GAMA Electronics bitsyu.net INTERNET PROVIDER
Mišarska 11, 11000 Belgrade Phone: +381 11 323 94 94 Fax: +381 11 322 72 81 Email: prodaja@bitsyu.net http://www.bitsyu.net
CRN: 7489706 Activity Code: 64200 VAT: 100290617 VAT No.: 128976171
Account Numbers: 160-92368-04 Banca Intesa, 180-0150660101000-90 Alpha Bank AD

# Internet Security

Although there is no such thing as absolute Internet security, there are some basic security mechanisms that can significantly reduce the potential risk.

Since most users have Windows installed, special attention will be dedicated to protecting Windows operating systems.

In order to protect your computer from malicious software, you are encouraged to:

1. Install antivirus software on your computer.
   Make sure that you choose a reliable antivirus program, able to protect your computer from malicious programs such as viruses, trojans, spyware, and other malicious software installed without your knowledge. Viruses are easily spread via e-mail messages and through exchange of programs with other people. These programs can delete or modify important data on your computer and even delete the entire contents of your hard disk. After you install an antivirus program, remember to also update virus definitions. Otherwise, your computer will be as vulnerable as before.
   **Note: Users of our ADSL service (private entities only) are granted a free license for Kaspersky AV Personal 2009.**
2. Take necessary precautions when opening email messages with unknown sender, especially if the message contains an attachment. Remember to scan every email attachment with the updated version of antivirus software.
3. If you don't have a hardware firewall, install a reliable network firewall on your computer or at least enable your default OS firewall.
   If your firewall is running when you're online, it will monitor and block the flow of data between the Internet and your computer in case it detects unauthorized access to computer. Firewall prevents and informs you abut any such attempts.
4. Get the latest updates and security patches available for your computer's operating system via Windows Update.
5. Microsoft Networks and File and Printer Sharing (Control Panel – Networks) can allow misuse of data located on your computer.
   If you have no need for sharing files over a network, delete Microsoft Networks and File and Printer Sharing. Exercise extreme caution if you want to enable file sharing over your network, especially if you are connected to the Internet.

### Tips for selecting a password

We strongly encourage you to change your password (for logging into the system, email, etc.) relatively often, for example once in every few weeks.

Examples:

| Bad example | Good example |
|---|---|
| pera | peRa14* |
| dunja1 | xd-01cf4 |
| miticp | goOd_One |

Of course, as these passwords are made public, they no longer present a good example.

**Malware removal guide**

Since malware writers constantly improve techniques to evade detection and expand methods to spread malicious programs, the following list of malware removal tools and methods is by no means complete.

If, despite all precautions, malware is installed on your computer, we suggest that you perform the following actions on all computers in network:

Run an antivirus program to check your computer. Remember to check both "c:" partition and other local and removable drives.

Additional checks can be made online via the following antivirus programs:

* http://www.kaspersky.com/kos/eng/partner/default/pages/default/check.html?n=1256923421050
* http://security.symantec.com/sscv6/WelcomePage.asp

Then, check your computer(s) for adware/Trojans:

* Spybot-S&D – http://www.safer-networking.org/en/mirrors/index.html
  (update to latest version before you run the program)
* Malwarebytes– http://www.malwarebytes.org, free version & update
* ComboFix – http://download.bleepingcomputer.com/sUBs/ComboFix.exe and
  http://www.bleepingcomputer.com/combofix/how-to-use-combofix – guide

Sort files by date in c:\windows, c:\windows\system32 and c:\windows\system32\drivers and look for any .dll and .exe files with a recent date and/or an unusual name. Then go to www.google.com and look up all suspicious program/file names. Read user comments about suspicious files in order to identify them as possible viruses or Trojans. Finally, upload said files to a free online scan service (such as VirSCAN at http://virscan.org) to check them for malware.

Make sure to change all your passwords for online services you use.

Run occasionally start – run – cmd:

* In console, type netstat -o.

Entering this command should get you a result similar to this:

Active Connections

| Proto | Local Address | Foreign Address | State | PID |
|---|---|---|---|---|
| TCP | 127.0.0.1:1890 | 127.0.0.1:1891 | ESTABLISHED | 3160 |
| TCP | 127.0.0.1:1891 | 127.0.0.1:1890 | ESTABLISHED | 3160 |

...

If there is ": 25" (or "SMTP") under the Foreign Address column, this indicates that the computer sends email messages without your knowledge. Last column (PID) indicates the process (program) responsible.

Use the command "tasklist/svc" to see list of services running in process. This way you can easily determine which PID (program) is infected. If the PID is 0 or 4, the virus is located in the boot sector and can only be cleaned if you boot the system from the installation CD. Boot sector virus is usually located in c: windowssystem32drivers estocudno.sys and must be cleaned manually.

Perform a WLAN environment check for the possibility of a virus in a wireless newtork with an infected computer.