FAQ AXE ONE

1 quai Joseph GILLET - 69004 LYON – www.fidit.com – contact@fidit.com

Q : Comment sauvegarder les données stockées sur mon serveur AXE one® ?

R : Votre serveur AXE one® intègre un graveur de DVD d'une capacité maximum de 4.5Go, ainsi qu'un script de sauvegarde paramétrable, dont vous pouvez programmer l'exécution à intervalle régulier.

Vous disposez d'un système de sauvegarde de masse qui écrase la dernière sauvegarde avec les nouvelles données SANS conservation de l'historique.

Nous vous conseillons de mettre en place une procédure d'échange de DVD basé sur le principe d'un DVD par jour et par semaine paire et impaire : marquage d'un DVD lundi semaine paire, un lundi semaine impaire, un mardi semaine paire, etc...

Chaque jour vous procédez à l'échange du DVD gravé la veille par le DVD du jour.

Vous bénéficiez dès lors de 2 semaines de sauvegardes différentes, avec la possibilité de conserver la semaine non active à l'extérieur de la société.

Sauvegarder ses données c'est bien, mais en vérifier la qualité, sur un poste Windows par exemple, c'est mieux !

Q : Je souhaite qu'une adresse soit marquée ****SPAM****

R : Demandez à l'administrateur de votre serveur AXE one® de saisir l'adresse concernée dans l'option « Filtre »« Filtre email » « liste noire » de son interface d'administration

Attention les indésirables utilisent rarement 2 fois la même adresse !

Par ailleurs avec la multiplication des usurpations d'adresse, vous risquez de vous priver de courriers de correspondant intéressant.

Q : je reçoit des emails de mes clients, de ma femme, … que mon AXE one® marque ****SPAM**** de temps à autre.

R : Certains opérateurs Internet sont régulièrement identifiés comme relais de spam.

Ex : laposte.net

Cela se traduit par un marquage ****SPAM**** certains jours !

Demandez à l'administrateur de votre serveur AXE one® de saisir les adresses concernées dans l’option « Filtre » « Filtre email » « liste blanche » de son interface d’administration

Si vous souhaitez vous assurer un "non marquage" ****SPAM**** sur les emails en provenance d’un nom de domaine bien précis, renseignez *@nomdedomaine dans cette même liste.

Le caractère * est un caractère joker.

Q : Comment installer le client HYLAFAX ?

R : En premier lieu, il faut installer le logiciel sur votre ordinateur :

1. Fermer toutes les applications actives.
2. Dans le dossier FIDIT de votre lecteur réseau P : (partage) Cliquez sur le fichier WHFC.
3. Cliquez sur Terminer puis Oui.
4. Suivre les choix proposés par défaut puis Finish.

Vous devez ensuite installer l'imprimante FAX :

1. Sous MS Xp, faire Démarrer, Paramètres, Imprimantes et Télécopieurs.
2. Cliquez sur Ajouter une imprimante.
3. Dans l'assistant ajout d'une imprimante : choisir Imprimante Locale, décocher « Détection et Installation automatique de l'imprimante Plug-and-Play », sélectionner port WHFCFAX.
4. Fenêtre ajout d'une imprimante : Fabricant Apple / Imprimante Apple LW12/640PS puis OK.
5. Nom de l'imprimante : Fax.
6. Cocher « Ne pas partager cette imprimante ». Répondre NON à « Imprimer une page de test ».
7. Terminer

Enfin personnalisez votre logiciel :

1. Copier le fichier « whfclang.fr » de partage\fidit dans C:\WINDOWS\SYSTEM32.
2. Faire Démarrer, Programme, WHFC.
3. Faire Fax, Prefs Utilisateur
4. Renseigner Nom, Login, E-mail avec vos paramètres personnels.
5. Cliquer sur Ok puis Oui.
6. Faire Fax, Prefs Système.
7. Renseigner Serveur avec « AXEONE ».
8. Dans Format, remplacer « %6.6 » par « %8.8 » et « %12.12 » par « %16.16 ».
9. Renseigner Dial Max. avec « 5 ».
10. Cocher « Barre de Tâches ».
11. Cliquer sur Ok.

Q : Comment intégrer **AXE** one® à un réseau de bureautique sous Windows ?

R : **AXE** one® intègre un serveur de fichier sous Samba. Il suffit donc dans votre bureau Windows de connecter un nouveau lecteur réseau. Vos documents sont alors stockées sur un poste unique.

Cette configuration est une base pour la centralisation des données. Cela permet à quiconque de travailler en toute indépendance sur l'ensemble des données sans avoir besoin d'allumer d'autre poste que le sien.

Par ailleurs pour vos postes nomades vous pouvez utiliser le logiciel WebDrive qui accélère notablement la navigation sur un poste distant via une connexion Internet.

Q : Avec **AXE** one®, est-il besoin d'opérations particulières pour se connecter à Internet ?

R : Absolument aucune ! la connexion à l'Internet est totalement transparente pour tous les postes du réseau quelque soit leur nature (PC, Mac, Unix). **AXE** one® gère la connexion Internet et permet à tout utilisateur de naviguer sans manipulation particulière inhérente aux connexions standard.

Attention : nous attirons toutefois votre attention sur la nécessité d'une gestion avancée et un contrôle rigoureux des trafics entrant et sortant sur Internet pour ce genre de connexion permanente.

C'est pourquoi **AXE** one® dispose de nombreux outils tels que le filtrage de mail, le filtrage d'URL, un anti-virus, etc…

Q : Avec **AXE** one®, peut-on se passer d'un anti-virus ?

R : **AXE** one® filtre tout le trafic Mail et élimine tous les virus connus avant que ceux-ci n'arrivent sur les postes clients grâce à l'intégration de l'anti-virus ClamAV.

Par ailleurs, avec **AXE** one®, votre anti-virus est toujours à jour, la base de données de signature étant automatiquement mise à jour par notre site central d'infogérance.

Toutefois il ne vous protège pas de l'introduction d'un virus dans votre réseau par le biais d'une disquette ou d'un CD-ROM. C'est pourquoi nous conseillons toujours d'équiper les postes clients d'un anti-virus complémentaire, de préférence d'une autre marque, Norton Anti-virus par exemple.

Q : Qui a inventé les virus informatiques ?

R : Bien difficile de vous apporter une réponse… un peu d'histoire peut-être :

Les virus ne font réellement parler d'eux que depuis le milieu des années 90. Pourtant, leur concept est apparu dans les premiers calculateurs électroniques, avec la mise en évidence, dès 1939, par John Von Neumann, de la théorie de l'autocopie de logiciels, concept utilisé par les virus.

L'analogie des codes malveillants avec les virus biologiques n'est pas anodine : leurs modes de contamination et de propagation sont quasiment identiques. Dans un premier temps, un virus informatique infecte un programme hôte dans lequel il va écrire ses propres lignes de code. Ensuite, tout comme un virus biologique utilise les ressources de l'organisme pour se reproduire, le virus informatique va s'exécuter à chaque fois que l'on active le programme qu'il a infecté. Ces nouvelles copies vont à leur tour infecter d'autres programmes et le cycle recommence ainsi, jusqu'à l'éradication.

Les premiers virus sont issus de recherches menées pour vérifier le bien-fondé de celles de von Neumann. Il en fut ainsi du jeu Core War, conçu dans les années 60 par les laboratoires Bell. Il opposait deux programmes chargés dans la mémoire vive d'un ordinateur. Le but du jeu était simple : chaque programme devait repérer l'autre et le détruire en s'autocopiant dans son code. Pour se défendre, chaque programme pouvait se dupliquer et s'auto réparer. Déplacement au sein de la mémoire, analyse de l'environnement et destruction d'un programme, Core War mettait en évidence toutes les principales fonctions des codes autoreproducteurs. Très vite, d'autres labos s'emparent de ce jeu pour analyser le comportement des programmes. Car, si au début les virus restent confinés dans la mémoire vive, leurs mutations les amènent vite à se reproduire sur le disque dur pour se propager ensuite d'une machine à l'autre. Le ver informatique est né.

Sans être impropre, le terme de virus englobe en fait trois familles de codes malveillants aux caractéristiques bien différentes. Il y a les virus proprement dits, qui, comme nous l'avons vu, ne sont pas autonomes et ont besoin d'une exécution du programme infecté pour devenir actifs. A l'inverse, les vers sont des programmes totalement autonomes. Il leur est ainsi possible de propager, via un réseau, une version fonctionnelle et complète d'eux-mêmes vers d'autres ordinateurs. Enfin, les chevaux de Troie et les bombes logiques ne se reproduisent pas. Ils contiennent des fonctions cachées pouvant s'exécuter en tâche de fond à l'insu de l'utilisateur.

Q : Mon Intranet « tournera » t'il sur **AXE** one®

R : **AXE** one® dispose d'un serveur de publication de pages Web Apache. Vous pourrez donc utiliser **AXE** one® comme support de votre Intranet, mais aussi de votre site Web public ou de votre Extranet.

Q : Mettre en place une connexion ADSL c'est ouvrir la porte aux pirates !

R : Bien entendu, il faut accompagner la mise en place d'une telle connexion des protections adéquates. Et il faut bien reconnaître que les dispositif physique (boîtier Firewall) ou les logiciels simples sous Windows offrent peu de garanties dans le domaine.

C'est pourquoi **AXE** one® intègre un pare feu IPCHAINS Firewall automatiquement mise à jour par notre site central d'infogérance qui vous protège des attaques connues.

Aucune des machines de votre réseau privé n'est visible de l'Internet sauf paramétrage spécifique sur votre demande.

Q : Comment sauvegarder mes données **AXE** one® ?

R : Concernant **AXE** one® toute la configuration et les paramètres du serveur sont automatiquement sauvegardés sur notre site central d'infogérance.

Concernant vos données personnelles, documents stockés sur Samba, il est possible de connecter une sauvegarde externe sur bande (DLT,DAT, ROBOT) et d'automatiser une sauvegarde périodique.

En option, nous avons la possibilité d'effectuer une sauvegarde externalisée sur un de nos serveurs.

Q : Mes clients n'arrivent pas toujours à lire mes propositions Word. Avez-vous une solution ?

R : Bien sur et très facilement ! Adressez à vos clients des documents au format pdf.

Le format .pdf est très utilisé pour la transmission d'informations sur Internet car il permet de transformer un document (photo, texte, tableau etc.) en un fichier qui ne peut être modifié. Cet outil est une sécurité pour les documents informatifs, contractuel ou les lettres importantes.

Avec **AXE** one®, le serveur de documents pdf se présente comme une imprimante disponible sur chaque poste client. Toute impression d'un document sur cette imprimante la transforme immédiatement en fichier pdf.

PS : PDF = Portable Document Format.

Q : Ma société possède plusieurs agences, que m'apporte **AXE** one® ?

R : Avec **AXE** one®, il est possible de construire un réseau privé virtuel (VPN) entre toutes vos agences et le siège.

Grâce à ce VPN, vos informations transiterons via le réseau Internet en toute sécurité. Elles seront cryptées et à l'intérieur de tunnels sécurisés.

Il est donc possible de relier des réseaux physiquement séparés par le biais de plusieurs serveurs **AXE** one®. Vos accéderont au réseau d'entreprise grâce a des connexions GPRS sécurisées.

Tous vos collaborateurs pourront alors partager les mêmes informations, utiliser un logiciel métier unique ou consulter un outil de suivi des clients comme notre produit GiBUS®.

Q : Comment **AXE** one®, gère les fax ?

R : Les fax entrant sont automatiquement convertis au format pdf et redirigés vers la ou les personnes de votre choix.

Vous pouvez aussi faire le choix de laisser tous les fax dans une boites aux lettres spécifique du serveur en libre service.

Pour les fax sortant, à l'image du serveur de documents pdf, le serveur de fax d' **AXE** one®, propose sur chaque poste client une imprimante fax.

Toute impression d'un document sur cette imprimante l'adresse automatiquement par fax au n° que précise l'utilisateur qui recevra un accusé de réception par mail.

Q : Comment créer un nouvel utilisateur sur **AXE** one® ?

R : Toute l'administration et la maintenance du serveur **AXE** one® s'effectuent par une interface Web, gestion des comptes d'utilisateur, des emails ou la surveillance du système.

De plus la gestion d'un site peut être déléguée à un utilisateur qui disposera d'une interface spécifique pour modifier les paramètres du site (dans les limites fixées par l'administrateur).

Cette interface Web permet également à chaque utilisateur de modifier les paramètres de son propre compte : alias de mails, répondeur, redirections automatiques de mail.

Nous vous invitons à consulter notre démonstration en ligne du site d'administration **AXE** one®.

Q : En matière de sécurité informatique quelle loi s'applique ?

R : De nombreux textes et Directives Européennes existent en la matière. Nous rappelons la principale en France dite Loi « Godfrain ».

Loi No 88-19 du 5 janvier 1988

Relative à la fraude informatique

Journal officiel du 6 janvier 1988

L'assemblée nationale et le Sénat ont adopté.
Le président de la République promulgue la loi dont la teneur suit :

Article unique

Dans le titre II du livre III du code pénal, il est inséré, après le chapitre II, un chapitre III ainsi rédigé:

Chapitre III

De certaines infractions en matière informatique

Article 462-2

Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois a un an et d'une amende de 2 000 F a 50 000 F ou de l'une de ces deux peines.
Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans les systèmes, soit une altération du fonctionnement de ce système, l'emprisonnement sera de 2 mois a 2 ans et l'amende de 10 000 F a 100 000 F.

Article 462-3

Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à 3 ans et d'une amende de 10 000 F a 100 000 F ou de l'un de ces deux peines.

Article 462-4

Article 462-4 : Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission sera puni d'un emprisonnement de 3 mois a 3 ans et d'une amende de 2000 F a 500 000 F ou de l'une de ces deux peines.

Article 462-5

Quiconque aura procedé a la falsification de documents informatisés, quelle que soit leur forme, de nature a cause un préjudice à autrui, sera puni d'un emprisonnement d'an à cinq ans et d'une amende de 20 000 F à 2 000 000 F.

Article 462-6

Quiconque aura sciemment fait usage des documents visés par l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende 20 000 F à 2 000 000 F ou de l'une de ces deux peines

Article 462-7

La tentative des délits prévus par les articles 462-2 a 462-6 est punie des mêmes peines que le délit lui-même.

Article 462-8

Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou plusieurs infractions prévues par les articles 462-2 a 462-6 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 462-7

Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre.

Q : Comment empêcher mes collaborateurs de consulter certains sites sur Internet ?

R : Votre préoccupation est légitime et c'est celle de nombres de nos clients.

C'est pourquoi **AXE** one® intègre des outils de filtrage de contenu. Cet outil est disponible via l'interface Web d'Administration de votre **AXE** one®. Il vous permet de déclarer manuellement toutes les adresses des sites à interdire ou d'utiliser des listes existantes et régulièrement mises à jours :

squidguard-adult => tente de bloquer le contenu pornographique : à ce jour plus de 390 000 sites bloqués
squidguard-warez => tente de bloquer l'accès aux logiciels pirate : à ce jour plus de 40 sites bloqués
squidguard-publicite => tente de bloquer la publicité : à ce jour plus de 400 sites bloqués
squidguard-audio-video => tente de bloquer l'accès aux morceaux de musique et de film pirate : à ce jour plus de 300 sites bloqués
squidguard-forums => tente de bloquer l'accès aux forums et webmails : à ce jour plus de 30 sites bloqués

Nous vous invitons à consulter notre démonstration en ligne du site d'administration **AXE** one®.

Q : Je suis envahi de mails publicitaires, que faire ?

R : Vous pouvez activer le filtre anti spam de **AXE** one®. Dès lors le sujet des messages SPAM sera automatiquement modifié et vous pourrez écarter facilement ces messages.

Attention, cette démarche est individuelle, en effet il n'appartient pas au serveur de supprimer tel ou tel courriel.

Vous devez donc choisir en toute connaissance de cause l'application ou non de ce dispositif. A l'instar de tous les systèmes anti spam, le filtre **AXE** one® n'est pas infaillible c'est pourquoi nous vous conseillons de ne pas détruire directement les messages marqués « ***SPAM*** » mais de les re-diriger vers un dossier spécifique.

Voici les paramétrages à appliquer à votre logiciel de messagerie :

Outlook Express

1. Menu outils
2. Menu Règles de messages
3. Une fenêtre Nouvelle Règle apparaît
4. Cliquez sur "l'objet contient des mots spécifiques" et "déplacez dans un dossier"
5. Cliquez sur le lien "contient des mots spécifiques" et entrez le mot « ***SPAM*** »
6. Indiquez le dossier vers lequel vous souhaitez déplacer le SPAM

Outlook

1. Menu outils
2. Menu Assistant de Gestion des Messages
3. Cliquez sur Nouveau et choisissez "démarrez à partir d'une règle vide"
4. Cliquez sur suivant et sélectionnez "avec des mots spécifiques dans l'en-tête du message"
5. Cliquez sur le lien "des mots spécifiques" et entrez le mot et entrez le mot « ***SPAM*** »
6. Cliquez sur suivant et sélectionnez "Déplacer dans un dossier"
7. Indiquez le dossier vers lequel vous souhaitez déplacer le SPAM

Q : Je reçois parfois des messages que l'on me demande de faire suivre à des amis. Dois-je le faire ?

R : Surtout pas ! Ces messages sont en réalité des « HOAX ».

Un hoax n'est pas un virus mais une fausse information que l'on tente de vous faire croire afin que vous la propagiez vous-même à vos amis.

Si vous recevez ce genre des messages, il ne faut pas en tenir compte et surtout ne pas le faire suivre à vos correspondants, afin de stopper sa diffusion en chaîne et d'arrêter de polluer les boîtes aux lettres (Cf http://secuser.com/hoax/index.htm).

Q : Virus, vers, chevaux de Troie … on en s'y retrouve plus, un peu d'aide ?

R : Nous vous proposons quelques définitions qui, nous l'espérons, vous permettrons d'y voir plus clair :

Les définitions de fonctions suivantes doivent souvent être légèrement adaptées aux circonstances. Les frontières de classification sont floues, et l'on peut retrouver dans certains parasites des apparences multiples.

- Les virus sont des programmes, souvent de petite taille qui ont la particularité de se reproduire sur un ordinateur en se copiant dans différents fichiers ou structures de disques durs. IL en existe plusieurs types, qui peuvent parfois se regrouper en un seul virus :
    - Les virus exécutables qui se copient sur les programmes eux-mêmes (ex : michelangelo).
    - Les virus de boot que l'on peut répartir en deux catégories :
        - Les virus de partition qui sont dans les fichiers de partition générés par fdisk, par exemple. Un format de les enlèvent pas, et ils sont lancés avant tout autre programme. Très efficaces car ils ne dépendent pas du système d'exploitation installé sur l'ordinateur. Un **fdisk /mbr** peut les enlever (ex : parity boot)
        - Les virus de boot à proprement parler, qui s'exécutent en même temps que le système d'exploitation : (ex : form)

      Ces virus furent pendant longtemps les plus courants car il n'est pas besoin d'installer un jeu ou quoi que se soit sur l'ordinateur pour l'infecter : un simple

oubli de disquette dans le lecteur suffit : dès que le message "disquette non système" apparaît c'est trop tard...

- Les virus compagnons. Drôle de catégorie pour ces virus spécifiquement DOS qui jouent sur le fait que le dos cherche quand on lance un exécutable, d'abord les **.COM** puis les **.EXE** et enfin les **.BAT**. Ces virus se dupliquent en créant un .COM qui reprend le nom d'un .EXE. Il est donc lancé en premier. Ils ont quasiment disparus.

- Les virus de FAT, un exemple : **DIR II**. Ce virus modifie la table d'allocation des fichiers pour que dès qu'on lance un exécutable, on le lance DIR II d'abord. Son éradication doit être faite avec un excellent anti-virus car une mauvaise manipulation peut détruire TOUS les fichiers (la FAT est très dangereuse à manipuler)

- Les virus macro. Cette génération de virus est basée sur le fait que les documents sont souvent interprétés par les programmes. Les macros Word, Excel et autres en sont les exemples les plus frappants. Il peut alors suffire de lire l'attachement d'un mail pour infecter un disque dur. Ils sont en pleine explosion car il est beaucoup plus courant de s'échanger des documents que des binaires. De plus, avec l'explosion d'Internet et de la messagerie, le phénomène s'est amplifiée.

- **Les vers** sont des virus modifiés qui nécessitent des connexions réseaux pour se propager. Certains virus génériques sont dotés de fonction de ver, tel QAZ. Les exemples de ver purs se trouvent généralement sur Unix :

  - Le ver de Morris "l'original"
  - Le ver Ramen
  - Le ver Lion
  - Le ver Adore

  Mais de récents événements ont montré la facilité de propagation de ces vers sur Windows NT :

  - Code Rouge (CodeRed) version 1, 2 et 3
  - NIMDA

  On pourra aussi noter que certains virus macro ou exécutables sont dotés de fonction d'appel automatique à la messagerie électronique, engendrant des réplication par réseau (ex : Iloveyou, bubbleboy,SIRCAM).

- **Les chevaux de Troie** sont des programmes qui en plus d'une fonction classique ont une fonction cachée nuisible : récupérer vos mots de passe, détruire votre

disque dur.

- **Backdoor** littéralement, porte de derrière. C'est une fonction ou un programme permettant à un pirate de prendre le contrôle d'un ordinateur à distance. Il peut être placé dans un cheval de Troie ou un virus. (ex : SubSeven, BackOrifice)

- **Les bombes logiques**. Ce sont des parties de programme qui effectuent une action nuisible sous certaines conditions (de date, de longueur de fichier, de disparition d'un nom d'un fichier du personnel). On les trouve dans les virus et dans les programmes que laissent certains programmeurs qui ont peur de se faire renvoyer.

- **Résident** : programme qui reste actif en mémoire après son lancement.

- **Signature** : les virus se recopient souvent en fait d'un programme. Aussi, afin d'éviter de re-contaminer un programme, il vérifient qu'ils ne l'ont pas déjà infecter en regardant une suite d'octets dans le fichier : c'est la signature du virus.

- **Furtivité**: Capacité qu'à un parasite à se camoufler des outils chargés de le détecter. Il peut modifier les appels systèmes pour qu'ils effacent les renseignements le concernant tels que la taille, la présence d'un dossier, sa présence en mémoire, etc...

- **Cryptage**: La définition, dans le cas des parasites, change un peu du standard. Le cryptage pour les virus ou les vers signifient généralement leur aptitude à rendre leur code suffisamment complexe, voir auto modifiant pour que l'analyse soit extrêmement difficile. Il existe ainsi des virus qui vont prendre des données, les décrypter, les poser dans une zone exécutable, les exécuter. Celles-ci vont à leur tour prendre une partie du code, le changer, etc.

- **Polymorphisme**: La signature des virus a rapidement été un de leur problème. Les sociétés d'anti-virus n'avaient qu'à comparer une chaîne d'octets pour savoir quel était le virus concerné. D'où l'idée qu'ont eu certains de modifier légèrement la descendance de leur virus pour rendre la signature plus complexe. La modification peut être faite par différents moyens :

    - ajout d'instruction inutile (fonction NOP en assembleur, boucle d'attente, calcul sans intérêt)

    - changer la manière de coder une instruction (a=b*c est équivalent à a=c*b ou encore à a=c+c*(b-1))

- **Virus dropper**: ce sont des programmes qui déposent des virus. Ces virus dropper peuvent être eux-mêmes des virus, ainsi certains virus macro déposent des virus

de boot, qui peuvent à leur tour lancer l'infection de virus macro...

- **Les Hoaxes** : ce sont de faux virus. Vous recevez un mail qui vous dit *attention n'ouvrez pas votre courrier, etc.* dans cette catégorie : PENPAL GREETINGS, GOOD TIMES, JOIN THE CREW, etc.,

  Sachez que le fait de lire un mail ne peut JAMAIS infecter un disque dur, à moins d'avoir une interprétation automatique des messages par un logiciel (si vous utilisez Outlook, vous tombez malheureusement dans cette catégorie)

  Pour savoir si un mail que vous recevez est vraiment un virus :

  - http://www.hoaxbuster.com Le site français de référence !
  - http://www.Vmyths.com Site indépendant
  - http://www.hoaxkill.com Idem
  - http://vil.mcafee.com/hoax.asp La liste McAfee
  - http://www.sophos.com/virusinfo/hoaxes Celle de Sophos

- **Les combinés** : ils sont plusieurs choses à la fois par exemple QAZ, qui a fait des ravages chez Microsoft, est un ver, un cheval de Troie, une backdoor et un virus

Q : un email revient me signifiant qu'il n'est pas possible de transférer des fichiers « .pif » ou « .scr » ou « .vbs » à travers le serveur AXE one® !

R : C'est l'anti-virus de votre AXE one® qui bloque ces fichiers.

Les fichiers PIF datent de Windows 3.x ; c'étaient des méta informations sur un programme MS-DOS pour optimiser son lancement sous Windows. Pour en savoir plus http://www.ac-nancy-metz.fr/services/tec/extensions.htm.

Aujourd'hui ces fichiers sont couramment utilisés comme pièces jointes d'Email pour propager des virus.

Q : Comment installer le générateur de fichiers « .pdf » dans AXE one® ?

R : Guide d'Installation sous MS Xp :

1. Fermer toutes les applications actives.
2. Démarrer / Paramètres / Imprimantes et Télécopieurs / Ajouter une imprimante.
3. Dans l'Assistant ajout d'une imprimante : choisir Imprimante réseau / Nom : \\axeone\pdf-generator.
4. Une fenêtre : Connexion à une imprimante s'ouvre "peut contenir des virus" : OK.
5. Une autre fenêtre "recherche pilotes d'impression appropriés" : OK.
6. Fenêtre ajout d'une imprimante : Fabricant : Apple / Imprimante : Apple Color LW 12/660 PS : OK.
7. Patienter.
8. Fenêtre imprimante par défaut : non
9. Terminer.

Q : Je souhaiterais que mon PC se mette à l'heure tout seul.

R : Vous pouvez synchroniser l'heure de votre PC grâce à votre serveur AXE one®.

Sur Windows Xp, double cliquez sur l'heure affichée en bas à droite de votre écran. Dans l'onglet « Temps Internet », tapez « ntp » dans la zone « Serveur ». Cliquez sur « Mettre à jour » puis patientez. Cliquez sur « OK ».

Votre PC se mettra automatiquement à jour chaque semaine.