Volume 11, Issue 2

March 2010

The Computer Club At Willow Valley

Special points of interest:

- Infected by the *Total Security* malware? How to remove it on page 5 of the electronic version.
- Want to protect your computer? See the *Computer Security and Privacy* column for basic software and security principles that will help. Page 6 in the electronic version.
- Also available only in the electronic version is the article *What Do Those Malware Terms Mean?,* page 13.
- Want to print a web page? See page 17 In the electronic version.

Inside this issue:

Coming Programs	2
Nominating Committee Update	3
Pop-Ups	3
Need Help?	3
The Equipment Corner	4
The Mission	4
The Leadership	4
Key Willow Valley Web Sies	18

The President's Pen by Sid Paskowitz

Membership Your Computer Club has 533 members at this writing, including 94 Lifetime members.

Current E-mail Addresses Needed One of the benefits of Club membership for those members that have an email address is that we can quickly notify members of very important information about computers or the internet, when it becomes available and needs to be shared.

Expanded Newsletter This Newsletter is distributed in two forms: paper and electronic. The electronic version is distributed via email, arrives a week or so prior to the paper version, has more technical content, and contains links that can be clicked to take you directly to cited web pages or documents. If you want to receive the Newsletter in electronic form, send an email to our Club Treasurer, Dick Dressel, at dresselrj@dejazzd.com.

(Continued on page 2)

Proposed Bylaws Changes by The Executive Committee

Membership Currently, the Bylaws state: "All residents of the Willow Valley Retirement Communities may become members in the Club upon payment of the required annual dues. Dues are due on May 1st of each year at a rate to be set by the Executive Committee by April 1st of each year."

The Executive Committee proposes that this portion of the Bylaws be changed to: "All Residents of the Willow Valley Retirement Communities may become members in the Club upon payment of the required dues. Similarly, Team Members needing recycled computers or components, and prospective Residents, may also become members. Membership renewal dues are due on March 1st of the renewal year at a rate to be set by the Executive Committee by February 1st of each year."

This change moves the payment of dues closer to the beginning of the year thereby reducing the current confusion about the date when dues are to be submitted. The other membership changes allow prospective residents and Team Members to participate in the Club.

Executive Committee The Bylaws currently state: "The Executive Commit-

(Continued on page 3)

Coming Programs

March 4, 2010	April 1, 2010	May 6, 2010
Resident Larry Gallagher	Resident Ron Dillon	TBD
Turbo Tax Demonstration	*Picasa*	*TBD*

All programs are held in the Education Room at the Cultural Center

President

(Continued from page 1)

The electronic version of the current Newsletter is available online in Information Central by clicking on the Newsletter link in the left column or by accessing this web address: http://eventregistration.willowvalley.org/kiosk/cclub/p/Newsletter.pdf.

Room Monitors Needed One of the realities of living in a retirement community is that Residents who volunteer their time and energies find they are no longer able to do the things they used to do. We are realizing this reality in the staffing of the Lakes Manor and Manor North Computer Rooms. We need more volunteers as monitors in the Computer Rooms. If you can help, please contact Dick Dressel for the North Computer Room or Gene Simasek at esim_37@yahoo.com for the Lakes Computer Room to get more information.

Lakes Computers Updated The Lakes Computer Room in C-217 is outfitted with Windows 7 computers that are speech-enabled. Microsoft recently made software available that allows an individual's speech patterns to be saved to a flash drive, which makes them usable on any computer with Windows Vista or Windows 7. I recently conducted experimental training sessions for Computer Room Monitors in the Lakes Computer Room and will now be offering Speech Recognition classes in the Lakes Computer Room for all Computer Club members. The classes will each be limited to four participants, will be scheduled at a mutually convenient time, will last about two hours, will require participants to bring a flash drive with not less than 1 GB of available space and will require some homework. If you would like to get a head start on Speech Recognition and see what it's all about, send me an email at wvrccc@yahoo.com. By the way, Windows Vista and Windows 7 computers include Speech Recognition at no additional cost but few PC owners know it's there.

New Willow Valley Website Willow Valley Retirement Communities' Marketing and Sales recently updated the website that presents our home to the world. They are interested in getting our reaction to the site which can be found at www.willowvalleyretirement.com. I have volunteered to assemble feedback from Club members. Please send comments or suggestions to wvrccc@yahoo.com.

Club Officer Nominations and Elections Larry Gallagher will announce the Nominating Committee's recommendations at the March monthly meeting. Election of Club officers will be at the April monthly meeting.

Copyrighted Files Copyrighted files should not be put on Willow Valley equipment without appropriate approval. No violations have been attributed to the Computer Club. Help keep our record clean.

Thank You, Volunteers We appreciate Residents volunteering to help improve the quality of life for other Residents.

Membership

(Continued from page 1)

tee shall be the officers and committee chairmen."

The Executive Committee proposes that this portion of the Bylaws be changed to: "The Executive Committee shall be the officers, committee chairpersons and past presidents." This change recognizes the value of the wisdom of past presidents during Executive Committee deliberations and decisions.

Nominating Committee Update by Larry Gallagher

At the April Meeting, the Computer Club will elect the following officers for a two year term: President, Vice President, Secretary, and Treasurer

The Nominating Committee, Larry Gallagher, Charlie Trumbo and Peg Wert, will present their nominees at the March Meeting. Nominations may be made to the Nominating Committee or at the April Meeting prior to the election. A person nominated by someone else must agree to serve prior to being nominated.

The Computer Club By-Laws regarding the election and duties of the officers may be found under Computer Club on Information Central. If there are any questions, please call one of the Nominating Committee members.

Technical Columns and Articles are written for our readers education and are available only in the electronic version of the newsletter. If you would like that version, ask Dick Dressel at dresselrj@dejazzd.com to add you to the Club's email list. This month's issue includes the column *Computer Security and Privacy;* articles on removing the Total Security malware, the meaning of malware terms, and web printing; a notice about the continuing insecurity of doing supposedly secure financial transactions on unencrypted Wi-Fi at home and while traveling; and a list of key Willow Valley web sites.

Pop-Ups by Al Williams

To close unexpected pop-ups, use Alt+F4. Using any other technique to close a malicious pop-up will result in your computer becoming infected.

If "Total Security" appears, do not pay the subscription fee! Total Security cannot be closed by Alt+F4 or removed by restarting your computer. It will prevent almost all activity on your computer except to pay the fee. For detailed instructions on removing this malware without paying the fee, see the technical article, *Removing the Total Security Malware,* on page 5 in the electronic version.

Need Help?

The Club is pleased to provide help Monday through Friday at 1:00 pm at the Lakes Manor Computer Room, C-217, and the Manor North Computer Room, M-107. Help is not available on the first Thursday of the month because the Club meets at 2:00 pm on that day.

The Equipment Corner by Ed Dahrsnin

Refurbished Systems The following refurbished system is available:

#193: Gateway K7-600, tower, Windows 2000 SP4, 600MHz AMD Athlon, 8.91GB free space, 64MB RAM, and HP Deskjet 940C printer

Miscellaneous We have 3 volt CR2023 batteries (suitable for motherboards to keep the system clock running) and a variety of CD-ROM's, floppy disk drives, keyboards, 2 button mice, various power supplies, and assorted cables. Please contact Ed Dahrsnin at 464-6591.

Donations We are once again accepting the donation of any used, working, tower and laptop computers (with power units and batteries) along with all software CDs. You may deliver them to the North's Computer Resource room on the first floor of M building after 1 pm on Monday through Friday.

Apple/Macintosh For Apple/Macintosh parts, please contact Bob Handler or Lee Wermuth.

The Mission

The Mission of the Willow Valley Computer Club is to:

- Provide the means to educate beginners or interested non-user on how to use a computer.
- Arrange for speakers to talk to the Club about subjects that would be of interest to those with some background and experience in computer use.
- Provide a forum for interchange of computer information among members.

For more information about the Club, contact Sid Paskowitz at 464-2127 or wvrccc@Yahoo.com

The Leadership

Officers

President: Sid Paskowitz

Vice President: Robert Kemp

Secretary: Gert Skelly

Treasurer: Dick Dressel

Community Representatives

Manor: Robert Kemp

Lakes: Gene Simasek

Committee Chairpersons

Program: Robert Kemp

Training: Bob McRobbie

Equipment: Ed Dahrsnin

Technical Support: Larry Gallagher

Website: Sid Paskowitz

Publicity: Wally Gordon

Newsletter: Al Williams

Mac Interest Group: Lee Wermuth

Room Coordinator: Dick Dressel

Microsoft Liaison: Ed Dahrsnin

Speech Recognition: Sid Paskowitz

Past Presidents

Larry Gallagher

Removing the Total Security Malware by Al Williams

What is it? *Total Security* is malware that claims to provide security for your computer. Once it installs, it will insist that your computer is infected with multiple viruses and will not allow you to close it or open other applications such as *Word* or *Excel* because, it will say, your computer is infected and it is too dangerous to allow any activity. It will also say that once you pay the subscription fee, that it will disinfect your computer and you will then be able to use all applications.

What is it doing? *Total Security* keeps all applications (programs) and *Task Manager* from opening so that its process cannot be stopped. There is one exception: it will allow *Internet Explorer* to execute—so that the subscription fee may be paid.

Overview of the Removal Process Since *Total Security* does not allow *Task Manager* to execute, the first step is to download an application that can stop processes to a computer that is not infected and then copy it to the affected computer. Because *Total Security* allows only *Internet Explorer* to open, the next step is to rename the copied application's executable name to the same name as *Internet Explorer*'s executable (*iexplorer.exe*). Once it is renamed, the application that can stop processes can be opened and the *Total Security* process stopped.

The final step is to remove *Total Security*'s files and registry entries.

The Removal Process On a PC that is not infected, download *Process Explorer* from *http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx* (The - between *en* and *us* is needed.)

Copy the downloaded *procexp.exe* to the affected PC's desktop using either a CD or a USB drive. Once copied, right click on *procexp.exe* and rename it to *iexplorer.exe*. Open the new *iexplorer.exe* by double-clicking it. Click *Run*. You will now see all the processes that are executing on the infected PC.

Locate the process named *tsc.exe* and click on the red X in the bar just below the menu bar. This will kill the *Total Security* process. If you do not see a process named *tsc.exe*, look for a process name that has random numbers or characters with a shield icon or a padlock icon to the left of the name. Kill that process. *Don't kill any other processes—many are needed for the stability of your computer.*

Total Security is now no longer executing but it has not been removed from your computer. If you do not remove this malware, it will re-hijack your computer when you restart your PC.

To remove *Total Security,* use your antivirus software. Since it didn't stop *Total Security* when *Total Security* began to execute, you'll first need to update the antivirus definitions and then initiate an anti-malware (anti-virus) scan. If your antivirus software still doesn't find *Total Security*, or you don't have antivirus software installed, there is a free anti-malware package that has a good reputation and is known to remove *Total Security*.

Go to *malwarebytes.org* and download Malwarebyte's *Anti-Malware*. Double-click on *Anti-Malware* to install it. Once installed, leave *Anti-Malware Update* checked (and, optionally, *Launch Anti-Malware*) and click on Finish. Open *Anti-Malware* and perform an update. Click on the *Scanner* tab. Click on the *Perform Quick Scan* option. Click on *Scan*. Once the scan is complete, check the boxes identifying found malware and allow *Anti-Malware* to remove the malware. Restart your PC to verify complete removal.

This article is an adaptation of the instructions on bleepingcomputer.com

Computer Security And Privacy by Al Williams

The ongoing goal of this column is to give you information that will help you to secure your computer. A February 18th article in the Wall Street Journal[1] states that more than 75,000 computers in 196 countries belonging to nearly 2,500 companies and ten U.S. government agencies were made part of a botnet by collaborating Chinese and Eastern Europeans cybercriminals who had free access to those 75,000 computers. The cybercriminals stole proprietary documents, contracts, upcoming versions of software products, usernames and passwords. They achieved this by enticing people to click on links in e-mails, malicious websites, and malicious advertisements to introduce the Zeus virus into their computers.

This issue's Computer Security and Privacy column is unusually long because of the desire to: 1. convince you of the desirability of following security principles and, because of the increasing security threats, 2. present as soon as possible basic security principles and software to you.

This issue also has an article, What Do Those Malware Terms Mean? *by Domenick Buttiglieri that presents helpful malware definitions and explanations.*

Beginning and Basic Users Is it worth the time and effort to become an intermediate or advanced user?[2] It means becoming more educated, gaining experience, and taking good care of your computer. The process is like that which drivers who are 25 years and younger go through before becoming good drivers. Initially their judgment is poor. They don't realize when they're in situations that are dangerous. At times they are overwhelmed with the simultaneous demands of watching traffic, controlling the vehicle, and staying on the road. And they know very little about taking care of their vehicle.

Comparable computer users go to any web site without concern, discuss intimate family situations on Facebook, click on links in e-mails, say things in e-mails that they wouldn't want known in public, tweet information best left un-tweeted, don't worry about their personal identity, credit card, debit card or financial information on their computers, don't keep their software up to date, etc. Are there consequences? Yes.

Theft from Individuals Most articles in the newspapers, on-line blogs, and security websites focus on small business cybercrime. That's because small business checking accounts typically have more money than the checking accounts of individuals. Since it currently is just as easy to attack small businesses as individuals – because small businesses do not have the Information Technology personnel to conduct security audits and plug security holes – cybercriminals are picking the biggest low hanging fruit.

As more small businesses and banks become familiar with the methods used to conduct cybercrime and the legal issues, a trend is developing. Banks will be required to provide "commercially reasonable" safeguards including aggressive monitoring of potential fraud and providing even more secure account access methods. Small business will use those secure account access methods and monitor their account activity at the end of the day so that fraudulent transfers are identified before funds are transferred the next day to waiting money mules.[3] As this trend continues to develop , individuals will become more frequent targets.

Symantec Corp. categorizes the causes of security breaches at small and midsize companies and assigns some causes to more than one category. Five of their security breach categories are:

- Improper/out-of-date security – 32%,
- lost/stolen laptop, smartphone, or PDA – 44%,

(Continued on page 7)

Computer Security and Privacy

(Continued from page 6)

- human error – 39%,
- Improper security procedures or education – 19%, and
- loss/theft of backup tapes or devices with sensitive data – 35%.

It is easy to see that individuals could also easily have these security breaches for the same causes. (Symantec also identifies an additional four categories for businesses that have no parallel with an individual's computer usage.)[4]

There is some information concerning theft from individuals. A study conducted from March 21, 2008 to April 15, 2008 documents theft from individuals using the spam method. This study tracked 347 million spam e-mails soliciting pharmaceutical purchases. The study found that the purchase rate was 1 in 12.5 million emails with an average purchase of $100. The resulting estimated annual income is $3,500,000. For an individual spammer using readily available malware kits, this is a very high rate of return.[5]

The total estimated loss due to ID Theft loss in the US in 2005 was $56,600,000,000.[6] The average individual loss due to ID Theft in 2007 was $5,720.[7]

Note that the theft data concerning individuals was reported by professional magazines, not popular media.

Individual Risk Is there any security or privacy risk for you? Typically, risk is thought of as the likelihood of financial loss. A helpful way to consider financial risk is to express it in dollars as Risk = Impact x Probability where the impact is expressed in dollars and probability is a percentage.[8] It can also be expressed as the risk of a damaged reputation where the damage is due to actual or implied immoral or illegal activities or statements. Computer users should consider both types of risk.

Is there anything on your computer that is risky? For financial protection, you should secure:

- Personal identification information such as name, address, Social Security number and date of birth
- Useable (liquid) financial information such as information about bank and investment accounts, and credit and debit card accounts
- User names (user ID) and passwords for all financial accounts, and
- Possibly, estate information

Individual Privacy For privacy, you should protect personal information that does not identify you but which you wish to keep private. Information collected by data aggregators through a variety of sources include:

Because commercial data aggregators collect information from many sources, they know many details about most adults in the U.S.

- Political party affiliations
- Fraternal organizations
- Donations
- Web-based telephone activities
- E-mail activity
- Authored blogs
- Social web site memberships such as Facebook, mySpace, Twitter and communications on those sites
- Google searches
- Purchases in the past year
- Books/magazines purchased online

Computer Security and Privacy

(Continued from page 7)

The best way for you to protect your privacy is to give information about yourself only to those who need it and not post it on Facebook, or send it through Twitter, on write about yourself or your family on your blog, etc.

Financial Information To protect your financial information, you need to make it secure:

- On your computer
- In your communications with others – e-mail and file transfers

Making backups of your data is an important part of keeping your information secure.

Legal Implications You should also protect your computer from use by hackers to avoid legal charges and prosecution as well as a damaged reputation. Common uses of a hacked PC are:[9]

- As a web server for malicious purposes
- To conduct e-mail attacks on others
- To support botnet activities

The owners of these computers do not see the servers or the data on the servers because the hackers use a stealth technology called Rootkits.

How Can You Protect Yourself? How can you prevent theft of your personal identity or money, or misuse of your computer? There are six basic principles for the individual user which should be consistently followed.[10] They are:

- Use strong and easily remembered passwords
- Use antivirus software
- Use a firewall
- Keep your software up to date
- Remember that there is no perfect technical solution – risk management is the key
- Remember that technology will not protect you from social attacks

Use a Strong Password Once a password is known, all of the information it was protecting is available to the hacker. Some applications (programs) and web sites limit the number of characters that may be used in a password. Hackers know that and use readily available tools to determine passwords that first look for words in a dictionary and then look for all possible combinations of the characters that could be used for a password. Using as many characters as possible for a password increases the hacker's difficulty in determining the password and a well chosen password makes it impractical.

According to *Scambray and McClure*, an eight character password incorporating upper and lower case letters and numbers would require 67 years to crack when using a 1.5GHz Pentium machine.[11] That is now a fairly slow machine and less than 67 years are required using a faster machine. If you also use graphical characters, the number of characters that may be used in a password increases from the 36 characters included in A-Z and 0-9 to 69 for all printable characters thereby significantly increasing the length of time required to crack the password.

What Is a Strong Password? What makes a strong password? Using a passphrase instead of a password is the first step. Passwords that use a word from the dictionary are very easy for hackers to crack. Using two words in a password (creating a passphrase) is significantly harder. Adding numbers and graphical characters forces the attacker to work their way through all possible combinations of characters. Passphrases are usually very easy to remember and are very strong. Here are two examples of a passphrase with upper and

Computer Security and Privacy

(Continued from page 8)

lower case letters, numbers, and graphical characters:

It isn't hard to create an easily remembered and strong password.

- The2ndRose!
- (Close2theData)

Another possibility is to use the first letters of a statement, poem, or anything else that has at least eight words and which you won't forget. An example is to use a password built from this statement: *Now is the time for all good men 2 come 2 the aid of their country!* The passphrase would be: *Nittfagm2c2taotc!* This type of passphrase is harder for the user but is very effective.

Use Anti-Virus Software Anti-virus software (now more commonly called anti-malware software) helps to protect your PC. This software recognizes malware, keeps it from executing, and quarantines it. There are many reputable manufacturers of anti-malware software. If you have anti-virus software from a reputable vendor installed, use it. Unfortunately, none of the anti-virus software packages identify and stop all existing malware. Also, many of the anti-malware software packages are slow and use a lot of memory as well as being expensive.

I am sometimes asked what I use. I use Sunbelt Software's VIPRE for anti-malware. It is fast, uses little memory, and is non-intrusive—at a reasonable cost. If you have more than one computer, Sunbelt Software also offers a site license. It works with all versions of Windows from Windows 2000 forward for both 32-bit and 64-bit systems.

Because none of the anti-malware software applications catch all malware, I also use Microsoft's Security Essentials. This software is free from Microsoft. To find it, go to www.microsoft.com and enter Security Essentials in the Search box.

Security Essentials takes more time to open an application than VIPRE. When running together the time to open an application is noticeably longer but the benefit of using two anti-malware applications is that malware is more likely to be detected.

I infrequently also use Malwarebyte's Anti-Malware software as an additional detector of malware. This free and highly regarded software is available at malwarebytes.org.

Most users should use two anti-malware packages to verify that there is no malware on their computer.

Once you have anti-virus software installed, please remember that when installing other software applications in the future, that the installation might not be successful because the anti-virus software might detect something during the installation process that it did not like. It is a very good idea to temporarily disable your anti-virus software if you are installing a software package from a vendor that you trust. If you forget and the installation fails, you can use System Restore to return your computer to a known good state.

Use a Firewall Firewalls block inbound and outbound communications according to rules. This feature keeps unknown software, including malware, from communicating with machines on the Internet or any local machines thereby protecting your PC.

Starting with XP Service Pack 2, Microsoft has turned on the firewall that provided with its operating systems. Unfortunately, the outbound feature is not enabled without user intervention and when enabled, the user must manually determine the outbound rules.[12]

Again, if you have a firewall software package from

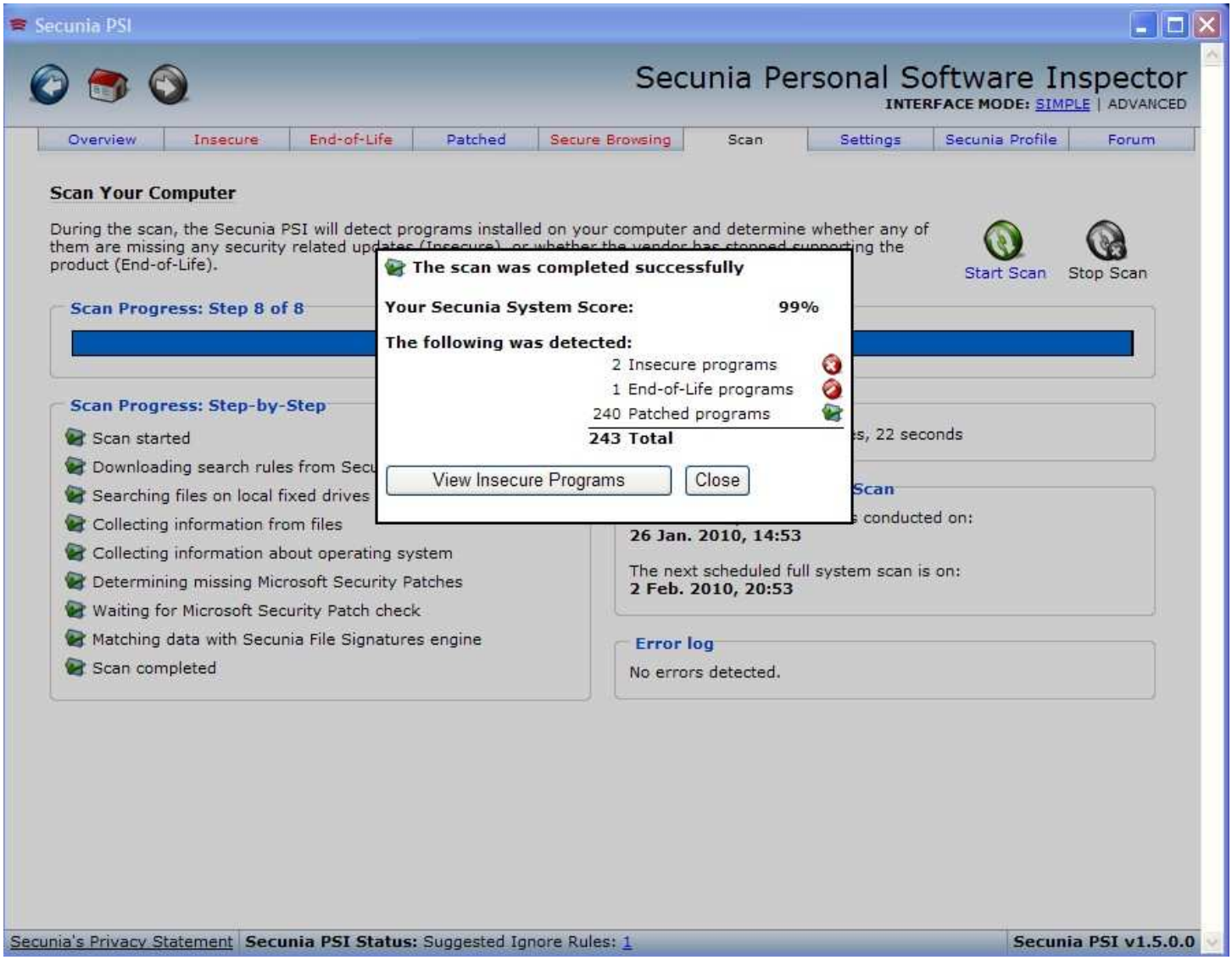
Computer Security and Privacy

(Continued from page 9)

a reputable vendor, use it. Note that some vendors combine anti-virus software and a firewall into one package and give it a name like Internet Security.

For a firewall, I use Sunbelt Software's Personal Firewall (SPF). This firewall does not require the user to create or modify any inbound or outbound rules. In addition, it is fast and has an excellent user interface with two modes: *Simple* and *Advanced*. In the *Simple* mode, SPF protects the PC without notifying the user of most of its activities. In the *Advanced* mode, SPF notifies the user of all activities. I recommend *Simple* mode for most people. It runs on Windows XP and Vista and sometime in early 2010, it will run on Windows 7. Also sometime in 2010, it will support 64-bit systems as well as 32-bit.

Keep Your Software Up To Date An important part of protecting your computer is to keep the software up to date. When a business performs a security audit, they look for out-of-date and undesirable software. One way to keep your software up to date is to re-



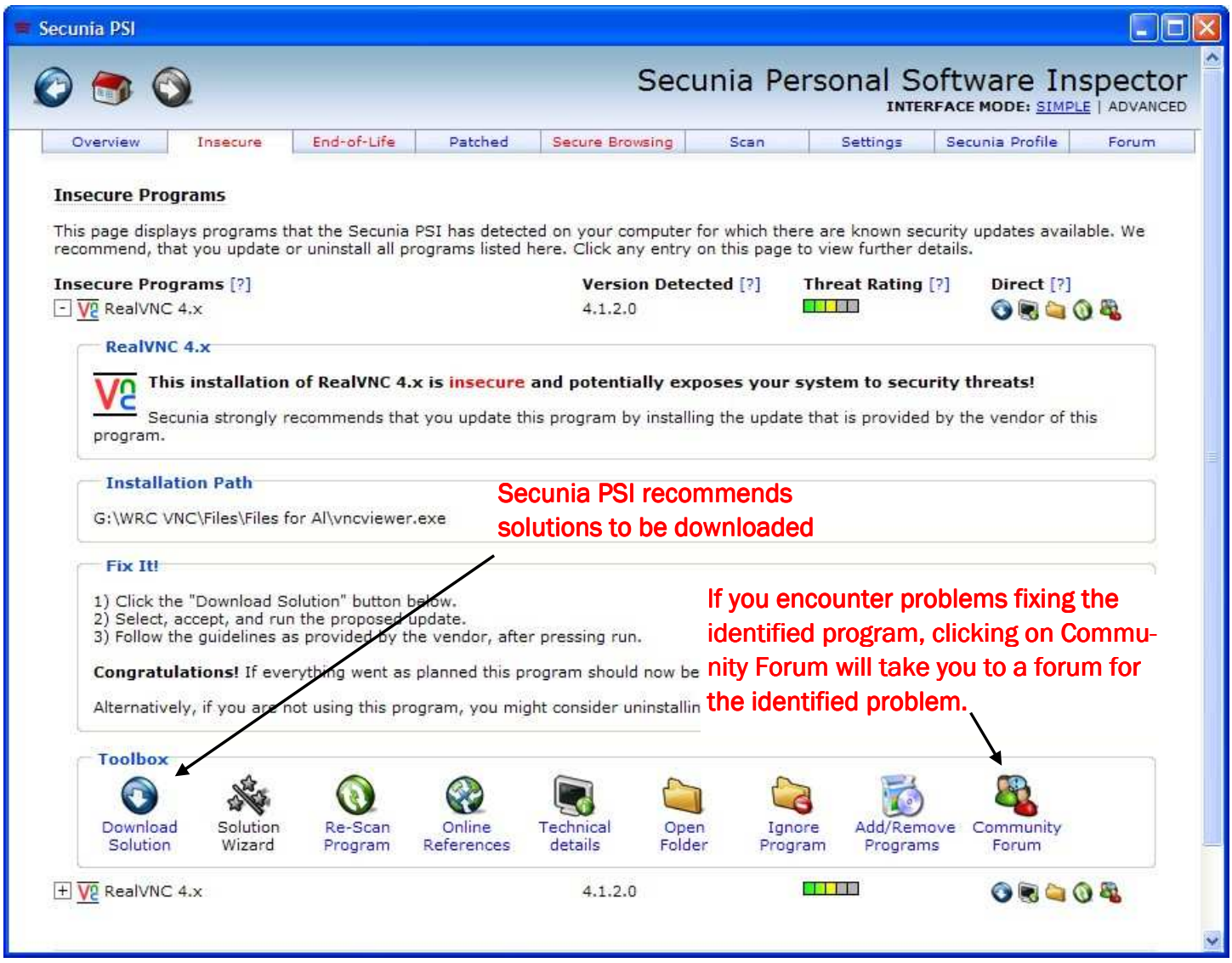
Computer Security and Privacy

(Continued from page 10)

view each application on your computer. But that is time consuming and difficult. Also, it isn't necessary because Secunia, http://secunia.com, provides a free software application that is very thorough at identifying software that needs to be patched. Secunia also provides an online software inspector but that inspector looks at only a limited set of applications and the version that installs on your computer should be used.

Download Secunia PSI from http://secunia.com. Double-click to install and allow Secunia PSI to scan. After it establishes an internet connection, it will scan your computer, looking for unpatched software. When finished, Secunia PSI presents a summary report. It also provides detailed reports about insecure programs, insecure browsers, and end-of-life programs. A screen shot of the summary report is on the previous page.

On the this page, the screen shot shows a software application that should be updated. PSI recommends a solution to be downloaded and, if the download does not fix the insecurity, identifies a



Computer Security and Privacy

(Continued from page 11)

forum that is discussing that problem.

A Tip: Adobe issues frequent updates for their Flash Player. Unfortunately, the updates install the updated player but do not remove the old player. As a result, Secunia PSI will continue to identify the old player as a security risk. Find the insecure player using the filename path displayed by Secunia PSI and rename it. For example, rename flash10d.ocx to flash10d.old.ocx.old. Otherwise, Secunia PSI will continue to find the insecure player. Renaming, instead of deleting, allows you to reinstate the old file if you should need it.

No Perfect Technical Solution It is very important to understand that the Internet and the Microsoft operating systems were designed to be open so that it would be very easy for anyone to connect computers, printers, routers, DVDs, CDs, etc. Since the advent of the first virus, Microsoft has been plugging known security holes while trying to keep the easy-to-use features that it designed into its operating systems. As time goes on, the steps described in this column will still be necessary to protect your computer, but as the hackers develop their skills, additional steps will be required.

Because the hackers will always develop hacks that need to be fixed or avoided, it is important that computer users understand that there is risk in using their computers and that they keep up to date.

Technology Will Not Protect You From Social Engineering The final basic principle is that technology will not protect your from social engineering. Malware authors understand human nature well and will continually work to craft malware that invites you to do something that will install the malware on your computer. It is up to you to be suspicious when you see something that you didn't expect and especially if it is too good to be true.

Future Columns In future columns, I'll address more advanced principles to protect your PC.

Endnotes:

1. The Wall Street Journal, February 18, 2010, page A3.
2. The comparison of users with different levels of expertise began in the January 2010 issue of this newsletter.
3. Riva Richmond, The Wall Street Journal, February 8, 2010, *Wanted: Defense Against Online Bank Fraud*, page R4
4. Ibid.
5. PC World, February 2009, pages 47-48
6. IEEE Spectrum, July 2006, pages 22-24
7. Information Week, October 22, 2007, http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=202600312
8. Scambray and McClure, *Hacking Exposed Windows: Windows Security Secrets & Solutions*, Third Edition, (McGraw-Hill: New York, 2008), page 4.
9. Washington Post, Security Fix, Brian Krebs, May 26, 2009 http://voices.washingtonpost.com/securityfix/2009/05/the_scrap_value_of_a_hacked_pc.html
10. Adapted from Scambray and McClure, pages 10-13
11. Scambray and McClure, page 139
12. PCTerritory's BestWare http://www.pcterritory.net/2009/08/enable-firewall-outbound-protection-in.html

What Do Those Malware Terms Mean? by Domenick Buttiglieri

How Does It Get Into MY Home? There are three avenues into your home. Junk snail mail enters your home every day. Answering junk mail advertisements brings a ton more junk mail. Then there is the telephone. Has anyone reading this not been contacted by a cold caller trying to sell something? Now there is the internet, the third avenue into your home. This avenue can be the most pernicious. You can personally deal with junk snail mail and telephone calls because you are very much aware of the contact. But with the internet, entry into your home can be hidden from your view and surreptitious. Your computer can be controlled without your knowledge by certain types of malware known as *Bots*, *Botnets*, and *Rootkits*. (Note: The definitions of the terms in this article were obtained from ESET, a company that develops protection against computer security threats. See www.eset.com)

What is a Bot? Short for *Robot* a *bot* is a program that is designed to automate tasks. Initially *bots* were used in the UNIX world to automate dull tasks that system administrators frequently perform. *Bots* can also be used maliciously to allow a remote attacker to control a victim's PC. The nature of many *bots* is such that it is as easy to control one PC as one hundred thousand PCs. *Bots* can be used to send spam, download and store illegal files, such as some types of porn, or to make computers participate in attacks on other computers. A *bot* can be made to search the victim's hard drive and send confidential information to a remote site on the internet in order to perform identity theft. Computers that are infected with *bots* are often called *drones* or *zombies*. Infected computers normally are part of a *botnet*.

What is a Botnet? A *botnet* is a group of *bot* infected PCs that are all controlled by the same "command and control center".

What is a Rootkit? A *rootkit* is a collection of one or more tools designed to covertly maintain control of a computer. Initially *rootkits* appeared on the UNIX operating systems (including Linux) and were a collection of one or more tools which allowed an attacker to gain and keep access to the most privileged user on the computer (on UNIX systems this user is called 'root' - hence the name) On Windows based systems, *rootkits* have more commonly been associated with tools used for hiding programs or processes from the users. When installed, a Windows *rootkit* uses functions in the operating system to hide itself, so as not to be detected, and is often used to hide other malicious programs such as *keystroke loggers*. The use of *rootkits* is not necessarily malicious, but they have come to be increasingly associated with undesirable behavior and malicious software.

What is Malware? In addition to *bots*, *botnets*, and *rootkits*, there other types of *malware*, which is short for malicious software. The term *malware* is used to generically describe any malicious software, regardless of its technical category.

The following also fall under the general term *malware*.

Virus: A *virus* is a program which replicates by copying itself, either exactly, or in a modified form, into another piece of executable code. *Viruses* can use many types of hosts, some of the most common are:

- Executable files (such as the programs on your computer)
- Boot sectors (the parts of code that tell your computer where to find the instructions it uses to 'boot' or turn on)
- Scripting files (such as Windows Scripting, or Visual Basic script)

What Do Those Malware Terms Mean?

(Continued from page 13)

- Macros within documents (this is much less common now, as macros in, for instance Microsoft Word, will not execute by default)

When a *virus* inserts itself into other executable code, this ensures it is run when that other code is run, and the *virus* spreads by searching for other 'clean' hosts every time it is run. Some *viruses* overwrite the original files, effectively destroying them, but many simply insert themselves in a way that they become part of the host program, so that both survive. Depending on the way they are coded, *viruses* can spread across many files in the system, across networks via file shares, in documents, and in the boot sectors of disks. Although some *viruses* are spread by e-mail, this does not make them *viruses*, and in-fact, most of the things that spread in e-mail are actually *worms*. To be a *virus*, the code simply has to replicate, it does not need to do a lot of damage, or even spread very widely (See *Payload*).

Worm: In computer terms, *worms* are really a subset of *viruses*, but they have the ability to replicate by themselves, they do not require a host file. Simply put, *viruses* infect hosts, and *worms* infest systems. Often *worms* exploit a vulnerability in services in network services. Such *worms* can spread very quickly across networks of vulnerable systems, as they do not require any intervention from users to run. However, the most common type of *worms* is carried in e-mails (it is important to note that it is not the e-mail which is infected, but that they carry the *worm* files). In the case of the e-mail borne *worm*, the recipient of the e-mail is the vulnerability that is exploited, usually with an enticing subject or message.

Usually *worms* are much easier to remove from a system than *viruses*, because they do not infect files. *Worms* often try to add themselves to the startup folder, or modify registry keys to ensure that they are loaded every time the system starts. Again, *worms* do not necessarily have to do any damage (See *Payload*).

Trojan Horse A *Trojan Horse*, often referred to as just a *Trojan*, is a program which purports to do one thing, but actually does another. Not always damaging or malicious, they are often associated with things like deleting files, overwriting hard-drives, or being used to provide remote access to a system for an attacker. Classical *Trojans* include *keyloggers* being delivered as game files, or *file deleters* masquerading as useful utilities. *Trojans* can be used for many purposes including

- Remote Access (sometimes called Remote Access Tools or RAT's, or Backdoors)
- Keylogging and password stealing (Most spyware falls into this category)

Spyware The term *spyware* has been used in two ways. In its narrow sense, *spyware* is a term for tracking software deployed without adequate notice to the user or consent and control by the user. Often the tracking is done by reporting information (anything from browsing history to credit-card or personal details) to a third party. Some *spyware* is delivered as part of another program (much the same way as a *Trojan Horse*), but some is delivered as a payload to a *worm*, or via websites which exploit vulnerabilities in browsers to silently install the programs in the background. There are also many programs which pretend to be *anti-spyware (AS)* programs, but are themselves *spyware*. (See www.spywarewarrior.org for a list of rogue *AS* and *anti-virus* (AV) programs). In its broader sense, *spyware* is used as a synonym for what the Anti-Spyware Coalition calls "Spyware and Other Potentially Unwanted Technologies." This can include

What Do Those Malware Terms Mean?

(Continued from page 14)

some types of *cookies*, *commercial keyloggers* and other tracking technologies.

Phishing *Phishing* (pronounced in the same way as fishing) is a social engineering attack which attempts to fraudulently acquire sensitive personal information, such as passwords and/or credit card details. Usually this is achieved by sending e-mail (or similar communication) masquerading as a trustworthy person or business with an apparently legitimate request for information. The most common *phishes* look as though they come from popular high-street banks, and usually contain some sort of threat of discontinuation of service, or other undesirable consequence if the instructions are not followed. Sometimes a mail will look very genuine, and will contain branding and content which may have originally come from the source that it is impersonating. Usually there will be a link in the e-mail that will take the recipient to a website (which also may look very much like the legitimate site), and this site will be used to capture the details being *phished*. It is important to remember that banks, and legitimate companies like Ebay or PayPal will never request usernames and passwords in unsolicited email. It is also worth bearing in mind that the links in *phishing* emails although they may look legitimate, will almost always point to a different site underneath. Always open a new browser session and type the correct address into the Address bar when you are trying to get to your internet bank or other online services.

Scam *Scams* are very similar to *phishing*, but are not usually interested in obtaining your details, they often appeal to a sense of compassion or to human greed. For instance, almost every disaster (earthquake, flood, war, famine) has generated large amounts of *scams*, usually in the form of appeals for charitable aid for a 'worthy' cause. Advanced Fee Frauds (sometimes called 419 *scams*) offer you the opportunity to get a large amount of money by supposedly helping the scammer to transfer even larger sums of money out of a country (often an African country such as Nigeria). These *scams* always result in you being asked to send the scammer some money to cover "administration" costs (often this is several thousands of dollars). Sometimes, these *scams* have resulted in the person being *scammed* disappearing, either killed or kidnapped after traveling to another country to meet their 'benefactor'. In less extreme cases, many people have lost thousands and thousands of dollars to these frauds. Some tips for avoiding such *scams*:

- Legitimate charities usually only send appeal emails to people who have explicitly chosen (opted in) to receive emails from the organization. Unsolicited, such emails are almost always fraudulent - particularly ones that appear quickly after a disastrous event.
- Don't be fooled by appearance. E-mails can appear legitimate by copying the graphics and language of a legitimate organization. Many include tragic stories of victims of the disaster. If in doubt, go directly to the organization's website, and find out ways to donate from there, and consider checking out the legitimacy of the charity on a site like www.charitynavigator.org
- Don't click through to links: links in emails can lead to "spoofed" Web sites that mirror the look and feel of a genuine organization.

There's no such thing as a free lunch - If it looks too good to be true, it almost always is.

Adware A type of *advertising display software*, *adware* are applications whose primary purpose is to deliver advertising content which may be in a man-

What Do Those Malware Terms Mean?

(Continued from page 15)

ner or context that is unexpected and unwanted by users. Many *adware* applications also perform tracking functions, and therefore may also be categorized as *tracking technologies*. Some consumers may want to remove *adware* if they object to such tracking, do not wish to see the advertising caused by the program, or are frustrated by its effects on system performance. On the other hand, some users may wish to keep particular adware programs if their presence subsidizes the cost of a desired product or service or if they provide advertising that is useful or desired, such as ads that are competitive or complementary to what the user is looking at or searching for. (Source: Anti-Spyware Coalition)

Hoaxes *Hoaxes* are usually silly pranks and are a form of chain mail. Computer virus *hoaxes* try to generate fear, uncertainty and doubt in the recipients, bringing them to believe that there is an 'undetectable virus' on their system (how can it be undetectable if you can detect it?). Some have actually been malicious in content, causing the recipient to delete files from their systems. They should simply be deleted. There is no good luck from sending them to 20 of your friends, nor are they a way in which you will learn anything about the security of your computer.

Payload The term *payload* describes the additional functionality that may be included in a *virus*, *worm* or *Trojan Horse*. For instance data stealing, file deletion, disk overwriting and/or BIOS flashing may be included. Note that the *payload* does not necessarily have to be damaging — for instance the *payload* of the *virus* known as Form A was to cause the keyboard to make clicking noises on one day a month — it did no damage other than that. In the case of a *Trojan*, it is the 'secret' function that the programmer wanted to achieve.

Do Your Part Various companies, governmental agencies, and individuals are working to alleviate the *malware* scourge. You can do your part by:

1) Installing security software on your computer, keeping it up to date and scheduling regular scanning

2) Changing your passwords frequently

3) Installing and maintaining the security features of your network including its firewall

4) Allowing Microsoft to automatically download program and security updates to your machine

5) Not clicking, under any circumstances, on advertisements

6) Not accepting or transferring chain letters under any circumstance

7) Not transmitting, under any circumstances, personal information, including Social Security numbers, via the internet or telephone—unless you know the other party and you called them.

Printing Web Pages by Larry Gallagher

Before printing a webpage you should always use *Print Preview* to insure that you are printing the entire page. Depending on the webpage layout, the text, especially the right hand side, and the graphics may be chopped off and large sections of the document may be missing.

If you find you do not have the entire page, you can change the orientation of the page from Portrait to Landscape either of two ways. If the *Print Preview* upper toolbar has *Page Setup* or *Portrait / Landscape* icons, select the Landscape setting. The screen view will change to the Landscape and the entire webpage should be available for printing. The other way is to *Close* the Print Preview page. Click *FILE* then click *Page Setup*. On the dialog box which follows, click the *Landscape* radio button under *Orientation* and select *OK*. Return to *Print Preview* and the screen should show the entire webpage. Either way the Landscape view will usually require more than one page.

If only a portion of a page is needed, that portion may be highlighted (selected), Ctrl+C pressed to copy the selected portion to the computer's electronic clipboard, and either print the selection (press Ctrl+P and click selection circle) or paste the selection into a word processor using Ctrl+V for further changes such as smaller font size

You can now click *Print* and have a hard copy of the webpage.

Serious Security Problem for Unencrypted Wi-Fi Connections by Al Williams

In mid-November of 2009, it was revealed that there is a serious problem in the Secure Socket Layer/Transport Layer Security protocol that is used to establish and ensure secure connections from your computer to on-line retailers, banks, investment firms, and any other web site where security is desired. Hackers have discovered how to conduct a man-in-the-middle attack at a hotel or motel room (using either a Wi-Fi or hardwired connection), or via an unencrypted Wi-Fi connection such as at a hotel lobby, airport, Community lobby, home, apartment, or the Cultural Center.[1]

An attack is invisible to the user. Until the flaw is fixed, users should do on-line shopping, banking, or investing using only their DSL or cable connections or an encrypted Wi-Fi network that uses WPA and AES (not WEP). When the flaw is fixed, an update stating the flaw has been fixed and describing any steps that the user must take, if any, will be in this newsletter.

Endnote:
[1]www.grc.com/securitynow, Steve Gibson, Security Now, "A Security Vulnerability in SSL", November 19, 2009

Reviewer Acknowledgment

The following individuals kindly reviewed this issue:

Domenick Buttiglieri

Jack Holden

Sid Paskowitz

Wendy Williams

Thank you to all,

Al Williams

Interested in reviewing the Computer Club newsletter before it goes to press, or providing advice about the content? Please contact:

Al Williams at atwms@comcast.net

Key Willow Valley Web Sites

These are URL links to key Willow Valley web sites. Please copy the URL to your browser's URL space, open the site, and then add them to Favorites/Bookmarks or create desktop icons.

Information Central: http://eventregistration.willowvalley.org/kiosk/cclub/index.asp

Kiosk Home Page: http://eventregistration.willowvalley.org/kiosk/default.htm

Resident Phone Directory: http://eventregistration.willowvalley.org/kiosk/cris%20files/phonesearch.aspx

Service Request: http://eventregistration.willowvalley.org/kiosk/wo.htm

Computer Club Newsletter: http://eventregistration.willowvalley.org/kiosk/cclub/p/Newsletter.pdf