



## **Internet** Les 10 règles d'or pour surfer sans danger

**Impossible de naviguer sur la Toile  
aujourd'hui sans firewall et antivirus!**

### **Règle 1:**

Mettre à jour très régulièrement son antivirus (certains éditeurs adaptent leur virus toutes les trois heures), en optant, au besoin, pour un update automatique. De même, les versions obsolètes de système d'exploitation (Windows 98 par exemple) résistent moins bien aux agressions.

### **Règle 2:**

Les attaques ciblent le plus grand nombre d'utilisateurs: les produits Microsoft sont donc plus visés. Les risques sont plus limités lorsqu'on utilise un navigateur gratuit comme Firefox ou qu'on travaille sur Apple.

### **Règle 3:**

En cas de doute sur la provenance, avant d'ouvrir un fichier ou des images stockées sur un CD, un DVD ou une clé USB, analysez-les.

### **Règle 4:**

Sous Windows, évitez de surfer sous le compte administrateur (créez un compte avec des droits restreints). Les virus auront ainsi plus de mal à s'installer et à activer d'autres logiciels. De plus, si un pirate prend le contrôle de votre ordinateur et que vous êtes en mode d'administration, il pourra effectuer toutes modifications au même titre que vous.

### **Règle 5:**

Configurez votre firewall et antivirus de manière à ce que le système ne soit pas trop ralenti. Mais ne les réglez pas au degré minimal (et, bien sûr, ne les débranchez pas).

**Règle 6:**

**Ne répondez pas aux messages d'inconnus, d'autant plus si l'on vous demande des données personnelles.**

**Règle 7:**

**Lorsque vous envoyez des e-mails à plusieurs destinataires, choisissez l'option «copie cachée» pour les adresses.**

**Règle 8:**

**Créez une adresse e-mail différente que vous pourrez facilement abandonner si vous fréquentez des forums de discussion.**

**Règle 9:**

**Ne communiquez jamais vos données bancaires dans un e-mail, comme le demandent certains hôtels. Pour ce genre d'informations, passez par un serveur sécurisé (avec la mention «https» dans l'adresse) ou par téléphone.**

**Règle 10:**

**Si vous envoyez des fichiers sensibles pas mail, compressez-les (par zip, par exemple) et bloquez-les par un mot de passe que vous enverrez par message séparé.**

**Huma Khamis**