AVMUG NEWSLETTER

September Newsletter

Antelope Valley Microcomputer Users Group

Next AVMUG Meeting:

Wed.Sept. 15, 2004
7:00 P.M.
Lancaster Senior Center
777 West Jackman
Lancaster, CA
Information: 661/940-9680

Important Information
Read this Newsletter carefully your name might appear in one of the articles.

You are encouraged to bring a photograph in so we have a few to choose from for a demonstration.

September's meeting should be a lot of fun.

Special Guest

This month, AVMUG has a special techniques demonstration program. We are privileged to have a talented AV Instructor, Ms. Sandra Huszar, explain how to take your favorite photograph, and through the use of one of several various techniques, transfer the image to fabric, a shirt, or other cloth object. This opens a whole new avenue of visual statement.

We will learn a new way to use our computers and inkjet printers, when combined with special transfer paper. She also will discuss using color copier transfer paper, as well as "direct to fabric printing" through use of fabric soaking solution. Imagine the things you could personalize with your own photographs!

Ms. Sandra Huszar

Don't forget to check out JB's article on Security Issues. It starts on page 6 and has some very good must know information.

How to Disable the Local Administrator Account in XP Pro

It's a good security practice to create a new account and assign it administrative privileges, then disable the built-in local administrator account. Why? Because if you leave the account enabled, hackers have half the information they need (which consists of the account name and password) to log onto your computer and create all sorts of problems. Here's how to disable the default administrator account:

1. Log on as an administrator (remember to be sure there is another account with admin privileges before you do this).
2. Right click My Computer and select Manage.
3. In the left pane of the management console, expand Local Users and Groups.
4. Click Users.
5. In the right pane, double click Administrator.
6. Click the General tab, then check the box labeled Account is disabled.

Click OK.

Windows XP Registry Back up:

Here's how in Windows XP.

1. Click on the Start menu.
2. Click on Programs.
3. Point to Accessories, then System Tools.
4. Select Backup.
5. Click Advanced.
6. Click Backup Wizard.
7. Select "Only back up system state data."
8. Now follow the rest of the wizard.

Windows 98 SE and Windows Me Registry Back up:

The ScanReg utility runs automatically every day and backs up your registry.

To manually back it up, type scanregw at the Run command.

Locking Down Your Registry

Windows uses a service called the Remote Registry service. The service is running By default. If another user has the skills to do so, they can remotely access your registry. Since the registry is basically the core of the operating system, this may make some of you uncomfortable.

Remote Registry is easy to disable

1. Open the Control Panel.
2. Open the Administrative Tools applet.
3. Open the Service applet.
4. Scroll through the list of services. Right click the Remote Registry service and click Properties.
5. Use the drop down arrow to change the startup type for the service to disabled.
6. Click Ok.

A quick restart and users on your network will no longer have remote access to your registry.

Don't forget system restore

By Charlie Paschal, PPCC

Viruses are always a threat, but did you know that one can "return" without warning if you don't turn off one Windows XP feature when cleaning up from a virus?

One of XP's great features is System Restore that can take your system back to a time when it was running better. I've used it countless times to return an ill-acting system back to a healthy time.

What if, though, you get a virus? Because System Restore can contain system settings that will restore the virus itself, it should always be turned off before you remove a virus.
To do that:

* Right Click on My Computer and select Properties and left click. Click on the System Restore tab and check the box labeled "Turn Off System Restore on all Drives."

Then, clean up the virus and reboot. Don't forget to turn System Restore back on after cleaning up the virus.

Hex, binary, Decimal numbers

By Charlie Paschal, PPCC

Ever wonder what people are talking about when they mention binary and "hex" numbers? It's the way computers "talk" and the language they understand. Our system, of course, is the decimal number system, which is 10 base. Binary is 2-based, while hex is 16-based. The binary is where you get the "1s and 0s" from because that's the only numbers used in that system.

For example, the decimal number 11 is 1011 in binary and B in hex. Since 1s and 0s can easily show numbers from 0-9, hex is used to represent numbers from 10 through 16, meaning at A is 10, B is 11, etc. Because binary numbers can get complex, hex is used because it makes it shorter to write and it's easier for humans to remember.
If you ever want to do some conversions yourself without having to learn the mathematical way of doing it, use Windows calculator. Go to View and select scientific. Plug in a number in decimal and then click on Hex or Bin to see the number in that system. For example, 999 is 3E7 in hex. In binary it's 1111100111. See? You can remember 3E7 but it's not as easy to remember the binary version.

Some Funnies:

If it ain't broke, then maybe I just haven't fixed it yet.

"There are 10 kinds of people that understand Binary, those that do and those that don't"

Disclaimer:

<>"By following any of our tips, advice, or recommendations (for software, hardware or otherwise), you agree not to hold AVMUG or any of It's MEMBERS responsible for any problems that may arise in following said advice. All of our tips, recommendations, and information are intended for you to use at your own risk.

Although all information given is proposed to be accurate at the time of publication, we make no guarantee, either expressed or implied, that the Information in this newsletter is totally error free and 100% accurate".

September 2004
Presidents Corner:

This year represents a turning point for AVMUG. The user group environment has changed and to meet the challenges of our new environment, we have had to change also.

Meetings were different when we were a larger group of 250 members, and big companies had big budgets and were willing to travel out to see us, and provide some expensive door prizes. Now we have to be more resourceful.

Our club's primary goal is to provide a forum to share information and experiences and help other members obtain the maximum benefit and enjoyment from their PC's.

Since our membership falls into three general skill groupings, it seemed logical to form workgroups to fulfill the needs of our novice, intermediate and more advanced members. About every other month, you get a chance to meet with your peers and be Don Latimer interactive as an equal contributing member of your workgroup. In our workgroup meetings, you have ample opportunity to ask questions, choose topics, and share information. Soon, we will have three networked computers available, and we will start a gamer's group, which would meet on another night- see Ken if you are interested.

This year, AVMUG participated in the Southwest Computer User Group Conference and we learned some valuable lessons. I found that many user groups have more productive meetings by having slightly longer meetings with a refreshment break. They are able to cover an additional topic or give speakers more time for presentations/demonstrations, or have longer question and answer periods. Since our current format is cramped for time, we will be looking into ways to make the meetings more productive. If you have any ideas, we would like to hear from you.

Our club is evolving to meet your current needs. We are encouraged by all the new members who have joined us this year, and by the feedback and cooperation you have provided. This is your club and we can continue to make it into something special. As a member of AVMUG, you must choose how you will participate in events and contribute to the success of the club. There are many opportunities and ways to help. See me if you'd like to work on a committee, or handle a project for the club or be part of our Talent Pool.

Our concern for September's meeting is to permanently fill the positions of Vice President, Secretary, and Newsletter Editor. Currently we need at least one prospect for the position of Secretary. Please contact me before the meeting, for more information.

We are going to get into something practical and creative for September's meeting – Ms. Sandy Huszar will show you some creative things you can do with your photographs and fabric.

See you Wednesday night - Bob

A little wisdom

"Life is not a journey to the grave with the intention of arriving safely in a pretty and well preserved body , but rather to skid in broadside, thoroughly used up, totally worn out, and loudly proclaiming
----WOW----
WHAT A RIDE!!

"Better to remain silent and thought a fool, than to speak and remove all doubt"

The two most common elements in the universe are hydrogen and stupidity

"Ms. Johnson, would you mind ordering me another computer? And you can cancel that call to tech-support."

A Prominent Security Issue

By J.B. Brown, AVMUG
September 9, 2004

In reading three popular computer magazines, viewing computer-oriented television and last, but definitely not least, the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT), has recently made a profound statement regarding the use of Microsoft's internet browser, Internet Explorer. The statement made "recommended for security reasons using browsers other than Microsoft's Internet Explorer". Although there are others available, it appears that Mozilla's Firefox Web Browser is very popular and in many cases has become the "browser of choice".

Undertaking a project such as changing web browsers and/or email clients is a big job which could lead to disaster if your system does not respond as it should after the change; therefore, I procrastinated making the change. The above alert was first released in June and last month, August, I made the conversion. The project was made less intimidating than first believed due to the fact that, in "surfing", I found enough information that made it possible for me to establish a step-by-step procedure in switching from Microsoft's to Mozilla's alternatives. I discussed the changeover made with two other club members and sent the information to them on making the change, and since, decided that it might be a good article to present to all AVMUG (Antelope Valley Microcomputer User Group) members, giving them the option to make the change. We, as a club, could also make a presentation at one of our upcoming meetings, with detailed instructions in making the browser/email client change, if so desired by our club members.

Some of you may be hesitant in undertaking this project and if so, that's OK! In conversing with Gibson Research today, I was given a "scoop" (term used in news gathering meaning information acquired that is usually not known by others) on some very important information relating to Internet Explorer. If you'd rather not make the change to an alternate browser, continue using IE, cautiously of course, and check the Gibson Research website http://grc.com/default.htm for a soon to be released freeware utility that will allow you to change your IE options, such as cookie acceptance "on-the-fly" to access sites that may be blocked due to your cookie acceptance policy chosen, either through a permanent setting if you frequent a site or making a change effective only for that session. This utility is slated for release at the end of this month (September). This is only one facet of the utility which will allow you to "surf" with high security using Internet Explorer. The, yet nameless, utility is in use by Steve in its final testing stages.

For those of you who wish to "take the plunge" and make the web browser/email client change, read on.

Let's Get Started!!

As a preliminary, but necessary step, go to… http://www.mozilla.org/products/firefox/switch.html
This is Mozilla's page entitled, "Switching from Internet Explorer to Mozilla Firefox". From here, you will download Firefox, and any browser plug-ins, add-ons and toolbars you may want to install. In downloading Macromedia Flash Player 7 and Macromedia Shockwave Player, use the following URL and select the file listed under Mozilla or Netscape. http://www.macromedia.com/shockwave/download/alternates
Next, download the other options needed from this page. By using the links supplied on this page, you're supposedly assured of getting the proper file downloaded for your Firefox browser. Before beginning the download process, I suggest making a folder/directory on a hard drive in which to place all downloads for this project, such as, "Firefox_TB_Files". Now, we're ready to download. At this page, download the following using the links provided, Firefox, Macromedia Flash Player, Apple QuickTime and Sun Microsystems Java Plug-in. Other downloads, if desired, would be Real Networks Real Player, Windows Media Player, Acrobat

Reader and Google Toolbar. Once these are downloaded, go to http://mozilla.org/products/thunderbird/ to download the Mozilla Thunderbird email client.

As a note in downloading some of the options above, you may want to consider alternative downloads for QuickTime and RealPlayer. Instead of installing RealPlayer and QuickTIme, which are said to be like IE and OE in that they have "issues", there is a QuickTime Alternative and Real Alternative, part of the K-Lite Mega Codec Pack v1.03 at 18 Mb.

Beginning the Installation Process

Now that we have our download files, let's first install Firefox by double-clicking on the downloaded file, FirefoxSetup-0.9.3.exe. This will start the installation process. As Firefox is installing, you will be prompted by a series of installation screens….Just follow the on-screen instructions to complete the main installation of Firefox. Once the installation is completed, there's a checkbox option to launch Firefox. Insure that the box is checked to automatically start up Firefox. Once Firefox starts, the Import Wizard will appear. Selecting the option to import from "Microsoft Internet Explorer", Firefox will automatically grab most of your Internet Explorer settings and transfer them to Firefox, including your home page and bookmarks. After the wizard is finished, answer "yes" to the dialog box that asks if you want to make Firefox your default browser. This insures that any program that sends you to the web will use Firefox rather than Internet Explorer. Later, we'll talk about the removal of Internet Explorer.

Let's Add Our Options

Install Macromedia Flash Player 7 by double-clicking the installer file in your folder of files. Follow the steps presented by the installer. Once that installation is complete, install Shockwave Player 10 from your download folder, again, following the steps presented by the installer. I recommend unchecking the box that installs the Yahoo! toolbar since that is designed for Internet Explorer and the whole point of what we are doing is to quit using that browser. Install the other items such as the Java Plug-In, QuickTime or alternate, Real Player or alternate, Windows Media Player, Adobe Acrobat Reader, Google Toolbar and any others.

Some plug-ins may or may not need to be reinstalled, so we should check to see if it is necessary to install them prior to doing so. To check, open Firefox (you should have an icon on your desktop for it that has a picture of a globe with a flaming fox wrapped around it) and type "aboutplugins" as the address in the address box. This will provide a list of the plug-ins installed on your computer. If you see Java, Real Player and/or QuickTime already listed in the listing of plug-ins, you may not need to do anything. If one or more is missing, follow the appropriate steps given below to install the plug-ins you need.

- ✓ ***Java***: Java may not be used on a lot of web sites, but it is still a good idea to install it, that way you do not have to worry about installing it later on, should you need it. You can download the installer for Java at http://www.java.com/en/download/ from within Firefox, not Internet Explorer. This will start the installer for Java. When you are prompted with a "Software Installation" window, click the "Install Now" button to start downloading Java. You may also receive a security warning screen shortly thereafter; click "yes" on this screen to continue the installation. Follow all of the remaining setup prompts you are presented with to complete the installation process.

- ✓ ***Real Player***: If you need to install Real Player, go to www.real.com, click the "Download RealPlayer" link and then click the "Download Free Real Player" link on that page. As we did earlier, save this file to disk and then close Firefox after the download completes. Assuming that you did not change the location it was downloaded to, you should find a file named "RealPlayer10GOLD _bb" on your desktop or in your download folder. Click the desktop icon or the installation file and follow the installation procedure. During the installation, I recommend that you uncheck all of the optional places RealPlayer will offer to place icons as

well as all of the "Make RealPlayer the default player for" options. Once you reach the registration screen, you may choose to click cancel and skip the registration without harming your Real Player installation.

- ✓ ***QuickTime***: If you find that QuickTime was not in the list of installed applications, go to http://www.apple.com/quicktime/download/ , click "Download" on the blue bar toward the top of the page, fill out the form and select the appropriate operating system (your version of Windows) and language and click "Download QuickTime." If you are running Windows 2000 or XP you may select the option that also installs iTunes, if you desire.

The Mozilla Thunderbird Email Client

Now that you have escaped the world of the insecure and adware/spyware-prone environment of Internet Explorer, you should seriously consider moving to a more secure email client than Outlook Express as well. Thunderbird is a very well designed e-mail client that takes design cues from its predecessor Mozilla Mail, as well as Apple Mail and others. To download Thunderbird for Windows, if you haven't already, go to http://www.mozilla.org/products/thunderbird/. Download and save the file to disk as we did with the plug-ins and then close Firefox once the download has completed.

You should now have a ThunderBirdSetup-O. 7.2 file on your desktop or in your download folder. Click or double-click that file and follow the installer's instructions. Once Thunderbird launches, cancel out of the "New Account Setup," and click "exit" when prompted. You will then be prompted about whether Thunderbird should be your default e-mail client. Click "yes."

Next, go to the "Tools" menu and click "Import." Select settings and click "next." If you get a file selection window (what you see when opening or saving a file), as I did in preparing these instructions, close that window. Next, select "Outlook Express" (or "Outlook" if you are using that instead), and click next. Now repeat this step for importing e-mail by going back into "Tools," clicking on "Import," and selecting e-mail. Again select "Outlook Express" or "Outlook" and follow the process. Finally, we do this once more for the address book, going back into "Tools" and then "Import," selecting "Address Book" and again selecting "Outlook Express" or "Outlook."

Once you have completed these steps, old messages will be located inside the "Local Folders" folder, which is in the left column of the Thunderbird window, in a subfolder entitled "Outlook Express Mail". New messages, on the other hand, will be located in the folder with the name of your e-mail server (perhaps "mail.sbcglobal.yahoo.com" for example).

For Hotmail Users Only

If you are a Hotmail user, you will likely notice that all of the steps we followed did not add your Hotmail inbox to Thunderbird. If you are not a Hotmail user just skip down to the final step, but if you do have a Hotmail account, a few extra steps are necessary. The reason for this is that Microsoft does not use a standard e-mail system for downloading e-mail from Hotmail and, "officially speaking," only Outlook Express and Outlook support downloading Hotmail mail. Do not be disappointed though. A program called Hotmail Popper provides a convenient way to download your Hotmail mail into Thunderbird. While Hotmail Popper is no longer free to use (it costs $18), the last version released for free is still available to download from
http://www.secretmaker.com/downloads/hotmailpopper-211.exe

After downloading this, you should be able to close your web browser again and find a file named "hotmailpopper-211.exe" on your desktop or download folder. Next, double-click "hotmailpopper-211.exe" to install Hotmail Popper.

After completing the installation, right click the Hotmail Popper icon next to the clock on the Windows taskbar (the icon that is a picture of a candle) and click options. You will notice an option to download folders other than the inbox as well as whether to down-

load the junk mail folder. It is up to you whether you want to select these options. After you have made your decision, click "OK".

Now, go back into Thunderbird, go to the "Tools" menu and click "Account Settings." You will see an "Add Account" button on the left side of the window. Click that and then proceed through the wizard. Enter your name however you prefer and use your Hotmail address for the e-mail address. On the incoming server screen, type "127.0.0.1" and then click next. On the incoming user name screen, enter your Hotmail/Microsoft Passport ID just as you would when logging into Passport on MSN.com.

After finishing, click the "Server Settings" item in the left white column of the "Account Settings" window. If you imported one or more e-mail accounts, you will notice that there is more than one "Server Settings" item on that left column; select the one that is located under your Hotmail e-mail address heading. On the right side of the window, check "Leave messages on the server" and then check "until I delete, or move them from inbox". Finally, click "ok."

Thunderbird Can Learn!! In contrast to Outlook Express, Thunderbird has a sophisticated junk mail (spam) filter built-in. The first time you download your e-mail in Thunderbird, you may notice a lot of messages are marked as junk mail even though they aren't junk. You can tell that a message is considered junk when there is a trash can next to its subject or, after selecting that message, you see "Thunderbird thinks this message is junk mail" above the message. You may also notice that there is junk mail that is not marked as junk. Do not worry -- this is normal when you first start using Thunderbird and is nothing to worry about.

The key here is to train Thunderbird to understand what mail is junk and what mail is not. To do this, notice which messages are marked as junk incorrectly, click on them and click the "Not Junk" button right above the message. Similarly, for messages that are junk but are not marked as such, you can click on them and then click the Junk button on the toolbar.

By doing this, you are starting the learning process that will help Thunderbird eliminate spam from your mailbox. Continue training Thunderbird in this manner over the course of the next few days or weeks until it becomes highly accurate at spotting what is not junk. In other words, what we are aiming to do is make sure that absolutely no mail is being incorrectly marked as junk. In the next step, we are going to make it so that junk mail does not go into your inbox, thus the reason why we want to make sure that the mail you want to receive is not incorrectly tagged as junk mail before we do this.

Once you have achieved success in getting Thunderbird to know what mail is not junk, you can turn Thunderbird on to full junk mail control, which will move junk mail into a separate folder so that it will not bother you. To do this, go to the "Tools" menu, click "Junk Mail Controls" and then select "Move incoming messages determined to be junk mail to…". You can pick out a folder to move junk mail to or leave it set as is. After clicking "ok," you will have completed your junk mail training and Thunderbird will allow you to enjoy your e-mail free of junk mail.

We're Almost Finished!!

We now can remove Internet Explorer if you're confident that Firefox is working properly. Under SP2 for Windows XP, it's easy. Just go to Start, Control Panel, Add or Remove Programs. On the left side is an option for adding or removing Windows components; just uncheck the box preceding Internet Explorer and do the same for Outlook Express. Do this only after you know your Firefox browser and Thunderbird email client are working properly. The other option, the only one I'm aware of and I'd recommend for general use, is using a program called ***IEradicator*** in removing Internet Explorer. Other options are available, but not as easy as using the above program. Again, IEradicator is the only program I'm aware of for IE removal, but there may be others available.

Congratulate Yourself!! You now have eliminated at least most of the threat to your computer and its data, provided you're using a good firewall, anti-virus software and a spyware blocker. Namely,

you will no longer have problems with adware, malicious scripts, Spam and pop-ups. But, before you get too comfortable with what you've done, I want you to read the following regarding "ShieldsUP!!" and then I want you to go to Steve Gibson's site, http://grc.com/default.htm and check your computer vulnerability using this great service being offered totally free by Gibson Research. Anyone who surfs the internet should take advantage of this great gift and opportunity. My system passed with a perfect "TruStealth" rating.....I hope your system does also. Thanks to Steve Gibson, Gibson Research, that's "Peace of Mind".

ShieldsUP!!

An Internet security vulnerability profiling service that can prevent system intrusions

By Steve Gibson, Gibson Research Corporation

Greetings!

Please take just a moment to read and consider the following three points:

Your use of the Internet security vulnerability profiling services on this site constitutes your FORMAL PERMISSION for us to conduct these tests and requests our transmission of Internet packets to your computer. ShieldsUP!! benignly probes the target computer at your location. Since these probings must travel from our server to your computer, you should be certain to have administrative right-of-way to conduct probative protocol tests through any and all equipment located between your computer and the Internet.

NO INFORMATION gained from your use of these services will be retained, viewed or used by us or anyone else in any way for any purpose whatsoever.

If you are using a personal firewall product which LOGS contacts by other systems, you should expect to see entries from this site's probing IP addresses: 204.1.226.224 thru-204.1.226.255. Since we own this IP range, these packets will be from us and will NOT BE ANY FORM OF MALICIOUS INTRUSION ATTEMPT OR ATIACK on your computer. You can use the report of their arrival as handy confirmation that your intrusion logging systems are operating correctly, but please do not be concerned with their appearance in your firewall logs. It's expected.

The numerical and text line below might (most likely will) uniquely identify you on the Internet and your Internet connection's IP address is uniquely associated with the following "machine name":

host-66-81-195-214.rev .ol.com

The string of text above is known as your Internet connection's "reverse DNS." The end of the string is probably a domain name related to your ISP. This will be common to all customers of this ISP. But the beginning of the string uniquely identifies your Internet connection. The question is: Is the beginning of the string an "account ID" that is uniquely and permanently tied to you, or is it merely related to your current public IP address and thus subject to change?

The concern is that any Web site can easily retrieve this unique "machine name" (just as we have) whenever you visit. It may be used to uniquely identify you on the Internet. In that way it's like a "supercookie" over which you have no control. You can not disable, delete, or change it. Due to the rapid erosion of online privacy, and the diminishing respect for the sanctity of the user, we wanted to make you aware of this possibility. Note also that reverse DNS may disclose your geographic location.

If the machine name shown above is only a version of the IP address, then there is less cause for concern because the name will change as, when, and if your Internet IP changes. But if the machine name is a fixed account ID assigned by your ISP, as is often the case, then it will follow you and not change when your IP address does change. It can be used to persistently identify you as long as you use this ISP.

There is no standard governing the format of these machine names, so this is not something we can automatically deter-

mine for you. If several of the numbers from your current IP address (66.81.195.214) appear in the machine name, then it is likely that the name is only related to the IP address and not to you. But you may wish to make a note of the machine name shown above and check back from time to time to see whether the name follows any changes to your IP address, or whether it, instead, follows you. Just something to keep in mind as you wander the Internet. ***Without your knowledge or explicit permission, the Windows networking technology which connects your computer to the Internet may be offering some or all of your computer's data to the entire world at this very moment!***

- For orientation and background, please examine the page links provided below for important information about Internet vulnerabilities, precautions and solutions.
- First time users should start by checking their Windows File Sharing and Common Ports vulnerabilities with the "File Sharing" and "Common Ports" buttons below.
- For orientation and information about the Port Authority system, click the Home or Help icons in the title bar . . .

ShieldsUP!! Services

Please see **Explain this to me!** below for information about Windows File Sharing and Internet port vulnerabilities.

The following 11 headlines will provide additional background, insight, and assistance when you access them on the Internet site at **<http://grc.com/x/ne.dll?Rh1dkyd2>)**

Explain this to me.
Sharing files among locally-connected computers is incredibly convenient and makes all kinds of sense. But Local Area Networking (LAN) technology was never designed for the global Internet. It seems that it wasn't thought through very well. (Oops.)

Am I really in any danger?
You might be thinking "Hey, the Internet's a huge place, right? No one's ever going to notice me." Sure. But technically savvy intruders are using high-speed "Internet Scanners" that can probe every computer in a small country within a short time! Nothing would make them happier than lifting your personal information, credit card numbers, bank account balances, and so forth through your computer's insecure connection to the Internet.

What can I do about this?
It's possible to spend no money and disappear from their scanners, or to spend a little bit of money and gain many valuable security capabilities. I'll show you how.

Network Bondage.
Microsoft's networking technology is only required for sharing files and printer services with other Microsoft-based PC's! It is not needed for connecting to the Internet or for using any Internet services. It has no business wandering around the Internet and should be disciplined to remain within your own computer or local area network.

Evil Port Monitors.
Many companies are already exploiting the fear of Internet intrusion by selling really bad solutions in the form of "intruder detectors" and "port monitors." I call these products "evil" because they make your computer more attractive and vulnerable to intruders ... and do NOTHING to protect you!

Personal Firewalls.
If you don't need to share files across the Internet you can easily secure your computer at no cost. I showed you how on the "Network Bondage" page. But if you do need to share your files, you must consider investing $30 to $40 in a good personal firewall. I discuss that and review four commercial products.

Further reading……
A lot of material has been written about security by wily hackers who are discovering new ways of gaining control of distant computers and security consultants who work to prevent that.

Your Thoughts, Questions, and Ideas.
This site's reports, suggestions, and techniques generates many questions, comments, and ideas. So, we created a public online discussion forum to host free and unmoderated discussion where people can interact and help each other.

Be notified of significant events!
I will next be creating a freeware "hyper-speed port scanner" followed by my own super-capable firewall to address many of the security problems I've discovered (and new ones that crop up!). I'd be glad to drop you a short note as those projects are completed and ready for you, or in significantly enhance this site. Our "User-Managed eMailing System" lets you come and go as you like, and specify what sorts of mail you want to receive. (And don't worry about getting too much from me . . . I get complaints that I never send enough!).

FAQ-Frequently Asked Questions?
This FAQ page is being maintained to answer the most often asked questions arising from these pages and to minimize repetition of hose questions in the online public forum. Please check here to see whether we've already addressed and answered any questions you may have.

Site History.
The demographics of past visitors is analyzed and shown statistically here, and a chronology of changes to this site is maintained.

Shields UP! is checking YOUR computer's Internet connection security. . .
currently located at IP:
66.81.195.214

Please stand by . . .

- **Attempting connection to your computer. . .** Shields UP! is now attempting to contact the Hidden Internet Server within your PC. It is likely that no one has told you that your own personal computer may now be functioning as an Internet Server with neither your knowledge nor your permission. And that it may be serving up all or many of your personal files for reading, writing, modification and even deletion by anyone, anywhere, on the Internet!

- **Your Internet port 139 does not appear to exist!** One or more ports on this system are operating in FULL STEALTH MODE! Standard Internet behavior requires port connection attempts to be answered with a success or refusal response. Therefore, only an attempt to connect to a nonexistent computer results in no response of either kind. But YOUR computer has DELIBERATELY CHOSEN NOT TO RESPOND (that's very cool!) which represents advanced computer and port stealthing capabilities. A machine configured in this fashion is well hardened to Internet NetBIOS attack and intrusion.

- **Unable to connect with NetBIOS to your computer.** All attempts to get any information from your computer have FAILED. (This is very uncommon for a Windows networking-based PC.) Relative to vulnerabilities from Windows networking, this computer appears to be VERY SECURE since it is NOT exposing ANY of its internal NetBIOS networking protocol over the Internet.

Unfortunate as it is, the dangers presented by unprotected use of the Internet are very real, and they are growing every day.

Please help to prevent system intrusions by spreading the word and telling your Internet friends about these free services. They will always be free, and they will be enhanced from time to time as other security needs and problems arise. I'll be glad to drop you a short E-Mail note when new solutions or significant improvements are made.
Check out our "User-Managed E-Mail System" here!

The world's Internet is an incredible facility, but like any powerful tool it needs to be used with care, wisdom, and caution. Unfortunately, not everyone with access to the Internet has your best interests at heart.

Checking the Most Common and Troublesome Internet Ports

This Internet Common Ports Probe attempts to establish standard TCP Internet connections with a collection of standard, well-known, and often vulnerable or troublesome Internet ports on YOUR computer. Since this is being done from our server, successful connections demonstrate which

of your ports are "open" or visible and soliciting connections from passing Internet port scanners.

Your computer at IP:
66.81.195.214 is being profiled.

Please stand by . . .

Total elapsed testing time: 6.400 seconds

PASSED **TrueStealth Analysis** PASSED

Your system has achieved a perfect "TruStealth" rating. Not a single packet - solicited or otherwise - was received from your system as a result of our security probing tests. Your system ignored and refused to reply to repeated "Pings" (ICMP Echo Requests). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very nice.

Port	Service	Status	Security Implications
0	<nil>	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
21	FTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

(Balance of port entries is eliminated in this article since they all show the same good results)

The condensed textual report of the Common Ports Probe findings displayed above, follows:

GRC Port Authority Report created on UTC: 2003-10-07 at 04:59:32

Results from scan of ports: 0,21,23,25, 79, 80, 110, 113, 119,135,139,143,389,443,445, 1002,1024-1030,1720,5000

0 Ports Open
0 Ports Closed
25 Ports Stealth

---

25 Ports Tested

ALL PORTS tested were found to be: STEALTH.

TruStealth: PASSED
. ALL tested ports were STEALTH,
. NO unsolicited packets were received,
. NO Ping reply (ICMP Echo) was received.

For help and information about the meaning and importance of "Open", "Closed" and "Stealth" port statuses, please see the Internet Port Status Definitions page.

Firewall Leakage Tester

Just so you know, WinXP's built-in firewall does not attempt to manage or restrict outbound connections at all. It appears to be a useful firewall for hiding the machine from the Internet (it has "stealth mode" unsolicited packet handling), but you will still need to use a good third-party personal firewall if you wish to manage and control outbound connections from your system.
Crucial as it is to protect yourself from malicious hackers outside, those bad guys represent only half of the threat. The Internet has proven to be an extremely fertile transportation medium for all manner of nasty Trojan horse programs, rapidly proliferating viruses, and privacy invading commercial spyware. As a result, it is no longer true that all of the potential problems reside outside the computer.

Your Internet connection flows both ways. . - so must your security.

Not only must our Internet connections be fortified to prevent external intrusion, they also provide secure management of internal extrusion. Any comprehensive security program must safeguard its owner by preventing Trojan horses, viruses, and spyware from using the system's Internet connection without the owner's knowledge. Scanning for the presence of Trojans, viruses, and spyware is important and effective, but if a piece of malware does get into your computer you want to expose it immediately by detecting its communication attempts and cut it off from communication with its external agencies.

Most personal software firewalls provide - or attempt to provide – application based management and control of outbound Internet communications.

Marketing & Exploitation of Loyalty and Trust

Just like people, no two firewalls are identical. Some are rather spartan where others have plenty of bells and whistles. Some are easy to use and some have been made too easy to use - rendering them highly insecure. And, sadly, there are others which are pure snake oil sucker bait. This situation is further complicated by the fact that in this weird and immature market, you don't get what you pay for. One of the BEST firewalls is completely free, and one of the most WORTHLESS is the most expensive.

The LeakTest Family

To aid in the exploration of product strengths and weaknesses, and to invite an independent consensus and confirmation of my findings, I am producing a series of completely FREE "LeakTest tools". These tools may be freely used for experimenting with, and revealing, the security strengths and weaknesses of various firewalls.

The first freeware- LeakTest v1.2 - is ready for you now. You will find it on the Internet at <http://grc.com/lt/leaktest.htm>

My Goal

The biggest problem with highly technical products like software firewalls - is that they are, ummmm, highly technical. When viewed from a great distance they often seem pretty much alike. And they all claim to be the latest state-of-the-art, most secure and amazing things ever to grace your hard drive. But few actually are. Many are simply junk.

When the security of your computers is hanging in the balance, you NEED to know which is which. By openly exposing the strengths and weaknesses of these products, two significant things will happen:

. YOU will be able to make fully-informed decisions about which products best suit your needs, and,
. Unable to hide in the darkness any longer, the forces of natural selection will induce these products to either improve or die.