PC Post

Official Newsletter of the
Modesto PC User Group.
Modesto, California

30 YEARS OF USER HELPING USER
December 2013, Volume 31.12

Inside this Issue

The group meets at 6:30 p.m. at Denny's Restaurant, 1525 McHenry Ave., for its Random Access Special Interest Group featuring questions and problems members are facing. At 7:30, following dinner, the presentation will start.

BOD Meeting – January XX, 7pm at Ridgeway's

Mavericks, Typhoid Terry and avast!

MPCUG President Is this the real Terry Fix? Alias--"Typhoid Terry"

Kirk Stockham has given Terry a new nickname--"Typhoid Terry!" Why! Because Mac Users have been rather "smug" about Windows being always "infected" by computer viruses--while Macs were not having these problems!

Not anymore--avast! has detected viruses--and especially Trojans on Terry's iMac!

Kirk suggested---"you have a presentation topic brewing....My Apple Computer Is Not Immune."

This is what the December program is all about--how avast! protects and scans for Trojans, Malware, etc. www.avast.com/free-antivirus-mac

Plus--an added feature--a quick look at the new FREE Mac operating system

www.compukiss.com
sandy@compukiss.com

The Affordable Care Website from a Programmer's Perspective

We have heard the word "glitch" over and over again in reference to the government's new health care website, Healthcare.gov. As a person who has personally coded thousands of lines of code and run several websites, I can assure you that what we are seeing with this website is not a bunch of small glitches. It is as fundamental failure. Read on for my take on it all.

How did we get here? First of all, with any web project, especially one as large as this, clarity of purpose is essential. The first thing you do in such a project is to decide definitive objectives and plot out a program of how to get to those desired results.

At 1900 pages, the size of H.R. 3962, the Affordable Health Care for America Act, is overwhelming. It crashed my computer several times before I was able to download the PDF. Add that to the fact that no one in Washington knew exactly what it contained when it was passed and you can understand why there was no clarity of purpose in developing the website.

Also consider the fact that outdated procurement and bidding processes for governmental work have become so overwhelming that only those companies who know how to manipulate the system can be successful in gaining these government contracts. The people who get the contracts are not necessarily the best and the brightest, but rather, those who can play the political game the best.

So we wound up with several contractors, led by CGI – the largest tech company in Canada. Although I have nothing against Canadians, it seems to me that something that we Americans will rely on so heavily would be better served by an American company. After all, we still have a very high standing in the technology world. What ever happen to "Made in the USA?"

And, as you know, cost overruns are rampant. The initial CGI contract was awarded at $93.7 million and their work has already raised the bill to almost $300 million. Would Apple, Amazon, or others allow such outrageous cost overruns when such lack of results have been shown?

I would like to also take a moment here to suggest that the US government be honest with the American people. When I look at the statistics for my CompuKISS.com website, I can tell

you exactly how many visitors we've had, where they are located, how many signup up for each form, what browsers they are using and a wealth of other information. Anyone who deals with websites knows these statistics are available. So for them not be able to tell us how many people have signed up is simply more political posturing. This is not a Republican or a Democratic issue. It is a political issue. Didn't we learn from Watergate that the cover up is usually worse than the original act?

And, unfortunately, it is obvious in this case that politics have driven the technology rather than the technology being driven by the customer. The user interface is terrible. A wealth of problems seem to have occurred because the government insisted on customer verification against IRS rolls instead of simply allowing the user to see the programs and costs before they signed in with personal information. While I can't be sure without actually seeing the code, I suspect that other last minute changes and political posturing also led to many of the current problems.

With everyone asking if, and when this can be fixed, I will add my take as an "old programmer" who worked on several large financial team programs and who also worked to make sure that several banks were ready for Y2K. As a programmer, I can tell you that finding all the "glitches" in 5 billion lines of code is not an easy job. And translating the data to be able to communicate with state agencies as well as hundreds of insurance companies is a monumental job. Add that to the fact that hardware issues, server capacity, load balancing, and other highly technical issues have to be taken into consideration.

While some modules of code for this new website may be able to be rescued and reused, the best situation is to start over again with a plain clear plan and no political maneuvering.

There is one main reason that I suggest this. A nest of system problems like those found in this website, ALWAYS translates into security issues. Poor programming leaves loopholes that hackers can expedite to perpetrate identity fraud, phishing, and other vicious plots. Bogus websites with names similar to healthcare.gov have already popped up ready to steal your personal information as you enter it.

Anti-virus software maker Trend Micro also reports that hackers and scammers are also already trying to capitalize on the health care confusion because you can not only sign up at healthcare.gov, but also at several state and third-party sites. They write, "When a person starts looking through sites to find one, at this time, they're faced with the challenge that there's no official marking or labeling that they can look at on a site to know that it's an officially sanctioned site …a survey of state and third-party sites also shows that official sites aren't required to provide the ability to verify the site using SSL (a security verification system): many of them don't provide it for site verification at all, though the Federal site does." It seems that many things were overlooked when this system was created and at least some of those will also cause security problems for end users.

With this new health care system, we are trusting the government with much of our personal and private information. Patching the current system is almost certain to be tried for political expediency. Making it useable may solve the immediate problems, but is sure to cause security problems in the future. This point not being made in most of the media, although for me, it is a major concern. And it should be for you, as well.

Phishing (Identity Theft) Now Considered as the #1 Web Threat
iwilsker@sbcglobal.net

Ira is a member of the Golden Triangle PC Club, an Assoc. Professor at Lamar Institute of Technology, and hosts a weekly radio talk show on computer topics on KLVI News Talk AM560. He also writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.

In several past columns, I have warned readers about the various methods and techniques that cyber crooks use in order to steal their identities. According to Wikipedia (en.wikipedia.org/wiki/Phishing), "Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication." While phishing has been around for several years, it has now become the major method of online identity theft; according to the cyber security service Webroot, "Phishing 2.0" (the latest iteration of this type of phishing) is currently the #1 web threat facing computer users.

In the past, it was thought that only inexperienced and unknowing computer users were

vulnerable to the original "Phishing 1.0" level of phishing attacks, as these unfortunate users would blindly click on any links in an email, and give personal and credit card information to all who asked. In order to protect these highly vulnerable individuals, as well as other more experienced users, the computing industry has upgraded web browsers and security software with the capability to detect most phishing attempts, and alert the user of the risk, or otherwise stop the phishing attempt in its tracks. Not to be impeded by the security improvements incorporated into newer browsers and security suites, and losing a major source of substantial but illicit revenue, the cyber crooks who profit handsomely by stealing the identities of others have created new and improved Phishing methods referred to by the security industry as "Phishing 2.0." According to Webroot, in discussing Phishing 2.0, "(Phishing 2.0 is) ... a new generation of sophisticated phishing attacks now target(ing) businesses. These phish evade traditional antivirus and anti-phishing products. Using targeted information - often gathered from social media sites - they fool even security-savvy employees into divulging sensitive information or visiting websites that infect machines with dangerous malware."

One very recent example of such a phishing expedition has been the recent deluge of emails directed against the faculty and staff of Lamar University, simultaneously directed at both their official ".edu" email addresses and their private email addresses. These multiple emails addressed to many of the employees are an apparent attempt to eventually bypass the security systems that are already in place; it does not really matter how good the university or corporate firewall or protective software, as many of the employees are also receiving redundant Phishing 2.0 emails at home, where the security may be likely to be weaker (or

non-existent) than the professional security systems employed by the organizations. While the sophistication of the Phishing 2.0 attacks are intended to penetrate most common security methods, the simpler Phishing 1.0 still can wreak havoc on individuals and their employers.

Over the past few days, I have been made aware of multiple university employees, as well as employees of some of the other nearby colleges, receiving the following email at both their work and home email accounts; this email arrived numerous times over a two-day period at my home and work email addresses, as well as many of my acquaintances, both Lamar University faculty and staff and the faculty and staff of the other local lower division colleges:

From: Lamar Help Desk <helpdisk@lamar.edu>
To: Recipients <helpdisk@lamar.edu>
Sent: Thursday, November 21, 2013 2:20 AM
Subject: Mailbox Re-Validation

Your Lamar Password will expire in two (2) Days, click the link below to validate your e-mail
http://lamar(xxxxxxx).eu.pn/login.php

Thanks
Lamar Help Desk

Knowing that a percentage of recipients will always click on email links, it is inevitable that some users will be duped into doing that. At first glance, this email appears to be legitimate, unless the targeted victim looks closer at it. The item that attracted my primary attention is that I do not have a "lamar.edu" email address, as I teach at one of the other local colleges, but my wife, who does have a "lamar.edu" email address also received multiple copies of this Phishing email; I had also received inquiries for other college faculty and staff who received this email.

While the simple header on this email appears to indicate that it is from the "Lamar Help Desk", notice that the word "helpdisk" is misspelled, with the suffix being "disk" rather than the correct "desk". The web link included in the email would also raise suspicion as to the real destination of the reply. While the beginning of the web address (URL) clearly says "lamar", there is a three word suffix (which I purposely redacted) creating a compound word after the prefix "lamar". Generally, the abbreviation ".eu" might indicate Europe, but this website actually has an upper level domain of ".pn" indicating that it is registered in the Pitcairn Islands. For those who may recognize the Pitcairn Islands in a historical context, this southern hemisphere, western Pacific islands are the home of the descendants of the mutineers of the famous British ship "The Bounty". I really do not see a Texas university having a major help desk located there. Examining the full headers of the phishing email, it appears to have originated on a server at the University of California - San Diego (UCSD), and been questioned by an IronPort spam filter, but still was delivered to many of its intended recipients. Many of these phishing emails also were not stopped by the generally very good spam filters utilized by several of the popular webmail providers, such as Gmail and Yahoo mail. It is possible that a hijacked account at UCSD was "milked" for information, providing the cyber crook with a list of attractive target ".edu" domains; it is also quite possible that the

hijacked account at UCSD became a "zombie", unknowingly sending out spam emails at the request of a "Zombie Master" who may control thousands of compromised computers.

I also performed a basic digital trace of the link on the email, and found that the server that it is using is actually located in Kiel, Schleswig-Holstein, Germany. The registered owner of the server has a Russian sounding name, probably a pseudonym. Only generic information about the webhost was available, rather than the more common detailed contact information (also often bogus) of the actual website owner.

Using a "sandbox" on my computer (a virtual machine where nothing can get out and threaten my home computer), I tried to access the phishers' website, but was blocked by my memory resident security suite; even though I was likely safe, I decided not to continue to load the bogus website. Based on prior experience, the website would likely appear to be a legitimate Lamar University website where users would be asked to enter their username, old password, and new password. Since this is a bogus website, the new password would likely not be implemented, but either of two events will be likely to occur, both leading to the same nefarious results. The cyber crooks could either use the current username and password entered by the victim, or can change the password to one unknown to the legitimate user, preventing his access to any Lamar University system. This username and password is the necessary first step to logon to any computer at the university, allowing for email access as well as access to other data components at the university. Since the cyber crook now has an apparently legitimate Lamar University username and password, the email system now becomes available to the crook, as well as access to any accessible network drives. The amount of valuable data that can be stolen is immeasurable. The entire email history of the individual can now be downloaded, giving the crook information about students, family, and any other content, including passwords to external web services. It would be quick and easy for the crook to determine external web accounts that are connected to the now stolen Lamar.edu email accounts, go to those websites, click on the "forgot password" links, and have the external password or a reset link sent to the purloined email box. Not just would this

process continue until the legitimate user contacts the real helpdesk and resets his password, but the identity theft will likely continue, until the legitimate user also changes any other external passwords linked to that compromised account.

This might just seem like a local issue, but Lamar, like most other universities, has faculty and staff engaged in research, such that the theft of the research (intellectual property theft) could result in financial loss, loss of a competitive advantage, and even a threat to national security, all because an employee clicked on an email link and thought that he was resetting an expiring password.

If anyone has ever clicked on this or the millions of similar emails asking for passwords, usernames, or credit card number confirmation, or responded to phone calls or text messages informing the victim that his debit card number and PIN needs to be confirmed in order to reactivate the card, that person is likely to be the victim of identity theft.

While Phishing 2.0 is primarily intended to steal information from businesses and other organizations, the crude technology of the archaic, simple, but still effective Phishing 1.0 will still snare plenty of prey. In addition to the immediate changing of passwords (after scanning and removing any malware that may have been planted by the cyber crooks), it will likely be necessary to change other passwords, check credit bureau reports (totally free from annualcreditreport.com) and challenge any questionable postings. Complete information on dealing with identity theft can be found on the Federal Trade Commission website at www.consumer.ftc.gov/features/feature-0014-identity-theft.

Play it safe; be suspicious, adopt a policy of never clicking on links in emails, social networking sites, or instant messages (text messages). If, for example, you get an email apparently from your bank or a major retailer asking you to click on a link to verify information or sign up for something, do not perform that task by clicking on the link, but instead going directly to the known website of the source.

Be careful of what you click on; the results may be devastating.

WEBSITES and SOURCES:

http://hosteddocs.ittoolbox.com/Phishing_and_Web_Security-WP_Mar13.pdf
http://resources.idgenterprise.com/original/AST-0102181_EECDatasheet_from_KnowBe4.pdf
https://e.wikipedia.org/wiki/Phishing
http://www.consumer.ftc.gov/features/feature-0014-identity-theft\
htts://www.annualcreditreport.com

Interesting Internet Finds - October
By Steve Costello, President / Editor,
Boca Raton Computer Society, FL
October 2013 issue, Boca Bits
www.sefcug.com / president (at) brcs.org

In the course of going through the more than 200 news feeds, I often run across things that I think might be of interest to other user group members.

The following are some items I found interesting during the month of October 2013.

How risky will it be to keep running Windows XP?
http://askleo.com/how-risky-will-it-be-to-keep-running-windows-xp/

POP vs. IMAP: What Do They Mean and Which One Should You Use?
http://www.ilovefreesoftware.com/31/windows/pop-vs-imap.html

Talk to your Navigating Device: Android or iPhone
http://geeksontour.tv/2013/08/talk-to-your-navigating-device-android-or-iphone/

Can You Really Be Anonymous Online?
http://www.makeuseof.com/tag/can-you-really-be-anonymous-online/

Why You Don't Need an Outbound Firewall On Your Laptop or Desktop PC
http://www.howtogeek.com/172349/why-you-dont-need-an-outbound-firewall-on-your-laptop-or-desktop-pc/

How To Use the New Google+ Photo Editing Tools
http://www.groovypost.com/howto/google-plus-photo-editing-tools/

Where to Donate Your Used Tech
http://www.wonderoftech.com/where-to-donate-your-used-tech/

How to Keep Your Internet Usage Private [INFOGRAPHIC]
http://socialmediatoday.com/socialbarrel/1765451/online-privacy-how-keep-your-internet-usage-private-infographic

How to View and Work on Google Drive Files When You're Offline
http://www.guidingtech.com/24186/google-drive-offline/

****
Most Fridays, more interesting finds will be posted on the Computers, Technology, and User Groups Blog: http://ctublog.sefcug.com/

The Tip Corner
By Bill Sheff, Novice SIG Coordinator
November 2013 issue, The LVCG Journal
www.lvcg.org / nsheff (at) aol.com

lvcg Lehigh Valley Computer Group

Buying a Computer
Some of us are considering purchasing a computer either as a gift or for ourselves. So usually one of the first questions is: which PC brand is best? Some swear by a particular brand, and there is probably an equal amount swearing at it. Let's consider the fact that every PC consists of different parts, even within the same brand or model. So let's look at what we should be considering in the purchase of a new computer. (For the purpose of this discussion I am leaving the choice of PC or Apple to the reader. Much can be said for either choice.)

Value! Before we decide on a price range we should consider what we want in a computer and then we can compare prices among various brands that are providing the same items within the "box."

So first off, do we want a Laptop or Desktop?
This used to be a simple choice. Laptops offered mobility, but sacrificed a lot of performance.

Today many laptops, while sometimes being slightly slower than similarly priced desktops, offer more than enough performance for more than just everyday tasks. With a desktop you can always add additional cards, but outside of an ability to increase memory there are not too many add-ons for a laptop. If you decide that you want the portability and convenience of a laptop, it should have a good screen since it is not easily replaceable. And while you are at it, consider what size screen fits your need. Today, not only can you get very large monitors, you can also get monitors that are touch sensitive (like a cell phone). Additionally, today's memory should be between four to eight GB depending upon how much graphic editing you plan to do, but you do not need any ram over 16 GB.

The increase in speed over 8GB is negligible. For normal use four GB of ram should be sufficient to handle most programs including the threshold needed for the operating system.

OK! Let's look further under the hood.
On a PC you should have a 400 Watt power supply to cover any additional cards you might require.

Laptops provide sufficient wattage. Today's hard drives are usually 7200 RPM so do not settle for the older 5400 RPM models. Most DVD drives have been upgraded to read Blu-ray, but you don't want to have to pay extra to be able to record Blu-ray. Also, do you want or need a light scribe disk burner to be able to print labels on the special light scribe disks?

Today's processors have greatly improved. Look for the Intel I3 (or higher) or an AMD A6 (or higher). I would suggest you do not use the older Celeron, Pentium or AMD E or X2 series.

Ports. I can only suggest you cannot have too many ports. A minimum of four to six USB2 ports should be the minimum. Also see if there is a firewire port and for sure an HDMI port for video transfer.

Most laptops provide a pcmcia card slot which allows adding many useful options. Also both usually have slots to slide in memory sticks.

Motherboards. Almost all motherboards offer video and audio on the board. I have found that except for gaming where you need higher speed graphics the on board audio and video are quite sufficient.

Warranty & Support
Pay careful attention to the warranty and support policies, because they are getting more complicated than ever. Many companies offer various levels of in-home, mail-in or even local repair.

If your warranty is “mail-in after 90 days for a period of 1 year,” it means if anything goes wrong hardware-wise, you’ll need to mail the computer in. You may wait up to two weeks to get it back.

Buying from a local computer shop can often result in faster service and better component choices (to reduce service costs), but may cost you a bit more initially. Since most computers work pretty problem-free after a brief burn-in period; there are some who suggest that additional warranties are not price effective.

Finally, while not readily apparent, tech support from the various brands should be a consideration when choosing a brand.

Reinstall your operating system
When you purchase a new computer you normally do not get any restore disks to reinstall the hard drive to its original condition in case of a virus or failure. Sometimes they suggest you make a copy of the restore disks and keep them safe. Often they suggest you can restore directly from the partition “D” drive for Vista or Win 7. The “D” drive is a “restore partition” which holds the recovery programs. This partition costs less to make than it does to manufacture restore discs. This is good if you cannot locate the restore disks at a crucial time.

If you feel you want to restore from a restore partition, and you can, back up your computer, at least all the files and data you want to save. You probably could do a “non-destructive” restore that will allow you to keep all of your files intact, but it’s always better to be safe than sorry.

All HPs and Dells manufactured within the past five years include them, as do most other computers these days. You can check for the restore partition by clicking START and then COMPUTER. What you’re looking for is labeled “restore” or “recovery”.

Next, click START and then enter “recovery” into the search box. Click on RECOVERY MANAGER.

When you run the recovery manager, you'll see a screen with various options.

If your problem is that one of the original programs that came with your computer has become corrupt, you use SOFTWARE PROGRAM REINSTALLATION. MICROSOFT SYSTEM RESTORE will close the recovery manager and launch Microsoft's system restore program to fix broken Windows. The final option here is REALLY the final option. SYSTEM RECOVERY is for when your system has become hopelessly corrupt and you need to start from scratch.

COMPUTER CHECKUP will check your system for errors and problems. If you're not sure what's wrong, this might be a good place to start.

RECOVERY MEDIA CREATION allows you to make the external disks you should have made when you turned your computer on for the first time. These disks are in case there was a total hard disk failure. You can take out the damaged drive and put in a new one and reinstall the programs.

Try and make those disks before the total hard disk failure. Once you have those disks made put them where they won't be lost or forgotten. Also on the screen mentioned above is a RECOVER REPORT which is pretty self-explanatory. Finally there is a REMOVE RESTORE PARTITION option on the screen.

Once you have restored your operating program be prepared to wait while all the updates get installed.

What Do I Do With a Flash Drive?
I really didn't know if I had to put in a tip like this, but once in a while we have to go back to basics just in case there are a few of us out there who are newbies, or just confused.

A USB flash drive is sometimes called a jump drive or memory stick. (A thumb drive is slightly different because they have a write-protect feature). In either case the drive is simply a data storage device just like a floppy disk, or even a hard drive. Unlike a hard drive it has no moving parts. It draws power from the USB port on your computer. There are other USB drives that are actually spinning hard drives and sometimes include external power plugs. USB ports can be located in the front or back or even both on a desktop, and usually on the sides of a laptop or all-in-one.

Once you put the drive into the port, the computer will recognize it as a removable drive and assign it a drive letter.

Now you can copy or move items to the drive, the way you would copy to a floppy or transfer to another file or folder. You can add new folders to the drive and do practically any other action that you can do with a regular drive.

It is a good idea to click the Safely Remove Hardware and Eject Media icon in your system tray to avoid any possible loss of data. This is not too important with the solid state flash drives, but is important with any USB drives that are spinning.

Besides having the ability to hold a lot of data, USB drives can also be used for creating a bootable USB drive and even putting many apps on it to keep some data from having to be installed on your computer.

I/O, I/O, It's Off to Work We Go

By Phil Sorrentino, Past President, Sarasota PCUG, FL
November 2013 issue, PC Monitor
www.spcug.org / philsorr (at) yahoo.com

The work I'm talking about here is computer data transfer. I/O or Input/Output is a term used to collect all the ways you can move data into and/or out of a computer. (This may be a review for some, but there are a few new ideas that might make it worth the time.) For all of those that have been with computers from the beginning, circa 1980, the only way into or out of your computer, then, was through the serial and parallel ports (the keyboard, mouse, and display interfaces were really internal and were only used for their intended purposes). Fortunately, the serial and parallel interfaces have been replaced with interfaces that are much faster and much more flexible and easier to use. Today, most of the I/O is conducted over the Universal Serial Bus (USB) interface. However, there are a few special purpose interfaces that have become basic to computer use.

Early on, audio was included in the computers bag of tricks so we now typically have an audio-in for a microphone and an audio-out for speakers. Many computers also have another audio-in, usually tagged as line-in. Audio-out is typically used to drive external speakers and line-in is typically used to input a stereo analog signal for use by audio processing software. Also added early on was an Ethernet connection which has become the computers on-ramp to the Internet. Yes, and Wi-Fi (Wireless-Fidelity) has certainly become the mechanism for all, laptops, netbooks, tablets, and smartphones to get on to the Internet. Wi-Fi is a wireless I/O and therefore needs no connectors or wires. It is all accomplished by the transmitter and receiver hardware and software, within the computer. There are two other wireless interfaces, Bluetooth and NFC. Bluetooth is becoming very popular as a way to easily connect various Bluetooth compatible devices to the computer with no wires cluttering up the computer area. Bluetooth sets up a PAN (Personal Area Network) around the computer, usually within 10 meters. Bluetooth is also finding its way into many places like the living room entertainment center and the automobile. NFC (Near Field Communications) is a very short range (less than 4 inches) wireless interface that may or may not be used on a computer but will probably be used with smartphones to help make the electronic wallet possible in the future.

Not so early on, around the time laptops became portable, rather than luggable, a video display output port started to appear. This became the very popular VGA (Video Graphics Array) output port (a.k.a. the RGB port because it provided Red, Green, and Blue analog video signals). The VGA port was typically used with an external display device like a larger display or a projector. For a brief time, the DVI (Digital Video Interface) began to take over the job of moving digital video information from the computer to an external display device,

but it was soon overtaken by a more comprehensive and versatile interface. Today, the VGA and the DVI port, is being replaced by a digital multi-media port, the HDMI (High-Definition Multimedia Interface) port. The HDMI port carries both digital video and digital audio signals from the computer to a digital display device. (HDMI is also used in most new digital entertainment centers and digital televisions. Many new digital TVs even provide multiple HDMI input ports, so you can connect cable boxes and DVD players to the TV.) HDMI is also being used on small devices such as smartphones and camcorders and as such is being made available in mini and micro sizes.

So besides audio and video, most of the digital data that is transferred to and from the computer is done via the USB ports. Modern computers usually have multiple USB connectors (laptops maybe 2 to 4, and desktops may have 2 to many). The USB port is a rectangular plug that is keyed so you cannot plug the connector in incorrectly. The USB connector also provides a limited amount of power to the device connected to it, which can be used to charge a battery or even power the device. Because the USB connector provides power to the connecting device, many smartphones and media players charge their batteries through the USB connector. Currently USB is at version 3.0. (Early versions were 1.0 which was little used, 1.1 which was very popular but slow at only 12 Mbps, and 2.0 which was ubiquitous, and fast at up to 480 Mbps.) USB 3.0 devices began to appear in January 2010. USB 3.0 has a maximum data rate of 5 Gbps, yes that's 5 thousand Megabits per second. That is a maximum and most data transfers will probably not be near 5 Gbps, but they will be very fast. Fortunately, USB 3.0 is backward compatible with both 1.1 and 2.0. Backward compatibility means that devices at any USB version can operate together, although the data transfer will only be at the speed of the lowest USB version. USB 3.0 connectors usually have a blue center post to identify them as 3.0. Because USB is used on so many small devices, like smartphones and tablets, USB connectors come in Mini and Micro sizes. USB has become so fast and ubiquitous that it has just about eclipsed the other, almost popular, serial bus, IEEE1394 (a.k.a. FireWire).

There are a few other interfaces that may show up on a higher-end computer. These tend to be for special purposes or are extremely fast. One interface, for the purpose of connecting external hard drives, is eSATA (external Serial Advanced Technology Attachment). This interface is not as popular as it was before USB 3.0 became available, but it is still a way to extend the computer's hard drive capability. Thunderbolt is another special purpose interface, rarely seen on typical computers, with speeds up to 10 Gbps. Thunderbolt can connect multiple compatible devices in a daisy chained configuration. DisplayPort is another special purpose Video Display interface that is very fast, it is advertised at up to 21.6 Gbps, and is designed for multiple displays. These very fast interfaces may be found on professional Display systems that require resolution and refresh rates far beyond those of HDMI. This type of display may be found in medical systems that may be used to display MRI Scans or X-Rays. DisplayPort may be found on some high-end machines, maybe gaming machines and if resolutions beyond 1080p ever find their way to the home, you may find DisplayPort driving those display devices.

The job of moving digital data around is tough work, but these interfaces seem to be up to the job, and I'm sure the ones that will come in the future will probably be faster, more versatile and even more capable

From Ray Nichols

If you have items you would be willing to donate for our club drawings, they will be gratefully accepted. Be sure to wear your name badge for the drawing.

Please also remember to bring your used magazines, books, videos, DVD's, and cassettes for distribution to Veterans in our area. If you have old household or device batteries, or used CFL (Compact Fluorescent Lamp) bulbs, bring them for legal recycling (it is against the law to dispose of them in the trash). Old Cellphones can be converted to Telephone Calling Cards for overseas Military Personnel. Old eyeglasses will be turned over to the Lions Club for reissuing to needy

Modesto PC User Group Officers

President	Terry Fix	524.8062	president@mpcug.net
Program VP	Jack Selover	656.9555	programvp@mpcug.net
Secretary	Barbara Meyer	543.0233	secretary@mpcug.net
Treasurer	Barbara Cameron	522.1389	treasurer@mpcug.net
Director-at-Large	Bob Meyer	543.0233	dal@mpcug.net

Appointed Positions

Membership	Barbara Cameron	522.1389	membership@mpcug.net
	Barbara Meyer	543.0233	
Webmaster	Jim Goodman	579.0122	webmaster@mpcug.net
Editor	Judy Taylour	661.252.8852	scvjudy@usa.net
Contact to Editor	Jim Goodman	579.0122	webmaster@mpcug.net
		912.8456	

PC Post

Editor Emeritus: William “Doc” Holloway – 1920-1996
Editor Emeritus: Claude Delphia
President Emeritus: Bud Bondietti – 1950 - 2008

Join the Modesto PC User Group

To join MPCUG (or just get more information about us, go to our Website and fill out the new member form or mail your check to: MPCUG, PO Box 251, Empire, CA 95319. 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. Opinions expressed in 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 unformatted MS Word or RTF text. Proofread and run your spell checker; watch for special upper and lower case in brand names. If you want to include a graphic, please send it as a jpeg attached to the E-mail submitting your article. Please note in the article where the jpeg should be placed. 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 E-mail as an attached file (Word or rtf). Please include your name, day and evening phone numbers.