



## Network Security Best Practices

---

**Audience:** Fastpay Clients

**Purpose:** To elevate the awareness of the need to keep business data and networks secure. The document provides tips, resources and best practice examples.

**Expiration:** This document should be reviewed yearly as to content as well as implementation.

---

**Last Updated:** 1/14/2008 3:56 PM

# Table of Contents

<b>Chapter One – What You Can Do to Manage Network Security</b>	<b>4</b>
<b>Overview</b>	<b>4</b>
<b>Easy Jobs</b>	<b>4</b>
• Install and update antivirus software	4
• Use software update tools	4
• Install spyware protection	4
• Install a software firewall	5
• Install spam filtering software	5
<b>Harder Tasks</b>	<b>5</b>
• Restrict equipment access	5
• Set permission levels	5
• Remove network access for former employees	5
• Create an e-mail and Internet use policy	6
• Require employees to use strong passwords	6
<b>Hire Help</b>	<b>6</b>
• Install a perimeter firewall	6
• Secure a Virtual Private Network	6
• Configure wireless security features	6
• Create back-up and restore procedures	7
• Configure database security	7
<b>Chapter Two – Tips for Password Security</b>	<b>8</b>
<b>Overview</b>	<b>8</b>
<b>Don't be complacent.</b>	<b>8</b>
<b>Know what makes a bad password.</b>	<b>9</b>
<b>Get proficient at creating good passwords.</b>	<b>9</b>
<b>Safeguard your password.</b>	<b>10</b>
<b>Change your password often.</b>	<b>10</b>
<b>Chapter Three – Shield Your Network from Clever Hackers</b>	<b>11</b>
<b>Overview</b>	<b>11</b>
<b>Social Engineering Tactics</b>	<b>11</b>
The caller isn't working on your network.	11
That e-mail isn't from Joe.	12
When the hackers go "phishing," don't take the bait.	12
Protect your company.	13
<b>Chapter Four – Tighten Wireless Network Security</b>	<b>14</b>
<b>Overview</b>	<b>14</b>
<b>Strategies to Keep Your Wireless Network Safe</b>	<b>14</b>
Assume you already have a problem.	14
Get a security policy in place.	15



Build a wall, not a quilt.	15
Crank up your settings.	15
Don't be afraid to take drastic measures.	16
<b>Appendix of Online Tools</b>	<b>17</b>
<b>Overview</b>	<b>17</b>
<b>Anti-virus</b>	<b>17</b>
AVG Anti-Virus – FREE	17
Trend Micro – Purchase/FREE Online Scan	17
<b>Anti-Spyware</b>	<b>17</b>
Microsoft Anti-Spyware – FREE	17
Spybot Search & Destroy – FREE	17
<b>Software Firewall</b>	<b>18</b>
Sygate Personal Firewall – FREE	<b>Error! Bookmark not defined.</b>
ZoneAlarm Personal Firewall – FREE	18
Windows Firewall – FREE	18
<b>Software Update Tools</b>	<b>18</b>
Windows Update – FREE	18
<b>Vulnerability Scanning Software</b>	<b>18</b>
Microsoft Baseline Security Analyzer – FREE	18

## Chapter One – What You Can Do to Manage Network Security

### **Overview**

Thanks to the continued presence of Internet worms, viruses and other threats to computers, network security consistently ranks as a top concern of business owners, even for those operating simple, small business networks.

The good news is that you and your employees can manage many of these security measures yourself without help from an IT professional. The network security steps listed below are ranked by degree of difficulty. Start with the easy jobs and work your way through the others as your time, resources and skill level permit.

See the appendix of this document for a list of online tools available to you to help protect your business network. Many of these tools and services are **FREE!**

### **Easy Jobs**

If you have ever completed tasks such as installing a program or setting up a printer for your computer, you should have little trouble performing these jobs.

#### **• Install and update antivirus software**

Antivirus software is easy to install and, once running, constantly checks to prevent infections that could damage or destroy your data across your network. But know that hackers constantly write new viruses and that your antivirus software is effective only if it knows how to find the latest threats. So when you install antivirus software, set it to automatically download updates **DAILY** to catch new viruses. If you bought a new PC that included antivirus software for a trial period, sign-up when the free period expires to continue getting updates or install another product.

#### **• Use software update tools**

Software companies like Microsoft have free tools you can use to update your software so it's more secure. For instance, it only requires a few mouse clicks to set Windows XP or Windows Server to use the Automatic Updates feature. This tool allows Windows to go online automatically to look for and install the latest updates to squelch security threats. Once you turn on Automatic Updates, it requires no further effort on your part. The software will update itself. The Microsoft Office System also has an automatic updating tool.

#### **• Install spyware protection**

Install and regularly update anti-spyware software, which looks for secretive programs that try to collect your passwords and account numbers. Microsoft has a free Windows Anti-Spyware program and a Malicious Software Removal Tool you can use to rid your PCs of unwanted software.

- **Install a software firewall**

A firewall examines data passing into your network and discards it when it fails to meet certain criteria. Software firewalls, such as the Windows Firewall built into Windows XP Professional, protect only the computer they are running on, but provide a good back-up defense to hardware firewalls. It's easy to turn on the Windows Firewall. If you are not running Windows XP then you may want to either upgrade your operating system to Windows XP or purchase a 3<sup>rd</sup> party software firewall product.

- **Install spam filtering software**

Spam is unsolicited commercial e-mail that infiltrates inboxes and can force employees to waste time sorting it. While primarily a nuisance, junk e-mail does carry a risk when it contains attachments that, if opened, could release a virus. Also, some spam falls into the category of "phishing," or tricking recipients into giving away passwords and other valuable information that could put a business at risk. Installing a spam filtering product, or configuring built-in Outlook 2003 junk e-mail filters, can help to significantly reduce spam.

### ***Harder Tasks***

This set of tasks can be more difficult. They require more technical expertise or ongoing management of your security policies and processes.

- **Restrict equipment access**

You can improve security by restricting physical access to your servers and networking equipment such as routers and switches. If possible, move these machines into a locked room and ensure only those designated to work on the equipment have keys. This minimizes the chance that someone unqualified can tamper with your server or try to "fix" a problem.

- **Set permission levels**

You can assign users different permission levels on a network using Windows Server. Rather than giving all users "Administrator" access, give individual users access to specific programs only, and define which user privileges are allowed to access the server. For example, you can grant permission to some users to read certain files stored on the server, but not to change them. Only your network administrators should be able to access all your system files and services.

- **Remove network access for former employees**

Eliminate the ability of former employees to log onto your network. It is easy to delete their access and user privileges, but if you wait too long, you may give disgruntled ex-employees an opportunity to damage or steal files.

- **Create an e-mail and Internet use policy**

A recent study reported that 6% of all e-mail messages are infected with viruses or other programs that can damage your computers. Create a company-wide Internet use policy that includes instructions to employees to not open e-mail attachments they do not expect. The policy should also address risky online activities and forbid such practices as downloading free utilities and other programs from the Web. Instruct employees to not share passwords or account information if they receive an e-mail asking for them.

- **Require employees to use strong passwords**

Passwords that are easy to guess can enable unauthorized people to gain access to your network. To prevent this, your security policy should require that passwords contain both letters and numbers. And, while passwords should be changed regularly, avoid requiring employees to change them too often. If they struggle to remember their passwords, they may write them down and post them on their monitors, making it easy for others to break into your computer system.

### ***Hire Help***

These tasks are not extremely technical, but you may want to consider hiring a computer or network consultant to handle them.

- **Install a perimeter firewall**

While a software firewall protects the PC it is installed on, a perimeter firewall is a hardware device that plugs into and protects your entire computer network. A notable feature is that it enables you to close down network ports. Because network ports enable communication between client computers and servers, you can strengthen your network's security and thwart unauthorized access by closing unused ports. This step is more difficult to implement and you may want an expert to help set up your firewall functions correctly.

- **Secure a Virtual Private Network**

Linking offsite users to your company's network over the Internet enables them to check e-mail and access shared files. A Virtual Private Network (VPN) lets you do this more securely. However, there's a significant security risk any time you make your network accessible to outsiders. You will want to bring in a security consultant because getting a VPN working properly can be tricky.

- **Configure wireless security features**

Anyone within radio range of a wireless network has the potential to listen in or transmit data on the network. If you plan to use wireless networking, bring in an IT professional to ensure security features are activated and that wireless encryption and access control features are properly configured.

- **Create back-up and restore procedures**

This task can be as simple as burning a CD with your data files on it and then storing it in a safe place. Windows XP includes a tool to back up and restore data to your PC. However, you may want to look at a more sophisticated solution. If you need your data to be available at all times, you should work with an IT expert who can add hardware to your system that builds in redundancy, making duplicate copies of files on a different hard drive every time you save them. That way if one hard drive fails, the back-up system can step in and keep your data flowing. You should back up files at least weekly, and practice restoring data periodically just to verify that you can.

- **Configure database security**

If you have a database that stores customer, sales, inventory or other types of critical information for line-of-business applications, hire IT professionals to ensure that this information is well protected. For instance, a database expert can shield Microsoft SQL Server from most Internet-based attacks by only allowing authorized users to connect to the database. They can also create back-up systems to restore your data if it is lost.

## Chapter Two – Tips for Password Security

### *Overview*

Whether it's a few PCs or hundreds on your network, there's one thing that can separate your system from being compromised: a great password. Why? Hackers want access to anything and everything. If they can guess your user name and password, you might as well have given them your wallet and the keys to your building.

### ***Don't be complacent.***

Attacks can and do happen. Hackers are a devious bunch and will stop at nothing to get into your network and files. They use three different methods to get to you: brute force, dictionary attacks and social engineering.

**Brute force** is the most time-consuming method. Basically, it involves a program that tries every combination of letters, numbers and keyboard characters to guess your password. It starts with trying every character, and then tries two-character combinations and then three-character combinations and so on.

The longer the password is, the exponentially more difficult it becomes to crack. According to password experts, a password that is eight characters in length and utilizes lower- and upper-case letters, numbers and keyboard characters won't be cracked for two years. This underscores the importance of being as random as possible when choosing your password.

Another method of attack is through the use of **custom dictionaries**. These dictionaries are filled with words and names, but also number and letter combinations, such as 11111 and abc123. Simple passwords such as "duke" or "ilovemydog" can easily be guessed.

The third and most effective method of attack is **social engineering**. This involves someone with criminal intent soliciting a password directly from a user. Many people divulge their passwords to co-workers and strangers without even realizing it.

For example, most small businesses don't have a dedicated information-technology staff. A hacker posing as someone from your company's Internet service provider could call in and get an unsuspecting employee's password by "testing the service." The hacker might request the employee's user name and password to log in and test the connection from the ISP's end. If the hacker sounds authoritative and legitimate enough, your whole network could be compromised.

If your business rents space in a larger facility, strangers probably roam the hallways unnoticed. A few innocent questions or a watchful eye can be disastrous.

### ***Know what makes a bad password.***

Because the attacks described above are becoming increasingly more common, you don't want to use anything in your password that's personal and easy to guess. Keep in mind the following don'ts:

- Don't use only letters or only numbers.
- Don't use names of spouses, children, girlfriends/boyfriends or pets.
- Don't use phone numbers, Social Security numbers or birthdates.
- Don't use the same word as your user name, or any variation of it.
- Don't use any word that can be found in the dictionary — even foreign words.
- Don't use passwords with double letters or numbers.

Some of the worst passwords are: password, drowssap, admin, 123456, and the name of your company or department. Finally, never leave it blank. That's a surefire way to let the bad guys into your system.

### ***Get proficient at creating good passwords.***

A good password is one that is easy to remember but difficult to guess. That sounds like a paradox, but it's really not.

There are a couple of different ways to create difficult-to-crack passwords. One is substituting letters with characters and numbers. To make it easier on yourself, try to use numbers and characters that resemble the letters they are replacing.

For example, you would never want to use the word "password" as your password. If you change it to p@7sw0rd!, you've got something that would take some time to crack but is fairly simple to remember.

Another method is to use the first letters of the words in a favorite line of poetry or a verse of song. "Hail, hail the lucky ones, I refer to those in love" becomes "H,hTL0,IR2t1L."

The best passwords are at least eight characters in length and use a combination of numbers, keyboard characters and upper- and lower-case letters. The longer your password is, the longer it will take someone (or more likely, some program) to crack it.



### ***Safeguard your password.***

At first, it may be difficult to remember your password. Did you substitute an "i" with a "1" or did you use a "1" to represent "L?" Most people will want to write the password on a piece of paper and place it underneath their keyboard or mouse pad. Or worse, they'll stick the password right on their monitor.

To help remember the password, use it immediately. Then log in and out several times the first day. Just don't change it on a Friday or right before leaving for vacation. You could write it out several times on a piece of paper. This helps record it in your mind. Just be sure to shred the paper when done.

Invariably, there may come a time when a password has to be shared. Let's say an employee is out of town to give a presentation but left the PowerPoint file on his desktop. You will have to get his user name and password to access that file. After you open the file, change the password and give him the new password upon his return. Then, as soon as the person gets back into the office, have him change the password again. Yes, it's a lot of work but well worth it.

### ***Change your password often.***

Your network administrator can force your employees to change their password every so often. By default, passwords are set to expire every 42 days in Windows Server 2003. Microsoft recommends having users change their passwords every 30 to 90 days, but encourages you to go with the smaller number. I think 30 days is a reasonable number here. You always want to side with caution when it comes to sensitive information.

Encourage your employees to change their passwords to personal Web sites as well — such as to banking, Internet e-mail accounts, shopping sites, and so on. Advise them not to use the same password for all of their sites. A particularly good hacker can cause personal financial ruin by gaining access to one username and password.

Juggling all of these passwords is not easy. You might want to consider a program that can do all of this for you. There are many free and for-purchase programs available on the Internet that will help you in doing this.

## Chapter Three – Shield Your Network from Clever Hackers

### **Overview**

You've got antivirus software and firewalls guarding your computers and routers. You religiously download security updates. You've done everything you can think of to stay secure. But your network is still at risk. Why? An employee could unwittingly give away the castle's keys.

The biggest threat to a computer is not a hardware or software problem. It's social engineering. What it boils down to is this: Someone will attempt to gain an employee's trust. Information can be elicited from that employee that puts everything at risk. Social engineering relies on the fact that most people are nice. They want to be helpful. There's a natural inclination to lend a hand when someone has a problem.

These efforts can be conducted over the telephone, via e-mail, or through instant messaging. Larger organizations are especially at risk, because employees do not know one another, but small businesses can be victimized too. Anonymity is important to the hacker. But the little fish at a company can also be "gamed."

### **Social Engineering Tactics**

#### **The caller isn't working on your network.**

One of your newer employees gets a call from a computer repair technician. "My name is Joe Smith," says the technician. "Your company's network is having problems, and I'm working on it. I need you to type in some commands." On the face of it, this is silly. Any legitimate repair tech is going to have access to the network, if that's what he needs. How else could he fix the thing?

The caller is playing on your employee's natural desire to be helpful. The employee is unlikely to understand the commands he is asked to enter. They may expose the structure of the network, or open a security hole.

The caller then asks the employee to enter commands that identify his desktop computer. "Aha," he says. "That's the machine that has been causing the problems. I'll need your username and password."

Once the caller has collected this information, you could have an identity theft problem. He has a route into your system and he knows how your network is structured. If you have a database of customers and their credit card numbers, he may download it. Or he could get into your payroll system where he will find Social Security numbers and bank accounts.



If your business is large enough, the caller could claim to be from the in-house IT department. Either way, the result is the same.

What to do? Train your employees to never, ever give out information to such callers. Computer repair personnel already have access to the network. If they don't, there's probably a good reason. And they should already have a password with system privileges. They don't need an individual employee's password. At the very least, employees should check with a supervisor before disclosing sensitive information.

### **That e-mail isn't from Joe.**

One of your employees gets an e-mail. It's from her friend Joe. It has an attachment. Without giving it much thought, she opens the attachment. It's something unappealing, so she deletes the e-mail and forgets it. Unfortunately, that attachment includes a Trojan horse. Your antivirus software should whack it but maybe you haven't kept the antivirus software up-to-date like you should. The Trojan could use a backdoor port in Windows to download more dangerous programs. These programs could find their way around your network, digging for credit card and Social Security numbers.

Employees should **never** open attachments they were not expecting. Legitimate return addresses are easily stolen by worms. The fact that the e-mail bore Joe's return email address is meaningless. If your employee wasn't expecting something from Joe, she should have checked with him before opening it.

### **When the hackers go "phishing," don't take the bait.**

An employee gets an e-mail message that his eBay (or PayPal, Citibank, America Online, etc.) account has a problem. He's told that he must go to a certain page for more information. The spam includes a link. When he clicks the link, a page with the company's logo opens. It explains that his account will lapse unless he re-authorizes it. It then asks for his username and password. Or it may ask for a credit card number, or perhaps a Social Security number. Sometimes, it requests his mother's maiden name (often used as a hint to get a password restored).

Recently, the web pages have become much better designed than the past so it makes it harder to tell that they are fakes. And the pages often contain the logos of eBay or other companies. You'll find links to the company's real pages. It's easy to be suckered.

So remember this: eBay isn't going to ask for a password. Neither will AOL or any other legitimate company. Delete all spam, including these pitches.

What, you may ask, does an eBay password have to do with my business? Just this: People often use the same password for everything. So the eBay password may also give access to your network, a bank account and other confidential areas.



### **Protect your company.**

A good security system will protect you technologically and socially. Your employees are there to do a job. They're probably overburdened, so they'll resist worrying about security. But you must train them never to give out sensitive information, unless they are certain of the caller's identity, and never to open an attachment they were not expecting. (Do you think passwords are safe? In a London study, passersby were asked at random to give up their passwords in exchange for a candy bar. Seventy percent complied!)

But even the best-trained employees can be suckered. The desire to be helpful can lead them down the garden path. Assume your system eventually will be invaded; keep critical information walled off from most employees. Only those with a real need should have access to databases or payroll information.

Even if a worm gets into your system, it can be thwarted. If you religiously update your antivirus software and Windows, worms can be knocked out or blocked. Be sure the firewall in your router has been activated and properly configured.

Worm and virus technology is rapidly growing in sophistication. Coupled with social engineering problems, the threat to your company is very real. You must stay alert.

## Chapter Four – Tighten Wireless Network Security

### **Overview**

Your wireless network is humming along. Your employees feel wonderfully un-tethered as they walk around the office exchanging ideas. Productivity is up. You wonder how you ever got along without Wi-Fi. Hold on. You might also be exposing your business to unseen dangers.

Ask the pros to name the top three mistakes small businesses make when it comes to wireless networks, and they'll tell you: Security, security, security.

"An unbelievably large number of small businesses install Wi-Fi networks in their facilities, but fail to change any of the factory default configuration settings on the wireless access points," says Greg Murphy, the chief operating officer for AirWave Wireless Inc., a San Mateo, Calif. network-management software company. "Since most access points have security settings disabled by default, this amounts to issuing an open invitation for intruders to connect to your network."

These mistakes can seriously hurt your company. Just ask the managers at the Lowe's store in Southfield, Mich., where hackers in 2003 reportedly tried to break into the home-improvement chain's customer database using a laptop and a wireless card. Three men pleaded guilty in the security breach that the company says cost it more than \$2.5 million.

Indeed, according to the 2004 Computer Crime and Security Survey published by the Computer Security Institute, overall financial losses from security breaches at the 494 companies polled — including those perpetrated via wireless networks — totaled \$141.4 million in the 12-month survey period. That represents a drop from the previous year's losses, but it is still roughly \$300,000 per company.

### **Strategies to Keep Your Wireless Network Safe**

#### **Assume you already have a problem.**

"A CEO shouldn't make the 'Three Mile Island' mistake," says Mike Klein, the chief executive for Interlink Networks, a wireless network security software company in Ann Arbor, Mich. "Don't assume the probability of an incident is low, and then ignore it. It's important to understand that most security breaches go undetected. A hacker who can freely access your network, or monitor your network traffic, is likely to do so undetected — reading confidential information and gaining competitive advantages over the airwaves."



There are a number of useful intrusion-detection applications, from stand-alone solutions such as the open-source Snort ([www.snort.org](http://www.snort.org)) to Windows Small Business Server's integrated intrusion-detection mechanisms, which can alert you when a specific attack is launched against your network.

### **Get a security policy in place.**

"If a business has deployed wireless, they must take the necessary steps to make sure it is secure," says Mike Peters, director of consulting for Calence, a Tempe, Ariz., networking company. "If a business has not deployed wireless as part of its IT infrastructure, the chances are pretty good that someone in their organization has installed a wireless access point for their own convenience. The first step any organization must take is to develop a comprehensive security policy document."

For details on how to write an effective security policy document, you might want to either hire a consultant or check out some of the literature available online.

### **Build a wall, not a quilt.**

Many security issues happen because you buy hardware and software from multiple sources, which is more likely to result in a quilt security solution instead of the wall that you want. "When installing a wireless network, most small businesses don't realize the importance of sticking with one vendor across the board," says Josh Radlein, a wireless systems engineer for CDW, a provider of technology products and services in Vernon Hills, Ill. "Problems can arise when mixing various vendor products, causing weak areas prime for security attacks."

Tip: Obviously, sticking with one vendor can solve the problem. But is it working? Try downloading the Microsoft Baseline Security Analyzer, which scans single systems or multiple systems across a network for common system misconfigurations and missing security updates.

### **Crank up your settings.**

"Wireless Encryption (WEP) should be turned on and set at the highest level," advises Gary Miliefsky, chief executive of PredatorWatch, a Chelmsford, Mass. security management company. "Administrative user name and passwords need to be changed immediately and frequently." (He says this will at the very least slow the wireless hackers down and act as a deterrent to casual cyber-thieves.)

Even with your settings turned up, you still need to make sure you get your latest patch or firmware upgrade for your wireless router. If possible, buy one that comes with a built-in firewall and learn how to use it and properly configure it.



**Don't be afraid to take drastic measures.**

Anil Khatod, president of AirDefense, an Atlanta wireless network security firm, says that 30% of his clients have determined wireless networks to be so risky, that they don't have them. "But even if you keep employees from using wireless, you still want to track rogues in your air space," he says. Where? They can pop up anywhere, from wireless-enabled laptops accessing your network through conventional means to PDAs, cell phones, printers and even barcode scanners. Several businesses have banned or limited cell phone use at work — a radical solution, yes, but if you're worried about the safety of your network, it's one worth considering.

There are other steps you can take, short of unplugging your network, which a professional can assist you with. They include using encrypted e-mail, switching to a more secure protocol, hiding your access points' service set identifiers (SSID) and requiring authentication between a device and an access point.

Wireless network security isn't the kind of problem that will go away if you ignore it. Odds are that if you haven't thought about it, it's already an issue. But there's a way to address this through careful planning, conservative software and hardware configuration and outside-the-box thinking.

## Appendix of Online Tools

### Overview

Note: Although Fastpay is providing this information as a service to its clients, it is in no way endorsing or providing any warranty or support on any of these software products. This is merely a list of tools that may help in fulfilling network security best practices but is by no means all-inclusive.

More information on securing your small business network can be found online at: <http://www.microsoft.com/smallbusiness/resources/articles/security-privacy.mspx> .

### Anti-virus

#### AVG Anti-Virus – FREE

- Great antivirus software that can be set to automatically update itself every day. And it is free to download and use indefinitely!

Link: <http://free.grisoft.com>

#### Trend Micro – Purchase/FREE Online Scan

- Very reliable anti-virus software that can be purchased for your PC and for your servers. They also provide a free online scan that you can use to check your PC for virus infections.

Link: <http://housecall.trendmicro.com> <http://www.antivirus.com>

### Anti-Spyware

#### Microsoft Defender – FREE

- Anti-spyware software that automatically updates itself. Free to download and use. (This is included in Windows Vista.)

Link: <http://www.microsoft.com/athome/security/spyware/software/default.mspx>

#### Spybot Search & Destroy – FREE

- Anti-spyware software that allows for more advanced protection. This may be a little complicated for novice PC users.

Link: <http://www.safer-networking.org/en/download/>



## **Software Firewall**

### **ZoneAlarm Personal Firewall – FREE**

- The best rated firewall software on the Internet.

Link: <http://www.zonelabs.com/store/content/company/products/zna/m/freeDownload.jsp>

### **Windows Firewall – FREE**

- If you have Windows XP or Vista then you already have this software. Go to the link to read how to make sure you have it enabled.

Link: [http://www.microsoft.com/windowsxp/using/security/internet/sp2\\_wfintro.mspx](http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx)

## **Software Update Tools**

### **Windows Update – FREE**

- If you have Windows (any version since and including Windows 98) you can use this free online service to update your PC. You should visit this site often. If you have Windows XP or Vista follow the directions on the site to enable automatic updates. Then you can “set it and forget it”!

Link: <http://update.microsoft.com>

## **Vulnerability Scanning Software**

### **Microsoft Baseline Security Analyzer – FREE**

- This utility can scan all the PCs on your network (or just your own PC) for any security vulnerabilities. It will compile a report of these vulnerabilities and tell you exactly how to fix them. This is a network administrator’s “must-have”.

Link: <http://www.microsoft.com/technet/security/tools/mbsahome.mspx>

### **Shields Up! – FREE**

- This utility scans your firewall from the outside to see if there are any vulnerabilities that you may need to take care of. This site offers many other free security tools that you may be interested in.

Link: <https://www.grc.com/x/ne.dll?bh0bkyd2>