

TECH-TALK!

By Burt Newman, CAS, MAS
Info@promoplanner.com

COMPUTER SECURITY ISSUES-WHAT HAVE YOU DONE LATELY?

In the last issue, the TECH-Talk column dealt with the issue of preserving your work; the output of your computer efforts. While that is an important topic and one that clearly requires continual attention, the immediate topic, computer security issues, is certainly equally important.

An unknown source is reported to have said, "When it comes to security, there are no sure answers" and "no system is totally secure". But doing nothing, because you are unsure, is certainly the "road less traveled" for those who respect security provisioning and wish to limit their losses & vulnerability.

Let's begin with a minimal rhetorical question checklist.

1. Do you have any type of computer security?
2. If so do you know what it is?
3. Has it ever been tested; is it operational?
4. Do you know how it works; if not, do you want to learn?
5. Is computer security an important issue for you?
6. Is there a once-stop shop or one size fits all solution?
7. Who do you trust with the information contained in your computer(s)?
8. What if anything do I need to do NOW?

While the above questions are submitted as rhetorical questions, this author will attempt to briefly discuss the answers to them as well as provide some supplementary information related to them as well. First and foremost you do indeed need to be concerned about computer security. Whether you have one machine or a network of machines, you should provide some degree of computer security for each machine and the network to which they may be connected.

Computer security could be simplified by dividing it into internal and external security issues. As such this commentary will be so divided.

Internal security consists of securing the information stored on individual or system computers and the access that is allowed to those computers by individuals in your employ. At the most basic level, one should have at least minimal password protection to each individual computer. This initially allows access by those whom you have chosen to give entry to this proprietary data. While in its simplistic form it is not an impregnable fortress, it is at least a way of keeping nosey eyes away. Likewise if your computers are left alone (when you walk away or are distracted into doing something else) the machine will temporarily shut down and the password will need to be reentered to regain access. Guarding the password is equally as important as developing one that is relatively uncommon. In effect, don't use your name, your nickname, your initials, birthday or passwords that others might already know or easily guess. Create some challenge; be creative! Don't use the same password here that you have previously used in another situation. And for sure, prevent at all costs "shoulder surfing" by employees, visitors or guests to your desktop. In effect, remember to never log-on with someone watching.

To be safe, frequently change your password(s) to ensure protection. Furthermore, keep your password in your head or at least on your person; don't write it down and put it on the monitor, under the keyboard, under the mouse pad, on the computer unit (CPU) or in the desk drawer. In essence, use judgement and common sense protection procedures yourself. Lead by example and make your employees equally cognizant of computer security and awareness.

Internal security also includes the screening of software programs and data files that are placed on your computer by you or your employees or friends. You should consider having one person responsible for deciding what gets into (and out of) your computer(s). New software can cause havoc with existing programs as you may have previously experienced. Data files entered into your computer can contain viruses or files that can corrupt your data. Previous discussions have dealt with virus protection, but be sure to scan any data files or attached files for viruses prior to allowing them into your machine. And frequently (daily if possible) update your virus definition files so you are current and have the latest weapons to ward off virus attacks. Too often computer damage comes from within; trusted employees, former employees or vendors whom we often overlook when determining our needed level of protection.

External security consists of securing the information that you transmit to and from your computer. When you utilize e-mail, the Web, IM, Private Networks, e-commerce and Wireless Technology you open yourself and your computer to a different level of computer security issues; those from others outside your immediate environment. This too is a vulnerability for which you need additional & different computer security protection such as Intrusion Detection Systems (IDS) and others.

Sooooooooooooooooo, in order to proceed, evaluate what type of computer security you have in place, if any, and develop a simple assessment plan of what you might need to protect both from within and outside. Then ask around and shop around for available solutions to solve your stated problem. There is no magic bullet or one size fits all when it comes to computer security or the price tags that accompany them as well. If a "real" or "rogue" hacker or former disgruntled employee has you targeted that is a totally different issue & requires other protections. But don't panic or give up the ship. For very reasonable cost or in some cases, no cost at all, you can find a variety of solutions. Ask for help and look at what others have done to protect their computer(s). In addition to anti-virus software programs, there are no cost simple firewalls and coded or encrypted messages & secure Web pages. Many are easy to obtain and easy to install via self-installed "wizards" for your use.

Once installed, test your security and check it out on a regular basis to make sure it is active, operational and is working to help you save your precious data. Get involved; become familiar with what you have and how it is suppose to work. This is not advanced rocket science and if you stay with simple solutions you should be able to learn enough about them to keep yourself informed. If you get stuck there are multiple options to learning more via seminars, classes, on-line information sites and on-line chat or discussion groups specific to a particular product. If you are still curious, do a search on the Web and you will be surprised at the volume of information available to you and easily within your grasp.

Finally, consider what would life be like if you lost all your computer data, if someone else compromised it or if the wrong people got a hold of it. There is a lot at stake and ignoring it by doing nothing proactive will eventually catch up with you. Security issues are continually changing and as new technology develops. Technology here-to-for unknown such as computer wireless technology (not just cell phones) will become the security technology to resolve in the short term. So by keeping alert and realistic you too can deal with the issues and be current in your attempts to protect yourself and your information. Keep in mind that computer security issues and their related solutions are constantly changing with additional challenges to formerly secure systems. The current thinking today seems to follow the concept of "layered protection". In this regard, anti-virus software coupled with firewall protection are a good one-two multiple layer of protection suitable to single computer users.

Keep thinking about how you choose to secure your computer(s) & how often you re-evaluate and revisit that concern. Continued attention to it will undoubtedly save you lots of problems now and in the future when you least expect a breach in your security as you think about "**Computer Security Issues-What Have You Done Lately?**"

Please Note:

The contents of all articles in the TECH-TALK! column are the personal intellectual property of **Burt Newman** and are Copyrighted © & Copyright Protected under Copyright Law. None of the contents may be copied or used without the author's expressed written permission and are placed in the GCPA Newsletter with his permission.