons déjà par demander à Firefox de toujours demander où enregistrer les fichiers que vous téléchargez :

Pour ceci, allez dans le menu « Outils » et ensuite dans « Options » :



Cochez ensuite la case « Toujours demander où enregistrer les fichiers » (voir cadre rouge de l'image ci-dessous) :



Pendant qu'on est encore là, changez la page d'accueil par la page de Google en tapant l'adresse à la main (voir cadre bleu de l'image ci-dessus) car la page originale de Google est mieux que celle façon Firefox (il y a un lien vers Gmail entre autres, ou encore les outils linguistiques). Cliquez ensuite sur OK.

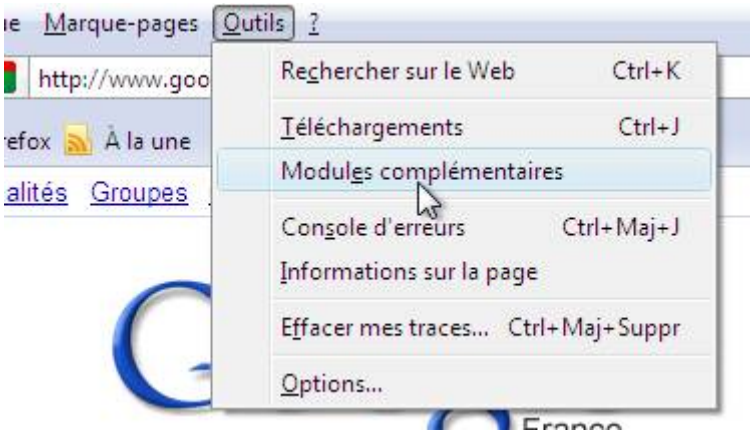
Voici les quelques réglages de base effectués. Installons maintenant quelques extensions afin d'améliorer un peu Firefox :

VIII.2.f) Installation d'extensions utiles

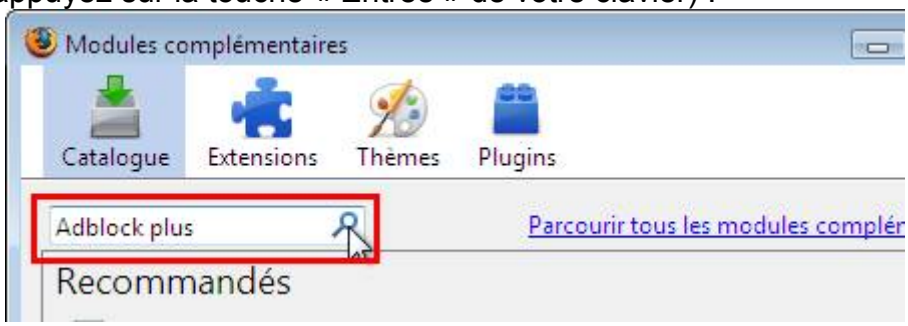
Voyons d'abord comment installer une extension. Ensuite, nous ferons une petite liste d'extensions utiles à installer. Puis nous verrons comment installer une autre extension dont la méthode d'installation n'est pas standard.

VIII.2.f.i) Installation d'extensions – Méthode standard

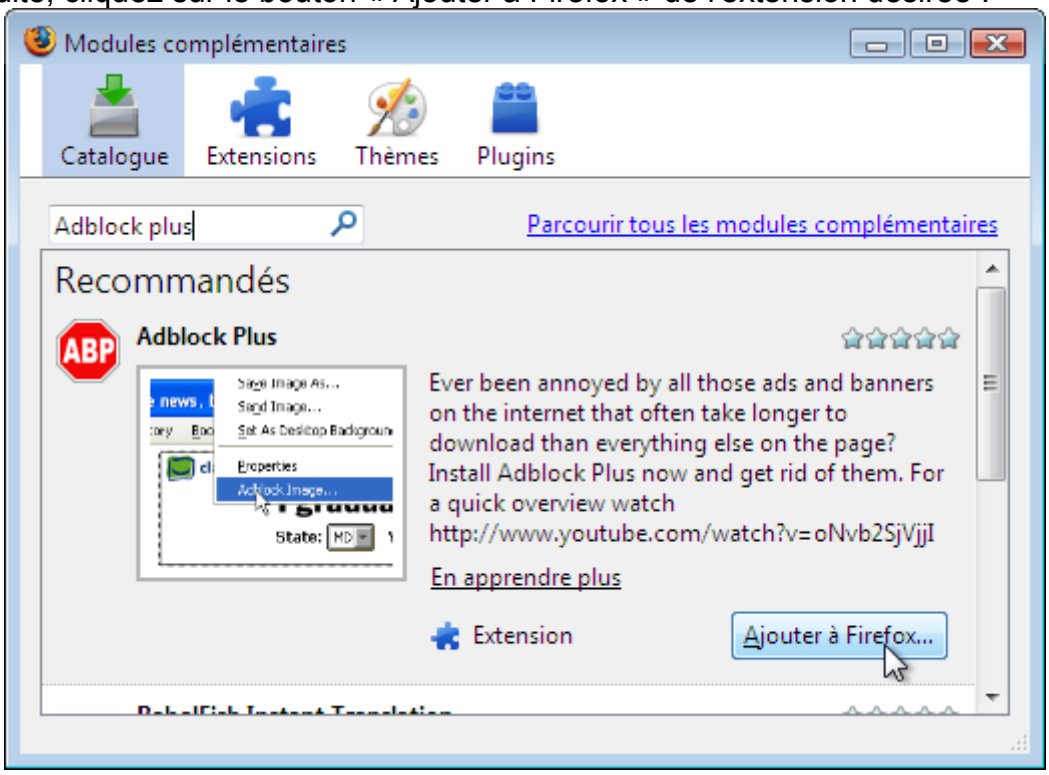
Pour installer une extension, cliquez sur le menu « Outils », et cliquez sur « Modules complémentaires » :



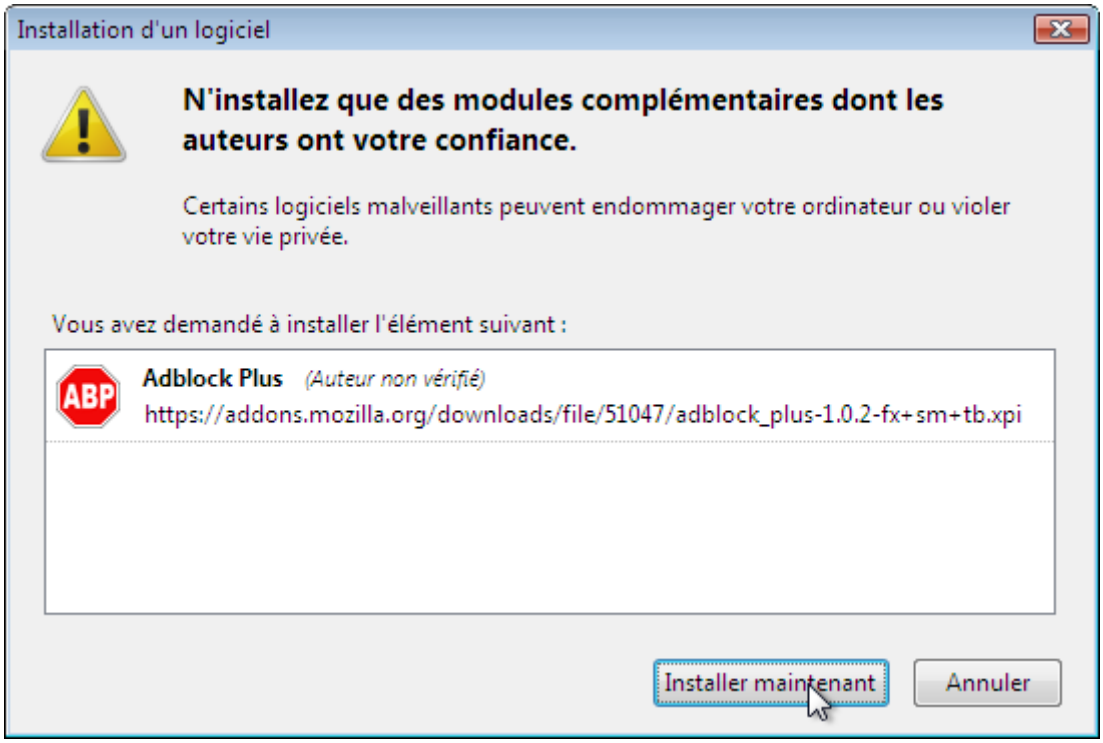
Dans la zone de texte, écrivez le nom de l'extension désirée et cliquez sur la loupe pour rechercher (ou appuyez sur la touche « Entrée » de votre clavier) :



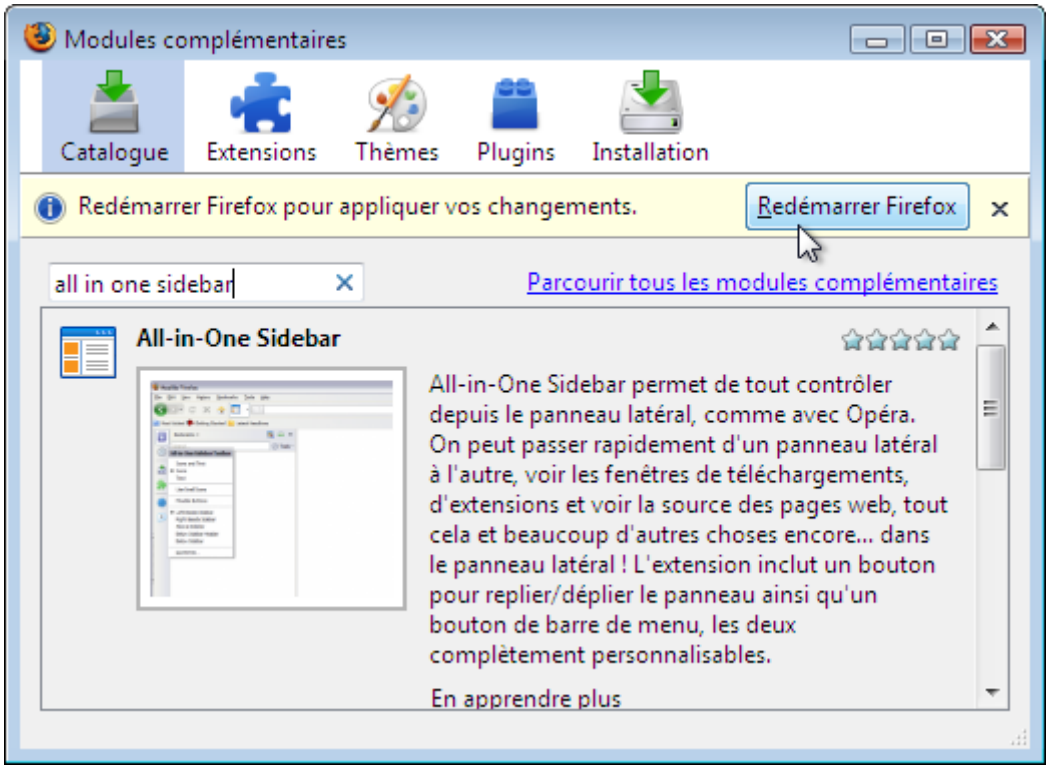
Ensuite, cliquez sur le bouton « Ajouter à Firefox » de l'extension désirée :



Patientez quelques secondes et cliquez sur le bouton « Installer maintenant » :



Répétez l'opération autant de fois que nécessaire pour installer d'autres extensions et cliquez après sue bouton « Redémarrer Firefox » :



VIII.2.f.ii) Liste d'extensions à installer

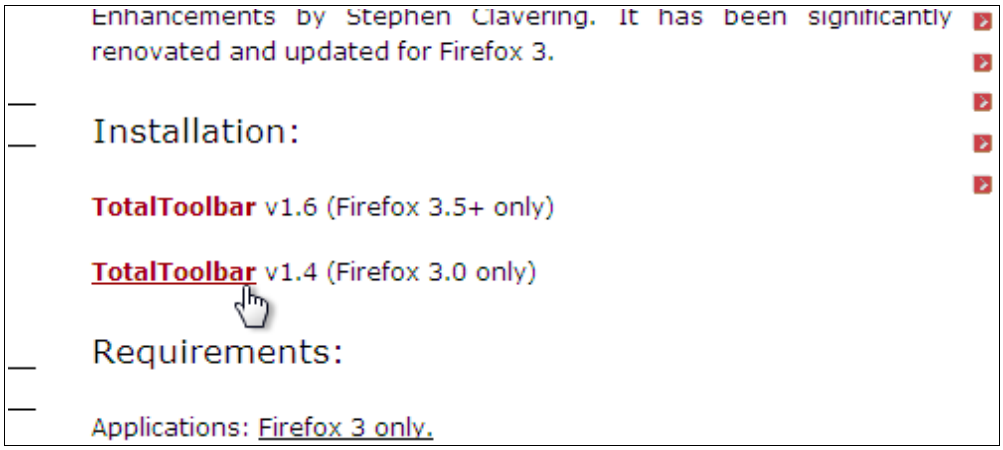
Extension	Fonction	Notes
Adblock Plus	Bloquer de publicité très efficace	
Adblock Plus : Hiding Element Helper	Outil pour rendre encore plus efficace le blocage de publicité	
All in one sidebar	Amélioration de la gestion du panneau latéral	
CustomizeGoogle	Améliore Google	

OpenBook	Permet l'affichage de l'arborescence des marques pages plutôt que les cinq dossiers les plus utilisés.	
Tab mix plus	Améliore la gestion des onglets	
Totaltoolbar	Améliore la gestion des barres d'outils	Utiliser section VIII.2.f.iii pour installer

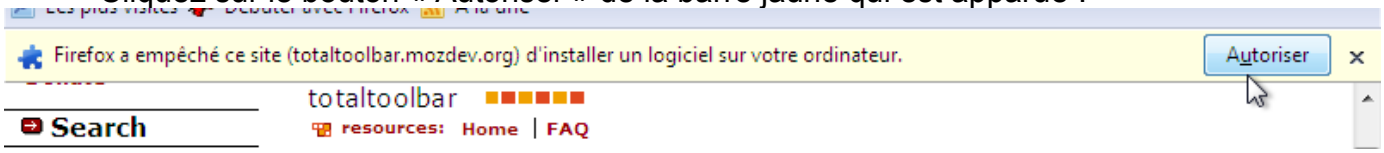
VIII.2.f.iii) Une dernière extension

Cette extension ne s'installe pas comme les autres. Il faut l'installer en allant directement sur le site de cette extension. Il faut donc aller dans Google et chercher « Totaltoolbar » (tout attaché) et trouver cette page :

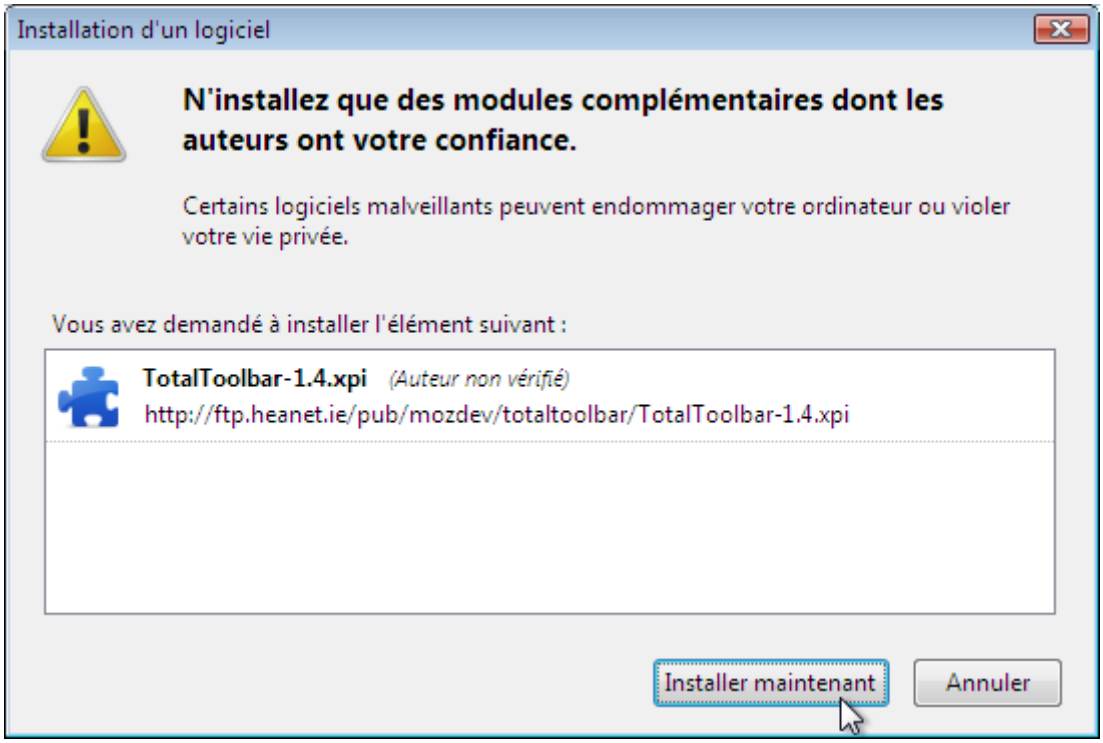
Cliquez sur le deuxième « TotalToolbar » si vous avez Firefox 3, ou cliquez sur le premier si vous avez Firefox 3.5 :



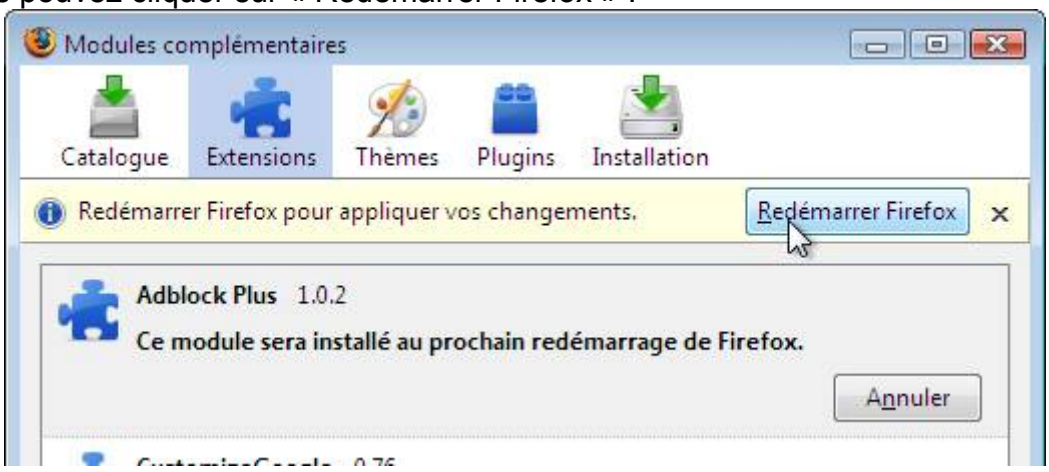
Cliquez sur le bouton « Autoriser » de la barre jaune qui est apparue :



Après quelques secondes d'attentes, vous pourrez cliquer sur le bouton « Installer maintenant » :



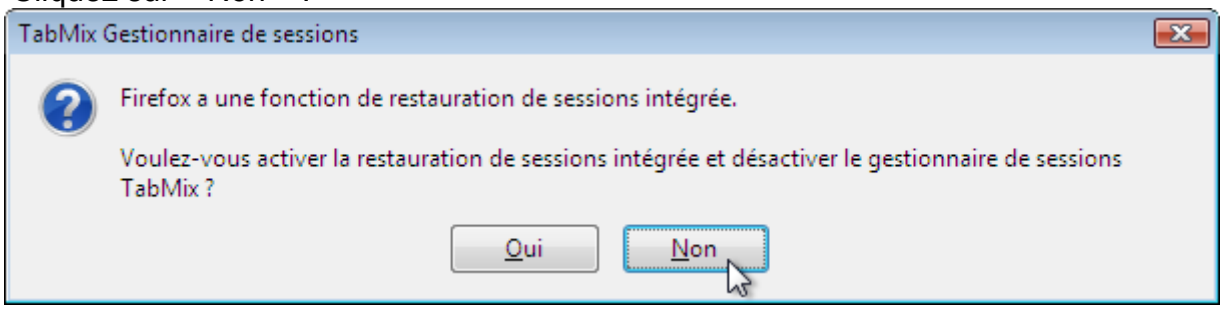
Vous pouvez cliquer sur « Redémarrer Firefox » :



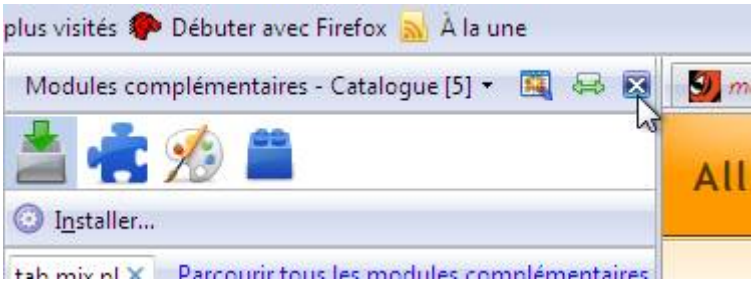
VIII.2.g) Premier lancement et réglages des extensions

Quelques réglages au premier démarrage seront nécessaires.

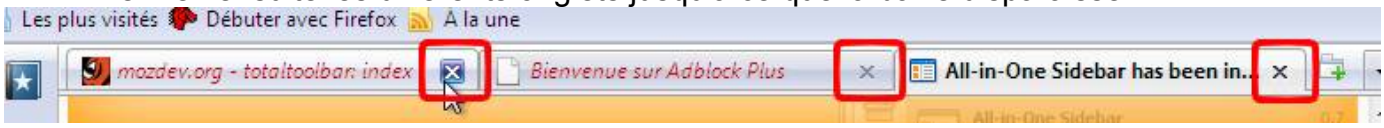
Tout d'abord, on vous demande s'il faut activer ou non la restauration intégrée de Tab Mix Plus. Cliquez sur « Non » :



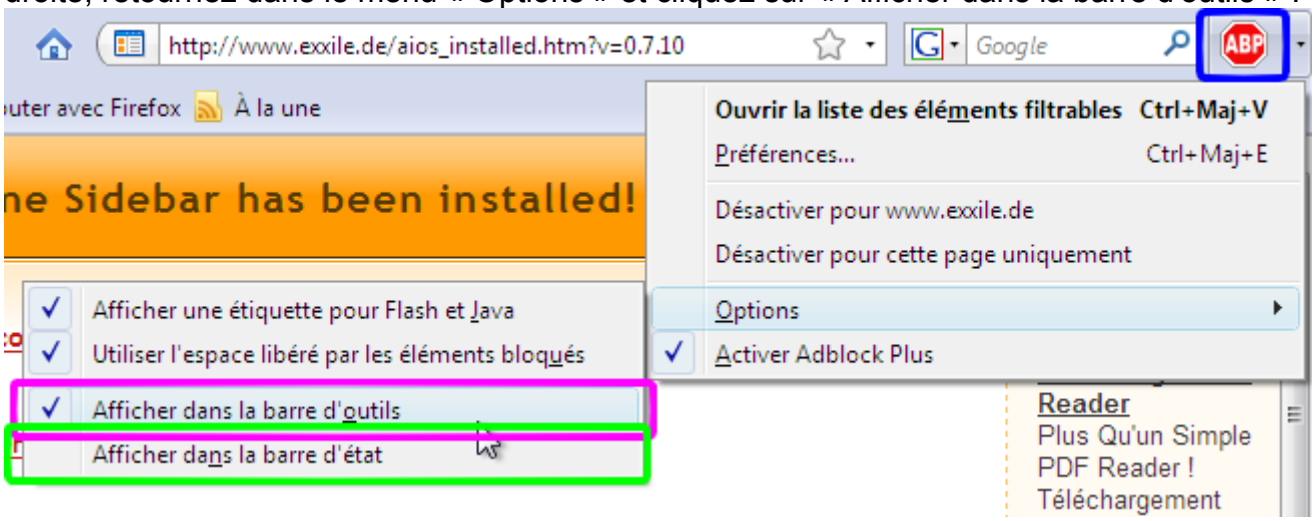
Cliquez sur la croix pour fermer le panneau latéral :



Fermez ensuite les différents onglets jusqu'à ce que la barre disparaisse :

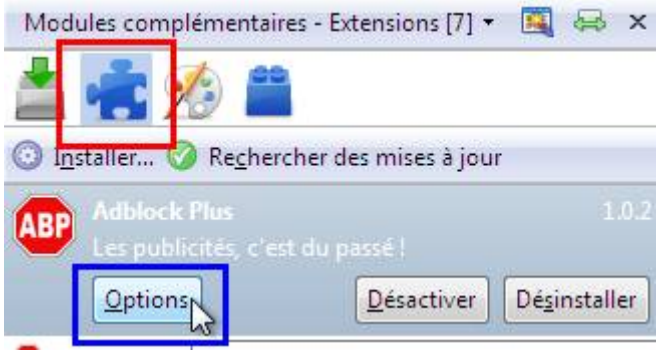


Cliquez ensuite sur le bouton ABP en haut à droite de Firefox, allez dans le menu « Options » et cliquez sur « Afficher dans la barre d'état ». Recliquez sur le bouton ABP en haut à droite, retournez dans le menu « Options » et cliquez sur « Afficher dans la barre d'outils » :

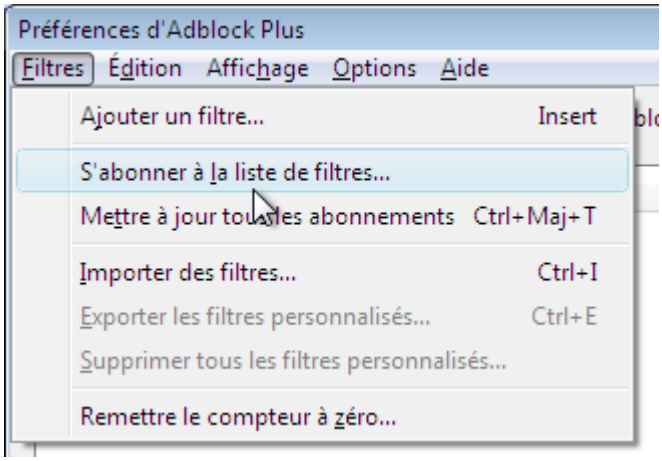


Cliquez sur le bouton des modules complémentaires dans la barre à gauche :

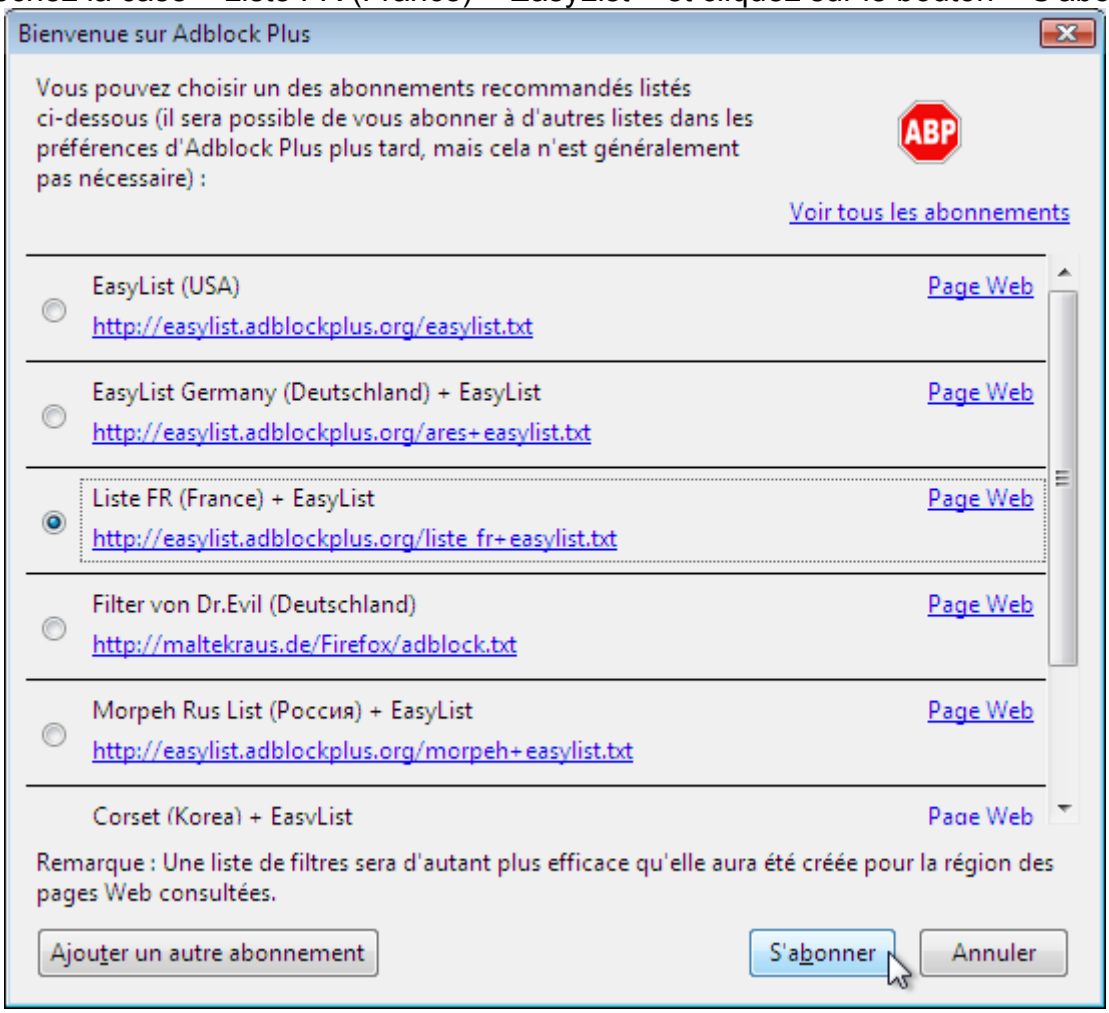
Cliquez sur le bouton « Extensions » (voir cadre rouge de l'image ci-dessous), cliquez sur « Adblock Plus » et cliquez sur le bouton « Options » :



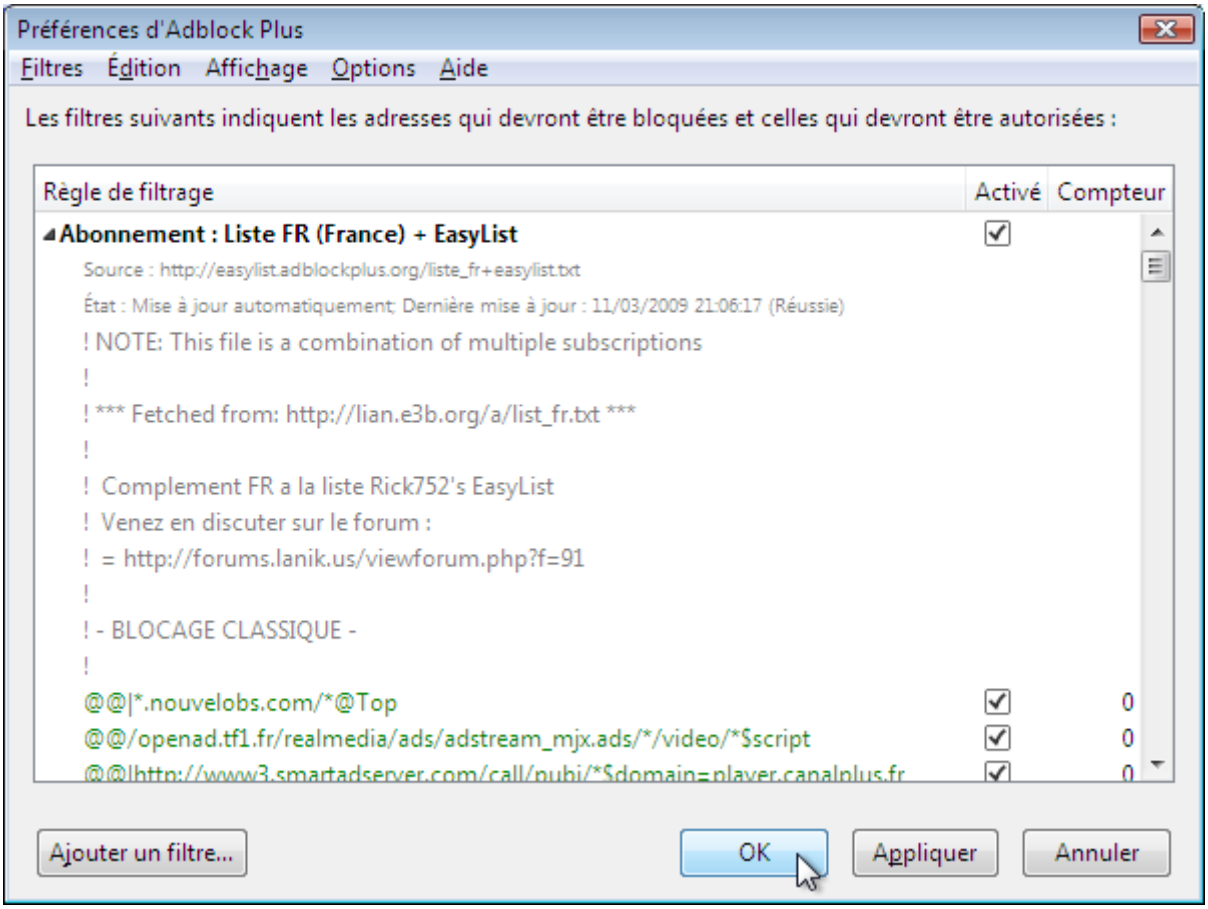
Cliquez sur le menu « Filtres » et cliquez sur « S'abonner à une liste de filtres » :



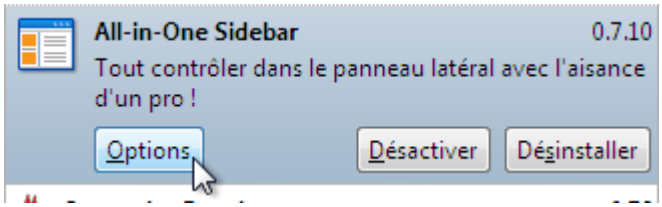
Cochez la case « Liste FR (France) + EasyList » et cliquez sur le bouton « S'abonner » :



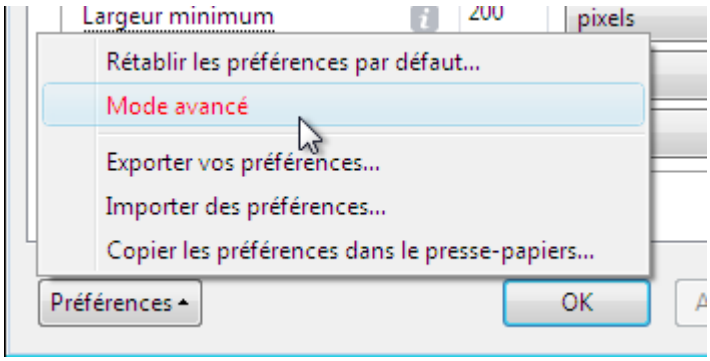
Cliquez sur le bouton « OK » la fenêtre de Adblock plus :



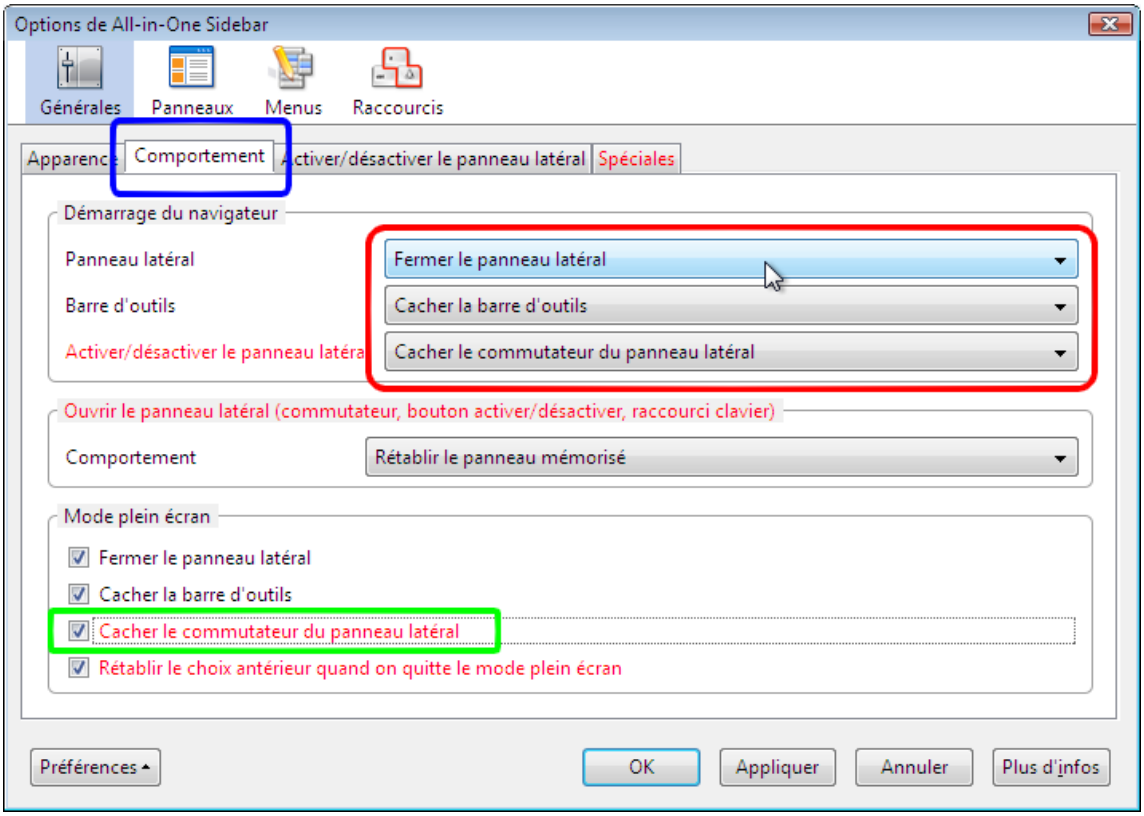
Ensuite, dans la liste, cliquez sur « All-in-one Sidebar » et cliquez sur le bouton « Options » :



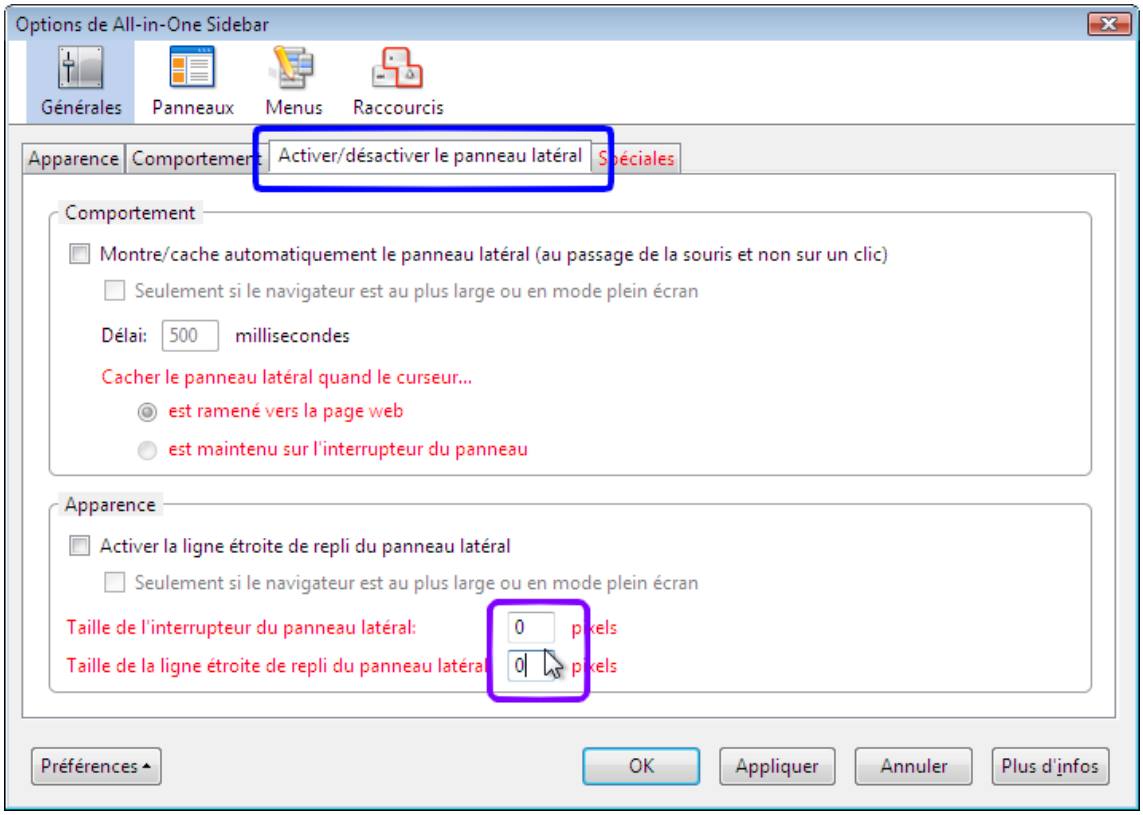
Dans la fenêtre qui apparaît, cliquez sur le bouton « Préférences » et cliquez sur « Mode avancé » :



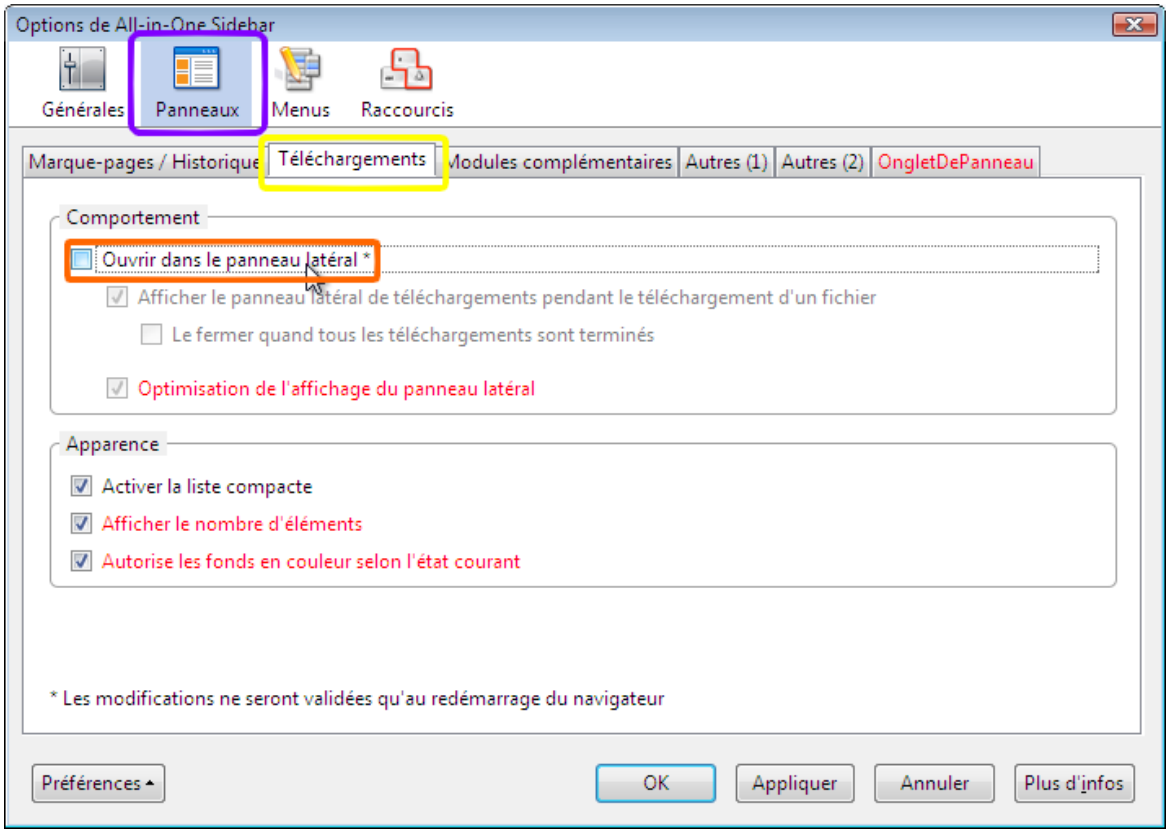
Cliquez sur l'onglet « Comportement », et mettez les trois premiers éléments à « Fermer le panneau latéral », « Cacher la barre d'outils » et « Cacher le commutateur du panneau latéral ». Cochez ensuite la case « Cacher le commutateur du panneau latéral » :



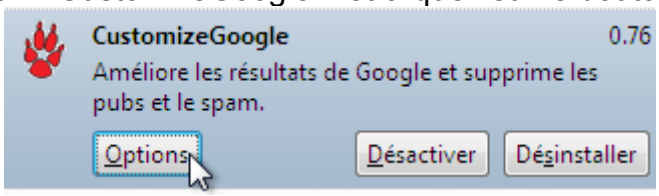
Cliquez ensuite sur l'onglet « Activer/désactiver le panneau latéral » et mettez les deux chiffres à 0 :



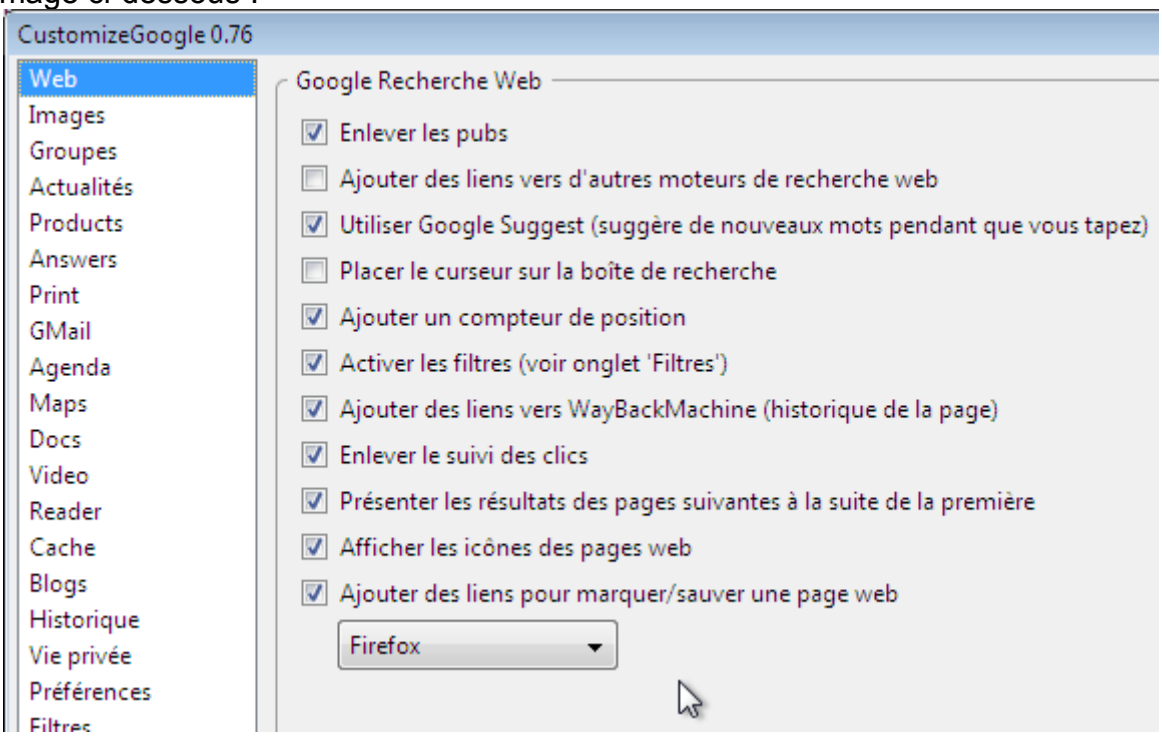
Cliquez ensuite sur « Panneaux », cliquez sur « Téléchargements », décochez la case « Ouvrir dans le panneau latéral » (sinon ça plantera à chaque fois que vous téléchargerez quelque chose : le panneau latéral s'affiche vide ou alors n'actualisera pas le fait que le fichier est en cours de téléchargement) et cliquez sur « OK » :



Ensuite, cliquez sur « CustomizeGoogle » et cliquez sur le bouton « Options » :



Cliquez sur « Web » (à gauche) et cochez/décochez les cases de la même façon que dans l'image ci-dessous :

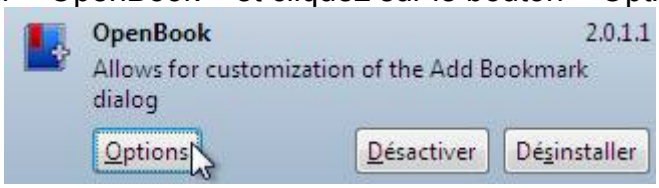


Ensuite, cochez les cases « Enlever les pubs » dans « Groupes », « Products »,

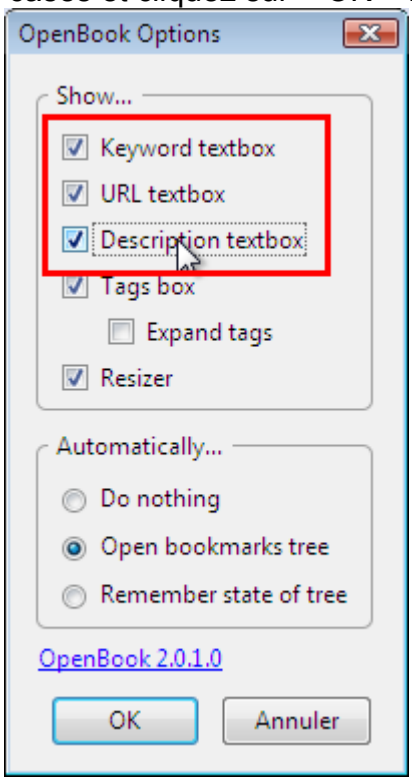
« Answers », « Print », « Gmail » et « Maps ».

Cochez la case « Version sécurisée (passer en https) » dans « Agenda », « Docs », « Reader » et « Historique » et cliquez sur « OK ».

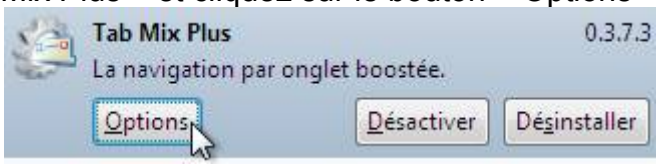
Ensuite cliquez sur « OpenBook » et cliquez sur le bouton « Options » :



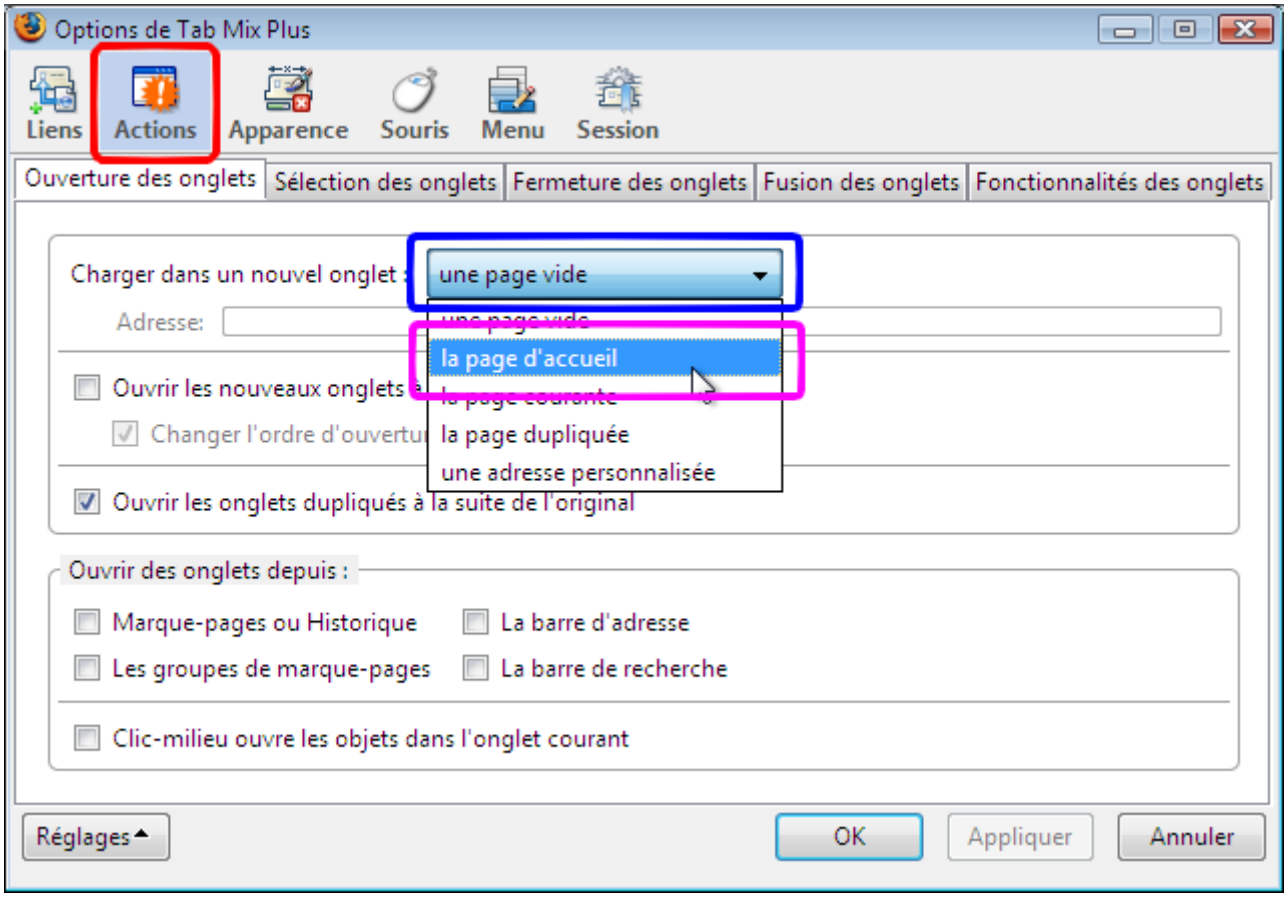
Cochez les trois premières cases et cliquez sur « OK » :



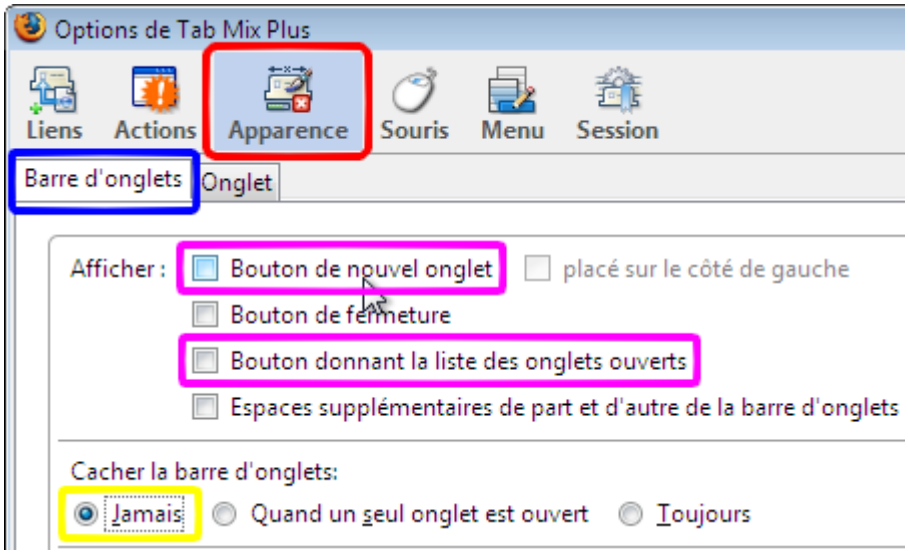
Cliquez sur « Tab Mix Plus » et cliquez sur le bouton « Options » :



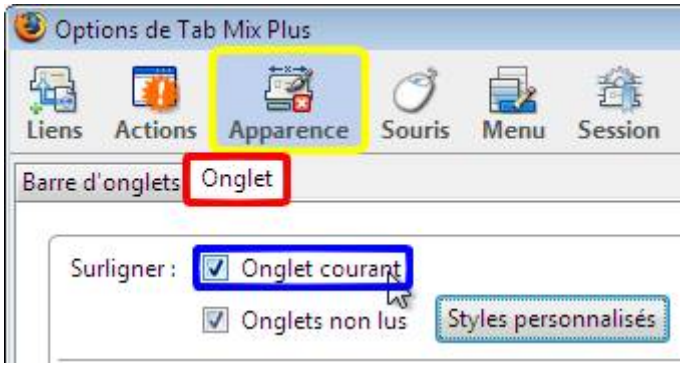
Cliquez sur « Actions », cliquez sur « une page vide » et cliquez sur « la page d'accueil » :



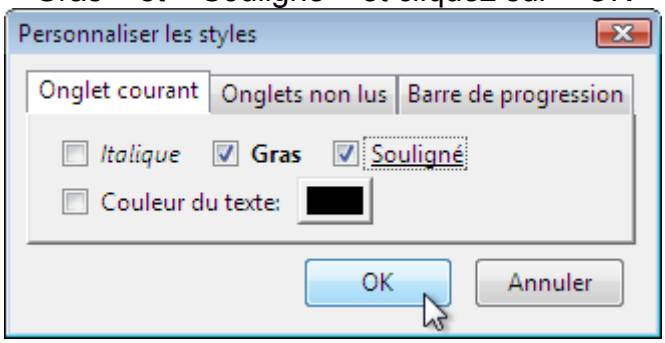
Cliquez sur le bouton « Apparence », cliquez sur « Barre d'onglets », décochez les cases « Bouton de nouvel onglet » et « Bouton donnant la liste des onglets ouverts », et cochez la case « Jamais » :



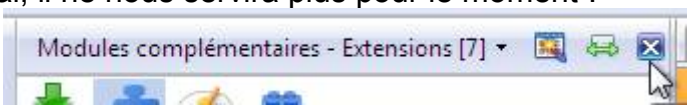
Cliquez ensuite sur « Onglet », cochez la case « Onglet courant » et cliquez sur le bouton « Styles personnalisés » :



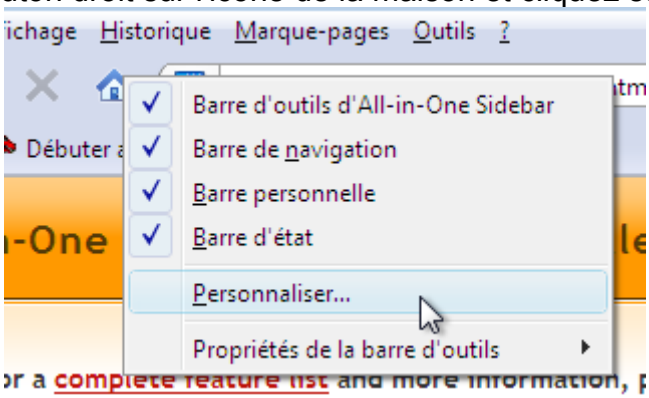
Cochez les cases « Gras » et « Souligné » et cliquez sur « OK » :



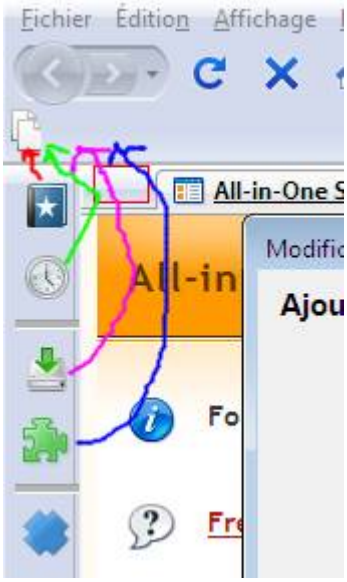
Cliquez sur « OK » pour fermer la fenêtre de réglages de Tab Mix Plus. Vous pouvez fermer le panneau latéral, il ne nous servira plus pour le moment :



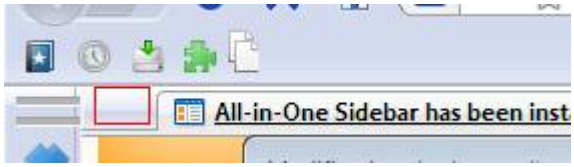
Cliquez avec le bouton droit sur l'icône de la maison et cliquez sur « Personnaliser » :



Ensuite, déplacez les quatre premières icônes de la barre de gauche juste au dessus :

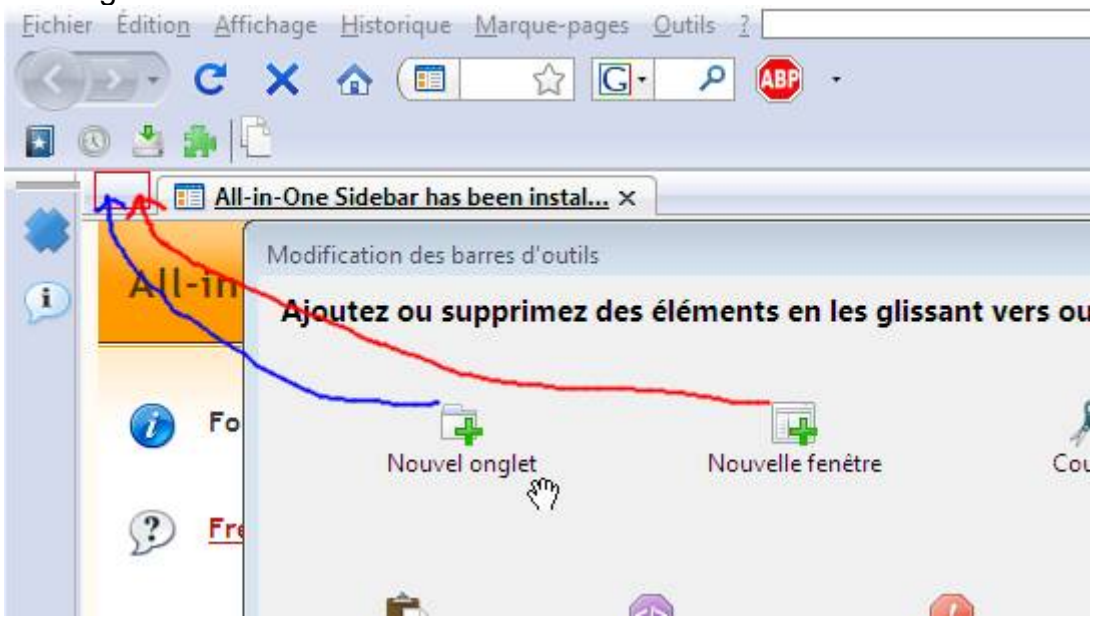


Veillez bien à ce que  soit tout à droite comme ceci :

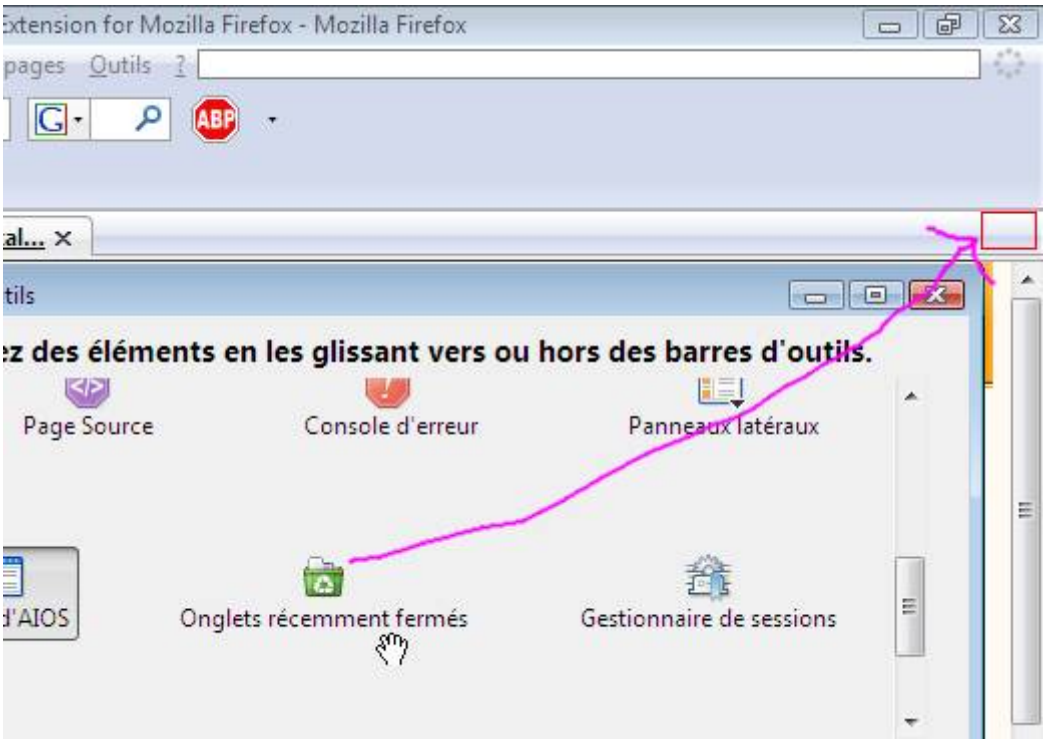


Vous pouvez aussi déplacer un des séparateurs afin de séparer l'icône  de l'icône  comme ceci :

Déplacez ensuite les deux icônes « Nouvel onglet » et « Nouvelle fenêtre » dans le cadre rouge en haut à gauche :

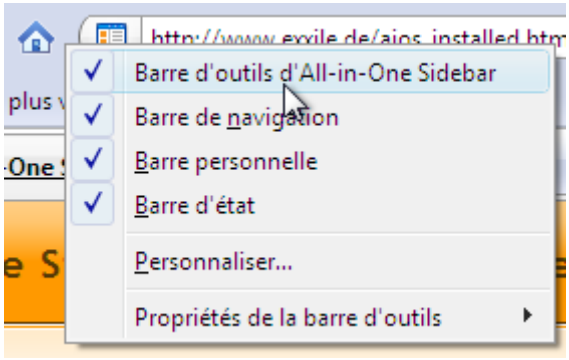


Déplacez ensuite l'icône « Onglets récemment fermés » dans le cadre rouge en haut à droite :



Puis cliquez sur « Terminer ».

Cliquez de nouveau avec le bouton droit sur le bouton avec la petite maison, et cliquez sur « Barre d'outils d'All-in-one sidebar » :



Voilà, les réglages sont terminés !

VIII.2.h) Importation de favoris depuis Internet Explorer

VIII.2.i) Mise à jour du programme

VIII.2.j) Mise à jour des extensions

VIII.3) Mozilla Thunderbird 2

VIII.3.a) Téléchargement

Allez sur cette page : http://www.mozilla-europe.org/fr/products/thunderbird/
Ou utilisez votre moteur de recherche favori pour y accéder :

Dès que la page sera sous vos yeux, cliquez sur le bouton « Téléchargement gratuit et immédiat » :

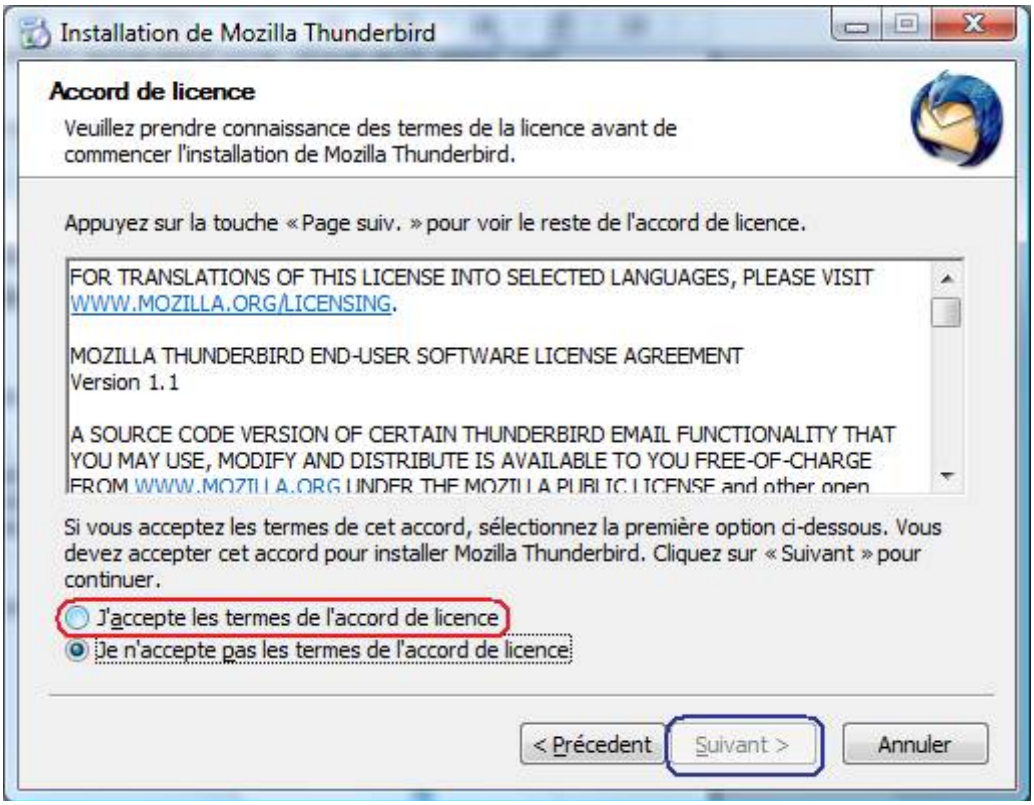
La procédure de téléchargement est ensuite la procédure habituelle de votre navigateur.

VIII.3.b) Installation

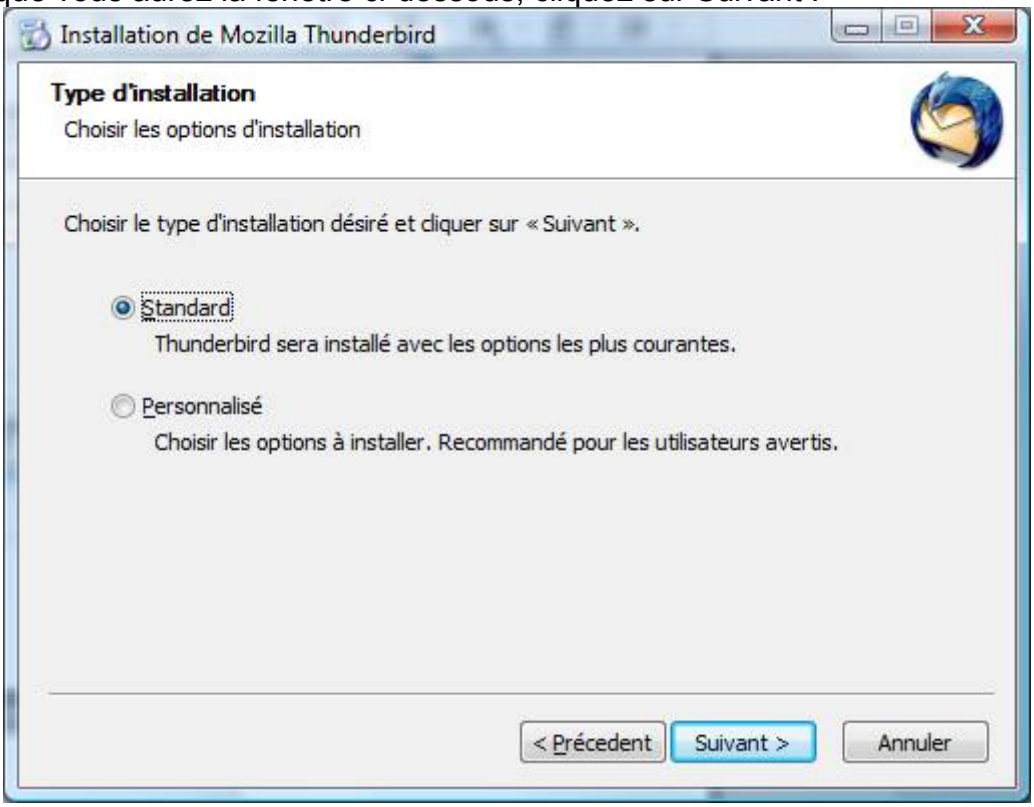
Ouvrez le fichier précédemment téléchargé (fichier qui est en fait le programme d'installation de Thunderbird), une petite fenêtre apparaîtra pour disparaître aussi vite pour laisser place à une fenêtre comme celle ci-dessous.

Lorsque cette fenêtre apparaît, cliquez sur le bouton Suivant.

Cochez la case « J'accepte les termes du contrat de licence » et cliquez sur le bouton Suivant.



Lorsque vous aurez la fenêtre ci-dessous, cliquez sur Suivant :



Thunderbird commence à s'installer.
Dès qu'il aura finit, cette fenêtre apparaîtra :

Décochez la case « Lancer Mozilla Thunderbird maintenant » et cliquez sur le bouton « Terminer ».

VIII.3.c) Création d'un profil

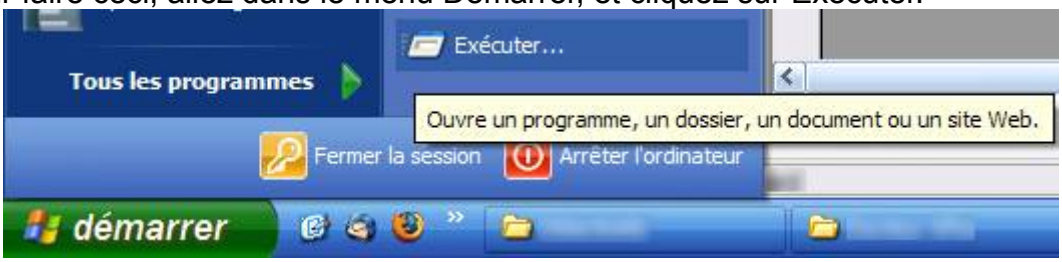
Petite explication sur les profils : un profil sous Thunderbird, c'est ce qui contiendra vos mails, vos réglages, vos mots de passe de messagerie, ...

Le fait de créer un profil est donc nécessaire. Par défaut, Thunderbird en crée un, mais le place à un endroit tel qu'en cas de problèmes (formatage, ...), il risque d'être oublié lorsque vous voudrez sauvegarder vos documents.

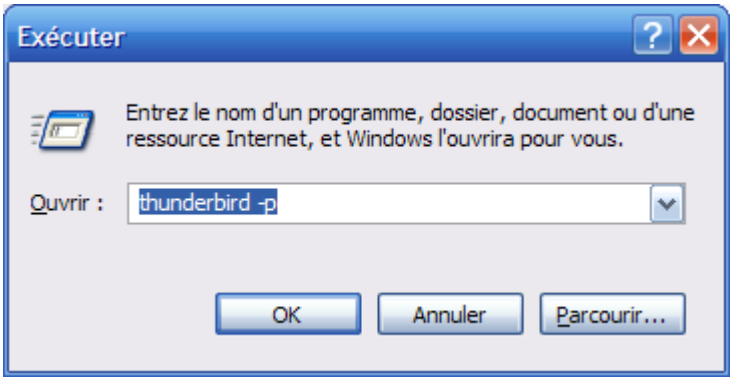
L'idée de cette étape est donc de créer un profil, mais dans le dossier « Mes documents », dossier qui a moins de risque d'être oublié, lui.

Sous Windows XP et antérieurs :

Pour faire ceci, allez dans le menu Démarrer, et cliquez sur Exécuter.

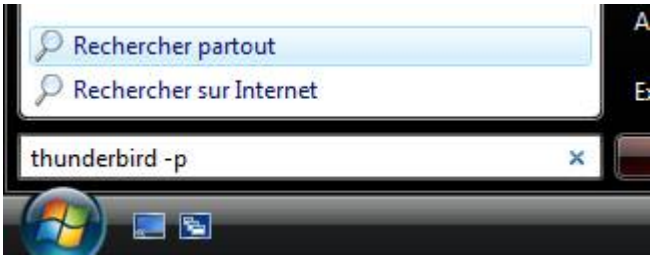


Dans cette fenêtre Exécuter, écrivez « thunderbird -p » (sans les guillemets) et cliquez sur OK.

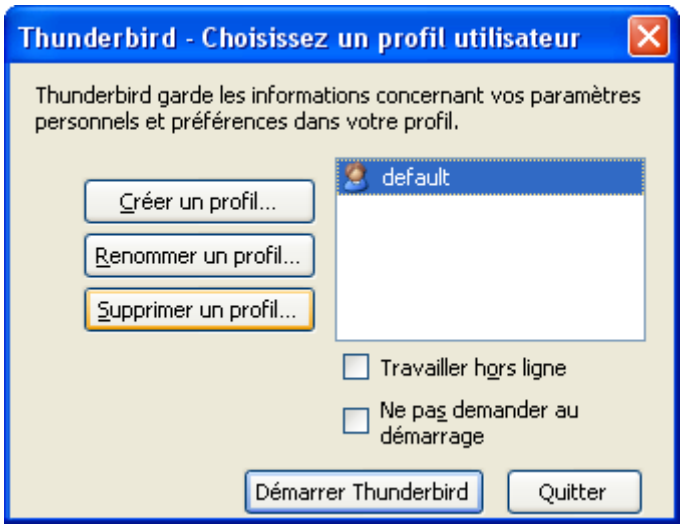


Sous Windows Vista et ultérieurs :

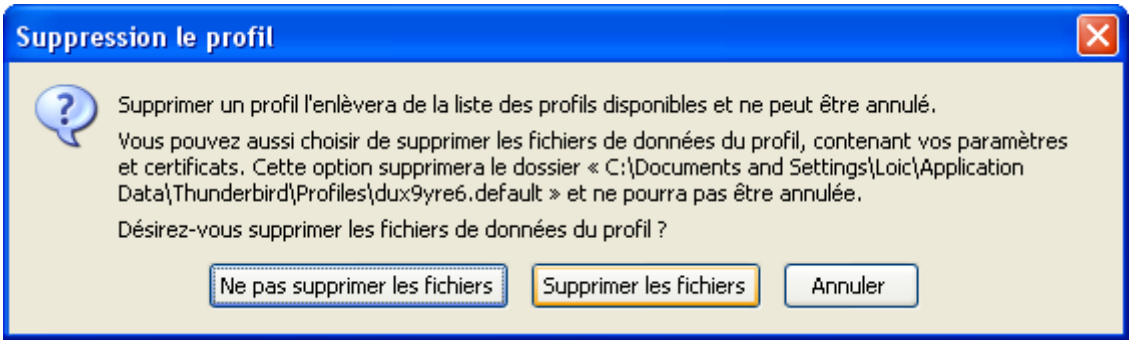
Cliquez sur votre bouton « Démarrer » et dans la zone de recherche, tapez « thunderbird -p » et appuyez sur la touche Entrée de votre clavier.



Quelque soit votre version de Windows, une petite fenêtre apparaît avec une liste des profils existants.

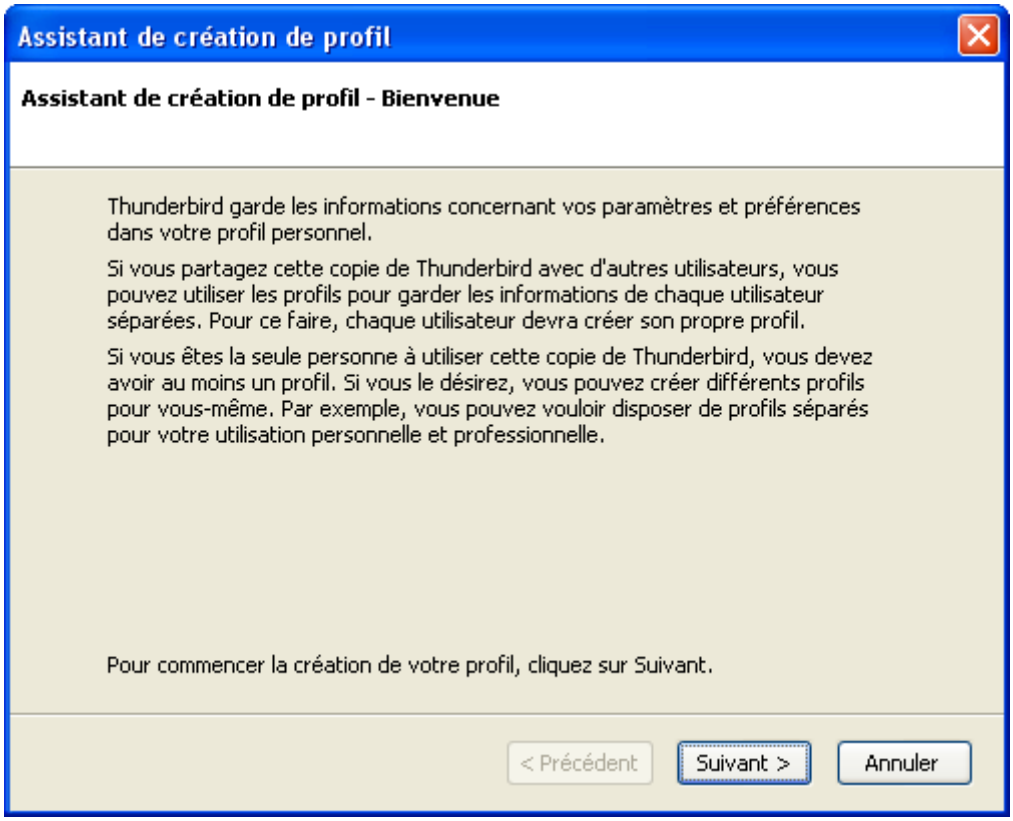


On va supprimer le profil par défaut et en créer un autre. Cliquez sur « default » puis cliquez sur le bouton « Supprimer un profil ».

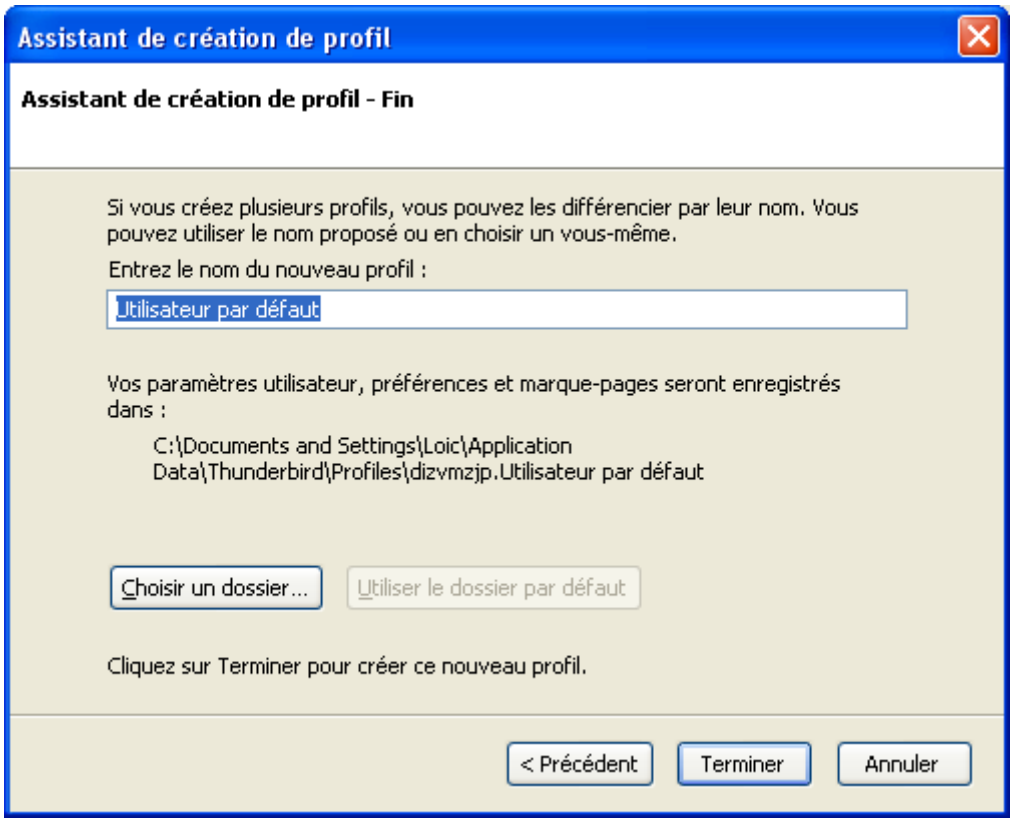


Cliquez sur le bouton « Supprimer les fichiers ».

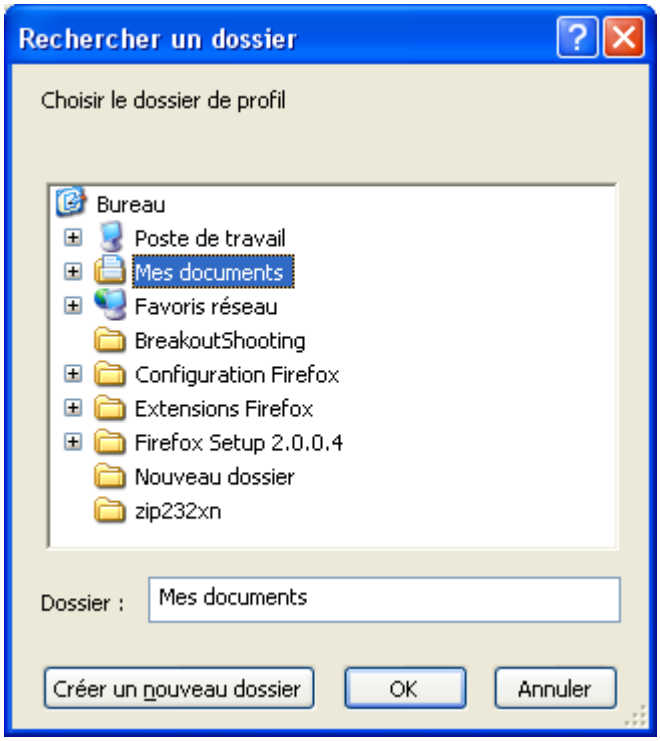
Cliquez ensuite sur le bouton « Créer un profil ».



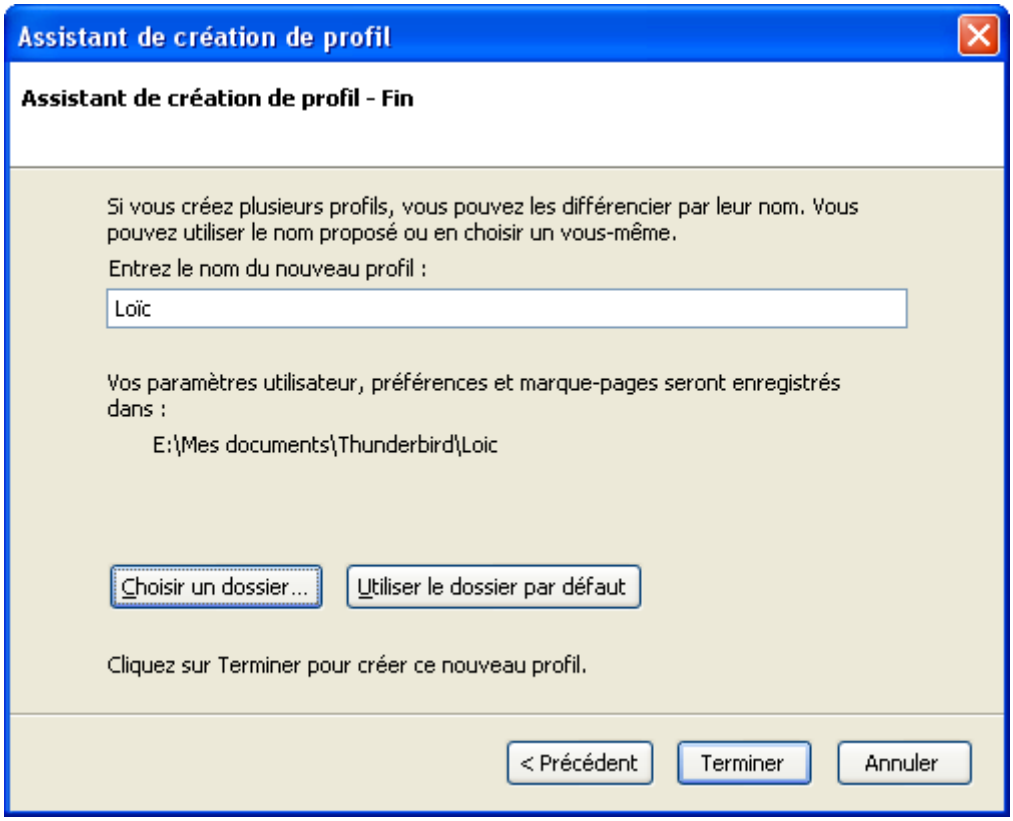
Cliquez sur Suivant.



Changez le texte « Utilisateur par défaut » par le nom que vous voulez donner à votre profil (de préférence votre prénom dans le cas ou plusieurs personnes utiliseront Thunderbird sur votre bureau Windows). Cliquez ensuite sur le bouton « Choisir un dossier ».



Cliquez sur le dossier « Mes documents » puis cliquez sur le bouton « Créer un nouveau dossier » (dans le cas de Windows Vista, via cette fenêtre, allez dans le dossier ayant votre nom d'utilisateur, et allez ensuite dans le dossier « Documents » et cliquez sur le bouton « Créer un nouveau dossier »). Nommez ce nouveau dossier « Thunderbird ». Puis cliquez sur ce dossier Thunderbird, et cliquez de nouveau sur le bouton « Créer un nouveau dossier ». Nommez le dossier avec le nom que vous avez donné au profil (pas obligatoire, mais comme vous doutez surement, ça sera plus pratique dans le cas ou il y aurait plusieurs profils).

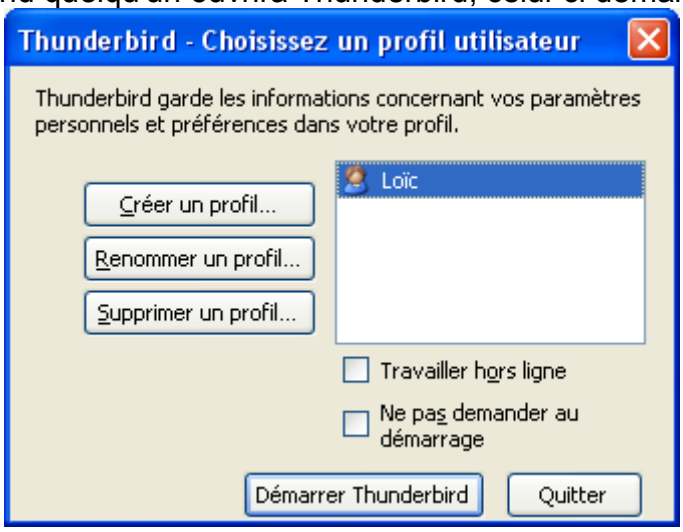


L'emplacement de votre profil devrait être écrit en clair sur la fenêtre, cliquez ensuite sur le bouton Terminer.

Répétez l'opération de création de profil autant de fois que le nombre de personnes

utilisant Thunderbird sur votre bureau Windows.

Si vous avez créé plusieurs profils, décochez la case « Ne pas demander au démarrage ». Ainsi, quand quelqu'un ouvrira Thunderbird, celui-ci demandera quel profil ouvrir.



VIII.3.d) Téléchargement d'extensions utiles

Les extensions sont de petits programmes qui permettent d'améliorer Thunderbird. Nous en téléchargerons un petit nombre (qui dépendra de vos besoins).

Il n'y a pas une seule et unique façon de télécharger une extension. Nous verrons donc comment télécharger des extensions sur deux sites différents. Pour celles qui ne se téléchargeraient pas de manière standard parmi la liste ci-dessous, l'explication sera donnée dans la partie Erreur : source de la référence non trouvée (page Erreur : source de la référence non trouvée).

Il existe une méthode permettant d'installer plein d'extensions en même temps. Donc il vaut mieux que vous téléchargiez tous les fichiers au même endroit.

VIII.3.d.i) Liste des extensions

Nom	Fonction	Endroit où télécharger
Bcc button	Ajouter un bouton pour envoyer un e-mail en copie cachés invisible dans le panneau de contacts lorsque vous écrivez un message	Section Erreur : source de la référence non trouvée Page Erreur : source de la référence non trouvée
Contacts Sidebar	Ajouter un panneau dans la fenêtre principale pour accéder rapidement aux contacts (à la façon de Outlook Express)	Mozilla ou Geckozone
CuteMenus - Crystal SVG	Ajouter des icônes aux menus de Thunderbird. Totalement inutile, donc indispensable. A éviter sur des PC un peu anciens qui auraient une tendance naturelle à planter.	Mozilla ou Geckozone
Delete Junk Context Menu	Ajouter une option permettant de vider les dossier d'indésirables d'un simple clic.	Mozilla ou Geckozone
Dictionnaire Myspell en	Thunderbird intègre un correcteur orthographique, mais il ne lui manque qu'un dictionnaire pour vous	Mozilla ou Geckozone

français	corriger. Le télécharger permet d'utiliser la correction orthographique.	
ImportExportTools	Ajouter des fonctions d'importation et d'exportation de messages dans différents formats dont l'EML	Section Erreur : source de la référence non trouvée Page Erreur : source de la référence non trouvée
MailTagger	Permet d'agrémenter vos messages de nombreux smileys à la façon de ce que permet Incredimail	Mozilla ou Geckozone
MinimizeToTray	Cette extension permet de réduire Thunderbird à côté de l'horloge. Il est ainsi plus discret et continue de vous avertir de l'arrivée de nouveaux messages	Mozilla ou Geckozone
MoreFunctionsForAdressBook	Ajoute des fonctions à votre carnet d'adresses	Section Erreur : source de la référence non trouvée Page Erreur : source de la référence non trouvée
QuickText	Permet d'insérer des morceaux de textes ou de code HTML (permet par exemple d'insérer facilement des signatures complexes).	Mozilla

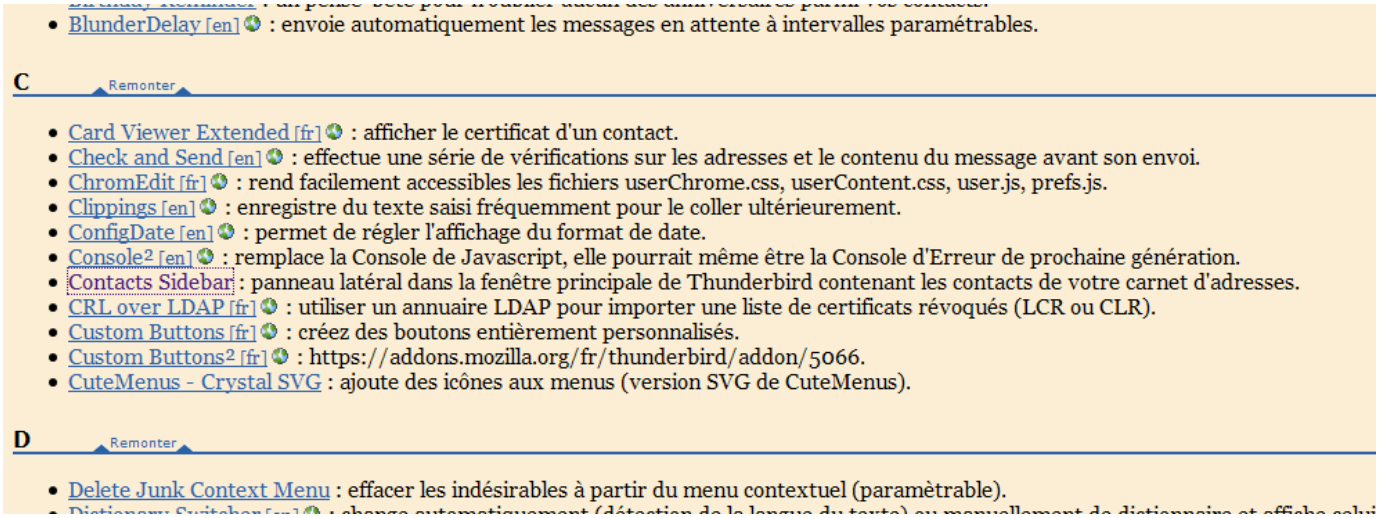
VIII.3.d.ii) Méthode sur Geckozone

Allez sur le site Geckozone : http://www.geckozone.org

Ou utilisez Google pour accéder au site.

Passez la souris au dessus de « Extensions » (sans cliquer), puis cliquez sur « Thunderbird ».

Recherchez l'extension désirée dans la liste et cliquez dessus :



- BlunderDelay [en] : envoie automatiquement les messages en attente à intervalles paramétrables.

C Remonter

- Card Viewer Extended [fr] : afficher le certificat d'un contact.
- Check and Send [en] : effectue une série de vérifications sur les adresses et le contenu du message avant son envoi.
- ChromEdit [fr] : rend facilement accessibles les fichiers userChrome.css, userContent.css, user.js, prefs.js.
- Clippings [en] : enregistre du texte saisi fréquemment pour le coller ultérieurement.
- ConfigDate [en] : permet de régler l'affichage du format de date.
- Console² [en] : remplace la Console de Javascript, elle pourrait même être la Console d'Erreur de prochaine génération.
- Contacts Sidebar : panneau latéral dans la fenêtre principale de Thunderbird contenant les contacts de votre carnet d'adresses.
- CRL over LDAP [fr] : utiliser un annuaire LDAP pour importer une liste de certificats révoqués (LCR ou CLR).
- Custom Buttons [fr] : créez des boutons entièrement personnalisés.
- Custom Buttons² [fr] : https://addons.mozilla.org/fr/thunderbird/addon/5066.
- CuteMenus - Crystal SVG : ajoute des icônes aux menus (version SVG de CuteMenus).

D Remonter

- Delete Junk Context Menu : effacer les indésirables à partir du menu contextuel (paramètrable).

Cliquez sur le lien « Télécharger [le nom de l'extension] pour Thunderbird » (il se peut qu'il y ait plusieurs liens de téléchargement car il existe des extensions valables pour Firefox et Thunderbird, dans ce cas, cliquez sur le lien ayant l'icône de Thunderbird) :

Vous pouvez aussi utiliser le moteur de recherche en haut à droite de la page :

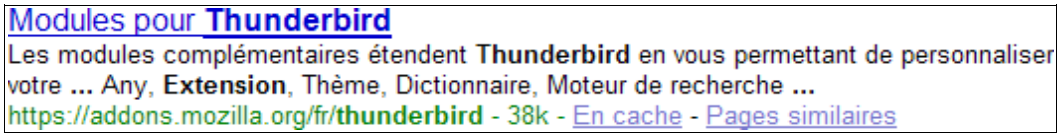
Appuyez sur la touche « Entrée » de votre clavier pour valider la recherche.

Cliquez sur le résultat le plus proche de ce que vous cherchiez.

La page qui apparaitra est celle qui contient le lien de téléchargement de l'extension.

VIII.3.d.iii) Méthode sur le site officiel

Entrez « extensions thunderbird » et trouvez ce résultat :



Allez à cette page.

Tapez le nom de l'extension désirée en haut de la page (voir cadre rouge de l'image ci-dessous) et appuyez sur la touche « Entrée » de votre clavier (par exemple ici, « Contact Sidebar ») :

Cliquez ensuite sur le bouton « Télécharger » et enregistrez le fichier proposé.

VIII.3.d.iv) Autres modules

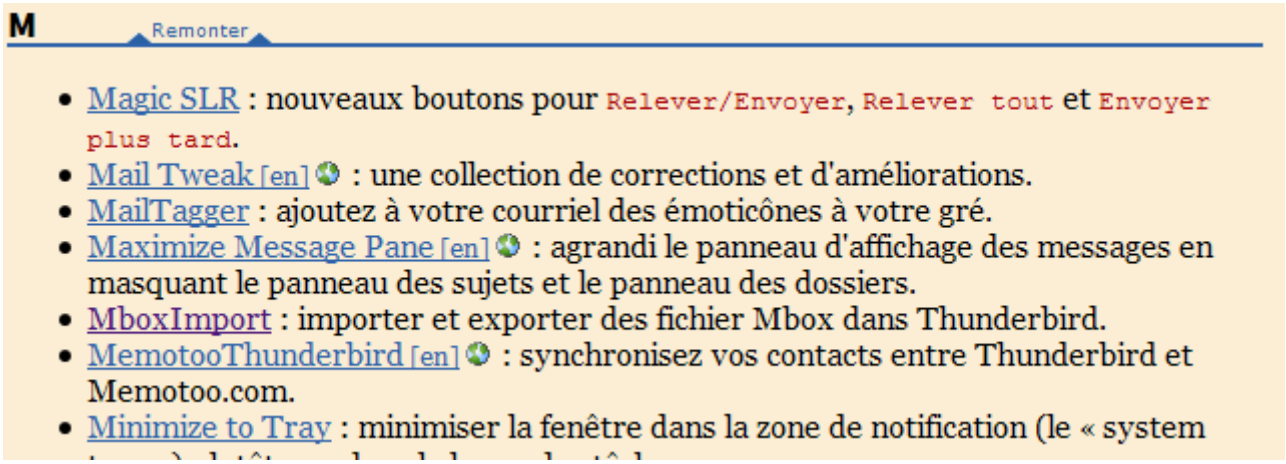
VIII.3.d.iv.1) ImportExportTools

Allez sur le site Geckozone : http://www.geckozone.org

Ou utilisez Google pour accéder au site.

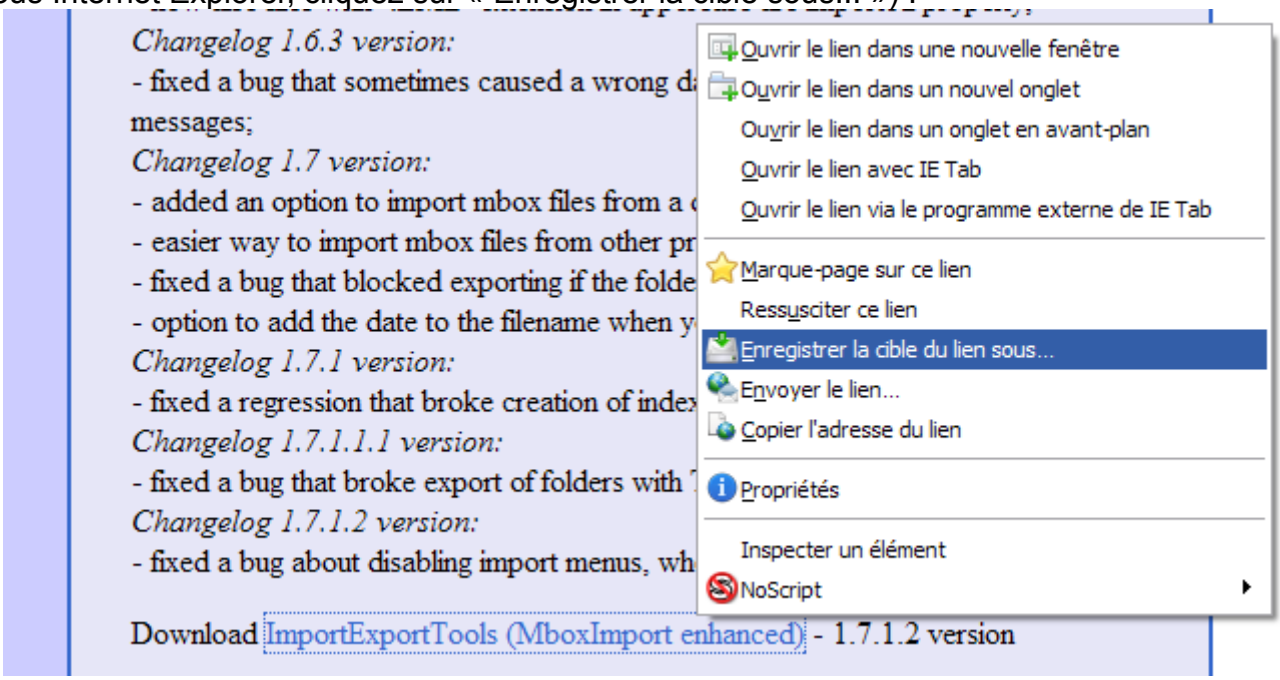
Passez la souris au dessus de « Extensions » (sans cliquer), puis cliquez sur « Thunderbird ».

Cliquez sur « MboxImport » (c'est l'ancien nom de cette extension).



Cliquez sur « Télécharger MboxImport sur le site officiel ».

Allez en fin de page et cliquez ensuite sur « ImportExportTools (MboxImport enhanced) » avec le bouton droit de la souris. Cliquez sur « Enregistrer la cible du lien sous » (pour Firefox, sous Internet Explorer, cliquez sur « Enregistrer la cible sous... ») :



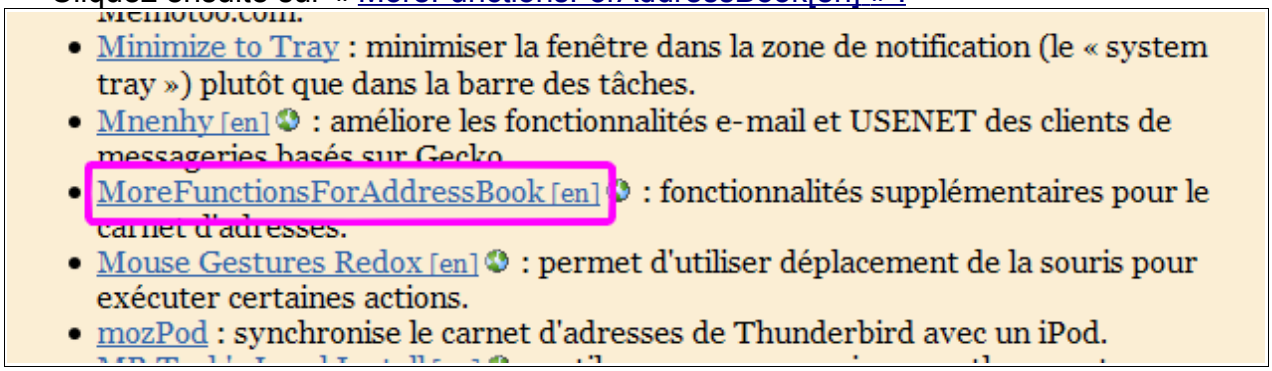
Enregistrez le fichier proposé.

VIII.3.d.iv.2) MoreFunctionsForAddressBook

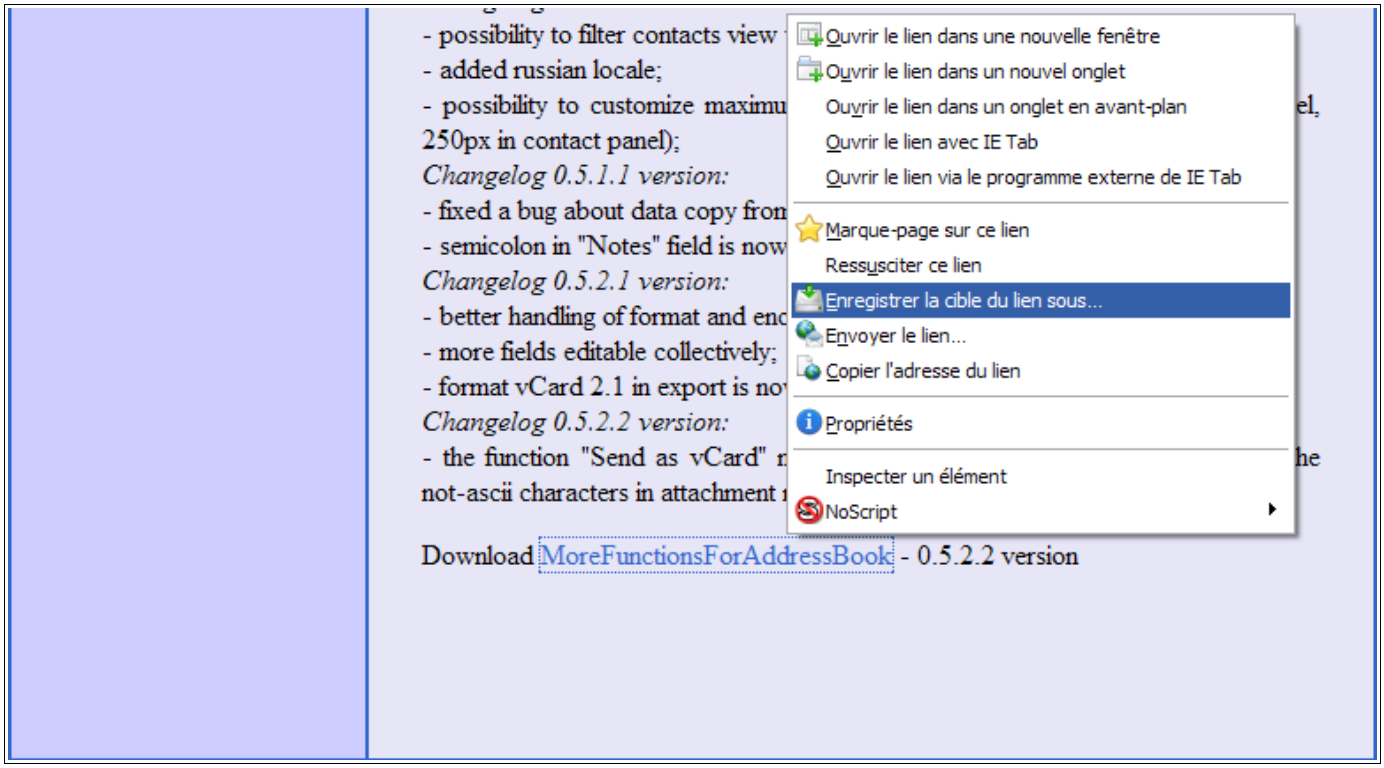
Allez sur le site Geckozone : http://www.geckozone.org
Ou utilisez Google pour accéder au site.

Passez la souris au dessus de « Extensions » (sans cliquer), puis cliquez sur « Thunderbird ».

Cliquez ensuite sur « MoreFunctionsForAddressBook[en] » :



Allez tout en bas de la page, cliquez avec le bouton droit sur « MoreFunctionsForAddressBook », puis cliquez ensuite sur « Enregistrer la cible du lien sous... » (Ceci pour Mozilla Firefox, sous Internet Explorer, cliquez sur « Enregistrer la cible sous... ») :



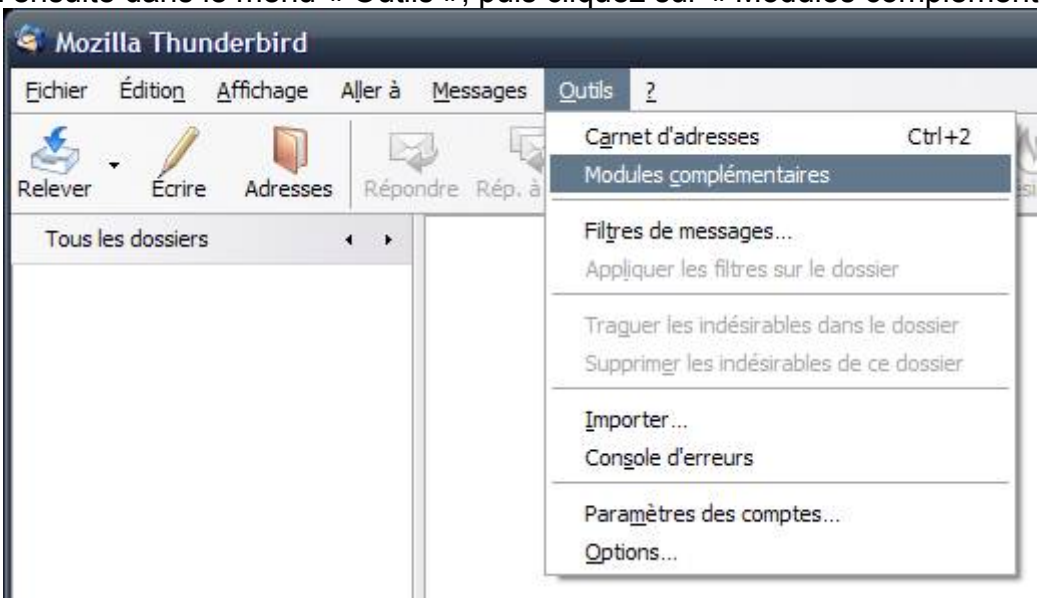
Enregistrez ensuite le fichier proposé.

VIII.3.e) Installation de ces extensions

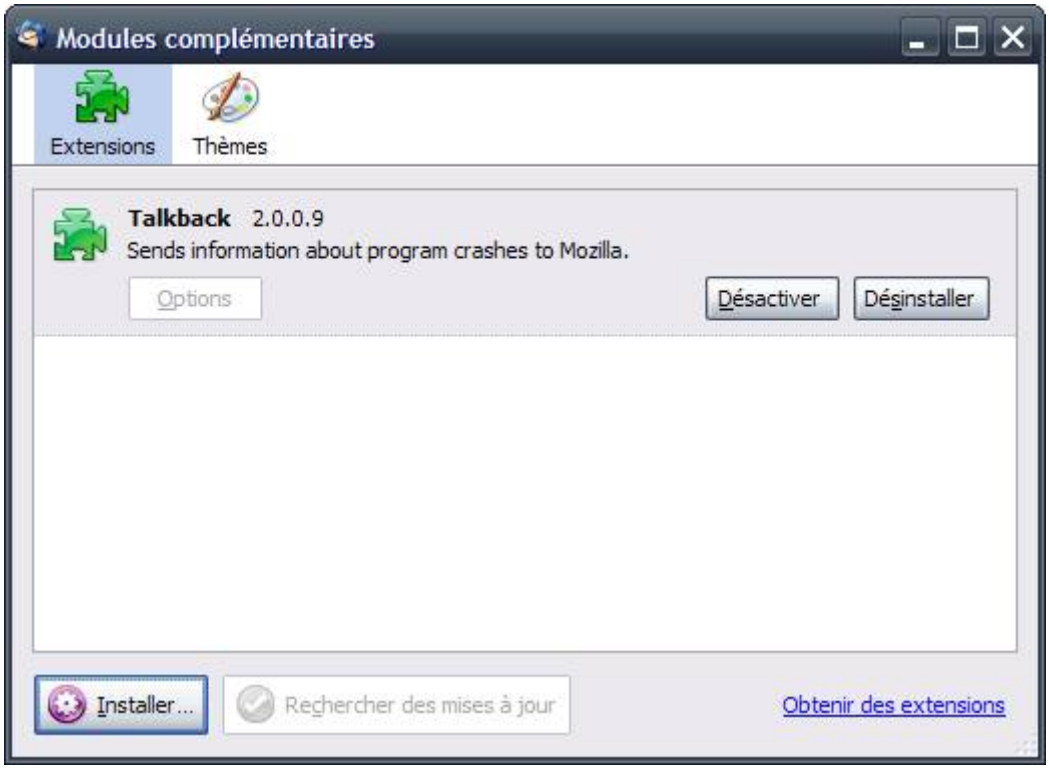
VIII.3.e.i) Installer une seule extension

S'il n'est pas déjà ouvert, ouvrez Thunderbird.

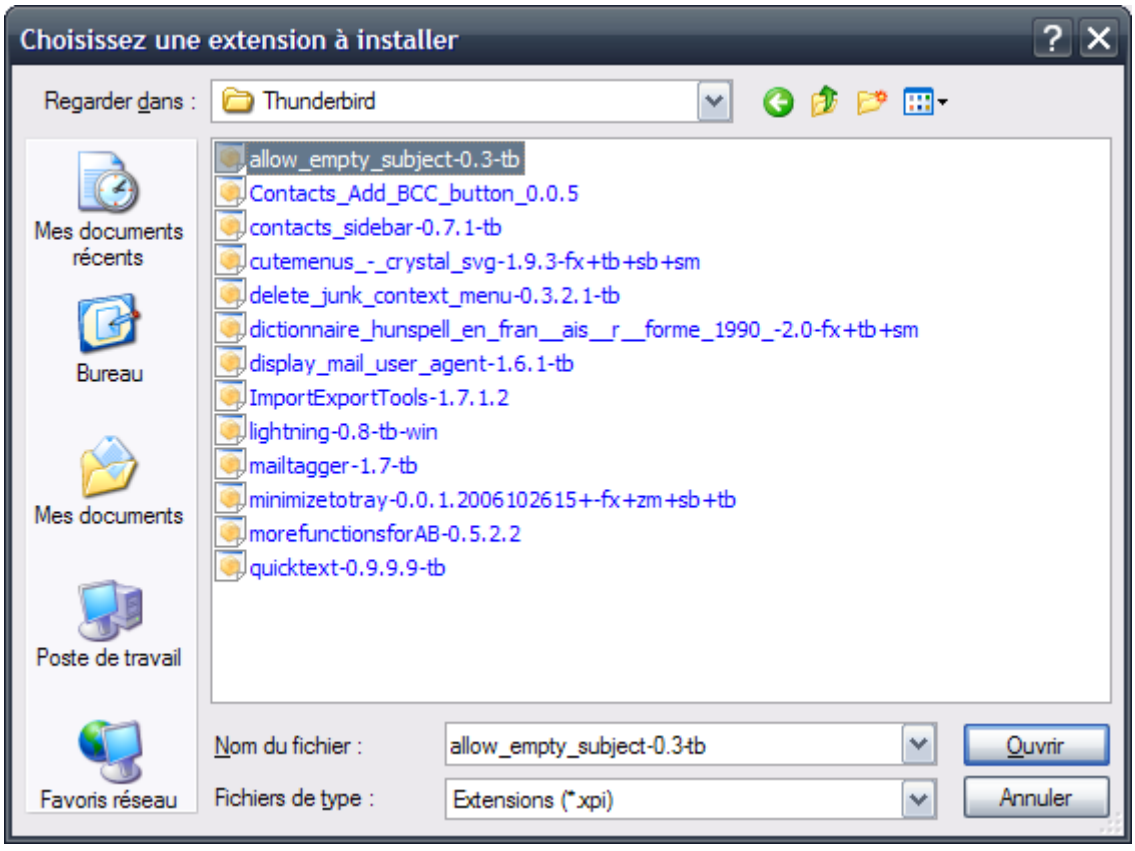
Allez ensuite dans le menu « Outils », puis cliquez sur « Modules complémentaires » :



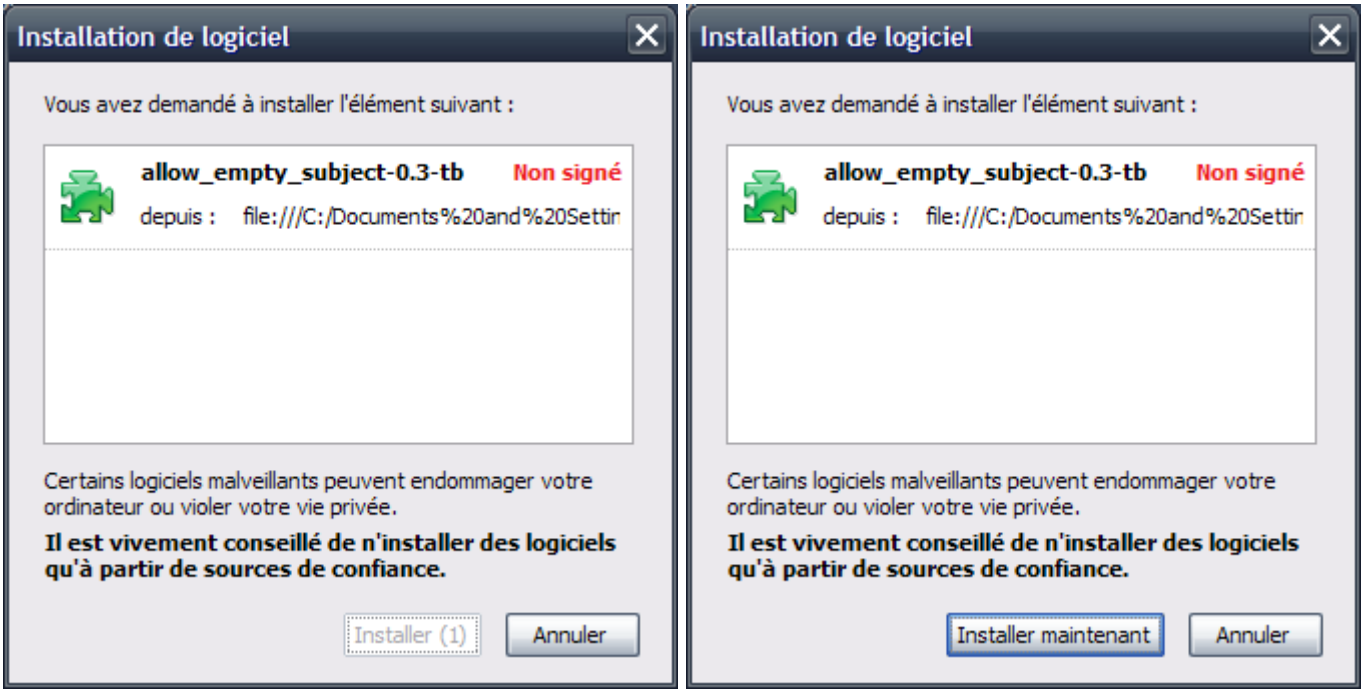
Cliquez sur le bouton « Installer » :



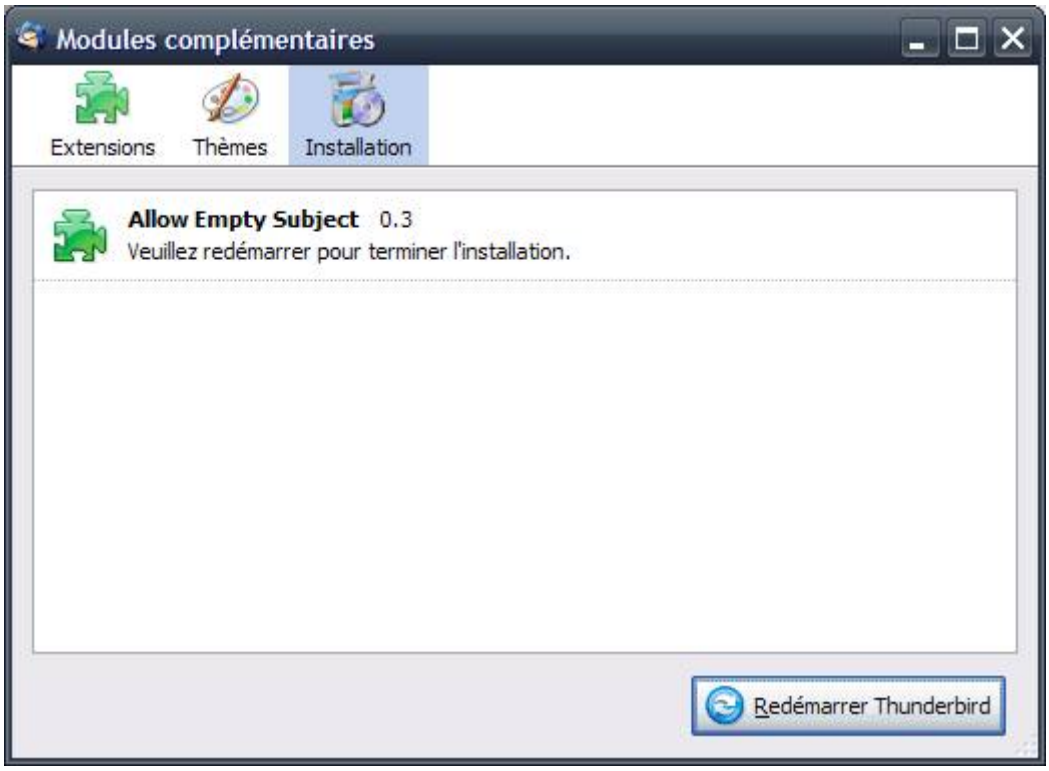
Cherchez l'extension à l'endroit où vous l'avez téléchargée et cliquez sur le bouton « Ouvrir » :



Patientez quelques secondes, et cliquez sur le bouton « Installer maintenant » :



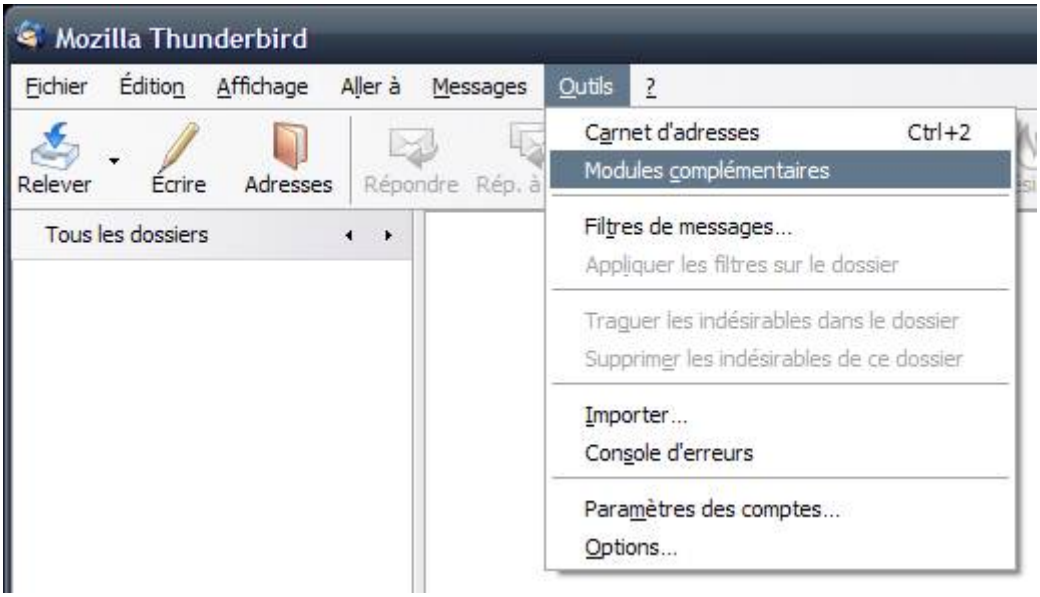
Cliquez ensuite sur le bouton « Redémarrer Thunderbird » :



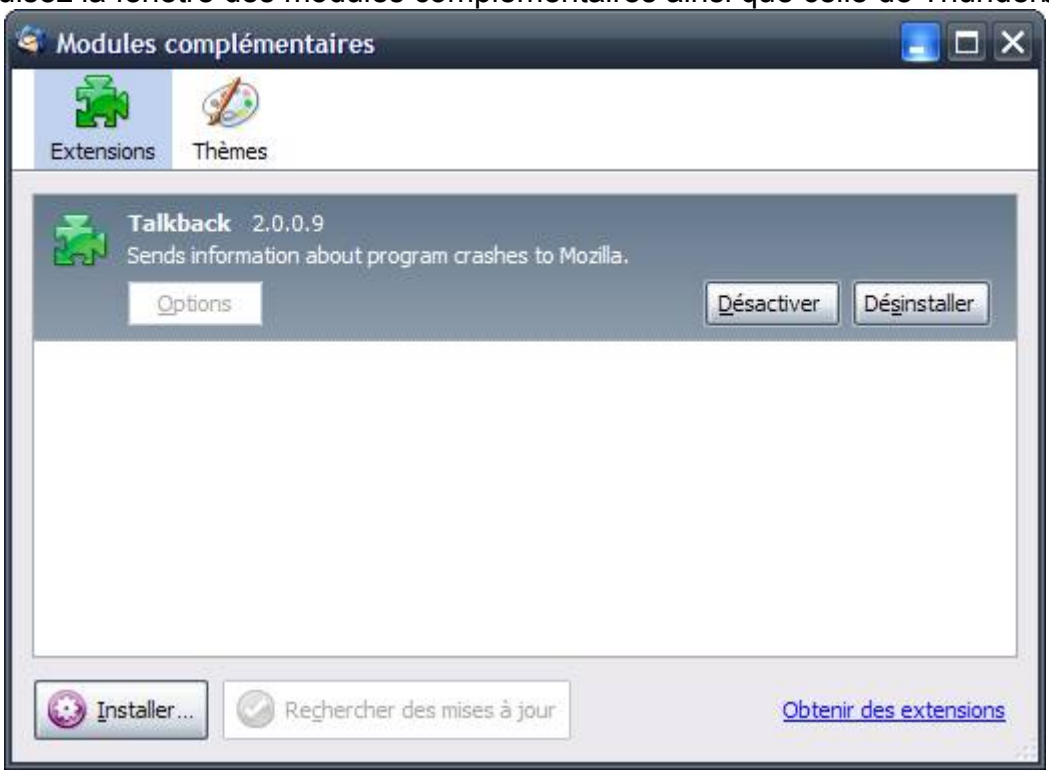
L'extension sera installée au redémarrage de Thunderbird.

VIII.3.e.ii) Installer plusieurs extensions

S'il n'est pas déjà ouvert, ouvrez Thunderbird.
Allez ensuite dans le menu « Outils », puis cliquez sur « Modules complémentaires » :

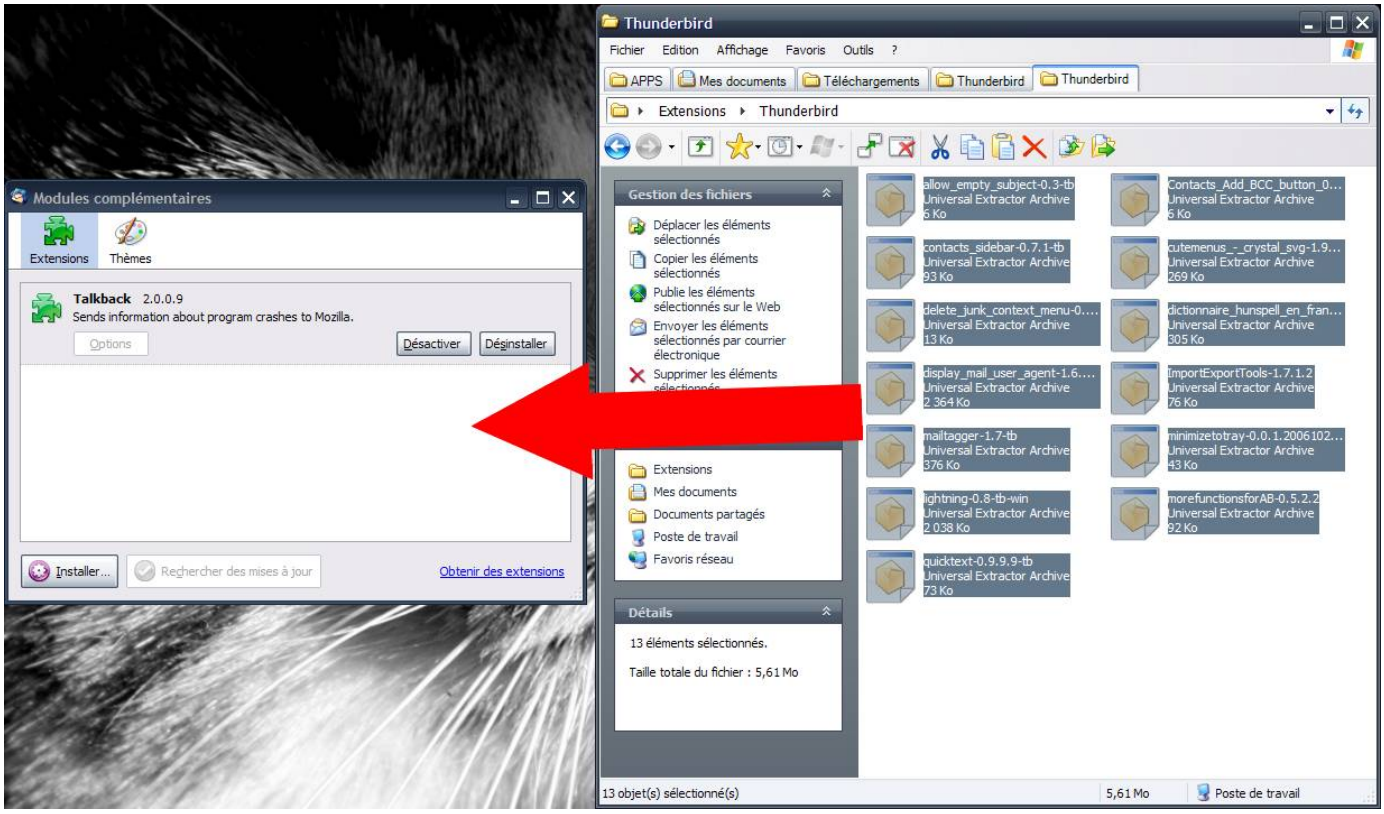


Réduisez la fenêtre des modules complémentaires ainsi que celle de Thunderbird.

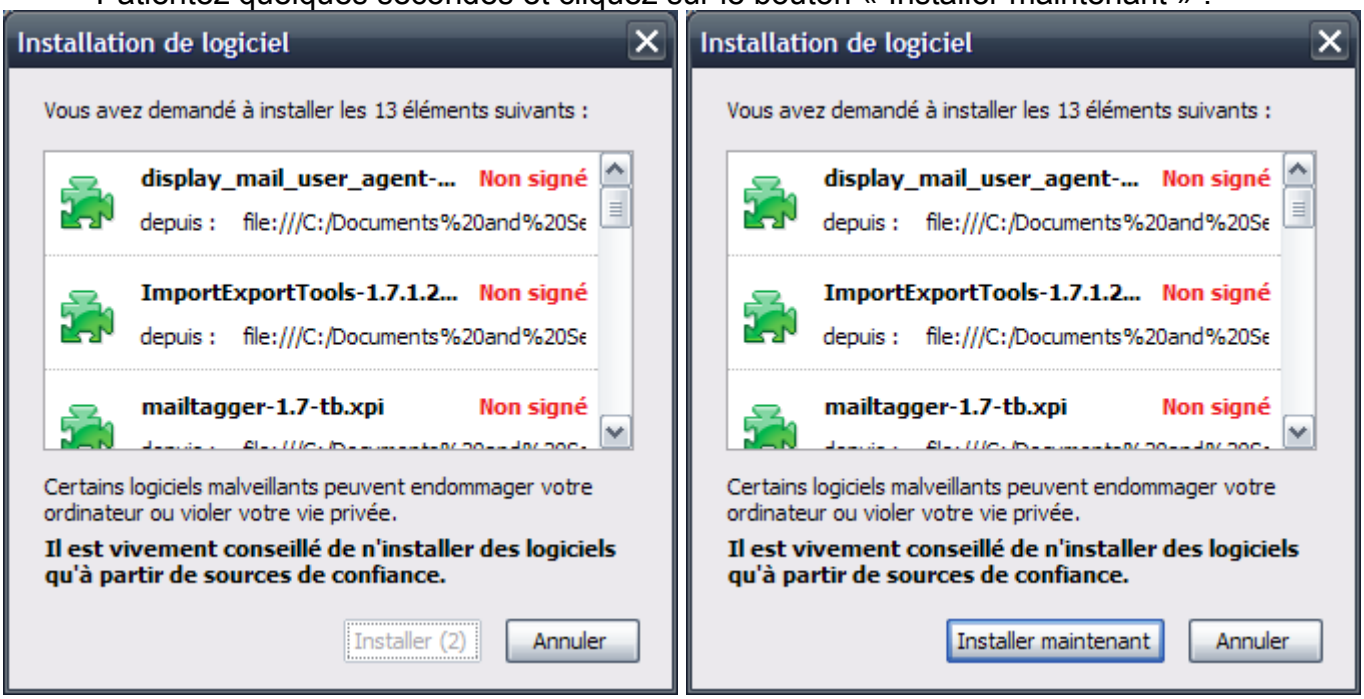


Ouvrez ensuite le dossier contenant toutes les extensions téléchargées à installer. Sélectionnez toutes les extensions et réaffichez la fenêtre des modules complémentaires à côté de la fenêtre de dossier.

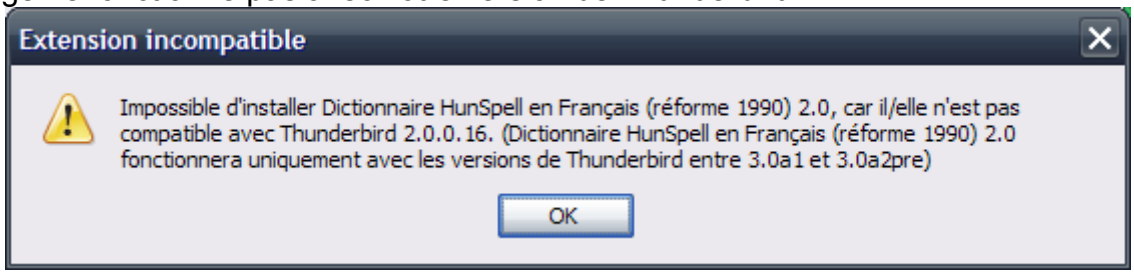
Déplacez ensuite les extensions dans la liste des modules complémentaires.



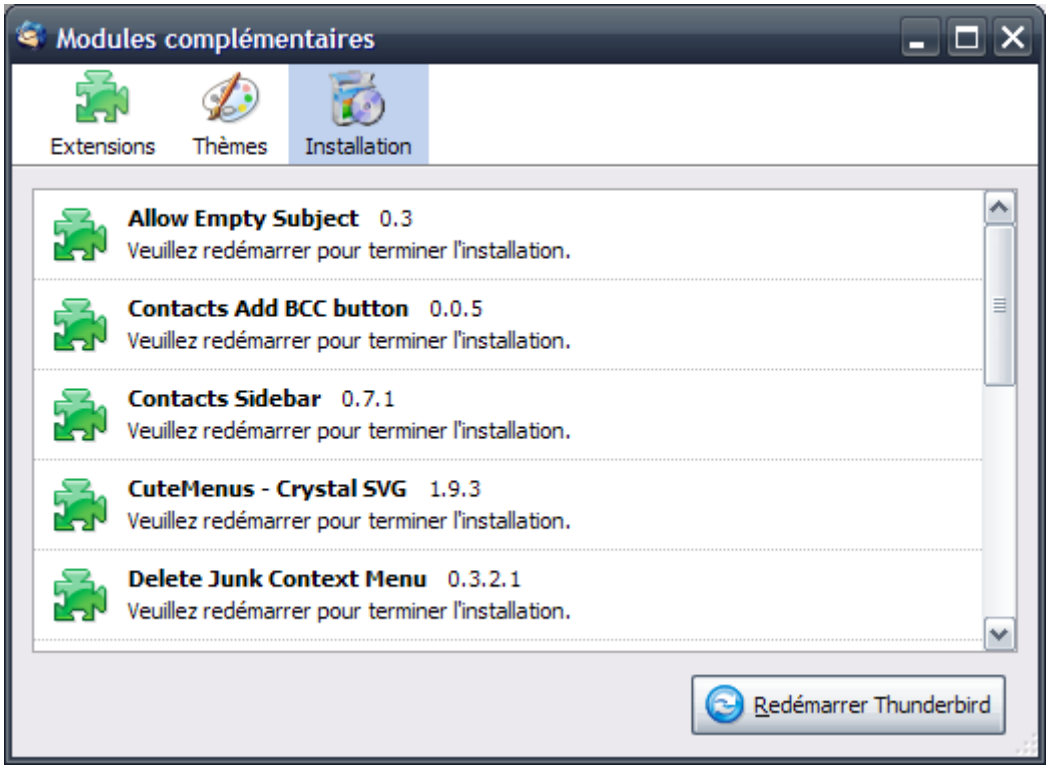
Patientez quelques secondes et cliquez sur le bouton « Installer maintenant » :



Si vous avez un message de ce genre, alors une des extensions que vous avez téléchargé ne fonctionne pas avec votre version de Thunderbird.



Cliquez ensuite sur le bouton « Redémarrer Thunderbird ».



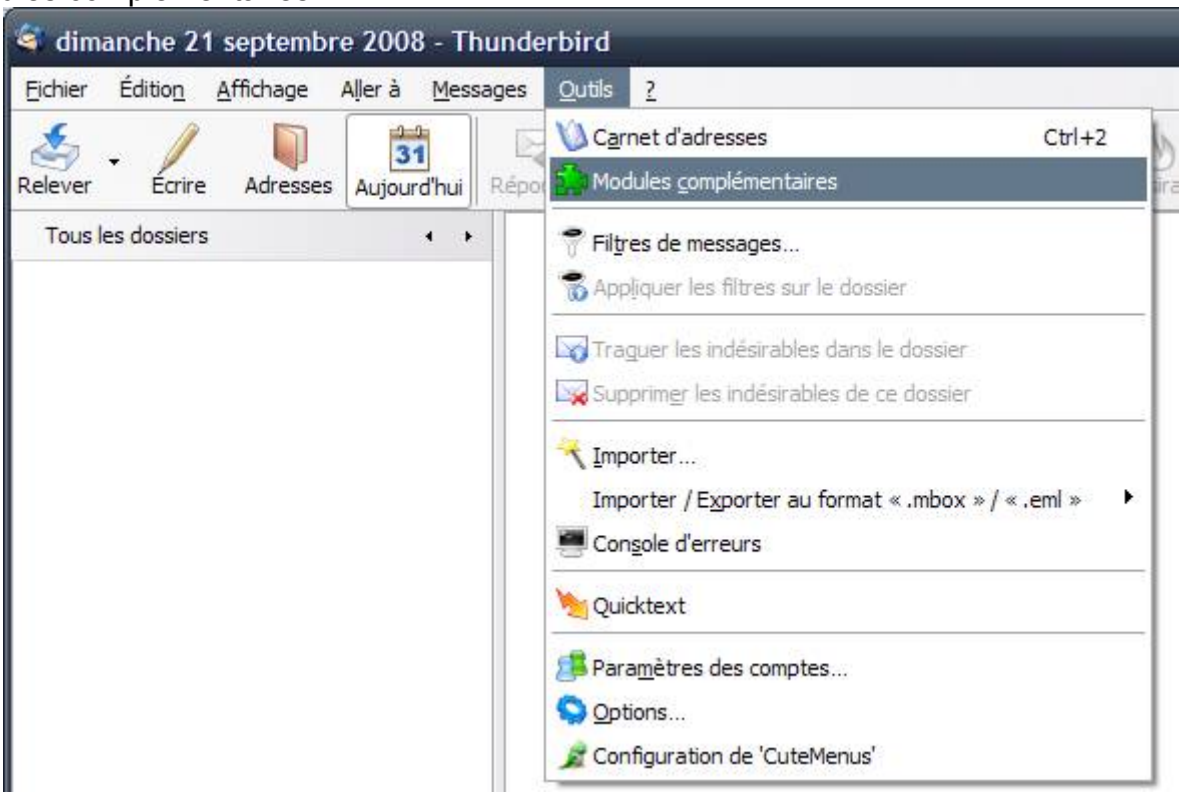
Plus il y aura d'extensions, plus le redémarrage de Thunderbird sera long.

Il est même possible que vous ayez une fenêtre vous demandant s'il faut arrêter un script ou continuer. Dans ce cas là, cliquez sur le bouton proposant de continuer.

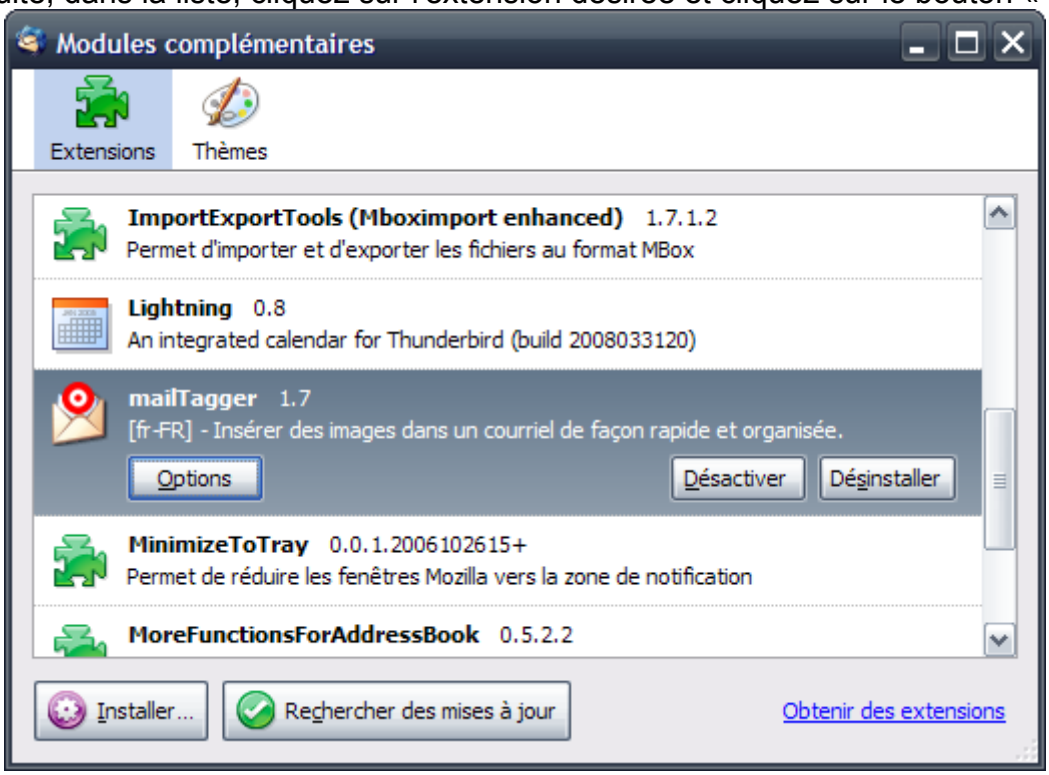
Certaines extensions peuvent afficher un message au redémarrage de Thunderbird. Fermez les différentes fenêtres de ces extensions.

VIII.3.f) Quelques réglages sur ces quelques extensions

Nous allons effectuer des réglages sur deux extensions : mailTagger et MinimizeToTray. Pour effectuer des réglages sur une extension, il suffit d'aller dans le menu « Outils » puis dans « Modules complémentaires » :



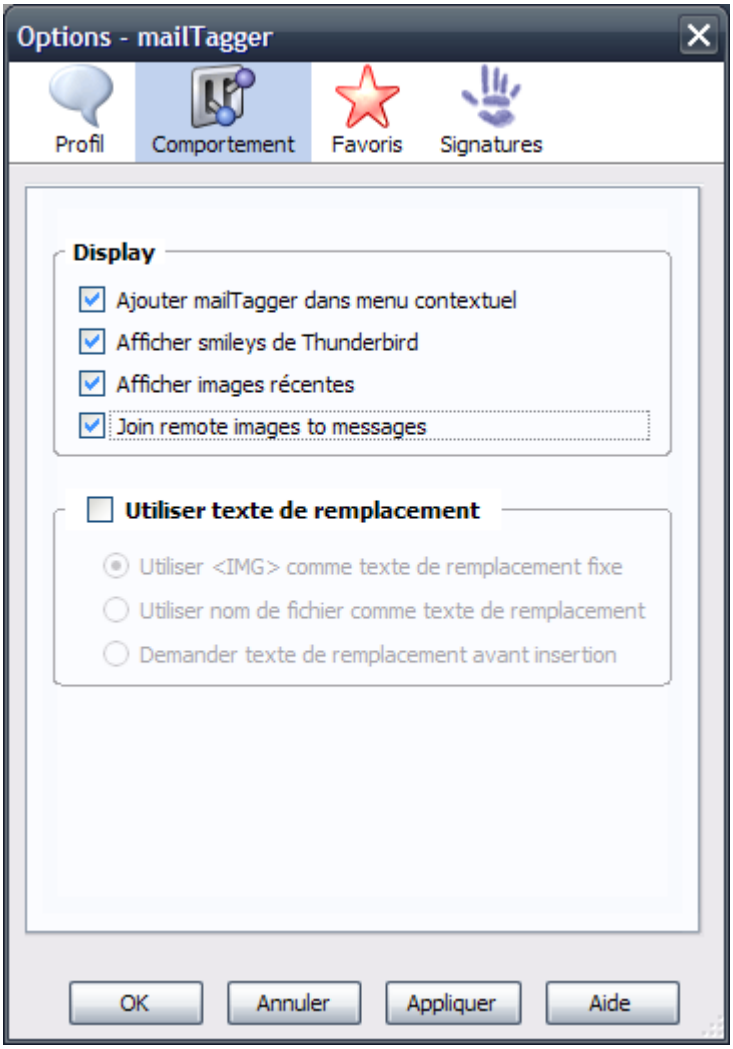
Ensuite, dans la liste, cliquez sur l'extension désirée et cliquez sur le bouton « Options » :



VIII.3.f.i) *MailTagger*

Décochez la case « Montrer les astuces au démarrage ».

Cliquez sur le bouton « Comportement » en haut de la fenêtre, cochez la case « Join remote images to messages » et décochez la case « Utiliser le texte de remplacement ». Enfin, cliquez sur OK.



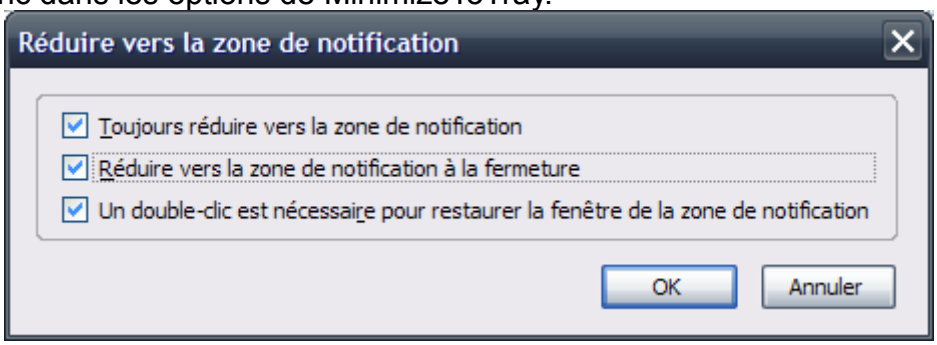
VIII.3.f.ii) MinimizeToTray

Par défaut, quand Thunderbird n'est pas ouvert, vous n'êtes pas averti de l'arrivée de nouveaux messages. Il peut donc être utile de le laisser ouvert en permanence.

Du coup, vous allez avoir un bouton supplémentaire dans la barre des tâches. Bouton qui risque d'être vite encombrant si vous avez tendance à manipuler beaucoup de fenêtres en même temps.

MinimizeToTray permet donc de réduire Thunderbird en un bouton à côté de l'horloge. Celui-ci devient donc discret et beaucoup moins encombrant. Cependant, ceci n'est pas le comportement par défaut lorsque cette extension est installée.

Allez donc dans les options de MinimizeToTray.



Cocher la première case permet de mettre Thunderbird en icône à côté de l'horloge

lorsque vous cliquerez sur le bouton « Réduire » de celui-ci.

Cocher la deuxième case permet de réduire Thunderbird à côté de l'horloge lorsque vous cliquerez sur le bouton de fermeture de Thunderbird. Ceci peut être très pratique car on a souvent tendance à fermer une fenêtre et la rouvrir peu de temps après. Je vous recommande donc de la cocher aussi.

Une fois les cases cochées, cliquez sur le bouton « OK ».

Si vous avez coché la deuxième case, vous devez peut-être vous dire que du coup, il n'est plus possible de fermer Thunderbird. Il est bien entendu encore possible de le quitter complètement. Pour ceci, repérez l'icone de Thunderbird à côté de l'horloge :

Faites un clic droit dessus, et cliquez sur « Fermer Thunderbird » :

VIII.3.g) Ajout d'un compte e-mail

VIII.3.g.i) A savoir avant de continuer

Pour des logiciels comme Thunderbird, il existe deux façons de récupérer votre courrier.

• La méthode Pop

• La méthode Imap

Chaque méthode a ses avantages et ses inconvénients.

Le protocole POP permet de récupérer votre courrier mais l'enlève de chez votre fournisseur.

Avantages : vos e-mails sont dans votre ordinateur. Vous pouvez donc être déconnectés afin de les relire.

Inconvénients : Comme vos e-mails sont dans votre ordinateur, il ne sera pas possible de les lire à partir d'un autre ordinateur.

Alors que le protocole IMAP permet de synchroniser votre compte de courrier avec votre ordinateur.

Avantages : Vous aurez une parfaite synchronisation entre plusieurs ordinateurs. Donc si vous marquez un courrier comme lu sur votre ordinateur, il sera marqué comme lu chez votre fournisseur, et donc sur tous les PC sur lesquels vous lirez votre courrier.

Inconvénients :

- Vos e-mails ne sont pas sur votre ordinateur. Si vous êtes régulièrement en déplacement et que vous n'avez pas toujours accès à Internet via votre ordinateur portable, vous ne pourrez pas relire vos e-mails.

- Vous serez aussi limités par la taille de votre boîte e-mail. Si votre fournisseur ne vous propose qu'un espace de stockage petit, comme vos e-mails restent chez votre fournisseur, votre boîte risque d'être pleine rapidement si vous conservez beaucoup de messages.

La méthode IMAP, quand elle est possible, est donc utile si vous avez besoin de lire votre courrier sur des ordinateurs différents qui ont un accès régulier à Internet. Alors que si vous ne lisez votre courrier que depuis un seul ordinateur, la méthode POP est plus simple.

Chacune des deux solutions a des inconvénients. Mais chacun de ces inconvénients ont des solutions. Solutions qui ont elles-mêmes leurs inconvénients.

En résumé, j'aurai tendance à vous conseiller l'Imap. Et nous verrons quelques réglages que vous pourrez appliquer pour contourner les inconvénients des deux méthodes.

VIII.3.g.ii) Quelle méthode utiliser ?

En fonction de l'adresse que vous voulez ajouter dans Thunderbird, la manipulation pour y parvenir peut varier. Voici un tableau non exhaustif donnant la méthode à suivre pour ajouter votre adresse e-mail pour que Thunderbird lise les nouveaux messages :

Fournisseur	Serveur POP	Serveur IMAP	Serveur SMTP	Méthode
Alice	pop.aliceadsl.fr	X	smtp.aliceadsl.fr	classique
AOL	X	imap.aol.com	smtp.aol.com	classique
Cegetel	pop.cegetel.net	imap.cegetel.net	smtp.cegetel.net	classique
Club Internet	pop3.club-internet.fr	imap.club-internet.fr	imap.club-internet.fr	classique
Free	pop.free.fr	imap.free.fr	smtp.free.fr	classique
Neuf	pop.neuf.fr	imap.neuf.fr	smtp.neuf.fr	classique
Noos	pop.noos.fr	imap.noos.fr	smtp.noos.fr	classique
Tele2	pop.tele2.fr	X	smtp.tele2.fr	classique
GMail	pop.gmail.com SSL	imap.gmail.com SSL	smtp.gmail.com SSL	classique + réglages pour Pop et SSL
Hotmail	X	X	X	Extension WebMail
Yahoo	pop.mail.yahoo.fr	X	smtp.mail.yahoo.fr	classique

Dans ce tableau, les serveurs POP et SMTP sont spécifiés, ils seront utilisés pour effectuer les réglages nécessaires.

Un « X » indique qu'il n'existe pas de serveur du type donné par l'en-tête de colonne.

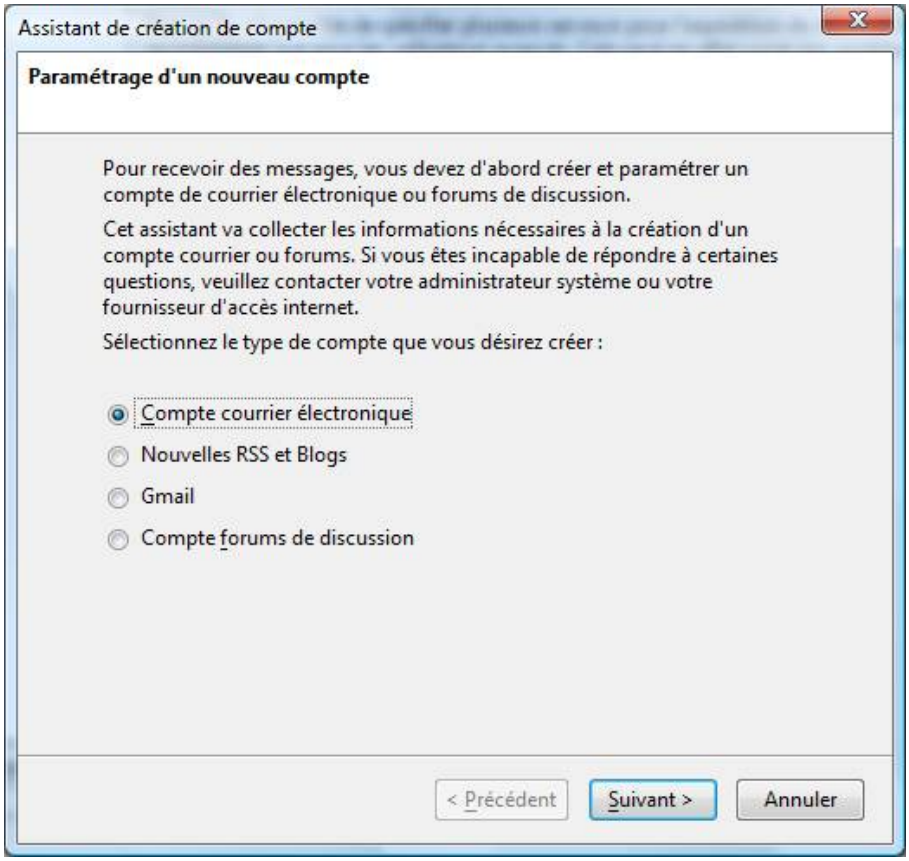
Pour chaque case où il est indiqué « SSL », il faudra suivre les instructions de la section VIII.3.g.iv (page 235) afin de configurer Thunderbird pour lire vos messages.

VIII.3.g.iii) Méthode classique

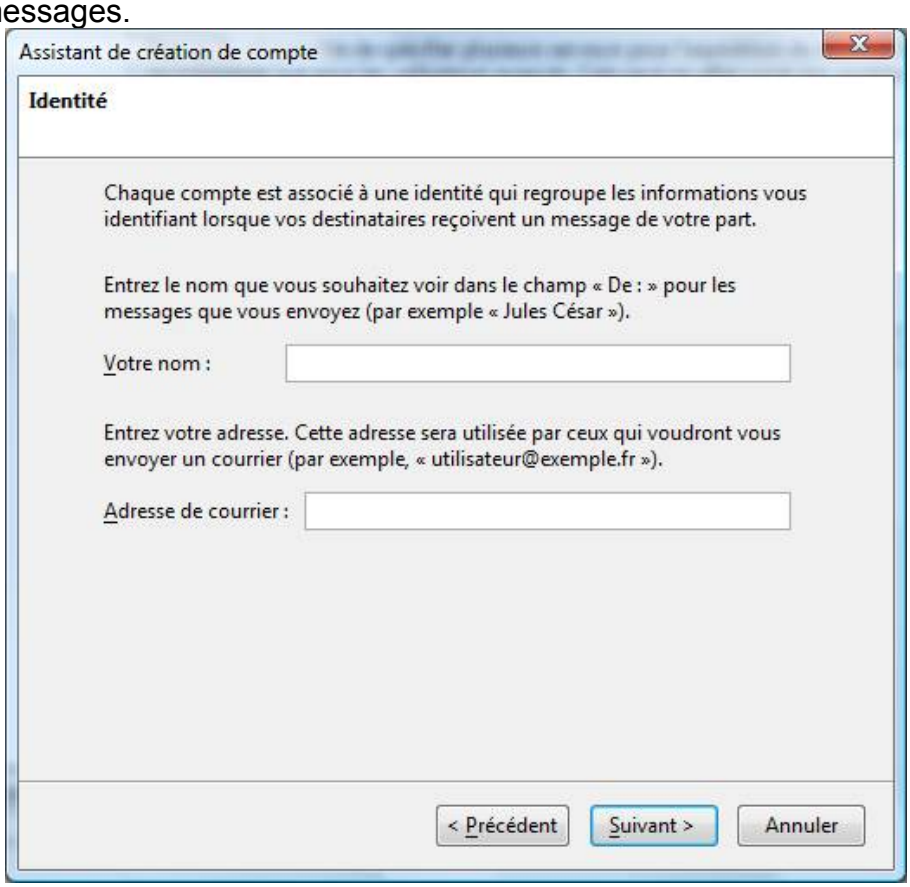
Allez dans le menu Outils, puis dans Paramètres des comptes.

Ensuite, cliquez sur le bouton Ajouter un compte.

Cochez la case « Compte courrier électronique » et cliquez sur le bouton « Suivant ».



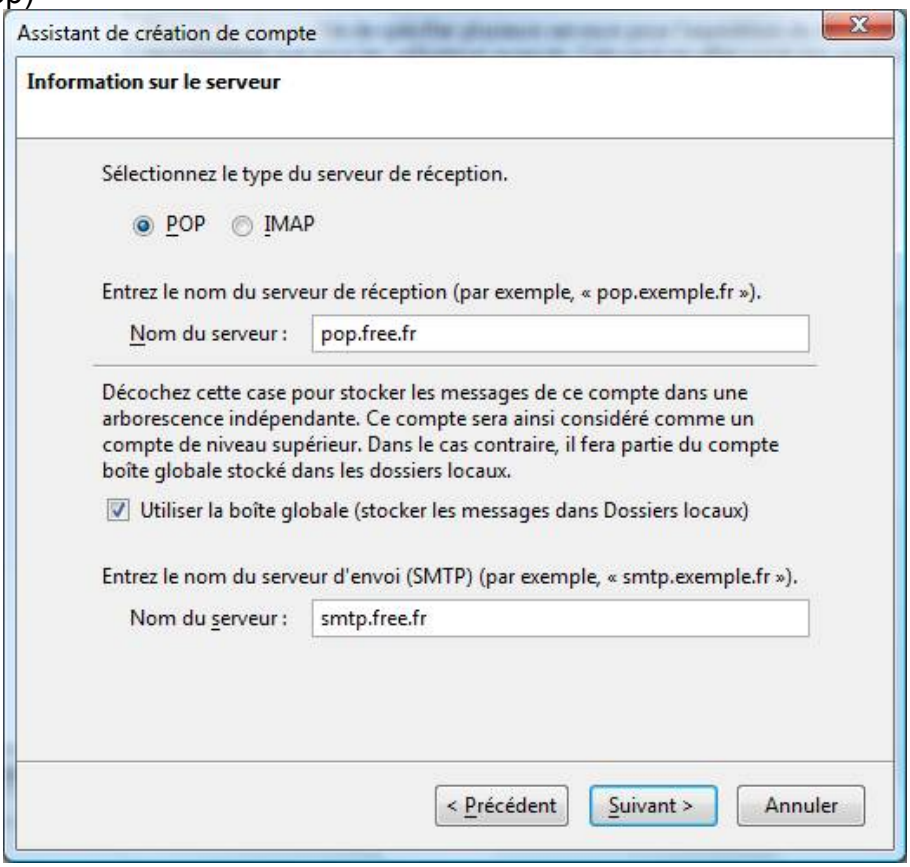
Dans la case « Votre nom », entrez le nom que les personnes verront lorsqu'elles recevront vos messages.



Et dans la case « Adresse de courrier », entrez votre adresse e-mail.

Cochez la case POP ou IMAP selon la façon dont vous voulez gérer votre courrier. Ensuite, entrez dans la première case l'adresse de votre serveur POP, et dans la dernière case l'adresse de votre serveur SMTP. (voir un peu plus loin si vous ne connaissez pas l'adresse de

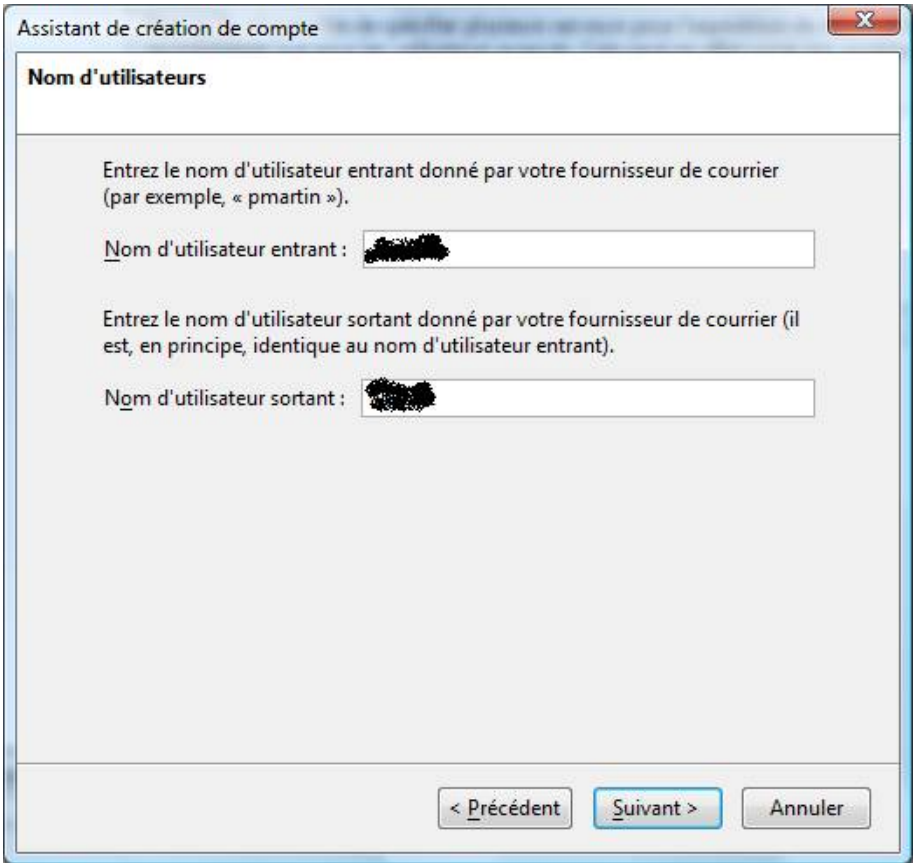
votre serveur pop)



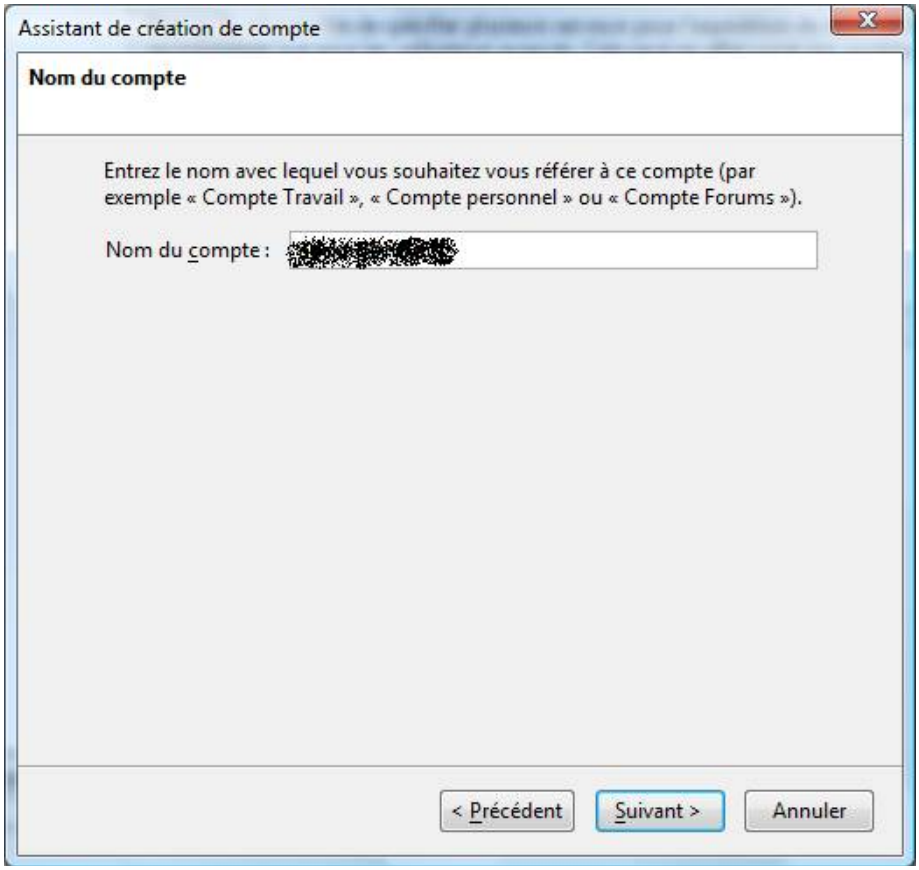
Laissez la case « Utiliser la boîte globale (...) » cochée si vous ne comptez utiliser qu'une seule adresse e-mail dans votre compte Thunderbird. La décocher créera un dossier avec le nom de votre adresse mail, et des sous dossiers Courrier entrant, Messages en attente, Envoyés, ... Un dossier par adresse e-mail que vous utiliserez sera créé.

Cliquez ensuite sur le bouton « Suivant ».

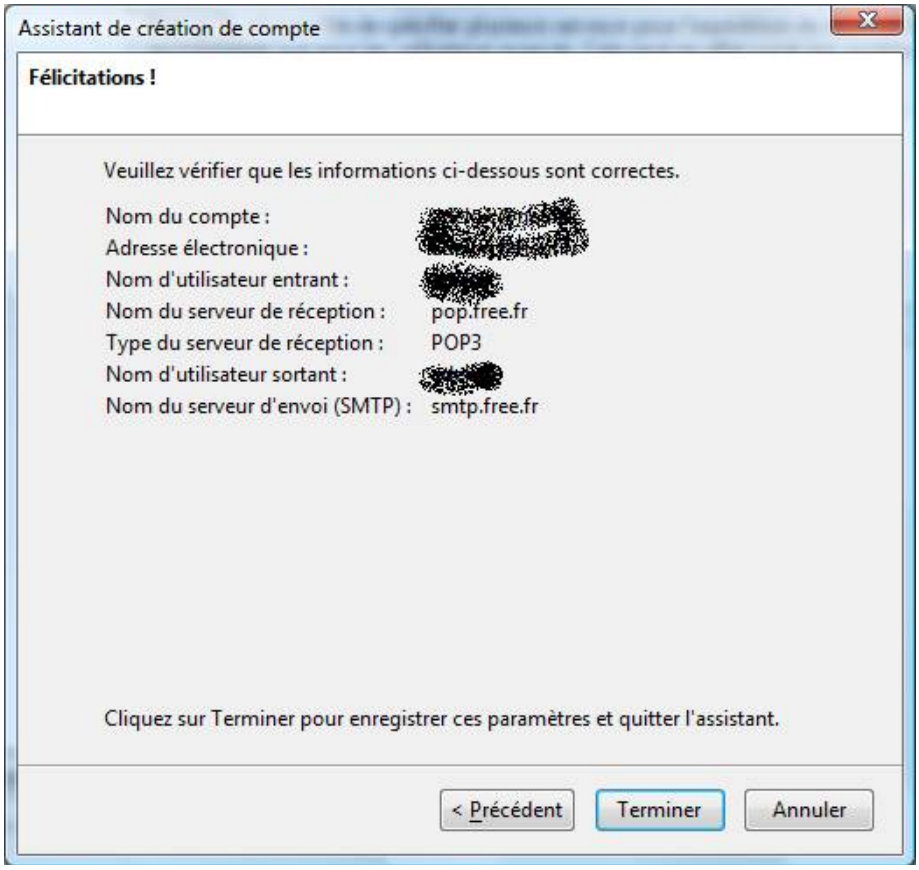
Cliquez sur le bouton « Suivant » (la plupart du temps, il n'y a rien a changer dans cette partie).



Mettez dans la case le nom que vous voulez donner à votre compte (vous pouvez mettre ce que vous voulez, ça ne changera strictement rien à la gestion de votre courrier). Cliquez ensuite sur le bouton « Suivant ».



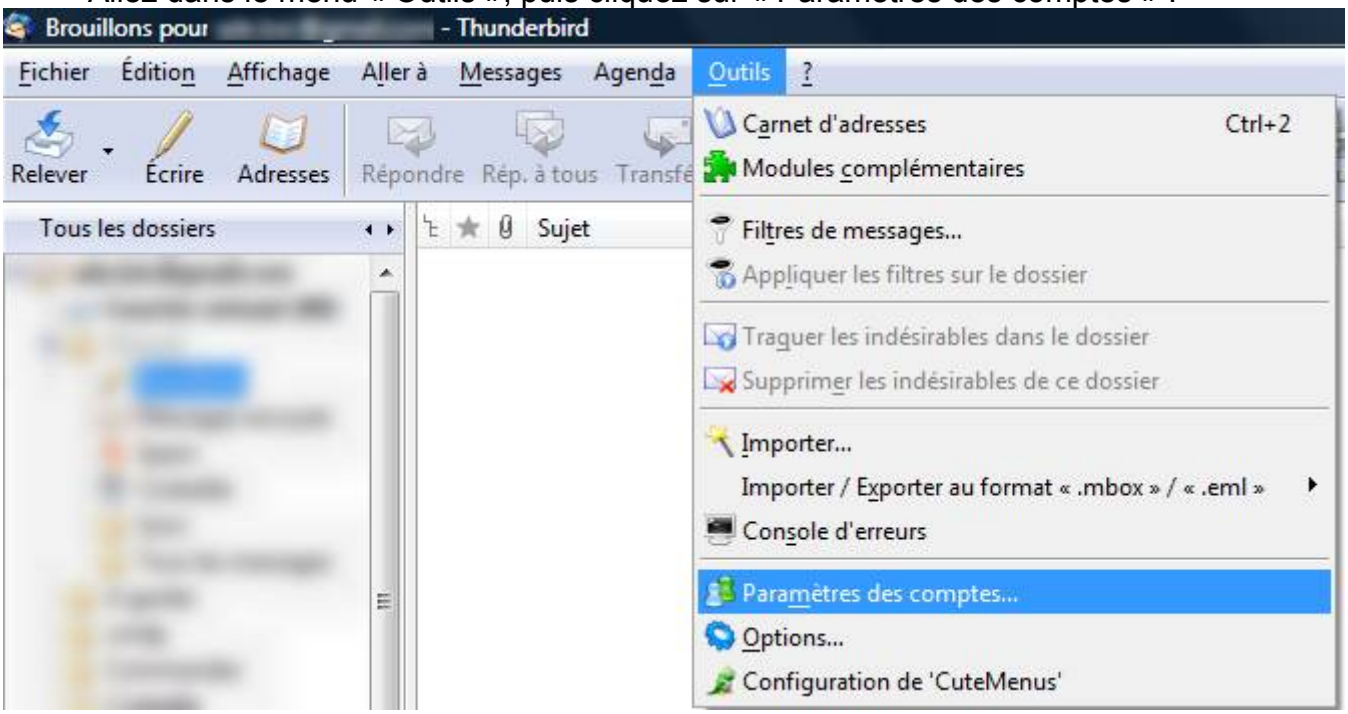
Cliquez ensuite sur Terminer.



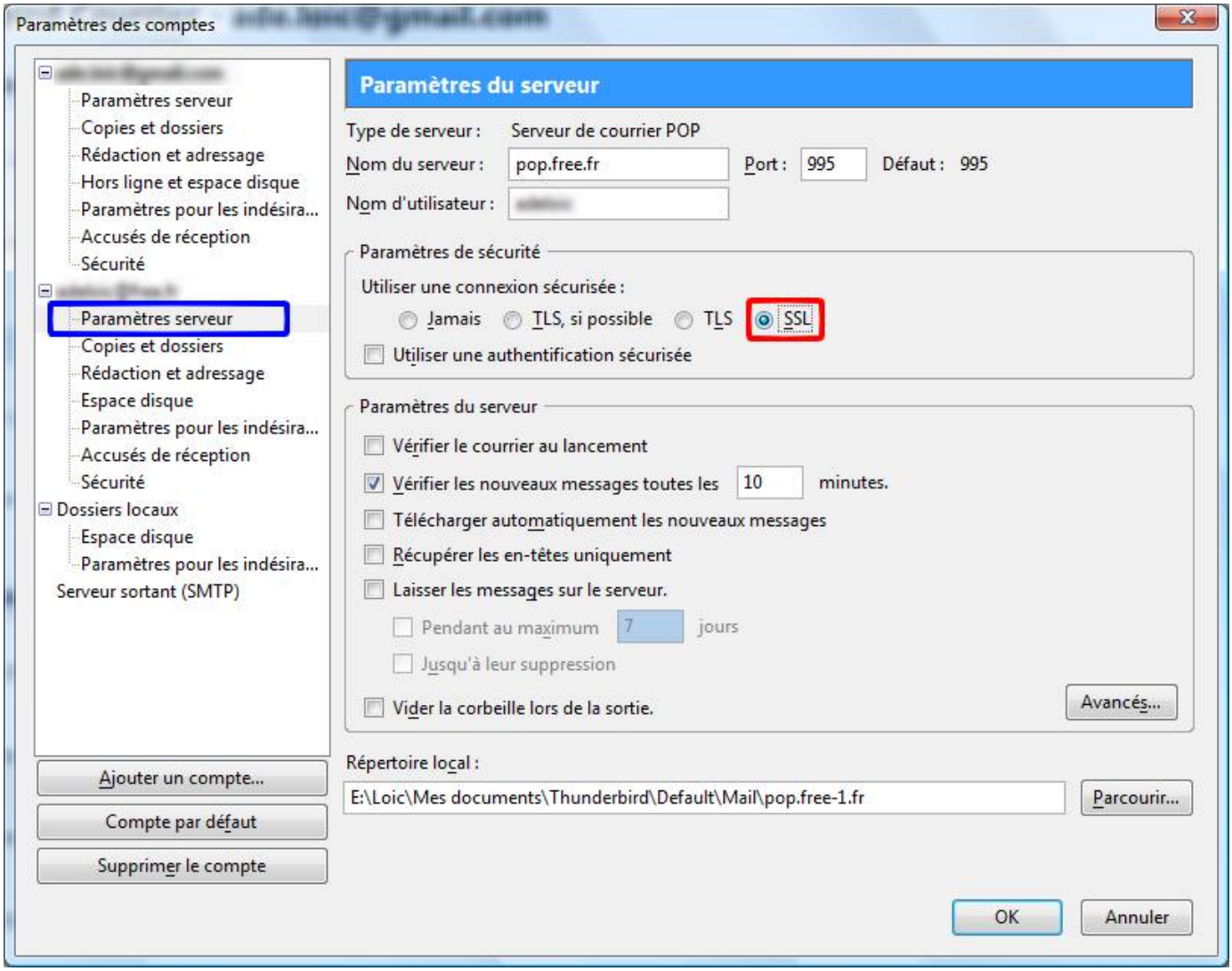
VIII.3.g.iv) <u>Configurer son compte avec un accès SSL</u>

VIII.3.g.iv.1) Pop

Allez dans le menu « Outils », puis cliquez sur « Paramètres des comptes » :



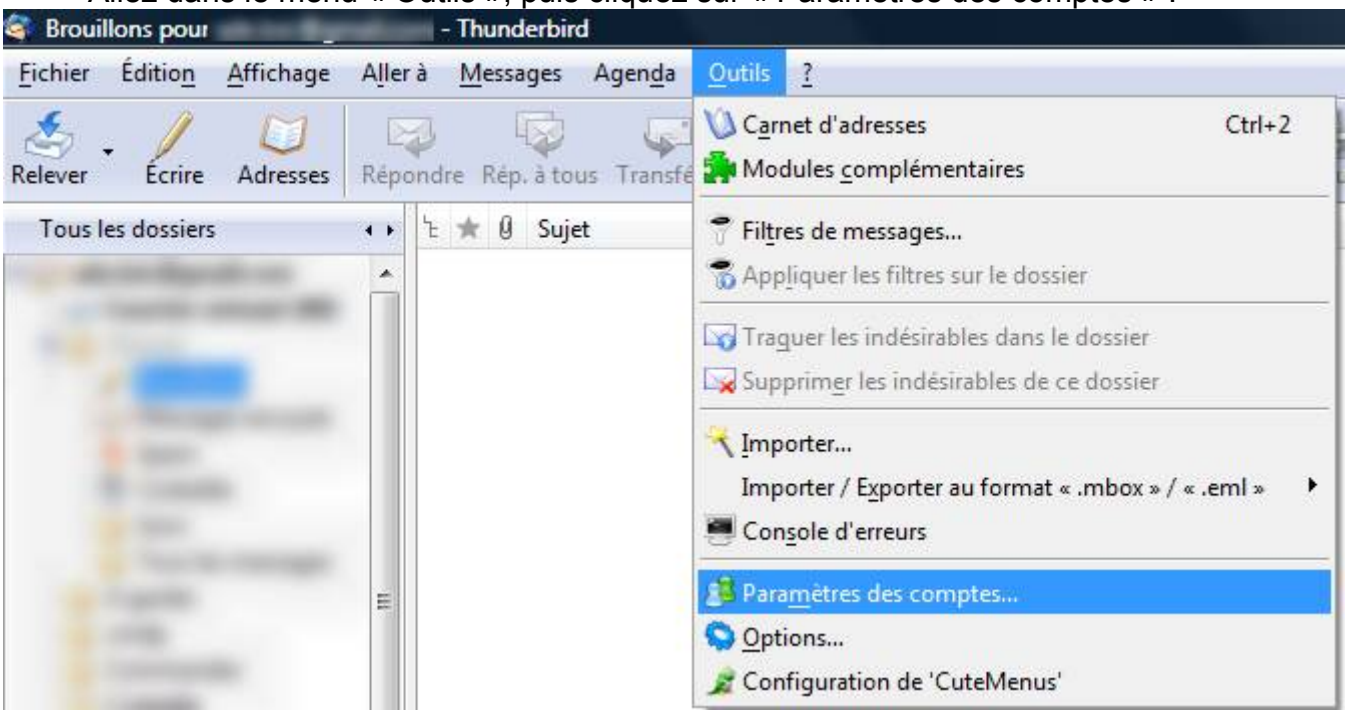
Cliquez ensuite sur le lien « Paramètres serveur » correspondant à votre adresse e-mail (voir cadre bleu de l'image ci-dessous) et cochez la case « SSL » (voir cadre rouge) :



Cliquez ensuite sur le bouton « OK ».

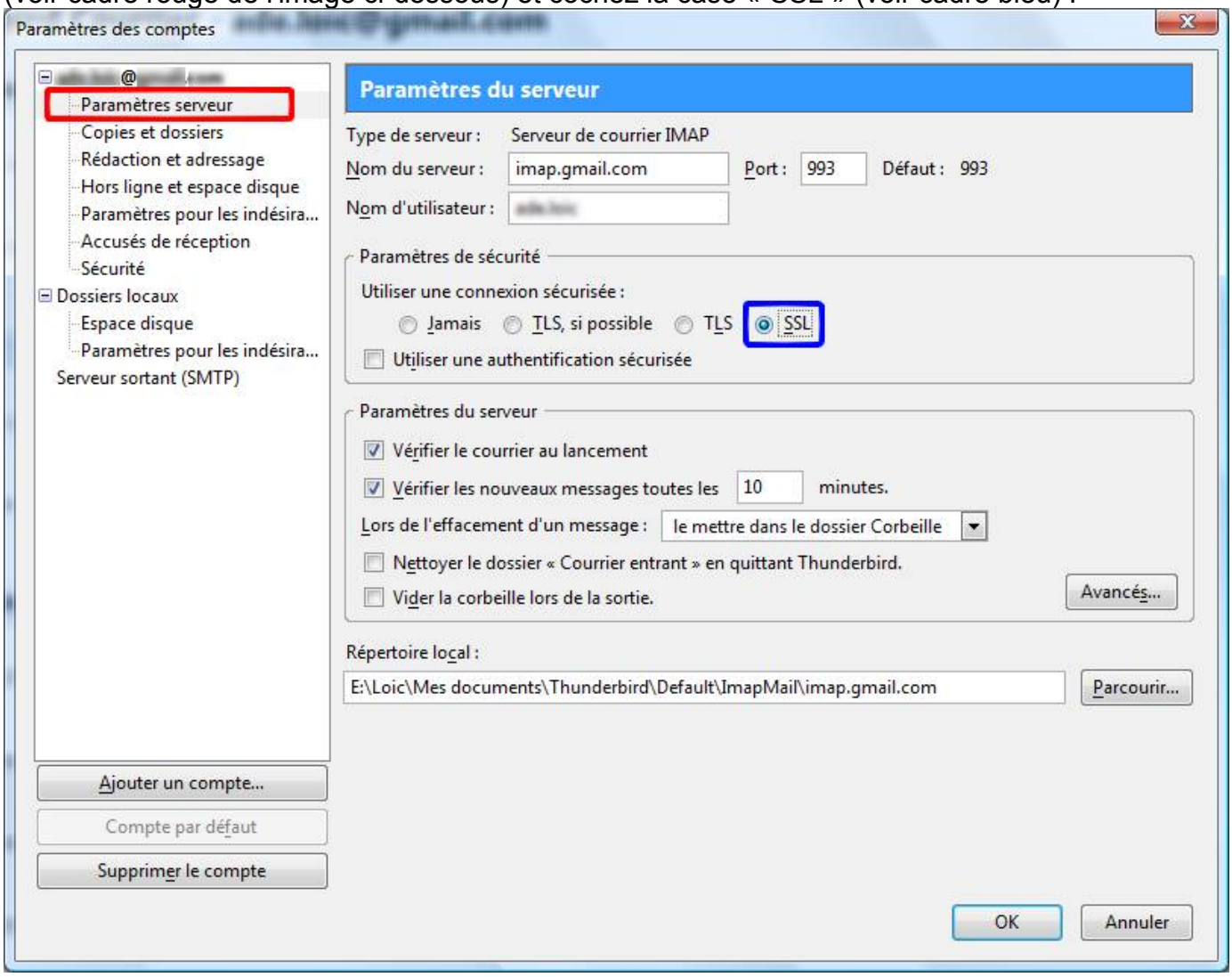
VIII.3.g.iv.2) Imap

Allez dans le menu « Outils », puis cliquez sur « Paramètres des comptes » :



Cliquez ensuite sur le lien « Paramètres serveur » correspondant à votre adresse e-mail

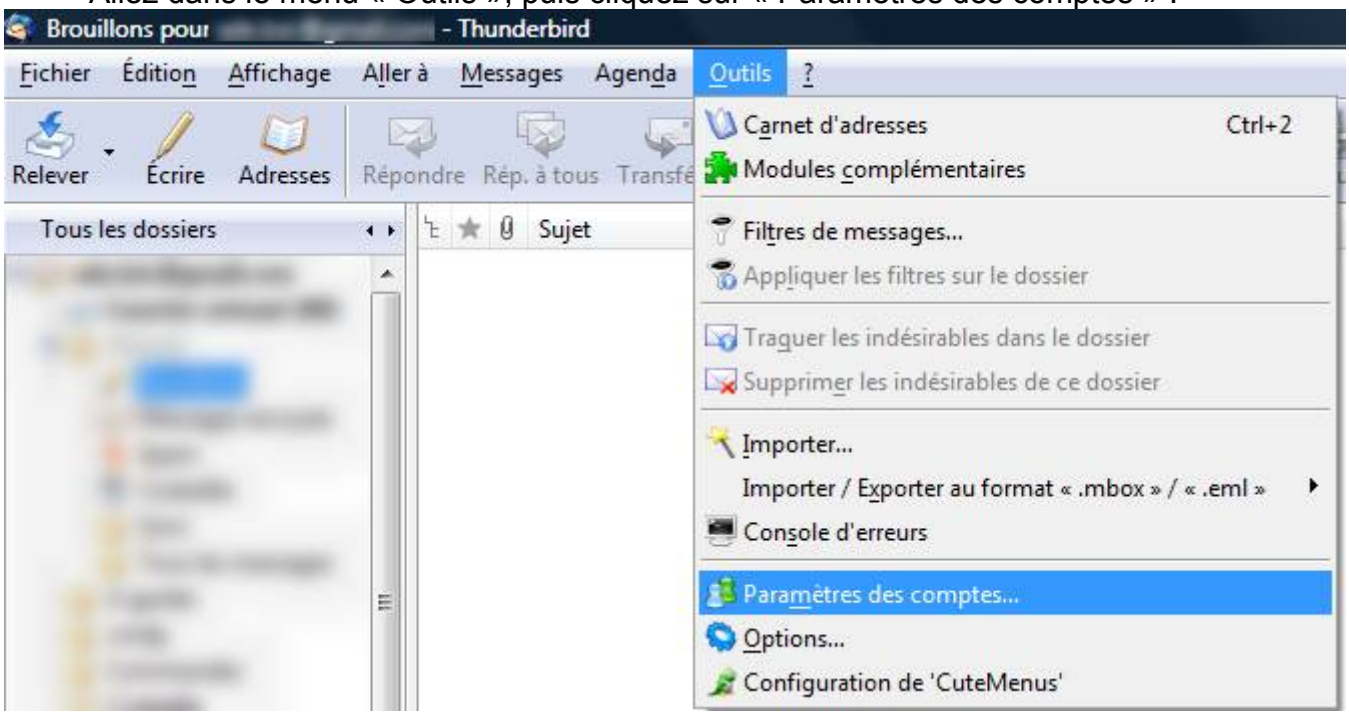
(voir cadre rouge de l'image ci-dessous) et cochez la case « SSL » (voir cadre bleu) :



Cliquez ensuite sur le bouton « OK ».

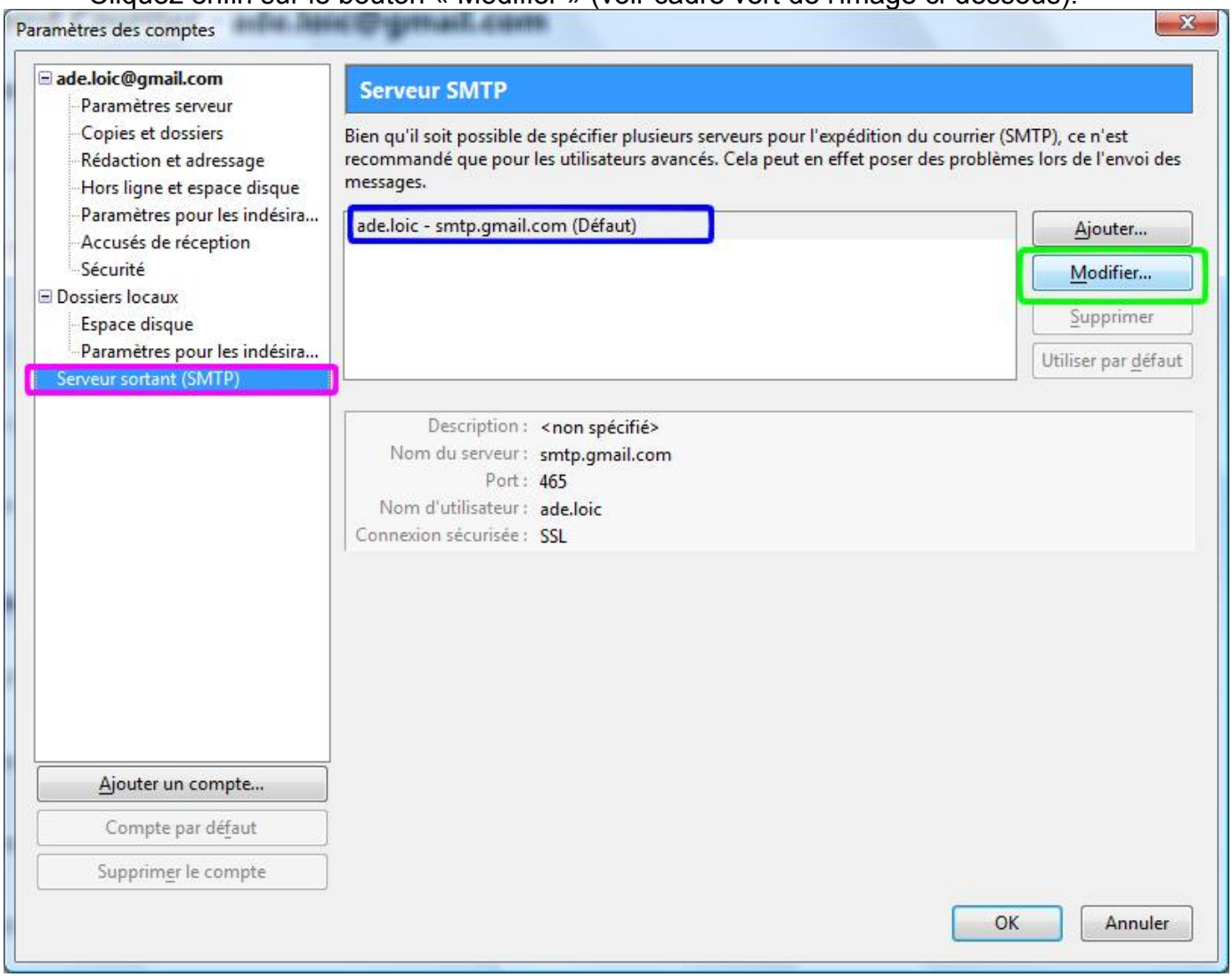
VIII.3.g.iv.3) Smtp

Allez dans le menu « Outils », puis cliquez sur « Paramètres des comptes » :

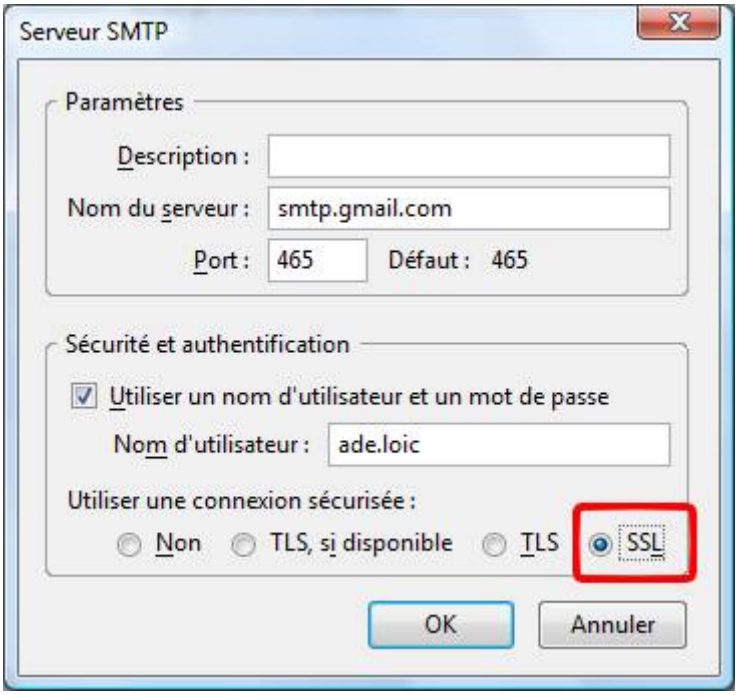


Ensuite, cliquez sur la ligne « Serveur sortant (SMTP) » (il se peut que vous deviez descendre un ascenseur qui n'apparait pas sur cette image car « Serveur sortant (SMTP) est en fin de liste / voir cadre violet de l'image ci-dessous), puis sur la ligne correspondant au serveur à modifier (voir cadre bleu).

Cliquez enfin sur le bouton « Modifier » (voir cadre vert de l'image ci-dessous).



Cochez la case « SSL » (voir cadre rouge de l'image ci-dessous), et cliquez sur le bouton OK.

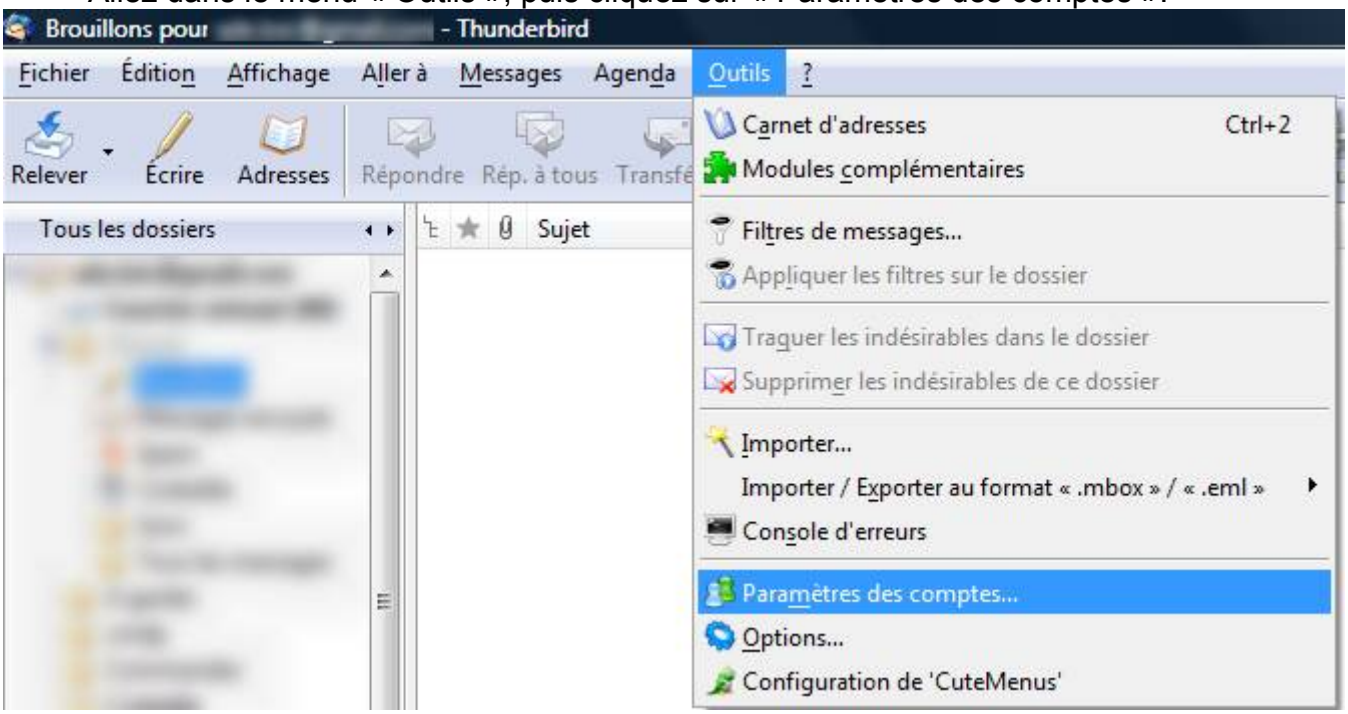


Cliquez sur le bouton OK pour fermer la fenêtre « Paramètres des comptes ».

VIII.3.h) Contourner les problèmes posés par la méthode Pop

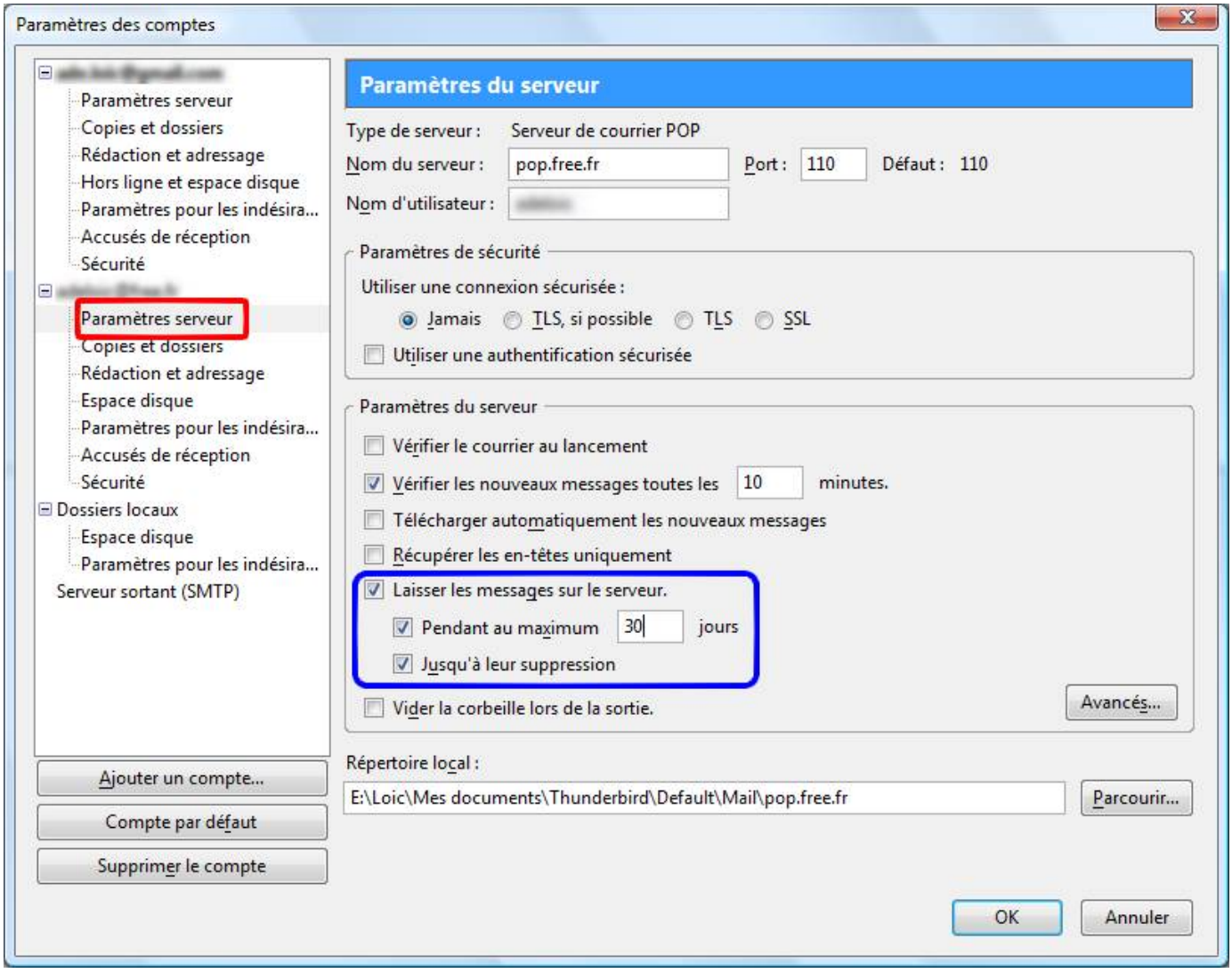
VIII.3.h.i) Impossibilité de lire ses messages sur plusieurs ordinateurs

Allez dans le menu « Outils », puis cliquez sur « Paramètres des comptes ».



Cliquez sur la ligne « Paramètres serveur » correspondant à l'adresse e-mail sur laquelle vous voulez effectuer le réglage. Cochez la case « Laisser les messages sur le serveur ». Vous pouvez aussi cocher la case « Pendant au maximum » et mettre la valeur que vous désirez. Ceci permet de laisser les messages chez votre fournisseur pendant au maximum 30 jours. Ce qui vous laisse un intervalle de 30 jours pour lire un message sur plusieurs ordinateurs.

Vous pouvez aussi cocher la case « Jusqu'à leur suppression » afin que, lorsque vous supprimez un message, il soit aussi supprimé chez votre fournisseur. Sans ça, il sera automatiquement téléchargé si vous lisez vos messages sur un autre ordinateur.



VIII.3.i) Contourner les problèmes posés par la méthode Imap

VIII.3.i.i) Impossibilité de conserver ses messages dans l'ordinateur

VIII.3.i.ii) Espace trop réduit

VIII.3.j) Débloquer les serveurs SMTP différents de celui de votre FAI

Cette petite étape est très importante dans le cas ou vous n'utilisez pas l'adresse e-mail de votre fournisseur d'accès. De plus en plus de fournisseurs d'accès bloquent les serveurs SMTP différents de ceux qu'ils offrent. Ceci permet de lutter un peu mieux contre le SPAM, mais cela bloque les utilisateurs d'adresses e-mail comme GMail qui utilisent Thunderbird ou Outlook Express pour lire leurs messages.

Voici donc la procédure pour plusieurs fournisseurs d'accès.

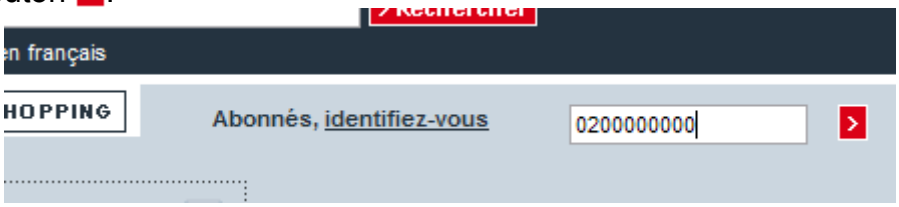
VIII.3.j.i) Procédures pour les différents FAI

Fournisseur	Procédure
Free	Voir section Erreur : source de la référence non trouvée (Page 241)
Orange	
SFR – Le neuf	Voir section VIII.3.j.iii (Page 242)
Tele2	Impossible

VIII.3.j.ii) Chez Free

Allez sur le site de Free : http://www.free.fr/

Dans la partie « Abonnés, identifiez-vous », tapez votre numéro de téléphone et cliquez ensuite sur le bouton ›.



Dans la case « Identifiant », votre numéro devrait réapparaître. Tapez votre mot de passe dans la case « Mot de passe ». Cliquez ensuite sur le bouton « Connexion ».

Cliquez ensuite sur le bouton « Internet » (voir cadre bleu de l'image ci-dessous) :

Cliquez ensuite sur le lien « Blocage du protocole SMTP sortant » (voir cadre violet de l'image ci-dessous) :

Décochez la première case « Activer » et cliquez sur le bouton « ENVOYER » :

Un avertissement vous préviendra ensuite que tout a correctement fonctionné. Il vous faudra par contre redémarrer votre freebox afin que les changements soient pris en compte. Pour ceci, il suffit de la débrancher électriquement et de la rebrancher.

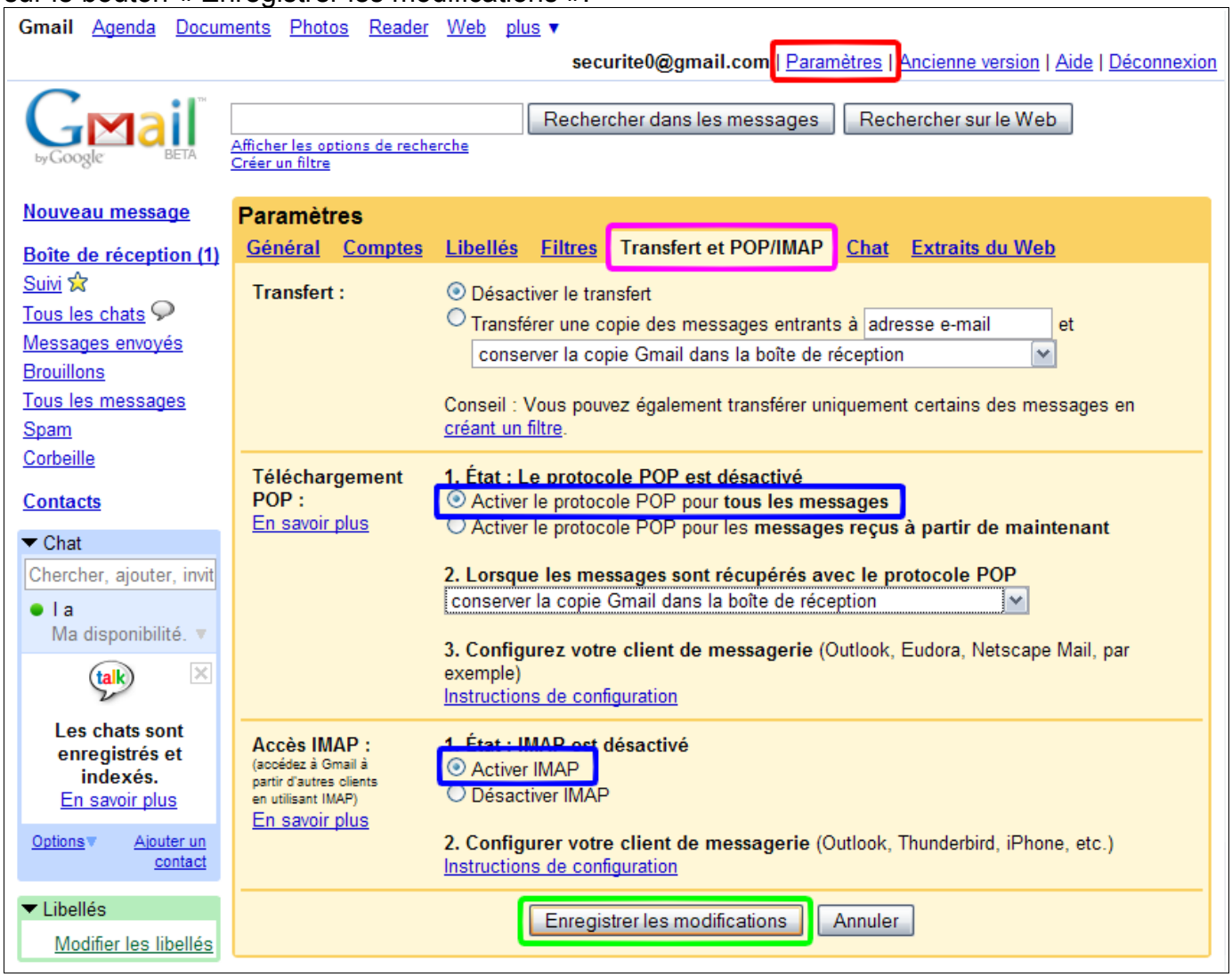
VIII.3.j.iii) Chez le Neuf

VIII.3.k) Quelques réglages supplémentaires pour quelques fournisseurs

VIII.3.k.i) GMail

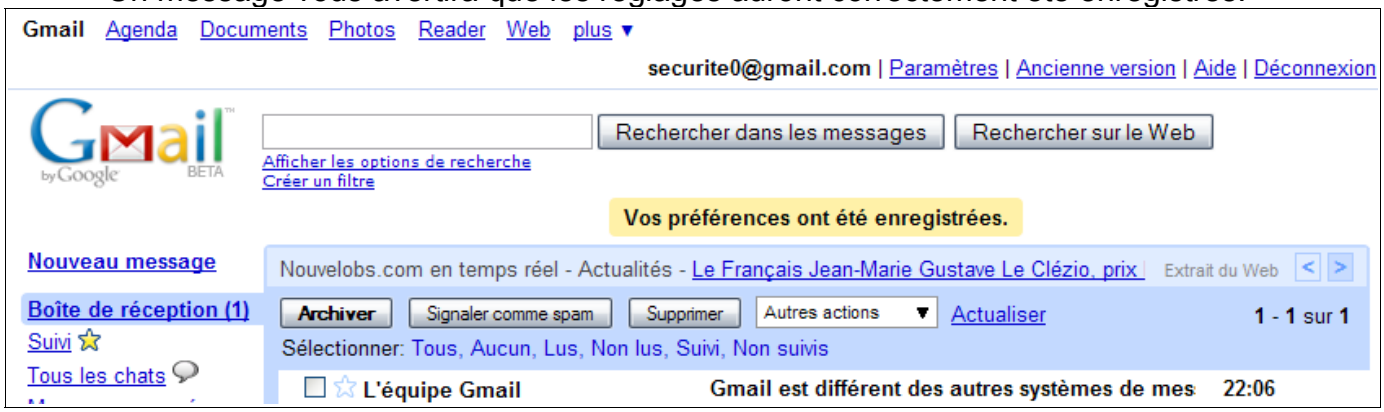
Pour Gmail, si vous souhaitez utiliser le protocole Pop ou Imap, il faudra aller sur le site de Gmail et se connecter à son nom.

Cliquez ensuite le lien « Paramètres » (voir cadre rouge de l'image ci-dessous) et sur « Transfert et POP/IMAP » (voir cadre violet). Cochez ensuite la case « Activer le protocole POP pour tous les messages » ou la case « Activer IMAP » (voir cadres bleus). Cliquez ensuite sur le bouton « Enregistrer les modifications ».



Vous pourrez ainsi lire vos messages d'une adresse gmail dans votre logiciel de messagerie préféré.

Un message vous avertira que les réglages auront correctement été enregistrés.



VIII.3.k.ii) La méthode Webmail

VIII.3.l) Quelques réglages de Thunderbird pour améliorer l'utilisation

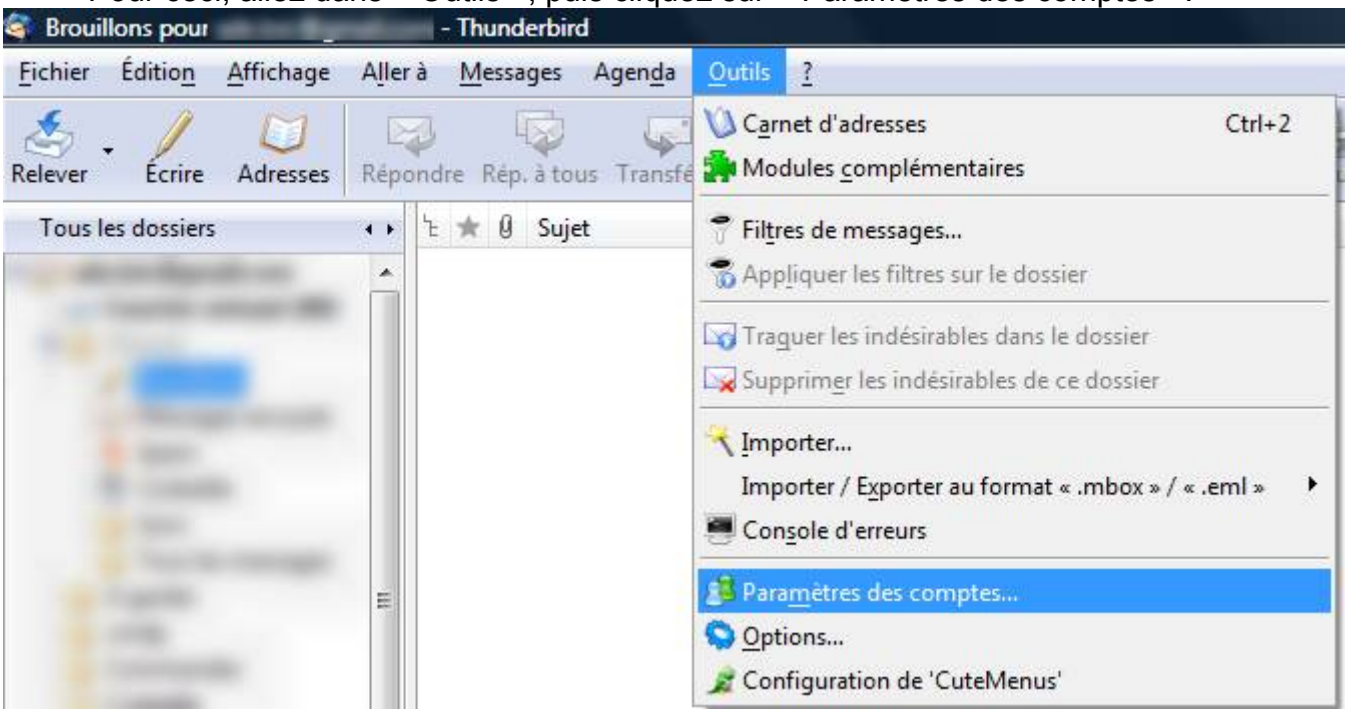
VIII.3.l.i) Réponses aux messages

Lorsqu'on lit un message qui est la réponse d'une réponse (d'une réponse ...), l'ordre le plus logique consisterai à avoir la conversation dans le sens chronologique. Donc le message le plus ancien au début et le plus récent à la fin.

Cependant, Il est assez désagréable pour la plupart des gens de devoir descendre un ascenseur à chaque fois qu'on veut lire le message le plus récent d'un e-mail.

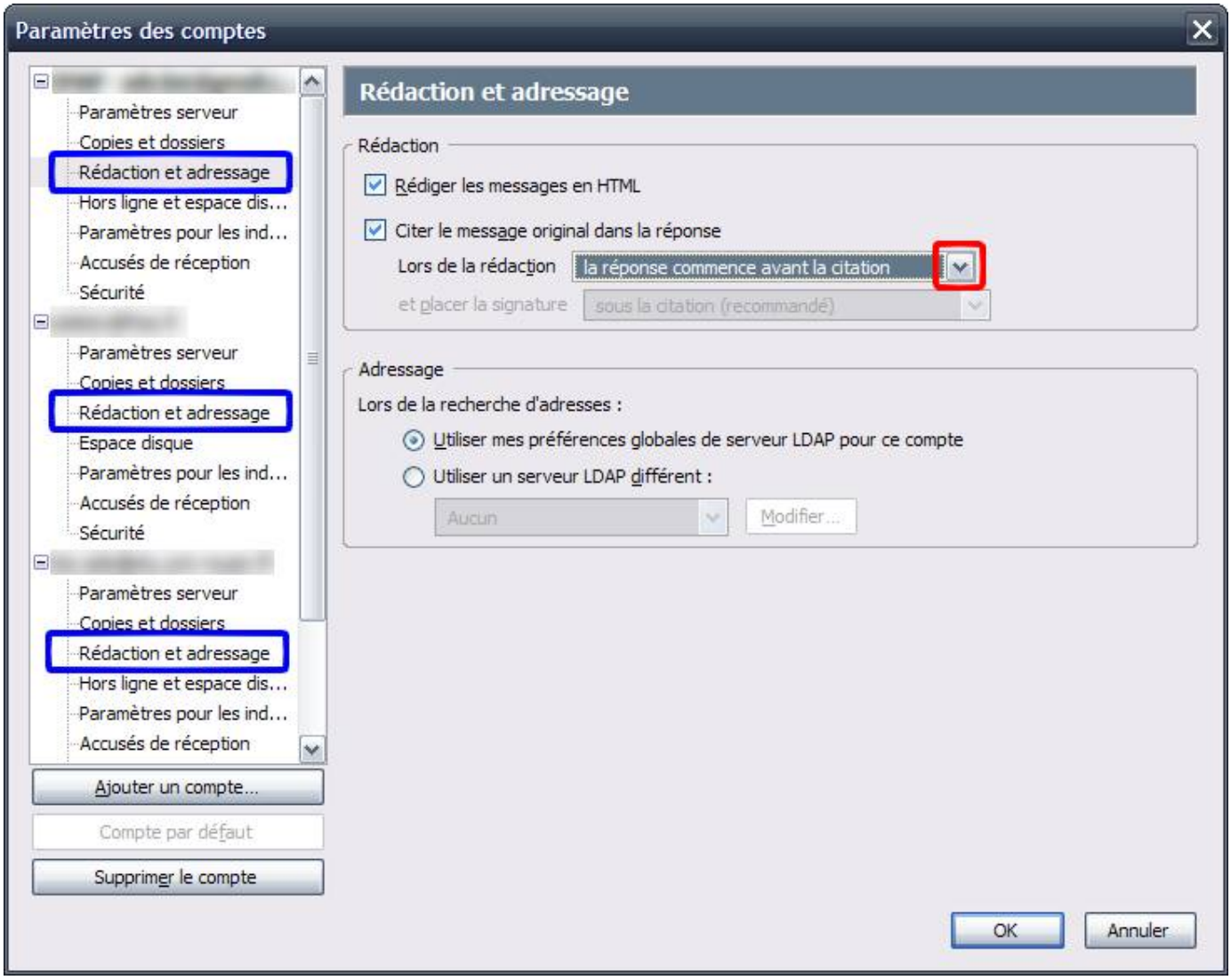
Il est donc possible de demander à Thunderbird, lorsque vous répondez à un e-mail, de mettre la réponse tout en haut du message, ce qui évitera à votre correspondant de descendre l'ascenseur très loin.

Pour ceci, allez dans « Outils », puis cliquez sur « Paramètres des comptes ».



Pour chaque ligne « Rédaction et adressage » dans la partie gauche de la fenêtre (voir cadres bleu), développez la liste déroulante nommée « Lors de la rédaction » (voir cadre rouge) et choisissez l'élément « la réponse commence avant la citation ».

Ensuite, cliquez sur « OK ».

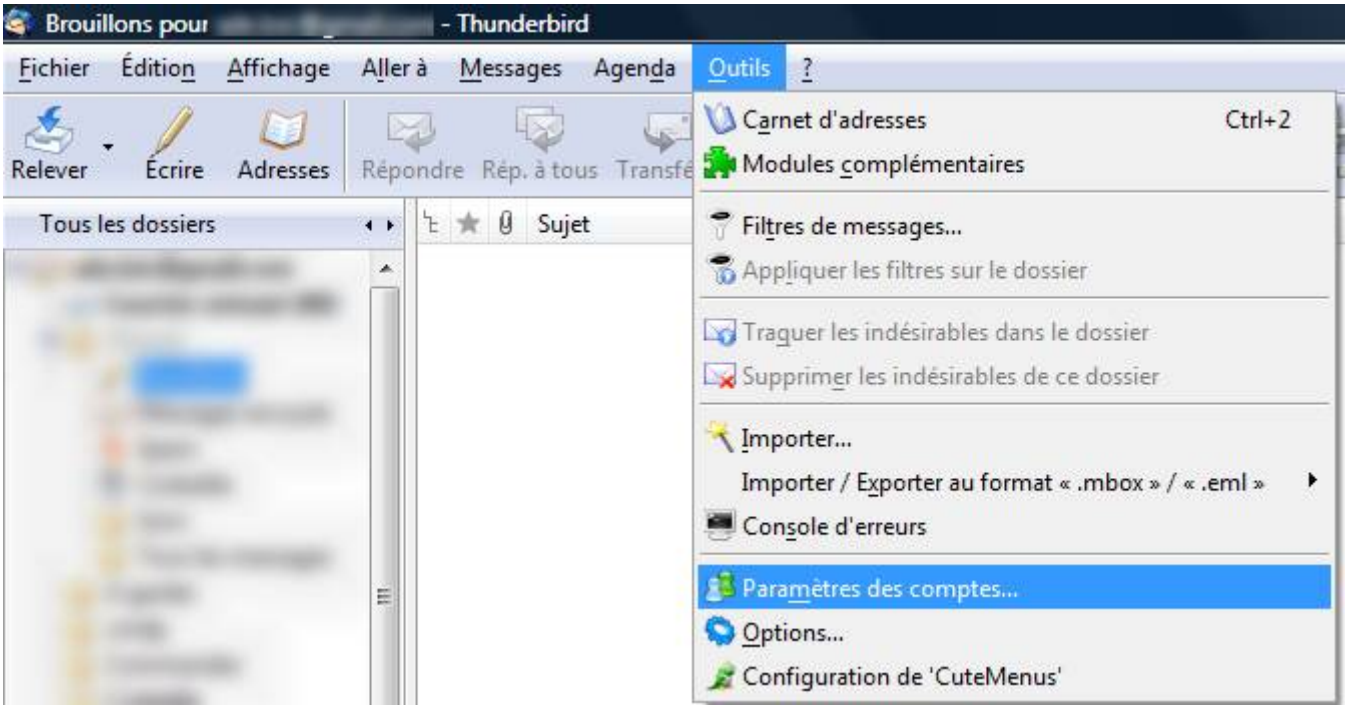


VIII.3.m) Quelques réglages pour améliorer la gestion du spam

Par défaut, tous les spams sont classés dans la boîte de réception et marqués comme spams (une petite flamme est visible dans une des colonnes quand Thunderbird a détecté qu'un e-mail est un spam). Cependant, si vous recevez beaucoup de spams, vous risquez d'être vite noyé entre les spams et votre courrier.

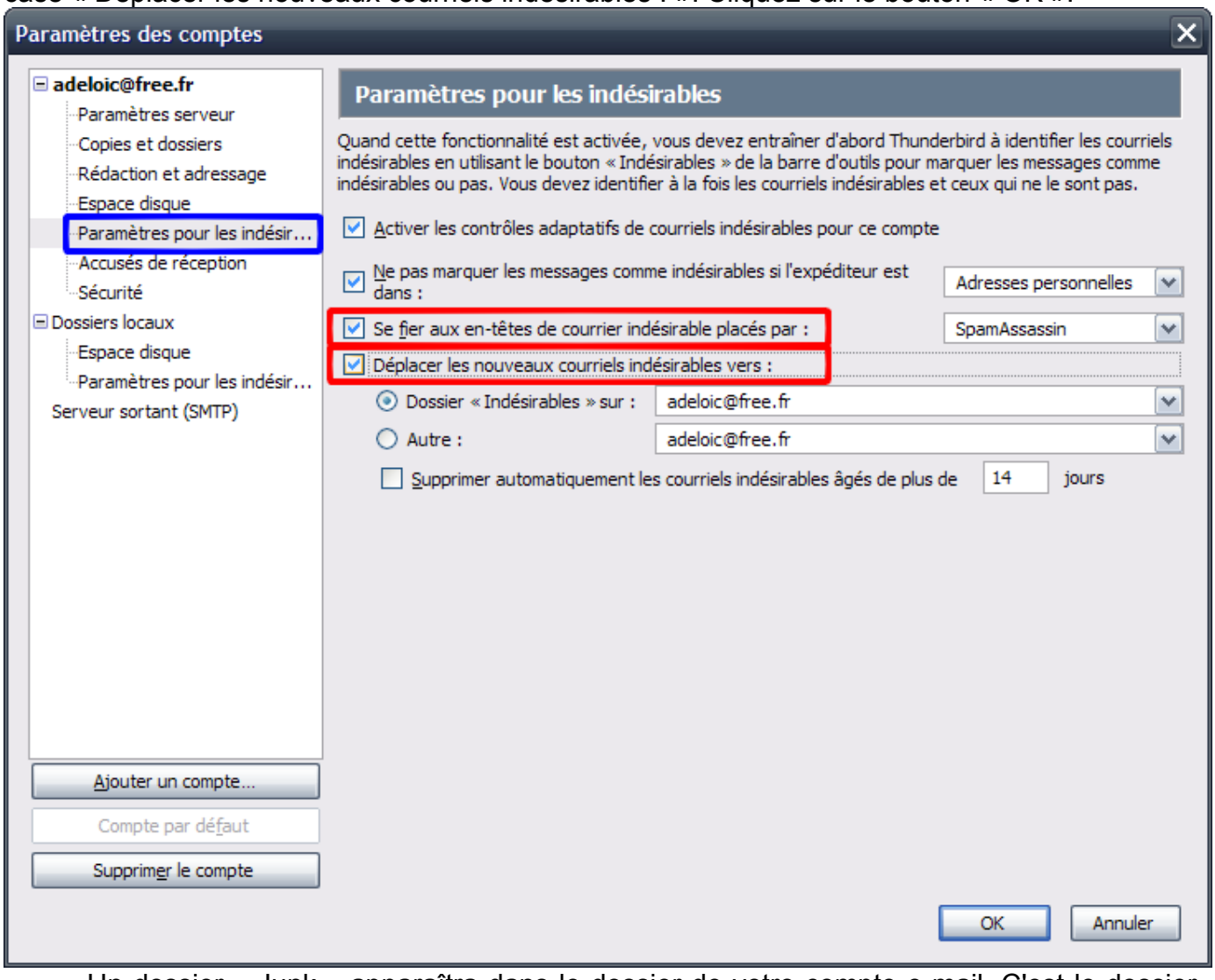
Il est possible de demander à Thunderbird de mettre tous les spams dans un dossier.

Pour ceci, allez dans le menu « Outils », puis cliquez sur « Paramètres des comptes ».



Pour chaque compte e-mail, cliquez sur la ligne « Paramètres pour les indésirables ».

Cochez la case « Se fier aux en-têtes de courrier indésirable placés par : » ainsi que la case « Déplacer les nouveaux courriels indésirables : ». Cliquez sur le bouton « OK ».



Un dossier « Junk » apparaîtra dans le dossier de votre compte e-mail. C'est le dossier des indésirables, dossier qui s'appellera « Indésirables » au prochain démarrage de

Thunderbird. C'est un petit bug de Thunderbird.

VIII.3.n) Importation de messages depuis Outlook, Outlook Express, Windows Mail, Eudora, Communicator 4

VIII.3.o) Importation du carnet d'adresses depuis Outlook Express

IX) Quelques petits messages de la part de votre ordinateur

Comme vous vous êtes peut-être rendus compte, la moitié de mes gros titres commençaient par le mot « quelques ». Cette partie répertoriera les quelques messages normaux que peut afficher votre ordinateur en ce qui concerne la sécurité de votre ordinateur.

Certains messages sont dus aux mises à jour automatiques des différents logiciels. Dans le cas ou vous ne trouveriez pas un message dans cette section, n'hésitez pas à regarder les sections concernant les mises à jour des différents logiciels.

Commençons par les messages fournis par Windows.

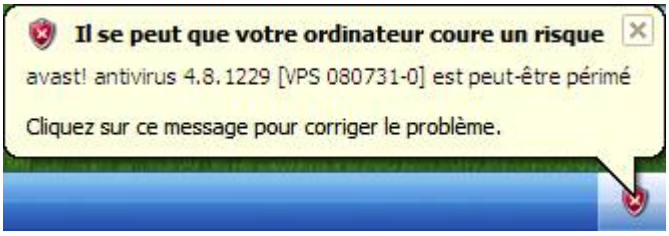
IX.1) Messages de Windows

Par défaut, Windows XP et Vista questionnent tout le temps les logiciels de sécurité. Ainsi, Windows connait l'état des différents logiciels et sais vous prévenir lorsque quelque chose ne va pas.

Voici quelques uns des messages que Windows affiche. Il se peut que Windows affiche plusieurs lignes de problèmes dans un message.

Les captures d'écrans sont celles de Windows XP, l'icône est presque identique sous Windows Vista et les messages sont identiques.

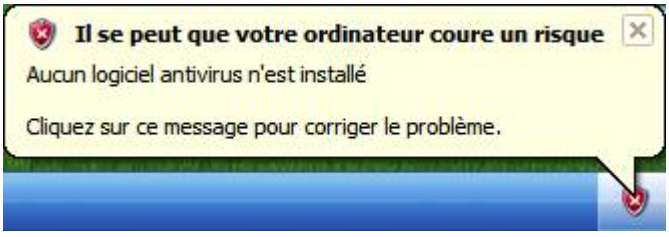
IX.1.a) Antivirus périmé



Il se peut que ce message apparaisse de temps en temps si vous n'utilisez pas régulièrement votre ordinateur. Ce message signifie en fait que votre antivirus n'est pas à jour. Ceci peut arriver par exemple après un retour de vacances, ...

Patientez une à deux minutes après vous être connecté à Internet et votre antivirus se mettra à jour automatiquement (comme Avast) ou vous demandera de le faire. Ce message devrait donc disparaître après la mise à jour. Sinon, vous pouvez forcer la mise à jour de votre antivirus.

IX.1.b) Antivirus introuvable

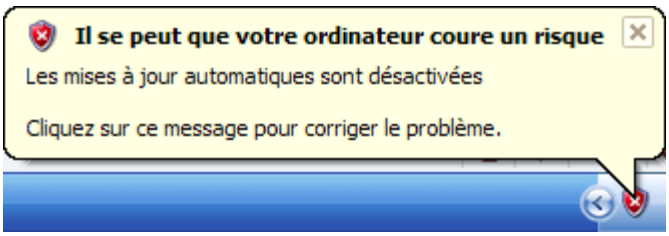


Soit vous n'avez pas encore installé d'antivirus, ce message est normal, mais vous devriez en installer un. Car même si vous n'êtes pas connecté à Internet, vous pouvez quand même attraper un virus (via les clés USB par exemple).

Il se peut aussi que votre antivirus soit carrément supprimé par un virus, ce qui expliquerai aussi l'apparition dans ce message pour le cas ou vous auriez déjà installé un antivirus.

En théorie, ce message peut aussi apparaître dans le cas d'un antivirus que Windows ne connait pas. Cependant, la plupart des antivirus sont maintenant reconnus par Windows et il est donc peu probable que ce message apparaisse pour cette raison (Avast est reconnu par Windows).

IX.1.c) Mises à jour désactivées

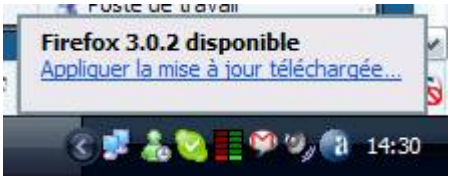


Le message est assez parlant dans ce cas. Il faut activer les mises à jour automatiques. Pour ceci, suivez les instructions de la partie Erreur : source de la référence non trouvée page Erreur : source de la référence non trouvée (pour Windows XP) ou la partie Erreur : source de la référence non trouvée page Erreur : source de la référence non trouvée.

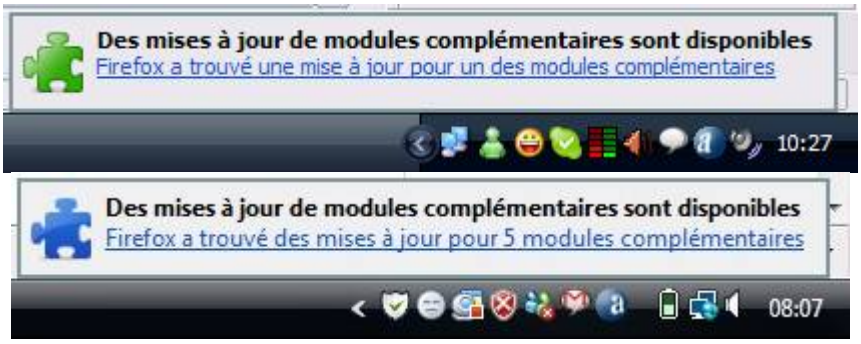
IX.2) Messages de Firefox

IX.2.a) Mise à jour du programme

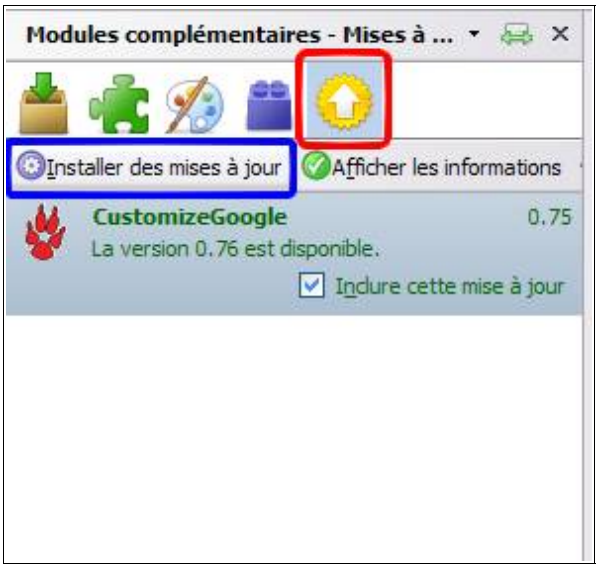
Ce petit message prévient qu'il existe une mise à jour de Firefox. Cliquez sur « Appliquer la mise à jour téléchargée ».



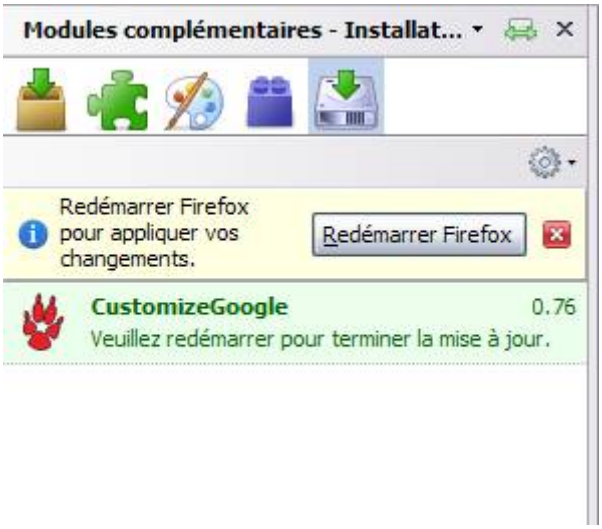
IX.2.b) Mise à jour des extensions



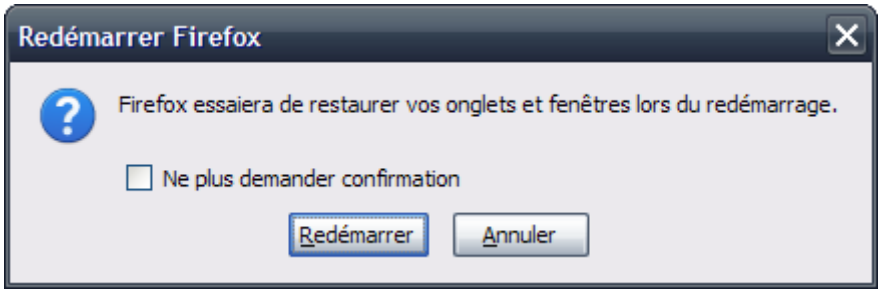
Cliquez sur « Firefox a trouvé une mise à jour pour un des modules complémentaires », ou « Firefox a trouvé des mises à jour pour X modules complémentaires ».



Cliquez ensuite sur la flèche blanche sur fond jaune (voir cadre rouge de l'image ci-dessus). Cliquez ensuite sur « Installer des mises à jour ».



Cliquez ensuite sur « Redémarrer Firefox ».



Cliquez ensuite sur « Redémarrer ».

Firefox se relancera avec l'extension (ou les extensions) mise à jour.

X) Quelques détails n'entrant pas dans les catégories précédentes

X.1) La gestion des cookies

Pour résumer ce qui a été dit dans la définition, les cookies ne sont pas inutiles, et étant des fichiers ne contenant que du texte, ils ne prennent presque pas de place sur un disque dur. Pour indication, les cookies présents sur mon disque dur au moment de l'écriture de cet article ne pesaient que 55 Ko. Je pouvais donc les mettre environ 26 fois sur une disquette pour qu'elle ne soit remplie.

Si toutefois vous voulez vraiment les enlever (pour le problème de sécurité que certains peuvent poser, ou pour d'autres raisons), il existe différentes méthodes :

• La méthode de tri :

De nombreux logiciels antispyware analysent les cookies. Exécuter une analyse suffit à éradiquer ces cookies espions. Voir les sections Erreur : source de la référence non trouvée à Erreur : source de la référence non trouvée pour la procédure avec Spybot Search & Destroy.

• La méthode à la main :

En fait, ce que j'appelle méthode à la main consiste soit à en enlever un en particulier, soit tous les enlever. Nous verrons les deux cas pour Internet Explorer et pour Firefox.

• La méthode brutale :

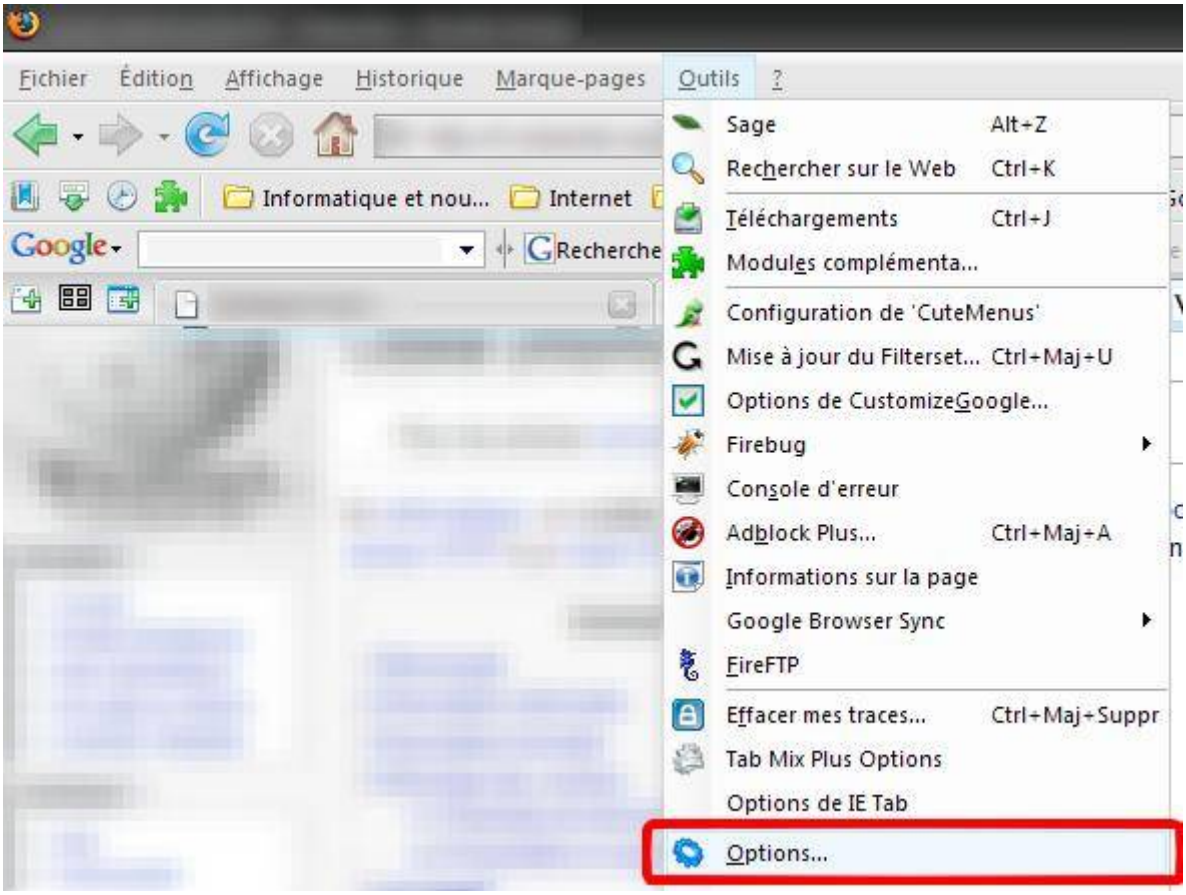
Elle consiste à supprimer tout les cookies sans exception.

X.1.a) La méthode à la main

Il est très très rare d'avoir besoin de supprimer un cookie en particulier. L'opération est cependant possible.

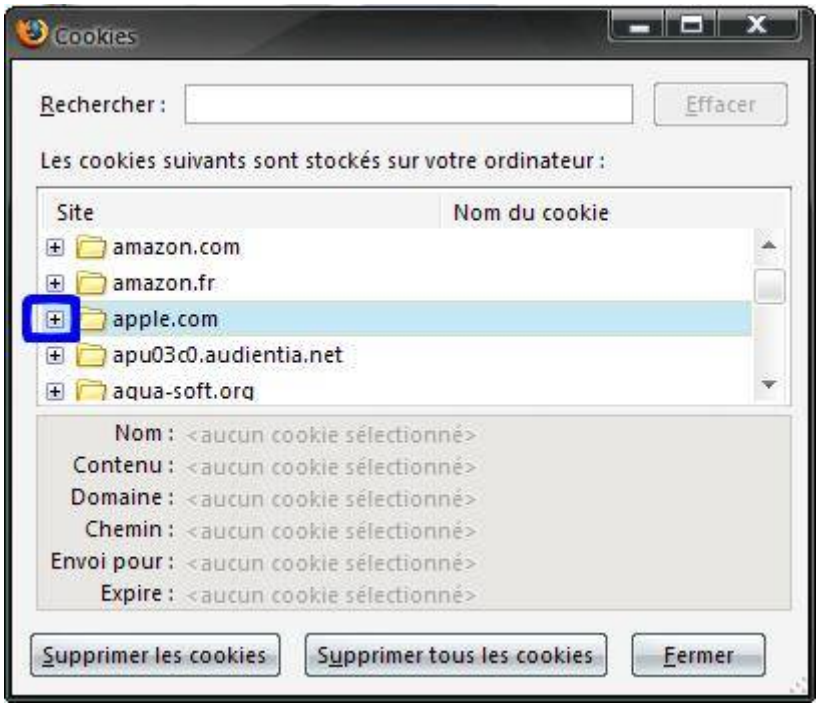
X.1.a.i) Effacer un ou plusieurs cookies avec Firefox

Sous Firefox, il faut cliquer sur le menu « Outils » puis sur « Options » (voir l'image ci-dessous) :

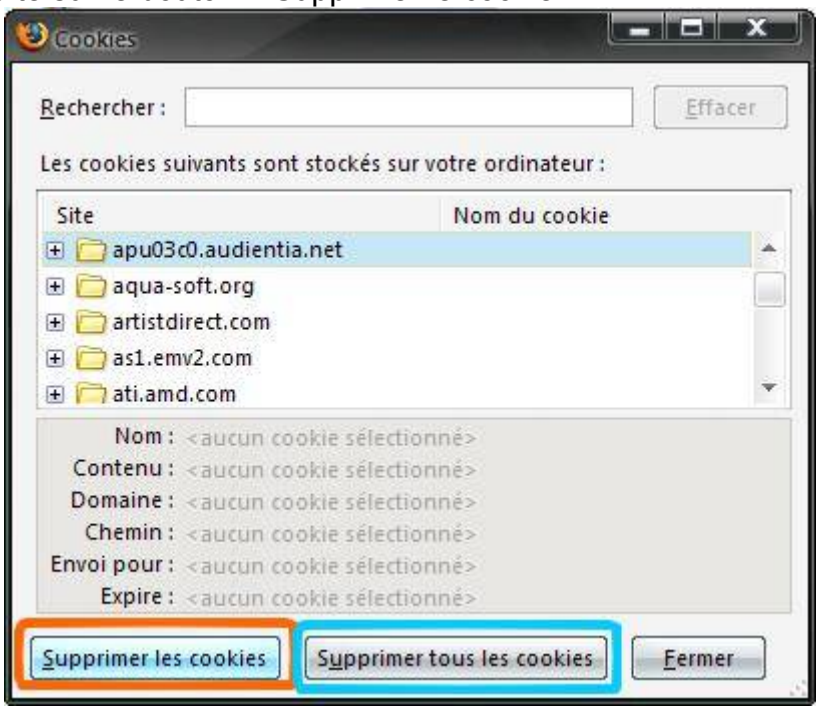


Cliquez ensuite sur Vie privée (cadre vert) puis sur le bouton « Afficher les cookies » :

Les cookies étant triés par site, il existe parfois plusieurs cookies par site. Cliquez sur le petit + devant chaque nom de site afin d'afficher tout les cookies de ce site :

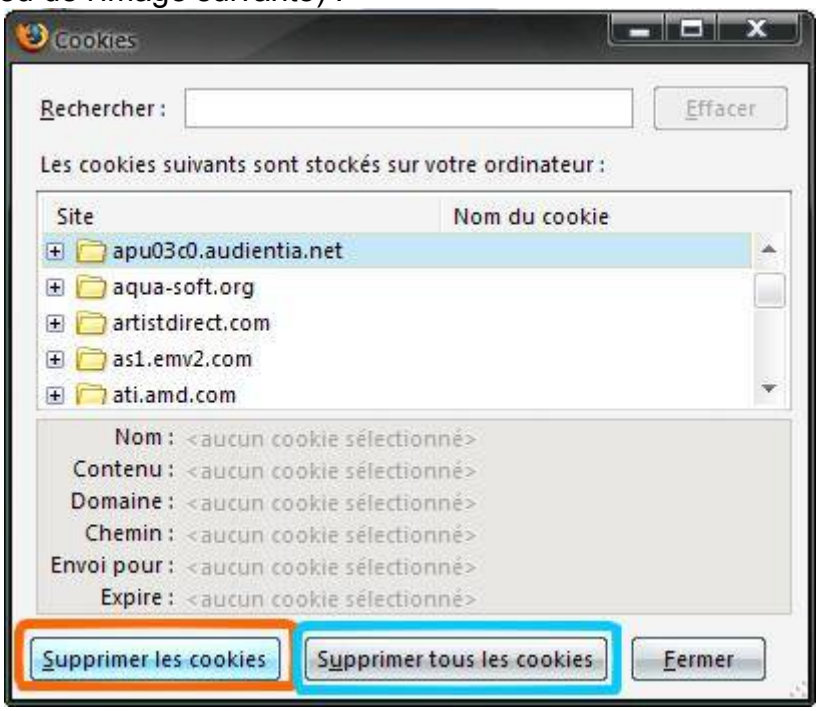


Cliquez ensuite sur le bouton « Supprimer le cookie » :



(Hors sujet : je n'ai rien contre Apple, au contraire, j'ai un iPod dont je suis très content, j'ai juste pris ce groupe de cookies en exemple)

Remarque : pour supprimer tout les cookies d'un site, il suffit de cliquer sur le nom du site et de cliquer sur le bouton « Supprimer les cookies » (cadre orange de l'image suivante), et pour supprimer l'intégralité de vos cookies, il est possible de cliquer sur « Supprimer tout les cookies » (cadre bleu de l'image suivante) :



X.1.a.ii) <u>Effacer un ou plusieurs cookies avec Internet Explorer</u>

Sous Internet Explorer 6 et 7 avec Windows XP : Allez dans le poste de travail, puis allez dans le disque dur (icône ou le nom contient très certainement « C: »). Puis allez dans le dossier « Documents and Settings ». Plusieurs dossiers se présenteront à vous, allez dans celui avec votre nom d'utilisateur (Si vous ne savez pas lequel c'est, cliquez sur le bouton Démarrer et tout en hait apparaîtra votre nom d'utilisateur). Allez dans le dossier « Local Settings » et enfin dans le dossier « Temporary Internet Files ». Vous y verrez entre autre des

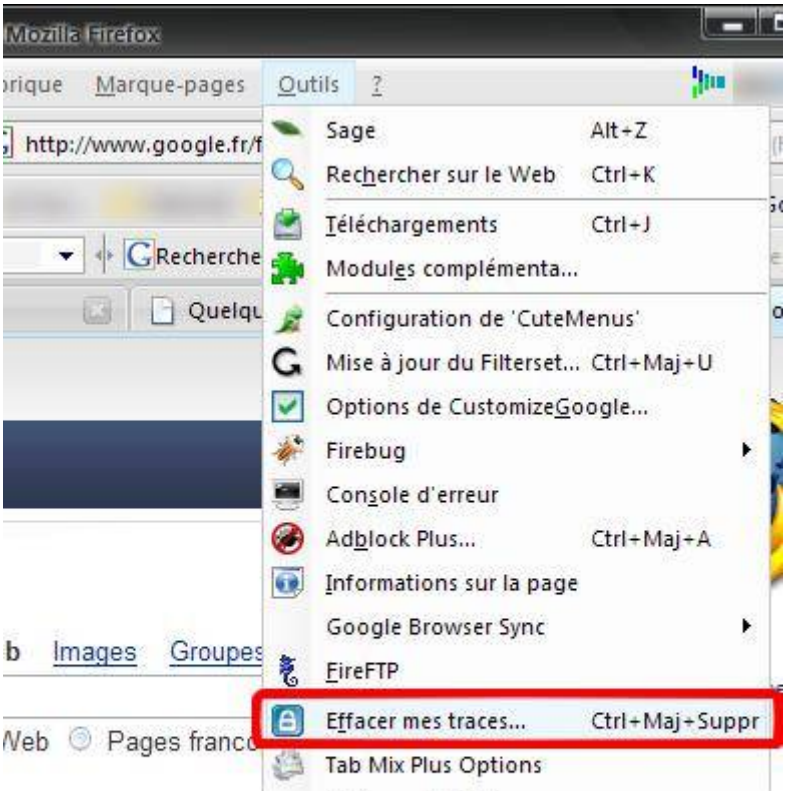
fichiers texte dont le nom commencera par « cookie ». Pour en supprimer un, il vous suffira de cliquer avec le bouton droit dessus et de cliquer sur « Supprimer ».

X.1.b) La méthode brutale

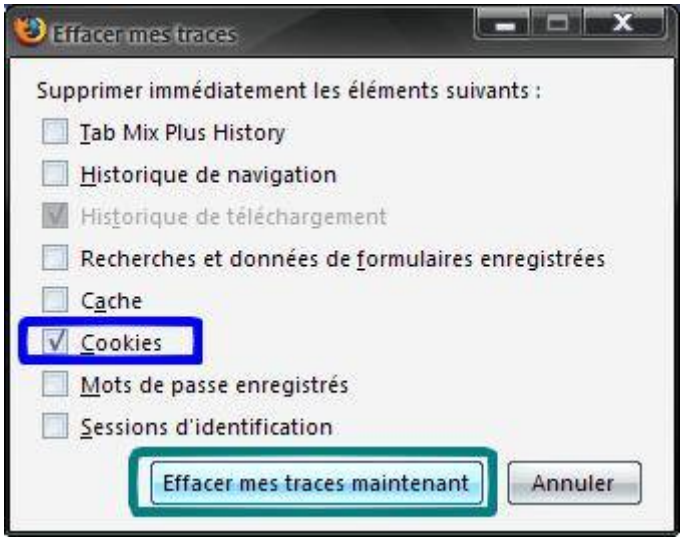
Cette méthode permet de supprimer l'intégralité des cookies de votre navigateur Internet.

X.1.b.i) Effacer tous les cookies avec Firefox

Pour cela, dans Firefox, cliquez sur le menu « Outils » puis cliquez sur « Effacer mes traces » :

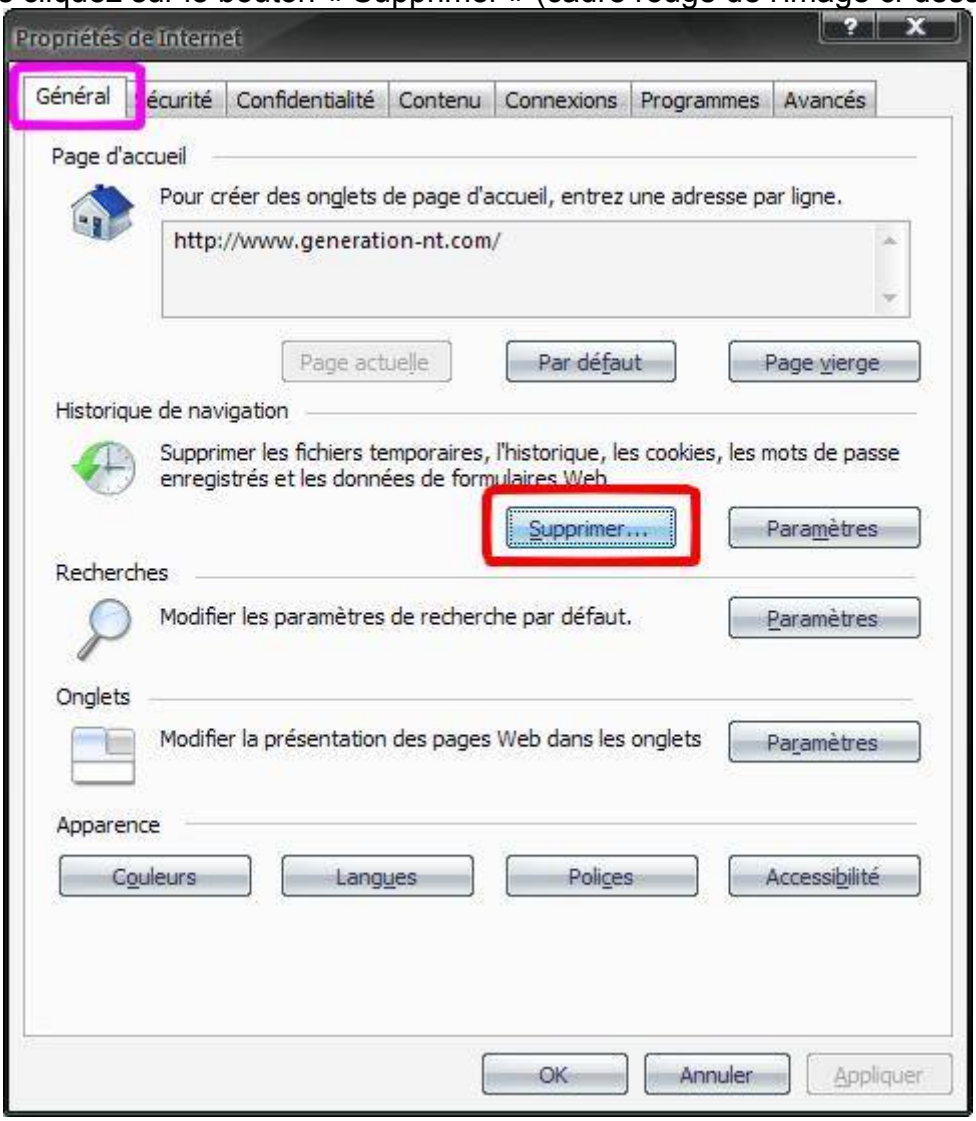


Cochez la case « Cookies » et décochez les autres (à moins que vous ne vouliez aussi enlever l'historique, nettoyer le cache, ...). Cliquez ensuite sur Effacer mes traces maintenant.

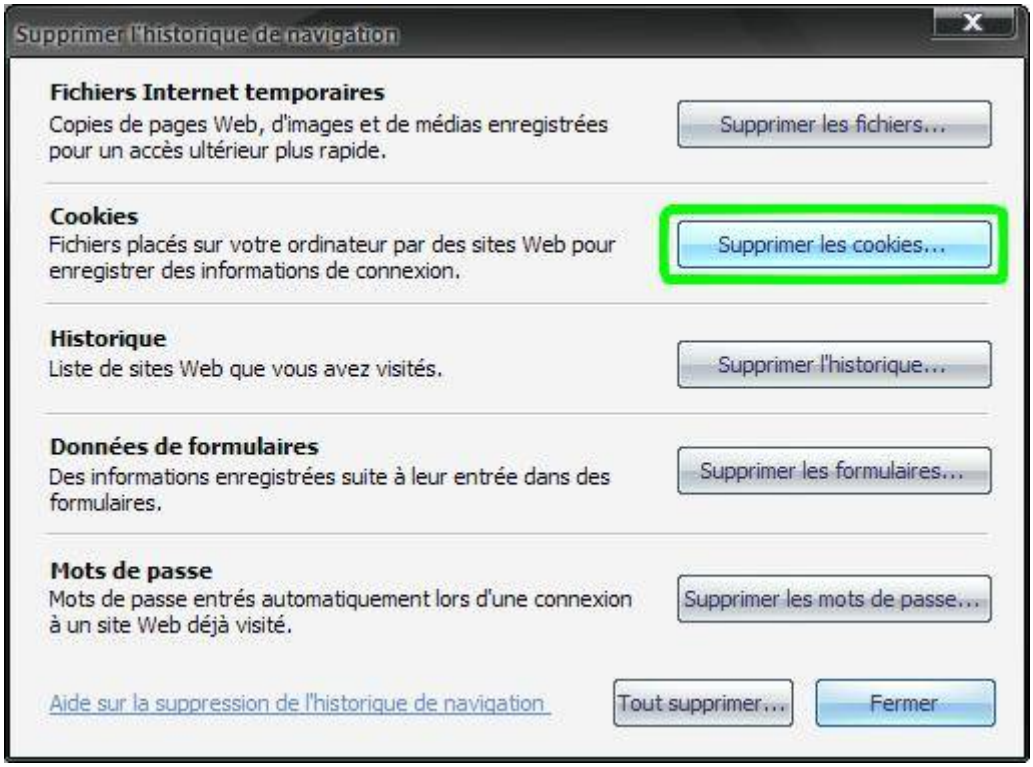


X.1.b.ii) <u>Effacer tous les cookies avec Internet Explorer 7</u>

Sous Internet Explorer 7, allez dans le Panneau de configuration, puis allez dans « Options Internet ». Ensuite, cliquez sur l'onglet « Général » (voir cadre magenta de l'image ci-dessous), puis cliquez sur le bouton « Supprimer » (cadre rouge de l'image ci-dessous) :



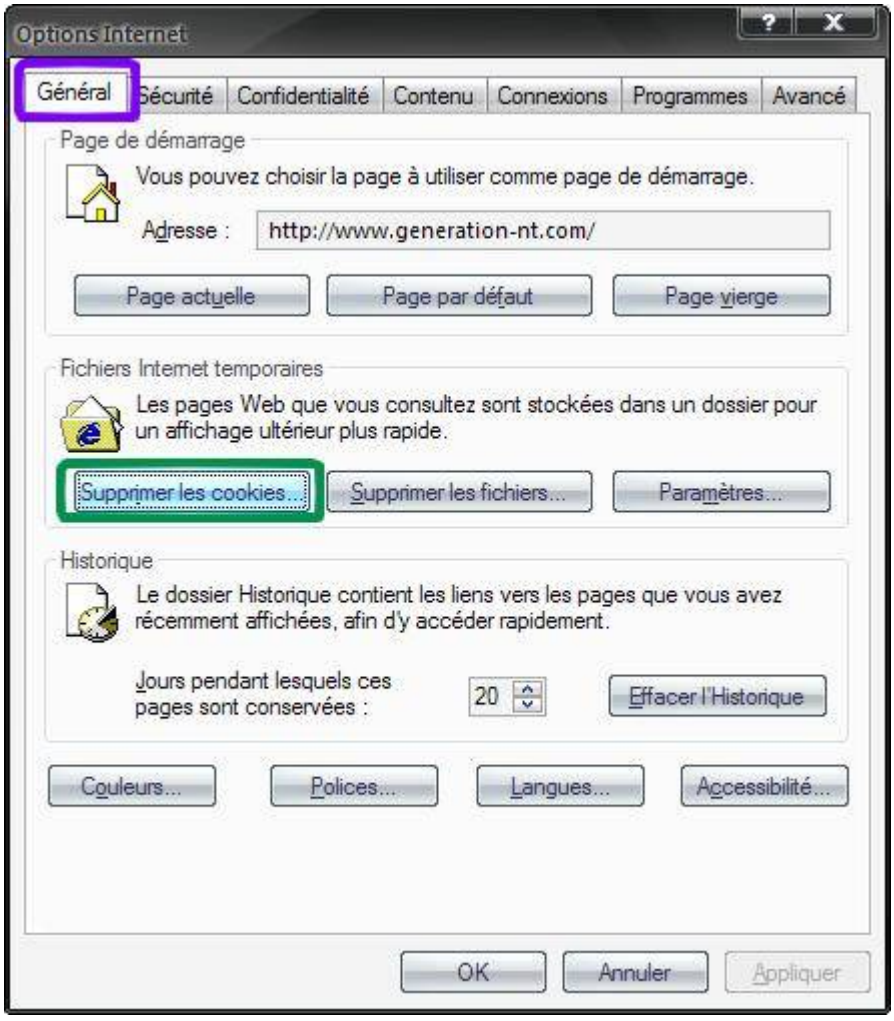
Cliquez ensuite sur le bouton « Supprimer les cookies... » :



Cliquez sur le bouton « Oui » puis cliquez sur le bouton Fermer et enfin sur le bouton « Ok ».

X.1.b.iii) <u>Effacer tous les cookies avec Internet Explorer 6</u>

Allez dans le Panneau de configuration, puis allez dans « Options Internet ». Ensuite, cliquez sur l'onglet « Général » (cadre violet) puis cliquez sur le bouton « Supprimer les cookies... » (cadre vert) :



Cliquez ensuite sur le bouton « Oui », et c'est terminé.

X.1.c) Conclusion sur les cookies

Les cookies étant tout de même des éléments utiles pour la navigation Internet (pour enregistrer des paramètres de pages tels que la langue, les identifiants et mots de passe, un certain nombre de réglages, ...), je recommande l'utilisation de la première méthode plutôt que les deux autres.

X.2) La fiabilité des sites selon McAffee

Pour Internet Explorer tout comme Mozilla Firefox (je n'ai pas testé pour les autres navigateurs, mais je pense que ça ne devrait pas poser de problèmes), McAfee propose une extension qui pourrait s'avérer utile.

Cette extension permet de vous avertir si le site représente un quelconque danger pour votre ordinateur, pour votre boîte e-mail (envoi de spams après inscription par exemple), pour votre compte en banque (phishing et autres arnaques), ...

Commençons déjà par installer cette extension :

La section Erreur : source de la référence non trouvée (page Erreur : source de la référence non trouvée) de ces pages vous permettra d'installer McAfee SiteAdvisor sous Firefox tandis que la section Erreur : source de la référence non trouvée (page Erreur : source de la référence non trouvée) vous permettra de l'installer sous Internet Explorer

La section Erreur : source de la référence non trouvée (page Erreur : source de la référence non trouvée) vous permettra d'apprendre à manipuler ce petit programme.

Il se peut que SiteAdvisor soit déjà dans votre ordinateur. Pour vérifier ceci, ouvrez votre navigateur Internet préféré, et regardez si dans la fenêtre du navigateur, quelque chose

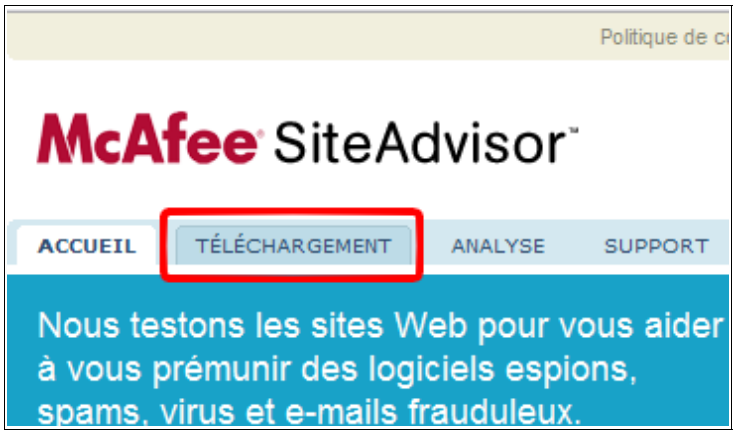
ressemblant à ceci apparaît :

Au lieu d'être vert, il se peut qu'il soit rouge, gris, ou jaune.
Si vous l'avez, alors SiteAdvisor est déjà installé.

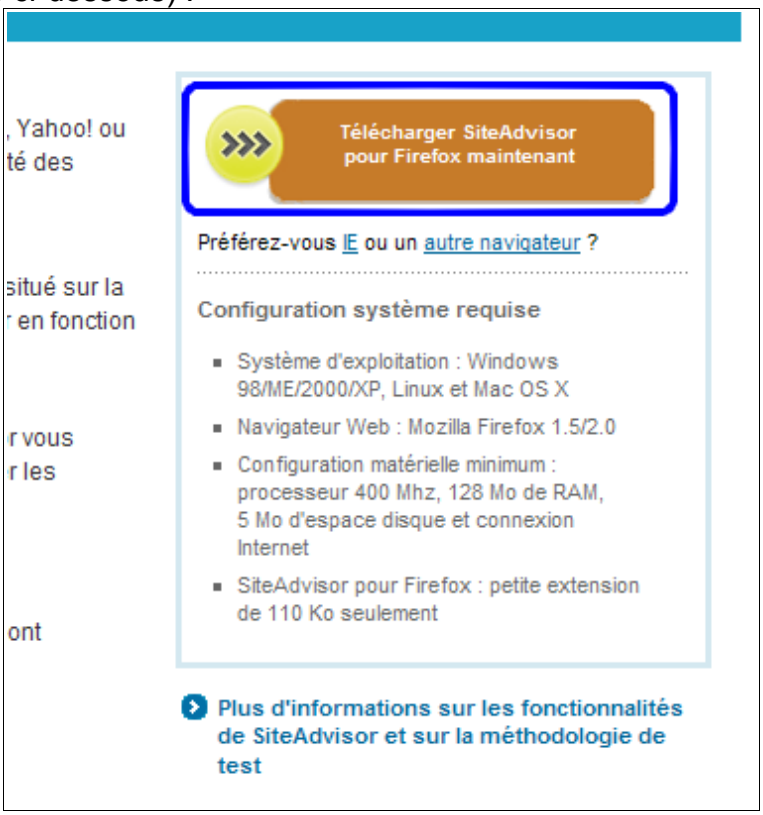
X.2.a) Installation de McAfee SiteAdvisor sous Firefox

Allez sur ce site : http://www.siteadvisor.com/

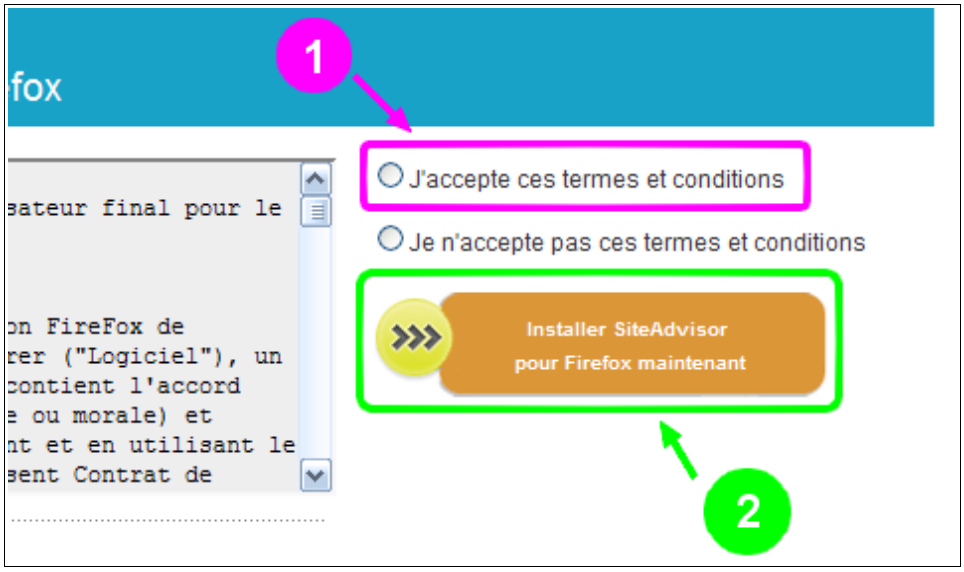
Cliquez ensuite sur l'onglet « Téléchargement » (voir cadre rouge de l'image ci-dessous) :

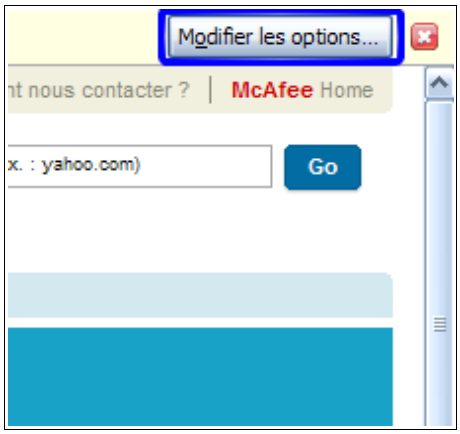


Cliquez ensuite sur le bouton « Télécharger SiteAdvisor pour Firefox maintenant » (voir cadre bleu de l'image ci-dessous) :



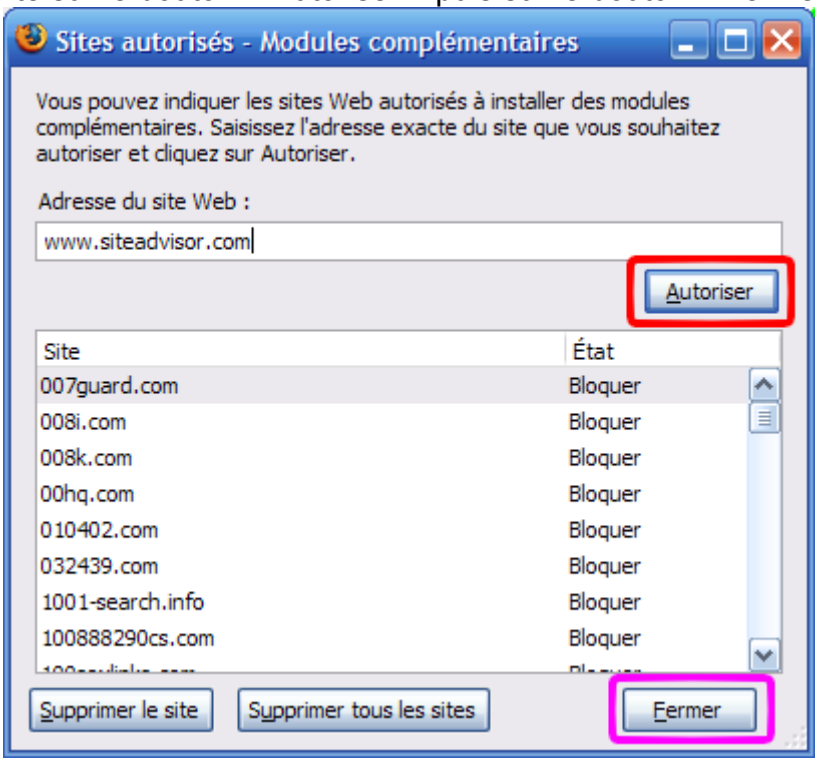
Cochez ensuite la case « J'accepte ces termes et conditions » (voir cadre violet de l'image ci-dessous) puis cliquez sur le bouton « Installer SiteAdvisor pour Firefox maintenant » (voir cadre vert) :



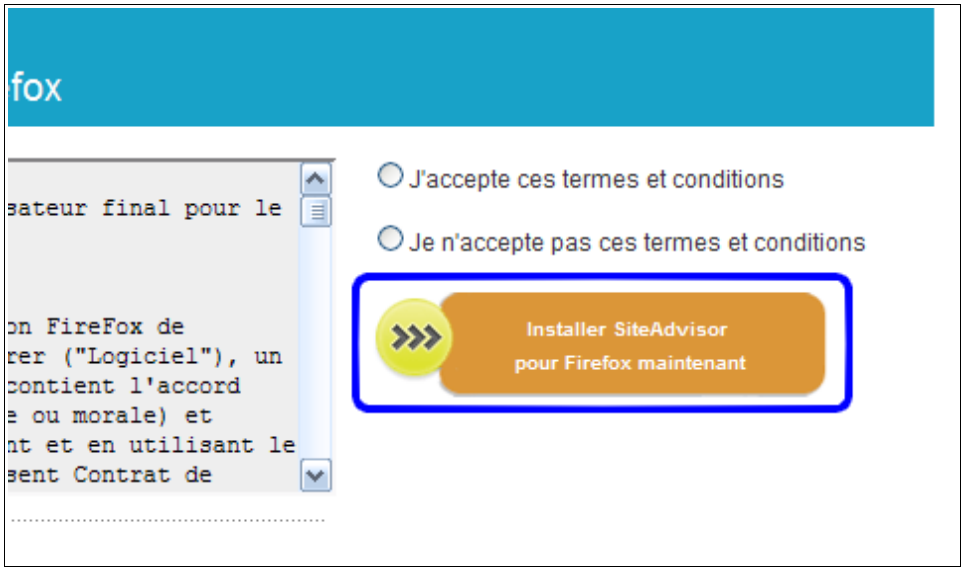


Cliquez ensuite sur le bouton « Modifier les options ».

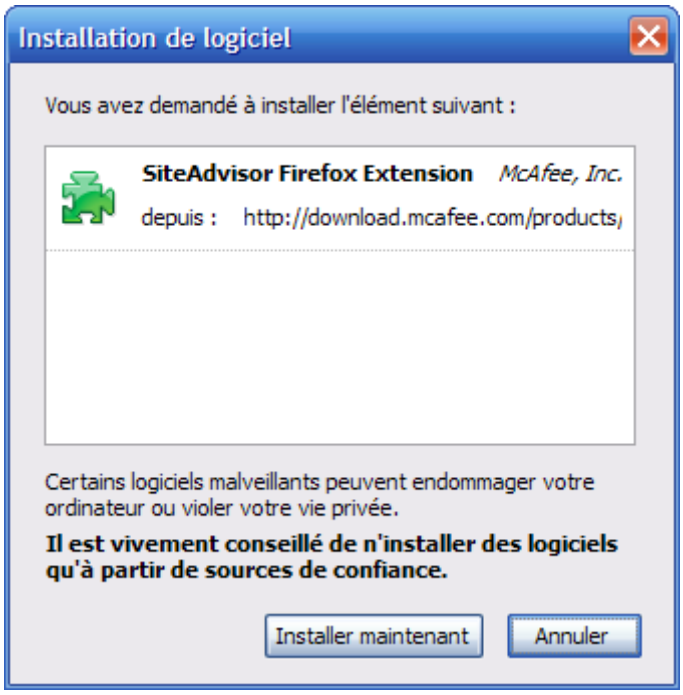
Cliquez ensuite sur le bouton « Autoriser » puis sur le bouton « Fermer » :



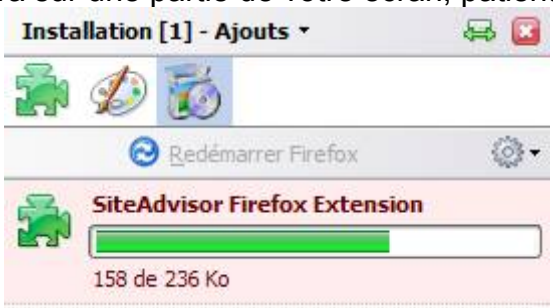
Cliquez de nouveau sur le bouton « Installer SiteAdvisor pour Firefox maintenant » (voir cadre bleu de l'image ci-dessous » :



Patientez quelques instants lorsque cette fenêtre apparaitra et vous pourrez cliquer sur le bouton « Installer maintenant » :



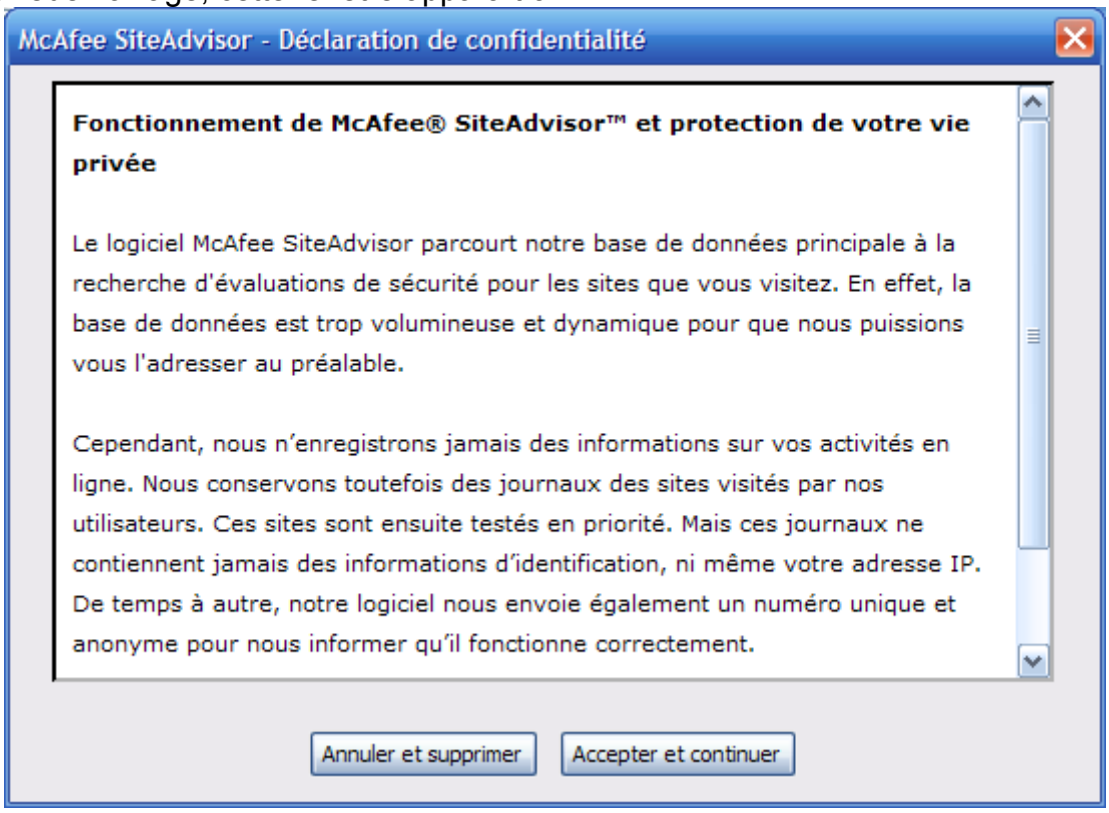
Lorsque ceci apparaitra sur une partie de votre écran, patientez quelques secondes :



Peu de temps après, le téléchargement de l'extension sera terminé. Cliquez sur le bouton « Redémarrer Firefox » quand il apparaîtra (voir cadre rouge de l'image ci-dessus).

Ceci redémarrera Firefox, ce qui fermera donc toutes les fenêtres ainsi que les téléchargements qui seraient en cours. Veillez donc à cliquer sur ce bouton uniquement si vous ne risquez pas de perdre du travail en cours.

Au redémarrage, cette fenêtre apparaîtra :



Cliquez sur Accepter et continuer.

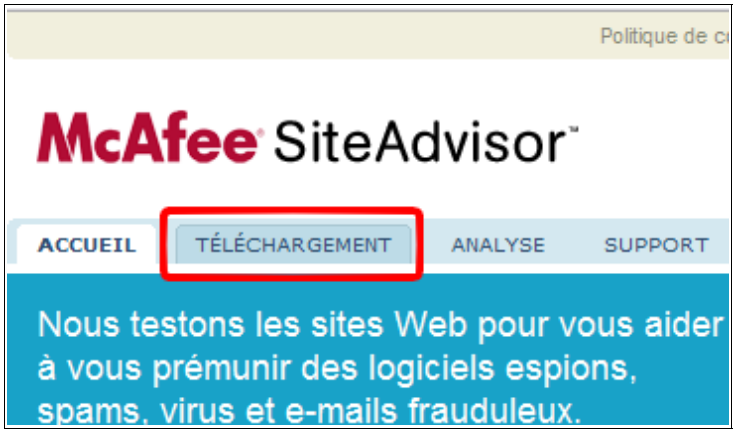
Firefox s'ouvrira, et en bas à droite apparaîtra un petit truc supplémentaire ressemblant à ceci :

Dans ce cas, ça signifie que l'installation a réussi.

X.2.b) Installation de McAfee SiteAdvisor sous Internet Explorer

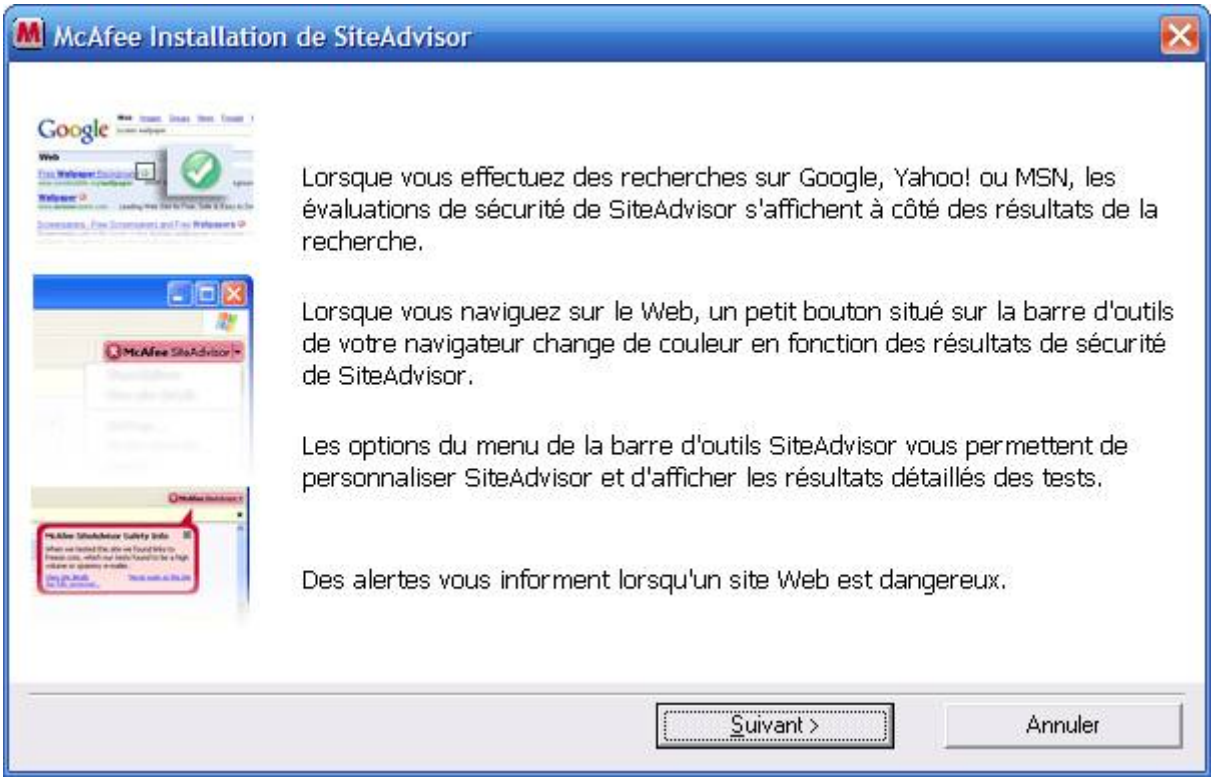
Allez sur ce site : http://www.siteadvisor.com/

Cliquez ensuite sur l'onglet « Téléchargement » (voir cadre rouge de l'image ci-dessous) :



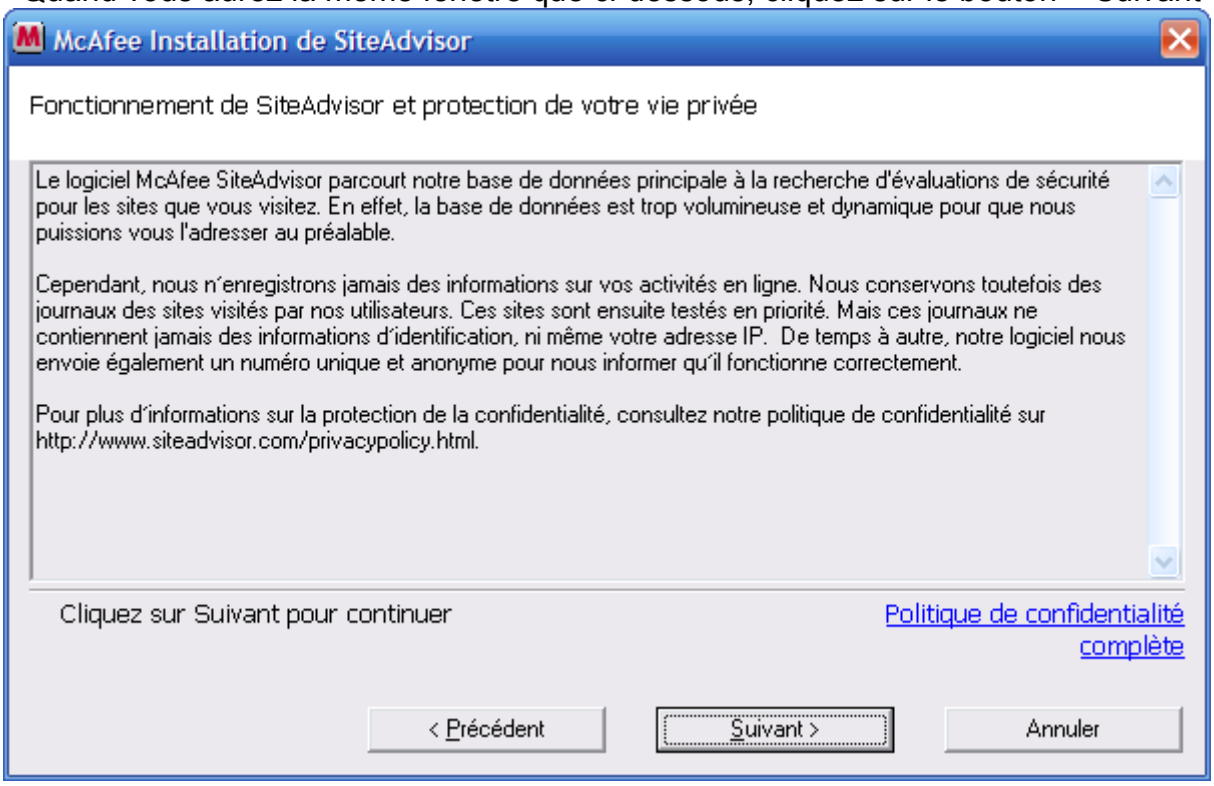
Cliquez ensuite sur le bouton « Télécharger SiteAdvisor » (voir cadre bleu de l'image ci-dessus).

Une fenêtre standard de téléchargement apparaît ensuite. Téléchargez le fichier.
Une fois téléchargé, ouvrez le fichier.

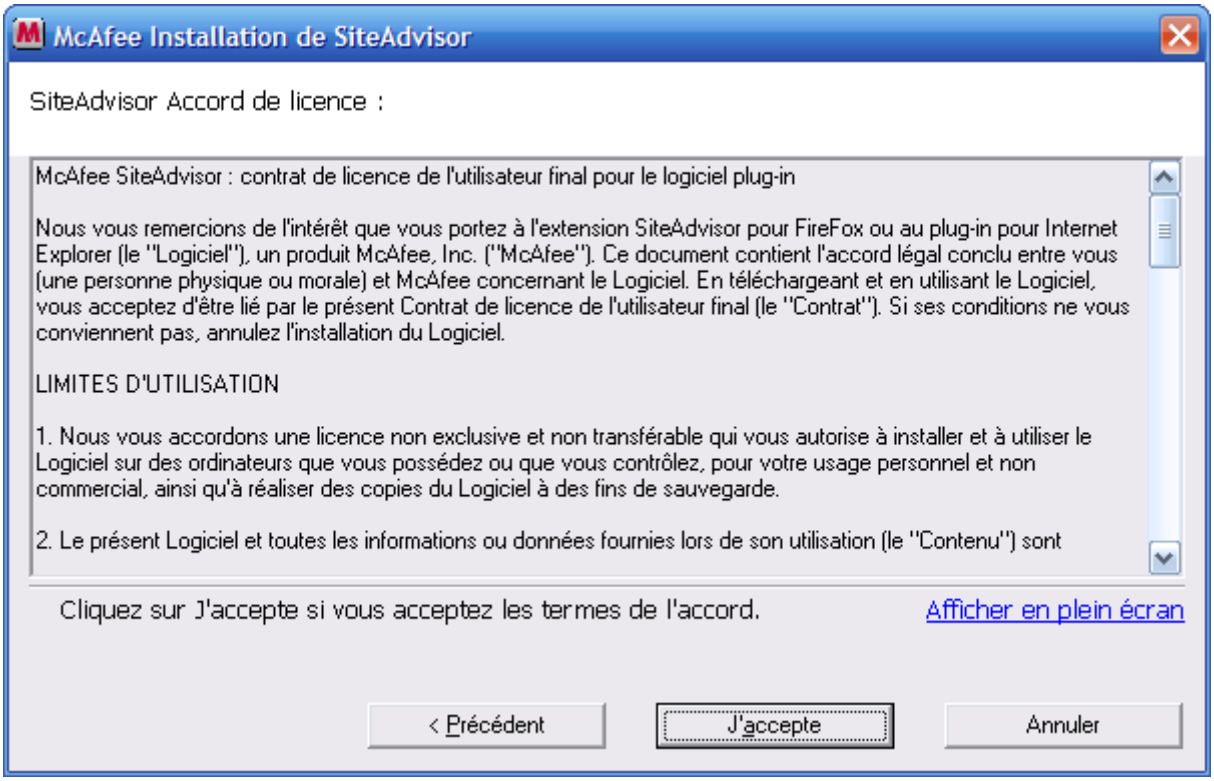


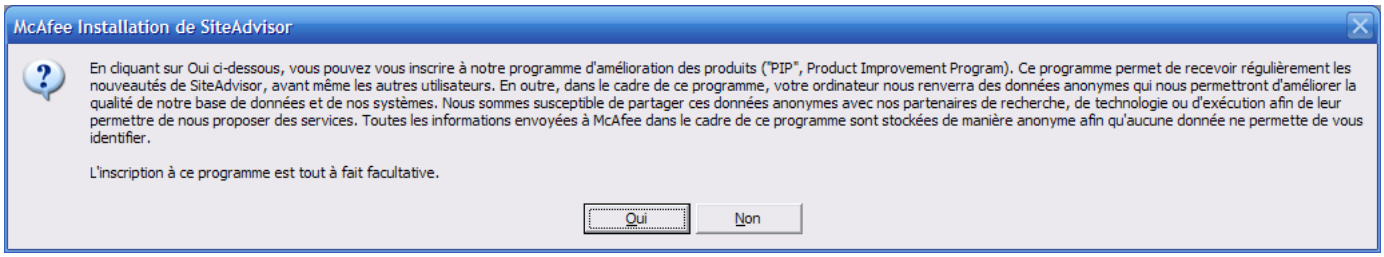
Quand vous aurez la même fenêtre que ci-dessus, cliquez sur le bouton « Suivant > ».

Quand vous aurez la même fenêtre que ci-dessous, cliquez sur le bouton « Suivant > » :



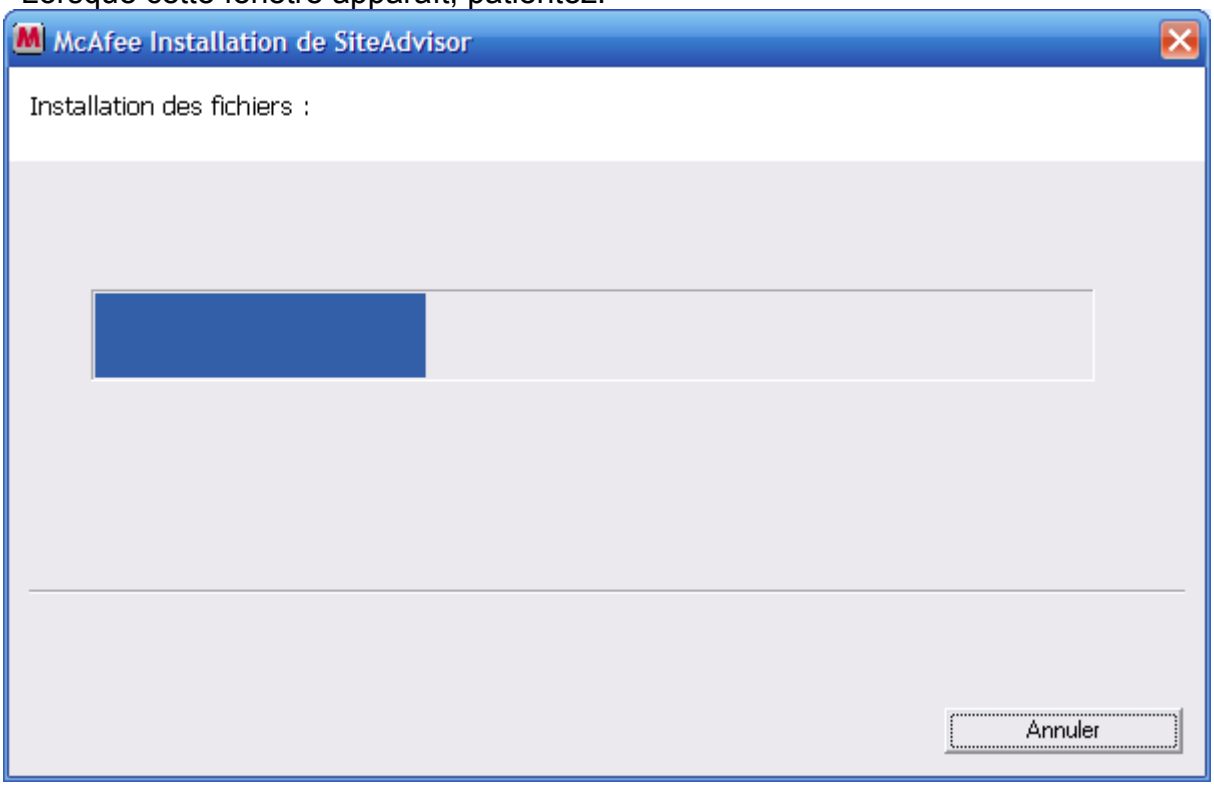
Cliquez ensuite sur le bouton « J'accepte » :



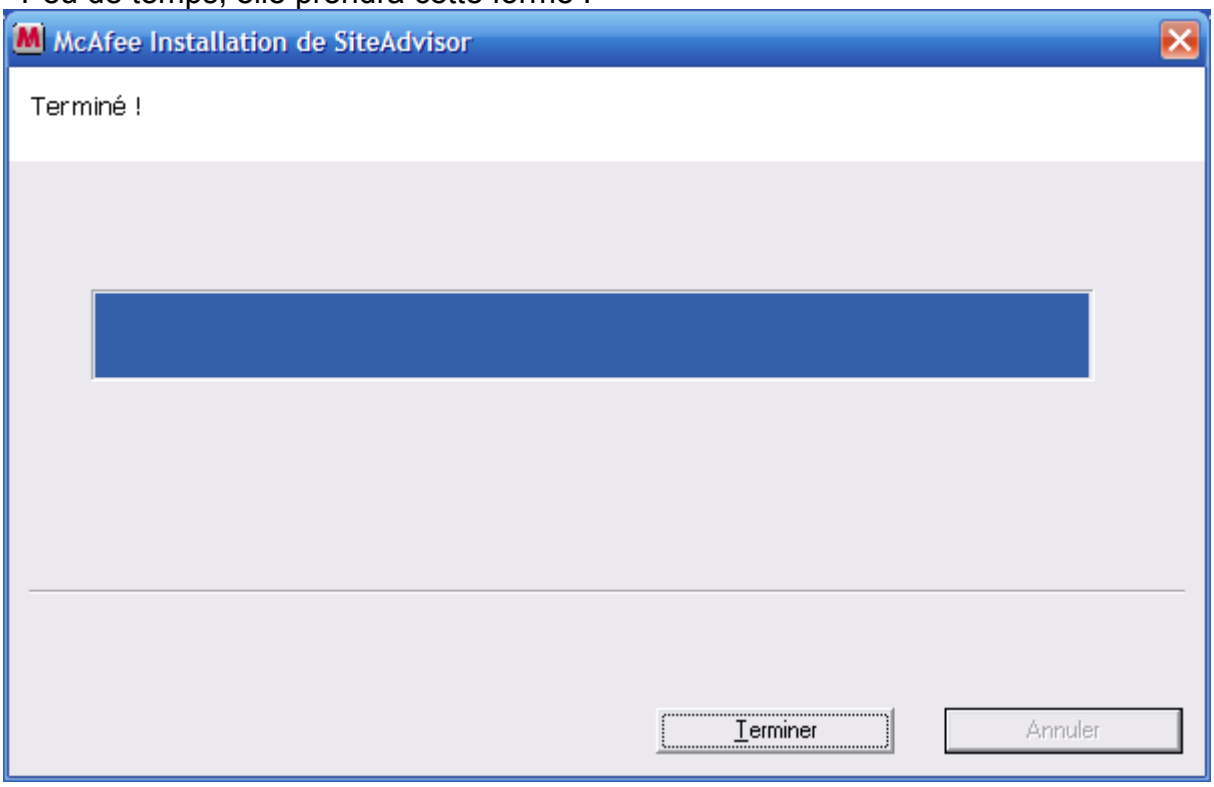


Cliquez sur le bouton « Oui ».

Lorsque cette fenêtre apparaît, patientez.



Peu de temps, elle prendra cette forme :



Cliquez sur le bouton « Terminer ».

Voilà, SiteAdvisor est installé !

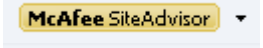
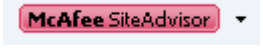
X.2.c) Fonctionnement et utilisation de McAfee SiteAdvisor

McAfee lance sur Internet des milliers de petits programmes afin d'analyser les pages pour savoir si elles représentent un danger ou non. De plus, les utilisateurs de McAfee SiteAdvisor peuvent aussi poster des commentaires sur les sites.

Ceci vous permet de savoir si le site sur lequel vous naviguez est fiable ou non.

Cependant, McAfee ne peut avoir analysé la totalité d'Internet, de nouveaux sites étant créés tout les jours. Ce qui fait que parfois, aucune information n'est disponible pour un site donné.

Il y a donc plusieurs états à SiteAdvisor :

- Le site n'a pas encore été analysé : 
- Le site a été analysé et est fiable : 
- Le site peut avoir des effets négatifs : 
- Le site est à éviter : 

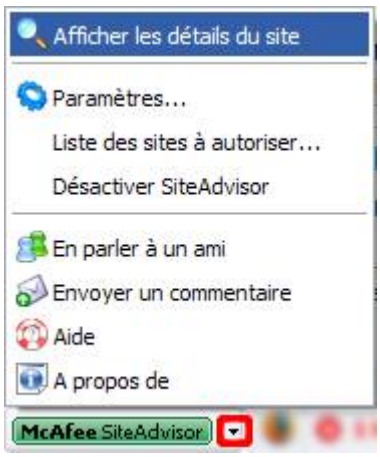
Les résultats sont à relativiser dans le cas ou l'avertisseur est jaune et rouge :

Parfois, les sites envoient du spam et sont marqués en rouge. Ça peut être le seul effet négatif de ce site. Du coup, en évitant d'entrer son adresse e-mail, il n'y a aucun risque sur le site.

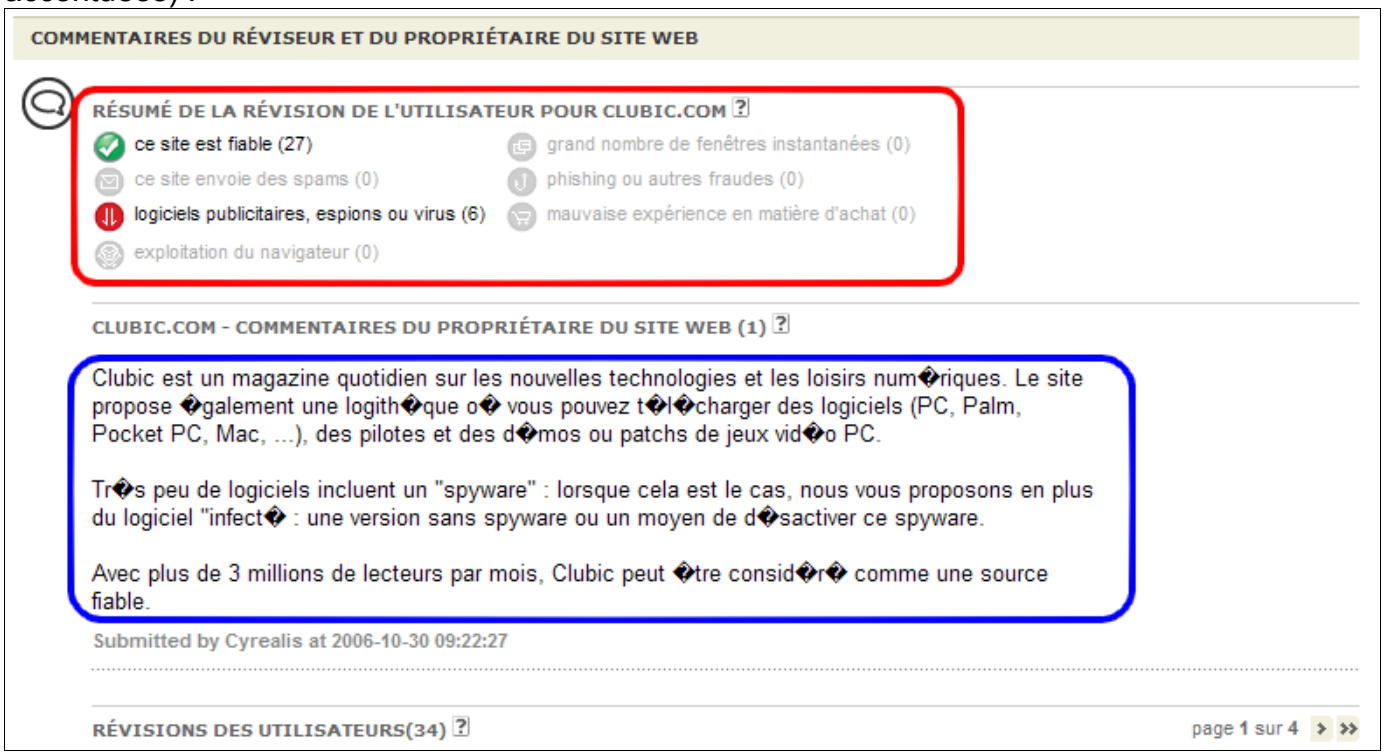
Ou encore, le cas Messenger Plus!. Ce programme permet d'améliorer Windows Live Messenger en lui ajoutant un certain nombre de fonctions plus ou moins utiles. Cependant, le programme d'installation abrite un logiciel considéré comme logiciel espion. Il est tout à fait possible de refuser le logiciel espion à l'installation (en refusant le sponsor). Ce qui fait au final que Messenger Plus! est à peu près sûr. Or, certains sites ne proposent que ce téléchargement de litigieux. Ce qui leur vaut un classement rouge.

Un dernier cas est aussi les sites menant à des sites classés rouges. Ceux-ci sont souvent classés comme rouges aussi si un trop grand nombre de leur liens est classé comme rouge.

Bref, un certain nombre de sites est tout à fait légitime. Pour vérifier dans le cas ou le site serait classé rouge si le site est légitime ou non, il suffit de cliquer sur la flèche à côté de l'avertisseur (voir cadre rouge de l'image ci-dessous) puis de cliquer sur « Afficher les détails du site » :



Vous aurez parfois sur le site un descriptif donné par l'éditeur (voir cadre bleu ci-dessous / comme vous pourrez le voir, SiteAdvisor a quelques problèmes avec les lettre accentuées) :



Il y a aussi les avis donnés par les utilisateurs (voir cadre rouge de l'image ci-dessus) et à la fin de la page Internet de SiteAdvisor.

Bref, vous pourrez juger si le site est fiable ou non avec l'aide de SiteAdvisor et ses utilisateurs.

X.3) Activation/Désactivation des scripts Javascript

Il existe une extension pour Firefox qui permet d'activer ou de désactiver les scripts Javascript à volonté.

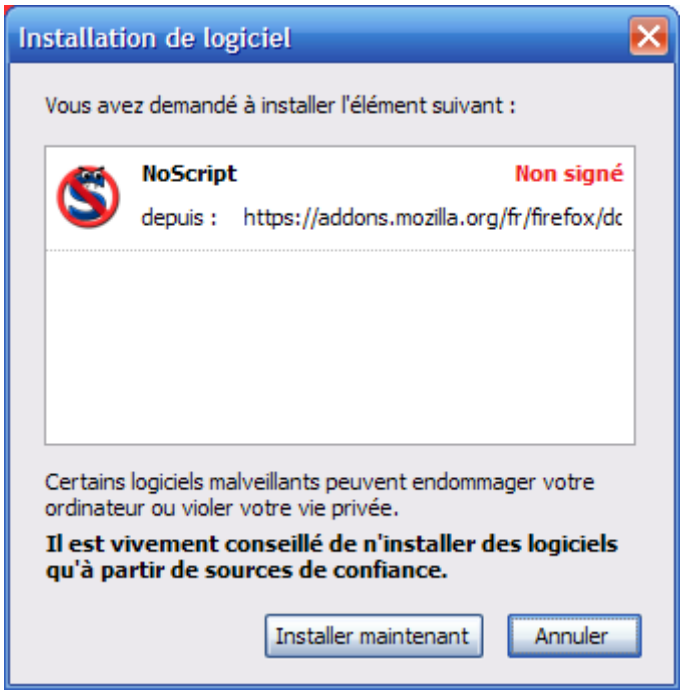
Cette extension fonctionne sur le principe de la liste blanche. C'est à dire que par défaut, tout est bloqué. C'est à vous, via l'extension, d'activer ou non les scripts d'un site donné. Cette extension peut donc se révéler contraignante au moins au début, car très nombreux sont les sites à utiliser le Javascript. Et bien qu'il soit souvent possible de naviguer sur ces mêmes sites, il est parfois nécessaire d'activer le Javascript pour certains sites.

Cependant, il arrive un moment ou on navigue toujours sur les mêmes pages, donc cette extension finit par se faire oublier.

X.3.a) Installation de NoScript

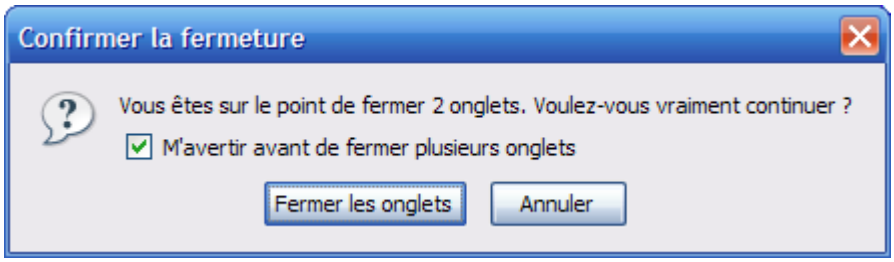
Allez sur cette page : https://addons.mozilla.org/fr/firefox/addon/722

Cliquez ensuite sur le bouton « Ajouter à Firefox » (voir cadre violet de l'image ci-dessus).



Patientez quelques secondes et cliquez sur le bouton « Installer maintenant ».

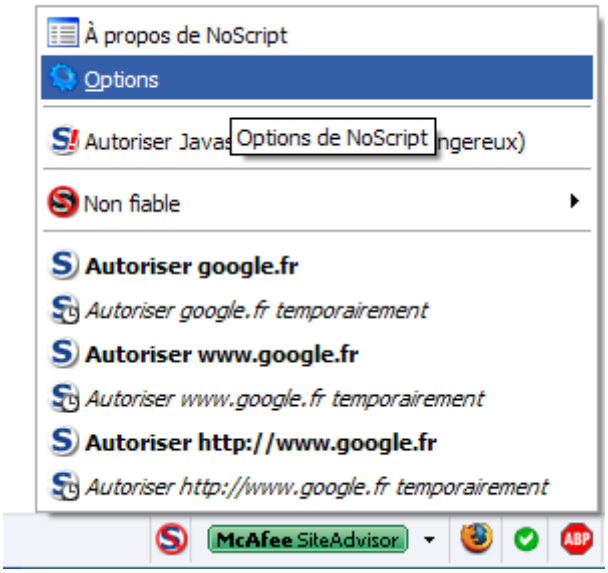
Patientez quelques secondes, et cliquez sur le bouton « Redémarrer Firefox ».



Si vous avez cette fenêtre, cliquez sur le bouton « Fermer les onglets ».

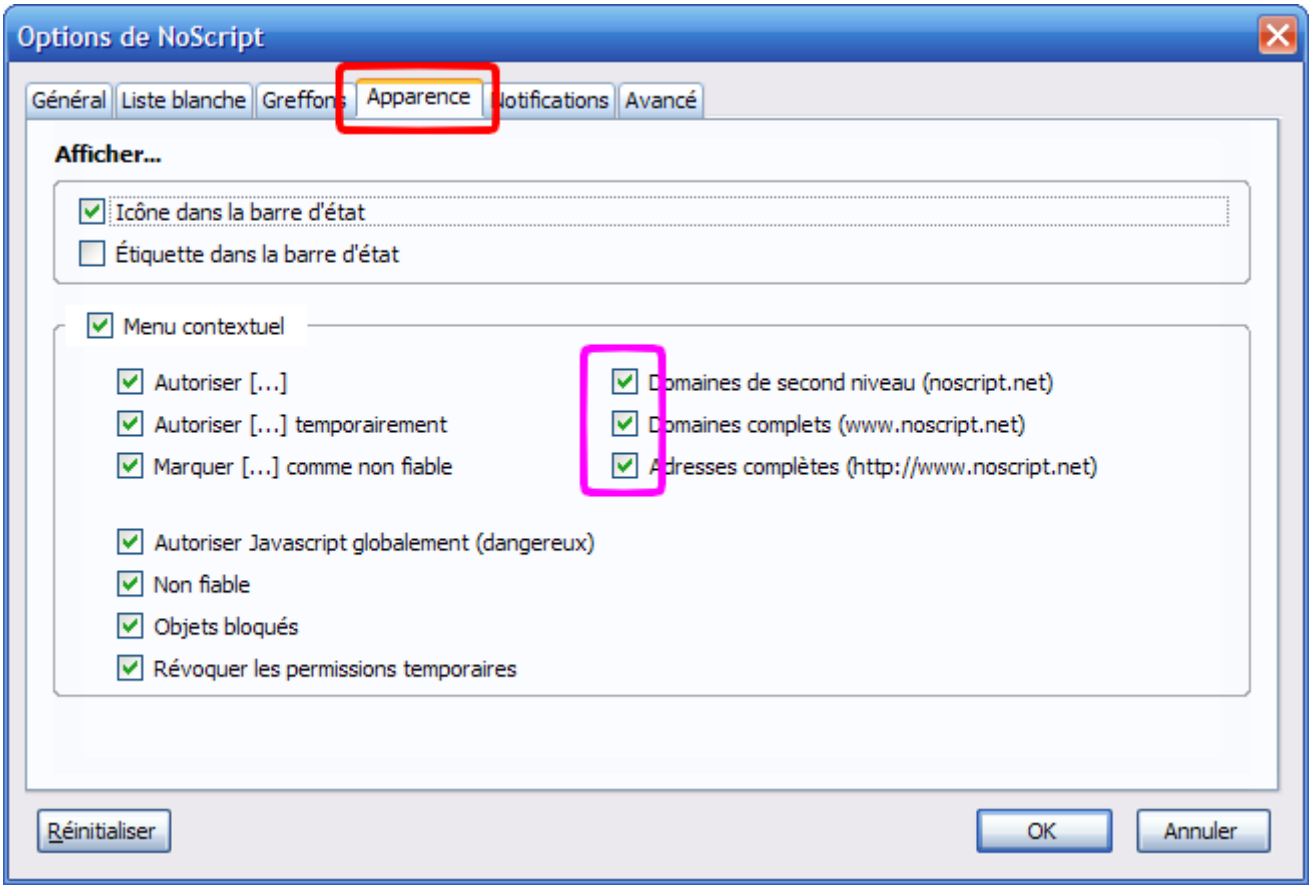
Voilà, une fois que Firefox réapparaîtra, NoScript sera installé.

X.3.b) Quelques réglages de NoScript

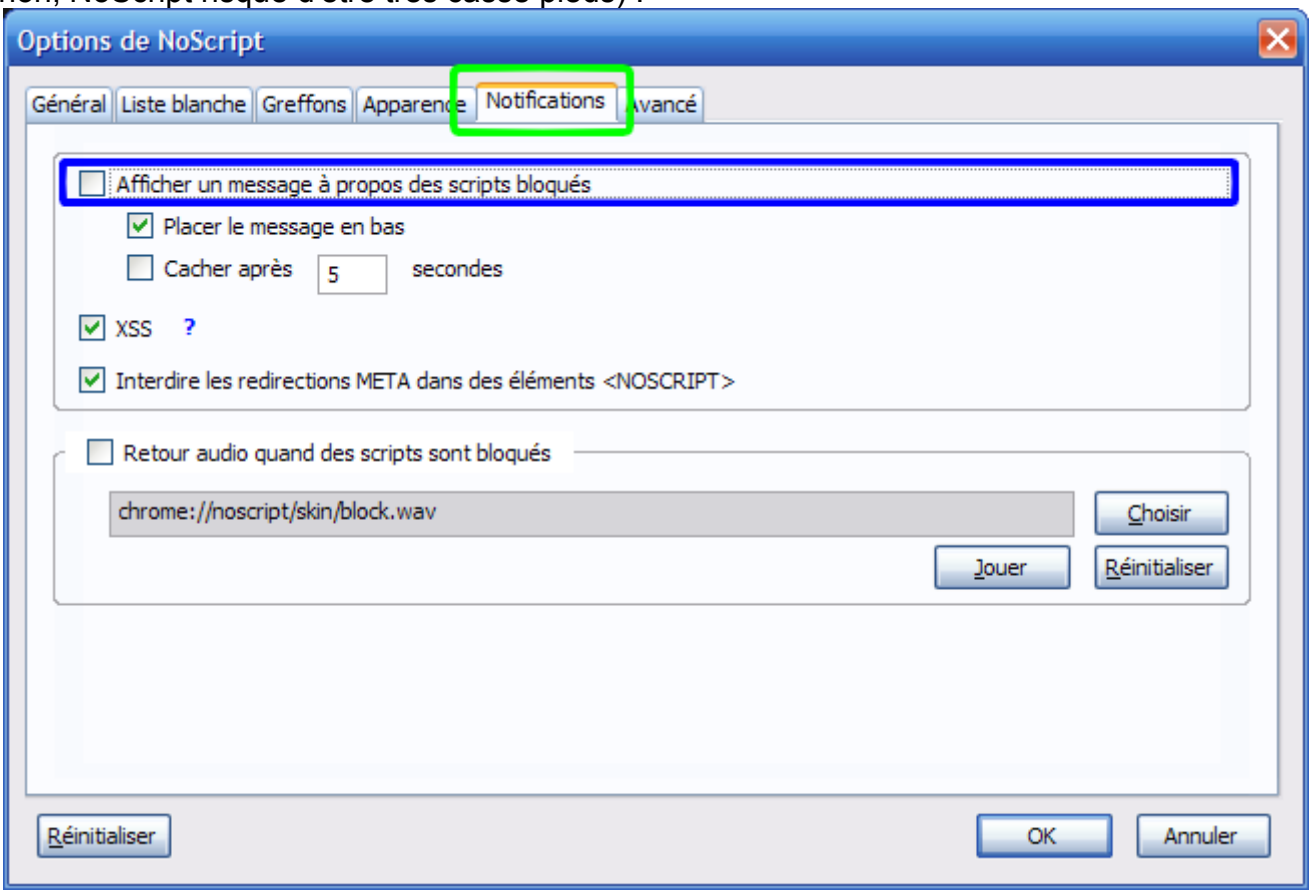


Cliquez sur l'icône de NoScript tout en bas à droite dans la fenêtre de Firefox (elle peut être l'une des icônes suivantes :), puis cliquez sur Options (voir image ci-dessus).

Cliquez ensuite sur l'onglet Apparence (voir cadre rouge de l'image ci-dessous). Cochez les trois cases nommées « Domaines de second niveau », « Domaines complets »



Allez ensuite dans l'onglet « Notifications » (voir cadre vert de l'image suivante) et décochez la case « Afficher un message à propos des scripts bloqués » (voir cadre bleu / car sinon, NoScript risque d'être très casse pieds) :

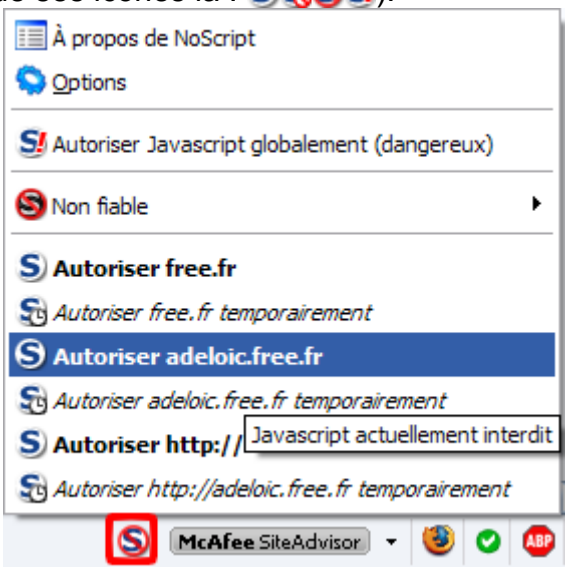


X.3.c) Utilisation de NoScript

Il arrive souvent qu'il y ait des sites qui fonctionnent un peu mal voir pas du tout.

Dans ce cas, vous avez deux façons de réactiver les scripts Javascript. Vous pouvez les activer définitivement ou juste temporairement.

Pour ceci, il suffit de cliquer sur l'icône de NoScript en bas à droite de la fenêtre de Firefox (elle peut avoir une de ses icônes là :).



Cliquez ensuite sur la ligne correspondant au site sur lequel vous êtes.

Prenez de préférence l'adresse complète du site (regardez dans la barre d'adresses de votre navigateur Internet préféré si vous ne vous souvenez pas de l'adresse du site sur lequel vous êtes), avec ou sans les http://. Imaginons que vous cliquiez sur « Autoriser free.fr » par rapport à l'image ci-dessus, vous autoriseriez la totalité des sites hébergés par Free, et donc plusieurs milliers de sites, et donc quelques uns qui sont sans doutes pas forcément très fiable.

Vous pouvez autoriser temporairement les scripts Javascript d'un site en cliquant sur la ligne avec le S et l'horloge ( ) correspondant au site.

Il se peut qu'il y ait énormément de lignes proposées pour accepter des Javascript, mais prenez de préférence l'adresse du site d'origine.

X.3.d) Recommandations de dernière minute à propos de NoScript

Ne connaissant pas comment sont conçus les sites de vente en ligne, j'aurai plutôt tendance à vous recommander d'accepter temporairement l'intégralité des scripts Javascript et de les désactiver tout après. Car il serais dommage de faire échouer la transaction à cause de scripts non activés, que vous soyez facturé et que vous ne receviez jamais votre achat.

Voici la procédure pour tous les activer :

Cliquez sur l'icône de NoScript en bas à droite de la fenêtre de Firefox, puis cliquez sur « Autoriser Javascript globalement (dangereux) ».

Pour les réactiver, cliquez sur l'icône de NoScript et cliquez sur « Interdire Javascript globalement (recommandé) » :

X.3.e) Conclusion sur NoScript

Les scripts Javascript sont à peu près sur la totalité des sites Internet. Certains ne sont pas indispensables, et même parfois, certains sites ont une version spéciale sans Javascript.

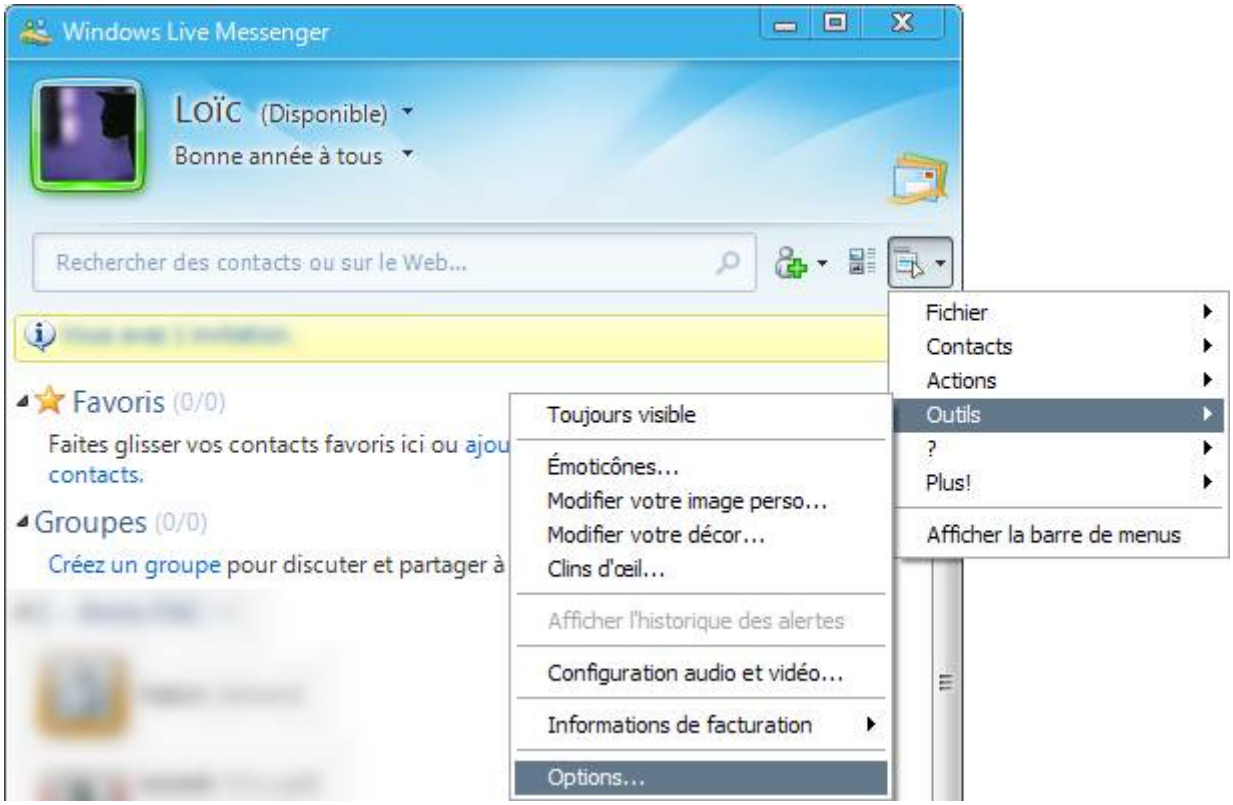
Bref, NoScript peut s'avérer être une extension intéressante pour augmenter la sécurité de la navigation sur Internet. Et bien qu'elle peut être assez casse pieds au début, on navigue régulièrement sur les mêmes sites Internet, et donc les réglages sont de moins en moins nombreux à faire au cours du temps.

J'aurai tendance à vous la recommander cette extension.

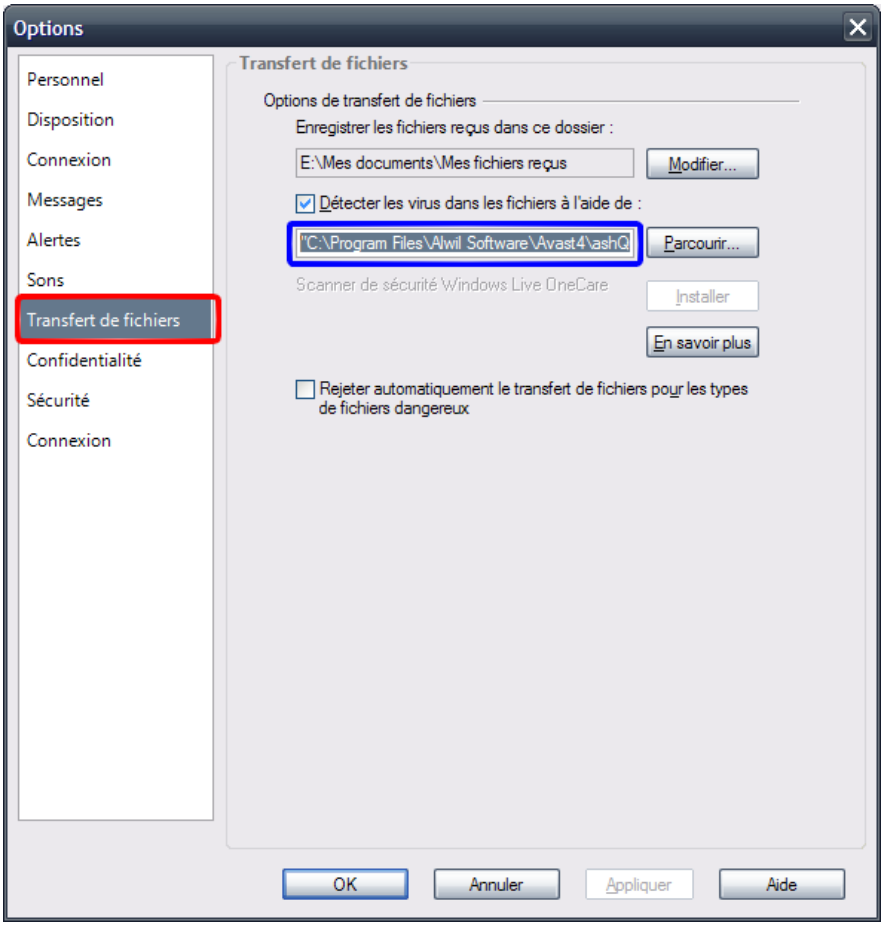
X.4) Windows Live Messenger 2009 et les transferts de fichiers

Windows Live Messenger propose d'analyser les fichiers que vous recevez lors d'une discussion afin d'y déceler des virus. Cela part d'un bon sentiment, mais le problème est que le scanner qui analyse les fichiers se met à jour à chaque téléchargement (ou presque) avant d'analyser enfin le fichier.

On va donc utiliser Avast pour analyser les fichiers transférés. Pour ceci, ouvrez la fenêtre principale de Windows Live Messenger.



Allez ensuite dans le menu « Outils » et cliquez sur « Options ».



Cliquez ensuite sur « Transfert de fichiers », cochez la case « Détecter les virus à l'aide de : » et dans la zone de texte juste en dessous, mettez ceci (en mettant aussi les guillemets) : "C:\Program Files\Alwil Software\Avast4\ashQuick.exe" "%1"

Si vous ne voulez pas réécrire la ligne ci-dessus (ce que je peux aisément comprendre), cliquez sur le bouton « Parcourir » et via la fenêtre qui apparaît, recherchez le fichier C:\Program Files\Alwil Software\Avast4\ashQuick.exe.

Ensuite, ajoutez à la main à la fin de la ligne un espace suivit par "%1" (en mettant les guillemets).

Cliquez ensuite sur OK.

XI) Une analyse régulière

Pour être sûr de la sécurité de son ordinateur, il vaut mieux faire une analyse et une mise à jour régulière de ses logiciels de protection.

Je vous recommande de faire une analyse tout les trois mois (au minimum, vous pouvez bien sûr le faire plus souvent) si rien ne cloche. Et si le comportement de votre ordinateur vous semble suspect, je vous recommande de faire une analyse maintenant.

Bien entendu, la périodicité d'analyse que je recommande dépend aussi de l'utilisation que vous faites de votre ordinateur !

Voici une liste des choses à effectuer :

• Mise à jour de son antivirus (Avast le fait automatiquement, mais vous pouvez forcer la mise à jour si vous le désirez, voir section Erreur : source de la référence non trouvée page Erreur : source de la référence non trouvée)

• Analyse antivirus (voir section Erreur : source de la référence non trouvée page Erreur : source de la référence non trouvée)

• Mettre à jour SpywareBlaster et protéger votre ordinateur (section Erreur : source de la référence non trouvée page Erreur : source de la référence non trouvée)

• Mettre à jour Spybot, vacciner son système et lancer une analyse (sections Erreur : source de la référence non trouvée à Erreur : source de la référence non trouvée, pages Erreur : source de la référence non trouvée à Erreur : source de la référence non trouvée).

XII) Conclusion

La conclusion de ces quelques pages précédentes serait qu'il faut absolument perdre la clicomanite aiguë. Il faut toujours réfléchir à ce qu'il se passe sur votre écran, et dès que quelque chose sors de l'ordinateur, il faut toujours se poser les bonnes questions, ça aide beaucoup à bien répondre.

Bref, sur votre ordinateur, réfléchissez avant d'agir !

Mais n'oubliez pas non plus d'analyser de temps en temps non plus.

XIII) Annexes

XIII.1) Liste non exhaustive de réponse à fournir à Comodo Internet Security

Ces quelques listes fournissent des indications sur des programmes connus que je juge fiables (ou non). Vous pouvez répondre comme ce que je vous conseille, cependant, si vous n'avez pas ces programmes d'installés, et que Comodo Internet Security vous demande pour un des programmes que vous n'avez pas, méfiez vous, réfléchissez et informez vous sur le contenu de votre PC.

Cette section est séparée exprès des autres (il y a un gros blanc sur la page précédente) afin de vous permettre de facilement la réimprimer en cas de mise à jour importante.

• Conserver et Autoriser : les logiciels de protection

Avast (tout modules)	PeerGuardian
Spybot	Windows Defender
SpywareBlaster	SiteAdv.exe
AVG	SAService

• Conserver et Autoriser : les programmes nécessitant Internet pour fonctionner

Google Earth	Google Talk
CrossLoop (et vncviewer)	Skype
adslTV	Yahoo Messenger
RssBandit	FileZilla
Mozilla Firefox	Miro
Mozilla Thunderbird	VDownloader
Internet Explorer	TubeMaster
Opera	RaimaRadio
Windows Live Messenger	Windows Live Writer
Bittorrent	MSN Messenger
Yahoo Widgets (widgets Internet)	
TerraExplorer (GeoPortail 3D)	
Free Download Manager	
FlashGet	

• Conserver et autoriser : les modules de mises à jour de composants ou de logiciels, et les logiciels se mettant à jour :

Adobe Updater	ManyCam (pour les mises à jour de

	ManyCam)
Yahoo Auto Updater	Unlocker (pour les mises à jour de Unlocker)
TMUpdate.exe (module de mises à jour de TubeMaster)	

• Programmes et composants (du système d'exploitation) moins évidents à conserver et autoriser

Volet Windows (Sous Vista, pour les gadgets nécessitant Internet : météo, flux RSS, ...)	
Processus hôte pour les services Windows (Vista) / Generic Host Process (XP, 2000)	
Application sous-système spouleur	
Service partage réseau du lecteur Windows Media	
Consolidateur SQM Windows (ils ont de ces noms parfois chez Microsoft)	
Windows Problem Reporting	
Microsoft Feeds Sychronisation (Synchronisation des flux RSS dans Vista)	
Processus de l'autorité de sécurité locale	
Gestionnaire de mises à jour du magasin Windows Media Center	
Program Compatibility Assistant User Interface	

• Conserver et refuser :

Cette liste contient un certain nombre d'éléments qui n'ont a priori aucune raison de se connecter à Internet.

Microsoft Windows Search Filter Host	

• N'autoriser que ponctuellement :

Tout programme d'installation (sauf programme louche)	
Traitement de texte et logiciels de bureautique	
Adobe Reader	
Lecteur Windows Media (ce logiciel a la fâcheuse tendance à vouloir accéder sur Internet même	

quand on lui demande pas, n'autoriser que quand c'est nécessaire)	

XIII.2) Abréviations et définitions

• FAI :

Fournisseur d'accès à Internet. Terme désignant l'entreprise vous fournissant l'accès à Internet. Certaines personnes appellent ça un provider.

• IE :

Cette abréviation signifie en Informatique « Internet Explorer ». Internet Explorer est un navigateur Internet conçu par Microsoft pour Windows.

• extension :

D'un fichier :

Un fichier a toujours un nom. Ce nom est composé de deux parties. Le nom et l'extension. Ces deux parties sont séparées par un point.

Un fichier « toto.bmp » a donc pour extension « bmp » (parfois, pour désigner l'extension, on donne aussi le point, donc on dit parfois « .bmp » pour cet exemple)

D'un programme :

Un programme peut avoir une extension. L'extension d'un programme est un petit programme permettant d'améliorer le programme de base. On appelle ça aussi plugin, addon, ...

Sommaire