

The KCS Enquirer

Information about the Computer Revolution

Volume 10 Issue 3

Fourth Quarter 2005

HAPPY HOLIDAYS

Year-End Refresher

Does MS Care?

KCS News

*Have a Very Merry
Christmas & a Happy New
Year*

The KCS staff wishes you a very happy holiday season and a prosperous new year. We want you to know we appreciate your friendship as much as your business.

Things to Remember – Do's & Don'ts

Do Backup

Backing up your data is probably the most important task you do. Losing data due to an equipment malfunction, disaster or sabotage can be extremely costly and disruptive. Make sure you have a good backup system and that you backup daily and store a current backup set offsite. Backup reports should be checked daily and test restores should be done periodically.

Do Have Redundant Server Data Storage

Your server should be setup so a single drive failure will not result in a loss of data. RAID (Random Array of Independent Drives) technology is the best protection against data loss and it

KCS Computer Technology Inc.

Novell Authorized Partner
Authorized Hewlett Packard Dealer
Microsoft Certified Professional on Staff
Certified Novell Administrator on Staff
Phone: **847-288-9820** Fax: **847-288-9822**
Web Page: www.kcstech.com
E-mail: sales@kcstech.com

Network Installations

Custom Programming

Custom Configured PCs

Digital Surveillance Systems

Phone Systems & Upgrades

SEE OUR WEB PAGE FOR QUOTES & ON-LINE ORDERING

also speeds up data reads writes to disk.

Do Have Adequate Power Protection

All your computers and peripherals should be protected by a good quality surge protector. A good quality surge protector is not a \$10.00 one from a discount store. Peripherals include printers, hubs, switches, print servers etc. Servers should be protected by an Uninterruptible Power Supply (UPS) along with a surge protector in some cases. For the best protection and to lessen the stress on servers the UPS should be a high capacity unit to

permit adequate time to shutdown properly with line conditioning to minimize voltage fluctuations which can weaken components.

Do Have an Internet Firewall

With all the on-line problems with spam, viruses and hack attacks it is critical that you have a hardware firewall device on your Internet connection. This is the first line of defense for on-line attacks.

Do Have a Good Anti-Virus Program

You need to have a good anti-virus program installed on all your computers, both servers and workstations.

Make sure the program is kept up-to-date or it will not be effective.

Do Have a Quality Anti-Spam/E- mail Virus Program

Spam (unsolicited and unwanted e-mail) is a nuisance and a time waster. E-mails carrying viruses are a growing concern. Make sure you are protected by a system that not only filters out spam and protects against viruses but also allows legitimate e-mail to be delivered to your mailbox.

Do Have Always-Active Anti- Spyware/Adware Protection

Adware and Spyware are programs that are loaded on your computer usually as a result of a visit to a Web site. They can also be contained in e-mail or hidden in downloads. Adware which is responsible for those annoying "pop-up" ads you see when working on-line. They use your computer resources and can become so intrusive that it becomes impossible to work on your PC.

Spyware is even worse. It not only can trigger pop-up ads but also monitors your computer usage and sends the information to companies that use it for market research and to tailor advertising based on your usage. Tailored advertising is then transmitted to you by way of pop-up ads or unsolicited e-mails. But the most danger is from unscrupulous companies that use spyware to steal private and personal information from your computer. They can retrieve passwords, user IDs, e-mail addresses, account numbers, credit card numbers, personal information and confidential business information. This data can be used to compromise your system, access Web sites you visit, including your on-line banking accounts, or steal your identity. This is a growing problem and you must protect yourself. The program you select should monitor constantly not just scan upon request.

Keep Your Wireless Network Private & Secure

If you are running a wireless network make sure it is secure and not broadcasting data that can be intercepted and used by others. Wireless networks should be set to the highest security possible that still allows easy access by authorized personnel.

Do Have Network Monitoring

It is important to keep a watch on your network both to identify and correct problems and to identify attempted or successful intrusions. These programs not only record activity but also can send out

notifications to alert you or your IT consultant of problems or attacks from the outside. With early detection and notification problems can be addressed before they become more serious.

Do Not Open Unsolicited E-mails or E-mails with Unfamiliar Addresses

E-mail is becoming the carrier of choice for delivering damaging programs to your system. If you encounter an e-mail that you are not positively sure is legitimate DELETE IT. DO NOT OPEN it since this can release the malicious program, be it a virus, adware/spyware, a worm, Trojan horse etc. Also never try to unsubscribe from an unsolicited mailing list since this will just verify your e-mail address and cause more problems.

Do Not Visit Unfamiliar Web Sites

Just by visiting a malicious Web site you can create problems for yourself. If it is not a well known site or one you heard about from reliable sources, stay away.

Don't Download Free Stuff

Other than trial software from well know and reliable companies, do not download items. Games, screen savers, wallpapers, surveys etc. are loaded with adware/spyware and viruses.

Don't Respond to Phony Warnings

A new trick that Internet pirates are using is to post an official looking message box on your screen telling you your computer software needs to be updated, your internal clock is wrong or that you have some type of problem that needs resolution. Responding by clicking the OK box can result in a lot of trouble. If you get a message, check to make sure it is legitimate before you do anything.

Never Give Out Personal and/or Confidential Information On-Line

NEVER, NEVER, EVER give personal or confidential information

to any Internet site unless you are absolutely, positively sure that you are on a legitimate site. There are phony Web sites out there that look like legitimate sites right down to trademarked logos. They will even show as secure sites with the locked padlock symbol at the bottom of the screen. Citibank is one of the victims of this type of deception. Many times people are led to these phony sites by an official looking e-mail that contains a link to the phony site. This is called phishing. Even if a request comes from a company you do business with it never hurts to give them a call to check if they have sent you an e-mail. NEVER GIVE YOUR SOCIAL SECURITY NUMBER TO ANYONE ON-LINE, PERIOD. No legitimate company should ask you for your social security number on-line. If they do, then we suggest you call them and give it to them by phone.

MS News

Do They Care?

Yes says Microsoft. So much that they are releasing OneCare Live in Beta (a public test version). OneCare Live is an anti-virus, anti-spyware program that also keeps your operating system up-to-date. It includes a backup system, disk defragmenter, file cleanup function and a software firewall. Whether they do this as well as 3rd party software manufacturers remains to be seen. However since they are responsible for the poor security features of their software you would think they would know how to handle the resultant problems. Regardless this will surely result in antitrust lawsuits. And you can bet that Microsoft will make money solving the problems they created.