The

PULP

Newsletter of the Hartford User Group Exchange

http://www.huge.org Volume 39 Issue --06

JUNE 16th General Meeting:

Gift Suggestions

Rev. Fleming Hall
2533 Main Street,
Glastonbury, CT

Q&A Session: 7 PM–7:15PM
Meeting starts at: 7:15PM

H.U.G.E

UGC

Apple User Group

Member of apcug

An International Association of Technology & Computer User Groups

The **PULP** is published monthly by and for members of the Hartford User Group Exchange, Inc. (**HUGE**). **HUGE** is a nonprofit organization whose aim is to provide an exchange of information between users of personal computers. The **PULP** is not in any way affiliated with any computer manufacturer or software company.

MEETING LOCATIONS

Rev. Fleming Hall
2533 Main Street,
Glastonbury, CT

From The Editor

by Stuart Rabinowitz

I missed an important computer (40th anniversary) milestone last month, on May 21, 1980 testing began on Pac-Man. it would be released for the holiday shopping season.

This month is Gift Suggestions. I hope we are able to meet in person. Otherwise, we will be meeting on-line again. Given the issues we've experienced with 'Free Conference Call', I've begun experimenting with 'Google Meet'. APCUG has offered the use of their 'ZOOM' license. Will let you know. If you have a preference, let me know.

In the News: COBOL programmers are in demand to fight the coronavirus pandemic, it seems many critical software systems in use by state governments (including unemployment compensation) are in COBOL.

The latest update to iOS contains COVID-19 contact tracing, but it is op-in and you have to turn it on. Apple publishes Maps mobility data to aid COVID-19 struggle

Ransomware deploys virtual machines to hide itself from antivirus software. A cybercrime store is selling access to more than 43,000 hacked servers. Ransomware Gang Demands $42M or It Releases Trump's 'Dirty Laundry'_

Hacker leaks 40 million user records from popular Wishbone app

Devastating Bluetooth flaw leaves millions of PCs open to malicious attacks Thunderbolt flaws affect millions of computers – even locking unattended devices won't help

A recent Windows 10 update is crashing systems and hiding files

Wink (a smart home platform) switched to a mandatory subscriptions of May 20.

Shade (Troldesh) ransomware recently shut down and released all of its decryption keys

A new MacBook with first ARM chip is coming

Send your comments to editor@huge.org

Until next month…Happy computing!!

A Little Computer Quiz

1 One of the earliest home computers to have color without a color graphics card was what computer?

2 How was this accomplished?

3 Actually, the same method was used by an earlier home entertainment system. What system was it?

4 Who came up with the process?

5 What was the first home video game console & who designed it?

May Quiz Answers

1 CAPTCHA is an anagram of what phrase?
A completely automated public Turing test to tell computers and humans apart

2 Who coined the term?
A Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford

3 When was it coined?
A 2003

4 When was version 1.0 first invented?
A 1997

5 GIT was developed b y Lins Torvalds as a means of of source control management and distribution for open source software. But it wasn't the first, what was the first?
A Source Code Control System (SCCS) released in 1972. GIT did not appear until 2005

Video Conferencing for Clubs
Author: Dick Maybach, Member, Brookdale Computer User Group, NJ
www.bcug.com
n2nd (at) att.net

Many clubs have periodic general meetings, often with refreshments, speakers, and perhaps demonstrations or hands-on activities. The social interactions here, including the welcoming of prospective members, are vital for the organization's health. Equally important are the committee meetings that support the organization. Here, much smaller groups, whose members know each other well, plan the club's activities, and it may be more efficient to conduct some of these as video conferences, which would eliminate the associated travel. There is a major caveat: teleconferencing is ineffective if there are tensions within the group. Meet in-person to discuss a controversial issue.

There are two popular free services suitable for meetings of small groups: Facebook Messenger (http://www.facebook.com/messenger/) and Skype (http://www.skype.com/en/). Both require that participants register for the respective service, and all can be accessed from Linux, Windows, and Mac computers as well as Android and iOS devices. (These free services are provided by for-profit companies, and the usual caveat applies; they can be changed or discontinued any time their owners determine they aren't sufficiently contributing to the bottom line.) If your club outgrows the scope of the free services, most vendors offer for-fee variants with more capabilities. You might also consider inexpensive paid services, such as EZTalks (http://www.eztalks.com/video-conference/) and Zoom (http://zoom.us/). Neither requires that users other than the moderator register for a service, but participants need to install the software. Both have trial versions that limit conferences to 40 minutes, which is certainly adequate for testing.

I'll use Skype as an example, only because I already use it for one-on-one calls. Microsoft is refreshingly open about what it considers fair use (http://www.skype.com/en/legal/fair-usage/). In particular, "Group video calls are subject to a fair usage limit of 100 hours per month with no more than 10 hours per day and a limit of 4 hours per individual video call. Once these limits have been reached, the video will switch off and the call will convert to an audio call." See the above URL for the other, quite reasonable, limits.

Skype's interface varies with its version and your hardware and software; as a result, what you see may differ somewhat from the screenshots here. Figure 1 shows Skype's opening screen, after the user has selected the *Chats* icon toward the upper left, and it shows one of Skype's puzzles for new users. My name appears at the upper left, but you must contact me by my Skype name, which is "skype,alias" and appears towards the bottom right of the welcome screen in the sentence, "You are signed in as skype.alias." (If you are not on the opening screen, find your Skype name by selecting the three dots to the right of your name at the top of the left panel, and then "Settings" followed by "Accounts & Profile.) Skype names are unique, but a search on a person's given name will likely produce dozens of hits.

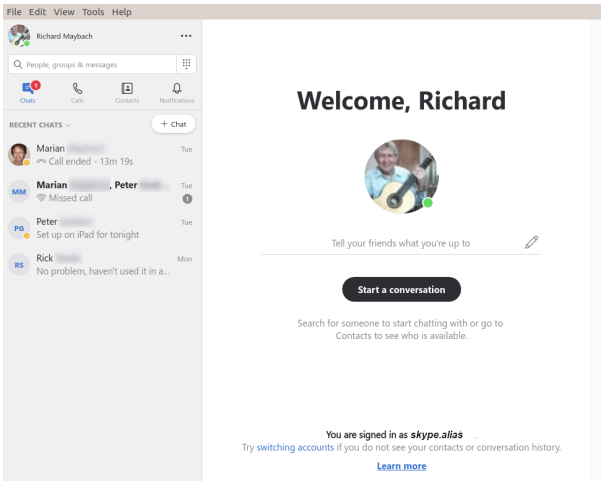

Figure 1. Skype Opening Screen.

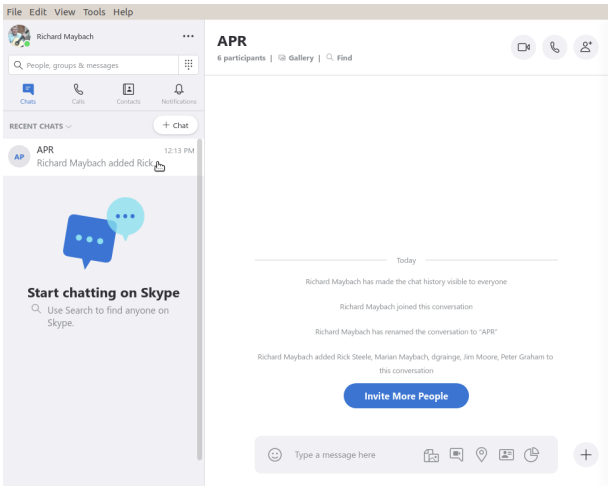

Figure 2. Define a Group Chat.

To communicate with someone you must first add their name to your contact list. Select "Contacts" in the menu bar toward the upper left, then select the + button; enter their Skype name, and select the associated Add button. This will work only if they have enabled "Appear in search results." (Go to Settings as above, then "Contacts" and "Privacy" to make this choice.) Many Skype names have the form "live:.cd.6f73e115260c0804", and sometimes searches using the full name fail, but succeed if you delete the "live:.cd." prefix.

Skype is different in that the moderator places a call to the participants, while other services require that the participants call into a conference. The set-up procedure varies with the version, and in Linux, it's done by setting up a group chat. Select "Chats" in the menu bar toward the upper left and the "+ Chat" button, and finally "New Group Chat." The result is in Figure 2. Select either the round button at top right, or "Select More People" toward the bottom, and add participants from your contact list. Selecting the camera icon at the upper right will start a video conference, and selecting the handset icon a voice conference. As the call begins, you will have an opportunity to ring the participants to alert them, which is probably a good idea.

Although Skype conferences can be as large as 50, at most 10 of these can be transmitting video. This isn't as restrictive as it may sound, as the audio participants still see the video. The screen is tiled, with a pane dedicated to each active video participant. As a result, each added participant reduces the size of all the others. Participants can disable their microphones to reduce the background noise and can also disable their cameras, using icons toward the bottoms of their screens, but these appear only when the cursor is active and on the Skype window. When disabled, a diagonal line appears on the associated icon. There is also a red handset icon here to terminate the call.

Skype's interface varies with its version and your hardware and software, which may make it difficult to introduce to your organization. Expect your first conference to be awkward; even those accustomed to one-on-one video calls may find it confusing. You will most likely want to hold practice sessions, but the effort is worthwhile as there is much to gain. Replacing a face-to-face meeting with a video conference means a 20-minute meeting lasts just 20 minutes, instead of 30 to drive there, 20 to meet, and 30 to drive home, perhaps in ugly weather or traffic.

- Staying Safe Online - A Rational Approach
- Pam Holland, Founder and President, Tech-Moxie
- December 2019
- https://www.tech-moxie.com/
- Pam (at) tech-moxie.com
-

We get *many* questions about online security. And we often get brought in to help clean up after an incident of fraud. As a result, we have developed what we consider 'a rational approach' to online security. Rather than focusing on all of the possible risks, we urge our clients to first address factors that present the highest risk. With respect to protecting from online risk, we apply the 80/20 rule. In short, 80% of the risk comes from 20% of the possible causes. In other words, if we just address the top possible risks, we eliminate the most common ways people are victimized online.

We suggest thinking about protecting your data as you might approach protecting your home. We all take reasonable steps to secure our homes; we lock our doors, close windows, and leave lights on. The goal is to *reduce* risk as eliminating risk is nearly impossible. The same is true in our digital lives. Taking small measures goes a long way towards keeping us safe, but it is nearly impossible to eliminate all risk.

Consider your personal risk factors. This is not unlike assessing your home for the risk of a break-in. If you live on the top floor of a high-rise, leaving your windows open does not present the same risk as if you were on the ground floor. With respect to your tech, do you have people regularly in your home that you need to protect your data from? Do you bank online? Do you have sensitive financial or other documents on your computer? Do you only use your computer for email? Do you or a family member have cognitive issues that might make you more vulnerable to fraud?

Based on our experience seeing the aftermath of fraud, taking steps to cover these six items will go far towards your online safety:

- **Use Unique Passwords.** I know this isn't what many want to hear, but unfortunately, the risk in re-using the same password is increasing. A few years ago, the common advice was to create a unique password that was hard to guess. Today, the risk is not that someone will guess your password - the fraudsters already know it. Large corporate data breaches (e.g., Equifax and Marriott) may have put our passwords into the hands of fraudsters. If you typically use the same password for multiple accounts (and worse if you have used it for years), fraudsters are more likely to be able to access your other accounts. To return to the home analogy, it is as if you have given out your key to numerous people over the years - it's now time to change the locks. Some options:
  - **Use a password manager** - This might mean allowing Chrome or your Mac to save your passwords or using a third-party service like LastPass. I am often asked if they are safe. The only answer that I can really give is that they are safe until they aren't. I have chosen to allow my passwords to be saved on my Mac. For me, it has reduced my risk (because I don't need to reuse passwords) while (somewhat) saving my sanity. *But a caution: If others have access to your computer, they may be able to view your passwords.*
  - **Write them down** - This works well for many. Of course, it is important to keep the passwords in a safe place.
  - **Develop a unique naming convention** - For example, you might take a short

phrase that you will remember then add something unique to that account site.

- **Make your passwords safer by using two-step authentication** - This is an option in most online accounts (email, Facebook, banking). How does it work? When you log in from a new device or location, you'll be sent a code via smartphone or landline. This makes it harder for fraudsters to log into accounts even if they have your password. To set up, go to the account or privacy/security settings in your online accounts.

- ***Never* Allow Remote Access to Your Computer** (unless you have sought reputable assistance like from Tech-Moxie 😉). Fraudsters would like nothing more than to gain access to your computer. They pretend to be from Amazon, Microsoft, Apple or another company you know well, offering to "help" you with a service issue. Assume fraud if you get an email, call or computer alert from a familiar company or government name. Once in your computer, they can access accounts and passwords. We have seen quite a lot of damage from these schemes.

- **Think Before You Click.** Assume links in the email are fraudulent unless you can prove otherwise by checking with the sender. Fraudsters easily create emails that look like they came from a friend, bank or even the government. The email might be friendly (*"Hey, check this out"*) or intended to provoke anxiety (*"your Amazon order for a diamond ring has just shipped"*) or seemingly innocuous ("*your computer needs service"*). Fraudsters are hoping to get passwords or other personal information. Remember, customer service doesn't come to you! Instead of clicking, go to the website directly via the internet.

- **Beware of Pop-Ups** A "pop-up" is a window or box that opens on your computer - often with a warning. Do not believe pop-up warnings claiming there is a problem with your computer. Never give them remote access. Warnings may claim to be from Microsoft, Apple or another company you are familiar with. What to do? Shutdown and restart your computer and the pop-up should be gone!

- **Update Devices Regularly.** Companies like Microsoft, Apple and Google lookout for software vulnerabilities that fraudsters can take advantage of. They issue updates to fix these issues. Some devices may be set to automatically update, but others may require you to take a specific action. This applies to computers, tablets and smartphones.

- **Beware the Telephone.** Scams change but follow common themes. Neither Apple nor Microsoft will call to alert you of problems. Government agencies such as IRS, Social Security Admin nor the local Sheriff will call claiming you owe money. If you are still in doubt, hang up and call the agency from a number that you have looked up independently.

- We hope you find these tips helpful - and as always, we are here to help!

Wi-Fi Security – Which one, WEP, WPA, or WPA2?
Author: Phil Sorrentino, Contributing Writer, The Computer Club, FL
October 2019
www.scccomputerclub.org
Philsorr (at) yahoo.com

Well, it finally happened. I tried to add another device to my home Wi-Fi network and I couldn't. I have been in fear of this happening for the last few years. No, it is not the fact that I tried to add one more device and that went over a limit. The limit on the number of devices you can have on a Wi-Fi network is only limited by the local IP addresses you set up, which was much higher than the number of devices I had on the network. I have had my current Router since July 2010. I bought it shortly after the 802.11n standard found its way into reasonably priced routers (around 2009). The "n" version followed the "g" version and increased the bit rate (speed) from about 50mbps to somewhere in the 100 to 300 Mbps area. (The actual speed you get from the router to a device is dependent on many things.) When I set up the Router I had a few older (legacy) devices that I still used. Some of those older devices didn't support the latest Security. So when it came to set up Security for the network, I chose the older Security standard "WEP." Although WEP is not nearly as secure as WPA2, every device supported WEP so there was no problem, until today, when I tried to add a device that did not support WEP. The new device, a security camera, only supports WPA and WPA2. So, now I have to change the Security used by my Router to either WPA or WPA2. This may not sound like much of a problem, but once I change it in the Router, I have to change every device that wants to use my Wi-Fi network. Yes, all the laptops and tablets, all the cell phones, all the Streaming devices, all the Smart TVs, all the smart bulbs and plugs, the wireless printer, any Wi-Fi extender access points, Alexa, Google Home, and all the phones and tablets owned by friends and family that use my Wi-Fi network when visiting.

The first thing I'll have to do is change the security used in the router. For this, I will need the Username and Password for the router. Many router's Username can be left blank and the default password is typically "Admin." (If you have changed either of these on your router, this is a good time to resurrect the correct Username and Password for future use.) Now, using a Browser, I'll go to the IP address of the router. Many routers use http://192.168.1.0 or http://192.168.1.1. Once at the router page, I'll put in the Username and password. Once in the router setup, I'll find Wireless or Wi-Fi Security and look for the Security type. Then I'll choose the desired Security type and put in a passphrase. I'll make a note of the new Wi-Fi Password for the future (a very important step). Now I can go around to all the devices that use the Wi-Fi and make the appropriate changes in their setups. Wish me luck.

So, what really is Wi-Fi security? Well, directly from Wikipedia "Wireless (Wi-Fi) security is the prevention of unauthorized access or damage to computers or data using wireless networks." Basically, Wi-Fi Security protects the data that goes between a Router and a Device. The device could be a computer, a wireless phone, a smart TV or DVD player, a smart LED bulb, any device that connects to the router, even a smart refrigerator. The most common types of Wi-Fi security are Wired Equivalent Privacy (WEP), and Wi-fi Protected Access (WPA). WEP, which is the older standard (Circa 1999), provides fairly weak security. It is well known that the WEP password can often be cracked within a few minutes with a basic laptop computer and widely available software tools. WEP used a 64-bit (or 128-bit)

encryption key. The key was manually inserted into the device and it remained constant. WPA was introduced around 2002 to solve some of the problems with WEP. Even if your router is six years old, it most likely supports WPA. WPA2 is a further improvement over WPA and is the current Security standard. WPA2 employs an encryption algorithm that encrypts the data with a 256-bit key, the longest of all the keys used, and the longer the key the stronger the security. WPA also employs a per-packet key, meaning that it dynamically generates a new key for each packet that is transmitted. In early 2018, WPA3 was announced. WPA3 will have several security improvements over WPA2, but it will take some time for it to show up in routers and devices.

To use WPA or WPA2, you provide the router with a "passphrase" between 8 and 63 characters long –the longer the better. The passphrase can be a collection of alpha and numeric characters, including special symbols like $, %, and #. (Actually, if you are familiar with the ASCII code, all ASCII printable characters; those decimal values between 32 and 126 can be used. Which, by the way, also includes "space".) The router will then use the passphrase and the network's name to generate unique encryption keys to be used on the network. The keys will constantly be changed to avoid being cracked. WPA2, the second version of WPA uses a more advanced encryption algorithm that is more efficient and more resistant to cracking. (All Wi-Fi products have been required to support WPA2 since about 2016. It was intended that WPA2 essentially replace WPA.) Although it is true that "the longer the passphrase, the stronger the protection, it may not be the practical way to go. A passphrase only 9 or 10 characters in length may be adequate for most home use. I can't prove it, but I have seen some research that showed that it would take a fast PC over 15,000 years to crack a WPA2 passphrase of only 10 characters. (Maybe you could do it in a year with 15,000 computers.) That kind of security would probably be enough for most of us.

So, now that we know what's behind Wi-Fi security, what shall I do about the original problem of what Security selection to use in place of WEP. Well, I guess the obvious answer is WPA2, as long as all devices support WPA2. Unfortunately, I may not find this out until I attempt to have all devices re-set-up with WPA2. I only have a few devices that are older than six years old, so it may just work out. Wish me luck.

Postscript: The upgrade to WPA2 worked out just fine. Unfortunately, about 2 months later I had to replace the router. I had to do the whole upgrade all over again, so now I'm really good at updating all my Wi-Fi devices.

PULP Staff

Editor Stuart Rabinowitz
Distribution George Carbonell

Membership: Anyone may become a member. Dues are $12 per year and includes a one-year subscription to The Pulp. Meeting topics, times and places can be found on page 1 of this issue.

Officers & SIG Leaders

Leader:	George Carbonell	860 568–0492	george.carbonell@comcast.net
Secretary:	Stuart Rabinowitz	860 633–9038	s.e.rabinowitz@att.net
Treasurer:	Stuart Rabinowitz	860 633 9038	s.e.rabinowitz@att.net
Director at Large:	Phil Manaker	860 659-4584	amanaker@earthlink.net
Director at Large:	Ted Bade	860 643-0430	tbade@cox.net
Director at Large:	Stuart Rabinowitz		
Web Manager:	Bob Bonato		bob@bonatodesign.com
Membership:	Martin Ritter		mcrct@cox.net
Integrated SIG:	Stuart Rabinowitz		

		June	2020			
	1 1867 1st description of typewriter	2	3	4 1979 1st demo of VisiCalc	5	6
7	8 1979 The Source goes online	9	10	11	12 1967 1st issue Computerworld	13
14	15	16 General Meeting 7 PM	17	18	19	20
21 1948 1st stored program run	22	23	24	25 1974 TI patents Datamath calculator	26	27
28 Tau Day	29	30				