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.

Free Tools and Tips to Help Secure Your Home PC

The explosion of the Internet and home computer use has created a very lucrative `business' for virus writers, spammers, spyware programmers, and hackers. Most home computer users believe that what they do on the Internet is safe, but we are finding out it is very difficult to stay ahead of the criminals. With so many possible ways to break into a computer, home users need a set of free tools and tips along with some basic user training to protect their online `communications'. This paper will emphasize free software a...

Copyright SANS Institute
Author Retains Full Rights

AD

Free Tools and Tips to Help Secure Your Home PC

By

John K. Hochevar

Practical Submission for the SANS GSEC Certification (Option 1, Version 1.4b)

November 9th, 2004

© SANS Institute 2005, Author retains full rights.

Abstract

The explosion of the Internet and home computer use has created a very lucrative 'business' for virus writers, spammers, spyware programmers, and hackers. Typically a home will own at least one computer that is shared by the household. The members of the family do a range of activities that may include e-mail, online banking, school research, etc. Most home computer users have the thought that what they do on the Internet is safe, but as we are finding out it is really becoming a cat and mouse game trying to stay ahead of the criminals. With all the different possibilities to break into a computer the home users need a set of free tools and tips along with some basic user training to make sure that their online 'communications' are protected.

This paper will emphasize free software alternatives to combat viruses/Trojans, protect against spyware, provide safe Internet browsing, prevent computer intrusions, and eliminate pop-ups. The software will all be for the Windows OS platform, concentrating on users with Windows XP SP1 and SP2. Each category will discuss the inherit risks and include a few pieces of free software that can help mitigate risks. In the second half of the paper, I will discuss Windows SP2 and also provide tools to give a baseline analysis of how 'secure' the machine is. This section will also include some basic settings within Windows XP that can be turned on or off to help secure the machine. The third and last portion of the paper will include end-user training that will include some easy to follow tips on safe computing.

Why this is important

Take a moment to think about how you have used your home computer in the past twelve months. I could bet that you have done at least one of the following, if not all of them:

- Online banking (Pay bills, read credit card statements…)
- Read/submit e-mail
- Chatting with friends, family, or co-workers
- Purchase items using a credit card
- Submit your taxes
- Store your family finances on your computer
- Logged into an account

These are all items that I am positive a home user would want to keep private and away from the intrusive people out on the Internet. These are also things that, if not properly secured can be shared on the Internet, whether it is on accident, or by someone snooping around on your machine.

There are preemptive measures that a home user can take to ensure the integrity and confidentiality of the information they access or store using their home

© SANS Institute 2005 Author retains full rights.

computer. But besides having tools that can keep viruses off your machine, or spyware from invading your computer, a user must be trained to watch out for scams and be knowledgeable of what they are doing.

As the number of users connecting to the Internet via a broadband source increases, so do the security risks. Broadband users are attractive in many ways. A new trend is developing where virus writer and spammers are teaming together to create 'zombie' networks of computers. A large number of the recent mass-mailing e-mail viruses allow the virus, once it infects the machine, to create a connection back to websites where it will upload information about the infected machine. The spammers will get involved to use these 'owned' machines to relay e-mail messages to their victims. The spammers love it because it creates a problem in tracking down who is responsible for originating the spam message.

These 'zombie' networks can also be used as computing power to spread viruses. A virus writer might load a new virus to an already infected machine to spread it to other computers. The virus writers like this for the same reason as the spammers do, it makes it much harder to find who started it.

The 'zombie' networks are causing havoc for Internet Service Providers. Comcast cable is a major provider of cable and broadband Internet service. Comcast broadband subscribers have created some of these 'zombie' networks unbeknownst to them. Daily e-mail totals of sent messages by Comcast subscribers have easily surpassed the 500 million mark. Comcast was able to combat this major problem by blocking SMTP traffic (TCP port 25; used by such products at Outlook and Outlook Express to send outgoing messages) at their major gateway. Doing this has reduced sent e-mail messages by 35 percent from Comcast subscribers, but it has not fixed the problem of all of these 'zombie' computer networks. (Hu, ZDnet)

For more information about Internet Service Providers and how many e-mails their subscribers send out each day, please visit: www.senderbase.org. You can also search by domain name for other web sites or companies you might be interested in seeing their e-mail statistics.

Free tools as alternatives to commercial products

Battling Spyware

Spyware is software that is installed unbeknownst to a computer user for a variety of reasons. Spyware is one of the ways to create a 'zombie' network as mentioned before. Spyware is used to 'infect' machines to send out spam e-mail messages, perform a Denial of Service attack (MyDoom.B e-mail virus attempted to perform a Denial of Service on the Microsoft homepage, but was unsuccessful (Author Unknown, eWeek), steal personal data such as credit card numbers, or even track the keystrokes you perform on your computer.

© SANS Institute 2005 Author retains full rights.

Some also consider adware in the same group as spyware. Adware is used to track the websites a user visits. They correlate the data to determine what kind of marketing item should reach the computer user in the form of a pop-up ad or a banner add on the top of a website.

Spyware has become such a problem that there is now a bill on the U.S. Senate floor (Thomas) just as there was a bill passed to convict e-mail spammers. Within this bill, the software considered as spam cannot be installed without the user knowing about it, it must have an easy uninstall option, and it cannot release information to the Internet without the consent of the user. (McCullagh, ZDnet) Some programs that are common, and would pass under this bill are Gator and Bargain Buddy. These programs are usually installed with other software programs. The user is prompted to acknowledge the installation of these, but the installation is usually so discreet and uninformative, that the user just continues to click, 'NEXT' or 'FINISH' until their original program they wanted was installed.

The two tools I use religiously in battling spyware are Adaware's SE Personal (http://www.lavasoftusa.com/) and Spybot's Search and Destroy (http://www.safer-networking.org/en/index.html.)

Both utilities have free for personal use versions and versions that you can buy with additional features. The free versions are sufficient to battle most spyware problems. These utilities are two of the first things I use on a friend's or family member's computer when they complain that their computers are running slow, or are having problems connecting to the Internet.

The best thing to do to battle spyware is to use both of these products in tandem. Sometimes Spybot Search and Destroy will find things that Adaware SE Personal will not and vise versa. The great thing about both of these utilities is that they have built-in update components. As long as you are connected to the Internet, you can update the signatures/definitions the programs use to identify and remove spyware components from a computer. You might be surprised the first time you run one of these programs as to the amount of possible spyware programs are found on your machine. A large number of spyware files found are usually cookie's placed on your machine by websites. These cookies are forms of adware which I mentioned earlier. It is just as important to clear these cookies out of your system, as it is to clear the rest of the spyware programs off.

Adaware SE Personal has a great forum where a user can ask questions or post their scan log results for further review and help. That forum can be found here:

http://www.lavasoftsupport.com/index.php?s=54db6bdebd336a543d491e7e999c9d48&c=36

© SANS Institute 2005 Author retains full rights.

Spybot Search and Destroy has FAQ and Contact links on their homepage. You can also use Google to search for 'Spybot Search and Destroy Forums':

http://www.google.com/search?hl=en&q=spybot+search+and+destroy+forum&btnG=Google+Search

Follow this link provided by Cnet downloads to learn further about Spyware tools, and try other Spyware utilities:

http://www.download.com/Spyware-Center/2001-2023_4-0.html?tag=dir

Protecting against Viruses and Worms

With the prices of computers drastically dropping in the past year, a lot of families are purchasing new machines for home use, or to send off with their kids in college. I'm familiar with a lot of people buying Dell machines. Dell offers free trial versions of McAfee or Symantec AntiVirus with each new purchase of a computer. These free trials usually last 90 days. So what happens when those trials expire, and the virus definitions go out of date? The user usually ignores them, and they end up getting infected with a virus and wonders why their machine slows down or fails to respond. Even if they do decide to sign-up for a year of service, they have to pay the same fee every year that they have the software!

Even though I normally use a commercial product that work has given me, I have also tested out the free AntiVirus product AVG AntiVirus. (http://free.grisoft.com/freeweb.php/doc/1/)

AVG doesn't seem as intrusive and doesn't bog down your system as much as a Symantec of McAfee product might. That being said, one might wonder if AVG AntiVirus is doing as good of a job as the Symantec or McAfee product. In my trials in comparing AVG and Symantec, AVG was able to keep up with the rash of mass-mailing e-mail worms that have sprung about in the past 6 months. I was thoroughly impressed with its performance, and would definitely recommend it if someone does not want to pay $50 a year renewing their commercial product.

AVG has the typical features of many AV products:

- Auto updates
- Real time scanning the moment a file is written to hard or floppy disk (includes USB drives)
- Scanning of incoming and outgoing e-mail messages
- Allows the scheduling of updates and scans
- E-mail support 24 hours a day, all year long

© SANS Institute 2005 Author retains full rights.

For help installing or using AVG Antivirus, please refer to this link from the AVG website: http://free.grisoft.com/freeweb.php/doc/3/lng/us/tpl/v5

In the event that you do not use AntiVirus software, or your AntiVirus software did not save you from infection, there are several AntiVirus vendors that offer free virus removal tools. My favorite is the Stinger from McAfee:

http://vil.nai.com/vil/stinger/

Stinger scans for a number of viruses during one sweep. It is very useful for a machine that you want to do a system check on, and try to clean all the viruses off at once. The link provided shows some Frequently Asked Questions, along with an update history showing the different viruses it can identify and clean from your system.

Symantec (www.symantec.com) and Sophos (www.sophos.com) also provide removal tools. Unfortunately, if you have a system infected with multiple viruses you will need to run individual removal tools.

It would be handy to keep virus removal tools on a USB thumb drive along with the spyware removal programs I mentioned earlier. If you are like me and run around house to house helping repair computers, the USB thumb drive is a great thing to have in your tool bag.

Follow this link to Cnet downloads to try other versions of AntiVirus software:

http://www.download.com/Antivirus/3150-2239_4-0.html?tag=dir

Using a personal firewall to protect against intruders

One of the easiest things you can do to protect you home computer is to use a software based personal firewall. Most personal firewalls are very interactive with the user, making it clear what program is trying to access the Internet, or what source is trying to access your computer from the Internet.

My favorite free personal firewall is a product by Zone Labs called Zone Alarm (http://www.zonelabs.com/store/content/home.jsp.) Zone Alarm was the first personal firewall that I used once I had a broadband connection at home and at work.

After an easy installation, there is a period of discovery involved with Zone Alarm and the programs that you use that access the Internet. Some popular applications that you might use are Outlook Express, AOL Instant Messenger, and Internet Explorer. Each time an application will try to access the Internet, Zone Alarm will prompt the user giving them some choices:

© SANS Institute 2005 Author retains full rights.

- Allow this program to always access the Internet
- Allow this program to access the Internet once (Will prompt again the next time it tries to access the Internet)
- Block this program from accessing the Internet always
- Block this program from accessing the Internet once (Will prompt again the next time it tries to access the Internet)

The free version of Zone Alarm also claims to make your computer invisible to intruders on the Internet. Zone Alarm uses a simplified intrusion detection system to block potential attack attempts from sources on the Internet. If your machine gets infected with a virus, Zone Alarm will prompt the user if that virus tries to make a backdoor connection to the backend web site where the virus would update data, or spread to other machines. This helps to notify the user that they are infected, so that they can use a virus removal tool, and update their virus definitions.

Some helpful Zone Alarm tips:

- There are several typical applications used within the Microsoft Operating System that will need access to the Internet to run a number of your applications. If you don't recognize the application that is trying to connect, type the name of that application into a Google search.
- Some typical applications such as Internet Explorer, AOL Instant Messenger, and Outlook Express continuously contact sources on the Internet. It is recommended to allow these programs always, unless you have the patience to click on the 'Allow Once' option repeatedly.
- If you make a mistake in allowing an application access to the Internet, you can always go back into the Zone Alarm configuration, and change the user-defined settings.

To view and test other personal firewall software, please take a look at the Cnet downloads page:

http://www.download.com/3120-20_4-0.html?qt=firewall&tg=dl-2001&search.x=0&search.y=0&search=+Go%21

Windows XP Service Pack 2 is delivered with a built-in software firewall. I will be discussing this later in the paper.

Internet Browser Wars

One of the hottest topics in the Microsoft world is the continuous release of security vulnerabilities within Internet Explorer. Internet Explorer is used by around 90% of all Internet users, which makes the browser a huge target for hackers.

© SANS Institute 2005 Author retains full rights.

Internet Explorer vulnerabilities are exploited in a variety of methods. A recent flaw in Internet Explorer is exploited by a new flavor of the MyDoom family of viruses. A user can click on a link, which sends them to a malicious web site whose content slips past the major AntiVirus companies scanning engines. An instance where an exploit is released before AntiVirus companies can update their definitions, and a software vendor can issue is patch, is called a, 'Zero Day Exploit.' The only way to avoid something like this is to warn the users not to commit the actions necessary to infect the machine (Lemos, ZDnet) Another recent flaw in Internet Explorer allows malicious coders to hide links within a hyperlink on a webpage. A user will click on a link thinking it will take them to a legitimate webpage, but it really sends them to a webpage that will download malicious code. This type of attack is frequently used in 'phishing' scams. I will cover 'phishing' scams later in the paper.

To combat the negligence of the Internet Explorer browser and Microsoft's inability to create a safe browsing environment, I recommend switching to the Mozilla Firefox browser. CERT (Computer Emergency Readiness Team) released a statement in June recommending that users use anything **BUT** Microsoft's Internet Explorer (Oates, theRegister) CERT feels that Internet Explorer is not safe enough for a user to maintain a secure browsing environment on the Internet.

Switching to Firefox is quite easy. Go to http://www.mozilla.org/products/firefox/ and download its first mainstream release of Version 1.0. By viewing that link, you can also see the benefits of using Firefox vs. Internet Explorer:

- Popup blocking (In testing, some web sites can still sneak their popup ads onto your desktop, or within an existing browser window)
- Tabbed browsing – a great feature that lets you open up multiple browser sessions within one browser 'container'
- Blocks the download of ActiveX controls which Microsoft was notorious for doing pre-Service Pack 2. ActiveX controls have become a major gateway for spyware to reach a user's computer
- Fully customizable to add any useful plugins developed by the large group of open source programmers

But, every piece of software can't be perfect. As displayed in this editorial by John Carroll, Firefox has a difficult time rendering some web pages that work just fine in the Internet Explorer browser. (Carroll, ZDnet)

If you are not satisfied with Firefox, and are still too frightened to go back to Internet Explorer, you can give Opera (http://www.opera.com/) a try, or switch to the MAC OS and use Safari (http://www.apple.com/safari/) which is built into the OS.

© SANS Institute 2005 Author retains full rights.

I think any home user will do fine with Firefox, but for those 1% of web sites that don't work right, quickly switch to Internet Explorer, and don't forget to come back home to Firefox!

Outlook and Outlook Express follow in the footsteps of IE

Along with the monthly release of patches for Internet Explorer, you can usually find a patch for vulnerabilities in Outlook/Outlook Express every three or four months. Even though the attacks on Outlook/Outlook Express aren't as famous as the ones for Internet Explorer, as a security professional I recommend using a different e-mail client.

Having just introduced you to Firefox as a browser alternative, I would like to recommend its Mozilla counterpart, Thunderbird (http://www.mozilla.org/products/thunderbird/.)

Thunderbird is very easy to install and setup. It allows you to use the same e-mail accounts that you were using within Outlook/Outlook Express whether they be from Hotmail, or your local broadband provider. Thunderbird uses a junk mail filter similar to those used within the web mail clients Hotmail and Yahoo!. These filters will store possible junk mail in a separate folder, allowing you to determine what is, and what is not junk. Another great feature is a fully customizable spam filter. Anytime you receive an e-mail that you didn't sign up for, or an e-mail you have no idea why it was sent to you, you can mark those e-mails as spam. Each new e-mail will pass through your updated spam filter looking for consistencies between the new message and any messages in the filter. If there are any similarities, the new message will be flagged as spam, and added to the spam folder. If it does not match any characteristics, it will be passed to your inbox whether or not it is legit. And the trend continues where you make decisions on legitimate e-mail, junk mail, and spam e-mails.

Other free e-mail tools that are great alternatives to Outlook/Outlook Express are Pegasus Mail (www.pmail.com) and a lot of web mail clients such as Hotmail (www.hotmail.com), Yahoo! Mail (mail.yahoo.com), and Google Mail (gmail.google.com). However, be careful with some of the web mail clients as they have had vulnerabilities in the past.

As always with open source software, please visit their homepages regularly looking for software updates and patches. As open source software becomes more popular to users, they will also become more popular to hackers.

Blocking those annoying popups!

Most users are just annoyed by those popups or popunders that are mainstays with a lot of popular web sites such as www.cnn.com and www.espn.com. What most users don't know is that popups from some websites can contain malicious

© SANS Institute 2005 Author retains full rights.

payloads full of spyware. Not only are these popups used for advertisements, but they are also used to track your Internet experience.

To protect against these annoying and sometimes harmful popups, a user has several options available. If you are using the Firefox browser, a pretty resilient popup blocker is already installed for you. If you insist of sticking with Internet Explorer, I recommend using the Google toolbar (http://toolbar.google.com/.) Not only does it do a great job in blocking popups, but it also allows a user to do a quick Google search right within the internet Explorer browser.

Other browser toolbars can be downloaded from Microsoft and Yahoo!. You can also try stand-alone browser popup software available for download on the Cnet downloads page:

http://www.download.com/Pop-Up-Blockers/3150-7786_4-0.html?tag=dir

Evaluating your Windows security

Microsoft offers a great utility called the Microsoft Baseline Security Analyzer (MBSA; http://www.microsoft.com/technet/security/tools/mbsahome.mspx.) The MBSA allows a user to do a quick scan of their system to evaluate its security.

MBSA will search for missing patches related to the operating system and it will also search for missing patches related to Microsoft software. It can check user accounts to see if they have passwords, and check against password policies for each account.

I recommend that anyone using the Windows Operating System download MBSA from the link provided to take a look at the security of your Windows system.

Windows XP Service Pack 2

Firewall Improvements

The software firewall in Windows Service Pack 1 wasn't very popular for most home users. It was very cumbersome to configure, which made it very user unfriendly. Service Pack 2 brings some noticeable improvements to the home user. The new Windows firewall tries to act as the commercial software firewalls act. It will prompt the user anytime an application tries to connect to the computer from the Internet. The prompt shows the user the application name, the manufacturer of the application, and a link to that manufacturer's homepage. The user now has a more granular approach to using the firewall because Microsoft made it much easier to configure for the home user.

© SANS Institute 2005 Author retains full rights.

The new firewall does have its downsides however. One noticeable disadvantage to this firewall is that is does not block or filter outbound traffic from leaving the computer. This will not aide in stopping a virus from propagating across the Internet. It will also not stop malicious spyware from sending information back to the backend spyware server.

Another downside is that the firewall only filters on packet headers. This means that it will only filter based on port number, not on the payload that the connection carries. The firewall will allow legitimate and malicious code over TCP 80 because it cannot tell the difference between the two. Other free and commercial firewalls will analyze the entire payload and compare it to intrusion signatures.

New Browser features

Microsoft added a popup blocked to the Internet Explorer 6.0 browser. This popup blocker acts pretty much the same as the built-in popup blocker within the Firefox browser, and the popup blocker toolbars.

A similar feature is related to the blocking of automatic downloads of ActiveX controls. ActiveX controls are used primarily to allow applications to communicate within the browser. Previous versions of Windows and IE allowed the automatic download of these ActiveX controls, and spyware/virus writers took advantage of this and built malicious code into websites using ActiveX controls.

Another helpful feature is what I refer to as 'download awareness.' If you attempt to download a file or a program from within Internet Explorer, the browser will prompt you with a warning. The warning will ask you to make sure you want to save this file, or run it directly from the download source. It shows you the filename, and any specific warnings with downloading certain files. This is something that can be very helpful when accidentally trying to launch attachments that you get in your e-mail accounts, especially if a virus is attached.

Automatic Updates

I view automatic updates as a critical part of the Windows Operating System. Many people don't have time to spend searching for new Windows updates. Within the automatic updates console, you can schedule downloads and installations of the critical updates for the Microsoft components. I have my updates scheduled to check and download every day at 3am. The only reason I don't have the automatically installed is that I might be running a certain process on my machine, and I don't want the machine to automatically reboot.

I recommend for the normal home user to setup their automatic updates to download and install the updates automatically. This provides a hands-free approach to updating your operating system.

© SANS Institute 2005 Author retains full rights.

Alternatively, a user can manually download updates for Windows Update. The link for Windows Update is windowsupdate.microsoft.com.

Security Center

The Microsoft Security Center provides a central location to review the status of some of the new security features. The Security Center provides information on the Windows firewall, your AntiVirus status, and another link to configure Automatic updates.

Personally, I don't think that the Security Center provides any value. The AntiVirus status has problems with several major AntiVirus products. For the most part it can pickup that AntiVirus is installed, but it is unable to keep track of the definition status. Several AntiVirus companies had to create patches for their products to interact with the Security Center's API.

Whether or not you pay attention to the Security Center, you should definitely configure automatic updates, have AntiVirus installed, and run some sort of personal firewall even if it is Microsoft's SP2 firewall.

These improvements and others were taken from the list of top ten reasons to upgrade to XP Service Pack 2 (Microsoft)

Quick and easy end-user training

Due diligence when installing applications

Some spyware and other malicious programs have a very sneaky way of being installed on your machine. Two of those aforementioned programs are Gator and Bargain Buddy. These applications are normally installed during the installation of another program. The way the software writers can do this is by sneaking some statements into the license agreements. It is important for a user to at least skim the license agreements before installing a piece of software they bought or downloaded. I don't expect someone to read the entire thing, but at least pay attention to the section headers within the agreement.

When installing an application, make sure you know what the application is for, and why you are even installing it in the first place. Some web sites will popup messages to a user asking them to install certain certificates or plug-ins to allow certain pages to render correctly within an Internet browser. If you don't know why these things are popping up, cancel them. Most of the time a user will realize that the web page will work just fine without installing those software pieces. Some web sites require the use of a Flash engine. Flash was developed primarily by Macromedia to display advanced web pages to a user. If you are trying to use a flash-based site, it is ok to download the plug-in related to flash.

© SANS Institute 2005 Author retains full rights.

Keeping track of what your kids do on the computer

Keeping track of what your kids do on the computer not only protects the computer, but it also keeps the kids out of trouble. Sexual predators have been using the Internet for years by joining chat rooms looking for younger kids to talk to and meet. Links to websites that your children might go to could contain inappropriate material or contain malicious code that can infect your machine with viruses and spyware. By controlling what your kids can and cannot access will protect your computer, protect your data, and protect your children.

IE History

A quick way to check which websites your kids are going to is by checking Internet Explorer's history. You can do this by pressing CTRL+H when the Internet Explorer browser is the active windows on your screen. The same command also works in Mozilla's Firefox browser. The browsers will open a toolbar on the left hand side, listing each website that the user has gone to for the past 'X' number of days, where 'X' is the number of days configured to save the Internet history. This setting can be configured in Internet Explorer by going to 'Tools → Internet Options → History → Change the number of days → Click OK.' Within Firefox you can go to 'Tools → Options → Privacy → History → Change the number of days → Click OK.'

Installed Programs

You can check up on what your kids are installing a few different ways. You can check the Add/Remove programs utility within the Control Panel. That will list most of the installed applications on a machine. You can also look at all the program files within the start menu to see all the applications and utilities installed. Lastly, you can check Microsoft's Rapid Restore menu to see what applications were installed on what day. The Rapid Restore menu allows a user to fallback to certain restore points in the event of an operating system failure.

Instant Messenger download folders

If your children use any one of the popular instant messenger software, you might be able to find files that they have sent or received from friends online. The folder where these files could be located would be named after their screen names. Files also shared during 'Direct Connect' sessions might also get stored here. Such files could be music, videos, or pictures.

Instant Messenger chat dialogue

Some instant messenger clients allow the user to save their chats by default. These chats are normally also located within the screen name folder within the application's Program Files directory. The chats will be listed by screen names

© SANS Institute 2005 Author retains full rights.

that your children communicate with. Each log file will contain the entire dialogue between the user and their online 'buddies' since the time the application was installed.

Temporary Internet Files

Internet Explorer, Firefox, and other browsers cache images, text, etc. within the browser. This allows for faster web page processing the next time you access a previously accessed page. Within this folder, you can sort by file type in case you want to look for inappropriate pictures and videos.

Browser cookies

Browsers are installed by default to use cookies on web pages that make use of them. The cookies store data about your visits to certain web pages. The cookies can also store userid and password information to allow a user to automatically login to a web page every time that they access it. By reviewing the cookies, you can also see a list of sites that has been visited by the user. The sites listed can be sites typed into the browser, and also sites that are accessed by banner ads and popup ads.

Google Desktop Search Tool

The Google Desktop Search Tool is a brand new utility released by Google (http://desktop.google.com/.) Once installed, the search tool will index your entire hard drive looking for:

- E-mails from Outlook/Outlook Express
- Instant Messenger chat logs
- Documents from Word, Excel, PowerPoint, Notepad etc.
- Internet Explorer Web Pages

This can be a great tool for parents to use when searching for files that were downloaded by their children, looking for chat logs, and checking on their e-mail accounts. The indexing doesn't take a very long time either.

The negative side to the Google Desktop Search tool isn't related to home use as much as it is related to use on public computers. Not only do you have to be careful on your home machine, but these types of applications can be installed on kiosk computers, or computers in coffee shops and universities. When using a public computer, I recommend only using it for anonymous access. Don't sign into online accounts, don't buy anything with your credit card, don't check your e-mail, and don't chat online with your friends. All of these things can be indexed by the Google Desktop Search Tool without you knowing about it.

© SANS Institute 2005 Author retains full rights.

File sharing programs

File sharing programs are a large contributor to spyware and virus problems. A lot of viruses in the past 6 months would load infected files into the KaZaA shared folder after infecting a machine. The infected files would be named after popular download files for copyrighted music, videos, and software, which are definitely the main purpose of using a file share network. Spyware writers have attached their malicious programs to legitimate downloads shared across file share networks. Along with the shared files, the file sharing programs themselves install spyware on user's machines unbeknownst to them.

Another reason to keep yourself and your children away from file share networks is the legal recourse that can be taken on the family if they are sharing copyright protected material. The explosion of file share networks primarily started to share mp3's across campuses. Now the file share programs have become popular in the home, and now are sharing copyrighted movies, videos, and software.

Staying away from file sharing programs not only keeps you away from viruses and spyware, but it also keeps you away from legal trouble.

Signing up for online forums, mailing lists, online accounts

A user's usernames and passwords are very valuable to prying eyes on the Internet. E-mail addresses are also just as valuable to spammers. It is important to protect your online accounts and e-mail addresses on the Internet. Here are some tips that I follow when using online accounts and signing up for things with e-mail addresses:

- Create a throw-away e-mail account. I use a separate e-mail account to signup for online offers, or other things where I do not want their e-mail notifications to pry into my personal e-mail accounts.
- Don't use the same username and password for each online account. If someone is able to obtain your username and password for one online account, they might try and use it on other popular sites such as Web mail sites and online merchants. This is especially important if you store your credit card information within some online merchant sites (I recommend against using this, but it does make online shopping much easier.)
- Create hard-to-guess passwords for your accounts. A password should contain letters, numbers, and special characters (! @ # $ % ^ ?, etc…)
- If you have a hard time remembering all your usernames and passwords for certain online sites, try using a password management application that will encrypt and store all your accounts. I have evaluated Password Agent by Moonsoftware (http://www.moonsoftware.com/pwagent.asp.) It works great, and the free version can store up to 25 accounts that you would like to keep protected locally on your machine.

© SANS Institute 2005 Author retains full rights.

E-mail best practices

- If you don't know the sender and/or don't know what it is they are sending you, simply delete the e-mail. If it was important, they will send it again with a more descriptive 'Subject:' or 'Body.'
- Don't post your personal e-mail address on the Internet. Several web 'spiders' are used to scan the Internet looking for e-mail addresses. These e-mail addresses are then added to spam lists, and sold to spammers.
- A common e-mail attacking method is called 'phishing.' Phishing is used to bait e-mail recipients to follow certain links used by scammers to pages that mock the look of popular sites such as Paypal, Hotmail, and online back accounts. On these spoofed pages, the attacker makes you think you are logging into a legit account to receive the money guaranteed in the e-mail, or to log in and reset your password. The attacker will then steal your information and use it to his/her advantage as soon as possible. If the scammer can reach 2,000 people with this attack, and only one person falls for it, it is still very successful to that attacker.
- Keep in my that a legitimate business will NEVER ask you for your critical information such as credit card numbers, personal identification numbers, or social security numbers through e-mail

Conclusion:

All the tools and technology today and in the next decade will not keep a home user 100% secured. At the end of the day, it really depends on how much the user knows, and how hard the user is willing to try to keep their information secure. I hope this paper can be used as a helpful guide for novice to intermediate home users. If there are any questions on the topics discussed or the tools used, please refer to Google or any other search engine to extend your research and knowledge.

© SANS Institute 2005 Author retains full rights.

Cited Resources

Hu, Jim. "Comcast reports 35 percent decline in spam." June 29th, 2004
URL: http://news.zdnet.com/2100-1009_22-5251909.html (November 7th, 2004)

Author Unknown. "MyDoom DoS Attack Fizzles." February 9th, 2004)
URL: http://www.eweek.com/article2/0,1759,1526189,00.asp (November 7th, 2004)

Bono/Towns. "Safeguard Against Privacy Invasions Act." (June 25, 2003)
URL: http://thomas.loc.gov/cgi-bin/query/D?c108:6:./temp/~c10824AKWI:: (November 7th, 2004)

McCullagh, Declan. "Spyware bill moves to Senate." (September 22, 2004)
URL: http://news.zdnet.com/2110-3513_22-5377997.html (November 7th, 2004)

Lemos, Robert. "New MyDoom draws on IE flaw to spread." (November 8th, 2004)
URL: http://news.zdnet.com/2100-1009_22-5443828.html?tag=zdfd.newsfeed (November 8th, 2004)

Oates, John. "CERT recommends anything but IE." (June 28th, 2004)
URL: http://www.theregister.co.uk/2004/06/28/cert_ditch_explorer/ (November 8th, 2004)

Carroll, John. "Firefox, bah humbug." (November 4th, 2004)
URL: http://news.zdnet.com/2100-9588_22-5438955.html (November 8th, 2004)

Microsoft. "Top 10 Reasons to Install Windows XP Service Pack 2 (SP2)." (Date Unknown)
URL: http://www.microsoft.com/windowsxp/sp2/topten.mspx (November 7th, 2004)

© SANS Institute 2005, Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**