PC Post

**For directions to
Destiny Christian
Center
see page 8**

OUR NEXT MEETING

MPCUG to explore beginners′ SIG

Web Master Jim Goodman will give and get ideas from all present when members of the Modesto PC User Group meet on Thursday, Aug. 28., as he prepares to launch a new Beginners' Special Interest Group,

Jim, while presenting his ideas for the first SIG meeting – scheduled for 6:30 p.m., Sept. 8, at Denny's restaurant ─ will take note of all suggestions and ideas presented in this audience-participation membership meeting. So come prepared with your concepts of what you need to know.

As usual, the membership gathering will begin at 6:30 p.m. with the Random Access Special Interest Group, where members can get their most pressing computer questions answered. Goodman's presentation will follow refreshments at 7:30 p.m.

The event will take place – for the last time ─ at Destiny Christian Center on Carver Road just south of Roseburg Avenue. Members and friends should park in front or back of the building and enter on the south side.

In September, monthly membership sessions will become dinner meetings at Denny's restaurant, 1525 McHenry Ave., due to the Christian center's inability to host nonprofit groups while retaining its special income tax status.

IMPORTANT MEETING DATES

**General Meeting — August 25 — Destiny Christian Center
Photo SIG Meeting — on hiatus
Board Meeting — September 6 — Ridgeway's Restaurant
Beginner's SIG Meeting — will resume this fall**

Welcome Judy Taylour, new joint PC Post editor

In assuming the editorship of the PC Post after we all suffered from the loss of Bud Bondietti, I knew that I had to limit my effort. I'm serving on the board or committees of multiple other organizations including the Patterson 2009 Centennial Committee on which I chair a major committee. At first, I only agreed to do three months after Bud's death hoping someone would step forward to take over the Post. After attending an MPCUG board meeting, I decided to take advantage of an offer to help with the Post and move forward with the editing in way that would minimize the usage of my time.

I had been sharing my editorship concerns with Judy Taylour, Santa Clarita Valley PC Group president and friend of Bud's whom she met at several APCUG events that Bud attended for us. Judy is very active in APCUG, the national organization MPCUG belongs to.

Judy's part of the Post co-editorship will revolve around filling the Post with appropriate articles from other newsletters and writers of computer articles. In viewing her selections, we will be rewarded with articles we need to read to keep up with the PC computing world. Welcome Judy, and many thanks…. *Claude*

Membership Report…. Hank Mudge

Members' dues expired in May

Richard & Katherine Pyle
Jerry Pack
Keith Schock
Bee Hagens

Members' dues expired in June

Robert & Barbara Meyer
Terence Fix
Gene Richards
Allan Romander

Members' Dues expired in July

Nick & Lorna Crooker
Orval Brewer
Richard Hitchcock

Members' Dues Expiring in Sept.

Sheryl Powell

Treasurer's Report…. Barb Cameron

Financial Statement	July 2008	
INCOME		
Membership	$0.00	
Interest on savings	0.00	
Donations	0.00	
TOTAL INCOME		$0.00
EXPENSES		
Destiny Church (June-Aug)	$75.00	
TOTAL EXPENSES		$75.00
CURRENT ASSETS		
Checking - USbank, Modesto	$1,330.80	
Savings - USbank	332.39	

Current Assets:		$1,663.19
FIXED ASSETS		0.00

Total Assets		$1,663.19

Claude's Bytes ….

By Claude Delphia, Editor Emeritus, Modesto PC User Group

Email problems and usage

Spam has caused some people to change their email usage to conduct business or effectively communicate with family, friends or associates. So the issue becomes how to deal with spam so it doesn't affect the efficiency of your activities via email.

When I moved back to Patterson 2½ years ago, I had to make a choice of Internet providers. Because Comcast was going to be my cable provider, I decided to use them for my Internet provider also. Prior to that I was using Charter and it was very satisfactory. My cable equipment meant that I didn't need to buy new equipment for Comcast.

I was then pleasantly surprised to see that they provided McAfee virus and spam program free as part of my package of services.

The amount of spam I receive went way down from what I was getting on Charter in Ceres. I literally get less than 10 spams a day on Comcast. I do get some spam that I unfortunately initiated by signing up on some website, but that's my mistake and has nothing to do with Liberian type spams to collect my $50m share of some bank account. I don't recall getting a Viagra or similar spam in several years.

So I recommend that if you are getting many spams a day, find out what anti spam programs are available, maybe even something your Internet provider might have to offer free. Nobody wants to have to pay to eliminate spam, but each of us must decide whether the spam is causing us enough trouble to pay to eliminate it, that is if we can't get a free anti spam program.

Weird spam

About a month ago, I started getting an email urging me to update my Adobe Reader to version 8.   When I clicked on it, it went to a special page to download the Adobe Reader version 9, which is the latest. On further checking, the page doesn't appear to be an official Adobe site. However it's unclear what is happening. I did download Adobe Reader 9 as I think it's better to have the latest version of that program. It also has some wonderful new features that if they were there before, I wasn't aware of them. It also has a different look than the older Reader 7 version.   Most people don't need the newer version, so don't bother unless you want newer features including the ability to Comment and highlight text in documents.

Crash, continuous rebooting

It seems to happen to all of us sooner or later: our computer starts to act up, many times without warning.

That happened to me early this month.   The computer had been working all day with no problems. I then went off to a meeting having turned it off. When I got back, I turned it on and after 3 automatic reboots I knew I had a problem, but I didn't panic. I knew I had some options.

The most important option was to know that Windows XP has a go back feature. I was actually pretty sure that something had been installed on my computer in the last eight hours that was causing the problem. I re-

member it as something that was automatic and it was known software already on my computer that needed an update. Actually there were probably several that day.

So I called Jim Goodman to talk me through the reboot in safe mood feature. It was incredibly easy. All I had to do was to restart the computer in SAFE mode by holding down F8 while computer restarted.

Fairly quickly I had the safe mode choice screen which was telling me that my computer hadn't restarted properly the last time. Down near the bottom of the list of options was an offer to restart at the last good point that the computer was working properly. I selected that and within minutes, Windows was back up and running just as if nothing had happened.

Take that Windows 98 and all those other old versions it took to get to XP. And maybe someday I'll even upgrade to Vista, well maybe if there is a real reason to do that.

iPhone for Boomers

by Sandy Berger, CompuKISS
http://www.compukiss.com / sandy(at)compukiss.com

Obtained from APCUG with the author's permission for publication by APCUG member groups.

According to the data from the International Communications Union, the world now has more than 2 billion cell phone or mobile phone subscribers. While some business and high tech users are using their phones for email and the Internet, I venture to say that most of those 2 billion users are only using their cell phones to make calls and to text message. In fact, I am sure that many users don't know how to do much more than that, even though their phones are capable of much more.

The reason is that up until now, cell phones with their tiny buttons and complex menu systems have frustrated many average users. The recent introduction of a fast, stable, and more affordable iPhone is poised to change all of that.

While the twenty- and thirty-something's are flocking to the iPhone as the latest status symbol, the forty- , fifty-, and sixty-something's are acquiring iPhones because there are no tiny buttons and no complex menu systems. In fact, the large bright touch screen, big icons, and the on-screen keyboard make the iPhone extremely easy to use.

One button brings up the Home screen of icons. The screen is clear and uncluttered. The icons are all easily identifiable by their picture, so the iPhone experience is very visual. The four most used icons are placed on the bottom of the screen. By default, they are Phone, Mail, Safari (the Internet browser), and iPod. You can put whatever you use the most on the bottom row. You can also rearrange all the icons to suit your taste.

The way you rearrange the icons is indicative of the ease of use of the entire gadget. To rearrange the icons on the Home screen, you simply press any icon and hold your finger down until all the icons start to wiggle. Then you drag the icons from place to place. To put an icon on the second page of the Home screen, you simply drag it off the screen to the right. The second page will appear with the icon on it. To return to the first screen

IPHONE (Continued from page 4)

of the Home page, just drag your finger across the screen in a leftward motion. To stop the wiggling and confirm that you are done moving the icons around, you simply touch the Home button You can't miss it because while other cell phones seem to have a million buttons, the Home button is the only button on the surface of the iPhone.

As you can tell by this explanation, the iPhone is also very tactile. You can move things around the screen with your finger. To make a web page larger, you simply flick your two fingers apart on the screen. Bring your fingers together and the webpage gets smaller. Double-tap the screen and the page fits the screen. To take a picture, you press the camera icon, aim the camera on it is actually fun!

On top of that Apple has added a Apps store to its iTunes Online Store. They have over 500 applications that you can add to your iPhone. Many are free. Others cost $1. Most of those which you have to pay for are under $10. Some of these applications are just for fun, some are for productivity. For instance, if you download an application called Recorder, you can turn your iPhone into an voice recorder. But you can also choose an application that turns it into an a light saber or one that lets you pop bubbles on the screen.

At $199 for the 8GB model, the iPhone has a lot to like. To use it you must subscribe to AT&T for two years. That is not unusual for a cell phone service contract. You also have to have an additional data plan that costs $30 a month. While this might seem costly, you get a lot for your money.

Not only is the iPhone intuitive, visual, and tactile, but it has access to the Internet and lets you send and receive email. It is like having a mini-computer in your hand. For many it will replace the laptop they drag along when traveling.

The iPhone is also a full-blown iPod that plays both music and video. Since it has its own speaker, you don't even need earbuds or headphones as you do with most other music players. Oh, and did I mention, it has the best audio quality of any cell phone I've ever used.
Am I hooked? You bet I am……. And the same thing will happen to many others who try the iPhone. It is poised to change the way we use cell phones.

This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

Secure Your Wireless Network

by Ira Wilsker, APCUG Director; Columnist, The Examiner, Beaumont, TX:
Radio & TV Show Host
iwilsker(at)apcug.net

WEBSITES:
http://www.fbi.gov/page2/may08/wifi_050608.html
http://www.pcmag.com/article2/0,2817,2293406,00.asp
http://www.fbi.gov/cyberinvest/protect_online.htm

Many of us have wireless networks (Wi-Fi) at home, and often use other wireless networks at the office, coffee shops, restaurants, hotels, airports, and a variety of other places. Many of us blissfully connect to whatever network is available, either free or pay networks, oblivious to the security threats we will likely encounter. We may feel safe behind the locked doors of our homes while we leisurely surf the net on our home Wi-Fi, unaware that our wireless signal can be picked up, without the use of any sophisticated hardware, a few hundred

(Secure Your Wireless Network—Continued from Page 5)

precautions with out Wi-Fi, we are open to attack by electronic eavesdroppers, identity thieves, and an assortment of hackers, crackers, and other miscreants, many of which may be bent on doing us harm. According to the FBI, "odds are there's a hacker nearby, with his own laptop, attempting to 'eavesdrop' on your computer to obtain personal data that will provide access to your money or even to your company's sensitive information."

Several years ago, while working on a cyber security grant, I took the liberty of driving down the major thoroughfares in town, including the downtown area, equipped with my notebook computer with wireless adapter, and my Garmin EMap GPS, carefully logging the many wireless networks I was receiving. About 80% of the networks that I received on my computer did not have adequate security, and could have been easily accessed from the road. This practice of driving around a city looking for open wireless networks is known in hacker circles as 'war driving', and there are many illicit websites that have detailed city street maps that accurately show the locations of these vulnerable networks. On a trip to New York City, one of my daughters asked me what the chalked symbols on the sides of buildings meant; I explained that 'war chalking' was the practice of labeling the buildings themselves that housed inadequately protected wireless networks. Anyone with a little larceny in his heart who was aware of the symbolism could easily penetrate the wireless networks thus disclosed. There is a large group of hobbyist hackers who delight in seeing how many wireless networks that they can penetrate in a given period of time. What the Wi-Fi hacker can do to the computer infrastructure and data of a vulnerable wireless network is only limited by his conscience.

Wireless hotspots, now common in fast food restaurants, coffee shops, airport waiting areas, and hotel lobbies, are other places that the innocent web surfer can be attacked while accessing the internet. Many of these business locations actively advertise their Wi-Fi hotspot status and availability. Again, according to the FBI, "there are 68,000 Wi-Fi 'hot spots' in the U.S., at airports, coffee shops, hotels, bookstores, schools, and other locations where hundreds or thousands of people pass through every day. While many of these hot spots have secure networks, some do not, according to Supervisory Special Agent Donna Peterson of our Cyber Division. And connecting to an unsecured network can leave you vulnerable to attacks from hackers."

Hackers have a variety of tools and methods that they can use to penetrate your wireless computer. One that I have personally experienced (but did not fall for) is the phony 'free wireless access' or inexpensive wireless connection that often appears on the list of wireless networks at airports and other areas. Hackers set up these hotspots in areas where there are likely to be many potential users (victims). Last January, in the Las Vegas airport (LAS), I picked up a very strong wireless signal from a source using the name (SSID) of "Free LAS Internet". I happened to know as a fact that in the area and terminal I was in, there was no free Wi-Fi access provided by the airport. What this most likely represented was a hacker trolling for nearby victims in the terminal. They commonly dangle the bait of free or cheap internet access, and wait for the hapless user to connect. Once connected, unless proper security precautions are in place and functional, the hacker may have access to any data that is on the victim's computer. Popular items to steal are user ID's, passwords, credit card numbers, and other personal information; this may also be used for sophisticated identity theft. Some hackers will install keylogging Trojans to record all of the victims' keystrokes. Other hackers may redirect the user to counterfeit websites for the purpose of stealing information. The FBI says, "Another thing to remember," said (FBI) Agent Peterson, "is that the connection between your laptop and the attacker's laptop runs both ways: while he's taking info from you, you may be unknowingly downloading viruses, worms, and other malware from

For the latest information about the MPCUG — Check our website at

WWW.MPCUG.NET

(Secure Your Wireless Network—Continued from Page 6
him."

There are several tips on wireless security that the FBI has published; they are mostly common sense precautions that we should all be doing anyway. First, try not to connect to an unknown Wi-Fi network; just because an available network carries the name of the hotel, restaurant, or airport does not necessarily mean that it is legitimate, as the SSID (name) can be easily forged. Other recommendations from the FBI include, "Make sure your laptop security is up to date, with current versions of your operating system, web browser, firewalls, and antivirus and anti-spyware software; don't conduct financial transactions or use applications like e-mail and instant messaging; change the default setting on your laptop so you have to manually select the Wi-Fi network you're connecting to; turn off your laptop's Wi-Fi capabilities when you're not using them."

Our home wireless networks are every bit as vulnerable to attack as is the road-warrior. One of my acquaintances has periodically used the wireless network of his neighbor (without his knowledge or consent) for broadband internet access, rather than subscribing to an internet service himself. This home user who had the open wireless system did not have any of the protective security features, like encryption, activated. It should be noted that firewalls generally do not provide any significant protection against unscrupulous wireless access. Virtually all home and office wireless systems utilize a router of some type to broadcast the signal.

Wireless routers offer some encryption, which should be utilized; many models turn off encryption by default, while others require it. It should be noted here that an encrypted signal is difficult for unauthorized users to utilize, and a very necessary security implementation. The two most common types of encryption available are the older and less secure WEP (Wired Equivalent Privacy), and the newer and more secure WPA2 (Wi-Fi Protected Access). Vista supports both forms of encryption, but XP generally only supports the older and less secure WEP. In setting up the encryption the user will initially be required to create a passphrase used to create the encryption key. Never use a default key if it is offered, and never use easy to guess phrases, words, family names, phone numbers, or other readily determinable passphrases. Instead, be sure to use a combination of random appearing upper and lower case letters and numbers, which will be harder for a hacker to crack. Security experts recommend that the encryption key and passphrase be changed on a regular basis, often every month or two. When the passphrases are changed, the keys on any computers connected the wireless router must also be changed or they will lose their access.

Wireless connectivity is a great convenience, and I use it frequently both at home and when traveling. Just be very careful when using wireless wherever you are.
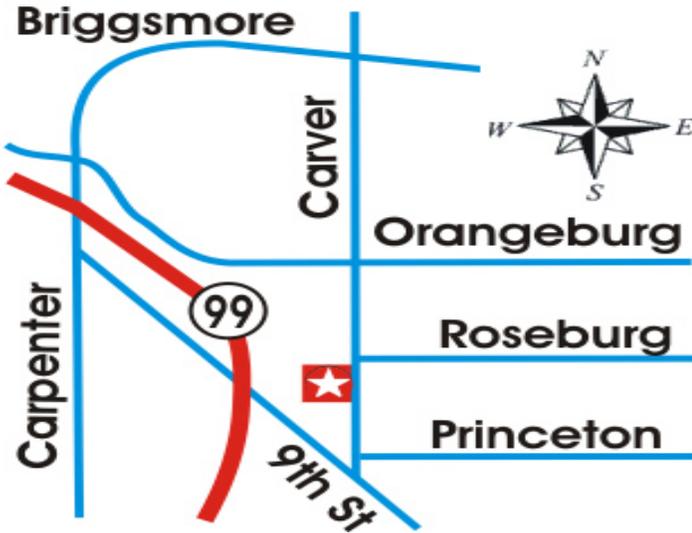
This article has been provided to APCUG by the author solely for publication by APCUG member groups. All other uses require the permission of the author (see e-mail address above).

Special Interest Groups and Meetings

Meeting Name	Leaders	Phone	Date / Time / Note
Beginners' SIG ………..	Jim Goodman ……..	579-0122	6:30 p.m. 1st Tuesday, Denny's 1525 McHenry Ave.
Board Meeting ……...…	Mike Kumler ………	531-2262 ………….	7 p.m., 1st Wed. of the month.
Random Access Q&A ………………………………….............…..……			6:30 p.m. before general meeting

The Club's Meeting Place

Our general meeting and the Random Access Special Interest Group are held at the Destiny Christian Center, 1161 Carver Road on the west side of Carver across from Sam's Food City. Parking is available both in front of and behind the Center. No parking along side of the Center, please.

Free classifieds for members. Email the text to the editor at editor@mpcug.net

Be sure and check our web site at least once a week at www.mpcug.net

Modesto PC User Group Officers

President ....Mike Kumler ....531-2262 .... president@mpcug.net
Program VP......................Elizabeth Leedom ....523-4218 .... programvp@mpcug.net
Secretary..........................Terry Fix........................524-8062 .... secretary@mpcug.net
Treasurer.........................Barbara Cameron.........522-1389 .... treasurer@mpcug.net
Director At Large ....John Selover ....

Appointed positions:

SIG Coordinator ....Jim Goodman.................579-0122 .... sig@mpcug.net
Press Relations ....Elizabeth Leedom ....523-4218 ....programvp@mpcug.net
Membership......................Hank Mudge...................529-1936 ....membership@mpcug.net
Web Master ....Jim Goodman.................579-0122 ....webmaster@mpcug.net
Editor ....Claude Delphia..............892-5037 ....

PC Post

Editors: Claude Delphia (MPCUG) and Judy Taylour (APCUG)

Editor Emeritus: William "Doc" Holloway — 1920 -1996
President Emeritus Bud Bondietti — 1950-2008
Claude Delphia, Editor Emeritus
Elizabeth Leedom, President Emeritus

Join The Modesto PC User Group

Web site: www.mpcug.net

To join MPCUG (or just get more information about us go to our Web site and fill out the new member form or mail your check to: MPCUG, P.O. Box 5122, Modesto, CA 95352-5122.Membership is just $24 a year and includes 12 issues of the PC Post along with participation in all meetings and events. You will also receive e-mail advising you of extra events or news.

The PC Post and Editorial Policy

The PC Post is published online 12 times per year and is available to all group members as a membership benefit. Annual group membership dues are $24.00.

For information write: Modesto PCUG PO Box 5122, Modesto, CA 95352-5122

Opinions expressed in the PC Post do not necessarily reflect the opinions or views of the members as a group or the Board of Directors.

The PC Post encourages group members to submit articles for publication. We would like to have articles which deal with the writer's experience with computer hardware and software or digital photography.

An article may deal with any computer-related subject provided it contains no libelous or offensive material. We can't use information copied from other publications without written permission except for quotes.

Articles should be submitted in MS Word text. Do not spend time formatting your article such as indents or centering. Please use only one space between sentences. and do not use bold, italicize or otherwise format the submission as we can't guarantee results in translation to Publisher. Proof read and run your spelling checker. Watch for special upper and lower case in brand names. Do not tab or indent to layout text.

If you want to include a graphic, please contact the editor for instructions.

We reserve the right to edit articles, for length or to improve readability. Longer articles may be published in several parts. We will not knowingly promote unlicensed businesses.

Letters to the editor are encouraged. All articles and letters to the editor should be submitted to the editor via email as an attached file. Call him at (209) 892-5037 before submission. Please include your name, day and evening phone numbers, and email address for contact.