SUPERCOM COMPUTER CLUB TECH TIMES

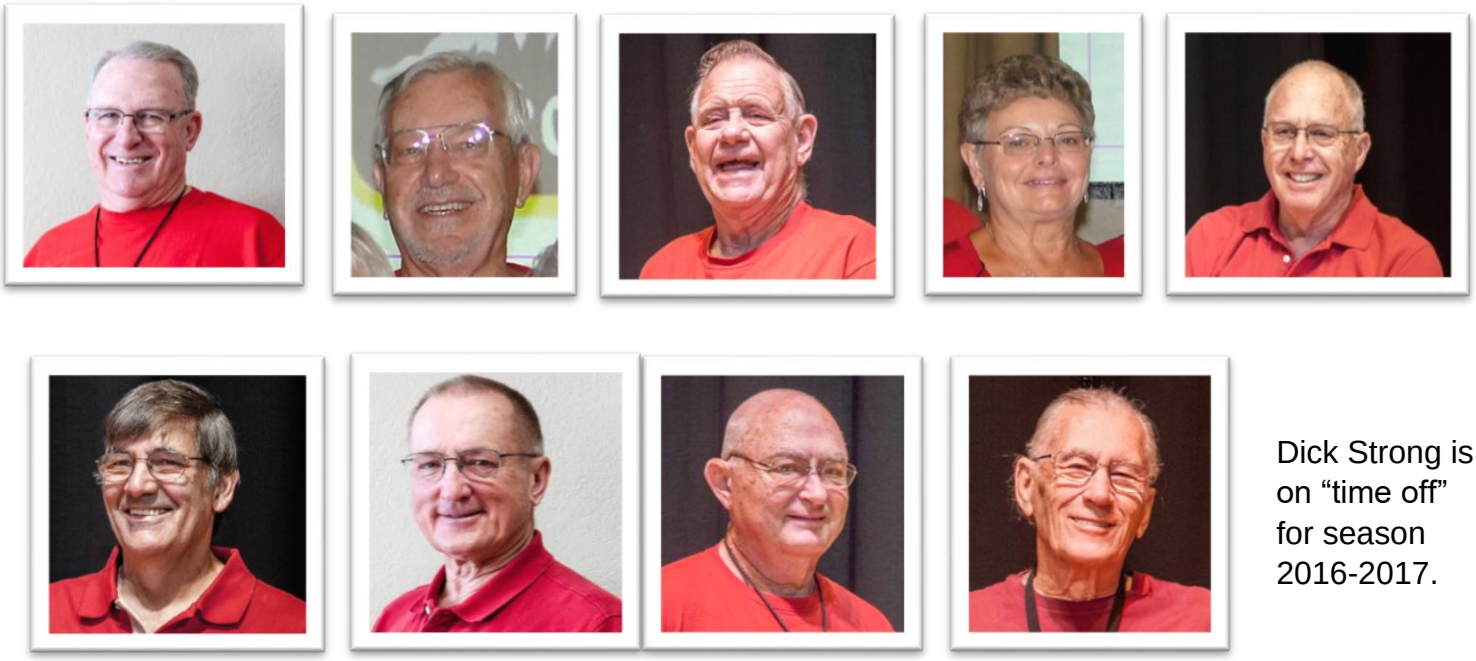
Volume 03 December 5, 2016

Objective:

To bring the latest technology news to you, our members. Tips and suggestions will help you to keep your device(s) running smoothly and help you be aware of threats. Technical tips will be coming to you through our Technical Committee.

Committee Members: (Pictured Below)

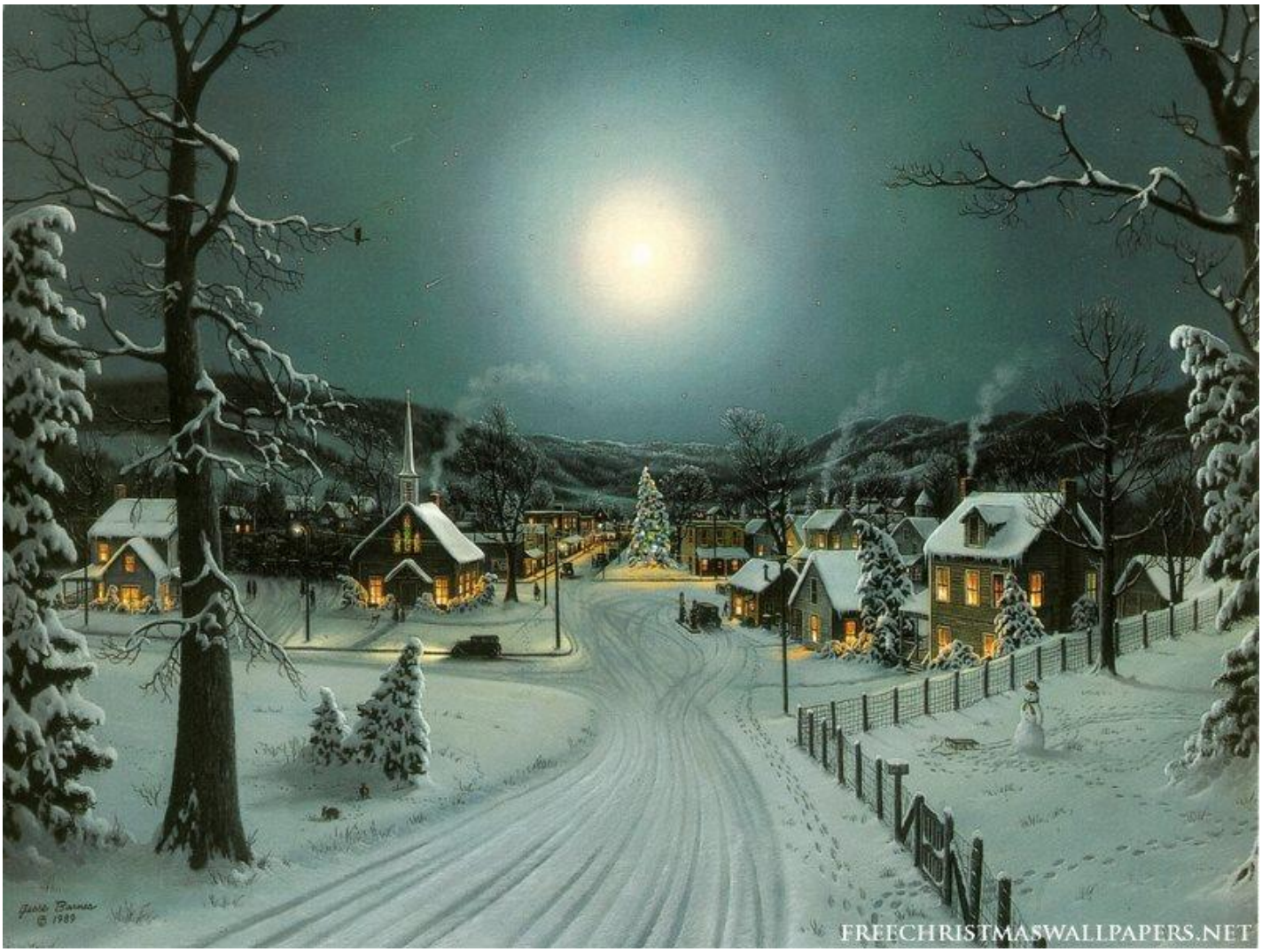
Ben Tarbell, Mike Gerkin, Jim Oliver, Peggy Bullock, Jim Mills, Rick Heesen, Lowell Lee and Steve Andreasen (Apple/Mac).



Dick Strong is on “time off” for season 2016-2017.

Greetings

It's beginning to look a LOT like Christmas, even here in the Valley of the Sun, AJ, Arizona! We see more and more Christmas decorations appearing around the park. That's a good thing!



Okay, beautiful picture but we Do Not have the snow!
Just a few things to share with you at this busy time of the year.

A couple from Ben Tarbell:

Adwcleaner

AdwCleaner is designed to remove crap from your system, but as with all things, make sure you back up your computer **and** create a System Restore point before continuing. That way, if you delete something you wanted to keep or mess up your computer, you can roll back to the way things were.

Step One: Download AdwCleaner

Head to the download page for AdwCleaner [click here] at Toolslib.net, the official home of this application. Click on **blue Download button.**

NOTE: Do not just Google **AdwCleaner** and install from wherever, because scammers are offering a fake version to trick people.

After downloading, you'll find the program in your **Downloads** folder {type **Downloads** in your search bar}. {left click to open}.

Find **Adwcleaner_x.xxx.exe** (most recent is Adwcleaner_6.030.exe).

Double-click [left mouse] the application to run it. You'll be asked about permissions.

Click "Yes" and you're ready to rock.

Step Two: Scan Your Computer With AdwCleaner

AdwCleaner's main interface offers three prominent buttons: **Scan, Clean, and Logfile.**

Click "**Scan**" to start looking for junk. The software will start looking for potentially problematic programs.

After a few minutes, you'll see a list of results.

AdwCleaner points out four kinds of malware, spread out across a few different tabs (in my case, "Folders" and "Registry". It will attempt to include:

- **Adware**, which you really don't want.
- **Potentially undesirable software**, which you might want but probably don't.
- **Toolbars**, which you probably don't want.
- **Hijackers,** which do things like change your default home page. You don't want these either.

Knowing this, you can read through the list, spotting anything you might actually want to keep. (**AdwCleaner** has been known to include some things you may want, like benign browser settings or Chrome extensions.) Be sure to **uncheck** anything you don't want removed.

If you ever aren't sure, google the name of the file, or check it against the Should I Remove It database.

If the folder has a gibberish name (like many Chrome extensions), you can navigate to the folder yourself and see what program or extension it may be associated with.

Repeat this process for the other tabs in **AdwCleaner's** interface–which can include

Registry keys,

browser settings and extensions,

shortcuts,

services, and more.

Again, be careful not to delete anything you actually want.

When everything is checked and ready to go, continue to the next step.

Step Three: Clean It Up

You can click the "**Clean**" button to automatically remove every checked item. You'll be warned about closing affected software.

After the cleaning process is complete, you'll be asked to **restart** your computer.

Make sure you close your other programs before this happens.

With any luck, your computer will be spick and span once again.

Credit to: http://www.howtogeek.com/275833/how-to-remove-toolbars-and-adware-with-adwcleaner/

Click on this website if you wish to read the full article for yourself.

PS: System Restore is not a good solution for removing viruses or other malware. Since malicious software is typically buried within all kinds of places on a system, you can't rely on System Restore being able to root out all parts of the malware. Instead, you should rely on a quality virus scanner that you keep up to date.

Ben

Below is the SIG Calendar for December 2016. One correction - There will not be a Facebook SIG on Tuesday, Dec. 13th.

December 2016 SIGs

◄ November | January ►

Sun	Mon	Tue	Wed	Thu	Fri	Sat
4	5 WIN 10 1 PM HOPI ANDROID 3 PM HOPI	6 MAC 10 AM LITTLE ROOM FACEBOOK 1 PM HOPI	7	8	9 9 AM COMPUTER MEETING	10
11	12 WIN 10 1 PM HOPI ANDROID 3 PM HOPI	13 MAC 10 AM LITTLE ROOM FACEBOOK 1 PM HOPI	14	15	16 9 AM COMPUTER MEETING	17
18	19 WIN 10 1 PM HOPI ANDROID 3 PM HOPI	20 MAC 10 AM LITTLE ROOM FACEBOOK 1 PM HOPI	21	22	23 9 AM COMPUTER MEETING	24
25	26 NO SIG	27	28	29	30 NO MEETING	31

And just in time for all you "on-line shoppers" here are some valuable tips from Mike Gerkin:

What should I know before doing my holiday shopping online?

In order to skip the lines and traffic, many people opt to shop online for gifts, even gift cards, during the holiday season. Unfortunately, hackers often target online shoppers to steal their personal information. Before you click, you might consider these tips for a safer online shopping experience.

Research websites before you shop. When shopping online, make sure you navigate only to reputable sites. You can research sites before you shop by reading reviews from previous customers or other search sources.

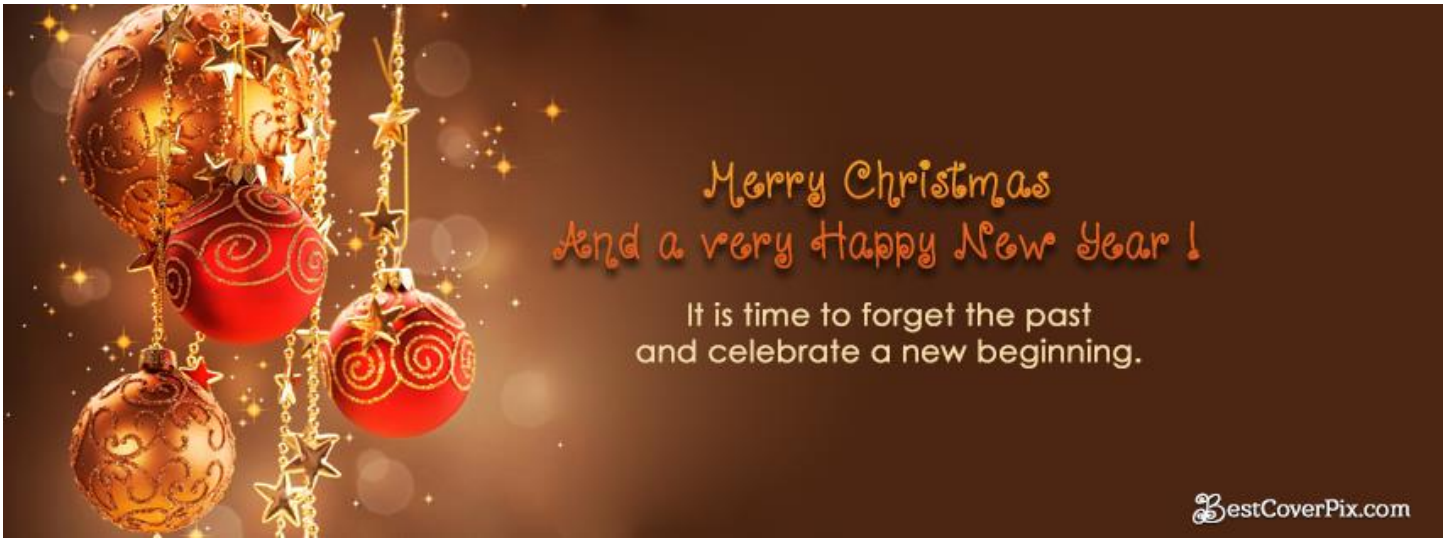
Choose passwords carefully. Create a strong password if you order through a new online account, and use different passwords when you shop on various websites. Follow password guidelines such as using a combination of letters, numbers, and capital letters or random phrases.

Be careful how you connect. Look for *https://* in the URL (the address area) and not just *http://*, since the "s" indicates a secure connection. Avoid public Wi-Fi networks when shopping online, as they often lack secure connections.

Search with purpose. Typing just one word into a search engine to reach a particular website is easy, but it sometimes isn't enough to reach the site you are actually looking for. Scam websites may contain URLs that look like misspelled brand or store names to trick online shoppers. You can also use a specialty search engine (e.g., one designed for clothing retailers or toy manufacturers) for optimal topical search results that will lead you to a reputable site.

Pay by credit card. Credit-card payments can be withheld if there is a dispute, but debit cards are typically debited quickly. Credit cards generally have better protection than debit cards against fraudulent charges.

Watch out for phishing and package delivery emails. Beware of emails containing links or asking for personal information. Legitimate shopping websites will never email you and randomly ask for your personal information. In addition, be aware of fake emails disguised as package delivery emails. Make sure that all delivery emails are from reputable delivery companies you recognize.



From Ben, Mike, Peggy and all the rest of the Tech Committee (Geeks for short)