

Informatique

DU DYSFONCTIONNEMENT DE L'ORDINATEUR ET DE SES PROGRAMMES

MUKUBI BUKONGO DAVID*

Résumé

La sécurisation de l'outil informatique qui est l'ordinateur ainsi que ses différents programmes et logiciels s'avère indispensable pour un bon fonctionnement de ce dernier. Ainsi, les résultats de cette étude relèvent que les précautions suivantes sont à prendre pour prévenir les pannes sont les suivantes : entretien de son matériel, prévention des pannes du système, suppression des fichiers inutile, contrôle des disques, protections contre les virus, protection contre les messages piégés, sauvegarde de sa configuration, mise à jour de son système automatiquement, activation du pare-feu de Windows vista, configuration du pare-feu de Windows vista, configuration des alertes de sécurité, ne pas installer l'antivirus non compatible.

Mots clés : ordinateur, pannes, sécurité d'ordinateur, dysfonctionnement du programme

Abstract

The security system of the data-processing tool that is the computer as well as its various application programs and software proves to be indispensable essential for any computer system to perform successfully. Thus, the results of this study reveal that the following precautions are to be taken into account to prevent eventual breakdowns : maintenance of its material, prevention of the breakdowns of the system, removal of unnecessary files, to discs control , protection against viruses, protection against trapped messages, safeguard of its configuration, updating of its system automatically, activation of the fire wall of windows vista, configuration of the fire wall of windows vista, configuration of safety alarms, avoid installing incompatible antivirus applications.

Key words: computer, security of computer, data-processing tool, application

1. INTRODUCTION

Semblablement dans bien d'autres domaines, en informatique, il vaut mieux prévenir que guérir. Il existe plusieurs technologies à mettre en place pour borner les risques d'erreurs du système, soit pour détecter un dysfonctionnement qui peut avoir des conséquences catastrophiques si l'utilisateur de l'outil informatique ne le traite pas immédiatement (Mohellebi, D. 2002).

Dans ces dix dernières années nous constatons l'utilisation accrue de l'outil informatique qui est l'ordinateur dans notre pays. Cet outil à ses préalables et ses

* Assistant à l'Université du Moyen Lualaba de Kalima « UML/Kalima », davidmukubi90@gmail.com

exigences avant son utilisation notamment le programme de base et les programmes d'application qui doivent être installés et bien équilibrés dans l'ordinateur. Cependant, la sécurisation de l'outil informatique ainsi que ses différents programmes et logiciels s'avère indispensable pour un bon fonctionnement de celui-ci. (Nkoko, F. 2008). Ainsi, les différents problèmes de l'ordinateur ainsi que ses différents programmes nous ont fait que nous puissions soulever ces deux préoccupations :

- Dans quelles circonstances les programmes installés dans un ordinateur peuvent provoquer des dysfonctionnements ?
- Quelles sont les précautions à prendre pour éviter ces pannes ?

L'hypothèse d'un travail étant la proposition des réponses aux questions que l'on se pose de l'objectif de recherche. Elle est formulée en termes des connaissances, telles que l'observation et l'analyse puissent fournir une réponse (Ronger P. 1971)

Compte tenu de ce qui est dit ci-haut nous avons formulé les hypothèses pour tenter de vérifier la véracité dans la présente étude.

Eu égard à ce qui précède, nous avons émis les hypothèses selon lesquels :

- la mauvaise installation des programmes liés à l'incompatibilité entre le système d'exploitation et les différents logiciels (programmes d'applications) ainsi que les programmes destructeurs appelés virus seraient à la base de dysfonctionnement de l'ordinateur.
- Les précautions à prendre pour prévenir ces pannes seraient multiples, l'on peut proposer quelques-unes tel que :- la Prévention des pannes du système ; l'entretien de ses matériels ; la Suppression des fichiers inutiles ; le Contrôle des disques ; Se protéger des virus ; Se protéger des messages piégés ; Sauvegarder sa configuration ; Mettre à jour son système automatiquement ; Activer le pare-feu de windows vista ; Configurer le pare-feu windows vista ; Configurer les alertes de sécurité ; Evitez d'installer l'antivirus non compatible ; tout ceux-ci contribueraient à prévenir les pannes de l'ordinateur.

Montrer les utilisateurs de l'outil informatique(ordinateur) :l'importance d'une bonne installation des programme compatible entre le système d'exploitation et les différents logiciels(programme d'application)en opérant des bons choix des programmes destructeurs (virus) et informer les utilisateurs de c'est outil sur les différentes précautions à prendre pour palier au dysfonctionnements de l'ordinateur reste l'objectif principal poursuivie dans cette étude.

Tout œuvre scientifique exige une méthodologie appropriée ; c'est ainsi que pour la réalisation de ce travail, nous nous sommes servis de la méthode analytique (Grawitz, M. 1974). Celle-ci a été appuyée par la technique documentaire.

Ce travail comprend la présente introduction, le développement et la conclusion. Le développement est structuré en deux sections l'une explique les dysfonctionnements provoqués par la mauvaise installation des programmes, l'incompatibilité entre le système d'exploitation et les différents logiciels (programmes d'application) et les programmes destructeurs ou virus de différentes pannes de l'ordinateur et l'autre présente les différentes précautions à prendre pour éviter les dysfonctionnements dans l'ordinateur.

2. REVUE DE LA LITTÉRATURE

Sur ce point, il sera question de présenter les différentes pistes des solutions au problème constaté.

2.1. Précautions à prendre pour lutter contre ces dysfonctionnements (Balemo, G 2007)

2.1.1. Sécuriser son installation et limiter les risques d'accident

Sécuriser son installation revient dans un premier temps, à pallier à tout risque électrique ; une précaution qui permet de prolonger la durée de vie de votre matériel et d'éviter également certains accidents domestique, surtout si votre foyer comprend de jeunes enfants. (Muchielli, R. 1971),

Voici alors quelques précautions à prendre pour limiter les risques d'accident :

- Lorsque vous installer la tour de votre ordinateur laissez suffisamment d'espace à l'arrière pour l'aération. Ne la posez trop près d'un mur et évitez de l'enfermer dans un meuble sans aération ;
- Ne superposez pas vos appareils les uns sur les autres ;
- Dépoussiérez régulièrement votre matériel. La poussière s'entasse vite et diminue rapidement l'efficacité de la ventilation en bouchant les aérations ;
- Pensez toujours à ventiler correctement votre unité centrale en faisant installer par un professionnel un ventilateur conséquent sur le processeur et un ventilateur de boîtier, raison pour laquelle tous ordinateurs actuels en sont équipés dès l'origine ;
- Si vous utilisez des multiprises, branchez-les toujours sur des prises murales intégrant une prise de terre et veillez à ce qu'elles comportent elles-mêmes un tel dispositif de protection ;
- Ne branchez jamais une multiprise sur une autre multiprise ;
- Essayez toujours d'installer votre ordinateur près d'une prise de courant ;
- N'hésitez pas à prendre une alimentation puissante (450w et plus) et bien ventilée. Sachez qu'il existe également des systèmes de protection électrique efficace. Ainsi, certaines prises intègrent un dispositif de protection contre la foudre ou les surtensions ;

- Une installation constitue une source de chaleur et génère une tension électrique importante. C'est pourquoi, il convient de ne jamais laisser de tissus ou de matière inflammables à proximité de vos appareils ;
- Ne laissez pas trainer vos câbles sur le sol ;
- Si vous avez de jeunes enfants, n'hésitez pas à utiliser des caches prises et à rendre difficile l'accès au câblage de votre installation ;
- Prenez également garde à tout liquide, ne posez jamais un verre d'eau, jus, bière sur votre unité centrale ;
- Adopter des meubles adaptés au matériel informatique (Nkoko, F. 2008).

2.1.2. *Entretien son matériel*

Si l'emplacement de vos appareils et les précautions d'utilisation élémentaires sont respectés, le matériel informatique ne nécessite pas un entretien permanent. Cela dit, il existe tout de même quelques points à surveiller en particulier pour éviter toute surprise désagréable :

- Evitez d'emmêler vos câbles. C'est ainsi que pour remédier, les deux solutions les plus efficaces sont les passe-câbles et les serre-câbles. Ces solutions permettent d'éviter les nœuds et de tirer dessous plus les déconnecter, ce qui diminue leur durée de vie. Notez également que les faux contacts génèrent des pannes qui ne sont parfois pas évidentes à comprendre (redémarrage du système sans aucune explication)
- Disposez correctement vos câbles, ne les pliez pas et trie-les soigneusement pour mieux vous y retrouver lorsque cela s'avère nécessaire. (Lamoureux, A. 2000)

Notice : Les pannes fréquentes, plusieurs dysfonctionnements peuvent s'expliquer lorsque des câbles sont écrasés sous un meuble ou lorsqu'ils subissent des déformations trop importantes.

Il vous est recommandé :

- De nettoyer vos lecteurs ou matériel avec des produits adaptés ;
- Pour dépoussiérer extérieurement, des coups de chiffons suffisent ;
- De ne jamais oublier de passer régulièrement l'aspirateur pour avaler toute la poussière autour de votre ordinateur ;
- De penser à protéger vos DVD et CD de la poussière ;
- De nettoyer des écrans LCD avec des produits spéciaux que vous trouvez dans des magasins spécialisés en matériel vidéo ou informatique. Le deuxième chiffon est évidemment de mise. Mais la meilleure façon de ne pas saturer son écran reste encore de ne pas mettre vos doigts dessus ;
- Lorsque vous changez les piles, de les remplacer toutes. N'utilisez pas une pile neuve et une autre usagée dans le même clavier ou la souris sans fil ;

- De ne laissez pas vos appareils allumés si vous ne les utilisez pas ;
- De brancher votre matériel de toutes sources électriques, au cas d'une inactivité prolongée de votre installation ;
- D'éviter d'expulser votre ordinateur ou votre écran à des sources de chaleur (radiateur ou fenêtre en élément) ;
- D'éviter les changements de température trop brusques. Le fonctionnement de certains appareils peut être perturbé par l'apparition de condensateur, notamment les lecteurs équipés de lentilles optiques ;
- Sur votre écran, de ne pas laisser une image fixe affichée pendant des heures, utilisez un économiseur d'écran ;
- Si vous déplacez un écran, de ne pas le faire en le tenant par les enceintes qui y sont fixés. (Michel, p. 1986)

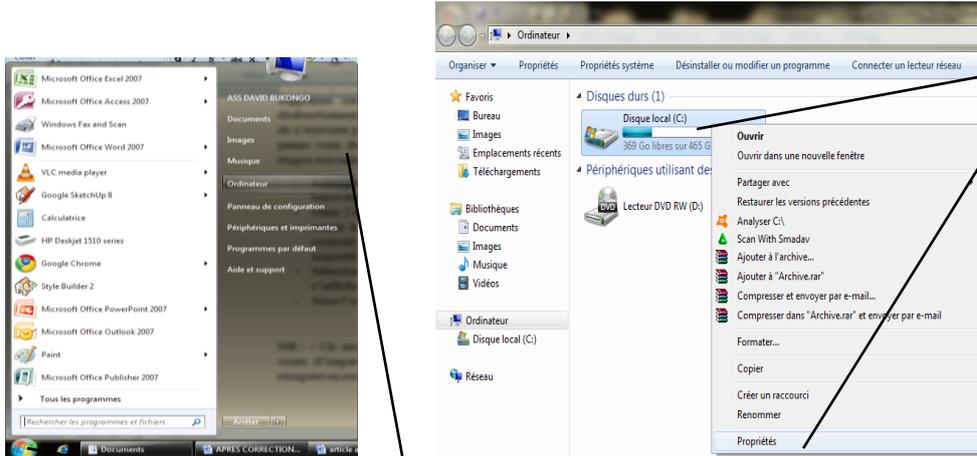
2.1.3. Prévenir les pannes du système

Après le matériel, il convient de sécuriser également son système pour prévenir les pannes les plus fréquentes.

a. Supprimer les fichiers inutiles

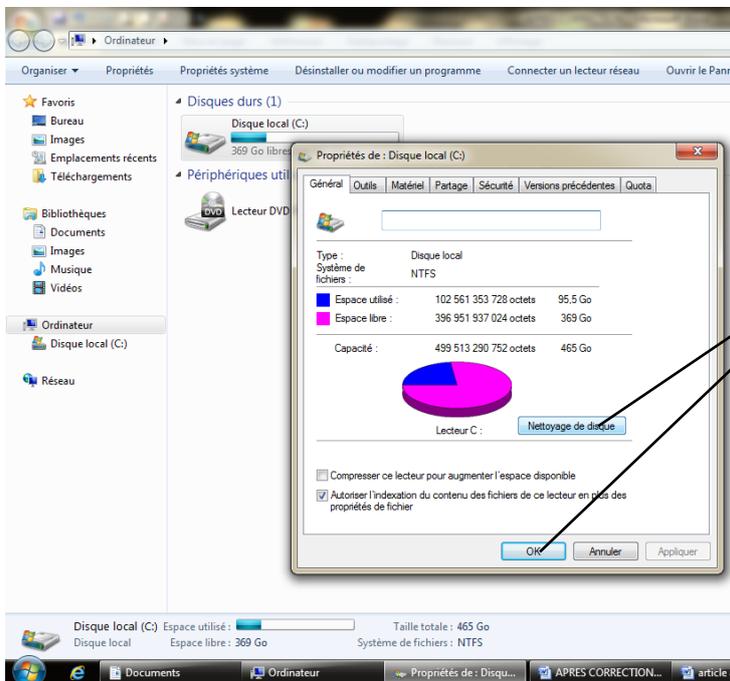
Windows vista, et certains programmes génèrent plusieurs fichiers temporaires pendant son fonctionnement. Parfois, ces fichiers ne sont pas supprimés correctement et s'ils s'entassent, cela peut provoquer toute de dysfonctionnement (erreurs disques) ou empêcher certaines de vos applications de s'exécuter par manque de place (Auchatraire, P. 1987). Pour éviter ce type de panne vous devez alors supprimer vous-même de tels fichiers en suivant les étapes suivantes :

- Sélectionner la commande ordinateur à partir du menu démarrer de la barre des tâches de Windows ;
- Dans l'arborescence de gauche, sélectionnez avec le bouton droit de la souris le lecteur à nettoyer (en général, celui qui porte la lettre d'unité centrale) pour effacer les fichiers temporaires générés par le système et majorité de vos programmes ;
- Sélectionnez la commande propriété à partir du menu contextuel qui s'affiche même nom ;
- Sous l'onglet général, cliquez sur le bouton « nettoyer le disque ».



Ici vous appelez le menu contextuel sur le disque a nettoyé puis vous allez passer à l'étape suivante après avoir cliqué sur la commande Propriété.

Menu démarrer puis commande



A cet étape vous cliquez sur la commande Nettoyage du disque et enfin sur Ok

NB : - Un message apparaît vous indiquant que le disque sélectionné est en cours d'inspection. Le système calcule effectivement l'espace pouvant être récupéré en exécutant l'assistant de nettoyage de disque.

- Une nouvelle boîte de dialogue s'affiche ensuite, et vous spécifie, pour chaque emplacement le volume des fichiers temporaires que vous pouvez supprimer.
- Cochez les éléments à supprimer sur la liste des fichiers à supprimer et valider par Ok pour nettoyer votre disque.

b. Contrôler les disques

Windows vista propose une commande spécifique pour vérifier l'intégrité de vos données. Cela permet de détecter des erreurs d'accès aux fichiers et aux dossiers. Vous pouvez également les réparer en toute simplicité en appliquant ce qui suit :

- Sélectionnez le menu démarrer/Tous les programmes/Accessoires/Invite de commandes de la barre des tâches de windows ouvrir la console de windows ;
- Tapez la commande chkdsk et validez par la touche entrée pour démarrer le processus de vérification de la partition ;
- Windows vérifie l'intégralité des données de la partition et si aucun problème n'est détecté, il affichera le message "windows" vérifie le système de fichier sans trouver de problème ;
- Vous pouvez alors renfermer la console en cliquant sur la croix qui se trouve à droite dans la barre des titres de la fenêtre.

Il sied de noter que si windows trouve des problèmes, vous devez alors relancer ceux commandes en ajoutant l'option/F pour que le système puisse réparer automatiquement les erreurs (chrdsk/F). Enfin, pour vérifier une partition différente de cette du disque principal C, il suffit d'indiquer l'unité du lecteur en la faisant suivre d'un deux-points, sous cette forme par exemple pour le contrôle de lecteur D : chkdskd : (Ginguay, M. 1987)

c. Se protéger des virus

Par internet, et plus particulièrement par e-mail les virus sont légion. Dès lors, l'installation d'un antivirus ne suffit pas toujours. Il faut également savoir reconnaître les messages suspects et identifier les extensions de fichiers à risque. Bien entendu, l'antivirus reste toujours indispensable (Mbula, B. 1991). Généralement, vous en êtes déjà équipé car la majorité des configurations modernes vendues sur le marché dispose, par défaut, d'un tel outil de protection, cela dit, si ce n'est pas le cas, voici un peu tableau qui vous sera utile pour télécharger et installer, sans plus attendre, votre antivirus.

Les principaux antivirus

Noms	Adresses	Commentaires
Kaspersky	www.kaspersky.com/fr	Léger d'une efficacité redoutable
NAV	www.symantec.fr	Simple à prendre en main
McAfee	www.mcafee.com/fr	La dernière version de virus scan mérite le détour

- Pour éviter d'exécuter un virus, vous devez connaître les fichiers et savoir les connaître par leur extension. Ainsi, l'extension des fichiers exécutables,

exemple : Com ou bat, constitue un véritable risque puisque ces fichiers peuvent exécuter n'importe quelle commande sur votre machine ;

- L'extension vbs, quant à elle, est également capable du pire et du meilleur. Elle correspond à une macro, c'est-à-dire à une série d'instruction collée dans un langage informatique spécifique le visual basic en l'occurrence. Selon son origine exécution peut entraîner des effets dévastateurs sur le système Windows ;
- Méfiez-vous également de certains documents a priori anodins, issu d'une application bureautique (word, excel,..) de fait, les extensions en doc ou docx et xls ou xlsx des commandes hostiles (une suite de commande) qui infecteront tous les autres fichiers issus de la même application concrètement, un document Word vérolé contaminera tous les autres documents Word qu'il trouvera. (Michel, P. 1986)

Par défaut, les systèmes Windows n'affichent pas les extensions de fichiers. Voici alors la marche à suivre pour le rendre visibles :

- Démarrer l'explorateur Windows et sélectionnez la commande option des dossiers et recherche du menu organiser ;
- Cliquer sur l'onglet affichage et, sur la liste paramètres avancés, désactivez l'option masquer les extensions des fichiers dont le type est connu.

d. Se protéger des messages piégés

Outlook express et windows mail représentent les logiciels de messagerie les plus utilisés actuellement, mais ils ne sont pas les plus performants. En fait, ils ont même des défauts comme celui d'être beaucoup trop compatible avec le format HTML des pages Web. Certes cela permet de composer des messages très réduisant et beaucoup d'utilisateur auraient du mal à se passer de telles fonctionnalités. Pourtant, cela représente également un risque important pour le bon fonctionnement de votre système. (Selemete, I. 2007), Dès lors, pour vous protéger de certains messages capables d'exécuter automatiquement des commandes pour votre système dès que vous les ouvrez, voici un petit réglage à effectuer sans plus attendre :

- Démarrer le programme outlook express ou windows mail ;
- Sélectionnez la commande option du menu outils ;
- Cliquer à présent sur l'onglet sécurité et, dans la section protection antivirus, sélectionnez les options zone de sites sensibles et ne pas autoriser l'ouverture ou l'enregistrement des pièces jointes susceptibles de contenir un virus. Validez ensuite vos choix en cliquant sur le bouton ok.

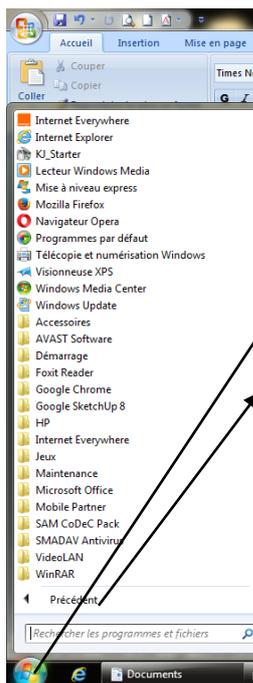
2.1.4. Sauvegarder sa configuration

Si vous avez créé plusieurs comptes d'utilisateurs, pour accéder à votre ordinateur, alors chacun d'entre eux dispose d'un dossier spécifique qui porte son nom dans le répertoire

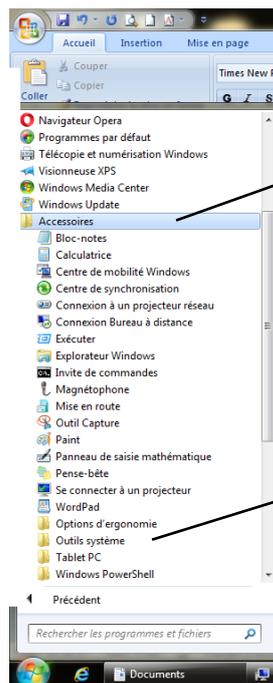
C:/utilisateur. Ce dossier contient des fichiers personnels indispensables à propos de son environnement de travail et de son navigateur sur internet. On y trouve, entre autres le contenu de son bureau, ses favoris, ses paramètres personnalisés pour chacune des applications qu'il utilise, etc. (Balemo, G. 2007)

Bref, toutes ces informations relatives à tous les utilisateurs de votre ordinateur sont essentiels pour ne pas devoir reconfigurer, pour chacun d'eux, leur environnement de travail après la réinstallation de Windows Vista ou lorsque vous effacez par mégarde leur dossier. (Rufino Filipe A. 2012) C'est pourquoi, même si vous perdez toutes les données de votre disque dur, il existe un moyen simple de récupérer tous vos paramètres de configuration, à condition toutefois d'avoir pensé auparavant à effectuer une copie de sauvegarde du fichier utilisateur. Dat, et plus généralement de tout le contenu des dossiers utilisateurs contenu dans le répertoire C:/utilisateur. Voici la méthode pour le faire dans les règles de l'art :

- Cliquez sur le bouton démarrer de la barre des tâches de Windows et sélectionnez la commande tous les Programmes/Accessoires/Outils système/Transfert de fichier et de paramètres Windows ;
- L'assistant de transfert de fichier et de paramètres s'affichent. Passez la première étape en cliquant sur le bouton suivant et sélectionnez l'option ancien ordinateur pour sauvegarder les données du système ;
- Sélectionnez votre support d'enregistrement, puis lancez la sauvegarde en cliquant sur le bouton suivant ;
- Pour restaurer les fichiers systèmes de vos utilisateurs, il suffit de relancer l'assistant de transfert de fichier et de paramètres et de sélectionner l'option nouvel ordinateur de l'étape 2.

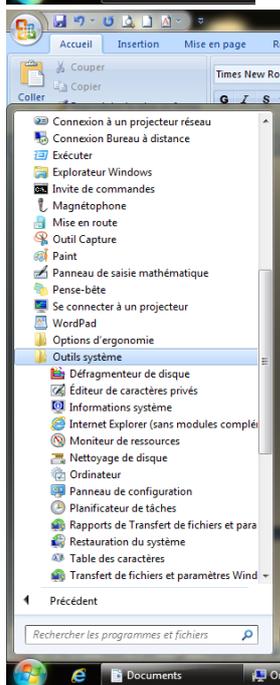


Comme vous constatez dans ce premier interface nous avons cliqué le bouton **démarrer** et puis sur **tous programme**. Pour passer à l'étape suivant on clique sur la commande **Accessoires**

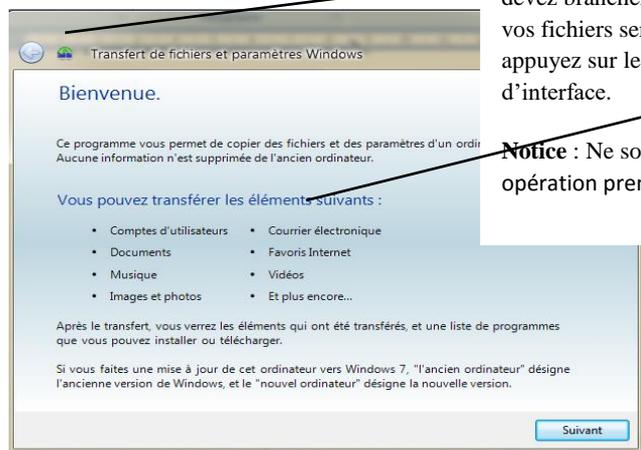


En cliquant sur la commande **Accessoires** voilà l'interface qui se présente. Pour passer à l'étape suivant il faut cliquer sur la commande **outils systèmes**

Et quand on clique sur la commande **outils systèmes** vous trouvez cette interface. Pour aller à l'étape suivant on clique sur la commande **Transfert des fichiers et paramétrage Windows**



Après avoir cliqué sur la commande **Transfert des fichiers et paramétrage Windows** l'interface suivante s'affiche où on vous présente tous les éléments que vous pouvez transférer. Avant de continuer ici vous devez brancher un autre ordinateur sur lequel vos fichiers seront transférés, si cela est fait appuyez sur le bouton suivant en bas d'interface.



Notice : Ne soyez pas presser car cette opération prend du temps

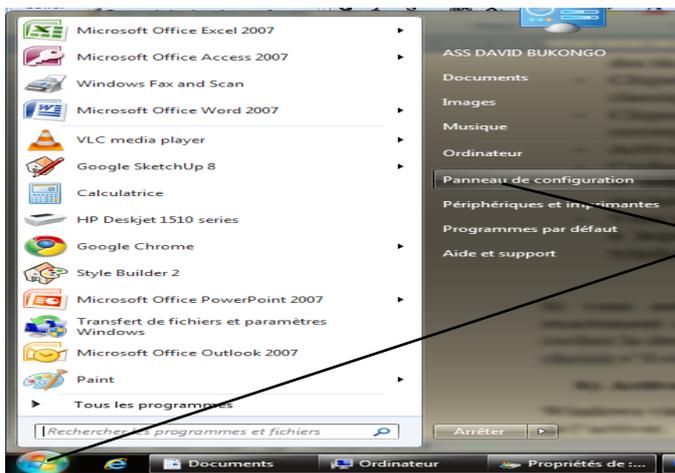
a) Mettre à jour son système automatiquement

Si vous n'activez pas les mises à jour automatiques de windows vista, vous risquez de les oublier et de ne pas pouvoir prévenir les pannes les plus fréquents de votre système. Dès lors, pourquoi ne pas le faire ?

Si vous n'avez pas activé des mises à jour automatiques du système immédiatement après l'installation de windows vista, il n'est pas trop tard pour bien faire. Deux

méthodes sont possibles : vous pouvez passer par le panneau de configuration ou par le centre de sécurité. (Mohellebi, D. 2002)

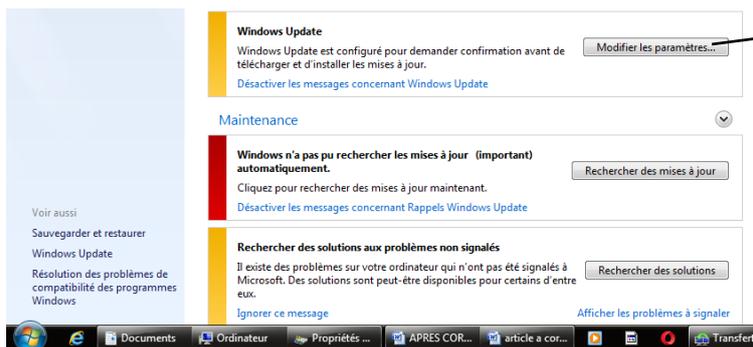
- Ouvrez le panneau de configuration à partir du menu démarrer de la barre des tâches de Windows ;
- Cliquez dans la fenêtre qui va s'afficher sur le lien intitulé affichage classique qui se trouve à gauche de fenêtre ;
- Cliquez sur l'icône Windows Update pour ouvrir la fenêtre correspondante ;
- Activez le lien modifier les paramètres ;
- Cochez l'option installer les mises à jour automatiquement (recommandé) et définissez la fréquence des mises à jour à effectuer automatiquement sur internet : tous les jours ou une fois par semaine à un jour précis ;
- Vous pouvez également indiquer, sur la liste déroutante suivante, l'heure à laquelle votre ordinateur se connectera automatiquement sur le site windows update.



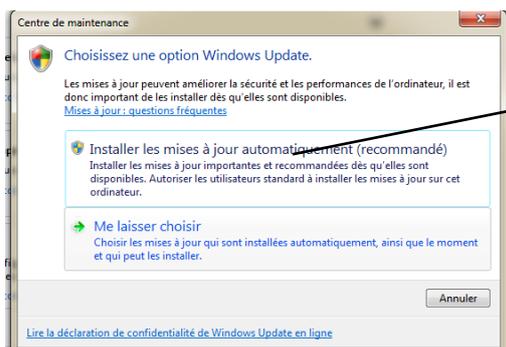
Comme la procédure nous indique d'abord on clique sur le bouton du **menu démarrer** de la barre de tâche puis sur la commande **Panneau de configuration**. Puis on passe à l'étape suivant.



Ici on clique sur la commande système et sécurité puis sur sauvegarde votre ordinateur



Ici vous cliquez sur le bouton Modifier les paramètres de la commande Windows Update pour passer à l'étape suivant



A partir d'ici vous pouvez mettre à jour automatiquement tout en étant connecté à l'internet sur le site Windows update

Si vous souhaitez installer vous-même vos mises à jours pour vérifier exactement ce que vous récupérer sur le site de Microsoft, il vous suffit de cochez la deuxième option intitulée télécharger des mises à jours, mais ne laisser choisir s'il convient de les installer.

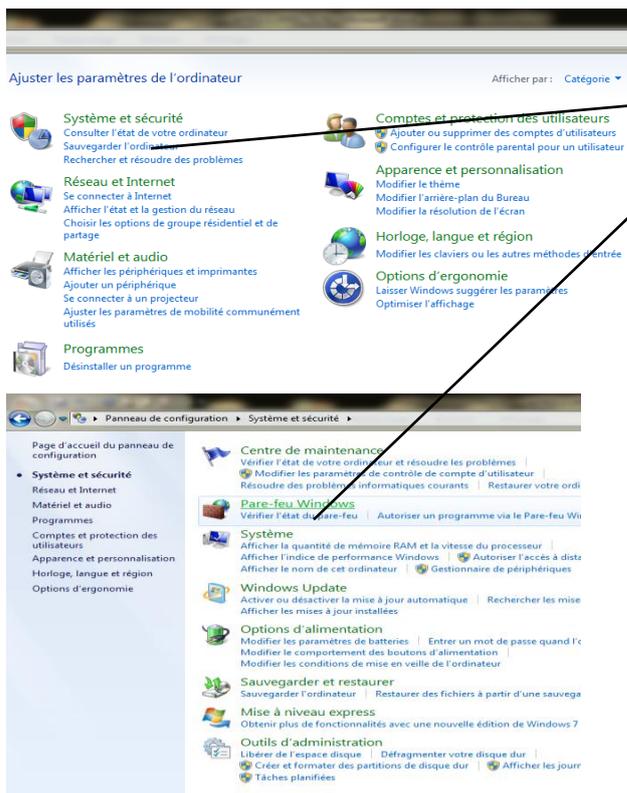
b) Activer le pare-feu windows vista

Windows vista intègre un pare-feu qui s'avère fort efficace, à condition toutefois de l'activer.

Un pare-feu, ou firewall en Anglais, permet de fermer tous les ports d'entrées de votre ordinateur lorsque vous vous connectez à l'internet. De cette façon, aucun utilisateur mal intentionné ne peut pénétrer sur votre système pour en prendre le contrôle les communications sortantes ressources à votre insu. De plus, le pare-feu bloque les communications sortantes, ce qui signifie qu'aucun programme n'a l'autorisation, par défaut, d'envoyer des données sur internet sans votre permission. Quoi qu'il en soit, cela ne ralentit en aucun cas votre liaison à internet et il serait alors dommage de vous en priver. Dès lors pour gérer la surveillance de votre pare-feu, vous devez utiliser les fonctionnalités du centre de sécurité de Windows vista :

- Ouvrez le panneau de configuration à partir du menu démarrer de la barre de tâches de Windows ;
- Dans la fenêtre qui s'affiche, cliquez sur l'icône du centre de sécurité qui s'affiche immédiatement ;
- Cliquez sur la flèche à droite de la mention inactive ou activée de la section dédiée au pare-feu automatique ;

- Si le pare-feu n'est pas activé, cliquez sur le bouton activer maintenant pour protéger immédiatement votre ordinateur ;
- Vous pouvez accéder à toutes les options de votre pare-feu en indiquant sur le lien pare-feu Windows disponible dans le menu de gauche de la fenêtre du centre de sécurité ;
- Dans la nouvelle fenêtre qui s'affiche, cliquez sur le lien « modifier les paramètres ».



Ces interfaces nous montrent comment faut-il procéder pour activer le Windows vista

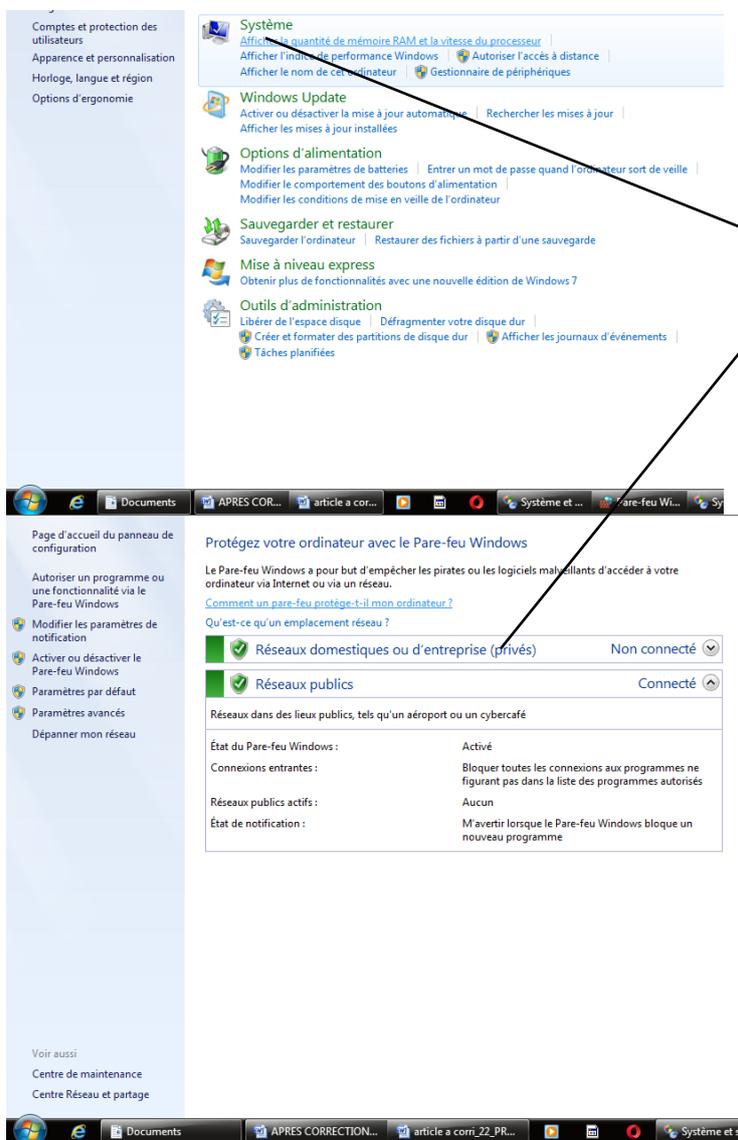
c) Configurer le pare-feu de windows vista

Après avoir activé le pare-feu de windows vista, il convient de le configurer correctement.

Si cette procédure peut s'avère assez compliquée lorsque vous utilisez des services particuliers (un serveur web installé sur votre ordinateur, par exemple, pour permettre aux inter routes de se connecter chez vous et de consulter les pages web de votre choix) il n'empêche qu'il existe des réglages basiques qui ne poseront aucune difficulté. (Mbula, B. 1991)

- Ouvrez le panneau de configuration à partir du menu démarrer de la barre des tâches de windows ;
- Cliquez dans la fenêtre qui s'affiche, sur l'intitulé de section sécurité ;
- Cliquez sur l'icône du pare-feu, puis, dans la fenêtre qui apparaît, sur le lien modifier les paramètres ;

- Dans la boîte de dialogue qui s'affiche, sous l'onglet général, vous avez la possibilité de permettre à votre ordinateur en cochant ou en décochant l'option bloquer toutes les connexions entrantes.

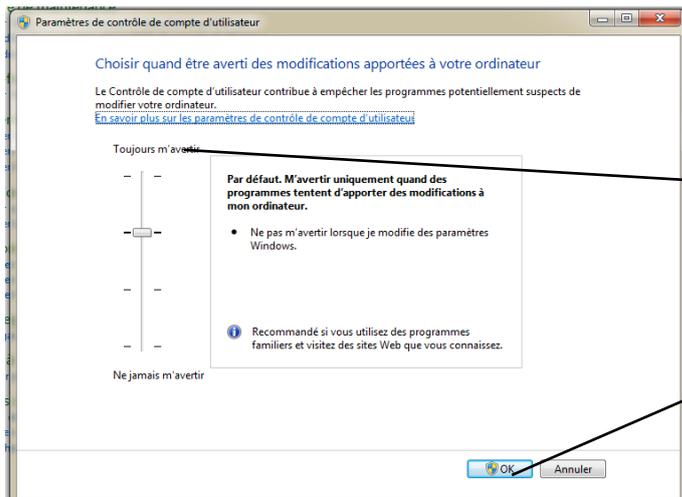


A partir d'ici vous avez la possibilité de configurer votre Windows comme l'indique les littératures mentionnées ci-haut

d) Configurer les alertes de sécurité

Les étapes à suivre sont les suivantes :

- Démarrer le centre de sécurité ;
- Cliquez sur le lien modifier la manière dont le centre de sécurité m'avertir pour afficher les paramètres des configurations du centre de sécurité ;
- Dans la boîte de dialogue qui s'affiche sur une des trois options disponibles



Ceci nous permet d'être au courant de tous ceux qui peuvent arriver dans nos machines en cliquant sur m'avertir toujours, enfin sur ok

1. Oui, m'avertir et afficher l'icône : le dispositif d'alerte est opérationnel ;
2. Ne pas m'avertir, mais conserve l'icône du centre de sécurité dans la barre des tâches de Windows vista ;
3. Ne pas m'avertir et ne pas afficher l'icône : désactiver les alertes et masquer l'icône du centre de sécurité dans la barre des tâches de Windows. (Michael K. 2009),

Et si vous utilisez Windows 7 par exemple vous devez installer l'antivirus **Kaspersky** qui est compatible à ce système d'exploitation. D'où son adresse est bien figurer à la page huit de ce projet.

e) L'antivirus non compatible

La plupart d'antivirus sont pris en charge par le centre de sécurité de Windows vista. Toutefois, si ce n'est pas le cas, vous pouvez le signaler dans les paramètres de configuration. (Ginguy, M. 1987)

3. CONCLUSION

A la limite de notre travail qu'a porté sur « Du dysfonctionnement de l'ordinateur et de ses programmes ».

Subséquemment, pour évoquer les différents problèmes de l'ordinateur ainsi que ses différents programmes, une question à deux volets a constituées notre problématique à savoir : qu'est ce qui provoque le dysfonctionnement entre l'ordinateur et les différents programmes qui y sont installés ? Quelles sont les différentes précautions que les utilisateurs peuvent suivre pour éviter cela ?

Eu égard à ce qui précède, nous avons émis les hypothèses de la manière suivantes : La mauvaise installation des programmes, l'incompatibilité entre le système d'exploitation et les différents logiciel (programme d'application) ainsi que les programmes

destructeurs appelés virus sont à la bases d'un mauvais fonctionnement de l'ordinateur et les utilisateurs doivent prévenir cela pour bien bénéficier des atouts qu'offre l'outils informatique.

L'objectif de notre étude était de montrer aux utilisateurs de l'outil informatique (ordinateur) les différents problèmes qui causent le dysfonctionnement entre l'ordinateur, le système d'exploitation ainsi que les différents programmes qui y sont installés et quelles sont les différentes précautions qu'il faut mettre en place pour éviter cela.

Par ailleurs, toute œuvre scientifique exige une méthodologie appropriée, pour la réalisation de ce travail nous nous sommes servis d'un certains méthodes et techniques. A ce propos seule la méthode analytique et la technique documentaire nous a été utile.

Les résultats de cette étude révèlent que les précautions suivantes sont à prendre pour prévenir les pannes :

- Prévenir les pannes du système ;
- Entretien son matériel ;
- Supprimer les fichiers inutiles ;
- Contrôler les disques ;
- Se protéger des virus ;
- Se protéger des messages piégés ;
- Sauvegarder sa configuration ;
- Mettre à jour son système automatiquement ;
- Activer le pare-feu de windows vista ;
- Configurer le pare-feu windows vista ;
- Configurer les alertes de sécurité ;
- Evitez d'installer l'antivirus non compatible.

4. BIBLIOGRAPHIE

- AUCHATRAIRE, P. (1987), *Chefs pour excel sur macintosh*. Paris : éd PSI
- BALEMO, G (2007), *L'utilisation de l'informatique dans les entreprises de Kinshasa*. Mémoire inédit Kinshasa : UNIKIN/FSEG
- DE LANDSHEERE, G. (1979), *Dictionnaire de l'évolution de la recherche en éducation*. Paris : PUF.
- GINGUAY, M. (1987), *Dictionnaire d'informatique*. Paris, New York, Barcelone, Milan : 3^e ed Masson
- GRAWITZ, M. (1974), *Méthodes des sciences sociales*. Paris : Dalloz
- LAMOUREUX, A. (2000), *Livre de recherche et de méthodologie en science humaines*. Paris : ESF

- MBULA, B. (1991), *Impact de l'ordinateur sur l'organisation du travail et la conception de cet indice par le personnel de l'UNIBRA Kisangani*. Mémoire inédit. Kisangani UNIKIS/FPSE
- MICHEL, P. (1986), *Comprendre l'informatique, s'initier pour maîtriser*. Paris : 4^e éd. INCEP, 7509
- MICHAEL K. (2009), *Linux, installation, configuration et administration des systèmes Linux*, Pearson éducation France 41 bis, rue des vinaigriers 8^e éd. 75010 paris
- MUCHIELLI, R. (1971), *Les questionnaires dans les enquêtes psychologiques*. Paris :ESF
- MOHELLEBI, D. (2002) ; *Les nouvelles technologies de l'information et de la communication et la capitalisation des compétences internes de l'entreprise*. Algérie : Université de Tizi Ouzou, Algérie. On line in <http://www.atelis.org> ;
- NKOKO, F. (2008). *L'informatique pour tous*. Kinshasa 10^e rue Limete n°18 se.
- Ronger, P. (1971). *Sciences sociales*, éd Dalloz, Paris
- RUFINO FILIPE A., (2012) ; *Culture et technologie de l'information et de la communication : Quelle approche du paradigme du développement ?* Presses Académique francophone
- SELEMETE, I. (2007), *Opinion des élèves finalistes de la ville de Kisangani sur la correction informatisée des examens d'Etat*. TFC inédit. Kisangani : UNIKIS/FPSE

