



S V E C C

SVECC Newsletter

Sunland Village East Computer Club

September 2008

Volume 5 issue 9

Inside this issue:

Top 11 Free	2
Network Security	3
Network Security	4
Network Security	5
Computer Help	6
Tips & Tricks	7
Exit laughing	8

Monthly Reminders:

- Run Disk Cleanup
- Defrag your hard drive
- Update Windows
- Update Spybot
- Update AdAware
- Run your Anti-virus

Summary Of SVECC Computer Lab

Well summer is winding down and our Computer Lab project is making headway. I thought we could use this edition of the newsletter to bring everyone up to date, and to encourage membership renewals, and payment of the \$20.00 special assessment.

I hope that as I go through the purchases made to date, everyone will realize that extreme care is being used in spending the clubs funds.

Below are some of the budgeted items and the actual purchases.

Budget 12 computers @ \$550.00 ea.
Actual 24 computers @ \$273.00 ea.

Budget 18 chairs @ \$15.00 ea.
Actual 22 chairs @ \$3.00 ea.

In addition to the 22 straight chairs we have purchased 14 secretary chairs @ \$5.00 ea.

Our new projection screen lists on the internet at \$355.00 and was purchased for \$125.00



Above is new lab directory purchased for \$10.00 from ASU surplus

Last week at the ASU auction we were able to purchase for \$150.00 a new HP laser printer that was on sale at Fry's for \$274.00.

A break down of the Computers is as follows:

24 Towers, with keyboard, mouse and power cord, Windows XP Operating System, anti-virus, and Open Office. \$115.00

18 Monitors (19") from Staples \$149.00 ea and 3 Monitors (19") from Fry's at \$119.00

In addition we have obtained a sink, 2 book cases, instructors desk, projection table, power strips, instructors chair, and locking storage cabinet.

Yet to be purchased 2 Linksys routers, 4 - 8 port gigabit switches, cables, and of course the cabinets to be built by Les Warren.

To date we are \$3000.00 under budget on the items obtained.

Top 11 free programs

SVECC (Sunland Village East Computer Club)



AVG Anti-virus:

AVG Anti-Virus Free Edition is the most popular free solution available at no cost to home users and provides the high level of detection capability that millions of users around the world trust to protect their computers.

AVG Anti-spyware:

AVG Anti-Spyware Free Edition is a popular free antispyware solution available at no cost to home users and provides a high level of detection capability.

IObit Smart De-frag:

- An "Install It and Forget It" feature that works automatically and quietly in the background on your computer.

- The ability to constantly keep your hard drive safe, error-free and running at its top speed and optimum performance.

- Eliminates slow downs, freeze-ups and crashes.

- IObit SmartDefrag is 100% FREE award-winning software that's for personal, home and small business.

- 100% safe from any spyware, adware and virus. .

- Designed for Windows Vista, XP, and 2000.

Just Zip-it:

Have you often felt that ZIP programs are just unnecessarily complicated? Have you ever tried to explain to your mother how to use WinZIP? Well, that's exactly what inspired the creating of "JustZIPit", the world's easiest ZIP tool.

Send To:

SendTo 1.6 simplifies sending any file or folder to any location on your computer, using the Right Click 'Send To' menu. You can even send to applications and FTP sites on the internet.

Revo Un-installer:

Revo Uninstaller helps you to uninstall and remove unwanted programs installed on your computer even if you have problems uninstalling and cannot uninstall them from "Windows Add or Remove Programs" control panel applet.

Revo Uninstaller is much faster and more powerful alternative to "Windows Add or Remove Programs" applet!

Firefox:

The award-winning Web browser is now faster, more secure, and fully customizable to your online life. With Firefox 2, we've added powerful new features that make your online experience even better.

Thunderbird:

Keep Your Vital Information Organized

Thunderbird 2 features many new enhancements to help you better manage your unruly inbox, and stay informed. Thunderbird 2 scales to the most sophisticated organizational needs while making it easy to find what you need.

Secure and Protect Your Mail

Mozilla has bolstered Thunderbird's acclaimed security and privacy measures

to ensure that your communications and identity remain safe. It's like having your own security guard online.

CC Cleaner:

CCleaner is a freeware system optimization and privacy tool. It removes unused files from your system - allowing Windows to run faster and freeing up valuable hard disk space. It also cleans traces of your online activities such as your Internet history. But the best part is that it's fast (normally taking less than a second to run) and contains NO Spyware or Adware! :)

CDBurnerXP:

CDBurnerXP is a free application to burn CDs and DVDs, including Blu-Ray and HD-DVDs. It also includes the feature to burn and create ISOs, as well as a multilanguage interface. Everyone, even companies, can use it for free. It does not include adware or similar malicious components.

Xplorer2:

The lightweight version of xplorer² is not as powerful as the professional version but it shares the same desktop browsing and file management engine, it sports dual panes and folder tabs, and gives many rival paid-for file managers a run for their money — literally! It is a complete little file manager, albeit lacking a bit in bells and whistles.

All of the above are available through links on the svecc.com web site.

Firefox:

The award-winning Web browser is now faster, more secure, and fully customizable to your online life. With Firefox 2, we've added powerful new features that make your online experience even better.



Wi-Fi Network Security

Wi-Fi Network Security

Tweaks To Keep Visitors Out

Wireless home networks are wonderful things. They enable you to share Internet connections, files, and printers without the need for complex wiring, and they untether portable devices such as notebooks and media players.

Nevertheless, wireless networks can be perilous for the unwary. This is an issue for everyone, not just big companies with sensitive data. Even the smallest home network can be a target, not only of malicious data thieves, but also of nearby bandwidth snatchers who hijack your connection and use it to access the Internet, send spam, or attack other computers. Also, if unauthorized users piggyback on your network, your connection will be slower.

Furthermore, if one of your neighbors has an unsecured network, your improperly structured system may accidentally connect to it. This may sound innocuous, but if you are on your neighbor's network, he could access personal information, such as your password.

The good news is that these issues are relatively easy to fix. It will take a little configuration, but the security and peace of mind you'll gain will be worth it. Note that the instructions in this article assume at least one of your PCs is running Windows XP SP2 (Service Pack 2). If you are running Vista, the OS (operating system) will automate many of these tasks for you. If you are running another version of Windows

on any of your PCs, most of this information still applies, but you won't have access to the automation wizards we mention.

Avoid The Neighbors

On WinXP SP2 PCs, the wireless networking utility will not connect to a strange, unsecured network without permission. (If any PC on your network uses the wireless adapter's networking utility, rather than the one in Windows, the Windows-specific instructions in this section won't apply. However, the adapter card's utility likely has parallel settings that you will manage in a similar fashion.) Furthermore, each time one of them connects, it will seek networks you have marked as preferred, in order of preference. However, during operation, the WinXP SP2 WZC (Wireless Zero Configuration) service periodically scans for the strongest signal.

If you have previously connected to available nearby networks from one or more of your PCs that support WZC (notebooks are likely culprits) and the signal on one of your home network PCs is weak or terminates suddenly, it's possible that PC will connect to the stronger signal. Adjusting your settings to prevent automatic connection can ensure this doesn't happen.

If your network router and adapter are WPA2 compatible (shown are the WPA2-compatible Belkin Wireless G Plus MIMO adapter and router), you'll be able to use the most secure encryption technology available for home networks.

On any PC with which you've connected to other networks, click the Start menu, select Control Panel, and double-click Network Connections. Locate the wireless adapter in the list of network connections, right-click it, and select Properties. If you see a Wireless Networks tab, click it. (If you do not see a Wireless Networks tab, your adapter doesn't support WZC and network hopping will not be a problem.)

Under Preferred Networks, if your home network is not listed in the first (most preferred) position, select it and click Move Up to rearrange it. Locate other networks on the Preferred list. If you do not want them, click the network and click Remove. Otherwise, click Properties and under the Connection tab, uncheck Connect When This Network Is In Range. (You'll have to re-enable this option if you ever want automatic connection to the network.) For your home network, automatic connection should be enabled.

Return to the Wireless Networks tab and click the Advanced button. Ensure that Automatically Connect To Non-Preferred Networks is not checked. Selecting this option will let WinXP connect to any available network, unsecured or no, if not preferred network is available.

Be Restrictive

Wireless networks transmit using radio waves, just like an FM radio, and can be picked up easily. In the early days of Wi-Fi, lack of range was a problem. With newer routers (some of which can



Wireless home networks are wonderful things. They enable you to share Internet connections, files, and printers without the need for complex wiring



Wi-Fi Network Security

broadcast up to 1,000 feet), users must contend with ranges that are too extensive (and inviting).



Take your notebook or other portable connected device (your smartphone, if it has Wi-Fi, is the easiest option) outside and try to locate your network. If the device sees it out on the road, so can others. Fortunately, you can adjust the access points to minimize bandwidth leakage.

Position the router and/or access points so that wireless transmissions don't travel outside the home region. If you have a large backyard, this could be near the center of the rear wall of the house. In communities with postage stamp-sized yards, the middle of the home, away from any windows, might be a better solution.

If your Internet connection enters your home in a highly exposed place such as the front of the house, the most secure, if slightly cumbersome, solution is to use a single, extended-length Ethernet cable between the modem and a securely positioned Wi-Fi router. If you add more access points for better coverage (indoor range when walls intervene is often 50 to 100 feet), keep the location rules in mind. This sounds like a bit of a hassle, and it is, but it will help secure your wireless network.

Don't Default

Your network equipment likely came with preset default identification settings. Two of these are the username and password, which you (or anyone who gains

access) can use to reconfigure the network from the device's Web-based administrative console. If you didn't change the default username and password during setup, it's important to do so ASAP or someone may have easy access to your devices. If you live in an area with a lot of traffic or close neighbors, consider changing these settings every few months.

Check your router's documentation for instructions on changing the username and password. You'll likely access an administrative console located on the Web site you visited during setup. Don't use your birthday, name, or address as part of the username or password; do use a combination of numbers and letters. For strong security, the username and password should be at least eight characters long.

A third default setting is the SSID (Service Set Identifier; the name of your network) your network broadcasts. With early versions of Windows, experts instructed users to change their SSIDs and hide them from view. However, for reasons we'll discuss under Shout It Out, hiding your SSID will not guarantee that it isn't broadcast. Consequently, we don't recommend that you hide the SSID, but it is a good idea to change it, and here's why.

Remember the WZC service we mentioned earlier? Because large networks often use the same SSID for multiple routers, WZC assumes that two signals in range of each other with the same SSID belong to the same

network. If it finds two same-name SSIDs, it only displays the stronger signal as an available network. If you and a neighbor both have networks with default SSIDs such as "linksys" or "default," you could inadvertently connect to your neighbor's network if it transmits a stronger signal.

Naming strength is not particularly important, although you shouldn't use your name or address. Consider changing the SSID to something that sounds secure—for example, incorporating a word such as "private" can discourage inadvertent connectors.

If you decide to change your SSID, you must change it globally on all network equipment and devices. WinXP SP2 computers with built-in Wi-Fi or whose network connector supports WinXP's Windows Connect Now can use it to change the network SSID (and may have already done so during setup). You can access it via the Start menu; select Control Panel and double-click Wireless Network Setup Wizard. For PCs, routers, and adapters that do not support Windows Connect Now, the configuration utility will likely be on the Web and/or installed on the PCs in question. Consult the documentation that came with each piece of network equipment for assistance changing the SSID.

Note that you may not need (or might not be able) to change some device SSIDs. If printers or other wireless devices can connect directly to one of the network PCs and you can share that functionality with the network

Check your router's documentation for instructions on changing the username and password. You'll likely access an administrative console located on the Web site you visited during setup.



Wi-Fi Network Security

through that PC (using a method such as file and printer sharing), you won't need to change the network name.

Shout It Out

During SSID reconfiguration, you may see an option to hide the SSID. Do not enable it. With a hidden SSID, your network will not broadcast its name, so users must know the SSID to connect. This sounds like a sensible precaution, but Microsoft recommends WinXP users against it, because this action will not completely conceal your SSID. In fact, it may even cause your devices to display your SSID at inopportune times as they send out frequent requests to join the network.

For example, the Wi-Fi adapter of a laptop associated with a hidden-SSID network will poll for the network periodically (whether or not the network is in range) and thus disclose the SSID to those who know how to pick it up. If the SSID is not hidden, the laptop will not poll for the SSID; it is able to connect to the network without searching for it. A notebook PC on a network with a hidden SSID can disclose your network's SSID anytime the Wi-Fi antenna is operating, no matter where you are, making it less secure than simply displaying your SSID at home.

Restricting MAC access (shown on the Web-based administrative console of a Linksys router) is a good way of protecting your network from casual invaders.

Go For The Big MAC

For another layer of security

(especially important if you live in an apartment and cannot restrict network transmissions to your personal space), you can implement MAC (Media Access Control) Address Filtering. Every network adapter or card has a unique hardware address, called the MAC address, that identifies it to the router. With MAC Address Filtering, your router only allows connections from devices whose MAC addresses the user has previously approved.

Check your router's documentation to see if you can set up MAC Address Filtering. This will deter wardrivers and casual bandwidth thieves. It will not stop dedicated hackers, who can discover MAC addresses and mimic them.

Scramble It Up

All wireless equipment supports encryption, which scrambles transmissions to make them hard for hackers to decipher. No matter what type of encryption your network supports, enable it. If you are running WinXP SP2 and your network equipment supports Windows Connect Now, you can use it to turn on encryption or adjust settings. (See "Use Windows XP's Wireless Network Setup Wizard" on page 28 for more information about using Windows Connect Now.)

In earlier versions of WinXP, you can use Wireless Network Properties (on the Wireless Networks tab; see the Avoid The Neighbors section of this article for instructions about how to access this tab) to change these settings. Otherwise,

you'll likely need to work with the utilities and/or Web interfaces of your various equipment.

Note that all equipment (including network access points, cards, PCs, wireless cameras, and other devices interacting with the network) must support the encryption type you choose (possibly through additional configuration or installation of drivers), which may limit your choices. Check your documentation for your options.


During initial encryption setup, you will likely choose a passphrase or a network key. Ensure this is strong using the criteria described previously. If you select a passphrase, the router may use it to generate network keys, either during setup or at login (depending on the encryption standard). Write down the passphrase you select and the first key generated, if any, as you may need them later.

The strongest form of encryption currently available is WPA2 (Wi-Fi Protected Access 2; consumers use the personal variant, called WPA2-Personal), but many network devices, as well as versions of Windows prior to WinXP SP2, do not support it. For a list of WPA2-certified products, visit certifications.wi-fi.org/wbcs_certified_products.php. Click Advanced Search and make WPA2 part of your search criteria.

by Jennifer Farwell



During initial encryption setup, you will likely choose a passphrase or a network key. Ensure this is strong using the criteria described previously.



Contact the Help Group for Computer problems only.

Tutoring on applications, or operating systems software is available at \$25.00 for a two hour session.

The helpers listed below volunteer their time to help Club Members

Please be respectful of their time this is not a 24/7 service

Under no circumstances will we help with Pirated Programs

Virus protection is the responsibility of the member, virus removal and anti-virus program or anti-malware program installation is done on a fee for service basis

We will only accept help calls from 9 am to 5 pm.

Computer Help Group

Group Leader Joe Zagar

Joe Zagar	480-373-9373	all systems and programs
Jeff Bowlds	480-984-5309	all systems and programs
Levern Swensen	480.986-5997	Hardware Installation
Red Malchow	480-984-5510	Hardware Problems
Warren Sommerfeld	480-984-1525	Photo editing

September 2008

SUN	MON	TUE	WED	THU	FRI	SAT
	1 Mesa Verde	2	3	4	5	6
7	8 Mesa Verde	9	10	11	12	13
14	15 Mesa Verde	16	17	18	19	20
21	22 Mesa Verde	23	24	25	26	27
28	29 Mesa Verde	30				

Computer Tips and Tricks

- **When to Update Drivers:** Some driver Web sites recommend that you update your drivers regularly. Newer drivers often expand functionality, so updating your drivers has a benefit. However, the old saying, "If it ain't broke, don't fix it," applies to computing. A new driver can cause problems with a functional configuration as easily as an older driver can. Conventional wisdom says the following: 1. If a device quits working or crashes your PC even though you have changed nothing, reinstall the existing driver. 2. If you are installing an older device on a new system, or if you have made changes to your system and a device is acting up, look for an updated driver. 3. If your device has never worked well or at all with the default driver (especially if the device and PC are of different vintage), experiment with old and new drivers to find the best one.
- **Memory Error Messages:** Memory-related error messages that appear when your computer first begins booting usually point to a bad memory module. The computer performs basic tests on all hardware when it's first switched on. If the information it writes to memory is not the same as the information it reads from memory, the computer stops booting and displays an error message.

In most cases you'll need to replace the bad module. If you have recently installed new memory, however, the problem could be a compatibility issue. Try removing the new memory and see if it solves the problem.

If you have multiple memory modules, try booting your PC with just one module installed at a time. This will help you isolate the bad memory module.

- Reprinted with permission from *Smart Computing*

SVECC

Editor
Joe Zagar

President
Delores Bruno

Sunland Village East Computer Club

Founded for the Residents of Sunland Village East

Mission: To help each other learn about Computers

Membership is open to all residents of SVE

Dues are \$20.00 per Year

Due October 1st

Plus a 20.00 assessment for 2008 only



Making your computer
Work for You

We are on the
Web SVECC.Com

***** They Walk Among Us! *****

I was at the checkout of a K-Mart. The clerk rang up \$46.64 charge. I gave her a fifty dollar bill. She gave me back \$46.64. I gave it back to her and told her that she had made a mistake in MY favor and gave her the money back. She became indignant and informed me she was educated and knew what she was doing, and returned the money

again. I gave her the money back again...same scenario! I departed the store with the \$46.64.



I walked into a Mickey D's with a buy-one-get-one-free coupon for a sandwich. I handed it to the girl and she looked over at a little chalkboard that said "buy one-get one free." "They're already buy-one-get-one-free", she said, "so I guess they're both

free" She handed me my free sandwiches and I walked out the door.

They Walk Among Us and Many Work Retail.

One day I was walking down the beach with some friends when one of them shouted, "Look at that dead bird!" Someone looked up at the sky and said, "Where?"

.....They Walk Among Us!

