

Desktop Computer Security

This guide explains how to secure your desktop computer. The guide and the resource list is primarily written for the Windows OS environment but also applies to other operating systems. The steps are ordered according to practicality. The first step being most practical, the last being the most difficult to implement. At the end of the guide is a resource list.

1. Anti-Virus: The most basic and most commonly implemented security element is anti-virus software. Most users choose one of the big two anti-virus software packages from either McAfee or Symantec-Norton but the free versions of several vendors are actually just as good and tend to run faster and have fewer technical issues. The key to anti-virus is to keep it updated and make sure it is set to run complete system scans daily. It is also a good idea to use a combination of an installed anti-virus scanner and an online anti-virus scanner. The combination of the two forms of anti-virus greatly increases the effectiveness of virus detection as anti-virus detection is not a perfect science and some scanners will miss viruses that other scanners will find.

2. OS Patches and Software Updates: Most users are familiar with the Windows security update process in which Microsoft releases monthly security patches for their operating system and core applications such as Internet Explorer and Microsoft Office. However, most users are unaware that many of the other applications on their computer system also require periodic updates to patch security issues. It is recommended that you either allow these applications to perform automatic updates if the feature is available, or go to the application publishers web site and check for any updates on at least a monthly basis. Software Vendors such as Adobe, Java, QuickBooks and other financial software should not be forgotten about when applying security patches as they have most commonly been found to contain exploits that could hurt your computer security.

3. Anti-Malware: Adware is fast becoming the biggest threat to desktop security. While virus infections are actually on the decrease, adware infections are increasing in both frequency and severity. While some adware is just an inconvenience, other infections are almost impossible to remove and can render a computer system totally useless over time. Worse yet, some adware is designed to also download spyware and other malware that can be used in identity theft. It is recommended practice to have several anti-malware programs installed on your computer. The following are recommended anti-malware programs: Ewido

Anti-Spyware and Ad-Aware SE are excellent as primary scanners. Additionally, SpyBot Search and Destroy provides both scanning and active system monitoring features. Although SpyBot is also an adware scanner it has an additional feature called Tea Timer. Tea Timer watches for new software trying to install and run processes on your computer and also watches the windows registry for any changes being made which would indicate the installation of new software. If anything is detected, you receive a pop-up notice and are given options as to what actions to take. Although it takes some knowledge and input from the user, it is an excellent way to protect your computer from the changes that adware attempts to make when it is trying to infect your computer. It should be noted that many of the larger antivirus companies are now including some spyware protection in there packages. While this is a step in the right direction, users should still consider having more than one form of malware protection active on their computer as the best practice in any environment is defense in depth.

4. System Utilities: There are several excellent free utilities that you can use to keep your system free of security threats. A system maintenance utility such as CCleaner is a must have. CCleaner cleans temporary files used by applications and the operating system including cookies and stored passwords. It also has a registry cleaner which cleans out dangerous security risks such as unused active-x components. Another indispensable utility is RootKit Revealer. Although it requires a somewhat advanced user to decipher the results, it will tell you if there is a possible rootkit installed on your system. Rootkits are very advanced software infections that are not detected by anti-virus, anti-malware or any online scanners. Rootkits can be used by hackers to completely reveal anything you do on your computer or steal any information or files on your computer. Rootkits are becoming more and more common especially as components of certain adware infection.

5. Software and Hardware Firewalls: The basic function of a firewall is to hide your computer or network from the outside world (the internet). Although firewalls can be quite complicated, the easiest way to set up firewall protection is to purchase a router. By connecting a router to your internet access DSL or Cable modem you, in effect, separate your computer or your network from the internet. If you are using a dialup connection for your internet you can install a software firewall. Although it is a bit more complicated, a software firewall does pretty much the same job as a hardware firewall. Windows XP has a built in software firewall that is very effective or you can download and install one of the many free software firewalls.

6. System and File Backups: Critical or sensitive information should be backed up to help prevent loss in case of a computer software or hardware failure. Your backup solution can be as simple as manually copying your files to a USB key or external hard drive; or burning a monthly CD or DVD with your critical information. Files such as pictures, documents, and music should all be included in your backups. Don't forget your e-mail settings, as this is vital to the timely restoration after a system crash. A newer method of backing up information is to use an online vendor. As long as you have an internet connection, the online vendor can be used to do full system backups and allow you access to your information from any other computer also connected to the web. A couple of good options are www.remotedatabackups.com, www.swapdrive.com and www.carbonite.com. No matter which backup option you choose the most important thing is to set a backup timeframe and stick to it; at a minimum a monthly backup is typically recommended.

7. Safe Computing Practices: Although sometimes hard to apply for inexperienced users, knowing the dos and don'ts of computing can go a long way towards a worry free secure computer. Users should make a point of constantly improving their user skills and updating themselves as to what security risks affect them. There are plenty of information sources on the web that are full of great tips on what to do and what not to do when using your computer and the internet. The basic practices include never opening suspect email attachments, using strong passwords that include both numbers and letters, not clicking on links to websites unless you know they are safe, only downloading from sources that you know are secure, making sure that banking and personal information is only entered into forms on secure web sites indicated by the "https" in the sites url (web address), periodically changing your passwords, and never responding to "too good to be true" offers.

8. Encryption: This is the process of making data unreadable unless you have a key to decrypt the data. The most common encryption is used when you access a secure web site (https) with your web browser. There are also programs available that can encrypt email messages to make them readable only by the intended recipient. You can also use encryption software to secure files on your computer.

Unfortunately even with all the preparation in the world occasionally there will be failures and problems that cannot easily be fixed. In most cases, it is best to call in an expert who can resolve the problem for you and will usually offer a warranty if the problem happens again. There are many companies that claim to do computer repair, but before you hire one of them you should ask what experience they have. Reputable companies require their

techs pass tests to prove their knowledge. Comptia's A+ certification is common in the computer world and so are Microsoft's MCP, MCSA, MCSE certifications. Regardless of what certifications they have, getting references or testimonials is also always a good idea. Some mobile computer service companies will come right to your door to fix your computer or networking problems. Other interesting options include www.onlinecomputerrepair.org and www.clickanerd.com which both provide online/phone technical support for problems you may be having.

RESOURCES:

- www.ca.com - CA Anti-Virus, Anti-Spyware, Anti-Spam solutions
- www.free.grisoft.com - Free version of AVG Anti-Virus
- www.bitdefender.com - Online virus scanner
- www.trendmicro.com - Online virus scanner
- www.remotedatabackups.com – Online Backup Solution
- www.sophos.com - Very good source of specific virus removal tools and virus information
- www.javacoolsoftware.com - SpywareBlaster - Anti-spyware protection shield software
- www.carbonite.com – Online backup solutions
- www.safer-networking.org - SpyBot Search and Destroy scanner and Tea_Timer monitor
- www.lavasoftusa.com - Ad-Aware SE adware scanner
- www.ccleaner.com - CCleaner - System maintenance utility
- www.sysinternals.com – RootkitRevealer - Rootkit detection software
- www.tomcoyote.org/hjt/ - HIJackThis - Browser hijacker detection tool
- www.swapdrive.com – Online Backup Solution