UnwiredOnline - Protecting Your Computer

Introduction
As the millions of personal computers of the world move from dial-up lines to permanent connections such as DSL, cable, or wireless broadband, a vast new array of potentially targets turn up on the Internet, at static IP addresses, for hackers to use, sometimes for fun, and sometimes to stage further break-ins.

Why should I care about security?
Your computer is on the Internet. Others on the Internet, anywhere in the world can try to access your machine. This is no different to being with any ISP, but with broadband, there are few major differences:

- Your computer is connected via a high speed link
- Many of us stay connected 24 hours a day
- Most broadband users are online whenever their computer is on

This makes these machines more interesting to hackers and therefore more vulnerable. The chances of someone snooping undetected around your hard disk if you are connected with a 56k modem are simply lower. Also, home or office networks can transfer viruses or worms via the network very quickly.

Good Practices
Nearly every version of Windows, by default, is horrendously insecure. Turn off File and Print sharing! Too many broadband users out there have their hard disks publicly exposed for all to see. Turn off Personal Web Sharing! It's a security breach waiting to happen.

There are a number of good security practices available that users can implement to provide better security protection on their computers. We have listed some good security practices below:

- **Email Attachment**
  Never open any executable attachment or script received by email unless you are very sure of its original and are convinced the originator has excellent virus/Trojan protection in place. (Don't even preview it in Outlook; turn the preview pane feature of Outlook off).

- **File and Printer Sharing**
  - Disable file and printer sharing, especially on PCs with open Internet access.
  - If you must have file and printer sharing on your home or office network, be sure to have passwords on your shared resources and only give write permissions when necessary rather than the default full control.

- **Install Antivirus Software to prevent Virus, Trojan and Worm attack**
  - Install antivirus software and keep it up to date. Scan email attachments before opening
  - MS Office: Switch on Word/Excel 97 Macro virus protection (Tools/Options/General/Macro virus protection) or run Word/Excel 2000/2002 with at least medium security settings. This will ensure the user is presented with a dialog box when documents containing macros are opened. If suspect Word documents are received by email, open them in Wordpad rather than Word, since macros won't be understood by Wordpad. Set the file-permissions of "normal.dot" to read only, to prevent viruses or Trojans from infecting your Word setup. If possible, configure your browser to ignore ActiveX and prompt when Java or Jscript or VBscript is run.
  - Don't stay connected to the network unless you need to
  - Switch off machines when they are not in use.
  - Back up your system regularly.

- **Keep up-to-date on security fixes for your operating system and programs**
  - If your computer runs Windows, you should frequently check the Microsoft Windows Update page at http://windowsupdate.microsoft.com/
  - If you have Office 2000 (Word, Excel, etc.), you should periodically check the Microsoft Office Update site at http://officeupdate.microsoft.com/
  - For Windows security in general, you'll find detailed information at the Microsoft Security & Privacy site at http://www.microsoft.com/security/protect
  - For Macintosh computers, a good source of security information and solutions can be found at MacInTouch Security Resources at http://www.macintouch.com/security.html

- **Install firewall software to prevent attacks from being successful**
  Installing a software firewall like ZoneAlarm is a good idea, and a hardware barrier of some kind is even better. But whatever you do, don't ignore the problem. Computer security is a very real threat for broadband users.
  - **ZoneAlarm**
    ZoneAlarm is a pretty good personal firewall, which places an emphasis on programs attempting to connect to the Internet without your permission. Best of all, it is free for personal and non-profit use. Grab your copy here: http://www.zonealarm.com/
  - **Norton Personal Firewall**
    Norton Personal Firewall is a firewall by utilities vendor Symantec. Norton Internet Security can also block banner and popup ads, as well as Flash and Java applets. Expect to pay commercial software prices. More information here: http://www.symantec.com/sabu/nis/npf
  - **Tiny Personal Firewall**
    Another good firewall product is Tiny Personal Firewall, a personal firewall made by the creator of the WinRoute software routing solution. Check it out here: http://www.tinysoftware.com

Conclusion

High-speed, always-on Internet connections have changed the way we communicate around the world, but they open our computers up to malicious attacks much more so than slower dialup connections. By following some basic procedures, you can minimize the damage or inconveniences caused by these attacks. Be sure to protect your computer and yourself.

At Unwired, we will be on the lookout for suspicious virus-like or worm-like activity coming from computers on our high-speed network. It is the responsibility of our customers to make sure their computers are protected and fixed in the case of an infection. In the event that we detect this type of activity, you will be notified by us that you may have a problem that needs immediate attention. In order to protect our network and others who use our service, it may become necessary to temporarily suspend Internet service to your computer until the problem is resolved. Thank you for your understanding and your continued business.