Sécurité PC & Internet.

Internet ⟶ Sécurité

Les ordinateurs sont présents maintenant dans **87%** des ménages au Luxembourg et le taux de pénétration d'Internet des ménages se situe à son tour à **77%, ce qui place le Luxembourg au deuxième rang des pays de l'UE après les Pays-Bas**. Dans ce contexte on peut également relever que les connexions à haut débit sont en nette progression (**plus 70% depuis 2004**).

Source : http://www.eluxembourg.lu

Malware:

Mot regroupant toute sorte de code malicieux.

Firewall :

Appelé aussi „**pare-feu**“ est le portier de l'ordinateur qui gère le trafic entrant et sortant des données informatiques. Il contrôle les ports de l'ordinateur, **il y en a 65.535.**

Troyen, trojan, cheval de Troie :

Programme malicieux qui contient au minimum un autre programme malicieux.

Spyware :

Petits programmes qui s'installent sur votre ordinateur à votre insu et qui espionnent vos habitudes de navigation. Ainsi vos habitudes seront envoyées au programmeur qui lui vous bombardera avec des fenêtres „pop-up“ contenant de la publicité ciblée !

Dialer :

Un dialer est un programme malicieux que vous pouvez attraper en téléchargeant des logiciels sur des plateformes douteuses. En principe un dialer ne peut être attrapé qu'avec un modem analogique. **Mais attention, avec le VoIP (Skype, etc.) il a été démontré qu'il est aussi possible d'attraper un dialer avec une connexion haut débit (adsl) !**

Un dialer est une connexion surtaxée et peut vous coûter très cher (50 €/clic, etc.) !

Les ordinateurs sont de plus en plus utilisés dans les écoles comme outil pédagogique. Internet est devenu un outil précieux dont nous ne pourrons plus nous passer dans le futur, mais internet est aussi une source qui contient beaucoup de risques ; des risques qu'il faut éviter et aussi savoir gérer, tels que :

- Le „**phishing**“.
- Les „**spyware**“.
- Les „**virus**“.
- Les „**Troyens, chevaux de Troie, trojans**“.
- Les „**malware**“, en général les „**dialer**“ ou connexion surtaxée.

Mais en respectant quelques règles nous pouvons surfer avec un maximum de sécurité. Voici nos conseils :

- **Installez un „antivirus“** et faites quotidiennement les mises à jour (**updates / live update**) de celui-ci. www.freeav.de et www.symantec.com
- **Installez un „pare-feu“** (**firewall**), de préférence un autre que celui de **MICROSOFT®**. Celui de **MICROSOFT®** ne contrôle que le trafic entrant et pas le trafic sortant. www.zonelabs.com
- **Installez un „antispyware“,** de préférence deux pour une meilleure performance. Nous vous conseillons „**Spybot Search & Destroy**“ et „**Ad Aware**“. www.safer-networking.org/fr/download et www.lavasoft.com
- **Téléchargez régulièrement** les mises à jour (**updates / patches**) de **MICROSOFT®,** mais aussi de **MAC®** et **de LINUX®** (nul n'est parfait) ! Ceci est un „**must**“, contrairement à ce que la plupart des gens croient !
- **N'ouvrez jamais** de courrier électronique de personnes inconnues et surtout pas les pièces jointes (attachments) !
- **Ne répondez jamais** à des courriers électroniques venant d'institutions bancaires, **eBay** et d'autres institutions. Il y a danger de „**phishing**“, appelé encore „**hameçonnage par courrier électronique**“ !
- **Installez une barre antisphishing.** www.spoofstick.com

Restez informé sur les dernières informations de sécurité, soit par abonnement à des Newsletter (**www.internetmonitor.lu**) et/ou en lisant des magazines PC !

En respectant ces quelques règles mentionnées ci-dessus vous pouvez surfer en toute tranquillité ! Veuillez remarquer quand même qu'une sécurité à 100% n'existe pas et est illusoire ! Le maillon le plus faible est et restera toujours l'être humain (nul n'est parfait) !

Gust MEES / Formateur pédagogique TIC http://www.internetmonitor.lu Partenaire officiel de CASES http://www.cases.lu

SÉCURITÉ

VEUILLEZ DÉCOUPER ICI