



Interested in learning more about security?

## SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

### Homeland Security Starts at Home - Security for the Home Computer User

This paper is intended to educate the average home computer user who uses the Internet but is not a computer expert. The content is presented in an easy to read format that is not overly technical or filled with computer jargon. Rather than being a complete and comprehensive "how to" for home security, the material presented in this paper will give you an introduction to the topic of home security and outline what steps you need to take to start securing your home computer. The topics that will ...

Copyright SANS Institute  
Author Retains Full Rights



AD

Streamline IT security environments  
and compliance processes.



## **Homeland Security Starts at Home – Security for the home computer user**

Michelle Johnston

GSEC Practical Assignment Version 1.3

March 25, 2002

### **Introduction**

This paper is intended to educate the average home computer user who uses the Internet but is not a computer expert. The content is presented in an easy to read format that is not overly technical or filled with computer jargon. Rather than being a complete and comprehensive “how to” for home security, the material presented in this paper will give you an introduction to the topic of home security and outline what steps you need to take to start securing your home computer.

The topics that will be covered are:

1. Why you need to be concerned about computer security.
2. Password security.
3. Virus and worm prevention.
4. Firewalls.
5. Security patches.
6. Data backup.
7. Testing your security.

### **Why do I need to be involved in Homeland Security?**

Many home users don't feel computer security is a concern for them for various reasons:

1. I don't have an always-on connection to the Internet such as DSL or a cable modem.
2. I don't purchase anything on the Internet, so I don't have anything to worry about.
3. I don't have a business, own real estate, or have any other assets anyone would be interested in.
4. I don't telecommute.
5. I have anti-virus software installed on my computer so I'm already secure.

Since September 11, 2001, security has been in the headlines and on the minds of most Americans. Unfortunately, when most people think of security, they think of the national security the government needs to provide to protect its citizens, the security their employer needs to provide in order to protect their assets, the car alarm on their car, or the home security system in their house. The average

person with a single computer or a very small home network of computers usually does not think they need to be concerned about cyber security, mainly for the reasons stated above. This is simply not the case.

If you connect even a single computer to the Internet for any reason for any amount of time, you need to be concerned about computer security. Why? Because once you connect to the Internet, you become part of the global information infrastructure. In the wake of the recent terrorist attacks, many people, including our government, are starting to realize that the security of our infrastructure needs to become a top priority.

America's information infrastructure is a source of both great strength and considerable vulnerability. The President recognizes that modern information technology is essential not only for making our Nation more prosperous but for making our homeland more secure. The President has launched a long-term program for using advanced information management technology to better protect the Nation. At the same time, the President's 2003 Budget requests significant funding for cyberspace security, an essential new mission for the 21st century given our growing dependence on critical information infrastructure, most importantly the Internet (The White House).

The government needs to be concerned about cyberspace security because most government offices, businesses, and facilities providing critical infrastructure services such as gas, water, and electrical power are all interconnected via the Internet. The average home computer user needs to be equally concerned because when they connect to the Internet, they become part of this interconnected infrastructure.

Imagine a terrorist electronically targeting our electric or water systems causing outages that would leave millions of people without water or electricity. Now imagine that your computer, because you failed to properly secure it, was part of this attack. Such an attack may sound far-fetched, however, a recent report issued by the Canadian Office of Critical Infrastructure Protection and Emergency Services suggests the following:

Despite bin Laden's use of telecommunications-deprived Afghanistan as his base of operations, the Canadian study doesn't rule out the possibility of al-Qaeda agents or sympathizers in other countries carrying out sophisticated and coordinated cyberattacks against critical infrastructure facilities, such as the U.S. telecommunications grid, electric power facilities and oil and natural gas pipelines (Verton).

In a recent roundtable discussion regarding the upcoming release of the President's Critical Infrastructure Protection Board's strategy for protecting the nation's network infrastructure, the following was revealed:

"We have audited a major airline and with just a browser, we were able to get into the reservation system and access the passenger manifest," Sanctum CEO Peggy Weigle says. "We audited a major utility grid, and we were able to get to the maintenance schedules. So you can have cyberattacks actually influencing physical security" (Marsan).

As you read this paper, I will show you some of the computer security issues the home user needs to be concerned about and the reasons they need to be concerned about them. You will learn why "risk assumed by one is shared by all (The SANS Institute. "Security Essentials Day 2: Threat and the Need for Defense in Depth," p.29)" and how you can become a better Internet neighbor and protect yourself by reducing these risks.

## **Passwords**

Most home computer users don't use a password to log into their operating system. Some may use a password if the entire family uses the computer and each user wants their "preferences" saved. However, the passwords used are typically weak since most people don't consider their family members a high security threat. While this may be true, the use of a weak login password usually trickles down to other areas in which you use a password. The reason for this is that most people tend to use three or less passwords for everything – their login account, their eBay account, their Yahoo account, their online banking account, etc. This means that if someone is able to figure out the password to any one of these accounts, they now have access to all of your accounts. A situation that I was in not too long ago illustrates this point.

Last year a friend of mine talked me and another friend into joining an Internet fantasy football pool (let's call her Green Bay Fanatic or GBF to protect her identity). Each week everyone would pick the teams they thought would win and whoever picked the most winners would win. Week after week GBF would win. My other friend (let's call her San Francisco or SF) and I got tired of losing, so we thought we would play a joke on GBF. SF knew GBF's stock account password because they were learning to trade stocks together. So, we tried that password on her Internet football account and sure enough, it was the same. We logged in and reversed all her picks for that week. We could hardly contain ourselves when we saw her later that day. When we got her to log into her account, you should have seen the look on her face! To this day we all still laugh about it.

It's true that the situation above was all fun and games and we even let GBF in on the joke before the games started so she could change her picks back. However, if some seedy character were able to get GBF's Internet football account password, they would then have access to her online stock account. Imagine the look on her face if she were to log on and see a zero balance.

The moral of this story is that you should always try to use strong passwords and you really should try to use different passwords for each of your accounts. Passwords are one of the most basic forms of security and, in some cases, they are the ONLY form of security being used.

### **Passwords – What Should I do?**

Use a different password for each of your accounts. I try to use a different password for each online account. Also, I don't use my computer login account username or password for any online account. I'm sure you are thinking I must be out of my mind to suggest that you have dozens different passwords. How in the world would you remember them all?

There are a couple of things you can do to make managing all of these passwords easier. You can keep all your online login usernames and passwords in a small notebook in your desk drawer. When you need to log into one of your accounts, simply refer to the notebook. NOTE: I do not recommend doing this at work where everyone, including the janitorial staff, has access to your work area. While it is true that if someone broke into your house and stole your notebook, they would have access to all your online accounts, this is still better than using the same username and password for every online account. If you go this route, I would suggest storing a copy of the password list in another, more secure, location so you could change them all if your notebook went missing – perhaps a fireproof safe where you could also store other important documents.

Another option would be to use a program to keep track of all your passwords. Since it is generally not advisable to write down your password, this option would be considered a better choice than the one above. An example of a program you might use is Counterpane's Password Safe [4]. This program is free and allows Windows users to keep their passwords securely encrypted on their computers. You can even have Password Safe generate a random password for you. This method is similar to the "notebook in your drawer" method with these added advantages:

1. The passwords are stored electronically and encrypted. Encryption is the process of converting "plain text" into a form called "cipher text." If you were to look at this cipher text, it would appear to be a huge mass of

- jumbled characters – not something you would be able to read. Since this encryption conceals the original data and prevents it from being used, it adds a layer of security.
2. You only have to remember one password – the password that allows you to access the Password Safe database containing the rest of your passwords.
  3. You can back up the database and keep it in a secure location. Should the database become corrupt or someone steals your computer, you still have a copy of all your account and password information. In the case of a theft, the password database on your system is encrypted and the thief would have to figure out the password to the database in order to gain access. Even if the attacker could eventually gain access to your password database, you will have had time to go to another computer and change all your passwords using the information in your backup.

This is a very easy way to keep track of each account's username, password, and any comments you want to add. It also makes it easy to make changes to any of this information.

Use strong passwords. By this I mean passwords that are hard to guess and can't be found in the dictionary. The reason you shouldn't use any word that can be found in the dictionary is because attackers often use automated programs to launch what's called a "dictionary attack" on your password file. This type of attack goes through a file that contains words from the dictionary and tries these words against your password. If your password can be found in the dictionary, it will be cracked in a very short amount of time. At a large technology company where password policies were in place, LC3 obtained 18% of the passwords in 10 minutes and 90% of the passwords were recovered within 48 hours [7].

When I ran LC3 on my company's network, it took only a few seconds to crack passwords that were words from the dictionary. The fact is, given enough time and resources, any password can be cracked. The objective is to make your password hard enough that it takes more time than is worth the effort to crack it.

A few other things you should remember are:

- Use a password that cannot be easily guessed. You should not use the name of one of your pets, kids, or spouse as a password, even if you add a leading or trailing number or special character. Other things that fall into the "easy to guess" category would be your birthday or the birthdays of your family members, your favorite sports team, or any other well-known information about yourself.
- Keep your password secret. Don't ever tell anyone your password for any reason. Remember my Internet football example earlier in this paper?

- Use a password that is at least seven characters long. If your password is too short, then it will be easy for a password-cracking program to try all possible character combinations. For technical reasons beyond the scope of this paper, you should use a password that is exactly 7 or 14 characters long if you are using Windows 2000 or earlier.
- Use a combination of upper and lower-case letters in addition to numbers and special characters.

So, how do you create a password that meets all this criterion yet is something you can remember? One way is to use something called a “passphrase” instead of a word. Think up a phrase that you can remember and then throw in at least one number, at least one special character, and use both upper and lower-case letters. For example:

The 2 best things about me; I'm a genius and good looking!

You might as well say something positive about yourself, right? Anyway, you can now use this passphrase to create the following password:

T2btam;lagagl!

That looks like a really crazy password that no one would be able to remember. However, it's simply the first letter of each word in your passphrase including punctuation. You use the same case, upper or lower, as you would if you were writing out the sentence completely. Since you, and only you, know what your passphrase is, the password will be secure. Most importantly, since it's just a bunch of letters, numbers, and special characters strung together, it will be hard to crack. As I said earlier, your password will never be impossible to crack, but you will have greatly increased the amount of time needed to crack the password, hopefully to a point that makes it not worth cracking.

### **The Virus and Worm Threat**

Almost everyone has anti-virus software installed on his or her computer. However, many home users are not aware of the proper use of anti-virus software. I've heard many friends say to me, “Anti-virus software came pre-installed on my computer, so I'm safe.” When I ask them how often they update their anti-virus signatures I usually get a strange look and an answer of, “My what?” I then explain to them that using anti-virus software without updating the signatures on a regular basis is pointless. It would be like tossing a net with a large hole in the ocean to catch fish. You would probably catch some fish, but a good number of them would escape through the hole.

A computer virus is similar to a biological virus in that it replicates and spreads from individual to individual [8]. Some viruses may seem harmless in that they do not do any damage to your files, but there is a cost to these so-called harmless viruses. A lot of the mass-mailer viruses that do nothing but email themselves to everyone in your address book and then to everyone in the address books of those people, do have a cost associated with them:

1. There is a loss of productivity associated with cleaning up the virus. End users may have to give up their computer for a time so that the virus can be removed. In addition to the productivity loss, there are costs associated with having one or more Information Technology staff clean up the virus and stop it from spreading. All this tech time being used to combat the virus could have been time spent doing something more productive.
2. There could be a loss of productivity in terms of Internet access times if the virus is widespread, thus taking up Internet bandwidth.
3. There is the possibility of productivity loss at any organization with an internal email server if their email server goes down due to the increased load caused by the virus. This is what is commonly referred to as an “availability attack” – bringing a system completely down or overloading it so much that it cannot respond to legitimate requests. Thus, the system is not “available” to the users that need to access it for legitimate purposes.

Maybe you are wondering why a paper on “home” computer security is giving you information about losses at an organization due to virus infection. This goes back to the introduction where I mentioned that you are part of a global community when you are on the Internet. If you get a mass-mailer virus at home and you spread it to everyone in your address book, there is a good chance that some of the email addresses in your address book are “work” email address, not just “home” email addresses. Thus, when you don’t follow safe computing practices, don’t use anti-virus software, and/or don’t update the signatures to your anti-virus software, you are directly contributing to all three of the problems listed above.

This seems like a good time to tie all this security stuff into the “homeland security” theme I outlined in the beginning of this paper. Remember the Code Red worm? Among other things, this virus was set up to launch a Denial of Service attack against [www.whitehouse.gov](http://www.whitehouse.gov) between the 20<sup>th</sup> and 28<sup>th</sup> of the month [9]. Although this deliberate attack on the U.S. government was not targeted at a critical infrastructure system such as the electrical grid or our water supply, it does illustrate the fact that it could have targeted one of these systems. You may be saying to yourself that your computer couldn’t have been part of the attack on whitehouse.gov because you are not running a server and you are not running IIS. However, if you are running Windows 2000, you may be running IIS

and not even know it; this is because many applications install IIS without the user's knowledge [10].

The SirCam worm taught us that you can't always trust an email attachment even if it comes from someone you know and looks like it might contain information relevant to you. Because SirCam takes a file from the hard drive of the infected user and uses the name of that file in the subject line, it might appear that someone you know is sending you a legitimate file [11]. Unless you are certain the sender intended to send you this file, you should not open it. A good precautionary measure would be to call the person or send them an email to verify whether the file was intentionally sent.

Maybe you practice "safe computing" and never open an email attachment unless you are certain it isn't a virus. This practice, which is a good one, will protect you most of the time, but not 100% of the time. The Wscript.KakWorm, discovered in December 1999, exploits a known Microsoft Outlook Express security hole. A user's PC can get infected without having to open an email attachment; simply reading the email message causes the system to become infected [12].

You probably already know that you can prevent your computer from virus/worm infection and keep from infecting others by installing anti-virus software. The most important thing you need to know is that you are not protecting yourself for long by just installing the software -- you need to update your virus signatures on a regular basis in order for your anti-virus software to be effective. The virus signatures are essentially a database of known virus and worm patterns. If you don't have the most recent list of patterns, then your database won't recognize any of the newly released virus/worms and, thus, won't be able to protect you against them.

There are several good anti-virus software packages on the market, but my favorite is PC-cilin by Trend Micro ([www.antivirus.com](http://www.antivirus.com)). It's easy to install and configure. It has a scan wizard to guide you through the process of scanning files on your computer. It has a scan manager that gives you the ability to schedule specific scans. You can set up web security and filtering. You can also set up email scanning so that PC-cilin scans your email for viruses as it's being downloaded. The feature I like the most, though, is the fact that PC-cilin automatically checks for updated signature files when I turn my computer on. This keeps me from having to remember to manually update the signatures and I know that I always have the latest pattern file.

According to the International Computer Security Association, more than 10,000 viruses have been identified and 200 new ones are created every month [8].

Those are staggering numbers that should illustrate to you the importance of using anti-virus software and keeping the signatures up to date.

## **Firewalls**

If you have made it this far, it should be clear to you why it is important to secure your home computer. Installing a firewall adds another layer of protection and is a must for any computer connected to the Internet. Going to bed and leaving the front door to your house wide open is equivalent to connecting your computer to the Internet without a firewall. Think of a firewall as a barrier between your computer and the Internet. It controls what comes in from the Internet and what goes out to the Internet. If set up correctly, a firewall can protect you from many types of attacks.

There are various types of firewalls with different features and abilities. A corporation might choose one type of firewall over another for various technical reasons, all of which are beyond the scope of this paper. What the average home user is most likely concerned about is:

1. Is the firewall easy to install?
2. Is the firewall easy to configure?
3. Is the firewall going to do what it's designed to do and protect my computer?
4. Is the firewall affordable?

Most firewall products on the market, both hardware and software versions, are going to give you some measure of protection if configured correctly. No firewall on the market will protect you from everything. So, you can be reasonably sure that whatever product you choose, it will most likely meet criteria three above. As for criteria four, there are several free firewall products on the market that are very good. Two of the free firewall products that I use are Tiny Personal Firewall by Tiny Software ([www.tinysoftware.com](http://www.tinysoftware.com)) and ZoneAlarm by Zone Labs ([www.zonelabs.com](http://www.zonelabs.com)). They both meet all four of the above criteria – they are both easy to install, easy to configure, do what they are designed to do, and are as affordable as you can get.

## **Security Patches**

Security patches are another essential element to a secure PC. Similar to patching a hole in your wall to keep out air, applying security patches to your computer keeps attackers from taking advantage of known vulnerabilities. If you don't patch the hole in your wall, cold air, rain, and numerous other things can get in. If you don't patch the "holes" or "vulnerabilities" in your operating system

and applications, attackers can “get in” or “gain access” to your computer and take advantage of these vulnerabilities.

I’m behind a firewall, why do I need to put patches on my system? “The best way to think of a firewall conceptually is like an umbrella. When you use an umbrella, it keeps a lot of the rain off of you, especially your head. However, some of those raindrops get through the perimeter defense (The SANS Institute. “Security Essentials Day 1: An overview of the information risk management framework,” p.22).” Thus, the best thing to do would be to eliminate the vulnerability by fixing or “patching” the problem. Once again, you are adding another layer of defense. If for some reason your firewall doesn’t stop an attack meant to exploit a known vulnerability, but you have patched your system for that particular vulnerability, then the attack will not be successful because your system is no longer vulnerable to that particular attack.

“It is estimated that 3,000 new vulnerabilities were announced during 2001, with more expected in 2002 (Symantec Corporation. “Is Patching a Priority for Your Enterprise?”).” There is a gap between when a vulnerability is discovered and when a patch is available for that vulnerability. During that gap, a hacker may be able to gain access to vulnerable systems. However, most attacks, viruses, and worms take advantage of vulnerabilities that 1) have been around for quite some time and 2) have patches available to fix them. This means that many of the virus and worm outbreaks of the past wouldn’t have happened if everyone kept their systems patched.

### **So what do I need to patch?**

You need to patch your operating system and you need to patch the applications you run on your operating system, such as Internet Explorer and Microsoft Office. Newer operating systems such as Windows XP are designed to check for patches/updates and notify you if any are found. You can then decide if you want to install them. On older versions of Windows, the easiest way to keep your system up-to-date on patches is to visit [windowsupdate.microsoft.com](http://windowsupdate.microsoft.com) on a regular basis. You may even have an icon for Windows Update on your start menu. Different versions of Windows will require different updates, but the information at Microsoft’s update site is pretty easy to understand.

Examples of non-Microsoft applications that should be patched include your anti-virus software, firewall software, and any finance software you use to do online banking. Some applications such as ZoneAlarm and PC-cilin will automatically check for updates. Other software vendors give you the ability to sign up for email notification of product updates. In either case, keeping up-to-date on operating system and application patches is a very important aspect of good computer security.

## Backup Your Data

Backing up your data is a task you should perform regardless of whether your system is secured. As far as security is concerned, this is your last line of defense. If someone gains access to your system and deletes your files, you will need to restore them from backup. However, the evil Internet hacker is not the only threat to your data. Your computer could be stolen, damaged in a fire, or your hard drive could crash. In all these cases, the only way to get your data back is from a backup.

There isn't a need to back up your software applications, such as Microsoft Office. If your computer crashes or files are deleted, you can always re-install the applications from the original program CDs. The same holds true for the operating system itself. What you want to back up on a regular basis are your data files – your Word and Excel files, data files from your financial programs such as Quicken, your email, etc. To make it easy on yourself, you might want to keep all your data in one location. For example, I keep all my data within sub-folders in the “My Documents” folder. When I want to do a backup of all my data, all I have to do is copy the “My Documents” folder to zip disk.

There are many different methods of backing up your data and several types of media you can back up to. What you use really doesn't matter – use what you are most comfortable with. The point is that you need to back up your data on a regular basis. How often you back up depends on the frequency your data changes. If you use your computer every day and you add, delete, and change files every day, then you may want to back up on a daily or weekly basis. If, on the other hand, you mostly use your computer to surf the Internet and don't have a lot of data that changes on a regular basis, then maybe backing up your data once a month is good enough.

Another factor to consider when deciding how often to back up is the importance of your data. If someone walked off with your computer today, could you live without the data that was stored on it? Well, technically you would live, but how hard would your life be if you had to recreate all the data from scratch. Would it even be possible to recreate the data? At the very least, it would be a big inconvenience.

Finally, keep your backup in a safe place. If your computer were destroyed in a fire, your backup wouldn't do you much good if it was sitting in a desk that was also destroyed by the fire. The best place for your backup is in a fireproof, waterproof safe at a location different from your computer. This might not be possible for everyone, but at the very least, you should be able to purchase a small, inexpensive fireproof safe and keep it somewhere in your house other than

right next to your computer. As with the other topics in this section, where you keep your backup media is a personal preference that will be different for everyone, but you should take some measures to ensure the safety of the media so it will be available in the event you need to do a restore.

## **Test your Security**

Now that you have taken steps to secure your computer, you should test your security on a regular basis. At a minimum, you want to test your security after you install new programs or install patches/updates to existing programs. Since the installation of software can potentially change the configuration of your computer, it is possible that these changes have affected your security. If you install software onto your computer on a regular basis and you always check your security after you do the install, then you are most likely checking it on a consistent enough basis. If, on the other hand, you rarely install applications and you are not consistent about installing patches and updates, then you might want to put a reminder on your calendar to check your security on a weekly or monthly basis. Security is not something you can set up and forget about -- it requires constant attention.

### Testing your passwords

If you wanted to test the strength of your passwords, you could purchase a program such as LC3, which will attempt to “crack” the passwords on your computer or network. You can get a 15-day trial so you can try before you buy [7].

Running LC3 is easy even for the novice user if you use the wizard, which will walk you through the process; you answer a few questions and you are on your way. If you are just testing your own computer, you will want to select the option to “retrieve from the local machine.” You then choose an auditing method of quick or common; the trial version will not let you do a brute force audit. I would recommend choosing the common password audit. You then choose the reporting options you want. I would select everything except “display encrypted password hashes.” The password hashes are just going to look like a bunch of characters strung together and will just clutter up your report. Click finish to begin auditing and you are on your way. When LC3 has finished its audit, it will display a dialog box with usernames, type of password, an indicator if the password was less than eight characters, and how long it took to crack the password if it was indeed able to crack it. You may also find that you had accounts on your machine that you didn’t know about.

Admittedly, most people are not going to bother paying for a password-auditing program just to test the passwords on their home machine, especially since it

can't test the strength of all your online passwords. This type of auditing is most useful for companies that want to make sure their employees are following the organization's password policies, but may be of interest to those curious about how long it would take a password cracking program to crack their password. In the password section above, I stated that any password could be cracked given enough time. The trial version of LC3 may not be able to crack your password, but if you purchase the full version and run a brute force audit, it will eventually crack your password. This is more of a curiosity item rather than a huge breach of security. If your password can withstand the LC3 common audit, then you are most likely following the password guidelines outlined above.

There are other password-auditing programs to choose from. Do a search from your favorite search engine on "password auditing" or "password cracking" and you will come up with thousands of hits. There are also companies that offer password recovery services to people who forgot their password to a program or a file such as a Word or Excel document; for example, [www.lostpassword.com](http://www.lostpassword.com) and [www.passwordbusters.com](http://www.passwordbusters.com).

### Testing your anti-virus software

This is pretty simple. There is something called an EICAR test file that you can use to test any anti-virus program [14]. You can download this test file and run a scan. If your anti-virus software detects the file as being a virus, then it is working properly. If you have real-time scanning turned on, your anti-virus software should warn you that it detected a virus when you click on the file to download it. If you do a search from your favorite search engine for "EICAR test file," you will find thousands of sites to download from. Also, don't forget to make sure you have the latest signatures. Look at the version you are currently running and compare it to the latest version on your vendor's web site. If they are the same, you are in good shape. If they are different, then your automatic update function isn't working or you are not updating the signatures on a regular basis.

### Testing your firewall

There are several Internet sites that will test your firewall. If you do a search for "testing your firewall," you will come up with thousands of hits. Listed below are a few of your options.

You can go to [www.auditmypc.com](http://www.auditmypc.com) and run a free firewall test and port scan. Click on the "Firewall Test" link and you will be presented with three different tests you can run – a "Basic" test, a "Trojan" test, and an "Info" test [15]. I recommend running all three.

Another interesting site you can use to test your firewall security is [www.hackerwhacker.com](http://www.hackerwhacker.com). If you have not visited this site before, you will need to enter your email address and press the scan button. You will then be emailed a passcode that will allow you to perform a scan on your machine. This verification process is meant to prevent unauthorized scanning of machines that are not yours. Warning: You will not be able to use a free webmail account such as Yahoo or any other email account from a domain that allows users to create an account without proper identification [17].

Gibson Research Corporation ([www.grc.com](http://www.grc.com)) offers a free Internet security checkup via its ShieldsUp! program. Simply follow the links to the ShieldsUP! page and click on the "Test My Shields!" or "Probe My Ports!" button to begin testing [18]. You should run both tests. After scanning your system, you will be presented with the scan results in plain English. Most of the site is designed for the average computer user and they offer some other interesting tools, so you might want to check out some of their other utilities while you're there.

### Testing your patches

You don't actually "test" a patch, you test for the presence of the patch on your system. If you are visiting the Windows Update site on a regular basis or your computer is set up to automatically check for updates, then you are probably in good shape as far as your operating system goes. However, I would still pay a visit to the Microsoft Personal Security Advisor site at [www.microsoft.com/technet/mpsa/start.asp](http://www.microsoft.com/technet/mpsa/start.asp). Simply click the Scan Now button and you will get a detailed report of your computer's security settings and recommendations for improvement [19]. Unfortunately, the scan will only work on Windows NT 4.0 Workstation, Windows 2000 Professional, and Windows XP. The most beneficial aspect of this scan is that it will let you know if you are not up-to-date on hotfixes. If you are not up-to-date, you can click on View Details and then click on the Hotfix Info link, which will take you to the hotfix URL so you can install it [19]. Warning: The installation of many hotfixes and updates will require you to reboot your computer. So, save all your work before installing.

If you are running Windows XP, you can install the support tools from your XP CD and run a utility called SPCheck. This utility can determine the service pack level of the following components:

- Internet Protocol (TCP/IP)
- NWLink (IPX/SPX) – most home users won't have this protocol installed
- Simple Network Management Protocol (SNMP) – most home users don't use this protocol either
- Client for Microsoft Networks [22]

When you install the support tools, on-line help will be installed as well. If you open the help, click on the “S” button, and then click “Spcheck.exe (Service Pack Check),” you will be taken to instructions that include examples of how to run SPCheck. Unfortunately, the support tools, including SPCheck, were designed for advanced users and run from the command line rather than a graphical user interface. The other unfortunate thing about SPCheck is that you need to download the spcheck.ini file from Microsoft before you can run it. If you download xpspch.exe from Microsoft’s web site and unzip it into the same directory that you installed the support tools in, it contains the spcheck.ini file [23]. Since the report output may be a little hard to understand for the novice user, I would recommend finding an experienced computer user to help you out.

Microsoft also offers an SPCheck tool for Windows 2000 called W2kspchk.exe [23].

### Testing your backups

The only way you can test your backup is by doing a restore. You can test by restoring a file to a location different from where it was backed up so that you don’t restore over the existing file. Some backup programs will let you do a verify after the backup is done. What this does is compare the data on the backup media to the original data to see if it’s the same. This still doesn’t guarantee that you will be able to restore the data at some later date, but it does aid in determining the validity of your backup. Due to the large number of backup programs, methods of backing up data, and media to back up to, I can’t really go into detail on how to do a backup, verify, or test restore. If you consult the manual or online help for your backup software, you should find instructions on performing these tasks. The point I want to leave you with here is that you can’t assume that just because you have made a copy of your data, that the copy is good. Verify to ensure you can perform a restore if necessary.

### **Conclusion**

Any time you are connected to the Internet for any length of time for any reason, you are subject to someone randomly or intentionally scanning your computer for vulnerabilities. Once the bad guy finds a vulnerability they can exploit, they may gain access to your data or passwords, install software on your machine that will allow them to control it and use it to attack other users, destroy your data, etc. This is why, at a minimum, you should employ these security techniques to protect yourself and others:

1. Use strong passwords and don’t use the same password for all your accounts.
2. Use anti-virus software and update your signatures on a regular basis.

3. Use a personal firewall.
4. Keep up-to-date on security patches for your operating system and your applications.
5. Back up your data on a regular basis.
6. Test your security on a regular basis to make sure the things you think are protecting you really are.

By following these guidelines, you are practicing what is generally known in the security community as “Defense in Depth” or layered security. What that means is that you are setting up multiple layers of security so that it will be harder for an attacker to get to your information. An example of this would be a locked box, within a safe, within a secured building, within a secured complex. In order for someone to get to the information in the box, they would first need to get through the complex perimeter security, then they would need to get past the building security, then they would have to break into the safe and finally, they would have to break into the locked box. While it is technically possible for someone to do all this, each layer of protection provides another hurdle for the attacker, slowing him or her down and giving you a chance at each stage to stop the attack.

The security cycle consists of three parts: prevention, detection, and response. The goal is to set up your system to prevent successful attacks so that you are not in a position of having to respond to an intrusion, which may have already exposed your information to the attacker.

### **Home Security Resources**

Below are a few good links to home security information that you might find useful.

[http://rr.sans.org/homeoffice/homeoffice\\_list.php](http://rr.sans.org/homeoffice/homeoffice_list.php) – The SANS reading room has an entire section devoted to home and small office security. Some of these papers might be a bit technical for the average computer user, but there is a wealth of good information here. If you are interested in other areas of security, the SANS site in general ([www.sans.org](http://www.sans.org)) is an excellent resource.

<http://www.homenethelp.com> – Home computer networking and Internet connection sharing help for the beginner and intermediate users.

<http://www.cert.org> – Check out their section entitled “For New & Home Users.”

<http://searchsecurity.techtarget.com> – This site is loaded with security information. You might want to begin by checking out the security basics section.

I also encourage you to do a search on “social engineering” and read up on the human factor of security, often referred to as the weakest link.

## References

[1] The White House. “Using 21st Century Technology to Defend the Homeland.” White House, Washington DC.  
URL: <http://www.whitehouse.gov/homeland/21st-technology.html> (1 Mar. 2002).

[2] Verton, Dan. “Report warns of al-Qaeda’s potential cybercapabilities.” Computerworld. 4 January 2002.  
URL: [http://www.computerworld.com/storyba/0,4125,NAV47\\_STO67092,00.html](http://www.computerworld.com/storyba/0,4125,NAV47_STO67092,00.html) (1 Mar. 2002).

[3] The SANS Institute. “Security Essentials Day 2: Threat and the Need for Defense in Depth.” Information Assurance Foundations - SANS. V1.11 (2002): 29.

[4] Counterpane Internet Security, Inc. “Password Safe.” Counterpane Labs.  
URL: <http://www.counterpane.com/passsafe.html> (3 Mar. 2002).

[5] Symantec Corporation. “Is Patching a Priority for Your Enterprise?” vulnerability management. 7 March 2002. Article ID: 1225. URL: <http://enterprisesecurity.symantec.com/article.cfm?articleID=1225&PID=11055631&EID=175> (8 Mar. 2002).

[6] [kathleen@drseuss.acs.calpoly.edu](mailto:kathleen@drseuss.acs.calpoly.edu) “A guide to Unix account passwords and password security.” 11 August 1999. URL: <http://www.acs.calpoly.edu/policies/passwords.html> (3 Mar. 2002).

[7] @stake, Inc. “About LC3.” Research: LC3. URL: <http://www.atstake.com/research/lc3/> (4 Mar. 2002).

[8] Trend Micro, Inc. “What Is a Computer Virus?” Virus Primer. URL: <http://www.antivirus.com/vinfo/vprimer.htm> (5 Mar. 2002).

[9] Chien, Eric. “CodeRed Worm.” Symantec Corporation Security Response. 19 September 2001. URL: <http://www.sarc.com/avcenter/venc/data/codered.worm.html> (5 Mar. 2002).

[10] Incidents.org by The SANS Institute. “Code Red Threat FAQ.” Version 0.2. 5 August 2001. URL: [http://www.incidents.org/react/code\\_red.php](http://www.incidents.org/react/code_red.php) (5 Mar. 2002).

- [11] Ferrie, Peter and Szor, Peter. "W32.Sircam.Worm@mm." Symantec Corporation Security Response. 26 February 2002. URL: <http://www.sarc.com/avcenter/venc/data/w32.sircam.worm@mm.html> (6 Mar. 2002).
- [12] Chien, Eric. "Wscript.KakWorm." Symantec Corporation Security Response. 30 December 1999. URL: <http://www.sarc.com/avcenter/venc/data/wscript.kakworm.html> (6 Mar. 2002).
- [13] The SANS Institute. "Security Essentials Day 1: An overview of the information risk management framework." Information Risk Management – SANS. V1.7 (2002): 22.
- [14] Trend Micro, Inc. "Solution 6095." URL: <http://solutionbank.antivirus.com/solutions/solutionDetail.asp?solutionID=6095> (10 Mar. 2002).
- [15] auditmypc.com. "Firewall Test and Port Scan." URL: <http://www.auditmypc.com> (10 Mar. 2002).
- [16] Anomaly, Inc. "Firewall Test Resources." URL: <http://www.homenethelp.com/web/howto/firewall-test.asp> (10 Mar. 2002).
- [17] Wallyware, Inc. "HackerWacker: See your computer the way hackers do." URL: <http://www.hackerwhacker.com/> (10 Mar. 2002).
- [18] Gibson, Steve, Gibson Research Corporation. "ShieldsUp!! NanoProbe Technology Internet Security Testing for Windows Users." URL: <https://grc.com/x/ne.dll?bh0bkyd2> (10 Mar. 2002).
- [19] Microsoft Corporation. "Microsoft Personal Security Advisor." 21 February 2002. URL: <http://www.microsoft.com/technet/mpsa/start.asp> (11 Mar. 2002).
- [20] The SANS Institute. "Information Security Reading Room: Home & Small Office Computing. 31 January 2002." URL: [http://rr.sans.org/homeoffice/homeoffice\\_list.php](http://rr.sans.org/homeoffice/homeoffice_list.php) (7 Mar. 2002).
- [21] Marsan, Carolyn Duffy. "Security Chief Details U.S. Cybersecurity Plans." Symantec Corporation Enterprise Security News. Reprinted from: InfoWorld Daily News. 12 March 2002. Article ID: 1235. URL: <http://enterprisesecurity.symantec.com/content.cfm?articleID=1235&PID=11164181&EID=178> (12 Mar. 2002).

[22] Microsoft Corporation. "How to Use the SPCheck Tool in Windows XP (Q312646)." Microsoft Product Support Services. 4 January 2002. URL: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q312646> (14 Mar. 2002).

[23] Microsoft Corporation. "How to Use the SPCheck Tool to Determine the Service Pack Level of Components (Q279631)." Microsoft Product Support Services. 20 December 2001. URL: <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q279631> (14 Mar. 2002).

© SANS Institute 2002, Author retains full rights.



# Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

<b>SANS Singapore 2009</b>	Singapore, Singapore	Jul 06, 2009 - Jul 11, 2009	Live Event
<b>SANS Rocky Mountain 2009</b>	Denver, CO	Jul 07, 2009 - Jul 13, 2009	Live Event
<b>SANS SOS London 2009</b>	London, United Kingdom	Jul 13, 2009 - Jul 18, 2009	Live Event
<b>SANS Future Visions 2009 Tokyo</b>	Tokyo, Japan	Jul 15, 2009 - Jul 17, 2009	Live Event
<b>SANS IMPACT 2009</b>	Kuala Lumpur, Malaysia	Jul 27, 2009 - Aug 01, 2009	Live Event
<b>SANS SEC563: Mobile Device Forensics Debut</b>	Baltimore, MD	Jul 27, 2009 - Jul 31, 2009	Live Event
<b>SANS Boston 2009</b>	Boston, MA	Aug 02, 2009 - Aug 09, 2009	Live Event
<b>SANS Atlanta 2009</b>	Atlanta, GA	Aug 17, 2009 - Aug 28, 2009	Live Event
<b>SANS WhatWorks in Virtualization and Cloud Computing Security Summit 2009</b>	Washington, DC	Aug 17, 2009 - Aug 21, 2009	Live Event
<b>SANS Virginia Beach 2009</b>	Virginia Beach, VA	Aug 28, 2009 - Sep 04, 2009	Live Event
<b>SANS SCDP SEC556: Comprehensive Packet Analysis - Sept. 2009</b>	Ottawa, ON	Sep 09, 2009 - Sep 10, 2009	Live Event
<b>SANS Critical Infrastructure Protection at Oceania CACS2009</b>	Canberra, Australia	Sep 10, 2009 - Sep 11, 2009	Live Event
<b>SANS Network Security 2009</b>	San Diego, CA	Sep 14, 2009 - Sep 22, 2009	Live Event
<b>SANS SCDP Cutting Edge Hacking Techniques - June 2009</b>	Ottawa, ON	Sep 15, 2009 - Sep 15, 2009	Live Event
<b>SANS WhatWorks Summit in Forensics and Incident Response</b>	OnlineDC	Jul 06, 2009 - Jul 14, 2009	Live Event
<b>SANS OnDemand</b>	Books & MP3s Only	Anytime	Self Paced