IN THIS ISSUE:
~ Virus Hoaxes

COMING NEXT MONTH:
~ The Scoop on PDA's

ReadyNetGo .... News

November 2002 **http://www.readynetgo.net**

TIP(s) OF THE MONTH

Web Browsing Tip #1

If you use Internet Explorer as your web browser and you get to a site which won't let you use the back button to access a previously viewed page, click the **arrow** on the Back button. A drop down list will appear and you can choose the exact page you want to re-visit.

Web Browsing Tip #2

When you use a search engine such as Google to locate websites, you can **right** click on a link and choose to open the page in a new window. This way if you click on many links and want to get back to the original search query, all you have to do is click on the original link on your task bar. This will significantly speed up your searching!

Web Browsing Tip #3

You've undoubtedly come across those "The Page Cannot Be Displayed" messages while clicking on a link or typing in a website address while surfing. If you click on a link and this page appears, before closing the window click on the **Refresh** button. If a page is slow to load it may get hung up temporarily. If the refresh button doesn't work and you know the site is active, try again at a later time. Interference and/or site maintenance could be limiting access.

Be Aware of Virus Hoaxes

Computer viruses are rampant nowadays. If that's not enough, you also have to worry about virus hoaxes – email messages that warn of a virus but have no legitimate cause for concern. These hoaxes can arguably do as much damage by inciting mass hysteria, clogging email servers, and decreasing worker productivity. Fortunately, there are some things you can do to figure out if a virus is a real threat or just another addition to your spam list.

The three major anti-virus software manufacturers have information on their site that lists the most prevalent hoax topics. To access this information, go to:

Symantec www.symantec.com/avcenter/hoax.html

Mcafee vil.mcafee.com/hoax.asp

CA www.ca.com/virusinfo
(Computer Associates)

Each site lists the name of the hoax and detailed information of its contents. If you are ever unsure of an email, check all three sites as your particular hoax may not be listed on every manufacturer's site.

(continued on back)

WWW (Websites Worth Watching)

1. www.holidays.net/thanksgiving - History, goodies, crafts and decorating ideas for this festive holiday.
2. www.thanksgivingrecipe.com - Food, food, and more food ....
3. www.thehungersite.com - Click a button to give food to those who need it around the world.
4. www.giveforchange.com - Online donation site with many matching grant opportunities. Double your donation today!

Tips on how to identify virus hoaxes:

1. Beware of claims that a virus is undetectable. In general, if you keep your antivirus software up-to-date, your system will detect the latest viruses.
2. Look at the subject line carefully. If the email message's subject line includes words such as "Urgent", "Warning", or even "Virus Alert", it's often a good indication that it will be a hoax.
3. Check the sources listed in the email message. Many hoaxes will quote a well known company such as Microsoft, the Federal Communications Commission (FCC), or an antivirus company. Go to the website listed and check to make sure that the information is legitimate.
4. Read the message entirely before deleting any files. Although thousands of viruses are written each month, only a handful will be cause for concern. By the time a virus reaches you (if your antivirus software doesn't catch it first), there will probably be a fix or patch on one of the antivirus websites. Except in rare cases, you should not have to delete files manually. If an email message insists that you delete files manually, this should raise a red flag.
5. Another red flag is when a virus alert urges you to tell everyone you know. Genuine alerts never do. If you're unsure and do not have time to investigate if the virus alert is real or a hoax, Do NOT forward it (except to your network manager). Your network manager will be able to investigate and forward any pertinent instructions to everyone in your office.

And Remember:

One of the best ways to determine if a virus is real or not is to frequently visit the following anti-virus software websites:

www.symantec.com	Click on Search Virus Encyclopedia
www.mcafee.com	Click on Virus Information
www.cai.com	Click on Virus Information Center

Anti-virus software manufacturers make it their business to alert consumers to the latest computer viruses. Information and virus patches are free on their site and all do a great job of alerting consumers to hoaxes as well as legitimate concerns.

If you're looking for non-industry related advice, there are also 3rd party websites which help alert consumers to virus hoaxes and spam alerts. Check out the following websites for news, updates, and additional ways to prevent viruses and hoaxes from invading your computer.

www.hoaxbusters.ciac.org

www.vmyths.com

www.stiller.com/hoaxes.htm