



Sécurité, c'est quoi ? **Ou, la sécurité à la maison en famille (et ailleurs) bien appliquée.**

Le mot **sécurité** n'a jamais été autant dans la presse depuis les trois dernières années. On parle beaucoup **d'antivirus**, de **firewall (pare-feu)**, **antispymware**, **d'antimalware**, **vulnérabilités**, **mises à jour**, **updates**, **trous de sécurité**, etc. Entre-temps nous sommes habitués à voir apparaître régulièrement ces expressions et termes techniques et même que certains termes font aussi part de notre langage quotidien avec nos amis, nos connaissances, nos proches et dans la presse.

Nous sommes devenus habitués à cette nouvelle **cyberculture**, qui nous impose à apprendre un nouveau **vocabulaire technique (informatique)** et à essayer de **devenir vigilant** et de suivre une **politique de sécurité**.

Mais comment habituer quelqu'un à suivre une politique de sécurité et à devenir vigilant ? Est-ce que nous savons vraiment ce que les mots « **sécurité** », « **politique de sécurité** » et « **vigilance** » veulent dire exactement et surtout ce que c'est cette mentalité qui est cachée derrière ces expressions ?

Franchement, je ne crois pas que la plupart des gens ont jamais appris ce que c'est la sécurité ! L'apprentissage à la sécurité se fait dès le jeune âge de l'enfant pour qu'une **mentalité de sécurité et de vigilance puisse s'établir à la longue ! L'expérience de la vie fera du sien alors pour que la vigilance se développe.**

Mais comment éduquer un enfant à la sécurité et à la vigilance ?

Ce n'est pas si difficile que ça pourtant, et probablement beaucoup de parents le font d'office en partie, sans se rendre compte que cela fait part de l'apprentissage à la sécurité :

- **Expliquer à l'enfant la différence entre le bien et le mal.**
- Éducation des enfants à la sécurité routière (passage clouté, feux de trafic, ceinture de sécurité...).
- Éducation à la maison aux dangers ménagers (fourchettes, couteaux, machines électriques, stylos, escaliers...).
- Éducation à la vigilance (se méfier de personnes inconnues, savoir juger les distances sur la route, ne pas s'approcher trop près des quais et des falaises, etc.).
- **Dès le jeune âge (3-4 ans) visiter avec l'enfant des sites Internet pédagogiques et ludiques** pour l'introduire dans le monde virtuel (Internet).
Exemple : <http://www.uptoten.com>.
- Donner des feuilles de coloriage traitant la sécurité à l'enfant, p.ex. **Mausi** :
http://www.internetmonitor.lu/download/Mausi_parapluie_15022006.pdf
http://www.internetmonitor.lu/download/Mausi_et_Nanti_15022006.pdf **et lui expliquer aussi avec des mots qu'il comprenne, qui sont les méchants et qui les bons.**
- **Expliquer à l'enfant que dès le démarrage de l'ordinateur il faut mettre en route l'antivirus ! (il se souviendra plus tard et il deviendra vigilant).**
- Renforcer le besoin de réfléchir : Questions et réponses, p. ex. : Qu'est-ce qui se passerait si... et donner ensuite des exemples pratiques...
- Éduquer l'enfant à toujours s'habiller selon la saison et lui expliquer pourquoi !!! (grippe, infections, épidémie, etc.)-> **sécurité personnelle et celle des autres (sens de communauté).**

- **Une politique de confiance entre l'enfant et les parents est de rigueur !** De préférence, installez l'ordinateur familial dans une pièce qui est fréquentée par tout le monde et ne pas l'installer dans une pièce fréquentée seulement par l'enfant. De cette façon vous avez toujours à l'œil ce qui se passe et l'enfant peut vous demander conseil à tout moment !
- **Ceci entraîne une atmosphère de confiance, car vous êtes présents quand l'enfant a besoin de vous !**

Les conseils parentaux pour les enfants

Essayez d'expliquer l'importance de l'outil informatique pour son futur travail et **motivez-le** à persévérer dans la matière. Il n'y a que les meilleurs qui auront un bon emploi dans le futur, la concurrence est grande, puis que tout le monde aura un ordinateur dans le futur !!! Et vous êtes à côté de l'enfant pour le superviser et guider, agissez et apprenez ensemble avec lui. Échangez vos connaissances, donnez-vous des défis réciproques, jouez un jeu intelligent en vous donnant des défis pour voir qui a les meilleures connaissances, le tout en respectant le fairness et l'honnêteté envers vous même et votre adversaire (votre enfant). Les règles sont à définir au début, laissez jouer votre imagination **pour définir les récompenses...**

De cette façon vous créez un terrain fertile à l'apprentissage des deux camps (vous et l'enfant) et en même temps une atmosphère entre copains, un terrain idéal pour favoriser un apprentissage adéquat et garanti !!! Jouez intelligemment ce jeu de la vie et de l'apprentissage et vous serez gagnant, il y a un joueur dans chacun de nous qui nécessite d'être activé. Et un petit zeste d'humour, combiné avec du taquinage rend le tout plus intéressant et détendu, un vrai défi qui fait plaisir.

L'emploi de temps et le filtre parental (s'il y en a besoin)

Fixez des heures précises et aussi un maximum d'heures d'utilisation sur Internet et l'ordinateur pour que l'enfant ne passe pas tout son temps sur l'ordinateur. Trop vite il y a une dépendance qui pourrait se développer. Soit que vous utilisez un filtre parental qui règle automatiquement l'emploi du temps et qui bloque l'accès dès atteinte au temps alloué ou bien que vous le faites sur une base d'entente commune. Pour ceux qui utilisent Windows Vista, le filtre parental est déjà intégré d'office. Le filtre parental peut être activé comme suit :

<http://www.clubic.com/article-71858-5-controle-parental-solutions-enfants.html>

Sinon, vous pouvez télécharger et installer un filtre parental, nous vous conseillons le filtre parental de chez « Optenet », dont voici des vidéo-formations gratuites :

<http://www.internetmonitor.lu/index.php?action=article&numero=996>

- **Les parents doivent eux-mêmes s'initier à l'ordinateur et à la sécurité** afin de pouvoir aider leurs enfants ! À cette fin ils peuvent bénéficier de l'aide des sites Internet suivants :
<http://www.internetmonitor.lu> et <http://www.cases.lu> et <http://safersurf.myschool.lu> !
- L'école doit aussi jouer un rôle primordial à l'éducation de la sécurité et de la vigilance :
 1. Quiz informatiques avec auto-évaluation et indices, ainsi que des Podcasts (fichiers audio)
 2. Théâtre Interactif et Pédagogique (TIP) www.ettelbruck.lu/internetstuff/tip/pedago
 3. Introduction de la sécurité dans les cours informatiques

4. **Éducation des enseignants, profs, formateurs à la vigilance et à la sécurité afin qu'ils puissent orienter adéquatement leurs apprenants !**
 - **Une charte d'utilisateur doit être mise en place en famille, au travail, ainsi que dans tout établissement éducatif.** Cette charte doit aussi être signée par les personnes, mentionnant des sanctions pour le non-respect !
 - **À la maison, et en famille, l'utilisation journalière d'Internet et de l'ordinateur doit être réglementée !**
 - **Apprendre aux enfants, dès le jeune âge, le code éthique et de morale suivant :**
 1. **Ce que tu ne veux pas que l'on te fasse, ne le fais pas non plus aux autres !**
 2. **Ce que tu ne souhaites pas ce qui puisse t'arriver, fais tout pour que cela ne puisse arriver non plus aux autres !**

Voilà, ceci c'est des consignes assez simple à suivre et aussi facile à mettre en place, **volonté présente, bien entendu !**

Pour créer une **charte d'utilisation**, voici **un exemple à la page 5**, comment on pourrait la définir. Elle n'est qu'à titre indicatif et peut être changée et/ou comporter des additions, ceci selon vos goûts et convictions !

Il faut créer un dossier, rangé bien visiblement près de l'emplacement de l'ordinateur et contenant les fiches suivantes :

1 fiche séparée pour les mois de mars et septembre, contenant les instructions pour nettoyer le disque dur, y compris une défragmentation du disque dur !

À chaque début du mois faire un backup du système !

Chaque 2^{ème} mercredi du mois faire les updates de Microsoft® ! (Microsoft® les publie les mardis, mais ils sont disponibles en Europe seulement les mercredis) !

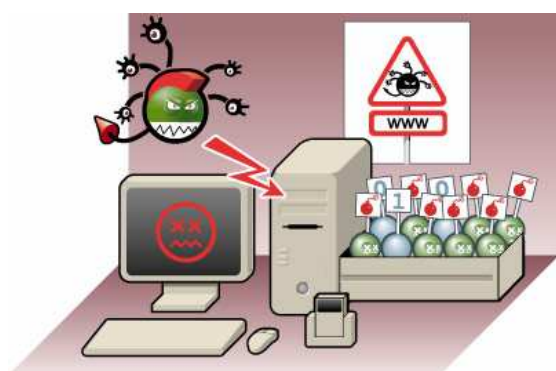
À chaque début du mois (même chaque semaine) faire un scan avec SECUNIA pour vérifier si les logiciels tels que « Java®, Adobe Acrobat Reader®, Macromedia Flash Player®, Adobe Flash Player®, Internet Explorer et Firefox®, etc. » sont mis à jour !

Insérer les didacticiels suivants :

- **A squared :** logiciel antimalware
- **Ad Aware :** logiciel antispysware
- **Spybot S&D :** logiciel antispysware
- **Secunia :** logiciel de contrôle de conformité des mises à jour
- **Sweepi :** logiciel de nettoyage du disque dur
- **CCleaner :** logiciel de nettoyage du disque dur
- **Défragmentation du disque dur**

Voici un tableau indiquant les adresses de téléchargement des didacticiels :

Logiciels	Adresses Internet
Sweepi	www.internetmonitor.lu/download/SWEEPI.pdf
CCleaner	www.internetmonitor.lu/download/ccleaner_27082006.pdf
Défragmentation disque dur	www.internetmonitor.lu/download/Defragmentation_du_disque_dur_avec_decoupe.pdf
Ad Aware	www.pcentraide.com/index.php?showtopic=188
Spybot Search&Destroy	www.internetmonitor.lu/download/Spybot_S_D_Tutorial.pdf
A squared	www.internetmonitor.lu/download/Tutoriel_12.11.2004..pdf
Secunia	www.internetmonitor.lu/download/Scan_gratuit_de_logiciels_installes_15122006.pdf



En plus des logiciels à télécharger, veuillez noter aussi qu'il existe des forums d'entraide PC.

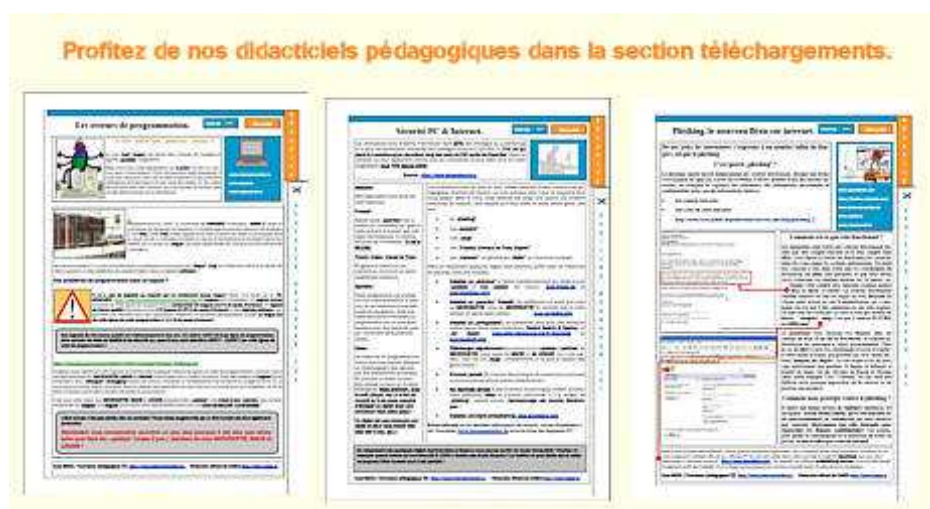
Ces adresses peuvent être très précieuses pour vous en cas de pannes et/ou problèmes de votre ordinateur et quand vous avez des questions concernant la sécurité informatique. N'hésitez pas à le fréquenter, c'est gratuit et des conseils

professionnels sont garantis !

Quelques bons liens :

Comment ça marche : <http://www.commentcamarche.net>

01.Net : <http://forum.telecharger.01net.com/>



<http://www.internetmonitor.lu/index.php?action=telechargement&>

Charte d'utilisation :

Par la présente, je soussigné(e).....déclare de prendre entièrement conscience de cette charte et de la respecter à la lettre, faute de subir les sanctions y prévus par la famille.

1. **Je dois être conscient** que dès que je me connecte à Internet, **je fais part d'une communauté de laquelle je suis en partie responsable.**
2. **Je suis moi-même, comme tout autre utilisateur de cet ordinateur, responsable du bon fonctionnement de celui-ci, aussi du point de vue de sécurité.**
3. **Chaque anomalie de l'ordinateur ainsi que les anomalies rencontrées sur Internet sont de préférence à rapporter à un parent et/ou responsable.**
4. **Chaque medium de sauvegarde (clé USB, caméra, appareil photo digital, disquette, cartes flash, etc.) utilisé sur cet ordinateur est à scanner d'office avec l'antivirus et un programme antimalware (de préférence « a squared ») avant d'utiliser celui-ci !**
5. **Quand nous sommes plusieurs dans la famille, les tâches d'entretien et de maintenance seront partagées entre les différents membres de la famille et ceci selon tour de rôle.**
6. **Cette liste des tâches à faire sera établie ensemble en famille avec accord commun des membres.**
7. **Je respecte le plan horaire** qui m'a été attribué pour surfer sur Internet. Ceci dans le seul but de me protéger d'un abus et d'une dépendance.
8. **Mes parents, de leur part, vont s'abonner à des lettres d'information (newsletter) sur la sécurité PC&Internet** et ils me tiendront au courant de nouvelles vulnérabilités. Si par exemple, moi-même je suis au courant de nouvelles de sécurité avant eux, je leur en fais part et j'avertis aussi mes frères et sœurs.
9. **La famille disposera d'un dossier contenant des didacticiels servant à sécuriser l'ordinateur.** Ce dossier se trouvera toujours à un emplacement prévu près de l'ordinateur, afin que chaque utilisateur puisse s'en servir, le cas échéant !
10. **Les « back up » sont très importants et doivent être faits de façon régulière.** Chaque membre de la famille qui utilise l'ordinateur est responsable pour que les « back up » soient faits régulièrement. **Si jamais un membre de la famille l'avait oublié, je l'avertirais de bien vouloir le faire ultérieurement dans les plus brefs délais.**

Cette charte d'utilisation de l'ordinateur et de l'internet a pour seul but la bonne entente entre les membres de la famille et de la communauté sur Internet. **Je dois être conscient que nous sommes tous responsables un vis-à-vis de l'autre !**



Il est important de suivre à la lettre cette charte, car le bien-être de nous tous en est dépendant !

Conseils et récapitulatif :

Afin d'être toujours mis à jour avec les dernières nouvelles sur la sécurité PC&Internet, veuillez vous abonner à la lettre d'information (newsletter) de « MySecureIT » à l'adresse URL suivante : <http://safersurf.myschool.lu>.

Abonnez-vous gratuitement aux fiches de sécurité informatique de mySchool! 



En collaboration avec l'Internet Monitor (<http://www.internetmonitor.lu>), site internet édité par M. Gust MEES, formateur pédagogique TIC (Gérant de l'Internetstuff ETTELBRUCK) et mySecureIT, mySchool! publie **52 fiches sur la sécurité informatique**. Ces fiches sont formulées de manière très simple avec un jargon technique limité au plus strict minimum afin que tout le monde puisse les comprendre aisément et en tirer un bénéfice maximal. Des liens vers des sites qui vous faciliteront la vie et beaucoup de captures d'écran qui rendent les explications encore plus claires vous feront adorer ces fiches. Réalisées plutôt pour des débutants que pour des pros en informatique, même ces derniers peuvent encore glaner l'une ou l'autre information précieuse.

C'est gratuit! Inscrivez-vous une seule fois ci-dessous et vous recevrez chaque semaine une des 52 fiches de sécurité.

... et une cure de wellness... pour votre ordinateur! Parmi toutes les personnes qui se sont abonnées à ce site, **10 personnes bénéficieront d'un check-up total de sécurité gratuit de leur ordinateur**. Ce check-up, offert gracieusement par l'Internet Monitor, vous permettra de faire vérifier tous les logiciels de votre ordinateur pour contrôler s'ils ne sont pas affectés par des virus, chevaux de Troie, spyware ou malware. Il va de soi que ces problèmes, une fois identifiés, seront éliminés par les spécialistes de l'Internet Monitor.

La sécurité informatique nous concerne tous!
Agissons!

Récapitulatif :

Essayez d'installer ces logiciels de sécurité et faites-en part de leur utilisation aux autres membres de la famille. Utilisez la charte d'utilisation et faite la signer par tous les membres de la famille (parents inclus) ! Employez les feuilles au format Excel[®], imprimez-les et désignez un responsable pour chaque semaine, qui devra se charger de remplir les responsabilités lui octroyées !

Avec cette méthode, qui vise la bonne entente dans la communauté, vous créez une atmosphère de confiance et les personnes seront responsabilisées. **La responsabilité est le premier pas envers l'apprentissage de la sécurité et de la vigilance.** Si cette méthode est bien pratiquée, vous n'auriez même pas besoin de contrôle parental, m'enfin, superviser de temps à autre ne fait pas tort non plus ! Et pour les sanctions, choisissez-les de telle manière qu'elles sont constructives (soyez créatifs, essayez de trouver quelque chose qui malgré la sanction est bénéfique pour la communauté).

Et surtout, n'oubliez pas à vous abonner à des lettres d'information <http://www.internetmonitor.lu> afin d'être toujours informé sur les dernières vulnérabilités. La mafia informatique (les cybercriminels) ne se repose(nt) pas, au contraire ils inventent sans cesse de nouveaux scripts malicieux. Mieux vaut être prévenu que d'être guéri !

Une guérison n'est guère plaisante et coûte aussi du temps, ainsi que de l'argent! Estimez plus au moins 50 €/heure (mars 2008) pour une intervention technique, qui en moyenne nécessite 5 à 6 heures pour décontaminer un ordinateur, si jamais il y a moyen sans avoir besoin de reformater !

Mode d'emploi

1. Téléchargez les didacticiels suivants :

Sweepi :

<http://www.internetmonitor.lu/download/SWEEPI.pdf>

CCleaner :

http://www.internetmonitor.lu/download/ccleaner_27082006.pdf

Défragmentation disque dur :

http://www.internetmonitor.lu/download/Defragmentation_du_disque_dur_avec_decoupe.pdf

Ad Aware:

<http://www.pcentraide.com/index.php?showtopic=188>

Spybot Search&Destroy:

http://www.internetmonitor.lu/download/Spybot_S_D_Tutorial.pdf

a squared :

http://www.internetmonitor.lu/download/Tutoriel_12.11.2004..pdf

Secunia :

http://www.internetmonitor.lu/download/Scan_gratuit_de_logiciels_installes_15122006.pdf

2. Téléchargez et imprimez les feuilles de travail (format Excel) aux adresses URL suivantes :

<http://www.ettelbruck.lu/internetstuff/charte/janvier.xls>

<http://www.ettelbruck.lu/internetstuff/charte/fevrier.xls>

<http://www.ettelbruck.lu/internetstuff/charte/mars.xls>

<http://www.ettelbruck.lu/internetstuff/charte/avril.xls>

<http://www.ettelbruck.lu/internetstuff/charte/mai.xls>

<http://www.ettelbruck.lu/internetstuff/charte/juin.xls>

<http://www.ettelbruck.lu/internetstuff/charte/juillet.xls>

<http://www.ettelbruck.lu/internetstuff/charte/aout.xls>

<http://www.ettelbruck.lu/internetstuff/charte/septembre.xls>

<http://www.ettelbruck.lu/internetstuff/charte/octobre.xls>

<http://www.ettelbruck.lu/internetstuff/charte/novembre.xls>

<http://www.ettelbruck.lu/internetstuff/charte/decembre.xls>

Le cas où vous n'aimez pas télécharger autant de fichiers, veuillez utiliser cette feuille de travail :

<http://www.ettelbruck.lu/internetstuff/charte/fichedemaintenancepc.pdf>

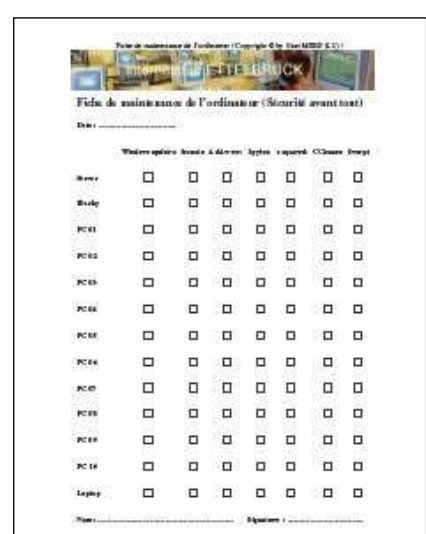
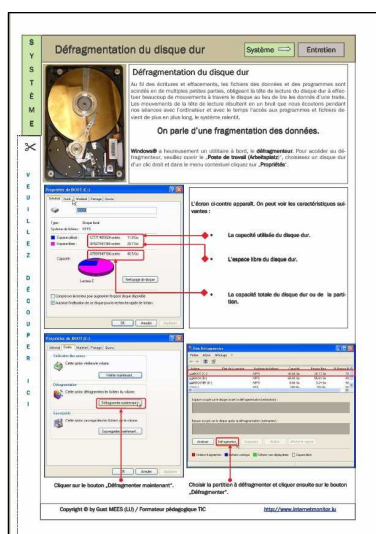
3. Imprimez-les
4. Préparez un dossier et classez-les (ce didacticiel inclus)
5. Téléchargez et installez les logiciels tels que conseillés dans les didacticiels
6. Scannez votre ordinateur avec ces logiciels tel que conseillé dans les didacticiels et selon le même ordre comme marqué ci-dessus, c'est-à-dire : d'abord « Sweepi », puis « CCleaner », suivi d'une défragmentation et un scan de « Ad Aware », puis un scan avec « Spybot S&D » et un scan avec « a squared ». Ensuite connectez-vous à Internet et faites un scan en ligne avec l'utilitaire de « Secunia » tel que conseillé dans le didacticiel.
7. Faites-en aussi un scan avec votre antivirus vers la fin de cette procédure.
8. Comme vous êtes maintenant un peu familiarisé avec ces logiciels, montrez leur fonctionnement ensuite aux membres de votre famille et profitez-en pour leurs expliquer en même temps l'importance de la charte d'utilisateur et l'importance de la sécurité.

Le cas échéant où vous ne disposeriez de logiciel pour ouvrir les fichiers au format « .pdf », veuillez télécharger le logiciel « Adobe Acrobat Reader® » à l'adresse URL

<http://www.adobe.com/products/acrobat/readstep2.html>

Si vous ne disposiez pas du programme « Excel® », vous pouvez télécharger la visionneuse à l'adresse suivante (lit les fichiers, mais ne peut pas en créer)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c8378bf4-996c-4569-b547-75edbd03aaf0&DisplayLang=de>



Mots clés :

- 1. L'éducation à la sécurité et de la vigilance**
- 2. La politique de sécurité**
- 3. L'atmosphère de confiance**
- 4. L'aménagement de l'emplacement de l'ordinateur**
- 5. Le filtre parental**
- 6. Les conseils parentaux**
- 7. L'organisation et répartition des charges--->la responsabilisation**
- 8. La motivation--->défi etc.**
- 9. L'information et l'apprentissage**
- 10. L'éthique et la morale**
- 11. Les conseils**

Chaque ordinateur sécurisé réduit l'efficacité des cybercriminels et de ce fait la réussite de leurs attaques !