

Small Business Computer Security, the Basics

Anyone in business today realizes both the natural dependency on computers in the workplace, and also the potential dangers associated with storing important data on them. Today's business owners are constantly being reminded that their company's data is at risk by the daily reports on various news stations, or even their favorite business-related website.

But what can a typical small business owner do to protect their network from these threats that are broadcasted in so many ways? Dangers lurk at every turn on the Internet. There are thousands of attacks or areas of security that could be discussed, but I am going to try and focus on three general nuisances associated with today's computers: viruses, spy-ware, and traditional "hackers" that will intentionally try to exploit your computer systems for various reasons. All of these attacks, although different, serve a specific purpose for the attacker, yet basically translate into three things for a business: lost productivity, lost data, and the end result... lost money. Here is brief descriptions of what the aforementioned attacks are, consist of, and what a typical small business can do to protect their technology investments.

Virus: A computer virus shares some traits with an actual virus that gets people sick. A computer virus must piggyback on top of some other program or document in order to get executed. Once it is running, it is then able to infect other programs or documents. Obviously, the analogy between computer and biological viruses stretches things a bit, but there are enough similarities that the name sticks. A computer virus can have many intentions. One common goal is the virus's desire to infect as many machines as possible. Some are harmless and are no more than an attempt for a hacker to spread their name and get recognition amongst their peers. However, this can still lead to slow computer performance or programs acting up. On the other side of the coin, viruses can be extremely harmful and delete data, cause complete computer interruption, give someone unauthorized access to your company data, or even be used in conjunction with thousands of other infected computers to launch grand-scale attacks. Viruses are still mostly transferred via email; however newer attacks will entice you via an email to a malicious website that will exploit a flaw in your computer to install the virus.

Protection from Viruses: If you are reading this article, and you still do not have current (this is very important) anti-virus software running on EVERY single computer you own, then shame on you. With all of the marketing commotion that surrounds viruses, you should already have antivirus software on all of your computers. If you don't, then hurry to the store and purchase it. Popular software in the antivirus market is made by Symantec (www.symantec.com) and McAfee (www.mcafee.com). Larger companies may look into a system that will scan emails prior to the email getting to a user's inbox for viruses. Also, be wary of what you open in your email. Do not open emails from people you do not know, and even if you do know the sender, take extra caution, as most viruses today will trick you into believing that the virus is sent from someone that you know.

Spyware: You may know spyware by one of its many names, adware, malware, trackware, scumware, thiefware, snoopware, and sneakware. Because of its stealthy nature, most Internet users are more familiar with the symptoms of spyware infection: sluggish PC performance, increased pop-up ads, unexplained homepage change, and mysterious search results. For virtually everyone surfing the Internet, malware and adware are a nuisance, but if you do not detect spyware on your PC, it can lead to much more serious consequences such as identity theft. Many people wonder how they get spyware installed onto their computer in the first place. Typically, spyware is installed onto your PC without your knowledge because the programs are usually hidden within other software. For example, when you are browsing a website, and a pop-up appears to install the latest online Casino game, it probably will give you that game, but you've also just installed spyware along with that. Another avenue for Spyware to infect your machine is through popular Peer-to-Peer File Sharing software such as Kazaa. The financial impact on a business that is plagued by spyware can toll very high. Costs paid to computer consultants to remove spyware, and a user's overall lost of productivity from a slow-performing computer can add up very quickly.

Protection from Spyware: Spyware is a huge problem in today's computing environment. Fighting Spyware starts with smarter use of your computer. The best defense against spyware and other unwanted software is not to download it in the first place. Here are a few helpful tips that can protect you from downloading software you don't want. Only download programs from web sites you trust, read all security warnings, license agreements, and privacy statements associated with any software you download, and never click "agree" or "OK" to close a window. Instead, click the red "x" in the corner of the window or press the Alt + F4 buttons on your keyboard to close a window, and be wary of popular "free" music and movie file-sharing programs, and be sure you clearly understand all of the software packaged with those programs. If you do happen to install Spyware on your computer, there are some tools available to assist in the removal of spyware. Be careful however when downloading these "free" spyware removal softwares, as even some of the removal tools incorporate spyware into their software. A popular product that does a good job of removing spyware is Lavasoft's Adaware (www.lavasoft.com). Larger organizations can look to companies such as Computer Associates (www.ca.com) for enterprise protection. There are instances when there is simply just too much spyware installed on a machine where these tools cannot help, and you'll be forced to format your hard drive and reinstall your operating system.

Hackers: The term hacker has many different meanings to many different people. A dictionary might define the word hacker as follows, "A person who breaks into, or attempts to break into, or use, a computer network or system without authorization, often at random, for personal amusement or gratification, and not necessarily with malicious intent. 2. [An] unauthorized user who attempts to or gains access to an information system 3. A technically sophisticated computer expert who intentionally gains unauthorized access to targeted protected resources, loosely, a computer enthusiast. 4. A person who uses a computer resource in a manner for which it is not intended or which is in conflict with the terms of an acceptable-use policy, but is not necessarily malicious in intent." As you can see, a hacker is someone with a very high aptitude in computing. By studying the inherent design of computer systems, a hacker will then attempt to compromise those systems for a purpose. Typically, they use a collection of tools easily downloadable on the Internet to exploit a flaw in a program or hardware system. Hackers do what they do for various reasons. Some do it for simple prestige amongst their peers, others for financial gain, and others do it to make a political statement. The impact of your network's security being breached can lead to very serious financial losses. Imagine your customer database being sold to a competitor or even what public response would be if you had to tell your customers that their personal information was stolen?

Protection from Hackers: I was once told, that no matter how good a safe you buy, there will still always be a locksmith that can un-lock it. The same goes for protection against hackers. However the amount of people with the expertise to bypass most security defenses, available to companies, are few and far in between. To keep your network safe, the following three items are an absolute must. A quality firewall at your network's perimeter to filter what goes in and out of your internet connection, desktop level firewalls to keep internal company computers safe, and the importance of performing updates to your computer's operating system and applications. Firewalls simply stated, filter data passing through them. They are in essence, inspectors that allow and deny data to be passed through them based on certain rules. Most quality firewalls will protect your network by letting the good data through and keeping the bad out. Recommended firewalls for small businesses can be purchased from companies such as Cisco (www.cisco.com), Watchguard (www.watchguard.com) or Sonic Wall (www.sonicwall.com). Firewall vendors typically have many different models available, so consult with your network security professional on what to buy. The important thing is that you have one in place. Desktop level firewalls provide a true multi-layered approach to security. This added level of protection strengthens your computer systems defense, and is especially helpful to companies that have remote workers. Most companies today do have firewalls on their corporate network; however no one ever thinks about the company president's laptop that gets brought home everyday. The president brings his laptop home and sets up his trusty remote connection back into his office over his broadband home Internet connection. The once protected laptop is now completely unprotected and connected directly to the corporate office, which gives a direct avenue for virus and hackers onto your corporate network. The great thing about desktop firewalls is that you can get some great ones for free! If you use the Microsoft Windows XP operating system, simply upgrade to service pack 2 and it includes a free and easy to use desktop level firewall. If you do not have Windows XP or just do not want to use their firewall, Zone Alarm (www.zonealarm.com) offers a great desktop level firewall. The last level of defense is to keep your networked systems up to date with the latest patches and fixes from their respective manufacturers. I will assume that most companies use Microsoft Windows products for most of their computing needs, so to keep your system updated simply go to <http://windowsupdate.microsoft.com>. You should check for updates twice a month.

Even though this article simply brushes the surface of network security, I hope it gives you insight as to some potential dangers out there and real incentive to implement better security for your company. Just as you have an alarm system at your office, please take the necessary steps to protect your company's computer network and data. If not, the costs of recovery I guarantee you will far exceed the costs to implement a secure network.

Jarrett M. Pavao studied at the University of Miami, is a Microsoft Certified System Engineer, and Citrix Certified Administrator. Jarrett is the Director of Business Technologies for Docutek, a systems integrator in Boca Raton, FL. Jarrett can be contacted at jpavao@docuteksolutions.com with any network security related questions or concerns.