



Network Advocates, Inc.
9001 Shelbyville Road
Burhans Hall, Suite 260
Louisville, KY 40222-8038
Phone (502) 412-1050
Toll Free (877) 412-1050
Fax (502) 412-1058
www.networkadvocates.com

Seven Essential Security Tips

- *Regularly download security patches.* For Microsoft software this is absolutely critical – at least once per month. Open your Browser and from the top Menu Bar select “Tools”. From this drop-down Menu select “Windows Update”. You will then be connected to a Microsoft website that will walk you through downloading the necessary System Updates and Security Patches. There is no charge for any Update or Patch. If you don’t patch -- **YOU ARE VULNERABLE!**
- *Use strong passwords.* Choose passwords that are difficult or impossible to guess. Give different passwords to all accounts. Use something like this:

Mnh10c!..... [My name has 10 characters!]

The above password example uses a mix of upper and lower case letters, along with numbers and a symbol. Using a phrase to help you remember it provides a very effective password.

- *Make regular backups of critical data.* Backups must be made at least once each day. At least once a month the backup media should be verified. Rotate backup media so you have multiple backup copies of the past. (Monday, Tuesday, Wednesday, Thursday + one disk/tape that is used one time and then stored offsite for at least 6 months before re-using.)
- *Use virus protection software.* That means three things: having it on your computer in the first place, checking daily for new virus signature updates, and then actually scanning all the files on your computer periodically. Check your settings at least once per month to make sure your antiVirus is staying up-to-date.
- *Use a firewall as a gatekeeper between your computer and the Internet.* Firewalls are essential for those who keep their computers online with DSL or cable modem connections but they are also valuable for those who dial in. If you use a dial-up connection to the Internet, a software firewall is sufficient. For those with a dedicated connection, such as DSL or Cable modem, you should invest in a hardware firewall which generally costs \$300 to \$600; software firewalls are under \$100.
- *Do not fall for “phishing” eMails.* Identity thieves are creating eMails and fake websites that are nearly identical to your bank, credit card company, PayPal, etc. Be suspicious of any eMail that asks you to “follow the link” and “update” or enter personal information. Always open a new browser, and login to the desired site on your own, rather than clicking a link in the eMail. Notify the institution mentioned in an eMail if you’re suspicious.
- *Do not open eMail attachments,* regardless of how enticing the Subject Line or attachment may be. Be **especially** suspicious of any unexpected eMail attachment from someone you **do** know because it may have been sent without that person's knowledge from an infected machine. If you don't know exactly what the attachment is, and that the person meant to send it to you ---- **DON'T OPEN IT!!!**

Know your eMail is safe before you open it. Use VirusGard™ eMail Service.
www.virusgard.com

