IN THIS ISSUE:
~ Secure Your PC

COMING NEXT MONTH:
~ Security Cameras

READY NET GO … NEWS

March 2008 **http://www.readynetgo.net** **610-856-0990**

Tip of the Month

Q: Having trouble sending large attachments through your email client?

A: Use an **online file transfer** service

If you've ever tried to attach a 5MB file to an email only to see it bounce back to your Inbox, you know how frustrating that can be.

Email attachments are limited for both size and file type for a reason. ISP (Internet Service Provider) servers process millions of bytes of data every minute. To reduce the possibility of the servers crashing, ISP's put a limit on the amount of data that can be sent from each company / individual. Likewise, network administrators may limit the size of attachments due to bandwidth limitations.

If you have trouble sending a large attachment through your email program, use an online file transfer service such as:

- *send*space - www.sendspace.com
  or
- Media Fire - www.mediafire.com

These sites allow anyone to upload a file on their computer to the company's servers. A link is then generated to the file and sent via email. The recipient clicks the link and downloads the file.

You can send files up to 300 MB (sendspace) or 100MB (media fire) for free and you do not need to register to use the service (unless you want to track and organize the files you upload and access them from any computer). Online file transfer services make sending large files quick and easy!

Protecting your PC

How to Secure your PC Against Infiltrations

Times are tough! We get calls everyday from people whose PCs have been infected with spyware, viruses or are deluged with SPAM. The problem is not going away and fortunately, there are several things that can be done that will help prevent infections and lessen the downtime associated with infiltrations. In this newsletter, we'll revisit some of the most important tips for securing your PC.

Email / SPAM

Where would we be without email?! Although it's quick and convenient, it can also be frustrating given the deluge of spam that we all receive. Fortunately, there are ways to combat SPAM and limit the chance of infiltrations.

TIPS: (for more tips, check out our **October 2006** issue)

1) Use a **free email address** or **create sub accounts** through your ISP (such as Verizon) for online purchasing, product inquiries, online surveys and questionable contacts. Yahoo and Gmail offer free email accounts that have excellent SPAM filtering built-in. Verizon DSL allows you to create up to 8 sub-accounts while Comcast cable offers up to 6. If SPAM becomes a problem with one of your addresses, simply delete the account and create a new one. Use your primary account only for friends & family.

2) For Outlook users, if the Junk E-mail filter isn't catching all of the SPAM, use a **third party anti-spam software program** to segregate your spam emails from your legitimate ones. Hardware appliances are also an option – we are currently testing an appliance specifically geared to catch spam. The device sits on the outside of the network and groups suspect emails together for review by each user.

WWW (Websites Worth Watching)

1) www.mygreenelectronics.org – Type in your zip code to find local recycling centers for electronic goods.

2) www.call2recycle.org – Recycle your rechargeable batteries & cell phones at retailers like Lowes, Home Depot, Sears, Office Depot, Radio Shack and more. Visit the website for specific locations.

If you need assistance with SPAM filtering, call us for specific options suitable for your situation.

3) Be wary of attachments in email even if it's from someone you know. Run the file through a virus checker before opening; even common .doc files can have a macro-based virus looming within.

Malware (viruses, Trojan horses, worms, adware)

In November 2007, it was reported that certain Google searches resulted in malicious websites appearing in the search results. If you clicked on any of these links, your computer would be infected if you didn't have the appropriate software patches installed on your PC. The intent was to deliver malware to a large number of unsuspecting people through a common avenue – searching the Internet. This hole has since been blocked but other holes may appear in the future.

TIPS:

1) Be careful when using search engines such as Google. When the results are displayed, pay attention to the address link BEFORE you click it. If it looks cryptic rather than an identifiable domain name, don't click on it (malicious example: http://luewusxrijke.cn/769.html)
2) Make sure your anti-virus software and firewall have the most recent updates. **DON'T** install multiple anti-virus and firewall products – you'll run into headaches. You **CAN** install multiple versions of anti-spyware products though, like the two free options, Spybot Search & Destroy and Lavasoft's Ad-aware. You'll find that all of the **anti-spyware software** products will catch different adware so **run many** and **run them often**.
3) Think you have a virus? Scan your PC using the free tool at http://housecall.trendmicro.com/
4) Since many email links are actually false, **don't click links in an email**. Type the address in a browser directly. It's an extra step but can prevent malware from being installed on your computer.
5) Create and use **strong passwords** (e.g., Run&tag6 or Free8wiLLy). If your password is in a dictionary, a proper name, or an identifiable number like your birthday, it will be figured out. Keep your list of passwords in a secure location or in a password protected file. Setup **parental controls on PCs** your children and teenagers use (especially teenagers!)

Downloaded software

One of the ways in which people receive malware is by **installing a product** that comes bundled with other software. Oftentimes, you aren't aware of this practice unless you read the End User License Agreement (EULA). Advertising is big business and many companies will sell the right for other company's to piggyback on their software so they can make additional profits. Some companies don't care what the additional software is so you have to be vigilant. **Read EULA's** for all software whether downloaded or purchased at a retail store. During the installation, if you are asked to download a piece of software that you aren't expecting, click NO.

Hundreds of security issues crop up each month; some are shared with the public and others are kept quiet especially if there is no quick fix. Make sure that you set your computer to receive Microsoft Windows' **Automatic Updates** automatically to ensure that your Operating System is protected. In addition, installed software is also vulnerable and serves as an avenue into your PC. Periodically check to see if the manufacturer of your installed software has released updates. Older software tends to have more bugs in the code so consider upgrading to the latest version if the software connects to the Internet such as FTP programs, financial applications, and security suites.

Programs to check for upgrades regularly:

Any product from Microsoft, HP, Symantec, McAfee, Adobe, WinZip