Polizia di Stato

Personal computer

Use a good antivirus software: any computer connected to the Internet has to be provided with such an application. It is also important to keep it updated.

Use a firewall: it could seem too much but the use of filtering applications as firewalls, provided they are adequately configured, can ensure fair protection against certain types of attacks and especially against other preparatory activities (such as for example TCO & UDP port scanning) attackers use to carry out before attempting an unauthorized access.

Install the latest security patches (that is, changes applied to a software to fix problems met by web developers or users): this refers both to the operational system and software.

Watch out for any suspicious malfunctioning of the operating system: it is advisable to be suspicious of any inexplicable malfunctioning of the operating system and try to identify the causes, if possible, by means of ad hoc tools.

Disable Java, Javascript and ActiveX:these technologies could really be a thorn in your side when surfing the Internet; as an alternative to make netsurfing less frustrating, it is possible to partially protect your PC using ad hoc tools which work as filters for interactive contents or surf the web through an anonymous proxy server.

It is advisable to use a computer dedicated to web surfing exclusively, not containing important data. If this is not possible, as is often the case, it is necessary to configure your computer accurately in order to avoid possible risks.

If you connect your PC to the Internet without adequate protection, you could havestrangers poking around in your data, both stored or shared.

It is advisable to use a limited account (inhibiting system settings change or software installation) especially when surfing the web: in this way any virus infecting your PC through any browser vulnerability could do little or no harm.

Perform regular backup of all sensitive data: it is also important to keep your data backups safe.

24/03/2011