May 2016

Visit our website at www.pcs4me.com Ken Johnson, Newsletter Editor

CALENDAR

SIG = Special Interest Group

This Week's Schedule

May 14 - Saturday - 1:00-3:00 PM
General Meeting - Leader: Ray Carlson
Location: Prescott Public Library

First Hour: Improved Apps in Windows 10

Ray Carlson will demonstrate setting up and using some of the improved apps in Windows 10. He will also demonstrate some of the benefits of Cortana and Google Now that have been cited as the reasons you ought to be using one of these digital assistants. Comments and suggestions from the audience will be encouraged.

Second Hour: Phil Ball will add his entertaining look at useful Tips and Tricks.

In addition to the presentations, the following are typical events which take place at our General meetings:

1) We hold an informal Flea Market in which you are encouraged to bring in your excess computer equipment or software and make them available for others to enjoy at no charge. Please deposit give-away items on the table in the back marked "Free Stuff." Any items left here at the end of the meeting are subject to disposal.

2) If you have items that are just too good to give away, you may set up a separate table and hold your own sale.

3) We conduct a raffle of gift cards at the end of the meeting, so make sure to get a pair of tickets from whoever is in charge and place one on the item you'd like to win.

4) We will also accept your used ink and toner cartridges for recycling. They are turned in to Think4Inc for credits which PCS uses to purchase office supplies from them.

Future Meetings:

May 21 - Saturday

There will be no PCS meeting today.

Calendar *Cont on Pg 2*

Future Meetings, continued:

May 26 - Thursday - 6:00-8:30 PM
Board of Directors meeting - Prescott Public Library; Elsea Room

May 28 - Saturday - 12:00 Noon-2:00 PM
Annual Picnic - Leader: Murray Smolens
Location: Goldwater Lake

Note that these dates are correct at time of publication but are subject to change.
Up to date information can be found on our website, www.pcs4me.com

Unless otherwise noted, our meetings are usually held in the Founder's Suite at the Prescott Public Library.

Prescott Computer Society
Officers & Board of Directors
2015-2016

Officers:		General Directors:	
President	Ray Carlson	Joan Baum	Murray Smolens
Vice Pres	Phil Ball	John Carter	Dick Mason
Secretary	JB Burke	Ken Johnson	
Treasurer	Edi Taylor-Richards		

Look in the sky! It's a bird, it's a plane...it's a drone!

Meeting review by Mike Hancock, Newsletter Committee, Golden Gate Computer Society

January 2016 issue, GGCS newsletter

www.ggcs.org

editor (at) ggcs.org

At the November 23, GGCS General Meeting, George Krieger, drone photographer, drone video producer and drone technologist, showed two drone-created videos: one of San Francisco seen from above and around Coit Tower; and one of Highway 1 road improvements in the Bixby Bridge/Big Sur area. Drones, or UAS's (unmanned Aerial Systems), usually have four rotors and are called quadracopters, and they have a camera similar to a GoPro, but gimbal-mounted.

The legal system is working on rules for all drones, except toys, to keep airspace safe, and permits drones to fly no higher than 400 ft. (will soon go to 500 ft.). Operators of delivery drones, of Amazon and Google speculation, will be required by the FAA to obtain a license and will have to fly no higher than 25 meters (83 feet) in the airspace over your property.

Since our airspace has over 100,000 planes and since there is the potential for millions of drones, it is clear that rules must be observed. See https://www.FA.gov/UAS.

New versions of drones take only six months to come to market and can broadcast signals from about 1,000 feet from the controller. 3D Robotics, a US-based company, makes roughly 80% of controllers, and DJI, a Chinese company, provides roughly 80% of drones themselves.

3D Robotics used to use open-source software, but this approach is changing; DJI is closed-source.

Drones, depending on the drone model and cost, have remarkable cameras with multi-gimbal

Continued on pg 3

stabilization, and dampeners.

The law today permits drones to fly only within eyesight of the operator but, with extras, they can fly up to five miles. Drones have heat sensors, GPS, accelerometers, pressure sensors, and Wi-Fi extenders, and they can take 3-D movies.

They fly in areas where the sensors can feed data back. They have been used to fly over blowing whales, which are not disturbed by their presence, to gather data. Elephants, on the other hand, are frightened, likely thinking the drones are swarms of bees.

From DJI, starter drones are the Phantoms 1 and 2; the 2 can fly 12 to 14 minutes with its stabilized GoPro and weighs under 5 lbs. All drones are battery operated. The DJI version has a camera, designed by DJI with Adobe support that takes RAW pictures.

The DJI Phantom 3 Professional has a 4K camera with Sony sensor, 94º wide angle f2.8 lens, and 3-axis gimbal stabilization. The camera can take 12MP still pictures. The main controller is the brains of the operation, collecting all data from the system, which includes GPS, inertial measurement, speed controllers, vision positioning, and auto takeoff and landing. It costs about $1,290.

The DJI Inspire is the flagship and can fly 15 miles at 50 mph. It has a Zenmuse 4K camera with a Micro Four-thirds CMOS sensor and a 15 mm f1.7 lens. It has a retractable landing system. The controller has a live map and radar and it has battery charge tracking. Basically, this small drone can do things that a much larger drone can do. The DJI Inspire 1 Pro costs about $4,500 in basic form. This manufacturer also sells the DJI Cosmos hand-held camera.

3D Robotics offers the Solo Quadracopter with 3-axis gimbal for an advanced GoPro camera. It employs a 1 GH2 Linux computer at the drone and at the controller. It can be automated for filming and has a touchscreen controller. The battery provides 15 mins flying time. The cost, including the GoPro camera, is about $1,900.

Another US manufactured drone is the Yuneec Typhoon 4K Q500, with handheld CGO gimbal steadygrip. Drones use photography for stills, panoramas, videos, mapping, and 360º Virtual Reality with GoPros. George showed us a drone video of mapping the Carmel Mission for an event setup, and felt that mapping will be the most lucrative use of drones in three to five years. He also showed us a video of a totally circular rainbow and a para-jumpers tracked by a drone. They are now also being used for photogrammetry and for providing aerial video of events.

Drones may operate no closer than five miles to airports. Much of the technology derives from military applications.

George then demonstrated a DJI multi-gimbal 15-pound drone in the meeting room.

This drone had a barometric pressure sensor to set altitude. Liability insurance is required for drone operators; Aerial Pack insurance costs $1,400/year. IDs are not yet required for drones. Control of drones is by 'packet' technology, thus if it loses signal, or if the battery gets low, it comes home.Ω

Internet Privacy
By Dick Maybach, Member, Brookdale Computer Users' Group, NJ
January 2016 issue, BUG Bytes
www.bcug.com
n2nd (at) att.net

Many of the entities that handle Internet traffic have little regard for maintaining our privacy. ISPs typically record the sites we visit and store our e-mail. Search engines keep histories of our searches and the sites we visit. Social media sites and Internet vendors collect as much data as about us as they can. Many make it available to both commercial and government entities. As recent headlines have shown, these data are often stored with minimal attention to security. For example because of Edward Snowden, we know that the NSA stored the data it collected unencrypted, on computers that had the means of copying it to portable media, and allowed maintenance staff to access to this equipment and to carry storage devices in and out of the facility. We know about Snowden because he disclosed what he had learned; we don't know how many others have quietly sold data to the highest bidder, and neither do their employers.

The point I'm trying to make is that the only one concerned about your privacy is you. The rest of the world will pry to the extreme limits of the law, and beyond, to profit from whatever it can find out about you. So what can you do? Actually, quite a bit, but there are trade-offs between the degree of privacy and convenience. I

Continued on pg 4

Continued from pg 3:

describe some of the tools I've found to be helpful and the inconvenience they introduce; you will have to decide which to use.

Protection While Browsing

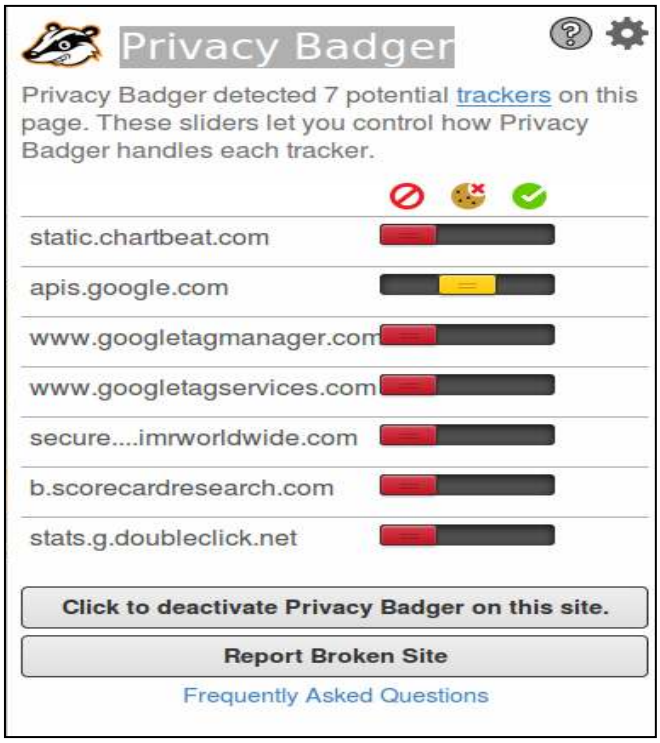
Certainly browsing the Internet exposes you to risk, as you often connect to sites about which you know little. I prefer using the Firefox browser, because it has some very useful add-on that help you protect your privacy, including BetterPrivacy, HTTPS-Everywhere, NoScript, and Privacy Badger.

Better Privacy (https://addons.mozilla.org/en-us/firefox/addon/betterprivacy/) protects against flash-cookies. These Local Shared Objects (LSOs) are pieces of information placed on your computer by a Flash plug-in that track your Internet use. BetterPrivacy lets you list and manage these Flash-cookies, e.g., to remove those objects automatically on browser exit. I use this as an "install and forget" add-on, and I've never found it necessary to disable it.

HTTPS Everywhere (https://www.eff.org/https-everywhere) is a Firefox, Chrome, and Opera extension that encrypts your communications with any website that offers https service. It's a result of a collaboration between the Tor Project and the Electronic Frontier Foundation. This hides your communications from any parties between you and the site, just as though you were talking to your bank. This too is an "install and forget" add-on.

NoScript (https://noscript.net/) disables JavaScript, Java, Flash, and other plug-ins, and as a result, seriously disables many sites. I start by enabling it everywhere, and disabling it, often just temporarily, only for those sites I trust and need.

Privacy Badger (https://www.eff.org/privacybadger) is available for Firefox and Chrome. It checks for tracking on every site you visit, and blocks it either completely or partially, depending on how each particular site behaves. You can click on the Privacy Badger icon to can see what action it's taking at the current site, as shown in the screen-shot below, which shows that cookies are blocked for apis.google.com and no content at all is accepted from the other six.



Note the Frequently Asked Questions at the bottom of the shot. Clicking on this will display information about what Privacy Badger does. By the way, the Avast antivirus extension blocks the installation of Privacy Badger and other extensions. Internet Explorer can also disable tracking, but only for specific sites. Interestingly, Privacy Badger identifies 11 trackers at https://www.microsoft.com/en-us/ and blocks cookies from the 10 of these it considers harmful.

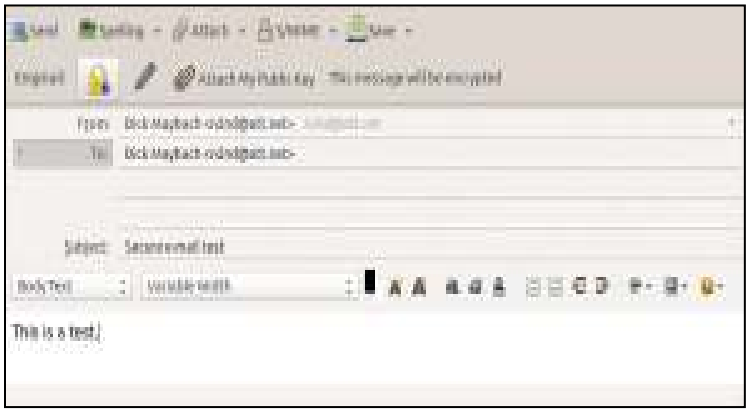
E-mail Protection

E-mail has much in common with postcards, in that everyone who handles it can see the contents. The only way you can safeguard your e-mail is to encrypt it, and the standard methods are Pretty Good Privacy, https://www.symantec.com/products-solutions/families/?fid=encryption, and its open-source variant Gnu Privacy Guard (GnuPG), https://www.gnupg.org/. Both of these adhere to the OpenPGP standard, http://www.openpgp.org/. (Also see https://en.wikipedia.org/wiki/Pretty_Good_Privacy.) They use public key encryption; that is, there are two keys, a public one and a private one. Files can be encrypted with either, but can be decrypted only with the matching one. You distribute your public key freely and carefully protect your private key. Your correspondents use your public key to encrypt messages to you, which only you can decrypt because only you have the matching private key.

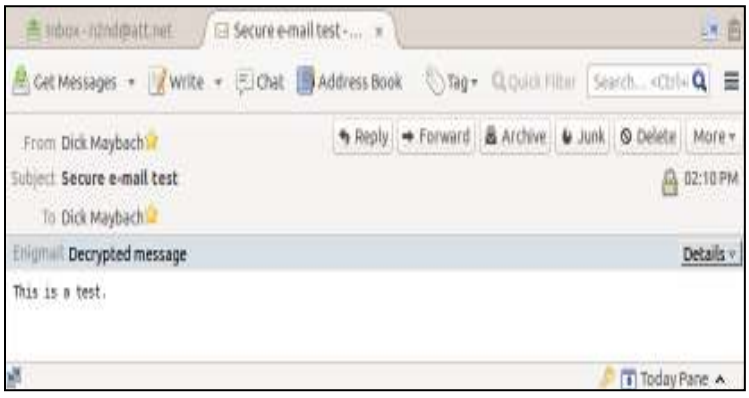
Continued on pg 5

Cont'd from page 4

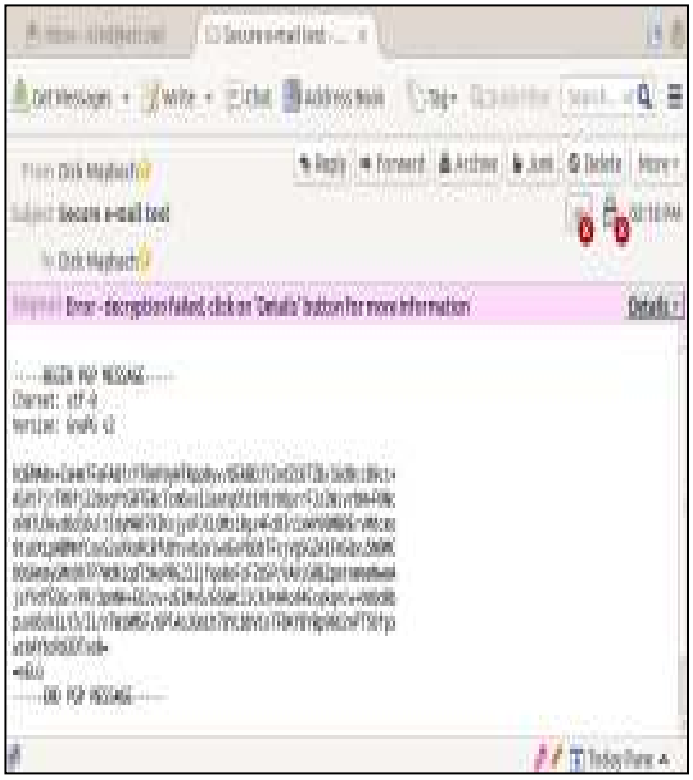
GnuPG is available for all the popular personal computer operating systems. However, it is a command-line program and is much easier to use if accessed a graphical front-end, such as the EnigMail add-on (https://www.enigmail.net/home/index.php) for Thunderbird, Mozilla's e-mail client. To encrypt a message, just click on the padlock icon, which will change from open to closed as shown in the screen-shot below.



When you click Send, you will see the unencrypted form of the message and a window asking for your passphrase. GnuPG passwords are stored in an encrypted database called a keyring, which requires this passphrase for access. The received message looks normal, although you may have to enter your passphrase to unlock it. (Depending on your settings, the system will remember a passphrase for a fixed time or perhaps for as long as you are logged on.)



Anyone reading your message without decrypting it will see only the following:



Once you have e-mail encryption set up and (here's the tough part) have convinced those with whom you correspond to do the same, it's very easy to use. I discussed e-mail encryption in more detail in my July 2014 article (available at http://www.bcug.com/.)

Protection at Wi-Fi Hot Spots

At home your PC is probably protected by a firewall in the cable modem provided by your ISP, but you have no such protection when you operate at a Wi-Fi hotspot. Indeed, widely-available software lets anybody using the same hot-spot capture all the traffic on it. You thus need extra protection, and I consider Tor (https://www.torproject.org/) to be essential here. It encrypts all your communication over a virtual private network and is available for Windows, OS X, and Linux. A snooper at a hot-spot sees only an https link to a node on The tor network; not only is he prevented from reading your packets, he doesn't even know with whom you're communicating. Your packets remained encrypted until they reach the exit node, which doesn't know where you are, nor does the machine with whom you're communicating. I discussed Tor in more detail in my June 2014 article.

If you use Thunderbird for e-mail, you can of course use EnigMail to encrypt your messages. For additional protection you can use the TorBirdy

Continued on pg 6

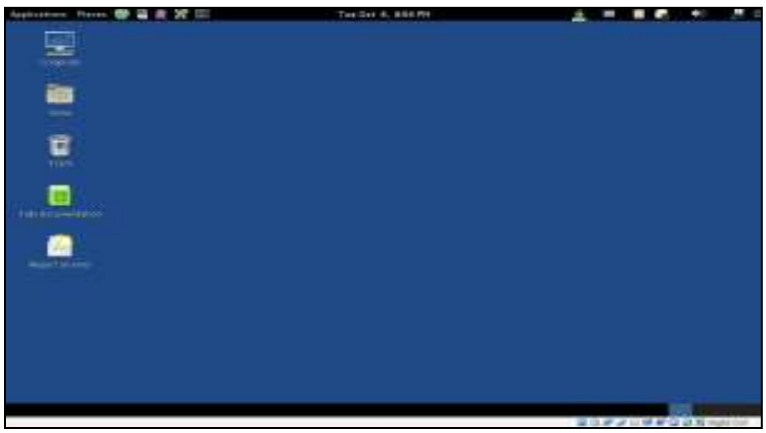
Continued from pg 5

(https://addons.mozilla.org/en-us/thunderbird/addon/torbirdy/) add-on. This routes all your e-mail, both sent and received, over the Tor network. It protects you against hot-spot snoops, but of course leaves you vulnerable to those in other parts of the network.

Protection at Insecure Computers

You must be careful when using a borrowed PC, either a friend's or especially one at an Internet cafe. Even if these are free of malware and are connected to secure networks, they often store passwords, Internet browsing history, and e-mail by default. If you must do something non-trivial, such as banking or e-mail, you should use a live USB memory stick with a secure operating system such as Tails, https://tails.boum.org/. This doesn't use the PC's hard disk at all, so it will neither be affected by any malware there, nor leave any traces of your activities. It uses Tor to access the Web, and thus prevents snooping from the network. Finally, when you exit, it wipes RAM. You can enable persistent storage to create an encrypted volume on the memory stick where you can store documents as well as Internet favorites, e-mail and e-mail addresses, and passwords. If you lose the memory stick and have used a good password, a finder won't be able to access your data. Tails has a virtual keyboard, which you can use if you suspect that the PC on which it's being used has hardware to record keyboard activity. You would use the virtual keyboard to enter passwords for example.

Yes, Tails is Linux, but as the screen-shot shows, its graphical interface should be familiar to almost any computer user. The most commonly-used applications are available on the menu bar at the top, and the rest reside in the Applications menu. As always though, you should experiment with it at home before you really need it.



Social Networks

Remember that anything you disclose will stay on the Internet and will be available to friends, enemies, relatives, employers, and all others, forever. Please use common sense. If on Facebook you talk about your new Porsche, your art and antique collections, and your upcoming three-week vacation to Spain, you shouldn't be surprised to return to an empty home and garage. Similarly, that hilarious picture of you spilling beer down your shirt may not be quite so funny if it shows up years later while you are running for public office.

Smart Phones

We have been discussing how to improve privacy when you use your PC, but I believe that smart phones are by far the bigger threat. While most PCs access the Internet through firewalls that are part of the router supplied by an ISP, cell phones typically connect directly to public networks and are always on. They allow tracking not only of their users Internet use, but also their geographical location. Yet, far fewer privacy and security tools are available for them and malware apps abound. Owners should review their uses of these devices, and the apps that are running on them, with respect to the associated potential loss of privacy. They will probably decide that some uses are better done from the relative security of a PC and some apps should be deleted. Protecting your privacy isn't difficult, nor need it significantly hinder your Internet use. It just requires that you learn to use the right tools and keep your wits about you.Ω

Need Help With Computers?

Did you know that the Prescott Public Library has a program of Computer mentoring on a one-on-one basis? They have several experienced volunteers who will work with you using one of the Library computers.

All you need to do is make an appointment with either the "Ask a Librarian" personnel or go to http://www.prescottlibrary.info/.