Bearly Bytes Newsletter

Big Bear Computer Club February 2017 Volume 17 Issue 1

President's Message - Yomar Cleary

Hello Everyone,

HAPPY 2017 TO ONE AND ALL

As we look at 2016 and the great year we had, it is clear to the Big Bear Computer Club board that we couldn't have achieved our many successes without the membership's support. We are grateful for your close collaboration with us in the effort to educate and empower all our members to be safer and more secure when going into the Internet.

For 2017 adopt the motto of, "STOP, THINK, CONNECT" before you open your web browser, an email attachment, or download, and even when on social media while working on any of your digital devices.

The Big Bear Computer Club board has lined up the first six months with some great presentations. We will have Bob Gostischa, Bruce Aronson and Jim McFarlan. Jim will be addressing Cyber Security at the June 13th meeting.

We won't be having the annual Christmas in July but instead we will have a Summer Potluck with music by Jim Lloyd's AudioMaverick DJ.

See you all at the Valentine meeting, February 14th at 1:30 pm.

CONTENTS

NEXT CLUB MEETING
February 14, 2017
1:30 - 3:00 pm

Ransomware

A video presentation and discussion about the growing threat of ransomware.

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.

Gmail Users be aware of Phishing

Phishing attacks usually involve bad spelling, obviously fraudulent URLs, or attachments that no one in their right mind would open. Good cyber criminals know that the public is getting wise, which is why their methods keep on getting sneakier.

Take this new method, for example: It's been making the rounds for a few months now, but is just now coming to light as those affected realize what's happened. It's sneaky, effective, and even those who know their stuff are falling prey.

If you don't use Gmail then you don't need to be worried about this attempt to steal your credentials—it's only targeting Gmail users.

How it works

It all starts in a Gmail account that has already been compromised. Reports say that perpetrators are accessing hacked accounts immediately and sending phishing messages to other Gmail addresses in the hacked accounts contacts list.

An email lands in the target inbox from the hacked address, and here's where it gets tricky: The phishing email **uses a legitimate subject line, text, and attachments** from emails already sent by that account, making it look completely legitimate.

More about IT Security

Gallery: The 10 biggest business hacks of 2016

Experts predict 2017's biggest cybersecurity threats

The phishing email comes with an "attachment" that is actually a screenshot of an attachment sent by that account in the past, like a spreadsheet or a PDF, for example. The trick is that the fake attachment screenshot is an embedded image with a link in it that takes the victim to what looks like a Google login page.

Thinking they need to re-authorize their account to view the attachment the user logs in, and their account is now in the hands of hackers. The cycle starts all over again—just one compromised account has the potential to affect dozens more.

Defending against it

This is one of the trickiest phishing methods yet because it's so hard to detect. Even the URL of the fake login page looks real: It even contains the accounts.google.com domain. There's just one exception, and it's the key to avoiding it: The URL is preceded by "data:text/html."

That prefix is telling your web browser to treat the document at the phishing website as HTML, which in turn is generating an address that looks just like a real Google login page, complete with the appropriate URL. The second you log in hackers have access to your account, and victims have said they're taking advantage of it right away.

Avoiding this particularly insidious phishing attack relies on personal diligence. When you click on an attachment of any kind be sure to pay attention to the web address in your browser. If it's preceded by data:text/html don't log into it.

Take time to secure your Gmail account now

You don't need to wait for a hack to secure your Gmail account. Now is the time to take advantage of other security methods like **two-factor authentication.**

Sure, it can be a bit annoying to wait for a code every time you login from a new device, but it's worth it: Your life is in your email account. No one else should have access to that information besides you and those you trust.

New Phishing Scams Target PayPal and Amazon Customers

Resource: VIPRE Security News
January 13, 2017

Mississippi Attorney General Jim Hood recently warned Internet users, particularly customers of websites PayPal and Amazon, about the possibility they could be targets of phishing via scammers intending to gather sensitive personal information or infect computers with viruses.

"These online services and businesses make it easy for consumers to shop and pay for items online, but there are people out there who want to use this convenience as a way to steal your money, or even worse, your identity," Attorney General Hood said in a statement.

One scam that has surfaced lately involves an email with a link alerting the receiver that his or her PayPal account has been limited for security reasons. If a consumer clicks on the link contained in the email and submits his or her PayPal username and password to that site, the scammer can obtain the consumer's login information.

The scammer can then log in to the consumer's legitimate PayPal account to spend any remaining funds, bill credit cards, or steal personal information. The link provided in the email directs consumers to the spoof PayPal website, which is not secure. It even misspells the word 'PayPal'.

Other phishing emails target Amazon customers, trying to steal personal information or install malicious software. These emails, which look like they are coming from Amazon, show up in various forms: an order confirmation for items customers didn't purchase (can also be an attachment to an order confirmation); a request for a username, password or other personal information; a request to update payment information; a message with links to fake websites that look like Amazon.com but actually prompt the installation of software.

These fraudulent emails frequently contain a forged email address from an Internet Service Provider and usually contain many typographical or grammatical errors.

Attorney General Hood recommends that consumers who have PayPal or Amazon accounts and receive similar emails not to click on any links or submit any usernames, passwords, or personal information via email. Instead, go to the companies' actual websites and use the sites' secure login to verify any account activity.

"Although these scams have been around for quite some time, they continue to try to lure victims," Attorney General Hood said. "I encourage consumers to protect themselves from fraud and identity theft on the internet through education and awareness."

Some tips to help protect against phishing emails:

Do not respond to any unsolicited e-mails of this nature.

Do not click on any attachments associated with such emails, as they may contain viruses or malware.

If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email.

If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.

Don't email personal or financial information. Email is not a secure method of transmitting personal information.

If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure").

What If an App Could Tell You When You're Getting Sick?

Resource: Smithsonian.com
By: Randy Rieland

A Stanford geneticist may be onto something. Body data collected by smartwatches and other sensors can tip us off to brewing colds or infections. Wouldn't it be great if you could get an early warning that you're coming down with something, even before you start to feel sick?

One day, says Michael Snyder, there may be an app for that.

Stanford researcher Michael Snyder led a study on how wearable sensors could help predict illnesses. (Steve Fisch/Stanford Medicine)

Snyder is a professor of genetics at Stanford and lead author of a recent study published in *PLOS Biology* suggesting that data gathered from smartwatches and other wearable devices could be used to clue us in on brewing health problems, from a cold to conceivably, diabetes.

For the past two years, he and his research team have been compiling the results from roughly 60 volunteers—himself included—who have been diligently tracking their bodies' behaviors through wearable biosensors. All those monitors—some people wore half a dozen—collected more than 250,000 measurements a day on everything from heart rate to blood oxygen levels to skin temperature to physical activity to sleep patterns.

The idea was to first establish baseline measurements for each person, then determine how deviations correlated with illnesses or other environmental factors that can affect health. For years, Snyder has been creating health profiles for a group of volunteers through more conventional methods, such as blood and urine testing. Then he took notice of the wave of new devices on the market.

"When wearables came out, we were very intrigued and wanted to see what we could learn from them," he says. "There is a huge advantage to working with wearables. They do continuous measurements and that's a real plus."

It allows tracking to occur over a long timeline and not just sporadically, when any number of random factors could affect the results. And that gave the researchers a clearer picture of how a person's body could reflect an illness before he or she was aware of it.

"The overall impetus," Snyder notes, "was to define what it means for people to be healthy on an individual level, and then when disease occurs, understand what's happening when it's occurring."

Catching Lyme in time

As it turned out, Snyder's participation in the research paid off for him personally. While on a flight overseas, he began to feel a bit light-headed, so he checked his devices. His blood oxygen level had dropped during the flight, which wasn't unusual, but it had fallen much lower than normal.

"And it didn't come all the way back when we landed. My heart rate was elevated as well," he says. "I measure myself often so it was pretty obvious that something wasn't quite right."

Continued page 5...

Continued page 4… Health sensing

Before leaving on the trip, Snyder had spent some time in western Massachusetts helping his brother put up a fence. He didn't notice if he had been bitten by a tick, nor did he see any indication of it. But the readings on his devices suggested something was going on in his body. Maybe it was Lyme disease, he thought.

Snyder was right, and able to get a prescription for the antibiotic doxycycline, which quickly took care of the bacterial infection.

He concedes that most people aren't so in touch with their body's signals that they can make that kind of diagnosis. But that's the point, he says, of exploring the potential of wearable devices as a warning system. And not just for festering colds or infections, but also possibly for chronic diseases, like diabetes.

The researchers found that based on blood tests, a dozen of the people in the study had insulin resistance, a precursor to Type 2 diabetes. The scientists then designed an algorithm that combined participants' data tracking their daily steps, daytime heart rate and the difference between their daytime and nighttime heart rates. From that, they were able to identify similar deviations in those who were insulin-resistant.

Snyder says more research needs to be done to prove those types of correlations, but the ultimate goal is to create an app that will be able to alert people when their body's numbers are going out of whack.

The case for health sensors

Snyder disputes the notion that having constant access to this kind of body data will turn us all into hypochondriacs or that it will boost patient demands for more lab tests.

"I don't think it would be any more than the invention of the oral thermometer led to more people going to the doctor," he says. "If you're a bit of a hypochondriac, you could set the alert threshold higher. But I think it could alert you to something going on and cause you to manage things better.

"I think it would be particularly valuable for parents with their kids or people who are caring for the elderly," he adds. "In the future, I think you'll just be able to look at your smartphone and see that your kid's temperature has been running high the last three hours. No school for them."

Snyder acknowledges resistance from some parts of the medical community regarding the potential risk of people relying too heavily on sensors to self-diagnose. But he sees a day when physicians will have easy access to their patients' digital data, and that that range of information, instead of a single heart rate and blood pressure check in the doctor's office, will make it easier to make an accurate diagnosis.

"More information has got to be more valuable than less information when it comes to managing your health," says Snyder. "[Otherwise] That's like driving around in your car with no gauges on it. Who would do that?"

AN EXAMPLE APP and

not intended as a sales pitch

achu - sick prediction for fitbit
On iTunes By Datapult Inc

achu is the first ever sickness tracking and predicting mobile app made for use with fitbit bracelets. achu is designed to predict if a user will get a cold by analyzing the day to day patterns in their fitbit data. achu uses a pattern recognition algorithm to give users health predictions based on their past and present data.

Beware of new image files you didn't download:
They may launch 'Locky' ransomware

Resource: digitaltrends.com

By Bruce Brown—November 27, 2016

If you see a new image or graphic file on your computer that you don't recall downloading, do not open it. The Locky ransomware program has moved on from MS Office Word to Facebook and LinkedIn vulnerabilities, and is now putting files on your computer that can lock you out of your data, according to Ars Technica.

Earlier this year Locky arrived on computers via a "malicious macro" in a Word document. In the last week, however, Ars Technica quotes Israeli security company Check Point reporting a "massive spread of the Locky ransomware via social media, particularly in its Facebook-based campaign."

Typically what happens is that when you click on an image thumbnail, rather than displaying the image in a separate window, the file automatically downloads. It would be natural for most people to then click on the downloaded image — and that's what executes the Locky code and immediately locks up all your files and demands ransom.

More: 'Locky' ransomware harnesses the power of Microsoft Word to trick you into paying

Vulnerabilities in Facebook and LinkedIn have been exploited by the perpetrators of the Locky attack, according to Check Point. "The attackers have built a new capability to embed malicious code into an image file and successfully upload it to the social media website. The attackers exploit a misconfiguration on the social media infrastructure to deliberately force their victims to download the image file. This results in infection of the users' device as soon as the end user clicks on the downloaded file."

When Locky is activated on your computer the ransomware locks you out of your files. The only way to retrieve your data is by paying a ransom, hence the term 'ransomware.' Ars Technica reports the current ransom to unlock a user's computer is about half a bitcoin, or $365.

Check Point stated it previously informed Facebook and LinkedIn of the vulnerability currently being used in the ransomware attack, but won't make the details public until those social media and other major sites fix the security flaw. The security firm's recommendations to consumers are: "If you have clicked on an image and your browser starts downloading a file, do not open it. Any social media website should display the picture without downloading any file. Don't open any image file with unusual extension (such as SVG, JS or HTA)."

Note, however, that the file extension could also be JPG, PNG, or any other common form.

The bottom line on avoiding this particular means of an attack by Locky is, if you click on an image and it starts to download, whatever you do, do not open the image file on your computer.

ONLINE SHOPPING, HOW SAFE IS IT?

Resource: Los Angeles Computer Society Newsletter By Leo Notenboom September 28, 2016

Online shopping is ubiquitous, and yet some avoid it completely. Why are some people afraid to shop online when it's arguably safer than offline?

As you might expect, I get many questions from computer users concerned about their security. With regular news of identity theft, credit card fraud, and database hacking, many people are understandably concerned about the security of their own information online, particularly when it comes to online shopping… so much so, that some actively avoid online shopping for fear of having their payment information stolen. In my opinion, they should be more concerned about the security of their information *off*-line.

Most of us now take online shopping for granted. I suspect some may even wonder that this article is needed at all. The fact is, there are still many people who are afraid to shop at online merchants – even well-known, reputable ones. Why? They're convinced that the internet is full of hackers waiting to steal their credit card information as it goes by. They're quite willing to give that same payment information – along with an image of their signature, no less – to a stranger at a restaurant or a grumpy clerk in a retail store.

As I wrote in another article, "most people have an over-inflated sense of risk when it comes to threats they don't understand."

On top of that, we're most comfortable with black and white absolutes: *yes* or *no*, *safe* or *not safe*. Unfortunately, the world isn't black or white. It's very important to realize that there are risks either way, online or off. There are very few risks that are truly unique to using your credit card online.

Yes, online shopping security issues exist. Your device could have malware in the form of a keylogger, which records everything you type. And yes, it's extremely rare, but your connection to an online merchant could be intercepted by someone watching and recording your payment information. Much more common, however, are things that apply regardless of how you use your credit card. The news reports we hear are major breaches at retailers and banks, where it doesn't matter if you used your card online or off. In fact, most of those break-ins are caught and dealt with so quickly that, if we are affected, it's only to the extent that we might unexpectedly get a replacement credit card.

I believe individual theft occurs more frequently off-line.

- A clerk might make a copy of your card and signature.
- A dumpster diver could grab your bank statements out of your trash.
- Someone might steal your new credit card out of your mail box.
- You use your card at a cash machine, but a thief has hidden a "card skimmer" on the reader that steals the information on your card as you use it.

These off-line methods are all much more com-mon than individual online theft.

And even though we seem to hear about online theft on a semi-regular basis, there's a strong argument that says they're still fairly rare occurrences, compared to the millions of card-holders and millions of transactions that hap-pen every day. Good sense implies good security. The fact is, regardless of how you use it, using your credit card represents risk. But then, so does getting out of bed in the morning.

Online or off

- Shop with merchants you know and trust.
- Watch for things out of place, be it some-thing odd about the card reader in a store, or a missing https padlock on a web site.
- Beware of phishing and other attempts to fool you into giving your personal information to those who would abuse it.
- Contact your credit card company whenever you think something may have happened.

My take is simple: shop online. I believe it to be generally safer than many physical in-person transactions. Online or offline, the risks are generally lower than you might believe. Don't let unfounded fear stop you from enjoying the convenience. I know I don't.

Big Bear Computer Club Board News

Dorthy Sirk has recently moved from Big Bear. She was our Name Tags/ Hospitality chairperson for our monthly club meetings, and now her position is open. If you would like to meet and greet folks that come to the club's monthly meetings, please contact Yomar Cleary (ycleary@charter.net).

In a few months Barbara Moore will be moving from Big Bear and leaving two positions open: Membership Chairperson and the Board position of Treasurer. Please contact Yomar Cleary (ycleary@charter.net) if you are interested in either of these two positions.

Now that Rosemary Llyod has stepped down as club president, she will become the club's new webmaster.

Your Computer Club donation is tax deductible.

Donations are accepted though Paypal.

Donate

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

Rosemary received a crystal award for her seven years as president of the Computer club and a gift certificate from Yomar Cleary on behalf of the Club..

Get started

amazonsmile

You Can Help Out the Big Bear Computer Club and at NO COST TO YOU

By using AmazonSmile!

The next time you online shop at Amazon, just go up to the address bar and enter smile.amazon.com from the web browser on your computer or mobile device. For each AmazonSmile purchase you make, Amazon will donate 0.5% of your purchase price to the Big Bear Computer Club. for the computer club to receive the donations, you need to select the Big Bear Computer Club as the non-profit organization of choice to receive your purchase donations.

If you have not signed up for Amazon Smile. Click on the "Get Started" button above.

If You've Got More Than 150 Facebook Friends, They're No Friends at All

Resource: fastcompany.com
by: Kit Eation

Social nets may be bees knees of Internet tech at the moment, but that doesn't mean it's all straightforward and fluffy: New research is suggesting that if you're friends with over 150 people on Facebook, the extras are meaningless.

This is a conclusion of some thinking by Oxford professor of evolutionary anthropology Robin Dunbar. He's recently expanded on some of his original research carried out in the 1990s on the human neocortex—this is a part of your brain heavily involved in language and conscious thought. It's the bit of brain matter that helps you relate to other people, on a friend-to-friend basis, and Dunbar's theory is that it can only handle a maximum capacity of roughly 150 ongoing, fully interactive friendships. If you know or are "friends" with more people than this, then actually you're probably merely acquaintances instead.

Dunbar's original research was based on people engaged in face-to-face, flesh and blood frienships...so he's updated it to consider the possibility that online friendships could actually enable a larger number of friends. His new research looked at the traffic of people with thousands of online friends to those with hundreds of pals or less. Perhaps unsurprisingly, given then very biological roots of his theory, it looks like Dunbar's 150 friend figure even holds true for online relationships—even with the ease and speed of the Internet, you can't overcome your basic brain programming relating to how many people you can be friends with.

And that means that all those folks with hundreds or even thousands of Facebook friends aren't really friends with that many people at all.

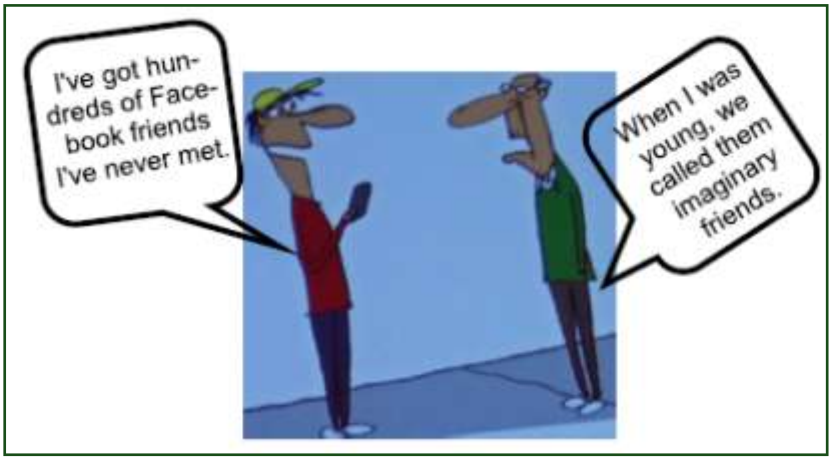
A bit of common sense thinking would suggest the same conclusion, of course, but to see it measured at a limit of merely 150 is a bit of a surprise.

The research may also have significant implications for how Facebook expands its live user status update systems in the future. It started as a one-to-one friending device, aimed at college-age people who were keen to find a forum that would let them engage socially online, but over time Facebook's expanded its reach and is now desperate to get you to transmit your data to everyone—essentially its asking you to consider that everyone's your friend. But people do tend to protect their friendship circles pretty fiercely, and Dunbar's 150 friend limit might just be a limiting factor for Facebook.

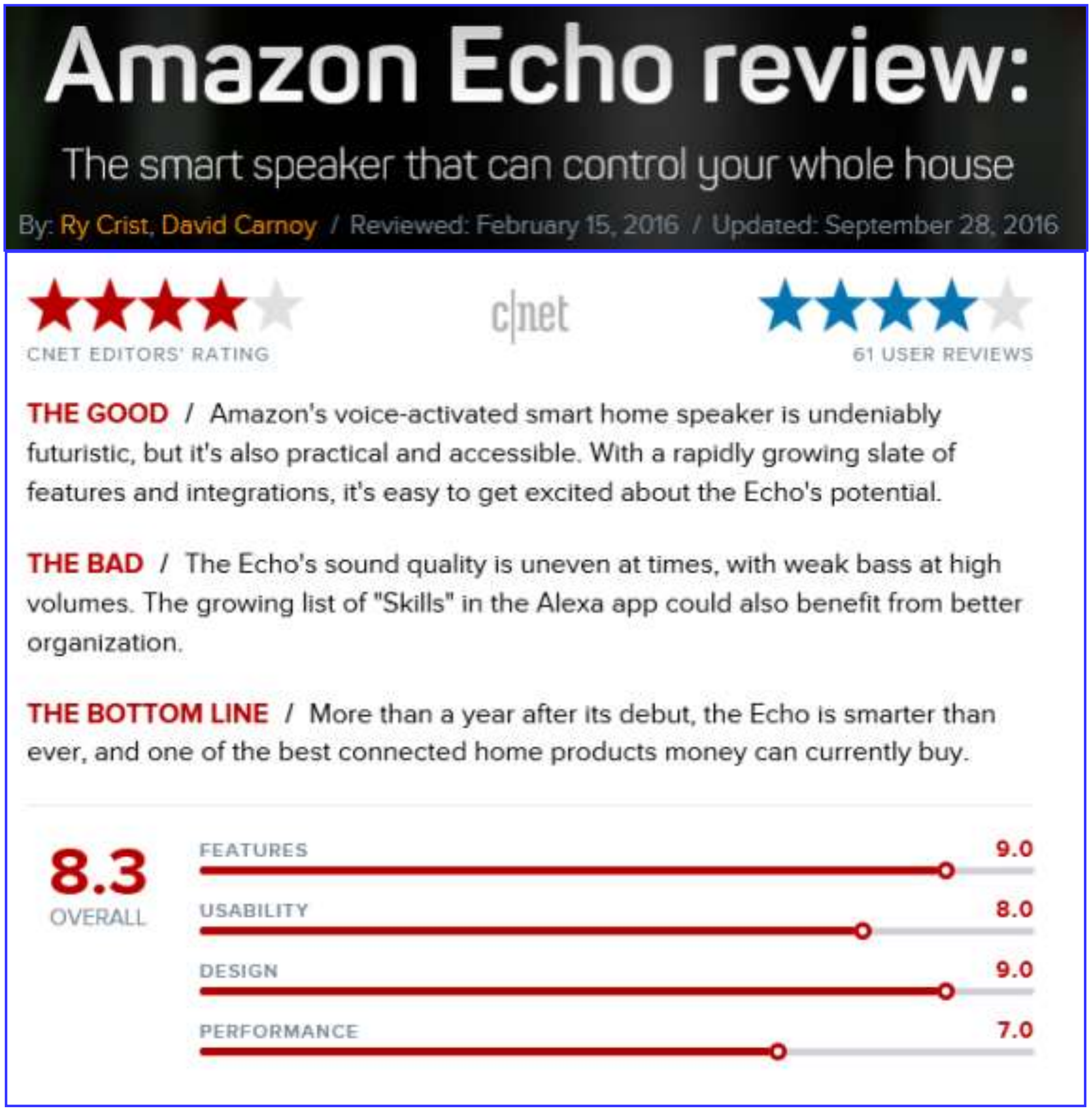
On the other hand, some noise was made recently by Anil Dash about high follower numbers on Twitter, and how this doesn't necessarily translate into real user attentiveness among a huge crowd. You may consider that Dunbar's theory is also applicable here, supporting Dash's stance, but I suggest it's actually more subtle than that.

Twitter is designed from the ground up as a one-to-many transmission system, and your identity is as protected as you like—your followers on Twitter most definitely aren't your friends. And consequently its users use it differently to the essentially similar status-updates within Facebook.

And now if you excuse me, I'm off to do some friendly Tweeting.


I've got hundreds of Facebook friends I've never met.
When I was young, we called them imaginary friends.

Amazon Echo



Amazon Echo review:

The smart speaker that can control your whole house

By: Ry Crist, David Carnoy / Reviewed: February 15, 2016 / Updated: September 28, 2016

★★★★☆ CNET EDITORS' RATING

★★★★☆ 61 USER REVIEWS

THE GOOD / Amazon's voice-activated smart home speaker is undeniably futuristic, but it's also practical and accessible. With a rapidly growing slate of features and integrations, it's easy to get excited about the Echo's potential.

THE BAD / The Echo's sound quality is uneven at times, with weak bass at high volumes. The growing list of "Skills" in the Alexa app could also benefit from better organization.

THE BOTTOM LINE / More than a year after its debut, the Echo is smarter than ever, and one of the best connected home products money can currently buy.

8.3 OVERALL	FEATURES	9.0
	USABILITY	8.0
	DESIGN	9.0
	PERFORMANCE	7.0

LibreOffice

By Dick Maybach, Member, Brookdale Computer Users' Group, NJ—August 2016 issue, BUG Bytes
www.bcug.com

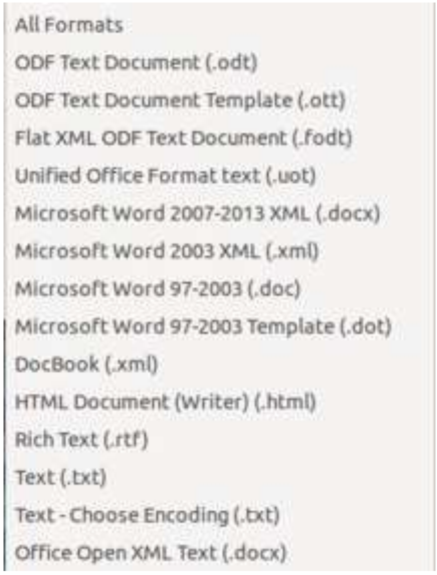
You can download **LibreOffice here**

LibreOffice originated in Germany in 1993 as Star Office, which became OpenOffice, first under Sun Microsystems and later under Oracle. In 2010 a group of developers, unhappy with Oracle's management of the project, formed the Document Foundation, and used the OpenOffice code as a basis for LibreOffice. Oracle later donated OpenOffice to the Apache Software Foundation, where its development appears to be lagging behind the vigorous pace of LibreOffice. Although LibreOffice and MS Office do similar tasks, their operating details differ considerably.

If you have used MS Office for a long time, then your first experience with LibreOffice will probably leave you frustrated with illogical menus and unpredictable operation. I've used LibreOffice for years (and OpenOffice before that) and those are exactly my feelings when I try to use MS Office. If you're thinking of installing LibreOffice and trying it for a few minutes, don't bother; you won't like it, because it's not an MS Office clone. If you are using MS Office casually at home, you have little reason to change, as LibreOffice offers no new capabilities. However, you may wish to consider changing if your environment changes, for example if you purchase a new computer or change operating systems. Now it makes sense to ask yourself whether to purchase a new version of MS Office or to make the effort to relearn your habits. If you really need something "Just like MS Office," then you should pay the money. A good comparison of these two suites appears at http://wiki.documentfoundation.org/Feature_Comparison:_LibreOffice_-_Microsoft_Office, but note that this is the Website of the Document Foundation, the publisher of LibreOffice. The two suites have different capabilities and features; if you do specialized work, check the Website referenced above for the features that are important to you.

You won't find a book on LibreOffice in your local bookstore, but you can download a good 388-page manual from http://www.libreoffice.org/get-help/documentation/. If after reading this you need more detailed information, the same site has manuals for the individual LibreOffice applications, but they are for earlier versions. There is also a 512-page tutorial on document styling at http://designingwithlibreoffice.com/, which you'll find interesting after you've mastered the basics. Some books are available from on-line vendors, but be careful, many are for older versions, and others are printed copies of what you can download for free. LibreOffice is evolving quickly; as a result, even the latest manuals are somewhat out of date with respect to minor details. Like all full-featured office suites, the LibreOffice applications are complex, and trying to learn to use them by trial-and-error will be tedious and frustrating, making a good tutorial essential.

Editor's Note: Write is the word processing program and it can save your written document in several formats



All Formats
ODF Text Document (.odt)
ODF Text Document Template (.ott)
Flat XML ODF Text Document (.fodt)
Unified Office Format text (.uot)
Microsoft Word 2007-2013 XML (.docx)
Microsoft Word 2003 XML (.xml)
Microsoft Word 97-2003 (.doc)
Microsoft Word 97-2003 Template (.dot)
DocBook (.xml)
HTML Document (Writer) (.html)
Rich Text (.rtf)
Text (.txt)
Text - Choose Encoding (.txt)
Office Open XML Text (.docx)

According to Maybach, "I have not run into problems converting Writer documents to Microsoft doc and docx formats. I understand that converting the other way can be problematic, as Microsoft sometimes employs undocumented features, and this is true for all LibreOffice applications."

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

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 the surprise gift.

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

The August Newsletter Winner was Del Johnson He received a USB Four Port Extender

Bits & Bytes

November 2016 Club Meeting

RAM Session and open discussion—Attendees brought their computers and software questions to the meeting.

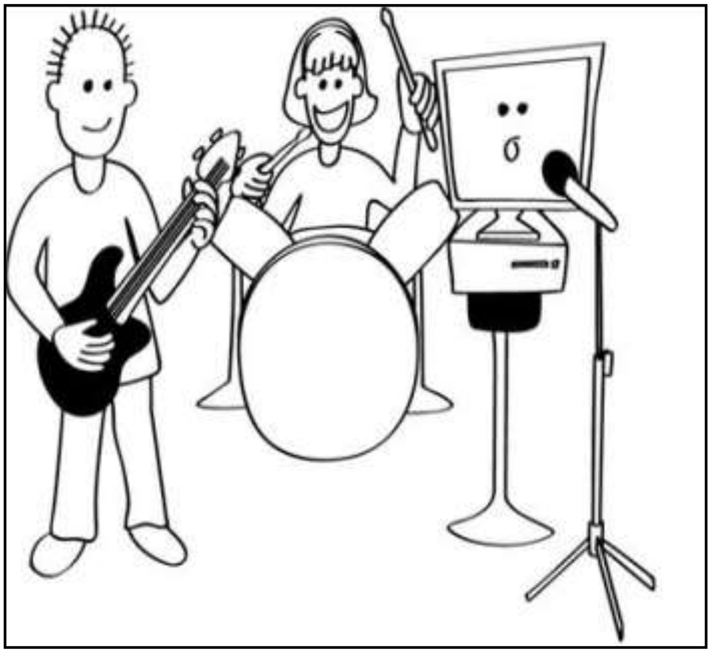
Attendees

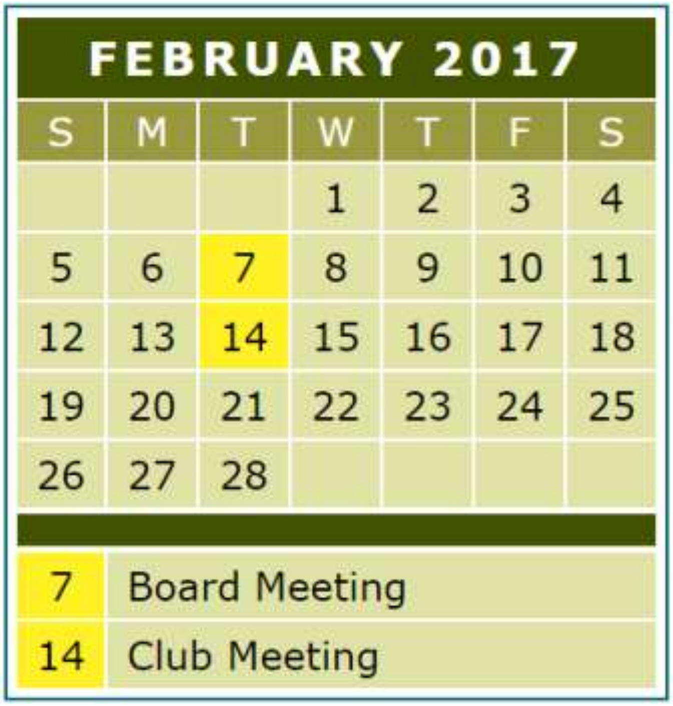
The Opportunity Drawing Winners

left to right ...

Russell Teeter.............	Sticky not dispenser
Sharon Teeter.............	Coffee Mug
Palm Palmquist	Club Notebook
Pearl Ann Gornik	Two Christmas coffee mugs
Marc Bush	Mini flashlight

This Month's Calendar





FEBRUARY 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				

7	Board Meeting
14	Club Meeting

2015 Website Contest apcug Second Place

bigbearcc.org

Group Newsletter Sites

apcug

An International Association of Technology & Computer User Groups

I want to
REFRESH my mind
DELETE all my problems
UNDO all my mistakes
and
SAVE the happy moments

Word Tips
By Rosemary Lloyd

Select a Theme and Style

Applies To: Word 2013=2016

Choose a document theme

- For a new document, select **File** > **New** and then select one of the themes.
- Or, select **Design** > **Themes** to change an existing document.
- Point to a theme to see how it will look in your document.
- Select a theme.
- Choose a new **Style**, if you want. Click the **More** drop-down menu to see all options.

Change the theme colors

- Select **Design** > **Colors**.
- Point to a color to see how it will look in your document.
- Select a color scheme.

Change the theme fonts

- Select **Design** > **Fonts**.
- Point to a font to see how it will look in your document.
- Select a font.

https://support.office.com/en-us/article/Video-Select-a-theme-and-style-a2a32660-6abf-4145-89bd-8550b91d8147?ui=en-US&rs=en-US&ad=US#ID0EAABAAA=Try_it!

Excel Tips
By Yomar Cleary

Hiding Individual Cells in Excel

This tip (6866) applies to Excel 2007, 2010, 2013, and 2016

Do you have a worksheet that needs to print out in a couple of different ways, for different users? Part of preparing your data for printing involves hiding or displaying some rows and some columns, as appropriate. You wondered if there was a way to hide the contents of individual cells, as well.

If, by "hide," you want to have the cell disappear and information under it move up (like when you hide a row) or move left (like when you hide a column), then there is no way to do this in Excel. Actual hiding in this manner can only be done on a row or column basis.

There are ways that you can hide the information in the cell, however, so that it doesn't show up on the printout. One easy way, for instance, is to format the cell so its contents are white. This means that, when you print, you'll end up with "white on white," which is invisible. Test this solution, though—some printers, depending on their capabilities, will still print the contents.

New Forum

Big Bear Computer Club Forum

The Big Bear Computer Club now has a Discussion Computer Forum a local internet information site www.socalmountains.com.

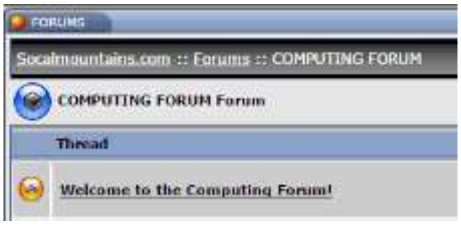
Once your on socalmountain's website,

- Click on "Home"
- Click on "Forums"
- 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 participate.

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



FORUMS

Socalmountains.com :: Forums :: COMPUTING FORUM

COMPUTING FORUM Forum

Thread

Welcome to the Computing Forum!

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 .... Barbara Moore
909.585.7981 barbmoorebbl@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 ………..…......... Bill Bryant
808.903.7918…..graphicelements@icloud.com

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

Webmaster .... Rosemary Lloyd
909.547.7257 Rosemary@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

Membership Chair …………. Barbara Moore
909.585.7981 barbmoorebbl@gmail.com

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

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

Name Tags/Hospitality…….…..………..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_(_____)__________________

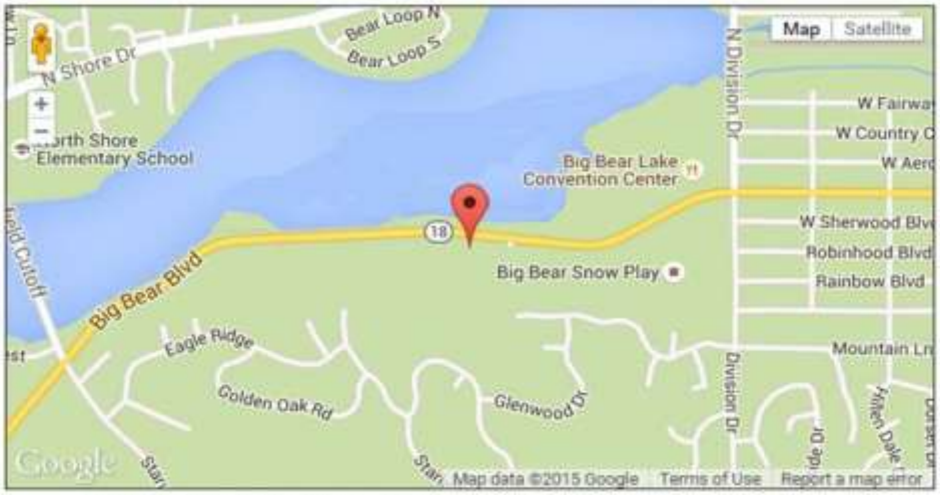
E-mail address ____

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

Name___________________________ ______________E-mail_____________________________

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 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