Lou & Polly Honored

Departure Report

As you all know, Lou retired from the President position. In appreciation the Group presented him with a gavel and block at the last meeting.

The band is hard to fully read due to it's laying on it's side. It reads:
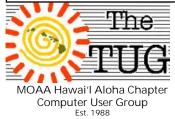Lou Torraca, TUG President 2000-2106.
President Emeritus 2017.
Thanks for your service and best wishes in your retirement an being an observer at future meetings.

Pauline (aka Polly) also left us by re-locating to California. She was supposed to be in attendance at the February session but didn't show due to a communication flap.

Early on she had told me she'd be at the meeting but later informed the new President that she would be unable to attend since her car would already have been shipped. So the disappointed group wished her a pleasant trip and happiness in her new digs.

I was able to contact her and deliver the present we had bought for her and the one Lou gifted her. Her label reads:
Pauline A. Leigh TUG Secretary/Treasure 2004-2016

MOAA Hawai'I Aloha Chapter
Computer User Group
Est. 1988

Last meeting I demo'ed a Windows utility named Winaero Tweaker.

A free application that let's users customize and personalize their copy of Windows 7, 8.1 or 10.

Tired of the word Shortcut showing up on your Desktop every time you create a shortcut? Remove Shortcut Arrow. Get rid of both with a few clicks using WinAero Tweaker.

Change background colors; change colors of Title bars; change Boot options; disable Cortana and Windows Defender effortlessly.

Winaero has a File Explorer look with all the items that can be manipulated in the left pane. Click on any one and you'll get a detailed, and I mean, *detailed* summary of what the change will do. With a link to show in detail how this tweak works.

Along with the details Winaero shows the many steps involved within the Windows Registry required to make this change. Winareo does it in a few clicks.

If you don't like the results, there is a Reset button to restore the previous settings.

Check this out, and download at winaero.com

Duolingo, Babbel and more language and translation online sites are on the agenda for the March meeting.
Attending - n'est-ce pas ?

Meet Kathy

Kathy Ebey is our new Secretary and Treasurer.

Born and raised in South Dakota. Graduated from Univ. of Maryland '68,and was first woman to earn a degree in Physical Distribution Management (Transportation) from UMD. Married to Jack, a retired Navy Supply Corps CDR. Worked as Navy civilian for over 30 years, the last 23 here at COMPACFLT (then CINCPACFLT) as Military Manpower Analyst. Retired in March '03. Hobbies are bonsai and reading. Volunteers at the USS ARIZONA Memorial Visitor Center. Has a 14 year old Papillion named Saba. Has extensive experience being a Club Treasurer. And is the Coordinator for the Neighborhood Security Watch Program for Newtown Estates Community Association (2500+ homes).

Be sure and great Kathy at the next meeting. She'll be glad to meet you and take your membership fee.

Spring clean your PC in 5 simple steps and prevent malware

Unlike classic cars or fine wines, software will not improve with age. That vintage operating system you're happy with because 'it works just fine' is the ultimate weapon for hackers looking for easy access to your files. Cyber criminals frequently and automatically scan websites and PCs with different types of malware to see if there are any vulnerabilities they can use to gain entry to that website or system. Outdated programs are the ultimate back door to your computer.

Not all hacks happen to business systems. In fact, targeting multiple individual users can actually be more lucrative for malware developers. Consider: How would you feel if your precious photo collection or work documents were at risk of being destroyed forever unless you chose to pay up? Consider the following 5 simple steps to spring clean your Windows PC. (*I have included a free program for each in parens should you need one.*)

1. Remove unused software (*GEEK un-installer)* Over time you've probably acquired quite a few applications that you're no longer using. You know the programs, like that trial CD burning program you downloaded to make your Granny a copy of the latest Michael Bublé album. Consider these apps the moldy leftover cheese rotting in the back of your fridge you forgot were there.

Delete them all. You won't regret it and if you need these programs again in the future, you can always download up-to-date versions. Aside from acting as backdoor access points for hackers, these programs take up space on your computer and slow it down. Who needs to scroll through 100 unused programs just to get the one you actually need?

2. Install all system and software updates (*Personal software inspector*) You're sitting at your computer and one of those little icons pops up alerting you to the fact that, yet again, you need to update another program. Constantly installing and updating your software may seem painful, and you may wonder why Windows needs to be updated every couple of minutes (or so it seems), but the cost of ignoring them may end up being much higher than the 2 minute restart that is required. So, why are updates so important? Because they address important changes to the program such as:

Security Vulnerability Fixes: More than 90% of software and operating system (OS) updates are to patch security vulnerabilities in programs. Bug Fixes and Product Enhancements: The best reason to keep software updated is to address security holes in programs, but it's also nice to have the latest features to improve your program's performance.

3. Do a malware scan (*Avira anti-virus/anti-malware scanner*) If you haven't got one already, make sure to install an anti-malware program

4. Back up your system

(*AOMEI Backupper Standard*)

While it can feel a little like having your car serviced – you know you should do it, but don't as often as you should — regular backups stored on a disconnected device really are the best defense, particularly against ransomware attacks. Ransomware will often explicitly target backups which is why it is important to store them where they can't be readily reached. In general, there are two options:

A.External hard drives are a

good option as they can be kept physically disconnected from your computer and locked away for safekeeping. However, if it remains plugged in, it is as susceptible to ransomware as the hard disk of your computer. So keep your backup separate. Keep it updated. And consider encrypting both your computer's hard disk and the portable one while you're at it.

B. Backing up online using a cloud service is a convenient option that will also protect your data in case of theft, damage or other physical threats. There are many reliable options such as CrashPlan, BackBlaze, Carbonite or MozyHome. These programs will run in the background, updating your files in the programs web storage. Keep in mind this option usually requires a monthly fee and the first backup can take quite a long time, particularly if you have a lot of files accumulated over the years.

An external disk drive detached from your PC gives you the guarantee that while it is not attached to your computer it can't be accessed. A cloud based file storage will auto-save in the background and can be disconnected by logging out. But regardless of your chosen method, regular (preferably daily) backups are still the best insurance policy against ransomware attacks.

5. Maintain a quality anti malware solution on your system (*MalwareBytes*)

Your first line of defense should always be an up-to-date PC security suite. Having an anti-malware solution that will monitor program behavior and catch any online threats, including ransomware, will create extra layers of protection. The important thing is that you pick the one that caters to your individual needs.
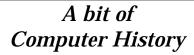

In summary: ultimate protection requires a layered approach While these tips may seem obvious, you should ask yourself: do you really do all of these things on a regular basis? Start your digital 2017 on the right foot and spring clean your computer with these easy steps, and just to be clear: you don't need to wait until next Spring to revisit them.
Have a great (malware-free) day!

Aloha,

Lou and in spirit Pooky

A bit of Computer History

First computer program to run on a computer

University of Manchester researchers Frederic Williams, Tom Kilburn, and Geoff Toothill develop the Small Scale Experimental Machine (SSEM), better known as the Manchester "Baby." The Baby was built to test a new memory technology developed by Williams and Kilburn -- soon known as the Williams Tube – which was the first electronic random access memory for computers. The first program, consisting of seventeen instructions and written by Kilburn, ran on June 21st, 1948. This was the first program to ever run on an electronic stored-program computer.

The Complex Number Calculator (CNC) is completed.

In 1939, Bell Telephone Laboratories completes this calculator, designed by scientist George Stibitz. In 1940, Stibitz demonstrated the CNC at an American Mathematical Society conference held at Dartmouth College. Stibitz stunned the group by performing calculations remotely on the CNC (located in New York City) using a Teletype terminal connected via to New York over special telephone lines. This is likely the first example of remote access computing.