By Merle Windler, Thoroughbred Systems, Inc.

Computer Corner

Use Common Sense to Keep Your Computer Virus Free

We have had numerous calls from rural water offices and cities in recent months asking for tech support for virus attacks on their office computers. I thought it would be a good time to ask this question: Are you following healthy computing practices?

Let's begin with the standard Internet safe-computing rules.

- ✔ Keep office computers use strictly business.
- ✔ Don't open email attachments from strangers.
- ✔ Don't give anyone your password.
- ✔ Don't use obvious passwords.
- ✔ Don't use the same password for multiple online sites.
- ✔ Obtain and use reputable AntiVirus, AntiMalware, and AntiSpyware software.
- ✔ Keep your protective programs and operating system up to date with the latest security patches.
- ✔ Follow good rules of data backup.
- ✔ When in doubt, "STOP" and call your computer support technician.

We could be impractical but totally safe by throwing away the computers and going back to the "Big Chief" tablet and an index card file as used to operate most rural water offices and some cities twenty-five years ago. Or, we could dramatically reduce and manage our risks by following "Safe Computing Practices."

First, use office computers for work-related activities only. Something as innocent as attempting to search for and find a favorite song to download and listen to while you work could expose your computer to viruses, malware and spyware. If done at all on a work machine, care should be taken to only use sites that are considered reputable like Rhapsody, Jango, Yahoo Music, AOL Radio, etc.

Don't open email with attachments from persons unknown to you. What seems like a harmless, cute photo, music file or document – might not be well-intentioned.

Don't give your password to anyone. Common scams include phone calls or email that appear to be legitimate contacts from your bank or credit card company asking you to confirm some account information or click on the attached link to correct a problem on your account. Never call the number given or use the link embedded in the email. Take a few seconds, look up and call or contact the proper numbers you have in your records. We have revealed several scams, including one to trick us into changing our phone service, by following this rule. Also, note that the IRS does NOT send email.

Don't use obvious passwords commonly known to others like the names of children, grandchildren or pets. When possible, use passwords that contain letters, numbers and possibly even symbols for increased security.

Don't use the same password over and over at various Internet sites. If one is compromised, they all are. Use different passwords and make yourself a "cheat sheet" and keep it in a secure place to keep track of them.

Make sure your computer has an antivirus program installed and running. DO NOT install more than ONE antivirus program. They can interfere with each other – and you end up without protection. The most popular antivirus programs presently include AVG, Avast, Kaspersky, Norton, McAfee, Microsoft, Panda, and Trend Micro.

DO NOT install more than ONE antivirus program. They can interfere with each other – and you end up without protection.

I recommend that computer users occasionally also run one of the free online "one-time" scans provided by well known and trusted companies like Kaspersky, Panda and Trend Micro. You may also want to run them if you suspect something might be abnormal as your computer is slower than usual, pop ups keep appearing that you didn't ask for while on the Internet, or you are redirected to a site you did NOT select.

Beware of all the scams!

Should you run into one of the Internet scams in which a message appears that malicious software has been detected on your computer and "suchNsuch" program wants to install on your computer to rid you of the infection – and the message IS NOT in the format containing the name of the antivirus program you know you have installed and running on your computer – IT'S A FAKE. DO NOT proceed. Do NOT allow it to install and run on your computer. Instead, exit the screen, site, Internet, and if necessary shut down your machine. But, DO NOT allow this supposed anti-virus program to infest your computer. If in doubt, "STOP" and call your computer support person.

Purchase the option for your antivirus program to also protect you from malware and spyware. Or, use a program like Malwarebytes Anti-Malware or Spybot Search and Destroy. Microsoft Windows Defender spyware protection is built-in for those that have Microsoft Windows 7; it can be downloaded for free from www.microsoft.com for those using Windows XP.

Operating system vulnerabilities

According to Microsoft's latest Security Intelligence Report, Windows 7 is four to five times less vulnerable to malware infections than Windows XP. A Cnet magazine article recently stated, "Microsoft Vista's infection rate was considerably lower than that for XP but still turned out to be double that for Windows 7. The 64-bit versions of Windows 7 and Windows Vista are less infection-prone than are their 32-bit counterparts, which Microsoft attributes to a couple of factors. First, the 64-bit versions of both systems may appeal to more tech-savvy users, presumably who would better know how to secure their computers. But second, Windows 64-bit offers a feature called Kernel Patch Protection, which protects the Windows kernel from unauthorized changes. Web browsers accounted for most of the vulnerabilities last year. But exploits that take advantage of Java vulnerabilities rose dramatically, surpassing every other category."

Keep your Microsoft Windows operating system and your protective programs up to date with the latest versions and patches. We have seen several instances in which a client choose NOT to install the latest security patches from Microsoft for their operating system because they "didn't have the time" for it. They were forced to take the time for it later when viruses were able to attack their computers through the weaknesses in their operating system that had NOT had the patches, circumventing their antivirus software they "thought" was protecting them.

Backup, backup, backup!

It's not a matter of whether or not something will happen some day and all the data on your computer will be lost... it's just a matter of "WHEN". So unless you don't mind losing all the information about your customer accounts, you had better be following good backup procedures. We recommend at a minimum burning a CD-R or DVD of all your important data at least ONCE per month. Usually this is done at the end of an accounting or billing period; then, store that backup in a safe place and keep it for five years. CD/DVD backup is still considered the most reliable and safe, cost effective backup method. Mirror drives that make an instant duplicate of all work done are great, but remember that mistakes made on one drive are instantly duplicated on the other. So, a virus affecting one drive is instantly duplicated as well. External USB drives, Flash/Thumb USB drives, and NAS/DAS backup units are all good too, but in my opinion, NONE of them exempt or replace doing at least a monthly CD/DVD of your critical data files. We have many clients subscribing to online Internet backup systems. We have seen several examples of clients finding out that the online backup systems were not functioning properly, therefore, they hadn't had a good backup in months. It is clear these DO NOT exempt or replace doing the monthly CD/DVD backup.

It's not a matter of whether or not something will happen some day and all the data on your computer will be lost... it's just a matter of "WHEN".

Keep this in mind. I don't think there is any such thing as too many backups. So I personally do a daily Flash Drive or USB drive backup of what I consider my critical important data. I have mirror drives on my computers, a NAS device with mirror drive as shared network storage. I additionally do a periodic entire drive image on removable "rack" drives on my desktop programming machines and STILL do a monthly CD/DVD stored in a fireproof safe of critical data.

Please keep these ideas in mind in determining what is right for your office. If your computer should fail for any reason the next time you start it, do you have the backups necessary to continue work?

Merle Windler and his wife Linda are owners of Thoroughbred Systems, Inc., Topeka. The company specializes in utility billing for cities and rural districts, computer networking and associated training. Contact: merlewindler@yahoo.com