Bearly Bytes Newsletter

Big Bear Computer Club June 2017 Volume 17 Issue 5

President's Message - Yomar Cleary

Hello Everyone,

The Big Bear Computer Board has been busy setting up the monthly computer training Workshops, all the way thru October. Check out the training for each month on page 2 and also by going to our club'swebsite: www.bigbearcc.org. The next Workshop is on Monday, June 19th on Microsoft Excel 2013 from 1:00 pm to 3:00 pm.

Jim McFarlan is our **guest speaker** at our June 13th Computer Meeting. He is a popular national speaker and author of the acclaimed cyber thriller, *"Aftershock: A Novel."* Jim will show you how to protect yourself against the rising online scams and schemes that threaten our personal identities, credit and banking accounts.

Tuesday July 11, 2017 starting at 1:30pm, we are having our annual **Barbecue Potluck Party** at the Big Bear Senior Center with door prizes and opportunities to network. The Club will provide hamburgers , hot dogs and the fixings, while you can bring a side dish such as potato salad, green salad, vegetable platter, or macaroni salad, or whatever you decide. You are invited...come and join a causal occasion of summer cheer.

CONTENTS

NEXT CLUB MEETING
June 13, 2017
1:30 - 3:00 pm

Cyber Security

Jim McFarlan, security authority, popular national speaker and author of the acclaimed cyber thriller, "Aftershock: A Novel", will discuss how you can protect yourself against the rising tide of online scams and schemes which threaten your personal identities, credit rating and banking accounts. You are a target and only you can protect yourself. Jim will show how you can stop the cyber criminals before they even start.

To be held at the
Big Bear Senior Center,
42651 Big Bear Blvd
Big Bear Lake

- Consider bringing a snack to share during break-time.

2017 Big Bear Computer Workshops

2017 BIG BEAR COMPUTER CLUB WORKSHOPS

Computer Club workshops are two hours from 1:00 pm to 3:00 pm on the 3rd Monday at the Senior Center. The workshop fee is $15.00.   Here are the workshops scheduled for this year:

June 19th-Microsoft Excel 2013

The purpose of this course is to provide students with the knowledge and hands-on experience required to perform basic tasks in the Windows environment using Microsoft Excel. Students will grow in their ability to identify the fundamental functions of Excel. Design and input basic spreadsheets in Excel, using formulas and functions.

Registration contact Sandi Ybarra at 909 585-8313.

July 31st– Windows 10 Settings

How to find the Settings in Windows 10. Look at and set privacy settings. Learn how to change them. Look at Update & Security settings. Learn how to set Windows Update. Discuss Backup and Recovery settings, including files, system image and system repair disc. Learn how to back up on a schedule.

Registration contact Rosemary Lloyd at 909 547-7257.

August 21st—Security

Devices include smart phones, tablets, and computers. Keep your device clean of malware. Learn how to use best practices to avoid infections. Prevention is the key. Use anti-malware as a secondary line of defense. Download apps from known good sites. Back up your files so you can restore them if your device becomes compromised. Discuss security settings on your device. (There is probably more.)

Registration: contact Marc Busch at 909 609-9266.

September 18th - Settings on Your Mobile Devices Workshop

Devices covered include Smart Phones (iPhone and Android), Tablets Android and Windows 10) and laptops (Windows 10 and macOS). Discuss what these different categories of devices mean. Learn how to turn the device on. Set it up out of the box. Basic device usage. Connect to Wi-Fi.

Registration contact Rosemary Lloyd at 909 547-7257.

October 30th– Microsoft Publisher

2013

This Workshop "Publisher" is especially helpful for folks that do newsletters. It completely creates a template, including headings, titles, small text boxes for sidebars, ads, etc. Learn what options it presents when working on computer projects that require more manipulating than Word or Excel offers, again it is really applicable to Newsletters, Ads, Professional stationery set-ups, side bar ads for existing documents.

Registration contact Sandi Ybarra at 909 585-8313.

How hackers can ruin your summer vacation

**From airports to hotels to that cute cafe you found,
it just takes one cybersecurity slipup to turn your holiday into a nightmare**

Resource: cnet.com

It was the Summer Olympics in 1996 in Atlanta. Ken Spinner, then a systems consultant -- and tourist in the city -- lost his credit card information.

But this was more than two decades ago, so it happened the old-fashioned way: a mugging at the ATM.

Today, hackers can steal your credit card information without leaving their couches. That's particularly worrisome if you're taking off for the summer. It's peak vacation time, but it's also the perfect season for hackers.

As Americans take more than 657 million trips between the Memorial Day and Labor Day weekends, they're vulnerable to cyberattacks that steal their credit card data and personal information. For cyber thieves, resort hotels and airports make for lucrative hunting grounds.

It's no different from why thieves and pickpockets target tourists on vacation: They're in an unfamiliar setting, they have their guard down and, more importantly, they've got money.

"It's like why people rob banks. That's where the money is," said Scott Petry, co-founder of the secure browser Authentic8. "If people go to vacation, they go to resorts."

From a cybersecurity perspective, hotels aren't exactly bastions of relaxation. Over three months in 2016, more than 1,200 InterContinental Hotels suffered hacks. Malware has also hit President Donald Trump's luxury hotel chain, along with Sheraton, Westin, Starwood, Marriott,Hyatt, Kimpton and Wyndham hotels -- the list goes on.

In every one of those breaches, thieves stole credit card information from the hotels, leaving thousands of unsuspecting customers open to getting robbed. It's not just your money these hotels are losing; addresses, phone numbers, names, and check-in and check-out times are all fair game.

In the age of unsecured Wi-Fi, there's more than one way to get burned at the beach.

Aaron Robinson/CNET said, "Point-of-service systems have become notoriously insecure," said Adam Levin, a consumer advocate and chairman of Cyberscout. "Can you think of anyone that hasn't had a [breach] at a hotel? There are very few that have escaped so far."

Because many hotels are chains, one breached location means hackers can break into the entire network for the "mother lode of information," Levin said. The stolen information can be sold online for up to $50 per account.

The majority of incidents start from a single employee at a hotel getting phished, he added.

So even if your family takes all the precautions to keep your credit card information safe, and the hotel you stay at is safe, it could be a part of a compromised network. You could do nothing wrong and still lose.

Levin suggests that hotels invest more in encryption and in testing their security systems regularly.

But the breaches don't stop at hotels. Airports, coffee shops, beaches -- any place with open Wi-Fi, really -- should have you on the lookout.

Safe travels

Don't fret too much, though. There are still ways to keep yourself safe.

When you're traveling and don't have your precious home or office internet access, be wary of any public Wi-Fi network you jump on.

Continued...Page 4

Continued… Summer Vacation

You might be setting yourself up for a man-in-the-middle attack.

That's when a thief will set up a bogus hotspot, made to look exactly like the public Wi-Fi you wanted to get on, like the hotel lobby's or the airport's. When

airport's. When you sign on, you're actually sending all your data to the hacker, without any warnings that you're being compromised in plain sight.

It happens so frequently that in Singapore more people are afraid of using public Wi-Fi than public toilets.

"People typically have their guard down when they're on vacation," said Spinner, now vice president of field engineering at software protection company Varonis. "They won't consider what the implications are if they go to a rogue Wi-Fi hotspot."

Spinner recommends avoiding banking websites or typing in sensitive information, and he encourages always using an encrypted connection.

In some more extreme cases, he'll recommend going "electronically

naked." That means leaving every piece of technology at home: your phone, your laptop, your tablet, your iPad -- you know, everything.

There are entire retreats dedicated to detoxing from digital life, so the idea of going on vacation without any technology isn't as farfetched as you may think. Spinner said he does it anytime he visits China or Russia. He explained it's because that's where "hackers emanate from."

Enigma Software took a look at cities in the US, Canada and Europe that have the highest malware infection rates, though not all of the victims are people vacationing.

"IT and cyber technology has changed since the Atlanta Olympics, but I think it's becoming harder and harder for people to keep their information private," Spinner said.

If you're heading to any of these cities, consider going electronically naked

US		Canada		Europe	
Orlando	(1,146% higher than the national average infection rate)	Ottawa	(1,031% higher)	Lisbon	(473% higher)
St. Louis	(958% higher)	Trois-Riveres	(153% higher)	Paris	(223% higher)
Denver	(759% higher)	Montreal	(122% higher)	Athens	(214% higher)
Atlanta	(738% higher)	Burlington	(110% higher)	Amsterdam	(147% higher)
Tampa	(696% higher)	Toronto	(80% higher)	Barcelona	(96% higher)

Don’t Be a Victim of Health Fraud Scams

U.S. Food and Drug Administration

What is a Health Fraud Scam?
A health fraud scam is a way to fool people about health products that may not be all they’re cracked up to be. They play on our desires for a quick fix and bombard us with deceptive marketing.

Who Do They Target?
All of us! Health fraud scams can be found everywhere promising help for many common health issues, including weight loss, memory loss, sexual performance and joint pain.

They target people with serious conditions like cancer, diabetes, heart disease, HIV/AIDS, arthritis, Alzheimer’s, and many more.

Bogus ads promising amazing results can be found many places, including:

- The Internet
- TV infomercials and radio
- Magazines and newspapers
- Direct mail
- Unsolicited emails

BE AWARE

Know the Risks
Relying on unproven products can lead to delays in getting the proper treatment and can cause serious or fatal injuries. Products for weight loss, sexual performance, and body building may contain harmful drugs or chemicals listed on the label.

Recognize the Red Flags —These claims are often used in scams:

- Miraculous Cure
- Quick Fix
- Ancient Remedy
- New Discovery
- Scientific Breakthrough
- Secret Ingredient
- Natural Cure
- Shrinks Tumors
- Lowers Blood Sugar
- Quick and Painless Cure
- No-Risk Money Back Guarantee

BE CAREFUL

Don’t be Fooled

If a product claims to cure a wide range of unrelated diseases, it’s probably a scam. No one product can treat or cure many different illnesses.

Some companies even recruit your friends, family, or coworkers to spread the word about their products through word-of-mouth marketing.

Personal testimonials by “real” people or “doctors” played by actors claiming amazing results can be a tip off that it’s a scam.

Protect Your Information
Never give out personal information including your Medicare ID # in exchange for a free offer.

HOW TO REPORT A PROBLEM

To report non-emergency problems with a Food and Drug Administration (FDA) regulated product contact the consumer complaint coordinator in your geographic area. For a list of the coordinators, and more information on reporting a problem visit: www.fda.gov/Safety/ReportaProblem or call 1-888-463-6332.

To file a complaint with the Federal Trade Commission about misleading ads or websites for health products call 1-877-FTC-HELP (1-877-382-4357) or visit ftc.gov/complaint .

AVOID HEALTH FRAUD SCAMS

Be Smart
If it sounds too good to be true, it’s probably a scam.

Be Aware
Claims such as “Miracle Cure” or “Quick Fix” are red flags – learn to recognize them.

Be Careful
Before taking an unproven or little known treatment, talk to a doc- tor or health care professional–especially when taking prescription drugs.

To learn more about identifying and avoiding health fraud scams visit: FDA.GOV/HEALTHFRAUD

FDA Defines Health Fraud

FDA DEFINES HEALTH FRAUD

The FDA defines health fraud as the deceptive promotion, advertising, distribution, or sale of a product represented as being effective to prevent, diagnose, treat, cure or lessen an illness or condition, or provide another beneficial effect on health, but that has not been scientifically proven safe and effective for such purposes.

HONEY GO AND TALK TO HIM, HE JUST FOUND OUT HE'S A PLACEBO
(c) 2008 MIKE BANNON WWW.MORGANTORANGE.COM

FDA
Label CO.
WARNING!
W NING!
WARNING! THE SKY IS FALLING!
WARNING! WARNING SIGNS MAY CAUSE VOMITING!
WARNING! PIGEONS MAY CARRY GUNS!

How Hackers can use radio signals to hack your phone

Resource: hackernews.com

What if your phone starts making calls, sending text messages and browsing Internet itself without even asking you? No imaginations, because hackers can make this possible using your phone's personal assistant Siri or Google Now.

Security researchers have discovered a new hack that could allow hackers to make calls, send texts, browser a malware site, and do many more activities using your iOS or Android devices' personal assistant **Siri** or **Google Now** — without even speaking a single word.

A Group of researchers from French government agency ANSSI have discovered that a hacker can control Apple's Siri and Android's Google Now by remotely and silently transmitting radio commands from as far as 16 feet away...only if it also has a pair of headphones plugged into its jack.

How does the Hack Work?

It is very interesting and a mind-blowing technique. The Hack utilizes:

- An iPhone or Android handset with headphones plugged in
- A radio transmitter

The radio transmitter sends radio waves to silently trigger voice commands on any iPhone or Android phone (with a pair of microphone-enabled headphones plugged in) that has Siri or Google Now enabled respectively.

The radio transmitter sends radio waves to silently trigger voice commands on any iPhone or Android phone (with a pair of microphone-enabled headphones plugged in) that has Siri or Google Now enabled respectively.

Where the headphones' cables act as radio antennas, which can be exploited to trick an iPhone or Android phone user into believing that the voice commands are coming from the user's microphone.

This could leverage a hacker to do whole lots of things on victim's mobile phone without even speaking a word, including:

- Make calls
- Send text messages
- Dial the hacker's number to turn victim's phone into an eavesdropping device
- Browse to malware websites
- Send phishing and spam messages using Facebook, Twitter or email

"*You could imagine a bar or an airport where there are lots of people,*" Vincent Strubel, the director of the research group at ANSSI told Wired. "*Sending out some electromagnetic waves could cause many smartphones to call a paid number and generate cash.*"

Dependencies:

The hack only requires:

- A headphone-connected iPhone or Android phone
- Siri enabled from the lockscreen — which is Apple's Default setting.

In its smallest form, this hack could be performed from a range of around six and a half feet.

A more powerful hack that ranges to more than 16 feet requires larger batteries and could only fit inside a car, the researchers say.

Changing To Another Email Service

Resource: **Jim Cerny**
Sarasota Technology UG, Florida
April 2017

frontier
Communications
High-Speed Internet · Telephone · Television

Almost all computer users use email – and you are one of them, right? Have you ever had to change your email address or change to another email provider? Recently here in Florida (and I hear in Texas and California as well) our Internet provider **Verizon has been taken over by Frontier**. As a result of this, Everyone had to change from Verizon to AOL for their email. Fortunately their Verizon email address will continue to be accepted by AOL (for now). The purpose of this article is to help you understand what steps are needed to change to another email. I do recommend Gmail because it comes with several other tools provided by Google and you most likely will never have to change to another email address.

Your first task is to go to the website and establish a new email account -- that is get your new email address and password. Please write it down and do not lose it! Once you have your new email ID your major concerns are forwarding your old emails to your new email address, getting your address book (or contact list) to your new email and to notify everyone of your new address. Some emails (such as Gmail) may ask you what your other email address is and automatically bring your contact list and forward any emails from your old address to your new address. They want your email business. But if your address book is not copied over for you then you will have to do it yourself. By all means "ask Google" how to do it. For example, ask Google "How do I get my AOL ad-dress book to my Gmail contacts?" What you will most likely have to do is to create a file of your address book by "exporting" it and giving it a file name, then copying that file by "importing" it into your new email. After you do this you need to examine your entire address book, name by name, to see that all the data was copied correctly. You will probably have some editing to do to straighten things out. For example, some phone numbers may not have been copied over or a nickname may have been placed as the last name, etc.

Next it is helpful to have all your old email "forwarded" to your new email address. This way you do not have to hurry to notify everyone on your list that you have a new email. If this is not possible, you may have to go into your old email and actually forward those important emails to your new email. From now on, only use your new email address.

Finally, send a nice email to everyone telling them your new email address. It also is essential that you read the "help" or "options" for your new email so that you are aware of how to create new email folders, sort your emails, find emails, etc. Although every email can do these basic functions, how it is done may be different on different emails. And if you are converting to Gmail, be sure to check out the many apps that are available to you with your Gmail account ID. Now you are ready to enjoy using your new email.

One word of caution -- what if you have used your email address to establish accounts with various on-line businesses or services? Movie channels, banking, club memberships, etc. may be using your old email address as your account ID. Unfortunately, all of these accounts must be changed to your new email ID. This may entail you having to enter all new passwords for all these accounts as well. This can be a real pain if you have many accounts, but there is really no other way around this, sorry. Be sure to write down all your IDs and passwords for every service or app which requires an account.

Good luck and please don't forget to Ask Google anything about your email. You will find very helpful instructions and videos to guide you. Now here's hoping that you will never have to change your

verizon
Verizon Communications Inc.

Photo by Jerry Land

Big Bear Computer Club Board News

We have started a Facebook page (thank you Bill Flanagan) for the computer club. Are any of you readers interested in doing the club's Facebook page?

Also, we have an opening for Name Tags/Hospitality chairperson for our monthly club meetings. You would meet and greet folks coming to the club's monthly meetings

Please contact Yomar Cleary
ycleary@charter.net

Your Computer Club donation is tax deductible.

Donations are accepted though Paypal.

Donate

You do not need a Paypal account to donate through Paypal.

Big Bear Computer Club Forum

The Big Bear Computer Club has a Discussion Computer Forum on a local Big Bear internet information site. Here's a link to the directly take you into the forum:

www.socalmountains.com

Once you're in the forum, Under General Topics click on "Computer Forum."

You can, optionally, bookmark the URL for an easy return for later reading.

You can read the forum without registering, but you need to register if you want to submit (post) a question or answer to someone else's post.

We hope to keep this as current as possible with the latest computer information.

You Can Support the Big Bear Computer Club at NO COST TO YOU

By using AmazonSmile!

For each Amazon purchase you, complete, Amazon will donate 0.5% of the purchase price to the Big Bear Computer Club.

Below is the link from Amazon Smile that will take you directly to the Big Bear Computer Club Amazon support page: https://smile.amazon.com/ch/74-3131147

You can consider sharing this link with your family and friends so they too can support the Big Bear Computer Club.

Big Bear Computer Club Website Links

- Club Bylaws
- Standing Rules & Policies
- Board Meeting Minutes
- BBC Cash Flow Statements

Download 200 Free Art Books, Courtesy of the Guggenheim

Resource: Smithsonian News

Titles devoted to Picasso, Rothko, Lichtenstein, Klimt and more are now available for your reading pleasure

Perusing through a beautiful, hefty art book is one of life's simple pleasures, but beautiful, hefty art books can be pretty expensive. Fortunately, the Guggenheim is on a mission to digitize its vast collection of titles. As Beckett Mufson reports for Vice*,* the museum has made 205 art books available for free download.

The project began in 2012, when 65 titles were released online, and the Guggenheim has slowly been growing its digital archive ever since. Among the latest additions are works devoted to Pablo Picasso, Mark Rothko, Roy Lichtenstein, Egon Schiele and Gustav Klimt. Fans of Wassily Kandinsky can browse through a 1946 copy of *On the Spiritual in Art,* an influential treatise by the pioneering abstract artist.

As KC Ifeanyi notes in *Fast Company,* most of the available books are rare or out-of-print titles, making the archive a great resource for art lovers—even those who aren't strapped for cash.

But if Lichtenstein's *Hopeless* and Schiele's *The Poet* aren't your thing, there are other institutions offering troves of free digital books. Getty Publications, for instance, has digitized 281 titles, while the Metropolitan Museum of Art has made 1,611 of its books available for free download. Happy reading!

***Aquarell 6* by Wassily Kandinsky (Public Domain)**

Apple COREner

By Gary Roerig, Front Range PC Users Group (FRPCUG), Fort Collins, CO, http:// www.frpcug.org

Worth repeating . . .

If you are on an iOS device (iPad/iPhone) please remember to not install anything from your web browser (normally Safari) especially anything that indicates Senior Discounts are available. I continue to see individuals who have clicked to install software from a web page, which then installs a Profile and allows a dummy email mail-box to be setup and . . . Voila . . . hundreds of SPAM email arrives. So stick to installing from only two places: Settings, General, Soft-ware Update for Apple iOS Updates and the App Store (white Upper Case A on a blue background). You will be a lot safer, but remember, nothing is fool proof so use good judgment.

Considering New devices?

My best advice is go to a physical store such as Best Buy or an Apple Store and handle the device you are interested in, such as an iPad, iPhone or MacBook, or even an iMac. Look at the screen size, feel the weight and then add some extra weight for a protective cover. Once you have decided on a model that best fits you, Google it and see what users are saying. Then Google it for the best price and go for it. Come into the Saturday Help sessions or email gro-rig35@gmail.com if you want some more advice or help. And as always, I am happy to help you set up the new device once you have it in hand.

Are iCloud and iCloud Drive the same thing?

Many Apple users are confused over “iCloud” and “iCloud Drive”. Most have turned on iCloud Drive without understanding what it is used for. On the other hand, iCloud, which would probably be of more use, is often outright refused simply due to a misunderstanding of what it is.

So what are we talking about here? Well iCloud Drive lets you securely access all of your documents from your iPhone, iPad, iPod touch, Mac, and Windows PC. So no matter which device you’re using, you always have the most up to date documents when you need them. For example, I store my training Word documents from my MacBook Pro on iCloud Drive but rather than lugging my MacBook around, I can open and edit the documents using my very light iPad.

Now iCloud is also on an Apple Server under the same Apple ID you use but it is a means of easily backing up iOS devices. The backups are always encrypted. There is no real difference between backing up to your computer or using iCloud, except iCloud is much simpler. When your iOS device is locked, on Wi-Fi and connected to power, the backup takes place automatically. When backing up to a computer you must use iTunes and your power cable and manually select to encrypt. Remember to properly eject your device from iTunes before disconnecting the cable if you decide to not use iCloud.

iCloud also provides a single repository for Contacts, Notes, Safari Bookmarks, Calendar items, etc. So let’s say you update Contacts or Calendar when on one device it will update the same information for all Apple devices that are logged into iCloud under the same Apple ID. There is a catch to using iCloud – you are provided a total of 5 GB of free storage by Apple per Apple ID. After that you pay $.99 per month for up to 50 GB. For me, having a “brainless” backup method and easy access to my documents regardless of the device I am using is worth the extra $.99 per month.

The Galaxy Note 7 is DEAD, but it will return in 2017

Resource: knowyourmobile.com

Samsung is encouraging all Galaxy Note 7 users that are still using their handsets to stop immediately and send them back in for whatever fate Samsung has in store for them.

Samsung's Galaxy Note 7 will get a re-release in June, according to reports. Just don't call it the Galaxy Note 7, however, as Samsung is apparently changing its name to the "Samsung Galaxy Note FE" – and, no, we don't know what "FE" stands for either.

The news comes via ETNEWS, which reports that Samsung. likely keen to make some money on its investment in last year's Note handset, will launch and release the Galaxy Note FE in June (right before the launch of the Galaxy Note 8).

Apparently, FE stands for "fandom edition" – though it could just as easily stand for fire and explosions.

"In terms of specs," notes BGR, "the Galaxy Note FE is expected to be exactly the same as the original Galaxy Note 7, only it'll feature a smaller 3,200 mAh battery. By reducing the battery capacity from 3,500 mAh and spreading out the components within the battery, Samsung is apparently confident that phones won't explode anymore."

Samsung issued a cull on Galaxy Note 7 handsets out in the wild via an update that rendered the handset useless.

Samsung is doing this because the handset is unsafe; it doesn't want any more explosions – that would be bad.

Samsung is encouraging all Galaxy Note 7 users that are still using their handsets to stop immediately and send them back in for whatever fate Samsung has in store for them.

The kill switch update, which is expected to appear on December 19, is simply a safety measure to ensure ALL Galaxy Note 7 handsets, especially rogue units, are terminated. The software update will prevent the handset from charging and effectively brick it.

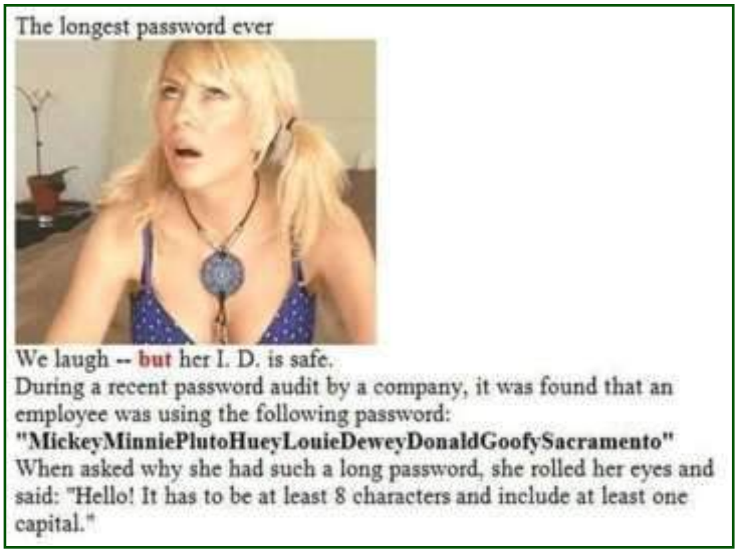
Of the ALL the Galaxy Note 7 handsets sold, 93% have been returned. These means there are still quite a lot of units left in the wild and this, of course, is a safety hazard and Samsung wants to nip this situation in the bud as quickly and painlessly as possible.

You cannot take a Galaxy Note 7 on a plane, for instance, it doesn't matter if it's in hand luggage or checked bags. Once these puppies started blowing up, the aviation industry, rightfully, took a hardline approach and implemented a strict ban on them.

About Bearly Bytes

Bearly Bytes Newsletter, past winner of SWUGC & APCUG Newsletter contests, is the official publication of the Big Bear Computer Club. Views expressed in Bearly Bytes are those of the authors and do not necessarily reflect the opinions of Big Bear Computer Club. Other computer user groups are welcome to reprint our articles as long as they give credit to the author and Bearly Bytes, Big Bear Computer Club.

Submissions: All BBCC members are encouraged to send letters, articles, questions, and comments to Bearly Bytes for inclusion in future issues. Submit as plain text in the body of an email and attach any graphics as JPEG or GIF format and send to: treadwell@bigbearcc.org



The longest password ever

We laugh -- but her I. D. is safe.
During a recent password audit by a company, it was found that an employee was using the following password:
"MickeyMinniePlutoHueyLouieDeweyDonaldGoofySacramento"
When asked why she had such a long password, she rolled her eyes and said: "Hello! It has to be at least 8 characters and include at least one capital."

Enter "Find the Bear"
contest to win a cool prize

1. *Locate this "BEAR"*
2. *Click on it*
3. *Fill in the form*
4. *and then Send*

At the next general meeting following this newsletter, a drawing will be held for all who found the bear. The selected winner will receive a surprise gift.

You will need to attend the meeting in order to receive the prize

The March Newsletter Winner was
Del Johnson!

Bits & Bytes

May 2017 Club Meeting

Marc Busch & Rosemary Lloyd presented information on Troubleshooting Hardware and Software. Attendees asked questions about issues they experienced.

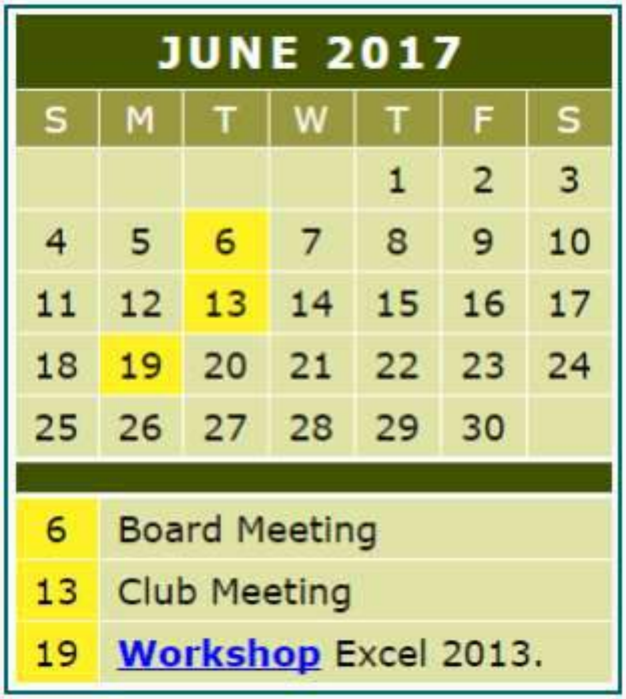
Attendees

The Opportunity Drawing Winners

left to right ...

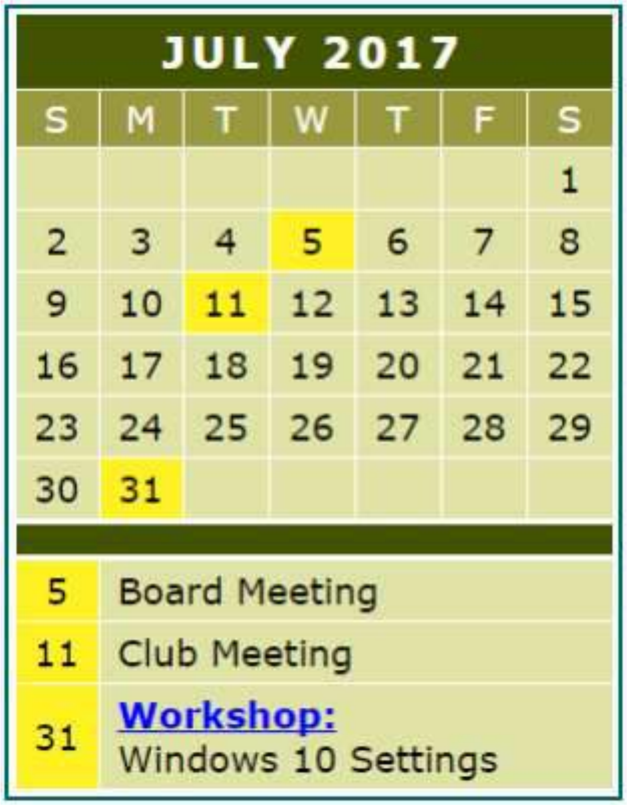
Russ Teeter	Carabiner
Bill Treadwell................	Box of pens
Marc Busch..................	.Pill Box
Rosa McFarlin................	Notebook
Not in picture: David Foltz......	Surface Shield Protection

Upcoming Calendar Events



JUNE 2017						
S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

6	Board Meeting
13	Club Meeting
19	Workshop Excel 2013.



JULY 2017						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

5	Board Meeting
11	Club Meeting
31	Workshop: Windows 10 Settings

2015 Website Contest

apcug

Second Place

bigbearcc.org

Group Newsletter Sites

apcug

An International
Association of Technology
& Computer User Groups

Word Tips

By Rosemary Lloyd

Maximize & Minimize the Ribbon

Applies To: Word 2013

The Ribbon is designed to respond to your current task, but you can choose to **minimize** the Ribbon if you find that it takes up too much screen space.

Click the **Ribbon Display Options** arrow in the upper-right corner of the Ribbon.

Select the desired **minimizing option** from the drop-down menu:

Auto-hide Ribbon: Auto-hide displays your document in full-screen mode and completely hides the Ribbon from view. To **show the Ribbon**, click the **Expand Ribbon** command at the top of screen.

Show tabs: This option hides all command groups when not in use, but **tabs** will remain visible. To **show the Ribbon**, simply click a tab.

Show tabs and commands: This option maximizes the Ribbon. All of the tabs and commands will be visible. This option is selected by default when you open Word for the first time.

https://www.gcflearnfree.org/word2013/getting-to-know-word/1/

Excel Tips

By Yomar Cleary

Enlarging the Formula Bar

The problem with an automatically adjusting Formula bar is that it can obscure other elements on the screen. If the Formula bar takes up two or three lines of depth, it overlays the column headers and other cells in the worksheet. This can be distracting, at times. Unfortunately, there is no way to instruct Excel to a) limit the Formula bar to a set depth or b) decrease the size of the type in the Formula bar so more can fit within a single line. The best you can do is to simply remove the Formula bar completely, so it is not visible. (If you have no Formula bar displayed, then it cannot expand and obscure information in the worksheet.) You can turn off the Formula bar in this manner:

1. Choose Options from the Tools menu. Excel displays the Options dialog box.
2. 2. Make sure the View tab is selected. (See Figure 1.)
3. Clear the Formula Bar check box.
4. Click on OK.

Windows 10 Tip

Secret Desktop Button

This desktop button actually dates back to Windows 7.

On the bottom-right corner of your page, there's a secret desktop button. Don't see it? Look *all the way* to the bottom and right, to the side of the date and time. There you'll find a small little sliver of an invisible button.

Click that and it will minimize all your open windows to clear the desktop.

You can change the behavior of this in Settings, between having to click or just having to hover the mouse over the corner.

Helpline

The following members have generously offered to help you with your PC problems by phone or by email:

Windows Beginners ....Yomar Cleary
909.214.6990 ycleary@charter.net

Microsoft Windows .... Rosemary Lloyd
909.547.7257 Rosemary@bigbearcc.org

MS Outlook .... Rosemary Lloyd
909.547.7257 Rosemary@bigbearcc.org

MS Excel .... Yomar Cleary
909.878.5622 ycleary@charter.net

MS Publisher .... Yomar Cleary
909.214.6990 ycleary@charter.net

Digital Photos .... Barbara Moore
909.585.7981 barbmoorebbl@gmail.com

CD Burning .... Rosemary Lloyd
909.547.7257 rosemary@bigbearcc.org

Computer Upgrades.................. Marc Busch
949.609.9266 bigbearjedi@charter.net

The Computer Club provides training at the monthly meetings when there is no presenter.

Persons with all levels of computer knowledge are welcome to attend the club's open meetings.

Your First 2 visits are free!
Bring a friend.
Annual Membership is $25 and spouse $5. All recurring membership dues are due in January.

THE BEAR WANTS YOU TO SHARE A TIP

Send tips to treadwell@bigbearcc.org

Officers and Key Leaders

President .... Yomar Cleary
909.214.6990 ycleary@charter.net

Vice President…. ………….......... Marc Busch
949.609.9266…………..bigbearjedi@charter.net

Treasurer .... Tom Brandau
213.446.1315 tombran44@gmail.com

Secretary .... Sandi Ybarra
909.585.8318 sandiscabin@gmail.com

Director at Large …….…..……… Jerry Merino
909.585.8714 gmerino@charter.net

Director at Large ……..…......... Del Johnson
909.584.9017……...deljohnson_ls@yahoo.com

Director at Large ………......... Bill Treadwell
909.730.4625 treadwell@bigbearcc.org

Webmaster .... Rosemary Lloyd
909.547.7257 Rosemary@bigbearcc.org

Assistant Webmaster ……..…..Bill Flanagan
909.866.9379 bill@bigbearcc.org

Newsletter Editor .... Bill Treadwell
909.730.4625 treadwell@bigbearcc.org

Publicity ....Yomar Cleary
909.214.6990 ycleary@charter.net

Equipment Chair .... Marc Busch
949.609.9266…………..bigbearjedi@charter.net

Technical Advisor … .... Jim Lloyd
909.584.9358 inquiries@sugarloafpc.com

Refreshments Chair …….……. Sharon Teeter
909.585.2026 sharonteeter1@verizon.net

Historian ....Sandi Ybarra
909.585.8318 sandiscabin@gmail.com

Sunshine Chair .... Angie Pezina
909.866.2314 apezina@gmail.com

Hospitality Chair……..…………vacant

General Information and Membership

Membership Benefits

- Monthly Meeting presentation and demonstration of popular hardware and software
- RAM (Q&A) sessions
- Tech News and Virus Alerts
- Door prize drawings
- Bearly Bytes, our award-winning monthly newsletter emailed
- Website: **bigbearcc.org**
- Free Software Review
- Member Help Line
- Member E-mail Notifications
- Member-only Discounts
- Training workshops

All this for only
$25 per year!!

BIG BEAR COMPUTER CLUB

A Non-profit 501(c)(3) corporation

Membership Application

☐New ☐ Renewal ☐ Update Information

Full Name ____

Mailing Address ______________________________________

City, State, Zip ______________________________________

Home Phone _(______)_________________ Cell Phone_(_____)_________________

E-mail address _______________________________________

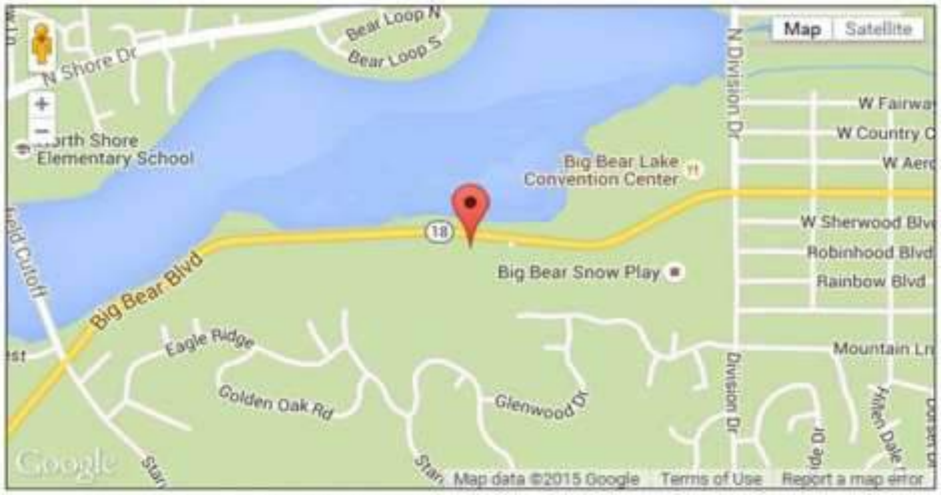
Adding Associates
For each Family Member (s) add $5/year towards your dues.

Name________________________ ____________E-mail__________________________

I agree that Big Bear Computer Club may use such photographs of me with or without my name and for any lawful purpose, including for example such purposes as publicity, newsletter, advertising and web content.

□ Yes □ No Your initials: _________

Mail your application and check for dues to:
BCC Treasurer
PO Box 645
Big Bear City, CA 92314
Or bring your application and dues to a monthly general meeting



Big Bear Senior Center, 42651 Big Bear Blvd., Big Bear Lake, CA

Mailing Address:

Big Bear Computer Club
PO Box 645
Big Bear City, CA 92314