MOTHERBOARD

A Publication of the Computer Users Group Of Redding, CA

Volume 2016, Number 03 http://cugr.apcug.org/ March 2016

Like Us on Facebook Cugr Redding ComputerClub, FB Group CUGRmember

YOUR C.U.G.R. PRESENTS

4th Tuesday, March 22, 2016, 4 - 6 PM

Guest Speaker, Professional Photographer

Michael Sauer

He will be talking about “Google products, such as the calendar, mail, Google+, etc. Michael is a professional photographer here in Redding. His practical business experience with Google will be really helpful to all of us Google users. And there’s plenty of time to let me know before the meeting if there is something in particular about Google usage you would like to hear him talk about. - Jane Quinn

Door Prizes

1. Silicon Power USB 64 Gig Jump Drive!

2. Selfie Stick (Use with Multiple Devices!)

3. $15 Cash Envelope!

One free ticket to each member at the door!

4 pm Social & Business & 4:30 Presentation

Social time & club updates. 4:30 Presentation

Sign in at the Greeting Table and pick up your name tag and please leave it in the Tag Box when you leave. Also please stay and help reset the tables to the Library’s original arrangement.

April - Hewie Poplock in Florida Using Skype
May - Frank Tona for Photo Contests & Tips

CUGR Calendar

CUGR Board Meeting During General Club Meeting March 22, at Redding Library in the Community Meeting Room.

BEYOND BASICS
10 AM, Saturday, March 19, Weekly, Thur. 1-3 PM
Jane Quinn SIG Leader

Windows 7 and 10. Multi-Media prgs., Photo Editing, eMail, Cloud software, and Google prgs.

See back page for more SIG information

General Meetings Are at the Redding Library 1100 Parkview Ave, off Cypress in the Community Room. Official Website is http://cugr.apcug.org/

For more information call any Board member listed on Page 2.

In This Issue ...

PRESIDENT’S MESSAGE
Jane Quinn..........2
JANUARY & FEBRUARY MEETINGS
CUGR..........3
SUMMER & MOSQUITOS
USANews Online Media 4
IN MEMORY OF BOB RICE
Judi Ball 4
CROWN CAMERA PHOTO OVERLOAD TIPS
Frank Tona..........4
WINDOWS LAB - ADWARE
Phil Chenevert..........5
BITS AND PIECES
Rush Blodgett..........5
CREATE A SYSTEM BACKUP FILE
Bill Ball..........5
BEYOND BASICS SIG UPDATE
Jane Quinn..........6
CUGR CALENDAR MARCH - JULY
CUGR Business..........6
R’S RAMBLINGS
Marlene Robinson 7
HOW TO MANAGE PASSWORDS...
Mike Hancock 7
MORE SECURITY VULNERABILITIES...
Ira Wilsker..........9
WHAT IS AN EXPLOIT KIT?
Dave Palmer..........10

Club Information

Club Website: **http://cugr.apcug.org/**

Club Mentors & Sponsors

Members Volunteering To Help Members!

Fred Skill, 243-3557, Sfskill@shasta.com
New Users, Free Library PC Classes,.......
Spread Sheets...

Jane Quinn, 365-0825, qjquinn7427@gmail.com
MS Windows 7 & 8, Photo/Video Editing,.
Internet, Cloud Software, Google Apps.

Bill Ball, 275-4632, bcard9@charter.net
Hardware, Software, MS Windows XP & 7

Colly Lord, 224-1633, johnclord@charter.net
General PC Help After Work Hours.........

Judi Ball, 275-4632, jebed@charter.net
DTP, Graphic Prgs ....
Photo Editing ....

Board of Officers and Directors

Motherboard link: http://cugr.apcug.org/PDF/MB201601.pdf

Jane Quinn ....**President**
SIG Leader, Vendor, Dir.
qjquinn7427@gmail.com 365-0825

Ed Beaulac .... **Vice President**
Past President
edbeaulac@gmail.com............222-4654

Belva Sullivent..............**Past President**
belvas@charter.net 241-9926

Mario Quinn.......................... **Treasurer**
gaucho7427@msn.com 365-0825

Ginny Wall . Acting Secretary, Name Tag Manager, Dir.
Tootseylou@aol.com................547-5104

Jan Brockett............... Membership**, Dir.**
jbrockett444@yahoo.com..........246-4721

Judi Ball................................Editor, Dir.
jebed@charter.net....................275-4632

Bill Ball ....**Dir.,** Mentor
bcard9@charter.net..................275-4632

Lyle VanNorman ....**Dir.**
bbcreelmx@yahoo.com.............242-0925

Margaret Martinovich ....**Dir.**
mjmartin56@sbcglobal.net........241-6378

Colly Lord.......Website Manager, Mentor
johnclord@charter.net 224-1633

Jeanie Richardson Dir., Photographer
Jeanier1954@ATT.net 347-5839

Help For Refreshments

The club is providing cookies and coffee at our meetings, but. we need voluteers to pick up these items at the store on their way to the library. The club will pre-pay the person on duty for the following month.

Please see details, Column 1, Page 4.

Motherboard Newsletter Staff

Judith E. Ball................................**Editor**
jebed@charter.net.....................275-4632

Rush Blodget ....**Bits And Pieces**
rblodget2@yahoo.com 241-4754

Jane Quinn .... **Proof Reader**
qjquinn7427@gmail.com...........365-0825

Marlene Robinson ....**R's Ramblings**
mm-kids@att.net 242-2429

Motherboard Newsletter Policies and Deadlines

The *Motherboard* newsletter is published monthly by the Computer Users Group of Redding, PO Box 494778, Redding, CA 96049-4778. The CUG is a 501(c)(3) non-profit corporation. Subscriptions are included in the $25 annual membership fee. The purpose of the newsletter is to inform members of upcoming events and provide information about the use of IBM compatible computers.

Disclaimer: Neither the CUG, its Officers, the Editor, nor the newsletter contributors assume any liability for damages incurred due to the use of information provided in this publication.

Reprints: Articles from this newsletter may be reprinted by other user groups if credit is given to both the author, CUG and the *Motherboard*. Mail a copy of the newsletter where the article is reprinted to the Editor at the address in the first paragraph of this text.

Personal Ads For Members:
Requirements are:
1. Advertiser must be a member.
2. The item must be computer-related.
3. The ad must be received by editor J. Ball by the *monthly date of the board meeting.* Sorry, no exceptions.

Other terms must be approved by the club's Board of Officers and Directors.

Article Submissions: All articles and reviews must be submitted to J. Ball by the ***Monday of the monthly Board meeting*** *(see Page 1 for date.)* Sorry, no exceptions.

***Motherboard* Editor** reserves the right to make corrections and deletions in all articles in the interest of grammar, style, and space.

President's Message

It's your club. Your input is of value to it.

Thanks to all that stepped forward at the last meeting to add to the conversation about Windows 10. If you missed it, you didn't see Bill Ball's presentation on creating a system Backup file for Windows 10. And Fred Skill, along with Ed Beaulac contributed their experiences with Windows 10. I showed some Youtube videos on Windows 10 from the APCUG foundation we are affiliated with. You will find some good topics by this group on YouTube. Simply query APCUG on the YouTube site. Everyone did a great job presenting Windows 10.

This month our guest speaker is Michael Sauer. He will be talking about Google products, such as the calendar, mail, and Google+. Michael is a professional photographer here in Redding and his practical business experience with Google and photos will really be helpful to all of us Google users. Plenty of time for you to let me know before the meeting what you would like to hear him talk about.

Lyle VanNorman will be bringing the refreshments this month. April's meeting refreshments will be covered by Jolaynne Williams, and in May Jan Brockett has volunteered for this task. Thanks each one of you for helping!

We need more volunteers for this simple task, please consider doing this for one meeting in the future. It's not difficult, and we will help you carry in the refreshments from your parked car. Call me at 365-0825, or email me at qjquinn7427@gmail.com

This past week I have made contact with Hewie Poplock from Florida, via the APCUG group. He will be doing his presentation to our group through **SKYPE**. He was one of the presenters in last weekends APCUG Video streaming program. I hope to make this connection work for the April Meeting. I will keep you posted about that progress. In the meantime you will find his Facebook postings really informative, as well as his website http://www.hewie.net/blog/3.

This is just another of many opportunities for us to connect with fellow computer hobbyists across the nation. You can find the posting for his video for Windows File Explorer on our Facebook account.

Continued on Page 6

January & February Meetings

CUGR Board Members, 2016

Margaret Martinovich, Georgeann Moore, Jane Quinn.
Standing behind: Jan Brockett, Lyle Van Norman, Frd Skill, Ed Beaulac.
Not shown: Ginny Wall, Jeanie Richardson, Bill Ball, Judi Ball
No longer with us: Anna Lee Horton, Bob Rice, both long-time board members.

CUGR Board Members 2003

Lyle Van Norman, Judi Ball, Jane Quinn, Margot Lintendre, Bruce Roth
In Back; Eugenia Goodman, Paul Colligan, Mario Quinn
Not shown: Darold Wright.
No longer with us: Anna Lee , Horton, Bob Rice, Bruce Roth

Congratulations To Our Winners!

Jeanie Richardson won the WD 1-T. External Drive!

Bernice Bennett won a Flash/Jump Drive Pen!

Joe Adams won the $15 Cash Prize!

John Brooks won $15 Cash in February!

Welcome Renewals

Colly & Sharon Lord

Summer And Mosquitoes

Amazingly, spring and summer are around the corner already, with mosquitoes hatching soon and some will be carrying the West Nile Virus (WNV), which, according to the Centers for Disease Control and Prevention (CDC), 2012 was the deadliest year on record for WNV. So precaution is the name of the game and to help the public safeguard bites of mosquitoes, the National Pest Management Association (NPMA) offers the following "Mosquitoes: Fact or Fiction?" guide:

Scented and citronella candles will protect me from mosquitoes: Fiction!.

Some types of candles will reduce mosquito populations in the immediate vicinity but will not prevent mosquitoes from biting. Accordingly, when outdoors, it is important to always use an effective insect repellent.

All insect sprays are the same: Fiction! The CDC recommends using an insect repellent that contains DEET, picaridin

Continued on Page 11

Ticket Cage To A Good User

The ticket cage shown in Bob Rice's obituary article is being offered at no cost to anyone or organization that can make use of it. We have come to a point when it is no longer necessary for us to use. So please contact Judi or Bill Ball at 275-4632 if you are interested.

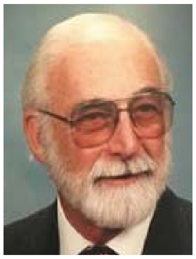
Necessary Newsletter Instructions:

Having an ad space for something you would like to sell, borrow, loan, give away, etc. will be available to all members. It does not have to be associated with computers.

The article about your item(s) must be in file (txt or doc) form sent to the editor via email, (nothing hardcopy will be accepted).

All pictures must be jpg format and enough resolution (180 - 200 dpi) to be seen clearly in the newsletter. No thumbnail pics.

It must be received by the editor no later than the first Monday of any month in order to be placed in the newsletter in time for that month's issue. jebed@charter.net.



In Memory Of
Bob Rice
8-18-1928 – 2-2-2016

Bob was born in Youngstown, Ohio and is the eldest of three sons. He is survived by his two brothers, his three children, five grandchildren, and two great-grandchildren.

Bob attended Happy Valley Baptist Church, and was an avid baseball fan, and very active in round dancing, ham radio, and the PC Club in the Redding area. Bob was a military veteran and served in the United States Marine Corps.

Bob was almost a charter member of our organization. He and Rush Bodgett hold the longest memberships, going back to the early 1990's. Bob played Santa many times over the years and the photo here is from 2009. He was a long-time board member also.

Bob built our ticket cage from scratch. Any similar cage would have cost quite a lot to buy at the time, so he volunteered at a board meeting to make it for us. It was well made and well used over the years when we needed it because of our much larger membership than now.

Bob's ashes were interred at the Northern California Veterans Cemetery (NCVC) with military honors.

Link to Bob's Wall Tribute and his photos and obituary by his family: (http://www.fremontchapeloftheroses.com/obituaries/Robert-Rice-15/)

CROWN CAMERA
TAKE YOUR BEST SHOT
EST.1957

Tips Sent To Motherboard By Crown Camera, Via Frank Tona.

How To Tame Your Photo Overload

Taking photos and videos have never been easier. But with this ease comes a new issue: What to do with all those images?

We completely understand. We're guilty of taking too many pictures too - but it's a good problem to have! Tame your photo overload with these quick tips:

1. Junk the bad images as soon as you take them. (You know you won't print, use or look at them later.)
2. Sync your devices with a cloud-based storage solution so your mobile images are automatically backed up.
3. Don't use a cloud storage? Upload your photos to your computer regularly. Sort them into folders and tag or save the very best ones in separate place.
4. Back 'em up pronto! Too many people procrastinate on making a copy of their photos until it's too late.
5. Have boxes of old prints and slides converted to digital format for less clutter and easier sharing with family and friends.
6. Share your favorites in person and on social media. Print and frame new pictures regularly, create custom photo books for family and friends, and make personalized image-inspired gifts. We admit, this is our favorite part too.

1365 Market St, Redding, CA 96001,
(530) 243-8333, (800) 655-4256

Windows Lab - Adware

Phil Chenevert, a CCCC member and instructor for Computer Lab Workshops, Cajun Clickers Computer Club, LA, March 2014 issue, Cajun Clickers Computer News www.clickers.org, ccnewsletter (at) cox.net

Definition

1 (Generically, adware spelled all lower case) is any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen. The justification for adware is that it helps recover programming development cost and helps to hold down the cost for the user.

Adware has been criticized because it usually includes code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge. This practice has been dubbed spyware and has prompted an outcry from computer security and privacy advocates, including the Electronic Privacy Information Center.

Noted privacy software expert Steve Gibson of Gibson Research explains: "Spyware is any software (that) employs a user's Internet connection in the background (the so-called 'backchannel') without their knowledge or explicit permission. Silent background use of an Internet 'backchannel' connection must be preceded by a complete and truthful disclosure of proposed backchannel usage, followed by the receipt of explicit, informed consent for such use. Any software communicating across the Internet absent of these elements is guilty of information theft and is properly and rightfully termed: Spyware."

A number of software applications, including Ad Aware and OptOut (by Gibson's company), are available as freeware to help computer users search for and remove suspected spyware programs.

The Chrome browser has a neat plug in called ABP that blocks almost all ads.

Bits And Pieces

by Rush Blodget; IMB/PCUG of Redding, rblodget2@yahoo.com

Please Read The Fine Print

I recently ordered a piece of computer hardware from a local store, which was on sale on Black Friday on the internet at a reduced price. After placing the order, I discovered that if I bought an additional inexpensive item I would get free shipping. I followed the initial order almost immediately with this second order. Inasmuch as shipping and handling was still part of the bill, a friend volunteered to pick my items up at the store. I paid for my order online, but was unable to have it picked up that day. Four days after my order was placed, I called the store to tell them that a different person would be picking up my order. At that time, they informed me that my order had been returned to stock the day before I called (three days was the limit to "hold" items even though paid for). I instructed them to reorder the items and I was assured upon asking that everything would be the same price — it turned out that the retail price not the Black Friday price is what I was charged — **so beware**.

Another strategy used by some of the major stores is to feature a popular item at a greatly reduced price. In the case that I was involved with, when I clicked on the item I was shifted to another item, not always relevant to what I wanted, and when I tried to go back to the original heavily discounted item it would be gone only to be found at the original retail price when the time for the discount had expired.

Why do I have to press one for English when you're just gonna transfer me to someone I can't understand anyway?

Create A System Backup File

Bill Ball, CUGR Member, bcard9@charter.net

At this moment with this version of Windows 10, this is how you can create a system image:

1. Open Control Panel and go to File History.
2. At the bottom of the left pane, you should see a link to System Image Backup, under "See also." Click this link.
3. The System Image Backup utility will open. Pick a place to save your system image backup (on a hard disk, on one or more DVDs, or on a network location), and click Next. Confirm your settings and click Start backup.

To use the system image to restore your PC that you have created:

1. Open the new Windows 10 Settings menu and go to Update & recovery.
2. Under Recovery, find the Advanced startup section and click Restart now. When your PC restarts, go to Troubleshoot, Advanced Options and choose System image recovery.

Create A Recovery Drive

A recovery drive can help you troubleshoot and fix problems with your PC, even if it won't start.

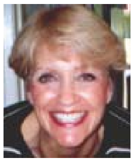
To create one, all you need is a USB drive that will hold all the files on your C Drive, plus one gig to allow for the recovery files. To see how much space you will need, go to your C Drive properties where the size of your C Drive is listed.

1. From the taskbar, search for "Create a recovery drive" and then select it. (You might be asked to enter your admin password or confirm your choice, if needed, but if you don't use an admin password this will not show up.)
2. When the tool opens, make sure "Back up system files to the recovery drive" is selected.
3. Then select Next.
4. Connect a USB drive to your PC.
5. After it is reconized by your PC, select it, and then select Next > Create. (A lot of files need to be copied to the recovery drive, so this might take a while.)

When it's done copying, you might see a "Delete the recovery partition from your PC link" on the final screen. If you want to free up drive space on your PC, select the link and then select Delete. If not, select Finish.

Beyond Basics SIG UpDate

by SIG Leader Jane Quinn, qjquinn7427@gmail.com



Thursdays, 1-3 pm, you’re invited to join us at the Senior Center in Anderson for a computer session in the classroom. For special projects I will give individual help at 3 pm. Contact me before to ensure I set aside time to devote to your project. *You can also connect to the classroom at high speed internet through SKYPE. ID is AAASCO2009.*

Our next monthly Multi-Media SIG is March 19. For directions contact me via e-mail above or phone, 365-0825.

How to Fix “Program has stopped

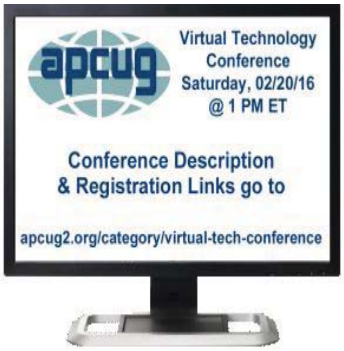
This past month I had a tragic event with my laptop. I couldn’t get any system related functions to work. It was something I know I triggered. Perhaps it was when I set the feature to stop using Edge as my default browser.

I searched the internet for answers to a non-working program. I found several answers, but here’s what worked.

Open Windows Explorer, in the search box type Action Center. Choose Programs> Program Compatibility Troubleshooter. It takes a few minute to build a list of your programs. I chose SYSTEM. Because that’s what I thought the problem stemmed from. You have to choose TEST THE PROGRAM in order to fix it. This may not work. At this point restart your computer. In my case, the Windows 10 returned.

Note: I will always try this method in the future for any program error issues.

APCUG Youtube Videos and VT Winter Conference 2016



apcug

Virtual Technology Conference Saturday, 02/20/16 @ 1 PM ET

Conference Description & Registration Links go to

apcug2.org/category/virtual-tech-conference

Saturday, a group of us watched a virtual conference together. For those who haven’t done a virtual conference I encourage you to try it the next free APCUG event. It is easy. Just respond to the invitation to register. Before the live conference, prepare you computer, tablet or iPad for the event. You will need to download the appropriate App for that device. The EventBrite web tool uses Zoom, the WEBINAR app that broadcasts the conference to you over the internet. You will need to create an Eventbrite account and then a password. You can use this account for any future Eventbrite live conferences.

Eventbrite is completely free. You create an event, similar to a Page in Facebook or Google+. Design your page, offer multiple ticket (free tickets also) options including reserved seating, and adding questions to get to know your attendees.

Send invitations and emails from your Eventbrite account. Let attendees spread the word with built-in sharing tools on your event page.

The latest APCUG conferences have been on East coast time. So we started watching Saturday at 10am. It went on for several hours. You’re not obligated to watch the whole program. We watched “Upgrading Your Laptop – by Greg Skalka”, — Utilizing iCloud on the iPad, by Sheila Bigel and I watched on my own Customizing Windows 10 —- Hewie Poplock (http://hewie.net/). I missed” The Gramps Project by Orv Beach”, which I later found out was about genealogy. That one I hope to catch when they post these videos to their APCUG YOUTUBE account later this month.

Watching Hewie Poplock demonstrate Windows 10 task view was so helpful. If you were one of those Users who had several monitors attached to your computer and jumped between them for different tasks, this is the concept in Windows 10. Assuming you don’t have the real estate for several monitors, you would use the Task View. Create as many desktops as you’d like. No need to minimize the windows when working on several tasks anymore.

The desktop’s become numbered when you create them starting from Desktop 1. You’ll discover that all desktops share the same Start Menu and Taskbar window. That program will remain open on Desktop 2. Jump between Desktops by clicking on the icon from the taskbar. Of course, you can still use the good old [Alt]+[Tab] task switcher to move between applications. If you select an application that’s on a different desktop, the desktop switch occurs along with the animated transition. The settings disappear when you shut down.

March Studies About Picasa

In March we will be studying how to handle our Photos with Google. And what to do about the existing Picasa photo albums we currently are using. Google is closing the Picasa program and replacing it with the Google Photos App.

PRESIDENT’S MESSAGE

Continued from Page 2

Our facebook name is “ComputerUsersGroupOfRedding”, and we can also be found at “CugrComputerClub” on Facebook, do not use the quotes in either address.

We have a Facebook group, “CUGR Members” where you can post information relevant to computing. Thanks to Jeannie Richardson, Lyle VanNorman, and Colly Lord for participating.

April’s Study On Facebook

Hewie Poplock, a board member from the APCUG organization, will be giving us a presentation using SKYPE to communicate with us from his Florida location. It will be our very first attempt to connect using streaming for our meeting. Should be exciting! Thanks **to all for your help and support** with the various positions and club chores.

Hope to see you there on March 22!

Jane Quinn

General CUGR 2015/ 2016 Meeting Schedule

Cut out and save.

4th Tuesday, March 22, 4-6pm
4th Tuesday, April 26, 4-6pm
4th Tuesday, May 24, 4-6pm
4th Tuesday, June 28, 4-6pm
3rd Tuesday, July 19, 4-6pm

R's Ramblings

Marlene Robinson, CUGR Member, mm-kids@att.net

A Walk Through History: An App By Shasta Historical Society

Are you looking for a spring outing? Then put your walking shoes on and use a QR app and an app from Shasta Historical Society (both downloaded to your smartphone) and take a walk through Redding's Historical Downtown area.

Bringing history to your fingertips is the tagline of the Shasta Historical Society's new project that lets anyone with a smartphone learn more about the stories behind local buildings.

The eight sites all located in or around downtown Redding, include Old City Hall, the Shasta Historical Society building, the Behrens-Eaton House, the Independent Order of Odd Fellows Reading Lodge, the Lorenz Hotel, Cascade Theatre, Bank of Shasta County, and the Diestelhorst Bridge. A sign featuring a QR code is placed at each location.

After downloading a QR code to your smartphone, go to the Shasta Historical Society website, which gives you a nugget of history in a short video from Historical Society member, Mike Grifantini. In the video he is in character talking about the sites as James McCormick, one of the founding partners of the McCormick-Saeltzer Store. This store, in the late 1880's, took up a block between Yuba and Placer streets at Market Street and was known as the "The Big Store." (Record Searchlight, 1/24/16, B1). Smartphone owners are able to read the QR, or quick response codes placed on the seven buildings and the Diestelhorst Bridge.

Recently the Historical Society conducted a guided walking tour. Those wishing to go on a tour can do so by visiting the locations and scanning the QR code with their smartphone, or by visiting shastahistorical.org. On the menu at the website, click on A Walk Through History. The site features a story map built by Far Nor Cal GIS. The project also received support from Viva Downtown.

"A Walk Through History" is a pilot project for the Historical Society, which hopes to have its members and others contribute to placing more QR codes at other historical points of interest throughout the area.

Call 243-3720 or visit shastahistorical.org for more information. (p. B4)

ENJOY YOUR SPRING WALK!

$$$ 50/50 Cash Raffle! $$$ This is The Next CUGR Drawing in July

The "50/50" stands for whatever cash is raised will be split between two ticket holders.

Tickets will sell for $5 each, or 3 tickets for $10. And you need not be present to win. So be certain that you print your **name and phone number** on the part of the ticket(s) that Jane will use for the drawing. And be sure to keep the stub for proof at time of drawing.

Tickets may be bought during all meetings up to time of drawing in July 2016, or during any of Jane Quinn's classes, or by mailing a check to Jane. If you mail the money to her, Jane will assign tickets and hold them for you until the drawing in July.

The next drawing will be at the Ice Cream Social in July, 2016.

qjquinn7427@gmail.com
phone: 365-0825

There are no door prizes during the July Social or December Party.

(By the way, the Quinns are not participating in the drawing.)

Good luck to all!

How To Manage Passwords And Use Dropbox

Meeting Review By Mike Hancock, Contributing Editor, Golden Gate Computer Society, June 2015 issue, GGCS Newsletter, www.ggcs.org, editor@ggcs.org

LastPass

GGCS guru Steve Shank told us that LastPass Password Manager is a powerful and flexible password manager that keeps your login information secure without your having to memorize all of it. You can automatically log in to any website once you have entered the username and password, once. This is achieved by setting up an account with your email address and a strong, complex master password that should be at least 12 characters long, and include upper and lower letters, numbers, and special characters.

All your passwords are encrypted "locally," that is, on your computer before the encrypted version is stored on your computer and is encrypted by a LastPass algorithm for every site you wish to access.

After creating your account, the LastPass download will appear as an add-on shortcut icon in your browser (LastPass works with all browsers). After you log in once with your Master Password, LastPass will then auto-fill all your passwords for you.

The plug-in also has a shortcut to your vault of existing passwords and can generate new, super secure passwords for new websites.

A mobile version, LastPass Premium, is available for $12/year. LastPass also allows you to save credit/debit card info, addresses, bank accounts, driver's license, and contact info. Having demonstrated LastPass, Steve also confirmed that it can handle certain multi-factor authentications that might apply to bank accounts, investment managers, etc., and even to your Master Password. It would be best to check with your facility to see if it's multi-factor service works with LastPass.

Finally, be warned that, if you forget your Master Password, you will not be able to recover your individual passwords, and LastPass cannot help you, because it doesn't keep your Master Password. So, it is essential that you be responsible for it.

LastPass does provide support, primarily through email. Your only fallback is to go to each website and use their method of password recovery, which can vary. Some sites may simply send you an email with a password reset. Others might require the answer to

Continued on Page 9

More Security Vulnerabilities Disclosed For Phones, Carriers

Ira Wilsker, Assoc. Professor, Lamar Institute of Technology; technology columnist for The Examiner newspaper www.theexaminer.com; deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.

If you are like me, I carry my cell phone everywhere, carrying on voice conversations, sending and receiving text messages, utilizing countless apps, and surfing the Web. Until recently, I gave very little heed to the security of these external communications as our smart devices are supposed to be somewhat secure. GSM carriers like AT&T and T-Mobile utilize encryption to make communications secure; CDMA carriers like Sprint and Verizon also claim to have secure networks. Yes, I do have a major security app on my Android phone that scans new apps and text messages for malware, as well as protects from hazardous websites. Google created Android to be secure, with apps running in a somewhat closed memory space, called by some a "sandbox," which is supposed to prevent purloined apps from talking over the phone. IPhone fanatics, along with many Apple fans in general, believe that their devices are immune to attack, as Apple would not dare to allow any threats to harm their beloved devices.

Now welcome to the world of stark reality. In a recent column, I wrote about two newly revealed vulnerabilities, known as "Stagefright" and "Certifigate," that may threaten the security, safety and privacy of nearly a billion smart phones and tablets. Since then, others have come forward demonstrating previously unannounced security vulnerabilities that threaten the security of our smart phones, often including both iPhones and Android devices in their threat assessments.

One of these newly disclosed threats explicitly targets the most technology innocent and uninformed among us. Appropriately called "grandma malware," this clever piece of malware sneaks onto Granny's phone using a compound method of infection designed to defeat many of the simplest security precautions. While recently updated Web browsers and desktop security software, as well as updated phone operating systems, have likely patched the vulnerabilities, Granny's often older and unpatched computer and phone may be vulnerable. The first step in the infection sequence occurs when the victim downloads an innocent looking app, often a game or simple photo utility, onto their computer using any one of the older versions of most of the common Internet browsers, which are still in wide use. This small utility, explicitly designed to appeal to a "grandma," does not itself contain any malware, and will pass the scrutiny of many of the less sophisticated desktop security products. This utility sits quietly and apparently innocently on the victim's computer, often performing its intended tasks. The app surreptitiously monitors Web surfing until Granny logs on to an app store, such as the Google Play Store. The malicious utility captures the logon and connection information from the app store; with this information, the malware is invisibly downloaded wirelessly to the smart device, installing itself on Granny's phone. Once installed, this malicious app immediately gathers personal data from the phone and sends it to parties unknown. Even if this malware is detected and removed in a subsequent security scan by a third party security utility, it is too late; all of the personal information was stolen within seconds of the app being installed on granny's phone. Granny's private information has just been stolen, and she might very well become an identity theft victim; as is common in criminal enterprises, the most vulnerable among us are more likely to be victimized.

Despite the travesty of purposely going after Granny, it is not one of the most insidious of the newly announced threats imperiling our smart phone usage. In recent days, a pair of IBM cyber security analysts, Or Peles and Roee Hay, uncovered a flaw in the Android operating system still being used in over a half-billion Android smart phones. This vulnerability, not yet formally named but referred to as a type of "masque" attack, could allow hackers to take over and remotely control vulnerable Android phones. According to these researchers, "Masque attacks are defined as malicious apps uploaded, say, from e-mails directing victims to fake Web links." According to Peles and Roee, Google has issued patches for devices running Android 5.1, 5.0, 4.4, and Android M, but as often the case for many Android devices (except some Nexus phones), it is up to the phone manufacturer or cell phone carrier to push these patches to their users, meaning that although the patches are available, over half of Android phones do not yet have the patches installed.

This "masque" attack vulnerability allows hackers to control the security privileges that are a part of the Android operating system, allowing compromised or counterfeit apps to access information on the phone that would otherwise be unavailable to the hacker. According to the researchers, this vulnerability allows the data thieves to steal personal information, capture banking information including logins and passwords, access the phone's cameras, download contact lists, and pilfer stored files and e-mails, sending the stolen information to a remote server. While this particular Android vulnerability was recently discovered by IBM cyber security experts, it is very similar to one discovered several months ago by FireEye that explicitly targets Apple's iPhones. The mechanism and modus operandi, as well as the data thefts, are almost identical between the Android and iPhone vulnerabilities.

A "masque" attack can occur when smart phone users download any of 11 authentic looking but counterfeit or contaminated apps that also appear to work properly when downloaded and installed. Among the most commonly downloaded iPhone and Android apps that enable this vulnerability are modified copies of Facebook, Twitter and WhatsApp. According to FireEye, iPhones are as vulnerable to these masque attacks as Android devices. According to Zhaofeng Chen, a senior research engineer

Continued on Page 9

HOW TO MANAGE PASSWORDS AND USE DROPBOX

Continued from Page 7

challenge questions. Perhaps your bank may require you to come into their branch in person.

Dropbox

Another GGCS guru, Marcelino Nogueiro, pointed out that, while many cloud storage programs, such as OneDrive, Google Drive, and Amazon Cloud Drive, exist, Dropbox has been around the longest, has the most users, and is the simplest of the cloud-based storage and file synchronization tools. This online storage service helps you share files between computers and mobile devices with the app installed. You can store and sync files by simply dragging and dropping them into the Dropbox shortcut icon on your desktop. These files are also available over the Internet using the Dropbox web interface.

You can share files (photos, for example) with others by creating a share file or folder. You can password-protect folders you share via email or if you share by sending a link the link is encrypted but anyone with the link can open the folder or file. Files are encrypted when you upload them and stay encrypted on the DropBox servers. Shared files are not encrypted after they are downloaded by the recipient.

When the DropBox program is installed and active, a green checkmarks appear on top of files and folder icon that have been synced and are up-to-date. By default, Dropbox syncs only files stored in a single, dedicated folder and subfolders. The default

Dropbox folder usually locates itself in C:\Users\(username)\MyDocuments\Dropbox.

Dropbox offers 2GB of storage free, which is not a lot compared with competitors, but this amount can be increased to 16GB by introducing friends to the service, at 500MB/friend. Paid personal plans, called Dropbox Pro, include 1TB of space for $9.99/m or $99/year.

For file collaboration, competing services, such as Google Drive, are better than Dropbox. It has applications for Windows, Mac, Linux, iPhone, iPad, Android, and Blackberry, and your files are available on any Internet-connected machine where Dropbox has been installed or has a web browser.

Once a folder or file has been synced, it is in Dropbox's cloud storage and can be deleted from your computer. Any time you use the Dropbox icon on your desktop, however, the files are also stored on your machine, so you haven't actually saved any storage space on the machine.

You can choose whether or not to sync automatically by turning off the instruction to sync in the Dropbox settings. A word of caution: if you have automatic sync turned on, files that you delete from the Dropbox folder on your computer will also be deleted from the Dropbox cloud storage.

If you only want to use Dropbox as a storage location in the cloud while being able to delete files from your local drive, do not use the sync feature; instead, use the Dropbox website to upload the files that you wish to store in the cloud.

MORE SECURITY VULNERABILITIES

Continued from Page 10

and scientist at FireEye, the 10 tainted apps that most threaten Apple devices are "WhatsApp, Twitter, Facebook, Facebook Messenger, Google Chrome, Blackberry Messenger, Skype, WeChat, Viber, Telegram and VK." These apps are often downloaded from genuine-appearing links in e-mails or SMS text messages, and mimic the functionality of the genuine app, but allow for the remote access to this valuable personal content. FireEye was quoted as stating that this iPhone vulnerability can steal or access a variety of information from compromised phones. Among the dastardly deeds that this masque vulnerability can perform include recording and forwarding phone calls placed on Skype, Wechat and other voice apps; intercept text and SMS messages from iMessage, WhatsApp, Facebook Messenger, Skype and other SMS apps; send real-time and historical GPS locations; access website histories; steal contact information and lists; and download photos from the phone. Apple has created patches and upgrades closing this vulnerability, and pushed these patches to many of its users, but there are inevitably iOS device users who have not received or installed these patches.

In recent days, on the Australian version of the "60 Minutes" news magazine, another cell phone vulnerability was demonstrated where hackers in Germany were easily able to listen in on a cell phone chat between individuals in Australia and the UK. This ability to readily capture live calls is known as the "SS7 Vulnerability." SS7 technology is widely used, legitimate and necessary for cell phone carriers to properly direct calls and text messages to their intended recipients. ComputerWeekly.com said, "Like any protocol, SS7 is vulnerable to exploitation by sophisticated and well-funded third parties with criminal intentions." In another ComputerWeekly.com story titled "Security flaw exposes billions of mobile phone users to eavesdropping," the online magazine says, "Hackers, fraudsters, rogue governments and unscrupulous commercial operators are exploiting flaws in the architecture of the mobile phone signaling system known as SS7. ... Billions of mobile phone users around the world are at risk from covert theft of data, interception of their voice calls and tracking of their location." SS7 is not a vulnerability in the phones themselves, as the vulnerability is not brand or operating system dependent, impacting Android, iPhone, Blackberry and other systems equally, but is in reality a vulnerability in the switching system utilized by the cell carriers themselves.

For those of us who routinely use Android, iOS or Blackberry devices without much thought about the inherent security vulnerabilities of the phones and cellular carriers, keep at least a spark of consideration in mind. While I am fully cognizant of the risks, I will continue to use my smart devices pretty much as I have in the past.

What Is An Exploit Kit?

Dave Palmer, Member, Tampa PC Users Group, FL, June 2015 issue, Bits of Blue, www.tpcug.org, dkp205 (at) hotmail.com

You may have heard the term 'exploit kit.' Maybe not. The term has become more prominent over the last decade as Internet crime has become more sophisticated. A few definitions will be helpful in explaining what an exploit kit is and how it's used.

A vulnerability is a weakness in a system that can be directly used by a hacker to gain access to a browser, a router, a system or a network. Vulnerabilities can result from mistakes in software, weak passwords or infected software. The vulnerabilities mentioned here are the software variety and require updates, patches, or fixes in order to prevent compromise by hackers or malware.

A zero-day vulnerability is a newly discovered vulnerability. It is completely unknown to the security community. It has not been recognized, analyzed or patched. Signature-based anti-virus software will not recognize it and cannot defend against it.

To take advantage of a specific vulnerability, hackers create software, called an exploit, specifically designed to take advantage it.

An exploit kit is a malicious software toolkit that automates the exploitation of browser and computer vulnerabilities for the purpose of spreading malware. I'm beginning to believe that 'toolkit' is too soft a term. 'Attack platform' is more accurate. The goal of an exploit kit is to automate the infection of computers or other systems.

Exploit Kit Basics

The earliest exploit kit was developed in Russia and was first seen in mid-2006. It was called WebAttacker, and it sold for $20 US and included tech support. Researchers and security analysts are currently tracking over 70 exploit kits around the world. Together they take advantage of more than 100 different vulnerabilities. While they can, and sometimes do take advantage of zero-day vulnerabilities, the vast majority of the time they attack vulnerabilities that have already been patched. Those computer users who are slow to patch their systems are therefore at highest risk.

Advantages Of Exploit Kits

Easy to use - Exploit kits are designed from the beginning to be easy to use. Their target market includes criminals with only low-level tech skills. They also provide a console or dashboard to help attackers track the performance of the infection campaign and provide information about the victims system. Did I mention tech support is included?

Flexible – Most exploit kits probe for multiple vulnerabilities. Their initial payload can include multiple exploits, or they may download exploits to match the victim’s vulnerabilities. Customers can often customize specific features to fit their business model such as ransomware, bank heists, botnet building, etc.

Evasive – Some exploit kits can probe for anti-virus programs and virtual machines. If found, these exploit kits may stop themselves from running to avoid being found and analyzed. Some exploit kits don’t write their payload to disk but run directly in the memory instead to prevent detection by anti-virus programs. They are called ‘file less infections.’ Exploit kits also use a number of other evasive techniques.

Continuously updated – Subscribers are continuously updated with the latest exploits against such software as Java, Adobe Flash Player, Adobe Reader, Microsoft Data Access Components (MDAC), and other programs and browser plug-ins.

Good Communications – Once an exploit kit is discovered and analyzed, authorities and security firms can usually block communication URLs (web addresses) within 24-48 hours. To counter this, authors of some exploit kits provide fresh communication URLs every hour plus an automated process to update the URL to stay one step ahead.

How An Exploit Attack Works

The hacker builds one or more websites that contain a 'landing page' and adds an exploit kit. To drive traffic to the exploit kit, the hacker has many options:

- Email spam - Spam campaigns using content such as warnings from the IRS, banks, and even police seem to work well. Fake alerts from legitimate companies that contain poisoned links are also popular. Unlike traditional phishing spam, the victim of these spam campaigns isn't taken to a look-alike site and asked for credentials. Instead they are directed towards a landing page that hosts an exploit kit.
- Purchased traffic – Underground markets have ‘traffic providers’ where traffic can be bought and sold.
- Compromised websites – When hackers compromise a website it's trivial to add a redirect. To slow down security analysts and authorities hackers typically add multiple redirects that change frequently.
- Malvertising – Malicious advertising is a relatively new and rapidly growing tool hackers have added to their arsenal. Hackers create fake companies and legitimate looking ads on existing online advertising systems to redirect victims toward exploit kits.
- Just prior to connecting to the exploit kit, potential victims are screened by automated traffic direction systems (TDS). Hackers can filter out unwanted IP addresses (like security companies) or target specific countries or companies.

Once a potential victim encounters the poisoned landing page, the kit quickly (in fractions of a second) analyzes the browser and its components to see what’s out of date. If there is a usable vulnerability, the correct exploit is loaded and executed. The hacker is then notified which exploit was used as well as the victim's country, operating system, browser and which piece of software on the victim's computer was exploited.

As a result, and without your knowledge, the hacker now owns your computer. Additional malware will be added to prepare it to become a vehicle for further crime. Just as smart street criminals don't use their own vehicles for street crimes, cybercriminals don't use their own computers for Internet crime. They will either use it to commit crimes or rent it out to other criminals as part of a botnet.

Exploit kits facilitate the addition of most other types of malware such as backdoors, droppers, banking Trojans, spyware, ransomware, botnet malware, scareware, keyloggers, rootkits, viruses, worms, adware, remote access tools, and ad fraud malware.

Earlier I mentioned that exploit kits could and probably should be considered attack

Continued on Page 11

CUGR
Membership Application

Name(s): ____
Address: ____
City:__________________________ State: _________ Zip: ______
Home Phone: _______________ Business Phone: ____________ __
E-mail Address: _________________________________ _____ _
Date: __________

$24
Dues Per Year.
$2 Dues Per Month
To be paid yearly in October.

□ New
□ Renewal
□ Cash
□ Check
Check #________

Be Sure To MAIL TO:
CUGR
444 Basalt Ct, Redding, CA 96003
(For general information call any Officer or Director listed on Page 2)

WHAT IS AN EXPLOIT KIT?

Continued from Page 10

platforms. A comparison could be made between exploit kits and unmanned military drones. Both carry sensors. Both carry weapons. Both can be programmed to operate with little or no human oversight. Both can be assigned a variety of missions.

Exploit kits are commercial products developed by teams of specialists. A recent example is the Blackhole exploit kit developed by Dmitry Fedotov (aka Paunch) and his team. Blackhole was one of the most notorious exploit kits of the last decade. Popular and quite profitable, it was first offered in 2010 and lasted through the arrest of the Paunch and 12 others in late 2013.

The Blackhole product itself and the service and management of the business was quite sophisticated and business-savvy. The scripts that made the software work were protected by a commercial coder to prevent other criminals from lifting & reusing the code. Blackhole was reported to have had thousands of customers and making $50,000 a month. Paunch was the first to use a ‘rental’ business model for exploit kits. Other licensing agreements were also available, all of which included tech support.

How To Protect Yourself

The standard excellent advice you've heard dozens of times before still applies. Run in Standard User Mode, NOT Administrative Mode. Stay patched & updated. Don't click on links in e-mail. And I'll add one item not typically mentioned: Configure your browser(s) to deny redirects without permission.

More Information

http://krebsonsecurity.com/2013/12/who-is-paunch/

https://www.trendmicro.com/cloud-content/us/pdfs/ security-intelligence/white-papers/wp-evolution-ofexploit-kits.pdf

https://blog.malwarebytes.org/intelligence/2013/02/ tools-of-the-trade-exploit-kits/

http://www.securityweek.com/black-hole-exploit-business-savvy-cyber-gang-driving-massive-wave-fraud

SUMMER AND MOSQUITOS

Continued from Page 6

or IR3535, and notes that "some oil of lemon eucalyptus and para-menthane-diol products provide longer-lasting protection." To ensure safe and effective use, always use products in accordance with label directions.

Water in birdbaths, containers, toys, etc. should be emptied regularly: Fact!

Mosquitoes need only a half inch of standing water to breed. After rainfall, empty any water that has collected in any container outside the house. Birdbaths changed at least three times a week.

Mosquitoes are more attracted to women than men: Fact!

Research has shown that mosquitoes appear to bite women more frequently than men due to their different hormonal make-up. Interestingly, women with blonde hair are often more frequent targets for mosquitoes.

Mosquitoes are more than just a nuisance pest. Their bites can cause harm to your family and your pets. To learn more visit site: pestworld.org.

PCUsers Group
of Redding
P.O. Box 494778
Redding, CA
96049-4778

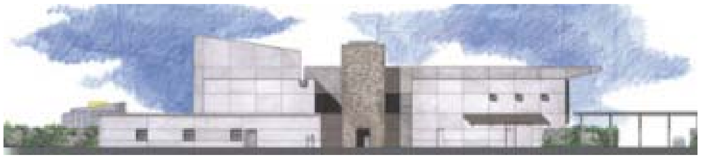
Why Join A Computer Group?

1. Benefit from a common interest in a personal (and costly) investment: Your business or personal computer.
2. Enjoy more of that investment by learning more about it.
3. Share tips and tricks, as well as new and old ideas.
4. Become exposed to a variety of new hardware and software without sales pressure.
5. Receive an informative monthly newsletter.
6. Have access to various club functions and all Special Interest Groups (SIGs).
7. Find out that no one needs to be alone and helpless with today's computer technology.

4th Tuesday

Monthly Meetings Are At

The Redding Library



1100 Parkview Ave.

off Cypress and to the right of City Hall.

We will be in the Community Room, which is inside to the left of the main library door.

Beyond Basics SIG

Saturday, 10 AM, March 19, 2016

At Jane Quinn's Home, for information contact:
Jane Quinn, 365-0825, qjquinn7427@gmail.com

Windows 7 and 10. Multi-Media prgs., Photo Editing, eMail, Cloud software, Google programs, and more.

This SIG expands beyond multi-media programs and devices to include Internet Browsers, YouTube, Free Software programs, or Apps that do so many various things. We will still work with photos and videos.

There's always a question and answer period. If we can't come up with the answer, we will find it together. I say "we" because we do work as a unit, expanding our knowledge and helping each other.

Every Thursday 1-3pm at the Anderson Sr Center 2081 Frontier Trail 365 3254, join us in the classroom. It's a walk-in format. I remain in the room after class to help anyone with their project or answer questions.