THE COMPUTER CORNER

No. 239: Safeguarding Your Data

Stan Kaplan, WB9RQR 715 N. Dries Street Saukville, WI 53080-1664
(262) 268-1949 wb9rqr@att.net

It is not unusual for me to run across good articles that are worthy of reprinting in the Computer Corner column. This is another one, from CERT, as was last month's. Reprinted by permission granted to Stan on 29Nov2017.

Official website of the Department of Homeland Security

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Security Tip (ST06-008) Safeguarding Your Data

Last revised: January 24, 2017. **Author** US-CERT Publications. It is especially important to take extra security precautions when multiple people use your computer—or when you store sensitive personal and work-related data on your computer.

Why isn't "more" better? Maybe there is an extra software program included with a program you bought. Or perhaps you found a free download online. You may be tempted to install the programs just because you can, or because you think you might use them later. However, even if the source and the software are legitimate, there may be hidden risks. And if other people use your computer, there are additional risks.

These risks become especially important if you use your computer to manage your personal finances (banking, taxes, online bill payment, etc.), store sensitive personal data, or perform work-related activities away from the office. However, there are steps you can take to protect yourself.

How can you protect both your personal and work-related data?

- **Use and maintain anti-virus software and a firewall** – Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall. Make sure to keep your virus definitions up to date.
- **Regularly scan your computer for spyware** – Spyware or adware hidden in software programs may affect the performance of your computer and give attackers access to your data. Use a legitimate anti-spyware program to scan your computer and remove any of these files. Many anti-virus products have incorporated spyware detection.
- **Keep software up to date** – Install software patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should turn it on.
- **Evaluate your software's settings** – The default settings of most software enable all available functionality. However, attackers may be able to take advantage of this functionality to access your computer. It is especially important to check the settings for software that connects to the Internet (browsers, email clients, etc.). Apply the highest level of security available that still gives you the functionality you need.

- **Avoid unused software programs** – Do not clutter your computer with unnecessary software programs. If you have programs on your computer that you do not use, consider uninstalling them. In addition to consuming system resources, these programs may contain vulnerabilities that, if not patched, may allow an attacker to access your computer.
- **Consider creating separate user accounts** – If there are other people using your computer, you may be worried that someone else may accidentally access, modify, or delete your files. Most operating systems (including Windows, Mac OS X, and Linux) give you the option of creating a different user account for each user, and you can set the amount of access and privileges for each account. You may also choose to have separate accounts for your work and personal purposes. While this approach will not completely isolate each area, it does offer some additional protection. However, it will not protect your computer against vulnerabilities that give an attacker administrative privileges. Ideally, you will have separate computers for work and personal use; this will offer a different type of protection.
- **Establish guidelines for computer use** – If there are multiple people using your computer, especially children, make sure they understand how to use the computer and Internet safely. Setting boundaries and guidelines will help to protect your data.
- **Use passwords and encrypt sensitive files** – Passwords and other security features add layers of protection if used appropriately. By encrypting files, you ensure that unauthorized people can't view data even if they can physically access it. You may also want to consider options for full disk encryption, which prevents a thief from even starting your laptop without a passphrase. When you use encryption, it is important to remember your passwords and passphrases; if you forget or lose them, you may lose your data.
- **Follow corporate policies for handling and storing work-related information** – If you use your computer for work-related purposes, make sure to follow any corporate policies for handling and storing the information. These policies were likely established to protect proprietary information and customer data, as well as to protect you and the company from liability. Even if it is not explicitly stated in your corporate policy, you should avoid allowing other people, including family members, to use a computer that contains corporate data.
- **Dispose of sensitive information properly** – Simply deleting a file does not completely erase it. To ensure that an attacker cannot access these files, make sure that you adequately erase sensitive files.
- **Follow good security habits** – Review other security tips for ways to protect yourself and your data.

Happy Computing!