Global Information Assurance Certification Paper

The Art of Securing your Home PC for Free:

A detailed guide to effectively securing your PC from the darker side of the Internet

David T. Chamberlain
GSEC – Practical
Opt. 1 – Ver.1.4b
May 10, 2003

Abstract

Antivirus and personal firewall software should be used on every home computer that connects to the Internet. Common reasons these and other security solutions are not used is that often people still do not understand the importance of the software, or they do not know how to go about acquiring and installing it, or they may not be able or willing to spend money for the software. This guide is intended to show that effective protection against the darker side of the internet can be achieved within a couple of hours without spending a small fortune. In fact, every product recommended in this guide is freely licensed for home use. This means that outside of the time required to download the software, roughly one hour using a 56K connection, home users can legally and effectively provide layers of protection to their PCs without spending a dime. In this guide you will be asked to examine what you are currently doing to protect your PC. We will then briefly discuss a few of the reasons why we should be concerned about protecting our computers and we will look at ways to test the security of your home PC. And finally, if you are lacking in any of these areas, we will discuss several security solutions to improve security, and how to obtain and install these solutions. The products we will discuss are Avast! 4 Home Edition, ZoneAlarm, SurfinGuard Pro 5.7, and Ad-Aware 6.

In the preparation of this guide, special consideration has been given to make it easy to follow. The target audience is meant to be anyone who surfs the Internet and is not already using a majority of the types of solutions listed above. An attempt has also been made to avoid an extensive amount of technical jargon unless definitions are also provided.

Evaluate your Knowledge of PC Security

Let us start this discussion with a short quiz…. Now wait just a minute, don't hit the "back" button quite yet. This is an easy quiz. I promise that if you pass it with at least 85% you can and should move on to some other important subject. But before you do, see if you can answer these questions relating to your computer use:

1. What antivirus software do you use? When was the last time you updated the virus definition database? Do you know when you last performed a full system scan? Does your software allow resident protection and is this feature actually enabled so that all files accessed are regularly scanned?
2. Do you use a personal firewall? If so, have you tested it lately against any of the online security scanners to verify that it is working properly?
3. When was the last time you checked for new patches, service packs, or other updates for your operating system, Internet Explorer, Netscape Navigator, Office and other Applications?
4. Have you ever installed new software from the Internet by selecting all defaults? Do you read the License Agreements? How would you check to see if you have any datamining components installed on your system? Are you comfortable with all aspects of the software installed on your system? And do you know if any of your personal information or data about your Internet surfing habits is being sent to other parties without your knowledge?

And that's it. I told you it would be a short quiz. If you were able to positively answer these questions and successfully passed the quiz, you should be congratulated. And you should probably stop reading right here. However, save a copy of this guide before you go, and send it to someone you think may have a little more difficulty answering these questions. You can probably come up with a lengthy list of people in just a few minutes.

The truth is that there are far too many people who connect to the Internet on a regular basis with either high-speed or not so high-speed Internet connections and yet cannot answer these questions.

I am often asked by friends, family, and co-workers, who know I work in the IT Industry, to help solve their home computer problems. I am no longer surprised to find antivirus software using out-of-date definitions, disabled, or altogether not present. Yet computers infected with some type of virus are often the cause of a number of problems I encounter on home computers. I have also found that the need to use a 'Personal Firewall' is still somewhat misunderstood by many, even among IT Professionals. I will give you two personal examples to demonstrate these problems.

I managed the office network and servers at several sites in a previous job. One day I started receiving alerts that a file server was detecting virus activity. When I began to look at the logs, I found that a worm virus on the laptop of one of the office staff members was attempting to replicate itself to any share it could find on the network. Luckily, these attempts were stopped by the antivirus software on the server. But the infected laptop should have been running the same antivirus software and I was curious as to why it had not detected and stopped the virus in the first place. I examined the laptop and found the antivirus software disabled. When I questioned the staff member about this, he informed me that he felt the software slowed his computer down too much. He also said that he was always careful not to open unknown files and he didn't feel he needed to worry about viruses. He quickly changed his thinking when I enabled the antivirus software on his laptop, which immediately started blinking and sounding the virus alarm. And after showing him the logs that contained several hundred attempts from his laptop to infect the main office server and others on the network, he offered heart-felt apologies and promised it would not be a problem again. The next day he told me he found two additional viruses on his home computer after installing antivirus software and performing a full system scan.

The majority of home users are aware that antivirus software should be used. And some are better than others at keeping their virus definitions up-to-date. But this alone does not provide adequate protection. I have a good friend who is a Network Engineer for one of the largest Internet Service Providers (ISPs) in the U.S. For a while he was responsible for setting up high speed connections for customers. One of the perks of the job was that he received a high speed (T1) connection to his home. He set up a personal website to host pictures of family reunions, trips, etc. His computer was connected directly to the Internet 24 hours a day. After about six months I noticed that his website was no longer online. When I talked to him about this, he said that his site was continuously being hacked into. After a hacker changed many of the links on a family photo thumbnails page, pointing them to pornographic images, he decided to pull his website offline. Imagine trying to explain this to your mother who thought she was about to see pictures of her grandchild's birthday party. I asked him what he was doing to protect his computer. Other than installing antivirus software, he hadn't taken the time to do anything else.

These are just two examples, but I could go on and I'm sure you are already familiar with similar stories. If not, I guarantee you will be soon enough. I used these examples of mistakes made by IT Professionals to show that this apathy towards computer security is common even among groups where you would least expect it. So if we are aware that there are so many online threats and computer security risks, why do we still sometimes seem to be slacking off in protecting our systems?

I contacted several friends and relatives to ask them the same questions listed at the beginning of this guide. Their answers are probably representative of computer users in general. The majority said they were only using antivirus software to protect their systems. Several said that their antivirus software no longer allowed updates because the subscriptions had expired. Most had heard of personal firewalls but didn't

know if they really needed one or how to go about deciding on one. Others said that because they only used a 56K connection, they didn't need to worry that much about security. One of the most common excuses I heard from those I questioned was that they didn't want to spend money to add any additional software. After pursuing this line of thought a little farther, it really boiled down to this one thing—there is still not enough understanding of the some of the dangers surrounding the Internet. (Or maybe I just have a lot of cheap friends.)

In response to all of these answers, I will be providing personal copies of this guide to everyone I questioned. There is no good excuse not to have a secure Home PC. The information is available, the solutions are many, and without spending any money it is even possible to provide excellent protection. In the next section after we talk about a few of the dangerous programs running out in the wild today, we will see that having a secure home PC is not only good practice, but has truly become a moral obligation for the entire Internet community.

Viruses, Trojans, and Worms, Oh my!

One of the earliest viruses I personally experienced was a variant of the "Happy" virus about 10 years ago. The one that infected my computer didn't seem to do any real damage, but occasionally the words "Legalize marijuana!" would pop up on the monitor. It was funny at first and then became annoying very fast. Other viruses have been, and continue to be the cause of much greater concern. The number of new viruses discovered each month varies, but the estimates range from 300 – 500 or more per month. A virus could be classified as any program that self-replicates. Worms are similar in that they are self-replicating. Worms can be much more invasive in that they often attempt to copy themselves to as many locations as possible, across network connections, email, or any way possible.

A Trojan (or Trojan Horse) is any program designed to be hidden in a legitimate program and which carries out actions unknown to the user while the legitimate program is run. They have become very advanced and are often very difficult to detect. Hackers have many tools available that will take just about any program and hide a Trojan within the program.

"Hackers Beware," by Eric Cole, is a book that describes literally hundreds of ways that hackers gain access to systems. Cole describes the popularity of Trojan Horse programs among hackers because it is such an easy way to gain access to systems. We (general users) have a natural tendency to pass entertaining files on to our friends.

> Trojan horses can cause extensive damage… A perfect example is seen around the holiday season. People send around the animated jpgs that have things like dancing reindeers. Users cannot resist the urge to pass these on… The covert function is launched when the overt function is being executed, so most users do not even know that it is happening. They think they are running an entertaining file, and in reality they are infecting their machine and their friends are doing the same. A common use of Trojan horses is to install backdoors so that a [hacker] can get back into the system at a later time. (Cole, p. 39)

One example of a particularly wide-spread and invasive Trojan is "SubSeven." This program has many variants and is constantly being changed to add functionality and make new versions more difficult to detect. Once installed on a user's computer, it gives the controller (could be anywhere in the world) almost complete control of your system. You could be sitting there surfing the Internet and someone could be logging all of your keystrokes as you connect to your bank or make other financial transactions. Or they could play games with you like sending a command to open your CD tray, or pop up a chat dialog on your screen… "Wake up Neo!"

Programs infected with Trojans, viruses, and worms are spread in many more ways than email attachments. With the popularity of many Peer2Peer file sharing services such as the now defunct Napster, KaZaa, Morpheus, ICQ, and others on the rise, the spread of Trojanized programs is also increasing. Peer2Peer file sharing services allow anyone to share any kind of software with anyone anywhere on the Internet. These services are often used by individuals to find and download music, software, movies, entertaining programs, images, or just about anything else. This makes it very difficult to validate that any program you download from one of these services is not harboring some type of Trojan or other virus. I cannot stress enough how easy it is for someone with malicious intent to hide a very nasty virus inside of any popular, legitimate-looking program.

It is bad enough that your computer could be the means of providing someone else with your personal information. But once your computer is compromised, you are not the only one who could end up a victim. A hacker with access to your system can use it to attack other systems. We sometimes hear on the news of incidents where websites are taken off-line in Distributed Denial of Service Attacks (DDoS). These attacks are often carried out by hundreds of unknowing home users whose infected computers, combined, are sending out floods of network traffic at specific targets on the Internet. The goal of the attacker is to deny legitimate access to the services of business, government, and other websites. Often these attacks result in the loss of millions of dollars in revenues to the victim companies, and sometimes the attacks are just a temporary annoyance.

You should read a very interesting and informative article on one such attack at http://grc.com/dos/grcdos.htm . This article details what happens when a website is targeted by a DDoS attack. It also chronicles some of the methods used by a 13 year-old teenager to effectively deny access to the www.grc.com website by controlling nearly 500 home computers infected with the SubSeven Trojan, and using them to carry out the attack.

Home users are not generally held responsible for any attack originating from their compromised systems. However, as the legal issues surrounding this problem continue to develop, it is likely that this could change in the future. I can imagine that at some point we may very likely be held responsible for damages done to others on the Internet if we are found negligent in providing proper security procedures on our personal computers. It is better to take a little time now to educate ourselves in some basic security practices.

Test Your System

At this point you may be very interested in trying to determine whether or not your home PC is up to par on security. You can run several tests from the following websites. These tests will attempt to scan your presence on the Internet and look for weaknesses. I would recommend running the tests fairly often, or anytime you make any changes or add software to your computer.

http://www.grc.com — Try the Shields UP! Test. Follow the links for Shields UP! This test will show you how your computer appears online to anyone that may scan your system looking for openings. It is also a great site for providing a lot of good security information.

http://www.symantec.com — Follow the links for the Security Checker. Symantec has a comprehensive scan that will attempt to see if what ports are open, if your antivirus software is up-to-date, and other tests.

http://www.hackerwhacker.com — Follow the links for Security Scan. This site also provides a lot of information and news about Viruses, Trojans and Worms.

How well does your antivirus software stand up to actual tests to find and neutralize viruses? The following website provides some comparisons for many of the different antivirus software products:

http://www.hackfix.org/miscfix/icons-av-all.shtml

If you are unsure about how to update your Operating System, Internet Explorer, Office and other applications with the latest updates and patches, examine this tutorial at Microsoft.com:

http://www.microsoft.com/security/articles/update.asp

Similar information can be found for the majority of the software you may be using on your system. You should go to the software developer's technical support link on their websites to search for updates.

And finally, don't forget to visit the SANS Reading Room for information to cover nearly all questions you may have concerning Information Security.

http://www.sans.org/rr/

If you have found any weaknesses when performing the system tests, you should pay close attention to the next sections where we will discuss some of the free solutions available to protect your system, and how to obtain and install them. After installing any of the programs, go back and retest the security of your computer.

Is Free Security Software any Good?

Many PC users already own and are using at least one of the many commercially available security solutions from Symantec (Norton AntiVirus), McAfee, or others. I am not recommending that you stop using those solutions and replace them with the ones we discuss in this guide. But I do advocate these free solutions so that you will have no excuse not to improve any weakness in the overall security of your PC.

There are many very good 'Total-Internet-Security' solutions for home and professional use available from the big-names in computer security. These solutions cost a little more but are generally worth the money when the consumer finds that the product offers good protection and ease of use. However, it is not necessary to spend a lot of money to provide the same protection. Given that the security can be achieved at no cost, it isn't worth the risk not to do anything.

Every free-for-home-use product in this guide has won multiple awards. In researching the various options, I took extra care in choosing the free solutions that received the highest marks from both professional and general consumer reviews. They are solid, tested solutions that can help provide layers of protection to your online experience. These solutions were all developed to address the inherent security weaknesses in the Windows operating system and other third party software that you have running on your PC.

Avast! 4.0 Antivirus, from Alwil Software, has been providing antivirus solutions since 1988. They also offer a wide variety of solutions for professional and business use. Alwil Software is also one of the few remaining companies to offer free-licensing of antivirus software for home, non-business use. Avast! 4 Home Edition offers resident protection, scanning of incoming and outgoing email messages, automatic backup system critical files (and repair in case of infection), and heuristics testing. Heuristics tests are used to search for new previously unidentified worms and viruses by looking for potentially harmful virus-like patterns in files. One thing Avast! Home Edition lacks, though is script blocking—but we will cover this area with SurfinGuard (discussed after the next paragraph).

ZoneLabs ZoneAlarm is one of the most preferred personal firewalls in the market today. It continues to win awards for providing a combination of excellent protection and ease of use for the consumer. ZoneAlarm 3.7 is the version out at the time of this writing and it has many new features to help the user understand how the firewall works and to enable the user to find out important information about scans and potential attacks against your PC. Once it is enabled, your PC will run in stealth mode, making it appear invisible on the Internet to deviants looking to gain access to your PC.

Finjan SurfinGuard Pro 5.7 helps protect your computer from new and unknown Virus, Trojan and other threats. It does this by placing "active content" such as Java, ActiveX, email attachments, and scripts in a "SafeZone" and monitoring their behavior.

Any suspicious or malicious activity will be blocked by SurfinGuard. This is particularly useful to defend against many of the email-borne viruses such as the “ILoveYou” virus that was famous a few years ago.

Lavasoft Ad-aware 6 is a very useful track-ware detection and removal utility. Track-ware could refer to forms of spyware, keyloggers, datamining (website usage tracking software), and more. Many types of software programs that Internet Surfers install have components that monitor your internet usage and send this information to other parties. Often these are use to provide customized advertising. Sometimes the information could have more dangerous results. If you often install software from the Internet by accepting all defaults and not reading the full details of the End User License Agreements, chances are likely that you already have a number of these components on your system. Use of this utility will help to maintain a greater level of privacy online.

By combining these solutions, or adding to whatever you are lacking from your present configuration, you will be improving the protection against a many of threats on the Internet today.

In the next sections I will give detailed information on how to obtain and install the software. I will also show the steps to follow to get the latest updates for each program and then how to access the help files. After the initial configurations of each software application, these programs will not need an extensive amount of fine-tuning, but you should still familiarize yourself with the features and usage. The “Help Files” in software programs are often overlooked in the same way that instructions for anything requiring assembly are usually set aside. However, the help files in these programs are well written and provide enough information to become very comfortable with the use of these security solutions.

Obtaining the Software

Avast! 4 Home Edition Antivirus Software

You may visit the Avast! 4 website to learn more about the products by selecting:

www.avast.com

Or, go directly to download the free version by following this link:

http://www.avast.com/i_kat_67.html

1. Scroll to the bottom of the page and select “avast! 4 Home Download.”
2. You will be given a choice to download the ‘English’ or ‘Czech’ version. Select your version and download location. (i.e.: select “US” under the first line – English option.)
3. Choose where to save the file and press “save.”
4. Now I would recommend registering for the software while you are waiting for the download to complete. By registering the software, you will be sent a ‘license key’ to the email address you specify. This key is required after installation in order to be able to update the software and virus definitions. If you choose to register now, continue to step five. Otherwise you will be given another chance to register after you install the software.
5. After the download begins, refer to the same web page from which you selected the download link. Near the top of the page is a link for registrations. Select the “registration” link.
6. You will be required to enter your email address and other information and at the end of the process, you will be sent a license key via email. On the last page before finishing the registration, you will also be given the option to receive an email message every time a new virus database update is released. This is a good option to remind you to stay up to date with the latest virus update.
7. This file will take approximately 20 minutes to download with a 56K connection.

ZoneLabs ZoneAlarm 3.7

You may visit the ZoneLabs website to learn about the products they offer at:

www.zonelabs.com

Or, go directly to the download the free version of ZoneAlarm by following this link:

http://www.zonelabs.com/store/content/catalog/products/sku_list_za.jsp?lid=pdb_za1

1. From the ZoneAlarm download page, select “download.”
2. You will see a screen showing other products offered by ZoneLabs and then will be prompted to save the file.
3. Select “Save” and then choose the location where you would like to save the file.
4. You will be given a chance to register ZoneAlarm during the installation described in the next section.
5. The download should take roughly 15 minutes on a 56K connection.

Finjan SurfinGuard Pro 5.7

You may visit the Finjan website to learn about their products by selecting this link:

www.finjan.com

Or, go directly to download the freeware version of SurfinGuard by selecting:

http://www.finjan.com/products/surfinguard.cfm#download

1. From the SurfinGuard Pro freeware download page, scroll towards the bottom of the page until you see the “Begin Download” button. Enter you email address in the space provided and click the “Begin Download” button. (This page also contains a lot of information about the use and value of SurfinGuard.)
2. The download file prompt will appear. Select “Save” and choose the download destination.
3. This file will take approximately 20 minutes to download with a 56K connection.

Lavasoft Ad-aware 6

You may visit the Lavasoft website to learn about their products by selecting this link:

www.lavasoftusa.com

Or, go directly to download the free version of Ad-aware by selecting:

http://www.lavasoftusa.com/software/adaware/

1. On the Ad-aware Standard page, select the “download” link near the middle, right-hand side of the page.
2. Choose from one of the many download locations. (i.e.: Select “Ad-aware 6 from tucows | 1.45 mb”)
3. Follow the directions shown for the location you chose to download the software. (Most likely you will just select “download” again.)
4. You should be prompted to “Save” the file. Choose the folder you would like to save the file to and select “OK.”
5. This file should take approximately 5 minutes to download on a 56K modem.

Software Installation and Configuration

Avast! Version 4.0 Home Edition (Antivirus)

Installation of Avast!

1. Double-click the setup program. It should be labeled similar to "setupeng.exe."
2. Click "Next" on the 'Setup Screen.'
3. Click "Next" on the 'Read me' Screen after verifying that your system meets the setup requirements.
4. If you agree to the End User License, select the "I agree" radial button and then click "Next."
5. Click "Next" to select the default installation destination folder. (Or make the desired location changes.)
6. I would recommend selecting the "Typical" setting on the 'Configuration' screen and then click "Next."
7. Review the installation information and then click "Next" to start the installation.
8. You will next be given an option to schedule a boot time scan of your hard drive the next time you restart the computer. If you have not recently scanned your computer, I would recommend selecting "Yes" to the boot time scan. (This will only happen the first time you restart the computer.)
9. Next you will be given options for configuring Avast! scan incoming and outgoing mail for viruses. Read the screen for a description of the change that Avast! will make to your mail configuration. Select "Next" to continue.
10. You can choose the setting to have Avast! "Automatically protect all [your mail] accounts." If you choose this option, I would recommend also selecting the box to allow Avast! to "Automatically protect all accounts [you] create in the future." Make your selection and click "Next" to continue.
11. Next you will be asked to select the SMTP and POP servers you use for your mail settings. If you have only one account, these settings will automatically be entered into the boxes. Make your selections and then click "Next" to continue.
12. Click "Finish" to finalize the installation. You will be asked to restart the computer. Save any work you may have open and then select "Finish" to restart the computer.

Post Installation Configuration of Avast!

After restarting your computer, we will look at a few additional configuration options. By default, Avast! will automatically run in 'On-access Mode' (or resident mode). This is one of the most important aspects of the antivirus software. It means that Avast! will constantly be running in the background to scan files accessed on your computer.

1. Select the 'Avast! Antivirus' icon that was created on your desktop. If you are not able to find it on your desktop, navigate to 'Start → Programs → avast! Antivirus → avast! Antivirus' to start the program.
2. A prompt asking you to enter the license key you received when you registered for the software. Enter the license key and select "OK." (You should have received this license key at the email address you supplied when you registered to download the software. If you did not register, you are given another chance to do so by selecting "Program registration.") If you do not enter a license key, the program will be activated in demo mode and will be good for 60 days after which time you will not be able to update the virus definitions.
3. A tutorial will appear providing general information about the options found in Avast! Also, you can select a detailed help file by going to 'Start → Programs → avast! Antivirus → Help.' In this help file, you will be able to get detailed information on how to configure any special settings within Avast! However, this software is designed so that after restarting your computer at the end of the installation, it is fully protecting your computer.

ZoneLabs ZoneAlarm 3.7

Installation of ZoneAlarm

1. Double-click the setup program. It should be named something similar to "zasetup_37_159."
2. Click "Next" to select the default location to install the software. (Or make changes to the destination if needed.)
3. Fill out the 'Registration' with your name and email address and click "Next." (If you do not fill out the registration, you will not be able to download updates to the software.)
4. Check the box on the next screen if you agree to the 'End User License Agreement' and click "Install."
5. Next you will be asked to complete a brief user survey before finishing the installation. Select the appropriate responses and click "Finish" to complete the installation.
6. You will be given the prompt that the installation is complete, and you will be asked if you want to start ZoneAlarm. Click "Yes" to continue. No computer restart is required before starting the program.

Post Installation Configuration of ZoneAlarm

1. After completing the installation choosing to start ZoneAlarm, you are walked through some 'welcome' information and given the opportunity to view a tutorial. I highly recommend going through the tutorial if you are not familiar with how firewalls work. Select "Next" to continue.
2. You are given the option to receive messages alerting you of the actions that ZoneAlarm performs. If you would prefer not to receive the messages but have

ZoneAlarm manage everything for you, you are given the option to select "Don't alert me at all – protect my computer silently."
3. The next screen gives you the option to allow ZoneAlarm to pre-configure access permission. If you are a little unsure about using the firewall, I would recommend choosing "Yes" and continue.
4. You are now given the option to view the tutorial. If you are new to ZoneAlarm, select "Yes" to view the tutorial. (You can always view the tutorial by selecting "Start → Programs → Zone Labs → Zone Alarm Tutorial")
5. A detailed help file is also available by selecting "Start → Programs → Zone Labs → Zone Alarm Help." Take a little time to become familiar with using ZoneAlarm. A little time now will pay off as you begin to receive messages about

Finjan SurfinGuard Pro 5.7

Installation of SurfinGuard

1. Double-click the setup program. It will be labeled similar to "SurfinGuardPro57b281."
2. On the 'Welcome' screen click "Next" to continue.
3. If you agree to the End User License, select "Yes" to continue.
4. Select "Yes" to agree to the 'Java runtime environment agreement' and continue.
5. Take note on the next screen. You are given the option to allow feedback to be sent to Finjan to help with their continuing development of this product. Their agreement states that no personal or private information is collected. This is optional and you can personally decide whether or not to install this feature. This states that you will always be prompted before any information is sent to Finjan, and you can verify what information is being sent and decide whether or not to send the information. If you decide that you do not want to install this feature, click "No" to continue.
6. On the next screen, accept the default installation location by clicking "Next." (Or change to the installation location of your preference.)
7. On the 'Start copying files' screen, select "Next" to begin installing the files.
8. The program is now installed and at the end you are given the option to view a 'Read me' file. Select "Yes" or "No" to view the file. (The 'Read me' file gives some interesting information about this version of the file.)
9. You will now be prompted to restart your computer in order to complete the installation. Click "Finish" to complete the installation and restart the computer.

Post Installation Configuration of SurfinGuard

After the computer restarts, SurfinGuard will automatically run in the background, and you will not be prompted to do anything else. I would point out two things that we have already done with the previous programs that we've installed.

1. Right click on the 'SurfinGuard' icon in the 'System Tray' and select "Settings." Select the 'Auto Update' tab and click on "Check For Upgrade Now" to make sure you have the most up-to-date software changes.
2. To view the 'Help' file, right click on the SurfinGuard icon in the 'System Tray' and select "Help → Help Contents." The help file should be able to answer most of the questions you may have about the details of using this product.

Lavasoft Ad-aware 6

Installation of Ad-aware

1. Double-click the Ad-Aware setup file. The file should be named similar to "aaw6."
2. At the 'Welcome' screen, click "Next" to continue.
3. If you agree to the License Agreement, click "Next" to continue.
4. Accept the default installation location by clicking "Next" to continue. (Or choose your preferred installation location.)
5. Click "Next" to begin the installation.
6. The installation should complete fairly quickly. Click "Finish" to exit the installation mode. No computer restart is required.

Post Installation Configuration of Ad-aware

1. Run the 'Ad-Aware' program by either double-clicking the icon placed on the desktop during installation or browse to program by selecting "Start → Programs → Lavasoft Ad-aware 6 → Ad-aware 6."
2. Click on the "Check for updates now" link near the lower right corner of the program window. After verifying and updating the program, you are ready to scan for any datamining components, keyloggers, malware, and other software that previously may have been installed on your system without your knowledge.
3. Review the 'help' file by clicking the "Help" button on the main screen.

Conclusion

In conclusion, I congratulate you for making it to the end of this guide. I hope you have found some information to spark a greater interest in steps and software solutions available to give you a greater feeling of confidence in your Internet experience. By following the advice contained in this guide, and following a few steps long enough to form some good computer use habits, you will have a less stressful and more productive time surfing the net.

Good luck

References

Cole, Eric. Hackers Beware: Defending Your Network From The Wiley Hacker. New Riders, 2001

Gibson, Steve. "Shields UP!" NanoProbe Technology Internet Security Testing for Windows Users. Gibson Research Corporation
URL: https://grc.com/x/ne.dll?bh0bkyd2

Gibson, Steve. "The Strange Tale of the Denial of Service Attacks Against GRC.COM."
URL: http://grc.com/dos/grcdos.htm (5 Mar., 2002)

"Checklist: Keep Software Up-to-Date." Microsoft, 2003
URL: http://www.microsoft.com/security/articles/update.asp

"HackFix: Misc Trojans." AntiVirus Software Detection Results.
URL: http://www.hackfix.org/miscfix/icons-av-all.shtml

"HACKYOURSELF Remote Computer Network Security Scan." HackerWhacker, 2000.
URL: http://www.hackerwhacker.com

"SANS InfoSec Reading Room." SANS
URL: http://www.sans.org/rr/

"Symantec Security Check." Symantec Corporation. 2003
URL: http://www.symantec.com

Alwil Software Avast! 4 Home Edition
URL: http://www.avast.com

Finjan SurfinGuard Pro 5.7
URL: http://www.finjan.com

Lavasoft Ad-Aware 6
URL: http://www.lavasoftusa.com

ZoneLabs ZoneAlarm 3.7
URL: http://www.zonelabs.com

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS