

## 30. Compilation Sécurité PC & Internet

Étant donné qu'il y a une circulation impressionnante de malware (code malicieux, virus, ver, dialer, troyen, spam, etc.) sur Internet, nous devons sécuriser notre ordinateur.

De nos jours aucun système d'exploitation (OS) n'est assez sécurisé par sa version d'installation d'origine. Ceci est le cas aussi bien pour Mac®, que pour Linux®, ou encore Windows®.

D'ailleurs une sécurité totale des systèmes d'exploitation (OS) n'est pas envisageable dans un proche avenir. L'évolution rapide des malware (virus, vers, troyens, etc.) progresse et une solution globale de protection n'est pas encore en vue!

### Plus aucun système d'exploitation (OS) n'est sûr de nos jours!

La vulnérabilité du système d'exploitation de Windows® est bien connue, mais les autres sont aussi vulnérables!

Veillez vous renseigner aux liens suivants:

Linux®:

[http://www.internetmonitor.lu/index.php?action=rubrique&id\\_rubrique=9160&mn\\_8948=true](http://www.internetmonitor.lu/index.php?action=rubrique&id_rubrique=9160&mn_8948=true)

Mac®:

[http://www.internetmonitor.lu/index.php?action=rubrique&id\\_rubrique=9668&mn\\_8948=true](http://www.internetmonitor.lu/index.php?action=rubrique&id_rubrique=9668&mn_8948=true)

**C'est pour cette raison que nous devons agir!**



### Comment sécuriser notre ordinateur?

Souvenons-nous des vieux proverbes qui disent:

“*Danger connu est danger vaincu*”. En allemand “*Gefahr erkannt ist Gefahr gebannt.*” En anglais “*forewarned is forearmed*”.

Ceci montre bien que si nous connaissons les dangers, nous deviendrons automatiquement plus vigilants et la probabilité que nous attraperons une de ces malware va déjà être réduite. C'est pour cette raison qu'il vaut mieux s'informer régulièrement! Nous vous conseillons de vous abonner aux newsletters de l'Internet Monitor à l'adresse suivante : <http://www.internetmonitor.lu>

Si après avoir pris conscience des dangers, nous installons en plus des logiciels de sécurité sur notre ordinateur, nous serons sécurisés au maximum.



### Ce qu'il faut faire pour sécuriser l'ordinateur :

1. installer un antivirus commercial ou freeware
2. installer un firewall (pare-feu)
3. installer un antitroyen
4. installer un antidialer
5. installer un antispyware
6. installer régulièrement les updates (patches) de chez Microsoft®, Mac® et Linux® !
7. respecter la Netiquette et la Chatiquette

## **Veillez noter quand même qu'une sécurité à cent pourcent n'existe pas et est illusoire!**

Comme nous sommes maintenant conscients qu'il y a des dangers, essayons de nous protéger avec les logiciels proposés par le marché. La plupart d'entre eux sont même gratuits (freeware/gratuciels), mais très performants et même meilleurs que les produits commerciaux (payants)!

### **AUTRES PRÉCAUTIONS À PRENDRE :**

Ne jamais ouvrir du courrier électronique (email) de personnes inconnues, surtout pas les pièces jointes (attachments)!

### **Nouvelle variante du phishing:**

[http://www.internetmonitor.lu/index.php?action=article&id\\_article=100645&id\\_rubrique=9975](http://www.internetmonitor.lu/index.php?action=article&id_article=100645&id_rubrique=9975)

Ne jamais ouvrir de courrier électronique vous demandant de saisir à nouveau vos données (banques, eBay, etc.). Danger de Phishing!

Il existe deux sortes d'attaques:

1. Attaques par courrier électronique
2. Attaques dues à un système d'exploitation pas mis à jour (Windows updates)

Lire aussi:

Phishing, le nouveau fléau d'Internet

[http://www.internetmonitor.lu/index.php?action=article&id\\_article=65165&id\\_rubrique=9975](http://www.internetmonitor.lu/index.php?action=article&id_article=65165&id_rubrique=9975)

Les arnaques bancaires se multiplient dans le monde

[http://www.internetmonitor.lu/index.php?action=article&id\\_article=69163&id\\_rubrique=9975](http://www.internetmonitor.lu/index.php?action=article&id_article=69163&id_rubrique=9975)

### **DESCRIPTION DE FONCTIONNEMENT DES PROGRAMMES (LOGICIELS) DIFFÉRENTS**

#### **L'antivirus**

L'antivirus est le système immunitaire contre les épidémies virales informatiques de notre ordinateur. Quand il n'y en a pas, nous sommes vulnérables et nous serons infectés tôt ou tard! Veuillez aussi lire l'article suivant:

Un PC sans protection ne survivrait que 20 minutes sur Internet

[http://www.internetmonitor.lu/index.php?action=article&id\\_article=68827&id\\_rubrique=9392](http://www.internetmonitor.lu/index.php?action=article&id_article=68827&id_rubrique=9392)



Une fois infectés, nous infecterons aussi les autres internautes. Comme Internet fonctionne selon le principe de la communauté, nous devons aussi faire attention aux autres internautes, les respecter. Dès que nous sommes connectés à Internet, nous surfons ensemble avec des millions d'autres internautes! Lire aussi:

Visual PC:

<http://www.internetmonitor.lu/pcsecurity>

Comprendre Internet:

[http://www.internetmonitor.lu/index.php?action=article&id\\_article=67356&id\\_rubrique=8949](http://www.internetmonitor.lu/index.php?action=article&id_article=67356&id_rubrique=8949)

Le PC, Internet et son utilisation:

[http://www.internetmonitor.lu/index.php?action=article&id\\_article=67449&id\\_rubrique=8949](http://www.internetmonitor.lu/index.php?action=article&id_article=67449&id_rubrique=8949)

Les dangers sur Internet en chiffres:

[http://www.internetmonitor.lu/index.php?action=article&id\\_article=85139&id\\_rubrique=8949](http://www.internetmonitor.lu/index.php?action=article&id_article=85139&id_rubrique=8949)

L'antivirus est le vaccin pour notre ordinateur. Il y a différents fabricants de logiciels antivirus, dont voici ci-dessous une liste des plus renommés et performants. Les logiciels (programmes) présentés ici sont des versions contenant un antivirus et firewall (pare-feu) dans un seul package:

Norton Internet Security™

McAfee®

Trend Micro PC Cillin®

Bitdefender®

AVG Anti Virus (freeware / gratuit)

Actuellement, un des plus performants (selon les tests de magazines professionnels PC) est Norton Internet Security™, que vous pouvez trouver à l'adresse suivante: <http://www.symantec.com>

Les autres logiciels mentionnés ci-dessus sont pareils, ils contiennent également un firewall (pare-feu). Lire aussi firewall et antivirus: <http://www.webwizardbiz.com/tutorials/firewalls/>

## Le firewall (pare-feu)

Le firewall (pare-feu) est le système anti-intrusion (système d'alarme) pour notre ordinateur. Il bloque le trafic des données non désirées entrantes et sortantes sur notre ordinateur. À voir comme un portier qui contrôle le va-et-vient. On appelle les logiciels (programmes) firewall aussi des desktop firewall.

Une autre sorte de firewall (pare-feu) est le hardware firewall. Celui-ci est branché par câble à l'ordinateur ou il est déjà intégré dans les nouvelles générations de Router. Le Router gère le trafic des données entre le serveur et les ordinateurs différents.

En version freeware (gratuciel) il existe aussi Zone Alarm Pro® qui est très performant et selon les tests de magazines PC professionnels, actuellement le meilleur (01.01.2005). <http://www.zonelabs.com>

Le firewall (pare-feu) de Windows® XP ne contrôle que le trafic entrant et pas le trafic sortant! Pour avoir plus d'informations concernant les firewalls, veuillez cliquer sur le lien suivant: <http://www.webwizardbiz.com/tutorials/firewalls>

## L'antitroyen et l'antidialer

Comme il existe aussi des troyens et des dialer, il faut installer un logiciel (programme) qui protège l'ordinateur et qui éradique aussi ces bestioles informatiques. Lire aussi les articles:

C'est quoi un dialer?

<http://www.webwizardbiz.com/tutorials/dialer/>

C'est quoi un troyen (cheval de Troie)?

[http://www.internetmonitor.lu/index.php?action=article&id\\_article=91039&id\\_rubrique=8949](http://www.internetmonitor.lu/index.php?action=article&id_article=91039&id_rubrique=8949)

Un programme (logiciel) très efficace, qui éradique ces bestioles informatiques (malware/troyens, virus, vers, dialer, etc.) et qui nous protège aussi contre ceux-ci est a2 (a squared) de Emsisoft. Ce logiciel (programme) est multilingue, très efficace et très facile à utiliser (aucune configuration). Vous trouverez un didacticiel à l'adresse suivante : Comment installer et se servir de a<sup>2</sup>

[http://www.internetmonitor.lu/index.php?action=telechargement&startdownload=Tutoriel\\_12.11.2004..pdf&startid=3402&id\\_classeur=803](http://www.internetmonitor.lu/index.php?action=telechargement&startdownload=Tutoriel_12.11.2004..pdf&startid=3402&id_classeur=803)

## L'antispyware

Des programmes espions, appelés aussi mouchards ou spyware s'installent sur notre ordinateur à notre insu. Ces programmes espionnent nos habitudes de navigation sur Internet et envoient les résultats obtenus de leur enquête à leur programmeur, qui revend ces informations à des polluposteurs (envoyeurs de spam) et/ou à des firmes non sérieuses faisant de la publicité forcée sur Internet.

L'effet que cela fait est, que nous serons bombardés par des fenêtres pop-up (fenêtres surgissant soudainement sur l'écran), montrant de la publicité sur des articles qui pourraient nous intéresser. On appelle ceci aussi de la publicité ciblée.



Une liste de logiciels (programmes) qui nous protègent contre ces espions et qui les éradiquent aussi, peut être trouvée à l'adresse suivante: [http://www.internetmonitor.lu/download/02\\_Spyware.pdf](http://www.internetmonitor.lu/download/02_Spyware.pdf)

Comment installer et se servir de Spybot Search&Destroy?  
[http://www.internetmonitor.lu/download/Spybot\\_S\\_D\\_Tutorial.pdf](http://www.internetmonitor.lu/download/Spybot_S_D_Tutorial.pdf)

Autant de programmes (logiciels) pour sécuriser notre ordinateur? Eh bien oui, malheureusement! Mais la tendance va vers des logiciels, qui intègrent toutes les fonctions mentionnées dans cet article dans un seul logiciel. Mais, tant qu'ils ne sont pas encore disponibles sur le marché, il nous faudra vivre avec cette situation et installer ces différents logiciels!

Veuillez suivre le "Guide pratique de la sécurité", que vous trouverez à l'adresse suivante et que vous pouvez aussi télécharger:  
<http://www.webwizardbiz.com/tutorials/guidesecurite/>  
Essayez de suivre ce tutoriel à la lettre et consacrez +/- 15 à 20 minutes par week-end pour votre sécurité et celle des autres.

Si tout internaute avait installé au moins un antivirus et un firewall (pare-feu), Internet serait déjà plus sûr. Une étude a démontré que 80% du spam serait généré par des ordinateurs non sécurisés, des PC zombies.

Votre ordinateur est-il un zombie?

[http://www.internetmonitor.lu/index.php?action=article&id\\_article=67428](http://www.internetmonitor.lu/index.php?action=article&id_article=67428)

Nos responsabilités sur Internet:

[http://content.myschool.lu/downloads/mysecureit/05\\_NosResponsabilite.pdf](http://content.myschool.lu/downloads/mysecureit/05_NosResponsabilite.pdf)

Nous vous conseillons de lire les articles mentionnés ci-dessus, afin de mieux comprendre l'importance de la sécurité pour nous tous!

## FAQ's (Frequently asked questions) :

### J'ai installé Windows® XP et le SP2. Suis-je sécurisé?

Réponses:

- 1) Non. D'abord le firewall (pare-feu) de Windows® XP ne bloque que les données non désirées entrantes et pas les données sortantes!
- 2) Il faut quand même faire les updates de chez Microsoft® régulièrement.
- 3) Il faut quand même installer en plus les programmes (logiciels) antimalware mentionnés en début de cet article!

### Comment nous informer sur les nouvelles menaces?

Vous avez la possibilité de vous inscrire aux newsletters du site internet "l'Internet Monitor" à l'adresse suivante: <http://www.internetmonitor.lu>  
Il suffit d'inclure votre adresse électronique et de cliquer sur "inscrire". Ensuite vous serez informés régulièrement sur les nouvelles menaces, sur les nouveaux produits, sur des didacticiels concernant la sécurité PC&Internet, des trucs et astuces sur le PC&Internet, des téléchargements gratuits, etc.

L'Internet Monitor est un site internet reconnu d'utilité public et professionnel. Il est d'ailleurs aussi répertorié dans le Guide des meilleurs sites internet et répertorié aussi chez lamooche.com, un catalogue professionnel de syndication de contenu XML (RSS, ATOM FEED)! <http://www.bonweb.com> <http://www.lamooche.com>

En plus Internet Monitor est partenaire officiel du Ministère de l'Économie Luxembourgeois et d'autres services des Ministères Luxembourgeois se réfèrent aussi à nos articles! <http://www.cases.lu>



Pour ceux et celles qui ont la possibilité de lire des informations RSS, nous syndiquons aussi notre contenu par cette voie, dont voici les liens:

<http://www.internetmonitor.lu/syndication.rss>

<http://www.internetmonitor.lu/atom.xml>

**Vous ne connaissez pas les fils RSS?** Veuillez suivre le lien suivant et lire le didacticiel à ce sujet:

(pas de connaissances techniques requises)

[http://www.internetmonitor.lu/index.php?action=telechargement&startdownload=RSS et BLOGS 23.11.2004..pdf&startid=3513&id\\_classeur=819](http://www.internetmonitor.lu/index.php?action=telechargement&startdownload=RSS_et_BLOGS_23.11.2004..pdf&startid=3513&id_classeur=819)

La syndication par fils RSS est l'avenir de la communication sur Internet! Simple, rapide et efficace. Jamais le flux d'informations n'a pu passer si rapidement. Internet nous ouvre la voie de la communication!



## Glossaire

- malware – Mot regroupant les virus, vers, dialer et toutes autres bestioles informatiques.
- troyen (Trojaner/trojan) – Programme malicieux cachant un deuxième programme malicieux.
- dialer – Programme générateur d'une communication surtaxée.
- antivirus – Le système immunitaire de notre ordinateur (obligatoire)!
- antitroyen – Programme protecteur et éradicateur de troyens.
- antidialer – Programme protecteur et éradicateur de dialer.
- antispyware – Programme protecteur et éradicateur de spyware (mouchards).
- polluposteur – Distributeur de courrier non sollicité (spam)
- phishing – Détournement et usurpation d'identité d'un site internet.
- firewall (pare-feu) – Le système anti-intrusion de notre ordinateur (obligatoire) !

## Liens:

Les 2 mondes: <http://www.webwizardbiz.com/tutorials/responsabilites/>

Visual PC&Internet: [http://www.internetmonitor.lu/index.php?action=article&id\\_article=70793](http://www.internetmonitor.lu/index.php?action=article&id_article=70793)

Netiquette: <http://www.sri.ucl.ac.be/SRI/rfc1855.fr.html#intro>

Chatiquette: <http://www.artetcraft.com/chat/netiquette.php>

Malware: <http://www.homepages.lu/gust.mees/mausi/securite/malware/>

Guide pratique de la sécurité: <http://www.webwizardbiz.com/tutorials/guidesecurite/>

Spyware: [http://www.internetmonitor.lu/index.php?action=article&id\\_article=83305](http://www.internetmonitor.lu/index.php?action=article&id_article=83305)

Dialer: <http://www.webwizardbiz.com/tutorials/dialer/>

Troyen: [http://www.internetmonitor.lu/index.php?action=article&id\\_article=91039](http://www.internetmonitor.lu/index.php?action=article&id_article=91039)

Antispyware installation: [http://www.internetmonitor.lu/download/Spybot S D Tutorial.pdf](http://www.internetmonitor.lu/download/Spybot_S_D_Tutorial.pdf)

Nos responsabilités dans Internet: [http://www.internetmonitor.lu/index.php?action=article&id\\_article=67346](http://www.internetmonitor.lu/index.php?action=article&id_article=67346)

E-book Security: <http://www.homepages.lu/gust.mees/pedago/ebook/index.html>

Vigilance (Éditorial): [http://www.internetmonitor.lu/index.php?action=article&id\\_article=67387&id\\_rubrique=10031](http://www.internetmonitor.lu/index.php?action=article&id_article=67387&id_rubrique=10031)

Le nouveau monde, le monde virtuel:

[http://content.myschool.lu/downloads/mysecureit/03\\_LeNouveauMonde.pdf](http://content.myschool.lu/downloads/mysecureit/03_LeNouveauMonde.pdf)

Zonelabs: <http://www.zonelabs.com>

## Comment savoir si notre ordinateur est bien protégé, bien sécurisé?

Rien ne vaut un contrôle pratique pour s'assurer. Pour ceci on vous propose deux formules différentes :

1. Visitez le didacticiel à l'adresse suivante et téléchargez-le (2 pages A4). Test en ligne gratuit (on-line):

[http://www.internetmonitor.lu/download/Online\\_Security\\_Check GRATUIT et performant .pdf](http://www.internetmonitor.lu/download/Online_Security_Check GRATUIT et performant .pdf)

2. Test des ports du PC, contrôler l'efficacité du firewall (pare-feu)

[http://www.internetmonitor.lu/index.php?action=telechargement&startdownload=Comment\\_tester\\_si\\_les\\_ports\\_de\\_mon\\_PC\\_sont\\_securises\\_19.12.2004..doc&startid=4175&id\\_classeur=918](http://www.internetmonitor.lu/index.php?action=telechargement&startdownload=Comment_tester_si_les_ports_de_mon_PC_sont_securises_19.12.2004..doc&startid=4175&id_classeur=918)

Après les avoir téléchargés, suivez les instructions et vous serez beaucoup plus confiants après!

Autres sites sur la sécurité:

<http://www.webwizardbiz.com/tutorials/security>

<http://www.internetmonitor.lu>

<http://www.homepages.lu/gust.mees/mausi/securite/malware/>

Blogs sur la Sécurité PC & Internet:

<http://www.internetmonitor.lu/pcsecurity>

<http://www.u-blog.net/pcsecurity>

Syndication RSS et ATOM:

<http://www.internetmonitor.lu/syndication.rss>

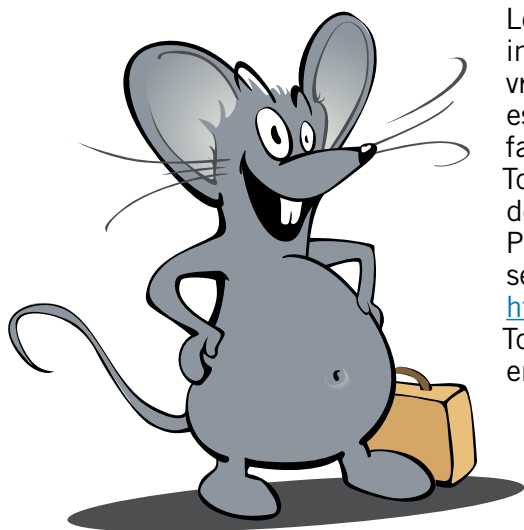
<http://www.internetmonitor.lu/atom.xml>

Au cas où vous ne disposez pas de lecteur RSS (RSS-Reader), nous vous conseillons Feed Reader, que vous pouvez télécharger à l'adresse URL suivante: <http://www.feedreader.com>

En plus vous trouverez un didacticiel sur l'installation et l'utilisation de Feed Reader à l'adresse URL suivante:

[http://www.internetmonitor.lu/download/feedreader\\_installation\\_et\\_utilisation.pdf](http://www.internetmonitor.lu/download/feedreader_installation_et_utilisation.pdf)

## RÉCAPITULATIF :



Le PC et Internet ont créé un nouveau mass média, une base de données inépuisable, grandissant à chaque seconde. Ce mass média nous ouvre le monde de la communication et de l'information. Pour tout ce qui est nouveau, il nous faut un certain temps pour nous habituer, nous familiariser, apprendre à nous servir de cette nouvelle technologie. Toute nouvelle technologie requiert aussi un entretien technique et des consignes de sécurité! Le PC et Internet n'y font pas exception! Pour vous faciliter la tâche, veuillez suivre le "Guide pratique de la sécurité", que vous trouverez à l'adresse URL suivante:

<http://www.webwizardbiz.com/tutorials/guidesecurite/>

Tout ce qui a été expliqué dans ce didacticiel s'y trouve et est expliqué en détail.

[www.cte.lu](http://www.cte.lu)

[www.myschool.lu](http://www.myschool.lu)

[www.mysecureit.lu](http://www.mysecureit.lu)

[www.etwinning.lu](http://www.etwinning.lu)



MINISTÈRE DE L'ÉDUCATION NATIONALE  
ET DE LA FORMATION PROFESSIONNELLE  
Centre de technologie de l'éducation



Copyright © 2005, [www.mySchool.lu](http://www.mySchool.lu)

Tous droits réservés. Ce document est la propriété de mySchool! (CTE) et peut être reproduit pourvu qu'aucune modification ne soit effectuée et que cette notice soit préservée. Les informations véhiculées par la présente fiche le sont dans l'espoir qu'elles seront utiles. La responsabilité des auteurs ne pourra être engagée à aucun moment.