By Merle Windler, Thoroughbred Systems, Inc.

Computer Corner

⚠CAUTION

Sometimes Antivirus Software is the problem!

Proceed With Caution

Everyone would likely agree that it would be foolish to have any computer on the Internet without antivirus protection software installed. Hundreds of new viruses and malicious software programs are produced everyday and are truly a threat to everyone who uses a computer, especially everyone using a computer on the Internet. But, sometimes the medicine is worse than the ailment, when taking the wrong prescription for one's needs. What does one do when the problem IS the antivirus software or other protective measures?

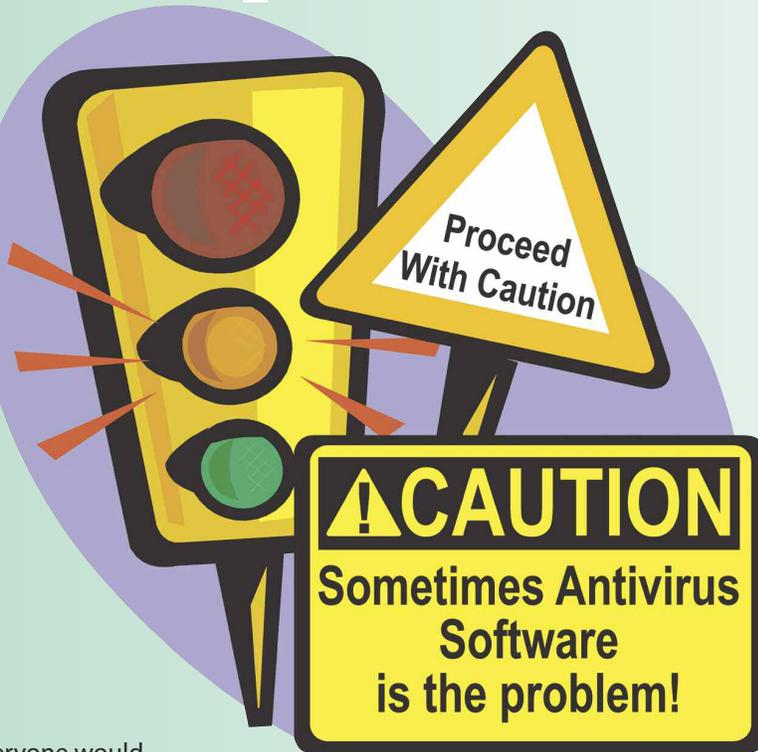Antivirus programs designed to help protect us from those who would use the technology of our own computers against us can, sometimes, unintentionally do harm. Most often, when a computer is running slowly, it's because it has picked up one of the thousands of annoying, mischievous programs on the Internet. One doesn't have to do something wrong to get into trouble; sometimes just being in the wrong place at the wrong time allows trouble to come in.

Being popular has a downside

Sometimes the problem is NOT these mischievous programs we refer to as a virus, but rather the very software installed on a computer to protect from them. The most popular and widely used antivirus programs tend to be a priority target for the many bad guys writing software intended to harm computer systems. Symantec's Norton Antivirus is one of these. In their case, to protect against this, their engineers have designed their product to embed their software during the windows installation. The very complexity of this can make the Norton antivirus installation more susceptible to corruption. Once corrupted, it can become very difficult to repair or uninstall the program, sometimes even requiring a total reinstall of the Windows operating system.

> **The most popular and widely used antivirus programs tend to be a priority target for the many bad guys writing software intended to harm computer systems. Symantec's Norton Antivirus is one of these.**

As the bad guys have become more sophisticated, so have the antivirus programs. When a product is designed to perform in a particular manner and has to be continually modified to defeat the attacks from the "bad guys", the end result is often a product that no longer performs as well as it did when it was in its unmodified form and functioned as was originally intended.

Certificate verification/community-based detection

One of the more recent attempts to combat the "bad guys" has been the implementation of "certificate verification". Software developers like myself must purchase a Code Registration Certificate, usually in the hundreds of dollars each, that has to be continually renewed in order to have antivirus programs "leave their programs alone" as recognized from a registered "good guy". Failure to use a registered certificate may result in a "false positive" identifying software as a threat and causing some antivirus programs to delete the suspect software.

What does this mean to the computer user? Software designed during or before the WindowsXP era, when this new detection technology was implemented, may cause older software to be deleted or damaged by the antivirus program. Norton Antivirus does not stop and ask the user if they want their software deleted; it just does it as an attempt to protect from what it sees as "unknown potentially dangerous software".

I've had to chuckle about the Symantec Norton AntiVirus program's repeated deletion of the old Symantec Q&A program (still used by many people in the water industry) as an unknown potential threat. The Q&A program, owned by the Symantec Company, is from before code signing certificates were commonly implemented, but, even though it was made by the same company as Norton AntiVirus, with fewer users these days, it may also activate the "community based detection" causing Norton to delete it without even stopping and asking the user if they want it deleted. The new "community-based detection" smart logic contacts the Symantec database over the Internet to check to see how many other Symantec Antivirus users are using the program in question. If the quantity of users is what they consider a low number, the software is deemed a potential threat and is often deleted from the computer without checking with the user for permission and without a warning or opportunity to not have the program deleted. It's a real problem for people running older programs or even new ones that are custom software installations.

Fortunately, there is an option to work around the problem. First, copy the deleted program back onto the computer from a backup and BEFORE running (opening) the software, "right click" on the .exe (the executable file that would open the software), then from the menu that appears, select (using the left mouse button) Norton FIle Insight. This will provide the opportunity to select "TRUST NOW". The antivirus program will then ignore the program and stop deleting it.

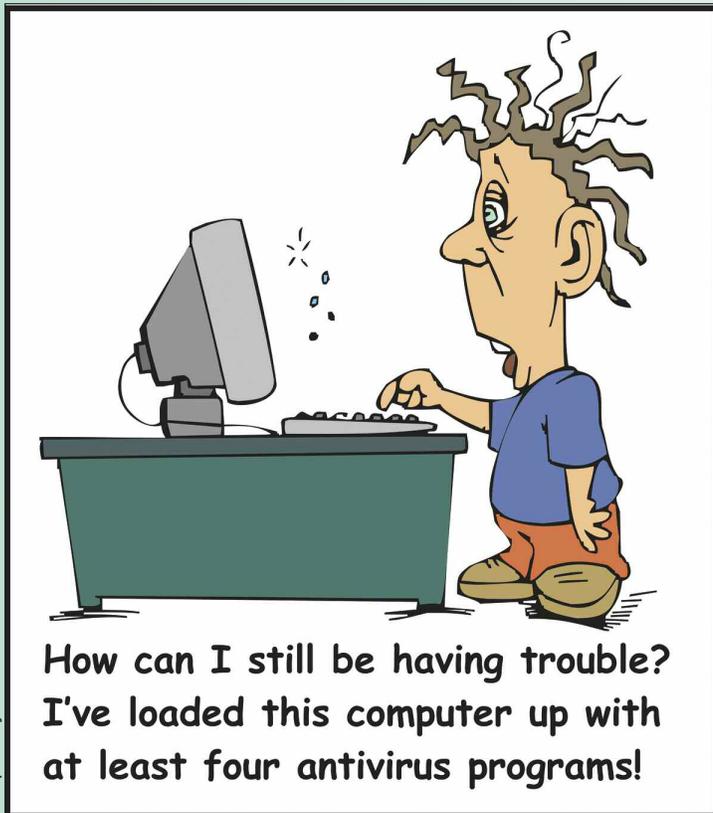## Why can't we just all get along?

Sometimes programs don't "play together" nicely. There have been many reports of Avast Antivirus and Malware AntiMalwareBytes not playing nicely together and causing computer lockups on some installations.

McAfee Antivirus had so much trouble with "false positives" reporting things as viruses that were not and updates that corrupted Windows installations of tens of thousands of computers a couple years back that McAfee offered free updates for two years to all the home users involved. Those free updates have only recently expired.

More is not always better

Sometimes people make the mistake of thinking that the more protection they have, the better. This may be true when trying to protect yourself from the cold by wearing long underwear and several coats and sweaters, but multiple antivirus installations will cause problems. To be clear, sometimes people confuse firewalls and virus protection; these are two separate items, each with its own task to do. Having a software firewall, and for that matter, hardware firewalls too, and an antivirus program is normal. But, never install more than one antivirus program on the computer at the same time. Most antivirus programs will detect that another already exists and provide a warning or refuse to install while the

> **Norton Antivirus does not stop and ask the user if they want their software deleted; it just does it as an attempt to protect from what it sees as "unknown potentially dangerous software".**

Graphic by Linda Windler

How can I still be having trouble? I've loaded this computer up with at least four antivirus programs!

Even the Microsoft Security Essentials and Windows Defender made by Microsoft to protect the Windows operating systems are not without a few "hitches". Though not bad for a free solution, there can be pitfalls. For example, our own software products generate temporary files to facilitate printing large files to expedite freeing the program to continue performing other tasks. MSE and Defender coupled with Microsoft's User Account Control feature (UAC) watch for unexpected activity on the computer. When we create a temporary file to expedite printing functions, the antivirus programs can sometimes falsely perceive these temporary files as a threat and take action either causing the program to run slowly, or in some cases, even lock up. The solution is to enter the settings section of MSE or Defender and select File Exceptions. Then, add .tps and .tpe data files to the list of files to NOT be attacked as a potential virus. Such occurrences are not uncommon in the computer industry.

When a computer is running slowly or acting a little "funny", the first thing to suspect is malicious software of some sort. Many malicious programs will immediately attempt to deactivate any antivirus protection on the computer. Keeping that in mind, if the antivirus does not seem to updating or running properly, it's a pretty certain sign that it has been compromised. Take action to check for and kill any malicious software. If that doesn't work, many times an antivirus program itself can be the cause of problems especially if the problems began after a recent upgrade. I will normally use a special scan from the Web, like TrendMicro Housecall, or download and run Microsoft Safe Scan to check for viruses. If nothing is found and the computer is still running slowly, especially if one of the large commercial antivirus programs is present, I will usually uninstall it and try Microsoft's solution, AVG or Avast and see if the computer "miraculously" is healed.

Sometimes the solution to ease symptoms is to change medicine.

When in doubt, research, and, the best solution, call an experienced computer support professional.

other is running. Having more than one antivirus program may result in neither functioning properly and leave the computer unprotected.

Help is available; sometimes even for FREE!

Microsoft offers its Security Essentials (MSE) free to all genuine Windows users of Windows XP, Windows Vista, or Windows 7 as an incentive for persons to not "pirate" their Windows operating system. In Windows 8, Windows Defender replaces Microsoft Security Essentials. Either will run in the background to help defend against viruses, spyware and other malicious software. If the user feels the need to run an extra scan suspecting the computer has "caught" something, then he/she can download and run "Microsoft Safety Scanner" and use it for ten days for free at http://www.microsoft/security. After ten days it will expire and will have to be downloaded again.

MSE is free to all genuine Windows, business or personal users while other popular programs like Avast and AVG are only FREE for home or personal use. Commercial users are supposed to purchase the more robust versions.

Merle Windler and his wife Linda are owners of Thoroughbred Systems, Topeka. The company specializes in software solutions for utilities and municipalities, computer networking and associated training. Contact: merlewindler@yahoo.com