# Global Information Assurance Certification Paper

# Self Defense on the Internet:
# Defense in Depth for Home Computers



GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b – Option 1
Nadeem A. Memon
February 21, 2005

## Abstract

Computers on the Internet are under attack. Computer security is not just something a business or organization should be concerned with. Home computer users need to think about secure computing as well. The importance of understanding the steps to take in order to safeguard a home computing environment cannot be overstated. Anyone who is concerned about the security of their private information, the proper functioning of their computer, not to mention maintaining their access to the Internet, needs to be aware of how to defend their home computing environment while connected to the Internet. Most of the tools available to assist in protecting against the compromise of a home computer are inexpensive when they are not freely available. The purpose of this paper is to motivate home computer users in particular to learn about computer security and explain the concept of layered security in a fairly non-technical manner that is accessible to the typical home user. Examples will be given of tools that can be used to create multiple layers of security with an emphasis on how each layer provides added security. Links to useful tools, additional techniques, and advanced topics are included in the Appendices for more sophisticated home computer users. Since Microsoft™ Windows operating systems are the most widely used today, this paper will focus on specific solutions to protect Windows users, although most of the concepts will transfer to users of other operating systems as well.

## Introduction – Why Is Security Important for Home Computer Users?

Most, if not all, computing professionals have some familiarity with the concept of computer security. Unfortunately, until fairly recently there has not been much of a motivation for non-technical home users to educate themselves in this area of expertise. The typical home user installs anti-virus software and pats himself or herself on the back. While it is an excellent beginning, anti-virus software alone is no longer a sufficient defense against the variety of attacks one can experience in the wilds of the Information Superhighway.

Home computer users often don't feel as though securing their home computing environments is a necessary task. The typical argument is "I don't keep anything important on my computer." Even assuming that such a statement was true, it completely ignores the frustration caused by a computer that is not working properly. There is a lot to lose even for people who don't keep any important data on their computer.

It has become increasingly common for home computers to have so many malicious software or malware programs installed that they become unusable. Those programs may be installed by other malicious computer users or by other malware. The end result is having a computer whose main function is that of a big, expensive paperweight.

A computer with malware installed may not only be unusable, it may be a danger to other computers on the network or Internet. The company that provides Internet connectivity to a home user with a virus-infected computer may choose to turn off the home users' Internet access if that virus-infected computer begins scanning the Internet for other computers to infect. Alternatively, if a malicious computer user has taken control of another person's computer, that malicious computer user may use that computer to attack other computers. Those attacks can get traced back to the compromised computer and the owner could be held responsible.

Even computers that are functioning properly and not attempting to infect other computers may not be safe for children to use. The Internet is a great resource for locating information. Unfortunately, its chaotic nature also makes it unsafe for children to have unrestricted access to it. Pop-up web ads from web sites or spyware that downloads pornography onto a home computer are real problems these days.[1]

Losing the ability to use one's home computer or even losing one's Internet access should be the least of a home user's worries when it comes to securing their home computers. It is not difficult to imagine a situation where a malicious individual gains access to another person's computer and uses it to store illegal data (e.g. pirated software or child pornography). Suppose that computer was confiscated by the authorities or some other member of the computer-owner's family found that data. It is

[1] Martin, Kelly. "When spyware crosses the line." The Register. 24 June 2004.
URL: http://www.theregister.co.uk/2004/06/24/spyware_crosses_line/ (2 Feb 2005)

possible that such an occurrence would result in many uncomfortable questions and potentially jail time. Unfortunately, the incident just described is not just a scary story. It has happened.[2]

If the scenarios outlined above are disturbing, they are meant to be. Home computer security is serious business. The task of securing a home computing environment falls squarely on home users. It is the intent of this paper is to assist users in putting the right resources in place to create as secure a home computing environment as possible.

## The Problem Defined

The typical home environment looks something like Figure 1 below.

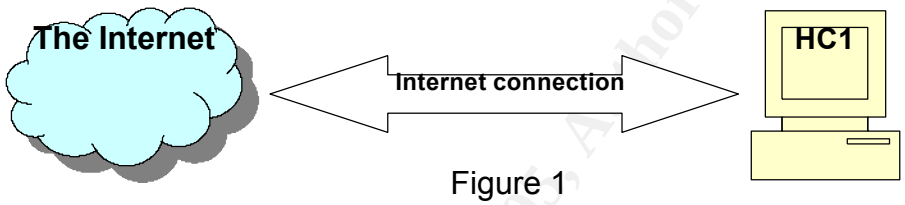


Figure 1

This picture describes a computer that is directly connected to the Internet. There may be a cable or DSL modem that the computer connects to in order to be connected to the Internet, but that is part of the Internet connection in this diagram. Having a computer directly connected to the Internet means that computer talks directly to other computers on the Internet and conversely other computers on the Internet can talk directly with that computer. There is nothing limiting that communication, so ANY other computer on the Internet can talk to that computer, including some computers a home user wouldn't want to talk to (e.g. a virus-infected computer). Speaking more technically, the network card in the computer has been assigned a public IP address, which means that any other Internet-connected computer can communicate and possibly connect to it. This is not an optimal situation. On the Internet, when someone knocks on your door, it's not always a good idea to ask, "Who is it?"

Most improperly secured computers in the configuration described in Figure 1 are sitting ducks for viruses and hackers on the Internet. In most cases, such computers will respond to all outside requests whether the owner of the computer wants them to or not. As a result, these unsecured computers can be compromised or "hacked" in minutes.[3]

---

[2] "Man cleared over porn 'may sue'." BBC News UK Edition. 31 July 2003. URL: http://news.bbc.co.uk/1/hi/england/devon/3114815.stm (5 Feb 2005)

[3] Acohido, Byron and Jon Swartz. "Unprotected PC may be hijacked in minutes." USA Today. 30 Nov 2004. URL: http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm (5 Dec 2004)

## The Best Defense

As is true in other situations, using layers of protection is the best way to defend a home computing environment. These layers will provide protection against most of the threats that can be found on the Internet. Some of the layers will overlap in their protection.

Those layers include:

1) Changing the home computer set-up so it no longer has direct access to and from the Internet
2) Making modifications to Windows in order to "harden" it or make it more difficult for unauthorized users to gain access to it.
3) Install utilities that scan and protect a computer from viruses and spyware.
4) Keep Windows and other applications up-to-date.

In the following sections we will use the analogy of the computer as a house to simply explain the steps a home user can and should take to secure their home computing environment. Just as there is no such thing as a perfectly secure house, there is no such thing as a perfectly secure computer. The goal of security is to make getting through to the home computer so difficult that anyone trying to get through to it will give up and go look for easier targets.

## Layer 1 – Close the Doors and Windows

A house that leaves the doors and windows open is not a very secure house. By the same token, a computer that is wide open to the Internet is not very secure either. The most important step to securing a home computer is to put a device that functions as a firewall between the home computer and the Internet as shown in Figure 2. The purpose of a firewall in a network is to block unsolicited communication from the Internet while allowing Internet connectivity for the computer in the home (HC2 in Figure 2).

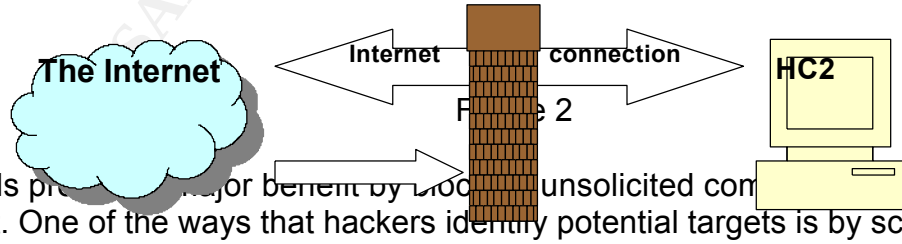


Figure 2

Firewalls provide a major benefit by blocking unsolicited communications from the Internet. One of the ways that hackers identify potential targets is by scanning a range of IP addresses on the Internet using a technique called a PING Sweep. Most Microsoft Windows operating systems (except Windows XP SP2) are configured to respond to those scans by default. By blocking these scans, a firewall makes it seem as though no computer is connected at a given address. With this first layer in place you can avoid a good deal of unwanted attention from malicious computer users on the

Internet.

In a corporate environment, this functionality is typically provided by a hardware device sitting between the corporate network and the company's Internet connection. While dedicated firewall devices may be a bit pricey for home users, cable/DSL routers can provide basic firewall functionality. A home user should look for a router that lists Stateful Packet Inspection (SPI) as one of its features.[4] There are also software firewall products like Zone Labs™ ZoneAlarm or Symantec™ Client Security. These solutions are generally inexpensive. A cable/DSL router can be bought for between $10-$100, depending on its other functions. Software firewalls can be found on-line for free or purchased for around $30-$60.

Hardware firewalls allow you to separate your home computer or network from the Internet. This separation makes it even more difficult to reach a home computer behind a hardware firewall. This additional protection allows home users the time to download operating system patches and service packs without having to worry about being hacked before their computer can download and install the updates.

Software firewalls have the added benefit of not only blocking incoming unsolicited Internet communication, but many products now offer the option of monitoring and/or blocking outgoing Internet communication as well. It may not be obvious why that might be necessary, but it can be enlightening to learn what programs a home computer user might have installed that are trying to send information out to the Internet from his or her computer. Having a software firewall installed can help a home user identify rogue programs sending information out to the Internet and block that outgoing communication. It is crucial that the home user does not simply instruct the software firewall to allow outbound Internet communication whenever it prompts for a decision, but actually make an effort to understand what programs are trying to send information out and why. This understanding will allow the home user to decide whether or not to allow a program to have access to the Internet. This process of deciding which programs will be allowed to send information out to the Internet is known as "training a firewall." Training a software firewall can be a painful task initially, but the reward is a more secure computer.

While having a hardware firewall and a software firewall installed may seem redundant, the two can provide complementary protection for a home user environment. Since there are free software firewall products available, there isn't really any excuse not to install one in conjunction with using a hardware firewall. The hardware firewall prevents traffic from reaching the home computer. Software firewalls, on the other hand, block unsolicited communication that has already reached a home computer, in addition to keeping track of information flowing out of the computer. To put it another way, installing a hardware-based firewall is like digging a moat around a house, while a software-based firewall is like locking the doors of a house.

---

[4] Weil, Alan C. and Eric W. Vaughan. "Securing Windows XP" Version 1.0. n.d. URL: http://www.tweakhound.com/xp/security/page_1.htm (5 Jan 2005)

## Layer 2 – Don't Invite Strangers In

Malicious computer users and malware writers realize that it is very difficult to reach a home computer that is behind a firewall. It is much easier to try to trick a home computer user into inviting them into the computer rather than by trying to get around a firewall. As a result, they have found different ways to sneak into your system.

A malicious computer user might send an e-mail that sends a user to a web site that installs software that allows him to get access to that user's computer. Alternatively, they may write malware programs to do their dirty work for them. Some of the most prevalent types of malware are defined below.

A computer virus is a piece of software written to mimic the behavior of biological viruses. In other words, it attempts to replicate itself and spread to as many hosts as possible. This process can lead to the destruction of data and can even affect Internet connectivity. In the best case, a virus will still cause a computer to run more slowly and potentially damage data. Virus writers will write programs to attack unprotected systems. Often they will use those systems to send virus-infected e-mails out to random people in the hopes of fooling them into opening the message and infect themselves.

Another type of malware is called a Trojan Horse. This is a type of software that attempts to enter a computer by disguising itself as something the computer owner wants. Once it is on a computer, it may act as a virus and replicate itself. It may also attempt to infect other hosts, or it may execute additional software code that allows another person to gain access to your computer. It is safe to assume that an individual using software like this to gain access to another person's computer is up to no good.

Spyware is a fairly recent problem compared to other Internet threats. Also known as Adware, it is software that is meant to record a computer user's web browsing behavior and send that valuable information to a company. That company then tells the spyware to open pop-up web browser windows with advertisements geared to that user's interests. Some spyware even keeps track of files downloaded from the Internet.[5] Spyware companies use a few methods to trick users into installing their spyware. In some cases they associate themselves with useful legitimate software. The spyware companies offer money to the software developers to bundle spyware along with the useful software written by the software developer. The software developer can then distribute their software by claiming it is "free" or "advertiser-supported". Meanwhile anyone who installs that application also installs some spyware. In this way, spyware is much like the Trojan Horse. Kazaa and Gator are examples of such programs. Another way spyware companies fool users into installing their software is by using pop-up windows to simulate Windows security alerts in order to get a user to click on the windows and install some spyware.

[5] Montgomery, Garth. "Daily Dispatch (Opinion) – Kazaagate Day 15: part 4." Apcmag.com. 7 Feb 2005. URL: http://www.apcmag.com/apc/v3.nsf/0/07A1C8CA269E79B5CA256FA1000F9763 (9 Feb 2005)

A computer infected with spyware typically has a number of symptoms. Usually it will run more slowly than usual. Web browsing will often take much longer than before the infection. The Internet Explorer start page may change from what it was previously set to. Also, pop-up advertisement windows will open frequently even when no web browsing is going on.

In addition to the detrimental effects on the home computer, another issue with spyware is that it remains in communication with the company that wrote it. The user has no control over that communication, and therefore has no idea what information (beyond the web sites he or she visits) is being sent back to the company. Adding insult to injury, in many cases the software takes a page from the virus writer's book by hiding itself on a user's computer and spreading itself out so that it becomes very difficult to remove. Often when spyware is installed, it will install additional spyware software, further slowing down a computer with the spyware installed. Ultimately, even the most benign ad-ware or spyware uses some computer processing power. As a result, a computer that is infected with spyware will often operate much more slowly than usual, in addition to inflicting pop-up windows on the user. For this reason, many people consider spyware to be just another type of virus.[6]

There are a few tools home users can find on the Internet that will assist in avoiding being tricked into installing any malware. One option that has been suggested lately is to install an alternate browser[7,8]. Internet Explorer (IE) is fairly old software that has not had a major revision since the introduction of Windows XP. Windows XP Service Pack 2 has added features that make IE competitive with more current browsers, but many people are beginning to switch to alternative like Firefox and Opera (see Appendix A for URLs). Although alternative browsers are gaining popularity, it is likely you will still need to use IE for Windows Updates, Office Updates, and any sites that are incompatible with alternative browsers.

If you are using a browser that doesn't yet offer the ability to block pop-up web advertising, you may also want to look into installing a piece of software that performs this function. Pop-up blocking can be a valuable weapon against inadvertent spyware installations. Pop-up web ads is one of the main ways that spyware gets installed. Free pop-up blockers for Internet Explorer are available on the Internet and can be found using just about any search engine. As always, any free utility should be investigated before installation

Another useful tool that not only can protect home users from spyware, but block a good portion of web advertising as well, is a *hosts* file. A *hosts* file is a text file that

---

[6] Arquette, Brett. "Spyware is a Virus." eWeek. 1 Nov 2004.
URL: http://www.eweek.com/article2/0,1759,1683485,00.asp (5 Feb 2005)
[7] Jones, Don. "Time to Dump IE?" Redmond Magazine. Oct 2004.
URL: http://redmondmag.com/features/article.asp?EditorialsID=439 (5 Feb 2005)
[8] Herzog, Heather. "Change in Internet Browsers Recommended." Penn State Live. 8 Dec 2004.
URL: http://live.psu.edu/story/9376

some operating systems, including Windows, use to match an Internet domain name like *www.yahoo.com* with its associated IP address (i.e. 216.109.117.106). Usually a *hosts* file is not used for anything these days since most Internet-connected computers use a Domain Name Server (DNS) to do this matching instead. As a result, it is possible to create a *hosts* file that redirects undesirable web sites to the loopback IP address (127.0.0.1) without affecting the ability to browse to other web sites. When a web browser attempts to go to one of those undesirable sites the web browser window will show an "Action Cancelled" message in the browser window instead of going to the web site.[9] Fortunately, there are a few sites that have already done the difficult task of compiling a list of sites most users will want to avoid, and created *hosts* files that anyone can download (See Appendix A for URLs). Those sites also provide great explanations on how to implement the *hosts* file, in addition to making use of some IE features to assist in blocking undesirable web sites. Once a user has created or downloaded a *hosts* file, the existing blank *hosts* file should be replaced with the new one. In order for the *hosts* file to continue to be useful, the home user will need to periodically replace it with an updated file, since there are always new undesirable sites being put up on the Internet.

The main idea behind this layer of security is that a home user must be vigilant and practice safe computing while connected to the Internet. To assist with avoiding and blocking known undesirable web sites, it is a good idea to research and understand techniques to modify Windows and IE that provide a safer Web-surfing environment.

Some basic rules of thumb are as follows:

1) Be aware of the web sites you are visiting. Know where you are on the Internet. Is it a reputable site, or is it off the beaten track?
2) Do not click on pop-up ads, including bogus security warnings.
3) Do not install software from random web sites, no matter how useful they may appear to be.
4) Make sure ANY software you want to install is not bundled with spyware. This is especially true for "free" software. Unfortunately, commercial software is not immune from this.[10]
5) Do not open e-mail from people you don't know

### Layer 3 – Get a Security System

Up to this point, the layers of security have been about avoiding and blocking possible threats to the home computing environment. But what if a computer has already been infected with malware? And how does a home user actively prevent malware from getting installed? It's time to talk about ways to combat evolving security threats from

[9] "Blocking Unwanted Parasites with a Hosts File." n.d.
URL: http://www.mvps.org/winhelp2002/hosts.htm (10 Oct 2004)
[10] Lynch, Jim. "TurboTax Customers Strike a Blow Against Intuit." 10 Jan 2003.
URL: http://www.extremetech.com/article2/0,1558,832473,00.asp (13 Nov 2004)

malware. Viruses, Trojan Horses, and spyware are dangerous because they are types of malware that are constantly being modified by unscrupulous individuals who are actively trying to circumvent a computer user's defenses.

Viruses and Trojan Horses can be dealt with for the most part by installing anti-virus software. There are several products available that should provide adequate protection, including a number of free packages (see Appendix A for URLs). In addition to installing anti-virus software, a home computer user should get into the habit of periodically running an on-line virus scan from one of the anti-virus software developers that offer scans on their web site. The best practice for on-line scans is to choose a web site for an anti-virus product that is different from the anti-virus software installed.[11] For example if the software installed is Grisoft™ AVG Anti-virus, then the on-line scan should be run at Trend™ or Panda™ Antivirus web sites (see Appendix A for URLs). Most on-line web virus scanners use ActiveX controls to conduct their scans. That means Internet Explorer is the only browser that can to be used. Needless to say, if a web scanner finds a virus that the installed software missed, it may be time to switch to another anti-virus software product.

In the short time that spyware has been proliferating on the Internet, it has become a large and serious problem. A survey of AOL users found that 80% had spyware installed on their computer compared to 20% infected with viruses[12]. Since spyware is a fairly recent phenomenon, the solutions for preventing it from being installed and/or removing it once it is installed are unfortunately not very mature. There are several useful products available for free. Two software programs that provide some measure of spyware protection are SpywareBlaster and SpywareGuard by Javacool Software™. The two best known products for spyware removal are Lavasoft™ Ad-aware and Spybot Search & Destroy(see Appendix A for URLs). At this time, there is no one complete solution for the prevention and removal of spyware that performs as well as most anti-virus software packages do with respect to viruses.[13] Anti-virus software developers have recently begun adding some anti-spyware protection into their products, which would combine spyware prevention and removal. Microsoft™ has also released a beta version of their anti-spyware program, which is also going to be free to individuals.[14] This software also combines the prevention and removal of spyware. The general consensus for spyware protection and removal is to have one spyware prevention product installed and at least two spyware removal programs installed in

---

[11] Skoudis, Ed. "Finding a second opinion: Using free Web-based AV scanning resources" 4 Nov 2004. URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1022311,00.html (20 Dec 2004)

[12] Roberts, Paul. "AOL survey finds rampant online threats, clueless users." Computerworld. 25 Oct 2004.
URL: http://www.computerworld.com/securitytopics/security/story/0,10801,96918,00.html?f=x10 (30 Oct 2004)

[13] Naraine, Ryan. "Study: Tools Let Spyware Slip Through Cracks." eWeek. 23 Nov 2004.
URL: http://www.eweek.com/article2/0,1759,1731474,00.asp (25 Nov 2004)

[14] Lemos, Robert and Dawn Kawamoto. "Windows anti-spyware to come free of charge." Cnet News.15 Feb 2005.
URL: http://news.com.com/Windows+anti-spyware+to+come+free+of+charge/2100-7355_3-5577202.html (15 Feb 2005)

addition to anti-virus software. That should be sufficient to protect against most types of spyware.

As mentioned above, there is no single Anti-spyware package that will remove all forms of spyware. Even using multiple anti-spyware solutions in combination is only about 70% effective.[15] Some spyware is so insidious that it can only be removed manually. That process usually involves advanced skills like editing the registry. Advanced spyware removal should really only be done by an experienced person who is comfortable working with the registry and takes proper precautions. Even then, it may be less work to simply format the hard drive and reinstall the operating system. While manual removal of spyware is beyond the scope of this paper some links have been provided that may assist in learning how to deal with the more tenacious forms of spyware (see Appendix B for URLs).

Most anti-virus and some anti-spyware software allow the ability to set automated scans. Automated scans are very convenient and can be set for times when a computer is on, but no one is using it. It is still a good idea to run a manual scan regularly to make sure the software is functioning properly.

### Layer 4 - Keeping Up-to-Date

All security software requires frequent updating. The constantly changing nature of many threats, particularly with respect to malware makes that fact a necessity. While some software products have features to automatically keep up-to-date, many do not automatically update. As a result home users need to be diligent about make sure to have their firewall, anti-virus, and anti-spyware software check for updates prior to each scan. One especially important thing to remember is that commercial anti-virus software is usually a subscription service. What that usually means is that license fee you pay for the software entitles you to one year of virus definition updates. After that one year is over, it is necessary to pay the subscription fee for each subsequent year of virus definition updates. This fact does not appear to be well understood by many home users.

While security software updates are important, it is also necessary to make sure to keep all other software on a home computer up-to-date as well. New security holes are found in Microsoft™ Windows practically every week. Fortunately, Windows XP has an Automatic Updates setting that allows a home computer user to make sure that Windows has the latest security patches installed. Home users should be sure to activate Automatic Updates if it is not already active, unless they regularly visit the Windows Update web site (see Appendix A for URL). For users of other Windows operating systems, it is necessary to visit the Windows Update web site on a weekly basis to download and install security updates.

---

[15] Livingston, Brian. "Anti-adware misses most malware." Windows Secrets Newsletter. 27 Jan 2005. URL: http://windowssecrets.com/050127/#story1 (30 Jan 2005)

Recently Service Pack 2 for Windows XP was released. It has added many security modifications and features. In particular it has added a software-based firewall to the operating system. It is not as functional as many of the products currently available, but it does offer some protection to home users. It also adds pop-up blocking functionality to Internet Explorer. Home computer users should try to do some research on any issues with applying Service Pack 2 and follow the installation instructions carefully.

In addition to the operating system, applications can have security patches as well. Take Microsoft™ Office as an example. While updates for Microsoft Office are not as frequent as with Windows, it is still important to visit the Microsoft Office updates web site (see Appendix A for URL) to make sure that the latest Service Packs and security updates are installed. The same is true for any software that is installed on a home computer. Not all software companies make it as easy as Microsoft to update their software, so home users may need to check the software companies' web sites to make sure that the software installed is up-to-date and fully patched.

## Putting It All Together

The first goal of a home computer user should be protecting their computer from the Internet. That goal can be accomplished with either a hardware or software firewall. Implementing both is worthwhile and inexpensive.

Once the home computer is isolated from unsolicited communication from the Internet, the home computer user needs to be cautious when using the Internet. One technique that can assist home computer users in avoiding undesirable web sites and spyware is to use a browser other than Internet Explorer for daily browsing. Another useful technique is using a *hosts* file.

No computer these days should be without anti-virus software. Now anti-spyware needs to be added to that list. Until that software matures, it will be necessary to have a couple of different anti-spyware packages installed. Fortunately, free versions of both types of software are available.

Finally, it is absolutely necessary for home computer users to keep the operating system up-to-date with the latest Service Packs and security updates. Security software needs to be regularly updated in order to continue to provide effective protection. Other applications should be updated and patched as needed, particularly when patches fix security problems.

The layers of security explained above are the simplest and most basic steps to secure a home computer. By no means are they the only steps that can be taken. There are other more advanced techniques that can be used to make a home computer more secure. Sophisticated home computer users are encouraged to continue researching this topic to learn those more advanced techniques.

Once a home computer user has all the tools in place it may be worthwhile to visit some web sites that offer the ability to test a computer's defenses to see if there are any holes that can be exploited by malicious computer users or malware. These scans are also known as penetration tests, since the scan is attempting to penetrate the computer's defenses. There are a few sites that offer penetration test scans for home users (see Appendix A for URLs). If an on-line penetration test shows minimal exposure, it's a good sign.

Home computer security is mainly about vigilance and education. Even with all the right tools in place, computers are still vulnerable if computer users are not careful on the Internet.

## Conclusion

Security for the home computer user is not just about protecting the home computing environment; it's about maintaining ownership over computing resources. Those resources include data on the hard drive, personal browsing history, processor cycles, and even Internet connectivity.

It is an unfortunate fact of life that there are individuals out there who have nothing better to do than try to take advantage of less savvy computer users who are minding their own business on the Internet. It is also unfortunate that so many tools are required to properly secure a home computer. For some people with slower computers, the cure may end up being almost as bad as the disease.

Home computer security issues are beginning to get recognition from the government as well as the private sector. Virus writers have been caught and punished[16,17], and legislation is in the works to punish spyware authors as well.[18] Some computer vendors have begun to feel the pinch of increased support calls related to spyware and have decided to take action.[19] Some Internet Service Providers are also recognizing the threat of spyware.[20]

The slow response time of both the government and the private sector to the security threats on-line are strong indicators that home computer users will need to continue to be vigilant in maintaining their own security for the foreseeable future. In addition, the

---

[16] United States. Department of Justice. Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison. 1 May 2001. URL: http://www.usdoj.gov/criminal/cybercrime/melissaSent.htm (15 Feb 2005)

[17] "Teen sentenced for Blaster worm variant." CNN. 29 Jan 2005. URL: http://www.cnn.com/2005/TECH/internet/01/28/internet.attack.ap/ (15 Feb 2005)

[18] United States. House of Representative. House Resolution 29 – Securely Protect Yourself Against Cyber Trespass Act. 4 Jan 2005. URL: http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.29: (note the trailing colon) (19 Feb 2005)

[19] Claburn, Thomas. "Dell Believes Education Is Best Way To Fight Spyware." InformationWeek. 20 Oct 2004. URL: http://informationweek.com/showArticle.jhtml?articleID=50900097&tid=16034 (10 Nov 2004)

[20] Roberts, Paul. "AOL Goes After Spyware." PCWorld. 6 Jan 2004. URL: http://www.pcworld.com/news/article/0,aid,114106,00.asp (10 Nov 2004)

dynamic nature of the threats on the Internet means that home computer security is a moving target. Home computer users will need to stay informed regarding the latest threats to their security. In the meantime, while we wait for a utopian Internet where everyone is safe to surf the Web without fear of being attacked or taken advantage of, prudent home computer users will have to take appropriate steps to defend themselves.

**Appendix A – URLs for software mentioned in the paper as well as some not mentioned**

Alternative Web Browsers to Internet Explorer

| | |
|---|---|
| Firefox | http://www.mozilla.org/products/firefox/ |
| Opera | http://www.opera.com/ |

Host Files

http://www.mvps.org/winhelp2002/hosts.htm
http://www.everythingisnt.com/hosts.html
http://accs-net.com/hosts/what_is_hosts.html

Free Anti-spyware Sofware

| | |
|---|---|
| Spybot Search & Destroy | http://www.safer-networking.org/en/index.html |
| Lavasoft™ Ad-aware | http://www.lavasoft.de/ |

Microsoft™ Anti-Spyware Beta
http://www.microsoft.com/athome/security/spyware/software/default.mspx
Other free anti-spyware software
http://www.thefreecountry.com/security/spywareremoval.shtml

Free Anti-Virus Software

http://free.grisoft.com/freeweb.php/doc/2/
http://www.avast.com/eng/avast_4_home.html
http://www.free-av.com/
http://www.thefreecountry.com/security/antivirus.shtml

Free On-line Web Virus-Scanners (you can use these to run scans from the web)
http://housecall.trendmicro.com/housecall/start_corp.asp (ActiveX)
http://www.pandasoftware.com/activescan/
http://security.symantec.com/
http://www3.ca.com/securityadvisor/virusinfo/scan.aspx
http://www.bitdefender.com/scan/licence.php
http://www.ravantivirus.com/scan/indexie.php
http://uk.trendmicro-europe.com/enterprise/products/housecall_launch.php (Java)
http://us.mcafee.com/root/mfs/default.asp
http://www.windowsecurity.com/trojanscan/ (Scans for Trojans)

Free Firewall Software

http://www.thefreecountry.com/security/firewalls.shtml
http://www.pcworld.com/howto/article/0,aid,112920,00.asp

Free On-line Penetration Testing

http://www.grc.com/default.htm (click on Shields Up!)
http://security.symantec.com/default.asp?productid=symhome&langid=ie&venid=sym
(click Start under Security Scan)

Free On-line Penetration Testing (continued)
http://www.dslreports.com/scan
http://scan.sygate.com/
http://www.auditmypc.com/freescan/prefcan.asp

Microsoft™ Updates

| | |
|---|---|
| Windows Update | http://Windowsupdate.microsoft.com |
| Office Update | http://Officeupdate.microsoft.com |

**Appendix B – Advanced Topics in Spyware Removal**

http://www.io.com/~cwagner/spyware/
http://www.firewallguide.com/spyware.htm
http://www.pcworld.com/howto/article/0,aid,118508,00.asp
http://spywarewarrior.com/
https://netfiles.uiuc.edu/ehowes/www/soft6.htm
http://www.benedelman.org/
http://msn.pcworld.com/howto/article/0,aid,117879,00.asp
http://msn.pcworld.com/howto/article/0,aid,118058,00.asp
http://msn.pcworld.com/howto/article/0,aid,118060,00.asp
http://msn.pcworld.com/howto/article/0,aid,118215,00.asp

## References


Acohido, Byron and Jon Swartz. “Unprotected PC may be hijacked in minutes.” USA Today. 30 Nov 2004.
URL: http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm (5 Dec 2004)

Arquette, Brett. “Spyware is a Virus.” eWeek. 1 Nov 2004.
URL: http://www.eweek.com/article2/0,1759,1683485,00.asp (5 Feb 2005)

“Blocking Unwanted Parasites with a Hosts File.” n.d.
URL: http://www.mvps.org/winhelp2002/hosts.htm (10 Oct 2004)

Claburn, Thomas. “Dell Believes Education Is Best Way To Fight Spyware.” InformationWeek. 20 Oct 2004.
URL: http://informationweek.com/showArticle.jhtml?articleID=50900097&tid=16034 (10 Nov 2004)

Herzog, Heather. “Change in Internet Browsers Recommended.” Penn State Live. 8 Dec 2004. URL: http://live.psu.edu/story/9376

Harbour, Thomas. “Defense in Depth on the Home Front.” 3 Apr 2003
URL: http://www.sans.org/rr/whitepapers/honors/1504.php (20 Feb 2005)

Jones, Don. “Time to Dump IE?” Redmond Magazine. Oct 2004.
URL: http://redmondmag.com/features/article.asp?EditorialsID=439 (5 Feb 2005)

Leath, Patria. “A Discussion of Spyware.” 2 Nov 2004.
URL: http://www.sans.org/rr/whitepapers/awareness/1546.php (1 Feb 2005)

Lemos, Robert and Dawn Kawamoto. “Windows anti-spyware to come free of charge.” Cnet News.com. 15 Feb 2005. URL: http://news.com.com/Windows+anti-spyware+to+come+free+of+charge/2100-7355_3-5577202.html (15 Feb 2005)

Livingston, Brian. “Anti-adware misses most malware.” Windows Secrets Newsletter. 27 Jan 2005. URL: http://windowssecrets.com/050127/#story1 (30 Jan 2005)

Lynch, Jim. “TurboTax Customers Strike a Blow Against Intuit.” 10 Jan 2003.
URL: http://www.extremetech.com/article2/0,1558,832473,00.asp (13 Nov 2004)

“Man cleared over porn ‘may sue’.” BBC News UK Edition. 31 July 2003.
URL: http://news.bbc.co.uk/1/hi/england/devon/3114815.stm (5 Feb 2005)

Martin, Kelly. “When spyware crosses the line.” The Register. 24 June 2004.
URL: http://www.theregister.co.uk/2004/06/24/spyware_crosses_line/ (2 Feb 2005)

Montgomery, Garth. “Daily Dispatch (Opinion) – Kazaagate Day 15: part 4.” Apcmag.com. 7 Feb 2005.
URL: http://www.apcmag.com/apc/v3.nsf/0/07A1C8CA269E79B5CA256FA1000F9763 (9 Feb 2005)

Munson, Shauna. “Defense in Depth and the Home User: Securing the Home PC.” 24 Jan 2003. URL: http://www.sans.org/rr/whitepapers/hsoffice/894.php (27 Dec 2004)

Naraine, Ryan. “Study: Tools Let Spyware Slip Through Cracks.” eWeek. 23 Nov 2004.
URL: http://www.eweek.com/article2/0,1759,1731474,00.asp (25 Nov 2004)

Roberts, Paul. “AOL Goes After Spyware.” PCWorld. 6 Jan 2004.
URL: http://www.pcworld.com/news/article/0,aid,114106,00.asp (10 Nov 2004)

Roberts, Paul. “AOL survey finds rampant online threats, clueless users.” Computerworld. 25 Oct 2004.
URL:
http://www.computerworld.com/securitytopics/security/story/0,10801,96918,00.html?f=x10 (30 Oct 2004)

Skoudis, Ed. “Finding a second opinion: Using free Web-based AV scanning resources” 4 Nov 2004.
URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1022311,00.html (20 Dec 2004)

Sleekluxury. “SLEEKLUXURY'S GUIDE TO COMPUTER SECUIRTY(sic).” 15 Feb 2004. URL: http://forums.techguy.org/showthread.php?threadid=204050& (10 Nov 2004)

“Spyware: How to Avoid It.” 26 Nov 2004.
URL: http://www.geekontherun.net/spyware2.htm (10 Feb 2005)

“Teen sentenced for Blaster worm variant.” CNN. 29 Jan 2005.
URL: http://www.cnn.com/2005/TECH/internet/01/28/internet.attack.ap/ (15 Feb 2005)

United States. Department of Justice. Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison. 1 May 2001. URL:
http://www.usdoj.gov/criminal/cybercrime/melissaSent.htm (15 Feb 2005)

United States. House of Representatives. House Resolution 29 – Securely Protect Yourself Against Cyber Trespass Act. 4 Jan 2005. URL: http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.29: (note the trailing colon) (19 Feb 2005)

Weil, Alan C. and Eric W. Vaughan. “Securing Windows XP” Version 1.0. n.d.
URL: http://www.tweakhound.com/xp/security/page_1.htm (5 Jan 2005)

Last Updated: July 24th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| 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 New York City 2017 | New York City, NY | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Salt Lake City 2017 | Salt Lake City, UT | 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 Chicago 2017 | Chicago, IL | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 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 |
| Mentor Session - SEC401 | Arlington, VA | Oct 04, 2017 - Nov 15, 2017 | Mentor |