www.pc-st.com

PC SECURITY TEST 2007

10 ESSENTIAL TIPS
TO SECURE YOUR PERSONAL COMPUTER

JUNE 2007

FOREWORD

This document is a compilation of essential tips to help users secure their personal computers. We do not claim that is exhaustive, or that it guarantees perfect security. It does, however, allow users to protect themselves against the primary risks of personal computer use. Please note that these tips were put together for personal, not professional, users. This document is obviously insufficient for a company, which deals with increased information flow and systemic complexity, and well as a greater number of users. It does not replace expert advice.

1. INFORM YOURSELF

Knowing what the risks are, what they do, and what solutions exist is already half the battle. There are many magazines, websites, and forums, for every level of technical experience, on the subject of computer security.

What do you need to know? What a virus is, what spyware is, what constitutes an attack. Know the way they work. Know the basic solutions, like antivirus and antispyware software, real-time protection, and firewalls. Know what they can do and, more importantly, know what they can't.

If possible, keep up to date with the evolution of new threats. Subscribe to a magazine or newsletter.

2. KNOW AND AVOID RISKY SITUATIONS

Be aware of risky computer behaviors—such as opening attachments, downloading files from unknown websites, and installing software of whose function you're unsure—and avoid them.

3. INSTALL GOOD ANTIVIRUS SOFTWARE

Choose and install a good antivirus program. Get to know how it works so you can get the most out of it while being mindful of its limits.

4. INSTALL GOOD ANTISPYWARE SOFTWARE

Choose and install a good antispyware program, or at least a spyware scanner. In the latter case, you must of course scan your computer regularly. Better still, install a real-time antispyware program, which automatically blocks spyware from installing itself onto your computer.

5. INSTALL A REAL-TIME SHIELD

The majority of antivirus programs are based on scanners that recognize viruses by signature. Although reliable, this procedure presents a significant drawback: it does not detect unreferenced viruses (new viruses or variants of known viruses). You should, therefore, install a real-time shield that protects vital system resources and detects all suspicious activity, such as registry access, deletion of system files, and the sending of mass emails.

6. INSTALL AND CONFIGURE A FIREWALL

A firewall monitors the flow of information between your computer and the network. It is an essential defensive element that protects against intrusions and malware (harmful software) that infects your computer through open ports.

7. TAKE THE TIME TO BACK UP YOUR DOCUMENTS

Even though it's a pain, you should take the time to make copies of your important documents. At the very least, back up your work files (Word and Excel documents, emails, address books, favorites, etc) on a USB key, an external harddrive or a CD or DVD. Better yet, make a copy of your entire disk with a special program. Your files are certainly worth much more than the price of whatever you back them up with and the fifteen minutes it'll take you to use it.

8. BE VERY CAREFUL WHEN USING PUBLIC COMPUTERS

If you have to use a public computer when moving, staying in a hotel, browsing in an internet cafe, or vacationing, take extra care. By "public computer," we mean a computer that is freely accessible to many different people. At all costs, avoid using these computers for anything personal or financial, such as logging onto your bank account online, or entering an important password (for an email account, software, a business extranet, etc). Even if the organization providing the computer is completely trustworthy, the people who use it after you may not be. If for some reason you have to enter a password on a public computer, we advise you to change it immediately afterwards from your own computer (or one that you trust).

9. CHOOSE GOOD PASSWORDS AND KEEP THEM SECRET

- Avoid passwords that are obvious or too short.
- Avoid keeping your password on a piece of paper on the screen or under the keyboard (!)
- Avoid keeping your password in a file on your computer.
- Avoid saving your password. Even if it is encrypted, there are many free tools that can recover it.
- Avoid using the same password for different accounts.

10. BE CRITICAL

When faced by a security alert, or an email that asks to you act immediately, be critical. Take the time to verify the source of the email and confirm its veracity. Never forget that, in computer security, the weakest link is the user himself, who often opens the door for the pirate.

In creating this document, we have tried to cover the essentials
in such a way as to be accessible to the greatest number of users.
This document was created in collaboration with computer security experts,
technicians who cope with these problems every day and assist users of all levels.
If you have a suggestion, a criticism, or a proposed addition, please don't hesitate to contact us at support@pc-st.com