Volume 12, Issue 6

November 2011

The Computer Club At Willow Valley

Inside this issue:

The President's Pen by Sid Paskowitz

Membership Your Computer Club has 506 members at this writing, including 149 lifetime members.

Senior TV Q&A For those of you who did not see Jim Cluck's Senior TV presentation at the September 1st Computer Club meeting at the Cultural Center or would like to see it again, a video of his presentation is now being shown on the in-house television channels. Jim's presentation is at 12:30 p.m. Tuesdays and Thursdays on Senior TV channel 4 and Comcast channel 822. On Mondays, Wednesdays and Fridays that time slot is used to display a video on the Electronic Registration System. In the not too distant future I hope to include a video on using a USB tuner that allows the viewing of television programs on a computer and the displaying of computer screens on television sets. The script used for the narration of that video will be available in Information Central.

(Continued on page 2)

OnStar Tracking by Al Williams

OnStar is well known as a service that enables users to request emergency services for an accident. The reason that they can provide information that is accurate for you, where you are, is because the OnStar system installed on your car transmits your GPS location to OnStar operators.

Although some users cancelled their subscriptions, OnStar continued to track their cars, recording where they drove and stopped for gas, the speed, direction, and any other information generated at the time of an accident, according to an IEEE report.[1]

On September 27, 2011, Computer World reported that OnStar has reversed their policy and will no longer track vehicles after a subscription completes.[2] Vehicle owners concerned that this is only a policy decision that could be reversed could arrange to have their OnStar equipment removed by reputable and knowledgeable organizations. •

[1] IEEE Spectrum Tech Alert, September 29, 2011

[2] http://www.computerworld.com/s/article/9220337/OnStar_reverses_course_on_controversial_GPS_tracking_plan

Coming Programs

November, 2011	December, 2011	January, 2012
Martin Klaver, Resident	Ron Dillon, Resident	Dave Marsh, Resident
Keeping Connected	*Digital Photography*	*Automated Bingo Caller Program*

All programs are held in the Education Room at the Cultural Center on the 1st Thursday of the month at 2:00 p.m. unless otherwise noted.

President

(Continued from page 1)

Senior TV Channels The right column of Information Central has a section on Senior TV and Senior TV Internet. Included are links to printable channel listings in channel number, channel name and channel category sequences. There is even a link to an on-line TV guide where you can scroll horizontally and vertically to see what is playing on each of the Senior TV channels. If anyone knows who set up that on-line TV guide, please let me know. I have some suggestions for changes.

Laptop Acting Funny? If you have a laptop computer and note from time to time that the cursor is jumping around the screen while you are typing, the problem may be that your arm or clothing is touching or is coming close to the touchpad. If you are not able to satisfactorily adjust the sensitivity of the touchpad, you may want to consider using an external keyboard and mouse. One of the benefits of Computer Club membership is that we may be able to provide you with the free mouse and/or keyboard that you need. Contact Ed Dahrsnin.

Security Essentials If you are using Microsoft Security Essentials and you get a pop-up when you first turn the computer on indicating that your computer might be at risk, what you are likely seeing is that the operating software has checked your computer before all the security software has had a chance to load. If the Microsoft Security Essentials icon in the application tray turns green, the popup indicating the computer may be at risk has been overtaken by events and may be ignored. Refreshing the desktop display or opening other programs should make the pop-up disappear. If the Microsoft Security Essentials icon in the application tray does not turn green, make sure your firewall is turned on, your security software is updated and run a full security scan on your computer.

AVG As I have stated earlier, I believe AVG is a memory hog and should be avoided, specially on older computers. My personal preference for security and utility software are Microsoft Security Essentials, Malwarebytes, CCleaner and Defraggler. (*Editor: These are very good software packages. Be certain that you select the CCleaner options that you want. Also, for a Windows 7 machine, you do not need defragmenting software because 7 automatically defragments weekly—unless you are doing something unusual*.)

Bad Guys I would like to emphasize a point we have made many times before: computer break-ins are very different from house break-ins. For someone to break into your house they physically have to be at your house and enter through a door or window. Bad guys that break into computers can be anywhere in the world where there is access to the Internet and your computer is connected to the Internet. Firewalls and security software will not protect you from the bad guys when you go to their web sites or open their email. It is like a robber at the front door of your home and you open the door to let them in. We are very fortunate at Willow Valley to have Resident Computer Kiosk units that can be used to browse the Internet or to open emails.

(Continued on page 3)

President

(Continued from page 2)

Resident Computer Kiosk units cannot be permanently infected with malicious software. Restarting a Resident Computer Kiosk unit when you start your session will remove any malicious software and correct any problems introduced by an earlier user. Restarting a Resident Computer Kiosk unit when you end your session will assure no later user can introduce malicious software that can report what you did during your session. (*Editor: Resident Kiosks are a very good idea for the general computer user. You can go to bad web sites or open a bad guy's email, if you are using software such as Sandboxie, Ubuntu as a live CD, or a Virtual Machine. Those software packages and others are readily available but most users do not want to bother to learn how to use such software. Hence, Sid's advice is sound*.)

Monitors, please! Monitors, we need monitors -- both kinds! We have computer towers that Ed Dahrsnin and his recycling team cannot use in assembling computer systems for Club members or for donation to Lampeter-Strasburg School District because we don't have computer monitors to go with them. If you have a working monitor that is sitting in a closet or cage, please drop it off in the Manor North Computer Room (M-107) Monday-Friday at 1:00 p.m. so Ed and his team can put it to good use.

We are experiencing too many days when the Computer Rooms are not open because no monitor signed up for those days. As our neighbors change their email accounts because of the new Senior TV service, more help will be needed in the Computer Rooms. Any Computer Club member with basic computer skills who is willing to spend a couple of hours each month as a Computer Room Monitor is requested to contact JoAnne Phillips at 464-6502 for the North Computer Room or Gene Simasek at 464-4605 for the new Lakes Computer Room (E-108). Let JoAnne or Gene know if you would like training to help you feel more comfortable as a Computer Room Monitor.

We are offering a special incentive for Computer Room monitors. We are placing books in the Computer Rooms for monitors' use only. David Pogue's book on Windows 7 and Russ Walter's book on the Secret Guide to Computers are for monitors' use and are not to be removed from the Computer Rooms. Sign up as a monitor now!

Secret Guide Russ Walter's new 703 page book Secret Guide to Computers & Tricky Living has been published. The book is listed at $25.00 each, but the Computer Club is getting special pricing of $10 each if you order through the Computer Club. Dick Dressel, Computer Club Treasurer, is taking orders for the book. Contact Dick via email at dresselrj@dejazzd.com or 464-6508 to place your order.

Resident Kiosk Changes The desktop display on Kiosk units have been modified to include four icons: Internet Explorer, Yahoo Email using Mozilla Firefox, Notepad and Restart Computer. The reason for the change is the new Yahoo! email program will not work with older versions of Internet Explorer; however, Firefox on the Kiosks will work with the new Yahoo! email program. If you want to use the new Yahoo! email program on a Kiosk, close all the screens until you get back to the desktop display that has the four vertical icons in the upper-left corner of the screen, then double-left-click on the Yahoo Email icon. •

In The News

A new owner of an iPhone4S said to Siri, the new voice recognition software that Apple put on the 4s:

"Who's your Daddy?"

"You are!", Siri replied in a man's voice. •

Word Tips From Bob by Bob Wilcox

These "Tips" will be helpful to people who use Word 2000 and some other versions of Word.

Problem #1 You have text that you want to highlight.

Solutions:

- If the text is a single word, simply double click before the word.
- If the text is a single line, place your curser to the left of the line to be highlighted, and, when the arrow appears, click on the arrow.
- If the text is several lines, click before the first letter of the text, then holding down the Shift key, click after the last letter of the text. Everything between the two places clicked will be highlighted.
- TIP: You could get the same result by placing the curser to the left of the first line, then, when the arrow appears, move the curser down to the last line of the text. However, if you inadvertently move the curser below the bottom of the page, you will accidentally highlight a lot more than simply the text you want to highlight. Clicking before and after the desired text prevents that from happening.

Problem #2 You type words without looking at the screen. When you do look, you find that your finger has accidentally hit the Caps Lock key, and all the words are in upper case. Naturally, you want them in lower case.

Solution: Highlight the words you want to change to lower case. Press shift and hold as you press the F3 key. All the highlighted words change to lower case. Change lower case to upper case the same way.

Problem #3 You keep a collection of jokes. Someone e-mails you a joke you'd like to add to your collection. But first you need to make sure that it doesn't duplicate the many you already have in your collection.

Solution:

- Pick out some unusual words in the new joke. If the joke, for example, has a sentence saying, "The terribly shy man blushed," you might pick the words, "terribly shy."
- Open your collection of jokes.
- Click on Edit, then click on Find.
- In the window, type in "terribly shy."
- Click on Find Next. The first place those words are found in your collection will be shown. Each time you click on Find Next, the next place those words are found will be shown. If there are no such places, you will be told so. And, when the search is completed, you will be told so. If the words have not been found as part of the joke in your collection, you'll know that the new joke will not be a duplicate of one you already have in your collection.
- TIP: If, when you first click on Find Next, you are told that the words were not found, check your spelling in the window to make sure you have typed the words with the correct spelling. The computer will look for exactly what you have typed in the window.

Problem #4 You have a list of items that you want to number.

Solution:

- Click on the paragraph symbol on the toolbar to make sure each item to be numbered is followed by a paragraph symbol. If not, hit the Enter key wherever you want a paragraph symbol to appear.
- Highlight the list.
- Click on Format.
- Click on Bullets and Numbering.
- Click on the numbering format you desire.

(Continued on page 5)

Word Tips From Bob

(Continued from page 4)

- Click on OK.

Problem #5 You are writing a letter. You realize that one of the paragraphs would read better if it moved up to appear earlier in the letter.

Solution:

- Highlight the paragraph you want to move.
- Click on the Cut icon on the toolbar (the one showing a pair of scissors).
- Move your cursor to where you want the paragraph to appear, and click.
- Click on the Paste icon on the toolbar (the one showing a clipboard). If that icon does not appear, an alternate method is to hold down the Control key, while pressing v.
- The paragraph will move up to where you want it to appear.

Problem #6 There is a paragraph that you don't want to delete but do want to insert in another document.

Solution:

- Highlight the paragraph you want to insert in another document.
- Right click anywhere in the highlighted copy.
- Click on Copy.
- X out of the document.
- Open the document into which you want to insert the copied text.
- Move your cursor to where you want the copied text to appear, and click.
- Click on the Paste icon on the toolbar (the one showing a clipboard). If that icon does not appear, an alternate method is to hold down the Control key, while pressing v

The copied text will remain in the original document, but will also appear in the document to which it was moved.

Problem #7 You have a document where all paragraphs are flush left. You decide that the first line of each paragraph should be indented. You indent several paragraphs with no problem. Then when you try to indent the first line of a paragraph, the whole paragraph indents.

Solution: Before doing anything else, click on the Undo Typing icon on the toolbar (the one with the curved arrow that goes up, then left). The paragraph will return to flush left. TIP: That method works for any unexpected change in formatting. If you click on the Undo Typing icon before doing anything else, the text will return to the format it had before the unwanted change occurred.

Problem #8 You are modifying a document so that the first line of each paragraph is indented. But when you try to indent the first line of a given paragraph, the whole paragraph indents.

Solution:

- Click on the Undo Typing icon on the toolbar (the one with the curved arrow that goes up, then left).
- Find a paragraph in the document where the first line is indented as you want it to be.
- Highlight that paragraph.
- Click on the Format Painter icon (the one with the picture of a paint brush).
- Place your cursor to the left of the first line of the paragraph whose first line you had tried to indent.
- Hold the left click on the mouse down, and move down until the whole paragraph is highlighted.
- Release the left click, and the paragraph will

(Continued on page 6)

Word Tips From Bob

(Continued from page 5)

adopt the format of the paragraph you "painted," with the first line indented.

Problem #9 You have a document with lines that are single spaced (let's say a Joke Book with a large number of one-liners), and you want the lines to be double spaced.

Solution:

- Click on the paragraph symbol on the toolbar to make sure that each item you want to be double-spaced is followed by a paragraph symbol.
- Highlight the entire text that is to be double-spaced.
- Click on Format.
- Click on Paragraph.
- In Line spacing, click on the down arrow.
- Click on Double.
- Click on OK
- The lines will be double spaced.

TIP: Use the same method, clicking on Single if you want to single space lines that are double spaced.

Problem #10 You have a document with a number of lines that should be alphabetized (Let's say it's a joke that consists of a large number of one-liners and you want them alphabetized so that, when you learn of a likely candidate to add to the list, you can more easily check to see if it's already among those listed).

Solution:

- Click on the paragraph symbol on the toolbar to make sure that each one-liner is followed by a paragraph symbol.
- Highlight the entire text that is to be alphabetized.
- Click on Table.
- Click on Sort.
- Click on the down arrow beside the Sort By window
- Click on Field 1.
- Click on OK.

Each one-liner will now appear in alphabetical order.

Problem #11 You would like to make sure that all words in your document are spelled correctly. The computer automatically places a red squiggle under misspelled---or repeated---words. If you like, it will also suggest spelling you might have intended. TIP: This is only an aid. For if the word you've misspelled is also a good word, the computer will not pick it up. For example, if you mean to type "branch," and you accidentally type "brunch," the computer will not find the error, because "brunch" is also a correctly spelled word, and the computer assumes that "brunch" is the word you intended to type. But, if you accidentally typed "brench," the computer will you tell you the word is misspelled, because "brench" is not a correctly spelled word. The feature is exceptionally helpful when you type a word that you think is spelled correctly, but isn't. For example, if you type "seperate," the computer will place a red squiggle below it to say it is a misspelled word. And, if you ask it to suggest the correct spelling, it will suggest "separate."

Solution:

As you type your document, right click on the first word that has a red squiggle under it. The computer will then suggest the correct spelling of the word you may have intended. You can click on the correctly spelled word, and it will replace the incorrectly spelled word in your document. You may also opt to click on "Ignore all," so it will remove the red squiggle from the word wherever it appears in your

(Continued on page 7)

Word Tips From Bob

(Continued from page 6)

document. If the word with the red squiggle is known to you to be a correct spelling, you can add it to the computer's dictionary by clicking on "Add."

You may want to type your entire document before checking for misspelled words. In that case, when you have finished typing your document, click on the Spelling and Grammar icon on the toolbar (the one with the check mark and ABC above it). It will then highlight the first misspelled word and suggest the correct spelling you might have meant. Click on the correctly spelled word. That will highlight it. Then click on Change. It will automatically replace the misspelled word, and the next misspelled word in your text will be highlighted.

Problem #12 You want the computer to alert you to any grammar errors you make.

Solution:

For example, if you type "a well deserved vacation," the computer will underline the words "well deserved" with a green squiggle. If you right click on the underlined words, the computer will tell you where the error in grammar is made and will suggest the correct grammar. In our example, it will suggest "well-deserved." When you highlight it and click on Change, it will replace the incorrect grammar. You may also opt to click on "Ignore" to tell the computer to make no change.

Problem #13 You have a Joke Book, and a friend e-mails you jokes that you would like to add to your collection. You copy the e-mailed joke, then paste it into your Joke Book. If the formatting of the pasted joke is different than that of the Joke Book, it may do some very strange things to your book.

Solution:

- Make sure that all formatting is removed from the joke before you paste it into your Joke Book. The joke will then adopt the formatting of your joke Book and will appear just as if you had typed it in yourself.
- Open the joke in your e-mail.
- Highlight the joke by clicking to the left of the first line of the joke and then, holding down the left click on the mouse, move down through the last line of the joke.
- Right click on the highlighted joke.
- Click on Copy.
- Click on File---Close.
- Open e-mail, and click on New.
- Place cursor in message area.
- Click on Paste
- Click on Format
- Click on Plain text
- Highlight joke
- Right click on the joke and click on Copy.
- Close out of e-mail.
- Open Joke Book.
- Click where you want joke to appear.
- Click on Paste icon.
- Edit joke to match the style of other jokes in the Joke Book.
- Save

Problem #14 The toolbar(s) at the top of the screen has disappeared.

Solution:

- Click on View.
- Click on Toolbars
- Click on Standard.
- Click on Formatting. The Standard and View toolbars appear at the top of your screen. •

Skype Tips by Al Williams

Use Skype? Have Skype problems? Here are some tips that help.

Tip 1 (For Intermediate Users) Skype does not use servers that it owns. Instead, it uses your computer as a server not only for the conversation you are having with someone else but also for conversations others are having. To keep your computer from being a Skype server for your conversation and others, use a router. Routers inherently do not allow computers on the Internet to access your computer because they use a technology called Natural Address Translation.

But, a router may not completely fix the problem. Many router manufacturers enable by default a feature called Universal Plug and Play (UPnP) because they do not want lots of phone calls from customers claiming that the router does not work. When enabled, UPnP makes it possible for the software on your computer to create port holes allowing software on the Internet to initiate communication with software on your computer. This is a very serious security problem. If your router has UPnP enabled, Skype will, by default, turn on UPnP on our router so that your computer will be a Skype server even though you are using a router.

To prevent this, log into your router and find the setting for UPnP. Make certain that UPnP is disabled and then save the change to the router. Also, open Skype, select Tools from the menu along the top of the Skype window, select Options from the drop-down menu, select Advanced in the left hand menu in the new window, and select Connection in the left hand menu. Then, uncheck the Enable uPnP check box. Click Save.

Tip 2 (For Advanced Users) Skype performance can be improved by creating a point-to-point connection instead of going through multiple Skype user computers. To do this, follow the instructions in the previous paragraph to get to the window that displays the uPnP check box. Change the Use Port 7591 for incoming connections to a different port number that is between 46000 and 65535 which is the range that users may use. Using lower numbered ports may lead to conflicts with other software running on your computer. Click Save.

Change your firewall such that it allows incoming Skype communications on the port that you selected in the previous paragraph.

The person with whom you will be communicating should also change the default port 7591 to another number in the allowed range for best performance. It does not have to be the same number as the one you chose.

When you use Skype to talk a person who has successfully changed the port number, Skype will recognize the fact that port numbers are different and will set up a point-to-point connection that does not go through intermediate computers belonging to Skype users. This provides the best possible Skype communications.

Tip 3 (For All Users) Skype encrypts all conversations so that no one else can overhear those conversations. It also records those conversations. Skype will provide transcripts of a conversation to anyone who Skype believes has the legal right to access the conversation. Therefore, beware! If you are using Skype in a country that provides minimal personal rights, certain types of comments could be disastrous. •

In The News

A new owner of an iPhone4s said to Siri:

“Tell me a joke.”

“Two iPhones walk into a bar. … I don’t remember the rest.” •

Is That Recommended Update Safe? by Al Williams

A window just showed up on your computer stating that Java needed to be updated. Clicking OK would cause the update to be downloaded and installed. Is it safe to click OK? Or, could that window have been displayed by malware wanting to download even more malware?

If you use Java and are aware of its update settings, then you know that it does periodic checks for updates and will notify you when an update needs to be downloaded and installed. In that case, the suddenly displayed window was very likely issued by Java.

But, how can you be sure that it is a valid Java update? How can you be sure about any update? There are two ways that I know of. The first way is to go to the web site for the software that says it wants to download an update. Some sites will automatically check the version of the software that you have on your computer against the latest version and display a Download button only if you need to update your software.

The second way is to use trusted third party software to tell you whether or not you do need an update. Microsoft displays installed software under the Add/Remove Programs under Control Panel (Windows XP), or under Programs under Control Panel (Windows Vista or Windows 7). If the software provider included the current version number in the name of the software, you can compare that number against the current version number of the software that is displayed on the software vendor's web site. Unfortunately, many software vendors do not include the version number in the software name.

Another trusted third party software package that will tell you whether or not an update is needed is Secunia. After installing and running Secunia PSI, it will display a list of any software that needs updating. If you ask it to do so, it will connect you to the provider's web site for downloading an update. This ensures that the web site with the update is valid and not a counterfeit hosting malware.

After downloading and installing the update, it is a very good idea to run Secunia again. On occasion, a series of updates must be installed but each is dependent upon the installation of another first. •

The ECPA Controversy by Al Williams

A recent article in the Wall Street Journal provides insight into the controversial usage of the Electronic Communications Privacy Act by the Federal government. The ECPA allows the government to obtain secret court orders to force companies in possession of certain information to turn it over.

The law was enacted in 1986, before the World Wide Web came into existence, and is being used to obtain information about email or cell phones without a search warrant or showing probable cause. The person being investigated is not notified.

In the case detailed by the Wall Street Journal, the Federal government obtained a secret court order to force Google and Sonic to provide email information generated by a contributor to WikiLeaks. The order sought the email names of the persons with whom the contributor was communicating.

The EPCA's author, U.S. Senator Patrick Leahy, has introduced a bill adopting many of the privacy concerns raised by technology aware companies including AT&T, Google, and Microsoft.

The U.S. Sixth Circuit Court of Appeals ruled in December 2010 that the government violated the Fourth Amendment when it obtained emails with-

(Continued on page 10)

A Hard Drive Tip by Al Williams

"Dad, my computer is frozen. I need help. I can't complete my work."

"What have you done so far, Amy?"

"I've been able to close all the programs. It took quite awhile because the computer is so sluggish. Then, I was able to restart the computer but it isn't finished restarting and is taking so long. Wait a second, Herb just told me that his computer is frozen. And, Crystal just said that hers is also. Herb will see if the other computers are frozen. Yes, they are! Is it a virus?'

"I doubt it. You all do have one piece of computer equipment in common: the server. Try restarting the server. It might say that it is running, but restart it anyway."

Minutes later.

"We restarted it. It displayed a message that the hard drive failed. Herb says that it has displayed that message before and that Scott knows about it."

What should I tell her to do next? I'm two hours away. I've tried to log into her network to help determine what is happening, but I can't log in because the computers are frozen.

"Mary just said that she copied all the files on her hard drive to the server a few minutes ago. Could that be the cause?"

"It could be. Ask Mary to delete all the files she put on the server."

"That did it! We can use our computers! Thanks!"

What happened? When Mary put all her files on the server, she almost completely filled the hard drive set aside for users on the server. A hard drive must have at least 10% of its capacity free (unused) so that the operating system can add and delete files. When Mary filled the server's hard drive, the operating system had no place to add files and the computers ground to a halt. When she deleted the files, the space that the operating system needed was now available.

What should you do? Make certain that at least 10% of your hard drive's capacity is unused. I frequently work with applications that move a lot of information to and from memory and the hard drive. For me, my experience is that I must have at least 15% of my hard drive unused. But, for people doing only email and surfing the web, 10% should be sufficient." •

The ECPA Controversy

(Continued from page 9)

out a search warrant noting that U.S. Post Office mail may not be intercepted and read nor may phone calls be intercepted – without a search warrant.

For more information, see the Wall Street Journal article.[1] If you are interested in digital privacy, you may wish to view the web sites of the Electronic Frontier Foundation, the Electronic Privacy Information Center, and others. A suggested search phrase for Google is "digital privacy". •

[1] *Secret Orders Target Email*, Julia Angwin, *The Wall Street Journal*, Monday, October 10, 2011, page A1

If You Don't Have A Computer by Sid Paskowitz

How can you write a letter or save your correspondence if you don't have a computer? One solution is use of a Resident Computer Kiosk unit. Although those units do not allow you to store your files on them, they do offer two facilities that enable you to create and store your correspondence.

The first facility is the Notepad software that can be accessed by double-left-clicking on the Notepad icon in the upper left corner of the desktop display. The desktop display results from closing or minimizing all open programs on the unit. Close windows by left-clicking on the X in the upper-right corner of the window. Minimize windows by left-clicking on the - (minus) in the upper-right corner of the window.

Notepad is a text editor that can also be used as a limited word processor. Font type and size can be selected. Margins can be set. Some page print formatting can be set.

Notepad by itself can allow you to write a letter, but it cannot keep it saved on a Kiosk computer. The key to saving your letters is your email account such as Yahoo or Gmail. There are some shortcuts you can use to facilitate that process. Those shortcuts are called keyboard shortcuts. There are numerous keyboard shortcuts; however, learning just a few of them can save you a lot of time searching your computer screen for the links to those functions.

The first keyboard shortcut is Control+A and is performed by holding down the Control key at the bottom left corner of the keyboard and pressing the A key. This keyboard shortcut highlights all the information in the area where the cursor is positioned. For example, if you are using Notepad to write a letter, you can highlight or select that entire letter by pressing Control+A. Note that you can get the same result by holding down the left mouse button and dragging the cursor from the top of the document to the bottom, or bottom to top, but that can be problematic when the document covers multiple screens. Control+A eliminates that problem.

The second keyboard shortcut is Control+C and is performed by holding down the Control key at the bottom left corner of the keyboard and pressing the C key. This copies the highlighted or selected information and places it on the computer's invisible electronic clipboard.

The third keyboard shortcut is Control+V and is performed by holding down the Control key at the bottom left corner of the keyboard and pressing the V key. This pastes the information from the computer's electronic clipboard into the location of the cursor on the screen display.

Putting those features together, you can prepare a letter, copy it to the electronic clipboard, open your email account, prepare an email to yourself with a subject being the name you are giving to describe your letter, and in the text box of your email, paste the letter you put on the electronic clipboard. When you send yourself that email, you have backed up and filed your letter.

What if you want to modify or send that letter to someone else at a later date? Use the reverse of that process by opening that email, copying the email text to the electronic clipboard, opening Notepad and pasting the information back into Notepad.

One more keyboard shortcut worth remembering. That keyboard shortcut is Control+Z and is performed by holding down the Control key at the bottom left corner of the keyboard and pressing the Z key. That shortcut undoes the last function you did on the computer. For example, if you deleted something by mistake, Control+Z can sometimes help you correct that mistake.

Finally, a reminder when using a Resident Computer Kiosk. Use the Restart Computer icon at the beginning and the end of each Kiosk session. Re-

(Continued on page 12)

Senior TV Feedback by JoAnne Phillips

Hip, hip, hooray!! We got connected yesterday afternoon while I was not home. The installation took less than 5 minutes and they took the little Comcast box. We are very pleased with the picture -- much better than Comcast with lots of honest to goodness HD 1080p channels. I refused to pay extra for HD from Comcast. The internet connection so far has been just fine. We streamed a movie from Netflix last night and never had to wait for buffering once.

Speedtest.net gave me the following readings at 11:26 this morning. This should have been about the best you can get as many are at church. I managed to test two ISP sites. The first was Fort Hays U at Hays, KS and the second was Overland Park, KS. Both use Comcast!!! Ft Hays was by far superior. Using open DNS I got 19.46 Mbps down and 2.55 up on one try and 16.3 down with 2.57 up on the second try. A try with Overland Park got me 6.25 down (marginal for our use) with 2.65 up. Pings were around 68 Mbps. Apparently Hays is dominant as I wasn't able to pick up Overland Park a second time.

We are happy campers. •

Editor: Testing your upload and download speeds is important to ensure that your connection to your ISP is performing as advertised. You should get similar results if you use different web sites to do the test. Sometimes the web sites do not allow you to connect to the same cities which makes comparing results difficult. However, you would expect the results to make sense.

I used my favorite speed tester, speakeasy.net on a Thursday night around 8:30pm. I got results that I have consistently seen over at least the last 6 years both here in Lancaster and in the Princeton NJ area. As always, Seattle is the slowest, this time with 4 Mbps up and 4 Mbps down. Going down the West Coast to San Francisco and Los Angeles, the download results were only slightly better while for all cities the upload remained right at 4 Mbps. The next city was Dallas, TX. From that city, on, the download speeds increased. There is something about going over the Rocky Mountains. Dallas was 9.44 Mbps down; Chicago, 11.63 Mbps; Atlanta, 10.28 Mbps down; New York, 24.55 Mbps down; and Washington DC, 14.27 Mbps.

I then tried speedtest.net, which was used by JoAnne. I consistently saw 4 Mbps up with slight variations. Seattle down was 4.4, Dallas was 9, Chicago 24.7, Atlanta 20.7, New York 24.9 and Washington DC 25.

The difference in download speeds between speakeasy and speedtest is due to two factors: the two sites are using different servers in each city and are also using slightly different networks.

Comcast's web site says that download speeds are up to 15 Mbps for their basic level service; I saw much better east of the Mississippi. The 4 Mbps down matches what I was told at the time I signed up. I have seen higher at times.

The point of my editor's note? Compare download and upload speeds between ISP competitors, compare the prices, try to determine the reliability of the ISP, and try to estimate the ability of the ISP to handle growth. Then, pick the competitor which best satisfies your needs. •

If You Don't Have A Computer

(Continued from page 11)

starting before you use the unit will clear any problems, including malicious software, caused by a prior user. Restarting after you use the unit will clear your work so no later user, or malicious software, can access what you have done. •

NSA Issues Recommendations by Al Williams

In response to the ongoing epidemic of computer break-ins by hackers, the National Security Agency (NSA) has issued *Best Practices for Keeping Your Home Network Secure*, which is a set of computer security recommendations for computer users at home. These recommendations cover

- Windows machines,
- Apple machines,
- home networks, and
- best practices for users.

The recommendations are attached to this issue of the newsletter as an appendix, which begins on page 16. They may also be found at http://www.nsa.gov/ia/_files/factsheets/Best_

Practices_Datasheets.pdf

and in Information Central.

Every computer user should read and implement the recommendations. •

Like to write an article for the club's newsletter? Articles are welcomed.

Please contact:

Al Williams at atwms@comcast.net

The Equipment Corner by Ed Dahrsnin

Refurbished Systems The following refurbished systems are available:

#231: Compaq PD1010, desktop, Windows 98SE, 350 MHz Intel Pentium II, 6.09 GB Free Space, 64 MB RAM, No printer

#240: Dell GX200, tower, Windows XP Home SP3, 733 MHz Intel Pentium III, 6.89 GB Free Space, 256 MB RAM, Epson Stylus 740 printer

#248: Dell Inspiron 8100, laptop, Windows XP Home SP3, 1000 MHz Intel Pentium III Mobile, 25.00 GB Free Space, 256 MB RAM, AOL 917W Monitor (Integrated monitor is not working), Dell Photo Printer 720

WEB TV System, with two keyboards and remote control. Use your TV set as a monitor.

The systems are free to any club member. You must pick them up. Contact Ed at 464-6591.

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 accept used, *working*, tower and laptop computers (with power units and batteries) from club members along with all software CDs. Used printer cartridges also accepted. 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. No Macs or Mac parts, see Lee Wermuth

The Mission

The Mission of the Willow Valley Computer Club is to:

- Provide the means to educate beginners or interested non-users 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: Dick Klahn

Secretary: Joan Burks

Treasurer: Dick Dressel

Community Representatives

Manor: Larry Gallagher

Lakes: Gene Simasek

Committee Chairpersons

Program: Dick Klahn

Training: Bob McRobbie

Equipment: Ed Dahrsnin

Technical Support: Tony Poulos

Website: Sid Paskowitz

Publicity: Wally Gordon

Newsletter: Al Williams

Mac Interest Group: Lee Wermuth

Computer Room Coordinators: JoAnne Phillips, Gene Simasek

Microsoft Liaison: Ed Dahrsnin

Past Presidents

Larry Gallagher

Reviewer Acknowledgment

The following individual kindly reviewed this issue:

Sid Paskowitz

Thank you,

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.aspx

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

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

Service Request: http://eventregistration.willowvalley.org/kiosk/ServiceRequest.aspx

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

Best Practices for Keeping Your Home Network Secure

The cyber threat is no longer limited to your office network and work persona. Adversaries realize that targets are typically more vulnerable when operating from their home network since there is less rigor associated with the protection, monitoring, and maintenance of most home networks. Home users need to maintain a basic level of network defense and hygiene for both themselves and their family members when accessing the Internet.

Host-Based Recommendations

Windows Host OS

1. Migrate to a Modern OS and Hardware Platform

Both Windows 7 and Vista provide substantial security enhancements over earlier Windows workstation operating systems such as XP. Many of these security features are enabled by default and help prevent many common attack vectors. In addition, implementing the 64-bit mode of the OS on a 64-bit hardware platform substantially increases the effort of an adversary to attain a system or root compromise. For any Windows-based OS, verify that Windows Update is configured to provide updates automatically.

2. Install a Comprehensive Host-Based Security Suite

A comprehensive host-based security suite provides support for anti-virus, anti-phishing, safe browsing, Host-based Intrusion Prevention System (HIPS), and firewall capabilities. These services work collaboratively to provide a layered defense against most common threats. Several security suites today provide access to a cloud-based reputation service for leveraging corporate knowledge and history of malware and domains. Remember to enable any automated update service within the suite to keep signatures up-to-date.

3. Limit Use of the Administrator Account

The first account that is typically created when configuring a Windows host for the first time is the local administrator account. A non-privileged "user" account should be created and used for the bulk of activities conducted on the host to include web browsing, email access, and document creation/editing. The privileged administrator account should only be used to install updates or software, and reconfigure the host as needed. Browsing the web or reading email as an administrator provides an effective means for an adversary to gain persistence on your host. Within Vista or Windows 7, administrative credentials can be easily accessed by right clicking on any application, selecting the "Run as Administrator" option, then providing the appropriate administrator password. Furthermore, all passwords associated with accounts on the host should be at least 10 characters long and be complex (include upper case, lower case, numbers, special characters).

4. Use a Web Browser with Sandboxing Capabilities

Several currently available third party web browsers now provide a sandboxing capability that can contain malware during execution thereby insulating the host operating system from exploitation. Most of these web browsers also provide a feature to auto-update or at least notify you when updates are available for

download. Also, promising approaches that move the web browser into a virtual machine (VM) are starting to appear on the market but are not yet ready for mass consumer use.

5. Update to a PDF Reader with Sandboxing Capabilities

A sandbox provides protection from malicious code that may be contained in a PDF file. PDF files have become a popular technique for delivering malicious executables. Several commercial and open source PDF readers now provide sandboxing capabilities as well as block execution of embedded URLs (website links) by default.

6. Migrate to Microsoft Office 2007 or Later

If using Microsoft Office products for email, word processing, spreadsheets, presentations, or database applications, upgrade to Office 2007 or later and its XML format for storing documents. By default, the XML file formats do not execute embedded code when opened within Office 2007 or later products thereby protecting the user from malicious code delivered via Office documents. The Office 2010 suite also provides "Protected View" mode which opens documents in read-only mode thereby potentially minimizing the impact of a malicious file.

7. Keep Application Software Up-to-Date

Most home users do not have the time or patience to verify that all applications installed on their workstation are fully patched and up-to-date. Since many applications do not have an automated update feature, attackers frequently target these applications as a means to exploit a targeted host. Several products exist in the market which will quickly survey the software installed on your workstation and indicate which applications have reached end-of-life, require a patch, or need updating. For some products, a link is conveniently provided in the report to download the latest update or patch.

8. Implement Full Disk Encryption (FDE) on Laptops

Windows 7 Ultimate as well as Vista Enterprise and Ultimate provide support for Bitlocker Full Disk Encryption (FDE) natively within the OS. For other versions of Windows, third party FDE products are available that will help prevent data disclosure in the event that a laptop is lost or stolen.

Apple Host OS

1. Maintain an Up-to-Date OS

Configure any Mac OS X system to automatically check for updates. When notified of an available update, provide privileged credentials in order to install the update. The Apple iPad should be kept up-to-date as well and requires a physical connection (e.g., USB) to a host running iTunes in order to receive its updates. A good practice is to connect the iPad to an iTunes host at least once a month or just prior to any travel where the iPad will be used.

2. Keep Third Party Application Software Up-to-Date

Periodically check key applications for updates. Several of these third party applications may have options to automatically check for updates. Legacy applications may require some research to determine their status.

3. Limit Use of the Privileged (Administrator Account)

The first account that is typically created when configuring a Mac host for the first time is the local administrator account. A non-privileged "user" account should be created and used for

the bulk of activities conducted on the host to include web browsing, email access, and document creation/editing. The privileged administrator account should only be used to install updates or software, and reconfigure the host as needed. Browsing the web or reading email as an administrator provides an effective means for an adversary to gain persistence on your host.

4. Enable Data Protection on the iPad

The data protection feature on the iPad enhances hardware encryption by protecting the hardware encryption keys with a pass code. The pass code can be enabled by selecting "Settings," then "General", and finally "Pass code." After the pass code is set, the "Data protection is enabled" icon should be visible at the bottom of the screen. For iPads that have been upgraded from iOS 3, follow the instructions at: http://support.apple.com/kb/HT4175.

5. Implement FileVault on Mac OS Laptops

In the event that a Mac laptop is lost or stolen, FileVault (available in Mac OS X, v10.3 and later) can be used to encrypt the contents of a user's home directory to prevent data loss.

Network Recommendations

1. Home Network Design

The Internet Service Provider (ISP) may provide a cable modem with routing and wireless capabilities as part of the consumer contract. To maximize the home user's administration control over the routing and wireless device, deploy a separate personally-owned routing device (a) that connects to the ISP provided router/cable modem. Figure 1 depicts a typical home network configuration that provides the home user with the network infrastructure to support multiple systems as well as wireless networking and IP telephony services (b).

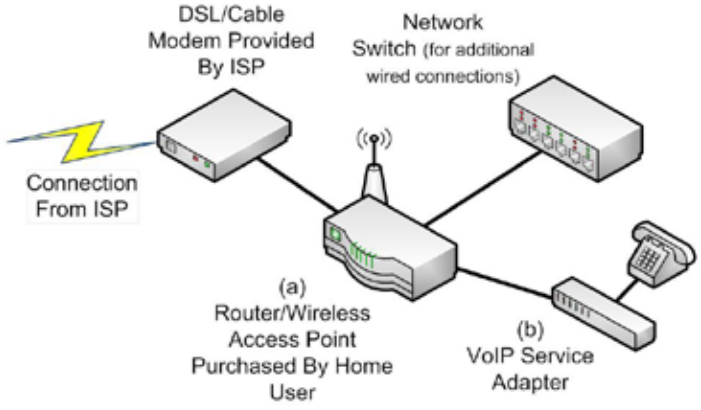

Figure 1: Typical SOHO Configuration

2. Implement WPA2 on Wireless Network

The wireless network should be protected using Wi-Fi Protected Access 2 (WPA2) instead of WEP (Wired Equivalent Privacy). Using current technology, WEP encryption can be broken in minutes (if not seconds) by an attacker, which afterwards allows the attacker to view all traffic passed on the wireless network. It is important to note that older client systems and access points may not support WPA2 and will require a software or hardware upgrade. When researching for suitable replacement devices, ensure that the device is WPA2-Personal certified.

3. Limit Administration to Internal Network

Administration of home networking devices should be from the internal-facing network. When given the option, external remote administration should be disabled for network devices. Disabling remote administration prevents an attacker from changing and possibly compromising the home network.

4. Implement an Alternate DNS Provider

The Domain Name Servers (DNS) provided by the ISP typically don't provide enhanced security services such as the blocking and blacklisting of dangerous and infected web sites. Consider using either open source or commercial DNS providers to enhance web browsing security.

5. Implement Strong Passwords on all Network Devices

In addition to a strong and complex password on the wireless access point, a strong password needs to be implemented on any network device that can be managed via a web interface. For instance, many network printers on the market today can be managed via a web interface to configure services, determine job status, and enable features such as email alerts and logging.

Operational Security (OPSEC)/Internet Behavior Recommendations

1. Traveling with Personal Mobile Devices

Many establishments (e.g., coffee shops, hotels, airports, etc.) offer wireless hotspots or kiosks for customers to access the Internet. Since the underlying infrastructure is unknown and security is often lax, these hotspots and kiosks are susceptible to adversarial activity. The following options are recommended for those with a need to access the Internet while traveling:

a. Mobile devices (e.g., laptops, smart phones) should utilize the cellular network (e.g., mobile Wi-Fi, 3G or 4G services) to connect to the Internet instead of wireless hotspots. This option often requires a service plan with a cellular provider.

b. Regardless of the underlying network, users can setup tunnels to a trusted VPN service provider. This option can protect all traffic between the mobile device and the VPN gateway from most malicious activities such as monitoring.

c. If using a hotspot is the only option for accessing the Internet, then limit activities to web browsing. Avoid accessing services that require user credentials or entering personal information.

Whenever possible, maintain physical control over mobile devices while traveling. All portable devices are subject to physical attack given access and sufficient time. If a laptop must be left behind in a hotel room, the laptop should be powered down and have Full Disk Encryption enabled as discussed above.

2. Exchanging Home and Work Content

Government maintained hosts are generally configured more securely and also have an enterprise infrastructure in place (email filtering, web content filtering, IDS, etc.) for preventing and detecting malicious content. Since many users do not exercise the same level of security on their home systems (e.g., limiting the use of administrative credentials), home systems are generally easier to compromise. The forwarding of content (e.g., emails or documents) from home systems to work systems either via email or removable media may put work systems at an increased risk of compromise. For those interactions that are solicited and expected, have the contact send any work-related correspondence to your work email account.

3. Storage of Personal Information on the Internet

Personal information which has traditionally been stored on a local computing device is steadily moving to the Internet cloud. Examples of information typically stored in the cloud include webmail, financial information,

and personal information posted to social networking sites. Information in the cloud is difficult to remove and governed by the privacy policies and security of the hosting site. Individuals who post information to these web-based services should ask themselves "Who will have access to the information I am posting?" and "What controls do I have over how this information is stored and displayed?" before proceeding. Internet users should also be aware of personal information already published online by periodically searching for their personal information using popular Internet search engines.

4. Use of Social Networking Sites

Social networking sites are an incredibly convenient and efficient means for sharing personal information with family and friends. This convenience also brings some level of risk; therefore, social network users should be cognizant of what personal data is shared and who has access to this data. Users should think twice about posting information such as address, phone number, place of employment, and other personal information that can be used to target or harass you. If available, consider limiting access to posted personal data to "friends only" and attempt to verify any new sharing requests either by phone or in person. When receiving content (such as third-party applications) from friends or new acquaintances, be wary that many recent attacks have leveraged the ease with which content is generally accepted within the social network community. This content appears to provide a new capability, when in fact there is some malicious component that is rarely apparent to the typical user. Also, several social networking sites now provide a feature to opt-out of exposing your personal information to Internet search engines. A good recommendation is to periodically review the security policies and settings available from your social network provider to determine if new features are available to protect your personal information.

5. Enable the Use of SSL Encryption

Application encryption (also called SSL or TLS) over the Internet protects the confidentiality of sensitive information while in transit. SSL also prevents people who can see your traffic (for example at a public WiFi hotspot) from being able to impersonate you when logging into web based applications (webmail, social networking sites, etc.). Whenever possible, web-based applications such as browsers should be set to force the use of SSL. Financial institutions rely heavily on the use of SSL to protect financial transactions while in transit. Many popular applications such as Facebook and Gmail have options to force all communication to use SSL by default. Most web browsers provide some indication that SSL is enabled, typically a lock symbol either next to the URL for the web page or within the status bar along the bottom of the browser.

6. Email Best Practices

Personal email accounts, either web-based or local to your host, are common attack targets. The following recommendations will help reduce your exposure to email-based threats:

a. In order to limit exposure both at work and home, consider using different usernames for home and work email addresses. Unique usernames make it more difficult for someone targeting your work account to also target you via your personal accounts.

b. Setting out-of-office messages on personal email accounts is not recommended, as this can confirm to spammers that your email address is legitimate and also provide awareness to unknown parties as to your activities.

c. Always use secure email protocols if possible when accessing email, particularly if using a wireless network. Secure email protocols include Secure IMAP and Secure POP3. These protocols, or "always use SSL" for web-based

email, can be configured in the options for most email clients. Secure email prevents others from reading email while in transit between your computer and the mail server.

d. Unsolicited emails containing attachments or links should be considered suspicious. If the identity of the sender can't be verified, consider deleting the email without opening. For those emails with embedded links, open your browser and navigate to the web site either by its well-known web address or search for the site using a common search engine. Be wary of an email requesting personal information such as a password or social security number. Any web service that you currently conduct business with should already have this information.

7. Password Management

Ensure that passwords and challenge responses are properly protected since they provide access to large amounts of personal and financial information. Passwords should be strong, unique for each account, and difficult to guess. A strong password should be at least 10 characters long and contain multiple character types (lowercase, uppercase, numbers, and special characters). A unique password should be used for each account to prevent an attacker from gaining access to multiple accounts if any one password is compromised. Disable the feature that allows programs to remember passwords and automatically enter them when required. Additionally, many online sites make use of password recovery or challenge questions. The answers to these questions should be something that no one else would know or find from Internet searches or public records. To prevent an attacker from leveraging personal information about yourself to answer challenge questions, consider providing a false answer to a fact-based question, assuming the response is unique and memorable.

8. Photo/GPS Integration

Many phones and some new point-and-shoot cameras embed the GPS coordinates for a particular location within a photo when taken. Care should be taken to limit exposure of these photos on the Internet, ensure these photos can only be seen by a trusted audience, or use a third-party tool to remove the coordinates before uploading to the Internet. These coordinates can be used to profile the habits and places frequented for a particular individual, as well as provide near-real time notifications of an individual's location when uploaded directly from a smart phone. Some services such as Facebook automatically strip out the GPS coordinates in order to protect the privacy of their users.

Enhanced Protection Recommendations

The following recommendations require a higher level of administrative skills to implement and maintain on home networks than the previous recommendations. These recommendations provide additional layers of security but may impact your web browsing experience or require some iteration to adjust settings to the appropriate thresholds.

1. Enhanced Wireless Router Configuration Settings

Additional protections can be applied to the wireless network to limit access. The following security mechanisms do not protect against the experienced attacker, but are very effective against a less experienced attacker.

a. MAC address or hardware address filtering enables the wireless access point to only allow authorized systems to associate with the wireless network. The hardware address

for all authorized hosts must be configured on the wireless access point.

b. Limiting the transmit power of the wireless access point will reduce the area of operation (signal strength) of the wireless network. This capability curtails the home wireless network from extending beyond the borders of a home (e.g., parking lot or adjacent building).

c. SSID cloaking is a means to hide the SSID, the name of a wireless network, from the wireless medium. This technique is often used to prevent the detection of wireless networks by war drivers. It is important to note that enabling this capability prevents client systems from finding the wireless network. Instead, the wireless settings must be manually configured on all client systems.

d. Reducing the dynamic IP address pool or configuring static IP addresses is another mechanism to limit access to the wireless network. This provides an additional layer of protection to MAC address filtering and prevents rogue systems from connecting to the wireless network.

2. Disable Scripting Within the Web Browser

If using third party web browsers such as Firefox or Chrome, use NoScript (Firefox) or NotScript (Chrome) to prevent the execution of scripts from untrusted domains. Disabling scripting can cause usability issues, but is an effective technique to reduce web bourne attacks.

3. Enable Data Execution Prevention (DEP) for all Programs

By default, DEP is only enabled for essential Windows programs and services. Some third party or legacy applications may not be compatible with DEP, and could possibly crash when run with DEP enabled. Any program that requires DEP to execute can be manually added to the DEP exemption list, but this requires some technical expertise.

Additional Published Guidance

Social Networking
http://www.nsa.gov/ia/_files/factsheets/I73-021R-2009.pdf

Mitigation Monday #2 – Defense Against Drive By Downloads
http://www.nsa.gov/ia/_files/factsheets/I733-011R-2009.pdf

Mitigation Monday – Defense Against Malicious E-mail Attachments
http://www.nsa.gov/ia/_files/factsheets/MitigationMonday.pdf

Mac OSX 10.6 Hardening Tips
http://www.nsa.gov/ia/_files/factsheets/macosx_10_6_hardeningtips.pdf

Data Execution Prevention
http://www.nsa.gov/ia/_files/factsheets/I733-TR-043R-2007.pdf

The Information Assurance Mission at NSA

SNAC DoD, 9800 Savage Rd. Ft. Meade, MD 20755-6704 www.nsa.gov/snac
SNAC@radium.ncsc.mil

NSA Creative Imaging – 48039