IN THIS ISSUE:
~ Protecting Your Computers

COMING NEXT MONTH:
~ Network Printers

READY NET GO … NEWS

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

Tip of the Month

Cookies, advertisements, pop-ups, pop-unders … the World Wide Web can be pretty frustrating at times with all the unwanted information that's thrown at us. Marketers are constantly looking for new ways to grab our attention. If you are looking for an out, here are some tried and true tips:

1) Install an ad blocking software such as Ad-aware (www.lavasoftusa.com). This program will scan your drives for spyware and either quarantine or delete the files.

2) If you are a fan of instant messenging – **STOP NOW**, but if you must, remember that marketers crawl through chat rooms looking for email addresses to add to their coffers. Use an email address you don't mind deleting if your inbox gets too bogged down – or consider modifying your email address to prevent unwanted solicitations.

3) Vary your passwords and change them often – every 3 months or so. The ideal is to create cryptic passwords; those having a series of letters, numbers & characters. Avoid using common words or phrases or identifiable numbers like your birthday.

Viruses, Worms, Trojans … Oh My!

Thousands of viruses, worms, and Trojan horses are discovered every day – some are severe affecting millions of computers, others are merely annoyances that only a few people will encounter. There is currently no end in sight to the business of hacking so for the New Year, be prepared by being proactive in protecting your computer equipment.

Viruses, worms, and Trojan horses have increased in numbers over the past few years due to the following reasons:

1) an increased number of broadband users (which has allowed code to move faster from computer to computer)
2) the proliferation of code available on hacker websites, and
3) the simple fact that there are more people using computers now than there were 5 years ago.

Many people don't think about maintenance when it comes to computers. In order to lessen the chance of your computer(s) being infected, heed the advice of security experts:

1) Install anti-virus software on all computers (PCs and servers) and ensure it is updated regularly
2) Install a firewall (hardware preferably)
3) Monitor your employee's online and email activities carefully

WWW (Websites Worth Watching)

1. www.virusbtn.com/ - Virus Bulletin; independent anti-virus advice

2. www.icsalabs.com - Offers information on security and certification; tests almost all anti-virus software

3. www.trendmicro.com – Excellent anti-virus software application. Highly recommended for business use.

Virus Protection

To find past newsletter issues, go to: http://www.readynetgo.net/newsletters

Install Anti-Virus Software

There are many anti-virus software options available today and nearly all do an excellent job at detecting uninvited code. Some of the major anti-virus software manufacturers are Trend Micro (recommended), Symantec, McAfee, Panda, and Computer Associates. All offer support for their products – some offer free email or phone support. Products like Trend Micro also provide spam filtering while other products offer utilities like Internet Firewalls.

TIP: In addition to updating your anti-virus software, also update your operating system. Microsoft's Windows Update site will automatically scan your computer and suggest critical updates as well as non-critical updates. You can pick and choose which updates to install. Many offer an uninstall feature so if problems arise, you can remove the update. Since Microsoft releases updates every month, plan on downloading your Windows updates along with your virus definitions regularly.

Install a Firewall

A firewall acts as a door to your computer or network. Without the appropriate key, outsiders have limited access. In a business environment, it is important to install a hardware firewall and supplement with software firewalls if desired. Two popular and reliable software firewall programs are ZoneAlarm and BlackIce Defender. You can adjust settings to be either very restrictive or open depending on your comfort and usage level. A hardware firewall is an actual appliance or piece of equipment that you connect between your network and router. The hardware firewall filters all incoming and outgoing data. Settings allow you to be restrictive or open according to your needs just like software firewalls.

TIP: If you have cable or DSL for your home Internet connection, you should also have a router installed. Most cable/DSL routers have built in firewalls. By default, these routers/firewalls are set to not allow traffic in from the outside. If you use a dial-up connection at home, you will only need a software firewall. Remember: Software firewalls are good for home use while hardware firewalls are better equipped for networks (business or home).

Monitor Your Activities Carefully

Be mindful of the websites you visit, don't give out personal information on insecure sites, and look at the web address to make sure you are on the site you want to be. Websites, in addition to email, can be a source for hackers to download code to your computer. By simply visiting a site, code can be transferred to your computer, which could enable access to your personal files and even prevent you from gaining access (by changing system passwords). Common sense is extremely important when surfing the web these days. Most sites are reputable and the Internet affords a wealth of information. Just be careful – if a site seems suspicious, find the information elsewhere.

One final point: If a screen popus up on your monitor unexpectedly, read the information displayed and DO NOT hit Download or Install unless you know what will happen.
Remember – When in doubt, click Cancel.

◆ **Remember** ◆
Backup your computer regularly &
keep your anti-virus software up-to-date

Happy New Year from Ready Net Go