Bearly Bytes Newsletter

Big Bear Computer Club September 2017 Volume 17 Issue 8

President's Message - Yomar Cleary

Hello Everyone,

Cannot believe that Fall is upon us and Christmas is just 3 months away!! Our last meeting for this year will be Tuesday, November 7th. For the last year in a half, we have held our meetings at the Bear Valley Senior Center and our "thanks" go to Parks & Rec for allowing us to provide our computer training meetings and workshops at the Center. In appreciation for allowing us to use the facility at no charge, the Big Bear Computer Club has donated $200 to the Senior Nutrition Program. This is a wonderful program providing meals at a very low cost to the local seniors.

When you read this newsletter, don't forget to look for the "bear logo" somewhere in the newsletter that when you click on it, it will bring up a page where you add your email for a door prize if you come to the meeting that month. There are lots of bear logos throughout the newsletter but there is only one magic one.

CONTENTS

NEXT CLUB MEETING

September 12, 2017
1:30 - 3:00 pm

Tips for Staying Safe Online and

The presentation by Bob Gostischa from Avast Software covers: Computers (Windows and Mac), tablets and Smart Phones. addressing three important areas: (1) the importance to use the right tools once you get to the Internet; (2) he will show how to exercise caution when visiting the internet, and (3) the importance to avoid the dangers found on the internet.

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

2017 Big Bear Computer Workshops

2017 BIG BEAR COMPUTER CLUB

REMAINING TWO WORKSHOPS

September 18th
Settings on Your Mobile Devices Workshop

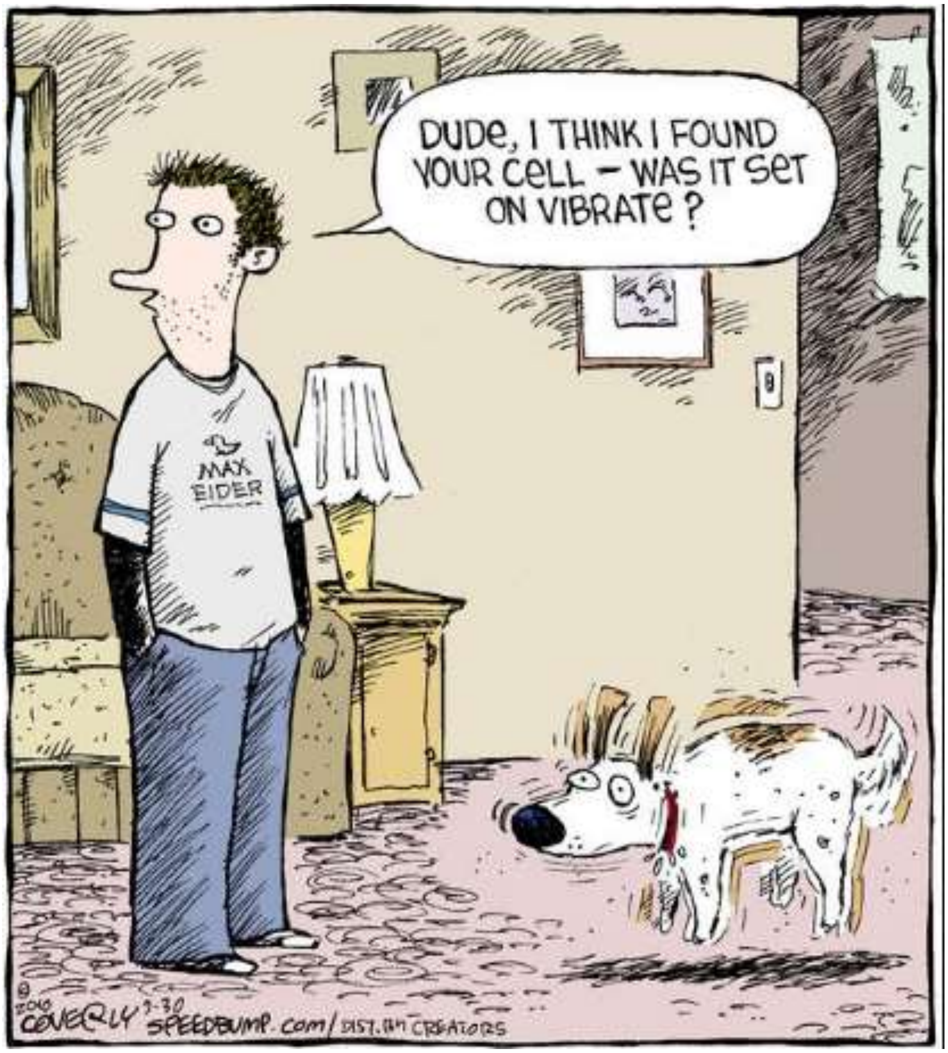
Devices covered include Smart Phones (iPhone and Android), Tablets Android and Windows 10) and laptops (Windows 10 and macOS). Discuss what these different categories of devices mean. Learn how to turn the device on. Set it up out of the box. Basic device usage. Connect to Wi-Fi.

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.


DUDE, I THINK I FOUND YOUR CELL – WAS IT SET ON VIBRATE?
MAX EIDER
©2010 COVERLY 9-30 SPEEDBUMP.com/DIST. BY CREATORS

Kaspersky's stellar antivirus goes free

Feature-limited but not dumbed-down

By Brad Chacos Senior Editor, PCWorld | JUL 25, 2017

Kaspersky has always charged a premium price for its antivirus product, and rightfully so. The software's topped independent testing results for years, to such an extent that in 2016 AV-Comparatives created a new "Outstanding Products" category for it and Bitdefender. But late Tuesday, the company announced Kaspersky Free, letting you deploy that top-notch defense without spending a single dime.

Kaspersky Free isn't as full-featured as the full-blown version, offering only antivirus protection for files, emails, and the web, along with table-stakes features like automatic updates and a quarantine for flagged files. "In short, the indispensable basics that no one on the planet should do without," CEO Eugene Kaspersky wrote. Think of it like the Windows Defender security tool native to Windows 10, but using Kaspersky's highly regarded technology. The streamlined focus helps keep Kaspersky Free's footprint smaller than that of the paid versions, Kaspersky says.

[Further reading: How the new age of antivirus software will protect your PC]

In turn, the free version's reach will help improve the protection for everyone, Eugene Kaspersky says, as more data feeds the company's machine learning engines. The premium Kaspersky Total Security suite also includes parental controls, online payment protection, and VPN access, which the free version lacks.

But even though it's free, Kaspersky's new product won't embrace anti-user practices, the CEO promises. "Kaspersky Free doesn't come cut with all the usual nonsense like advertising-oriented user-habit tracking and confidentiality infringements – which free AV normally suffers badly from in order to make it financially worthwhile to its manufacturers," he wrote.

Them's fighting words!

Kaspersky Free will start rolling out in the U.S., Canada, and "many of the Asia Pacific countries" today, July 25, for Kaspersky's 25th anniversary, before rolling out to the rest of the world over the coming months. At the time of writing, however, the announcement post's link to the Kaspersky Free pager directed to Kaspersky USA's homepage.

The story behind the story: A free, user-friendly version of Kaspersky? Sounds awesome! It also sounds like great PR at a time when a dark shadow's cast over the company, however.

Bloomberg recently published a report claiming that the security company "has maintained a much closer working relationship with Russia's main intelligence agency, the FSB, than it has publicly admitted." Kaspersky has firmly denied the claim, but that hasn't stopped the Trump administration from moving to block the company from a list of government-approved vendors.

CEO Eugene Kaspersky addressed those concerns head-on when announcing Kaspersky Free: "The same protection without compromise: we detect *any* cyberthreat regardless of its origin or intention – even if certain folks don't like it."

National Cyber Security Awareness Month

https://staysafeonline.org/ncsam

National Cyber Security Awareness Month (NCSAM) – observed every October - was created as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online.

Since its inception under leadership from the U.S. Department of Homeland Security and the National Cyber Security Alliance, NCSAM has grown exponentially, reaching consumers, small and medium-sized businesses, corporations, educational institutions and young people across the nation. 2017 marks the 14th year of National Cyber Security Awareness Month.

With recent legislation and support from the White House, cyber security is continuously a popular topic of discussion and rightfully so. More specifically, there is even stronger focus on consumers and their cyber safety. Everyone at every age is a consumer, and thus this year each theme will focus on the consumer and his/her needs regarding cybersecurity and safety. NCSAM 2017 also marks the 7th anniversary of the STOP. THINK. CONNECT.™ campaign. Each year, NCSAM highlights the overall message of STOP. THINK. CONNECT.™ and the capstone concepts of the campaign, like “Keep a Clean Machine,” “Protect Your Personal Information,” “Connect with Care,” “Be Web Wise,” “Be a Good Online Citizen,” "Own Your Online Presence" and "Lock Down Your Login."

Presidential Proclamation

President Barack Obama once again declared October as National Cyber Security Awareness Month in 2016. See the proclamation here.

2017 Weekly Themes

NCSAM focuses on a different cyber security issue for each week in October.

Week 1: Oct. 2-6
STOP. THINK. CONNECT.™: Simple Steps to Online Safety

Staying safe and secure online is our shared responsibility. Here is easy-to-follow, actionable advice for everyone. STOP: make sure security measures are in place. THINK: about the consequences of your actions and behaviors online. CONNECT: and enjoy the internet.

It is critical for anyone using the internet to continually learn about and consistently practice good cyber security habits. To better protect yourself, you should secure your home networks and mobile devices and take the time to learn how to use the internet more safely, securely and responsibly. Week 1 will address the top consumer cyber concerns, provide simple steps to protect against these concerns and teach you what to do if you fall victim to cyber crime.

Week 2: Oct. 9-13
Cybersecurity in the Workplace Is Everyone's Business

Whatever your place of business – whether it’s a large or small organization, healthcare provider, academic institution or government agency – creating a culture of cyber ecurity from the breakroom to the board room is essential and a shared responsibility among all employees.

Every organization needs a plan for employee education, training and awareness that emphasizes risk management, resistance and resilience. Week 2 will showcase how businesses of all types can protect themselves, their employees and their customers against the most common cyber threats. The week will also look at resources to help organizations strengthen their cyber resilience, including the National Institute of Standards and Technology Cyber security Framework.

Week 3: Oct. 16-20
Today's Predictions for Tomorrow's Internet

Take a look into our future through the lens of the connected internet and identify strategies for security, safety and privacy while leveraging the latest technology. With the explosion of digital interconnectivity, it is critical to explore everyone’s role in protecting our cyber ecosystem.

Continued... page 5

Continued… Cyber Security

Smart cities, connected healthcare devices, digitized records and smart cars and homes have become our new reality. Week 3 will remind you that your personal data is the fuel that makes smart devices work.

While there are tremendous benefits of massive interconnectivity, it is critical to understand how to use cutting-edge technology in safe and secure ways.

Week 4: Oct. 23-27
The Internet Wants You: Consider a Career in Cybersecurity

A key risk to our economy and security is the shortage of cyber security professionals to protect our extensive networks. Growing the next generation of a skilled cyber security workforce – as well as training those already in the workforce – is a starting point to building stronger defenses.

According to a study by the Center for Cyber Safety and Education, by 2022, there will be a shortage of 1.8 million information security workers. It is essential that we graduate students entering the workforce to fill the vast number of positions available and use technology, safely, securely, ethically and productively. Week 4 will encourage students and professionals to explore cyber security as a viable and rewarding profession. Key influencers – like parents, teachers, guidance counselors and state and local officials – will learn more about this growing field and how to engage youth in pursuing cybersecurity careers.

Week 5: Oct. 30-31
Protecting Critical Infrastructure From Cyber Threats

The systems that support our daily lives – such as electricity, financial institutions and transportation – are increasingly dependent upon the internet. Building resilience in critical infrastructure is crucial to our national security.

Week 5 will look at how cyber security relates to keeping our traffic lights, running water, phone lines and other critical infrastructure secure. This week is also the transition to November's Critical Infrastructure Security and Resilience Month, highlighting the tie between cybersecurity and our nation's critical infrastructure.

STOP. THINK. CONNECT.™

Cybersecurity begins with a simple message everyone using the internet can adopt: STOP. THINK. CONNECT.™ Take security and safety precautions, understand the consequences of your actions and behaviors online and enjoy the benefits of the internet.

Use National Cyber Security Awareness Month to begin incorporating STOP. THINK. CONNECT.™ into your online routine.

For more ideas on promoting National Cyber Security Awareness Month, visit the Get Involved page.

Our Shared Responsibility

We lead internet-connected, digital lives. From our desks and homes to on the go, we work, learn and play online. Even when we are not directly connected to the internet, our critical infrastructure – the vast, worldwide connection of computers, data and websites supporting our everyday lives through financial transactions, transportation systems, healthcare records, emergency response systems, personal communications and more – impacts everyone.

Cybersecurity is the mechanism that maximizes our ability to grow commerce, communications, community and content in a connected world.

The internet is a shared resource and securing it is *Our Shared Responsibility*. Our Shared Responsibility is once again the theme for National Cyber Security Awareness Month 2017.

No individual, business or government entity is solely responsible for securing the internet. Everyone has a role in securing their part of cyberspace, including the devices and networks they use.

How to Shake the Hook After a Phishing Attack

By Douglas Bonderud

Phishing is a key part of the threat actor's toolkit, especially to get cyberattacks off the ground. As noted by Dark Reading, some estimates suggested that 91 percent of all cyberattacks start with a phishing attack. This shouldn't come as a surprise given the increasing sophistication of automated security tools and the reliable social pressure exerted on employees when they see emails that say "act now" or "your account has been compromised."

But it begs the question: Are cyber criminals more advanced than the users they target? Research firm Imperva created 90 honeypot email and file-sharing accounts to find out. Here's a look at the phishing attack playbook — and how users can shake the hook.

Not So Sophisticated

The Imperva team monitored their fake accounts over a period of nine months, using traps contained in links and documents to discover how threat actors operated and what they were doing with stolen data. The researchers found that while malicious actors have distinct preferences when it comes to exploitable data, they're unconcerned about both attack speed and their own security.

For example, the report noted that 25 percent of phishers went after business-related data by looking at email subject lines. But over 50 percent of cybercriminals took more than a day to access accounts after they were compromised, Help Net Security said. Additionally, 74 percent of threat actors triggered bait alerts within three minutes of accessing email inboxes, indicating that they're likely using manual techniques rather than automated tools.

Despite having access to massive amounts of personal information, less than half of all compromised credentials were exploited. This indicated that attackers may have such a wealth of data available that they can pick and choose accounts with the highest value.

Phishers were also unconcerned with avoiding security scrutiny. According to Help Net Security, 83 percent "did little to cover their tracks." Of the 15 percent who erased new sign-in email alerts from the inbox, most neglected to clean up the trash folder, and just 39 percent made any effort to obfuscate their origin IP using Tor services or proxies.

Swimming Free From a Phishing Attack

There are some hooks users simply can't avoid. For example, Computer Business Review reported that a Gmail phishing scam leveraged actual Google links and the company's use of OAuth to trick users into providing third-party permissions, without the need for victims to re-enter credentials. But the laziness and sloppiness of most phishing attacks creates a small window for users: If they act quickly and decisively enough, it's possible to wriggle free.

First, pay attention to email inboxes and file-sharing account alerts. If there's any indication that a new user has signed in or secondary email addresses have been added for recovery, chances are a phishing attack is underway. Users need to check both the trash and sent folders to see if any suspicious messages have appeared or were sent out to other potential victims.

The Imperva team found that if users changed their password within 24 hours of the original phishing attempt, there was a 56 percent chance of preventing account takeover. By notifying email and file-sharing providers of potential attacks, along with changing all connected usernames and passwords — such as banking portals, e-commerce storefronts and any government accounts — it's possible to frustrate most phishing efforts.

Phishing works — and continues to work — because email is ubiquitous and users don't do enough to effectively secure accounts. But attackers are no better, leaving ample opportunity for on-the-ball observers to lock down accounts and send phish hooks back up empty.

FBI E-Mail Updates

Online Scammers Require Payment Via Music Application Gift Cards

Complaints filed with Internet Crime Complaint Center (IC3) from 2017 show online scammers are asking victims to pay fraudulent fees using music application gift cards as part of multiple fraud schemes. These schemes include auction frauds, employment/opportunity scams, grandparent scams, loan frauds, romance scams, ransomware, tax frauds, and various other online schemes.

In this scam involving music application gift cards, the perpetrator directs the victim to a specific retailer to obtain music application gift cards of varying amounts. Once the victim has purchased the gift cards, the perpetrator directs the victim to reveal the numbers on the back of the cards and provide them to the perpetrator via telephone, email, text, or a designated website. Once the perpetrator obtains the music application gift card data, the perpetrator either continues to request additional funds through more gift card purchases or ceases all communication with the victim.

The financial impact to victims can range from hundreds to thousands of dollars. IC3 victim complaint data from January through June 2017 involving music application gift cards indicate that these scams have impacted hundreds of victims with reported losses exceeding $6 million.

This scam is also associated with other fraud scams involving victims having won a prize, needing to pay a tax debt, having qualified for a loan, or that a friend or relative is in trouble and needs a payment via music application or other prepaid gift card to assist.

General Online Protection Tips

- Recognize the attempt to perpetrate a scam and cease all communication with the perpetrator.
- Research the subject's contact information online (e.g., email address, phone number); other individuals have likely posted about the scam online.
- Resist the pressure to act quickly. The perpetrator creates a sense of urgency to produce fear and lure the victim into immediate action.
- Never give unknown or unverified persons any personally identifiable information (PII).
- Ensure all computer antivirus and security software and malware protection are up to date.
- If you receive a pop-up or locked screen, shut down the affected device immediately.
- Should a perpetrator gain access to a device or an account, take precautions to protect your identity. Immediately contact your financial institution(s) to place protection on your account(s), and monitor your account(s) and personal information for suspicious activity.
- Always use antivirus software and a firewall. It is important to obtain and use antivirus software and firewalls from reputable companies. It is also important to maintain both of these through automatic update settings.
- Enable pop-up blockers. Pop-ups are regularly used by perpetrators of online scams to spread malicious software. To avoid accidental clicks on or within the pop-up, it is best to try to prevent them in the first place.
- Be skeptical. Do not click on any emails or attachments you do not recognize, and avoid suspicious websites.

If you receive a pop-up or message alerting you to an infection, immediately disconnect from the Internet to avoid any additional infections or data loss. Alert your local FBI field office and file a complaint at www.ic3.gov.

Hackers Demonstrate How Easily Voting Machines Can Be Breached

AUGUST 1, 2017

One of the nation's largest cybersecurity conferences is inviting attendees to get hands-on experience hacking a slew of voting machines, demonstrating to researchers how easy the process can be. "It took me only a few minutes to see how to hack it," said security consultant Thomas Richards, glancing at a Premier Election Solutions machine currently in use in Georgia.

The DEF CON cybersecurity conference is held annually in Las Vegas. This year, for the first time, the conference is hosting a "Voting Machine Village," where attendees can try to hack a number of systems and help catch vulnerabilities.

The conference acquired 30 machines for hackers to toy with. Every voting machine in the village was hacked. Though voting machines are technologically simple, they are difficult for researchers to obtain for independent research. The machine that Richards learned how to hack used beneath-the-surface software, known as firmware, designed in 2007. But a number of well-known vulnerabilities in that firmware have developed over the past decade.

"I didn't come in knowing what to expect, but I was surprised by what I found," he said. He went on to list a number of actions he hoped states would take to help secure machines, including increasing testing opportunities for outside hackers and transparency in voting machine design.

View Full Story From The Hill

Big Bear Computer Club News

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.

The Computer Club can recycle you old printer cartridges and cell phones.

Bring them to a club meeting and we will take them off your hands!

A simple way for the club to raise some funds.

- Brother Lasers
- Dell Inkjets
- HP Lasers
- Samsung Laser
- Canon Inkjets
- Dell Lasers
- Lexmark Inkjets
- Canon Lasers
- HP Inkjets
- Lexmark Lasers
- Cell Phones

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

amazonsmile
You shop. Amazon gives.

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

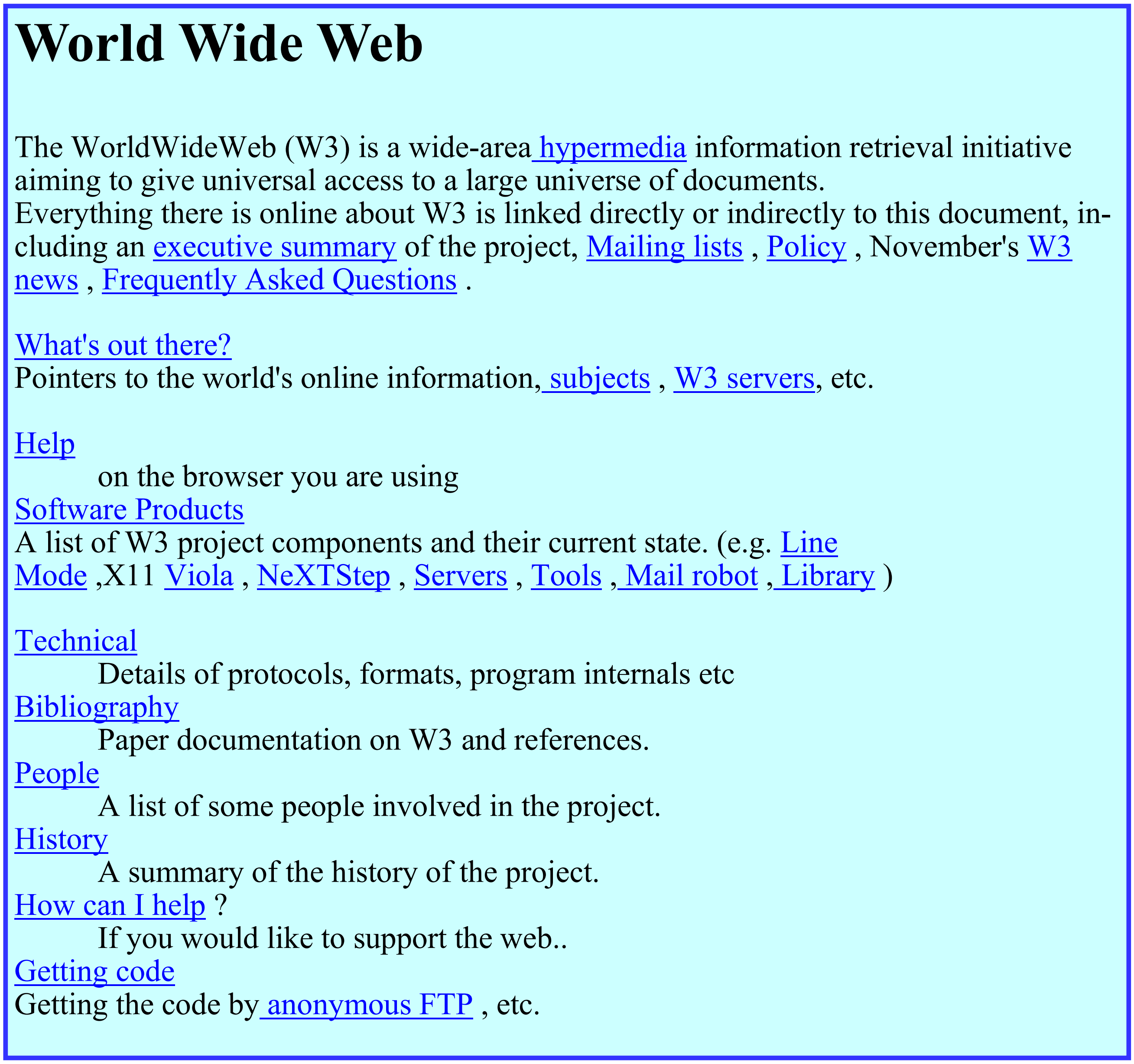
You can consider sharing this link with your family and friends so they too can support the Big Bear Computer Club.

Big Bear Computer Club Website Links

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

The First Internet Webpage

The first webpage was not very fancy—but very practical— compared to today's highly formatted, big text, colorful, and full of pictures laid out to distract you from what's supposedly pertinent. (Editor's opinion).



World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.
Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.

Help
    on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)

Technical
    Details of protocols, formats, program internals etc
Bibliography
    Paper documentation on W3 and references.
People
    A list of some people involved in the project.
History
    A summary of the history of the project.
How can I help ?
    If you would like to support the web..
Getting code
Getting the code by anonymous FTP , etc.

Microsoft Internet Explorer Tips

Reference	Tip
IE	Dictionary definition and related links on Microsoft Internet Explorer.
Browser	Display all your browser and connection information.
Internet	All other tips relating to the Internet.
Shortcuts	Microsoft Internet Explorer shortcut keys.
TIP3	Easily send a web page to a friend.
TIP8	Tabbed browsing tips.
TIP9	Browsing only safe Internet web pages.
TIP12	Move back faster in your browser.
TIP16	Undo closed Internet browser tab.
TIP17	Quickly bookmark a web page.
TIP18	Shortcut key to get into the address bar.
TIP20	Quickly scroll up and down on a web page.
TIP21	Make the browser window full screen.
TIP24	Quickly move forward and backwards using the mouse wheel.
TIP25	Automatically complete a URL.
TIP26	Open link in new window or tab.
TIP27	Print only sections of a web page.
TIP28	Increase and decrease web page font size.
TIP29	Move forward and back using the keyboard.
IE	Full listing of Internet Explorer questions and answers.

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 a surprise gift.

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

Bits & Bytes

July 2017 Club Meeting

Last month's meeting was Part II about Trouble Shooting Hardware

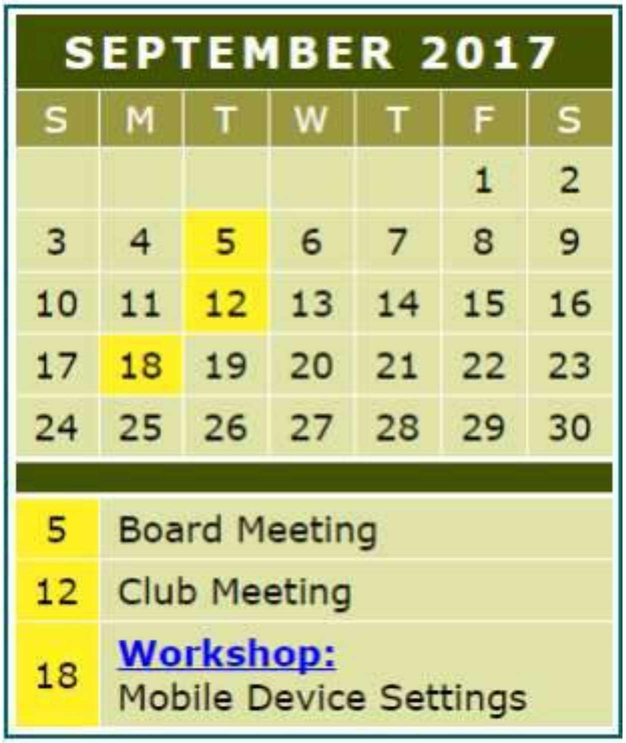
Attendees

The Opportunity Drawing Winners

left to right ...

Marc Busch ....Magnetic Roller Clip
Sharon Teeter ....Sticky Notes
Mary Lou McJilton ....First Aid Kit

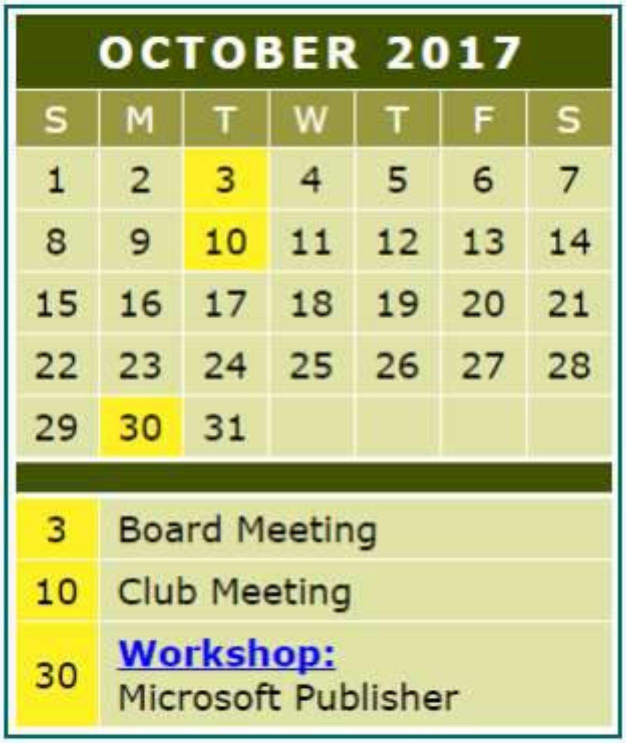
Upcoming Calendar Events



SEPTEMBER 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

5	Board Meeting
12	Club Meeting
18	**Workshop:** Mobile Device Settings



OCTOBER 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				

3	Board Meeting
10	Club Meeting
30	**Workshop:** Microsoft Publisher

2015 Website Contest
apcug
Second Place

bigbearcc.org

PEACHPIT
USER GROUP
PROGRAM MEMBER

Group Newsletter Sites

apcug

An International
Association of Technology
& Computer User Groups

webucator
customized INSTRUCTOR-LED training services

PEARSON
Education
OFFICIAL MEMBER OF PEARSON EDUCATION
User Group Program

RemoteCourse

Word Tips

By Rosemary Lloyd

Add Commands to the Quick Access Toolbar

Applies To: Word 2013

Located just above the Ribbon, the **Quick Access toolbar** lets you access common commands no matter which tab is selected. By default, it shows the **Save**, **Undo**, and **Repeat** commands. You can add other commands depending on your preference.

1. Click the **drop-down arrow** to the right of the **Quick Access toolbar**.
2. Select the **command** you want to add from the drop-down menu. To choose from more commands, select **More Commands**

The command will be **added** to the Quick Access toolbar.

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

Excel Tips

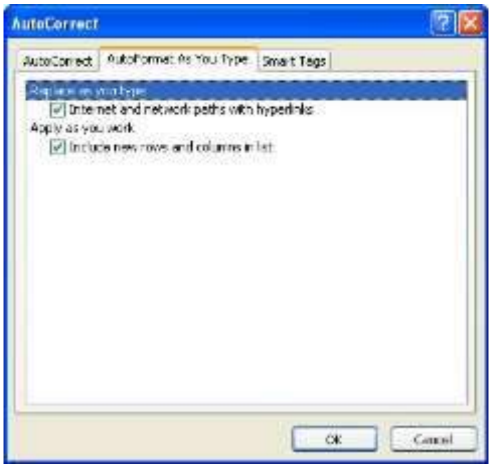
By Yomar Cleary

REMOVE HYPERLINK

When you enter a Web address or a LAN server address of a file into an Excel cell, it automatically converts to a hyperlink when you leave the cell. This is part of the "Web-aware behavior" of Excel, first introduced in Excel 2000.

If you want to turn off the automatic conversion, you can follow these steps if you are using Excel 2002 or Excel 2003:

1. Choose AutoCorrect Functions from the Tools menu. Excel displays the AutoCorrect dialog box.
2. Make sure the AutoFormat As You Type tab is selected. (See Figure



AutoCorrect

AutoCorrect | AutoFormat As You Type | Smart Tags

Replace as you type

☑ Internet and network paths with hyperlinks

Apply as you work

☑ Include new rows and columns in list

OK | Cancel

Figure 1. The AutoFormat As You Type tab of the AutoCorrect dialog box.

3. Clear the Internet and Network Paths With Hyperlinks check box.
4. Click OK.

Mac

Run Windows

We know, we know - who wants to run Windows? But sometimes it's handy, whether to play the latest games or run some niche piece of software that has no Mac equivalent.

You can either run Windows alongside macOS with a virtualization app such as VMware Fusion, Parallels Desktop or VirtualBox, or partition your hard disk to install Windows on to run it full-bore on your hardware using Boot Camp Assistant (in your Utilities folder).

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

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 Application

BIG BEAR COMPUTER CLUB, INC.

P. O. BOX 645 – BIG BEAR CITY, CA 92314

Membership Application—$25.00 – Associate $5

You can pay your dues at the monthly meeting, by mail -- make checks to Big Bear Computer Club, or by Pay Pal (Go into our website www.bigbearcc.org and go to “Donate.”)

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

□New □ Renewal □ Update my 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.

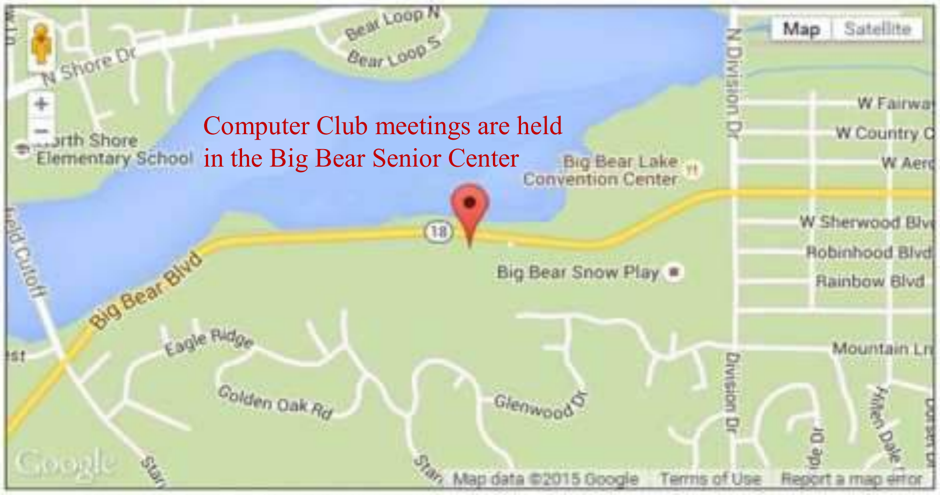
I agree that Big Bear Computer Club may use such photographs of me with or without my name and for any lawful purpose, including for example such purposes as publicity, newsletter, advertising and web content.

□ 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

All this for only
$25 per year!!

Mailing Address:
Big Bear Computer Club
PO Box 645
Big Bear City, CA 92314



Computer Club meetings are held in the Big Bear Senior Center

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