IN THIS ISSUE:
~ Quick Tips (Security)

COMING NEXT MONTH:
~ MS Word Tips and Tricks

READY NET GO … NEWS

May 2004 **http://www.readynetgo.net** **610-856-0990**

Tip of the Month

"Bytes" of Computer Info

- **1 bit** = 1 or 0

  (the smallest unit of data)

- **8 bits** = 1 Byte

  (typically 1 character of data)

- **1 kilobyte** (KB, kb) = 1,024 Bytes

  (most computer file sizes are listed in KB's)

- **1 megabyte** (MB,mb) = 1,024 KB or 1,048,576 bytes

  (~ 600 page paperback = 1 MB)

- **1 gigabyte** (GB) = 1,024 MB

  (1,024 paperbacks or the entire No. American phone directory)

- **1 terabyte** (TB) = 1,024 GB or 1,099,511,627,776 Bytes –

  (The entire Library of Congress is estimated at 64 Terabytes)

- **1 petabyte** = 1,024 terabytes

  (1 petabyte = approximately 20 million 4 drawer filing cabinets full of text.)

- **1 exabyte** = 1,024 petabytes

  (1/5 of an exabyte = total printed material in world; **OR**

  5 exabytes would be equal to all of the words ever spoken by mankind)

Security Tips

Here's a rundown on how you can keep your computers running smoothly and stay ahead of the security curve:

- **First and foremost, install anti-virus and anti-spyware software on all computers connected to the Internet and update these programs regularly.** Quite often a virus will start in a business because someone inadvertently saved a document to a disk at home, brought it into the office and connected to the network. Make sure everyone in the office understands the importance of anti-virus software and safe computing practices (like scanning external disks before opening any files).

- **Use a hardware or software firewall to prevent outsider's unauthorized access.**

- Remind all computer users to only **open expected email attachments** and to never open attachments with extensions like .exe, .vbs, and .scr even if the email comes from someone you know. If you did not specifically request an attachment, be safe and delete it before opening.

WWW (Websites Worth Watching)

1. http://198.6.95.31/sbsavg.asp – Going on a trip this summer? Check out this AAA site for retail gasoline prices by U.S. State
2. www.fuelcostcalculator.com – Another AAA site to estimate the cost of fuel for a road trip. Enter start city, destination, and miles per gallon to get the estimated cost of a one-way or round trip journey.
3. www.gasbuddy.com – Need specific info on gas prices at a particular gas station around the U.S.? Search this site and find the best deal …
4. http://donotcall.gov – Official site of the National Do Not Call Registry to remove your telephone and cell phone #'s from telemarketing lists.
   You can also call: 1-888-382-1222

The importance of these first three tips cannot be stressed strongly enough. In addition, encourage users to:

- Use the **Windows Update** feature found in Windows XP and 2000. You can set this program to auto download and notify the user when updates are ready to install. **Critical updates** and **security updates** are the most important as these will patch "holes" in the software's code; a hole in which a hacker or virus could gain access to your computer. As Microsoft gains more and more attention, it is very important to patch your system as the updates become available. For instance, Microsoft released a patch in April that prevented the recent <u>Sasser Worm</u> from overtaking Windows XP and 2000 machines. Computers that had the update installed prior to the outbreak were not affected.

- Use secure passwords on all computers. **DO NOT:** use common names; your birth date or other personal identification names or numbers; or use passwords less than 7 characters. **DO:** use a mix of uppercase and lowercase letters, numbers and characters and use long passwords (over 7 characters). The longer and more cryptic the password is, the harder it is to guess. Password cracking programs are easy to come by and it's one of the first things that hackers use to gain access to computers. <u>Try this:</u> Think of a sentence or phrase and use the first letter of each word as your password. **Ex:** TBoNTBTitQ translates as "To Be or Not To Be, That is the Question"

- Since Microsoft isn't the most popular kid on the block, MS software is still going to be a major target for disruption. Consider switching browser's if you primarily use Internet Explorer. Although **Internet Explorer 6.0** is becoming more secure, it won't have an embedded pop-up blocker until the next service pack (sp 2) comes out (sometime this summer). **Netscape 7.1**, meanwhile, already has a pop-up blocker and many more security features available. Bottom line: consider switching to a browser like, Netscape, Mozilla, or Opera (free with banner ads, $40 for no-ads). Each browser has its own style, so try them all out for a period of time before relying on just one. Keep in mind, though, that certain functions require the use of IE, such as Outlook Web Access (OWA). You will still need to use IE periodically if these functions are important.

- **Manage cookies**. Some cookies are beneficial; they remember information about you so that internet browsing can be quick and convenient. For instance, many websites like Amazon.com have a 1 click ordering system to save time during checkout. Simply enter your information in once and the next time you visit, Amazon remembers who you are and all of the information it needs in order to process your new order. All of this is done with a cookie. Other cookies could be malicious like some adware (see April 2004 newsletter). Since cookies track your information, they could be used to track your online activities for less than honest purposes. When it comes to cookies, the old adage still stands – When in doubt, throw it out!

- Delete files from the **temporary Internet folder** regularly. Whenever you visit a webpage, certain images are downloaded to your computer automatically. Cleaning up these files will not only clear out any pop-up ad images, it will also help reduce the used space on the hard drive.

- **USB flash drives** are a quick, convenient way to store data. But due to their small size, they are very easy to misplace. If you keep sensitive data on the USB drive, consider password protecting the files so that if the drive is lost or stolen, the party who finds it cannot access your sensitive data.