DATALINE

SCV COMPUTER CLUB

Published by Santa Clarita Valley Computer Club … We're User Friendly **Volume XXXI, Issue 10**
Serving the Santa Clarita Valley, CA since 1988 **Editor: Judy Taylour**

Bella Vida
SCV Senior Center
27180 Golden Valley Road
Santa Clarita 91350
2nd Monday of the month
6:30 – 9:00 pm

In This Issue

October 14, 2019 – 6:30 pm
It's going to be a Zoom meeting!

Protecting Your Digital Life

Between ransomware, data breaches, cryptojacking, supply chain attacks, and mobile malware, it's never been more important to protect your digital life.

avast

Welcome to the Information Superhighway with Bob Gostischa, IT security expert and Avast Evangelist.

Staying secure and guarding as much of our privacy as possible is a constant challenge. Between phishing, scams, ID theft, ransomware, data collection, and mobile malware, it's never been more important to protect our digital life. Our security and privacy are constantly in danger of being attacked from many sources and Bob will explain the importance of guarding our online presence. This presentation covers how we can protect our presence on the web as well as our computers (Windows and Mac), tablets, smartphones, and other smart devices.

He will also share what he uses to keep his computers and smart devices as well as his connected Internet of Things devices secure.

We'll also learn about Omni, a powerful online security solution that offers three dimensions of comprehensive protection, including: Home network security for all of the IoT connected devices in your home. On-device security for Windows, Mac, Android, and iOS devices. It was released in August. We'll be the first group to have a presentation on the app.

We'll be able to see each other, if you have a web cam – if not, we'll see a silhouette. We'll also be able to talk to each other. We did it in February and had a good time.
If you have Avast stuff (hat, t-shirt, etc.) please wear it!

President's Corner
Security is Important - Why Does it Take So Long (and Cost So Much)?
Author: Greg Skalka, President, Under the Computer Hood User Group, CA
October 2019 issue, Drive Light
www.uchug.org / president (at) uchug.org

I am a technology user. I use all sorts of tech products, applications and services. I have laptops, desktops and Chromebooks. I have mobile devices - smart phones and tablets. I have home Internet access and I access the web from other places as well. I have a home network and I have smart home devices (cameras, TVs, voice-controlled assistants, smart lights and appliances). I use lots of software. I search the web, bank and buy things online and send emails and texts. I'm not much for social networks, but I do appear in posts by others, especially my wife. I've got a lot of the things a typical middle-class American would have.

I use a lot of technology, but all I want to do is use it. I don't want to have to struggle to make it work, fix it or spend a lot of time and money keeping it working safely. I want it all to work every time as I expect it to work. Unfortunately, there is a lot more to our tech lives than that. None of the tech revolution we have seen in the last decades would have been possible without money. It is commerce, capital and the desire to make a profit that brought us most of this, including Microsoft, Google, Uber, Tesla and all the rest. Some key government investments in technology, in the space program, DARPA and the military-industrial complex helped with fundamental research, but the capitalist entrepreneurs filled in the rest. Money made tech great, but money also made it unsafe.

Entrepreneurs take legal risks to gain rewards; criminals try to find the least risky ways to make money, legal or not. Each new tech device, app or service that comes out is studied for vulnerabilities by the criminal elements intent on exploiting it for monetary gain. Now that technology has interconnected the world, we can be the victims of crime originating from all over the globe. Even nation states can get in the game, trying to steal information for economic and political purposes.

All this leaves the poor tech user vulnerable. The rapid rate of change, the ease of use and ubiquitousness of these product and services just add to the risk. How does a user evaluate the threat and defend against it? Is it all worth the cost?

The criminals are out there, ready to hack, snoop, steal and deceive. They want your personal information to steal your identity and your passwords to steal your money. They want to trick you into sending them gift cards and Bitcoin. Who is going to protect the tech user from all the cyber threats? Can the government protect us? Laws may be passed, regulations put in place and enforcement attempted, but citizens are still victimized. Unfortunately sometimes the government is part of the problem, not protecting the sensitive data we entrusted to them.

Can the companies we buy products and services from protect us? Their desires for profit over all else have created some of our tech problems. They will sell us devices that are not secure if they think it makes business sense. They'll collect and monetize our personal information and then often fail to protect it adequately. It seems we as tech users must find ways to protect ourselves, as no one else will take responsibility for our security. Unfortunately, that means additional costs in terms of money and time are

required to keep our assets (money, identity, personal safety) secure when using all these tech items and services in the new global digital electronic world.

There is no practical way to remain 100% secure in our modern connected world. Even if you turn off all of your devices, disconnect them, put them in a box and seal it up (and cancel all your related services), you are not safe. The government still has your personal information, and even if you are not on Facebook, others could post about you. You will have to go back to paying with cash, shopping and banking in physical locations and communicating through personal visits and letters. Unless you want to step back into the 1950's, you will have to adopt some additional safeguards with every new tech item you acquire.

Safety as a tech user is not an absolute, but a matter of degree. More time and money spent to safeguard our activities will provide more relative safety and security, but trade-offs will need to be made. More security comes at a higher cost and usually a greater inconvenience as well. A user can make their tech life more resistant to attacks by cyber criminals and become more resilient should bad things happen, but it will require more time, money and effort on their part. Lots of articles are written about protecting ourselves online and describing precautions we all should take, yet cybercrime is still prevalent.

I think I take care of my tech household pretty well, though there is always more that can be done. The things I value most (finances, identity, property) I protect the most, while things of a lesser consequence I am a bit looser with. In some ways I probably go overboard in caution, but there are probably some risks I don't take as seriously as I should. I'm pretty careful with physical security, using strong passwords, encryption, a VPN and two-factor authentication where appropriate.

I'm pretty resistant to social engineering threats and am very careful with my personal information. Exercising care and vigilance online is good, but it requires effort and some investments. I have several laptops and desktops that my wife and I use, as well as a couple of Chromebooks. All the computers we regularly use run Windows 7, so I am presently working towards replacing at least some of them with Windows 10 computers ahead of the Windows 7 security sunset in January 2020. This considerable cost in new hardware and software and in time to set everything up is strictly due to Microsoft's desire to make Windows 7 obsolete; I would be perfectly happy staying with Windows 7 otherwise. I'll be spending money on new systems, probably buying new software and spending time teaching my wife how to use the new OS. I'll probably compromise by keeping a couple of old Win7 computers or laptops to run software I can't convert to Win10 or don't want to spend more on. I still have a Windows XP computer that I keep off-line to run certain programs. I'm actually writing this article on it; I've yet to find a Microsoft Word version I like overall as much as version 6.

Even when security updates are provided for free, our time is usually required to oversee their installation. If nothing else, the time required to install updates represents time we are unable to use our devices. While Windows 10 may force automatic security updates, they can wind up being applied at the most inopportune times. I don't mind as much the automatic updates my Chromebook gets from Google, as they are downloaded in the background and quickly applied on the next power-up.

In addition to computer updates, our network items often require security patches. Few users may pay much attention to updates for their routers, however, unless they are alerted somehow. I have a Netgear Orbi mesh Wi-Fi router, which I love for its performance and ease of use (but not so much for the initial cost). Because I'd registered the product and downloaded their app, I recently received an email that an update was available for my router's firmware. I initially tried to apply the update through the app (on my smart phone) but was unsuccessful. I was able to enter into an online chat through the app with their tech support, and thus began a two-hour process to finally get my router system updated.

I assumed I would be able to easily update through the Orbi app, but the support tech told me my installed firmware version was too old, and I instead would need to download and install an intermediate version from a web link. I find the small screen of a phone too difficult to use for this kind of activity, so pulled out a Chromebook, logged into my Orbi router and went to the web link. This also allowed me to keep the support chat going separately through the app on my phone.

Once I got to the web link, I found I would be downloading a zip file. There may be ways to unzip on a Chromebook, but I don't know them, so I switched again and logged in with my Windows laptop. The support tech said to apply the update first to the satellites (my mesh system consists of one router and two satellite units) and then to the router. The update page was a bit confusing, and I inadvertently updated the router first. Fortunately I was still connected to the tech support person, so after a number of additional steps, I successfully updated all components.

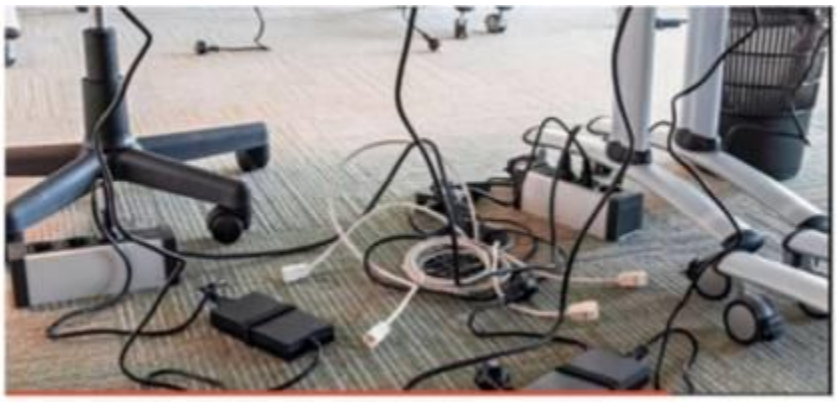
It is almost time to renew my anti-virus, and I need to make some decisions about it. I've been using ESET Internet Security for many years and really like it (and think it protects me, but who really knows). I'm not sure what I should use going forward on Windows 10, as I've heard that Microsoft's Win10 built-in protections are as good as anything else, and obviously are at no extra cost. I always buy ESET on sale ahead of when I need it, so I already have new copies to put on my Win7 computers. That seems like a waste, as I won't have these computers on the Internet past January. Still, I shouldn't cut corners on protecting my online banking computer, at least until I am switched over completely to Windows 10.

Though I may be spending a lot of time and money getting my new computers set up, it hopefully will increase the odds that I'll have secure systems that will help protect my data.

Making Your Tech "Fit" – Cords, Voice, Sound, and other hazards

Author: Debra Carlson, Technical Advisor, CVC Computer Club, CO
Q4 2019 issue, Tech-Notes
cvc.computer.club (at) gmail.com

Cords – Whether tripping or kicking (and disconnecting) them … or getting the contents of your desktop lost in the shuffle … cord / cable management is both a convenience and a safety issue.



Some basic principles:

- Label each Cord you plug into your outlets / surge devices.

Hint: When you get a new device, unplug the power cord from the device and attach the outlet end of the new device to this with a twist tie (or tape). Pull the old cord from the outlet end and it will fish your new cable to the surge strip or outlet. This doesn't work in a "mess of wires" but is good for many setups.

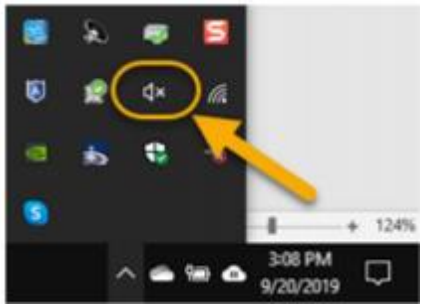
If you have many peripherals intermittently connected to your machine (a couple of cameras, a scanner, an external drive), consider a cable management "toy" for that as well.

Voice – You may have a microphone built into your webcam (or the webcam in your laptop), part of a headset, or a separate microphone. Settings are most often tested in an app that uses the microphone (e.g. Skype). External units may connect to your machine by audio jack, USB cable or Bluetooth (wireless). Two things are important:

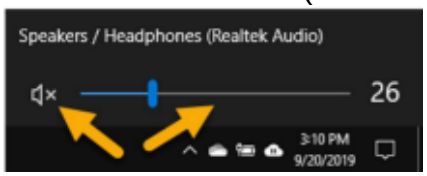
1. Train transcription software completely if you use it. It will help minimize errors in the text.

2. If you are using this for dictation, assume there are going to be errors! Check for them … this will help avoid embarrassment over the messages you may send.

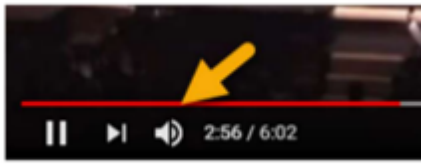
Sound – The biggest issues with speakers – USB, audio jack, Bluetooth, or Wi-Fi is accidental muting. This may happen on the speaker – especially if the on/off switch is a button rather than a knob control OR …



Your sound is muted (see the X next to, or on top of the megaphone)



If not muted, the volume may be too low.



Your YouTube or other video may need either unmuting or volume adjustment (YouTube shown).

You may need to adjust the speaker volume AND the volume of the audio/video – setting both of them to maximum can interfere with sound clarity.

Other hazards

- UPS units and surge/power strips can be great, but many have on/off switches. Be sure your unit is not in a position where it can be easily kicked (or hit) – and shut off.

- All computing devices can overheat. Have circulation space -- at least a couple inches each side on a tower, and if you have a laptop that lies flush on a desk, consider a cooling pad or other prop (I like bread cooling racks – right height and size).

Old program CDs make good drink coasters, wind chimes, or decorative hangings / picture frames. A couple ideas to make your desk area manageable and clear some clutter.

Interesting Internet Finds – October

Author: Steve Costello
scostello (at) sefcug.com

While going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members. The following are some items I found interesting during the month of September.

The following are some items I found interesting during the month of September 2019.

How To Reinstall Windows Without An Installation Disc
https://askleo.com/how-to-reinstall-windows-without-an-installation-disc/
This question comes up all the time at user meetings. Leo Notenboom provides several excellent answers. Basically everything he says in the post boils down to being ready before the need comes up.

Is Linux Really Immune To Viruses and Malware? Here's the Truth
https://www.leetvofficial.com/is-linux-really-immune-to-viruses-and-malware-heres-the-truth/
Linux is becoming more popular now, especially with support for Windows 7 coming to an end. Before you switch you should be aware of the virus and malware issues.

Microsoft Proves It's For the People by Adding an Emoji Button to New Keyboards
https://www.reviewgeek.com/25262/microsoft-proves-its-for-the-people-by-adding-an-emoji-button-to-new-keyboards/
Amidst all the noise surrounding the new Surface devices that Microsoft unveiled last week, the company apparently announced a pair of new keyboards that have two new keys: one for Microsoft Office and another for emoji.

4 Things To Look For When Buying A USB Hub
https://www.maketecheasier.com/things-look-out-for-buying-usb-hub/
There are still a lot of USB devices around, and less USB ports on computers these days. If you don't have enough ports on your laptop, or desktop, you will need a USB hub. This post tells you what you need to look for to make the best purchase. (Note: I have several hubs that I use often.)

How To Optimize Your Google Drive Storage
https://www.online-tech-tips.com/google-softwaretips/how-to-optimize-your-google-drive-storage/
If you use Google Drive storage (and if you have a Google account you should) it should be optimized. This post explains how to optimize the storage.

Encrypt Public Wi-Fi With Firefox Private Network For Secure Connection
https://www.ilovefreesoftware.com/12/windows/internet/plugins/encrypt-public-wifi-with-firefox-private-network-for-secure-connection.html
If you use Firefox there is now an option to have a free, secure connections. Check out this post to learn all about it. It is not the best option but is better than no VPN at all.

You Probably Don't Need a Screen Protector
https://www.reviewgeek.com/24991/you-probably-dont-really-need-a-screen-protector/
Screen protectors are sold as a necessity, but they're not as useful as they used to be. In fact, ditching the screen protector can save you money and make your phone more pleasant to use.

****

Wi-Fi Security – Which one, WEP, WPA, or WPA2?
Author: Phil Sorrentino, Contributing Writer,
The Computer Club, Florida
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 pass phrase 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-setup 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.

Review: MailWasher Pro – Another Level of Protection
Author: Jim Fromm, Editor / Webmaster, MOAA-The TUG, HI
October 2019 issue, The TUG newsletter
www.the-tug.org / editor (at) the-tug.org

Our September meeting was mostly Q&A; one of the questions received via email was about MailWasher Pro. I am going to save some keyboard clicks and refer to it as MWP. It is a utility that lets you look at the headers of all the emails in all of your mailboxes before downloading. It is very useful if you have multiple mailboxes. I have 12 email addresses, (don't ask), and eliminates the ads, solicitations, requests from Amazon for reviews, etc. before they ever make it into my mail program. Besides saving space, it decreases the chance of getting bit by malware. Here's a portion of the opening screen.

You have three immediate choices. Check for new mail, Wash (delete) mail and Select the mail program you want to use. Messages are listed in order received (default) or you can click on the title bar to separate them to your liking. Clicking on the box in the Delete column will select those emails for deletion. When you've finished picking the ones you don't want, click on the bar of soap icon. They will be deleted from the listing—but—like a bad penny, they are not completely gone. The messages are moved to the Recycle bin and will remain there until you clean it out.

If you want to recover one, or more, or those in the Recycle bin, merely right click on the email and select Restore. You'll need to have designated an email address to send them to. They will be sent to that address and show up in MWP again.

After you've decided which ones go and which ones stay, click on Mail Program. Your designated mail program will launch and download the mail into their respective Inboxes.

- If you've signed up for a number of ezines that you no longer want and have been unable to unsubscribe, click the box in the delete column.
- If you receive emails urging you to verify your subscription, for which you've never signed up for, click the box.
- If you get email from companies offering you discounts on products that you're never going to buy, click the box.

Simple as that.

You can mark messages as spam and block them via sender, and even domain.

Avoid viruses, spam, junk mail and other pesky emails with MWP. Works with all email programs. I use Outlook 2019. Set-up is easy; MWP will import the settings for your existing email accounts.

Now, here comes the part that will turn some of you penny pinchers off. MWP is not free. The initial one-year subscription costs $29.96 and can be used on three computers, including your mobile devices. Renewals are $24.95 per year, three computers. I just renewed with a 2-year renewal for $43.16. I've been using MWP since version 1, they are now into version 7.

Hooray!!, there is a free 30-day trial version. You can use it with full functionality for 30 days and then, subscribe or take your chances and do without it.

Travel to https://www.firetrust.com/products/mailwasher-pro# to get the trial version or pay to help the authors.

Smartphone Map Apps vs. Dedicated GPS Devices
Author: Dorothy Fitch, Editor, GVR Computer Club, AZ
October 2019 issue, Greenbytes
www.ccgvaz.org / newsletter (at) ccgvaz.org

public domain image from pxhere.com

I recently heard an interesting report on a local television station about the pros and cons of using your Smartphone vs. a GPS device to find your way when you travel. I am

certainly not an expert on this topic but wanted to share a few things I discovered as well as some links so that you can learn more, too.

I hadn't really thought about it, but perhaps the biggest difference between the two is that Smartphone map apps use cell tower signals to provide your location and generate maps. GPS devices, such as Garmin or TomTom, use satellites for positioning.

What this means is that if you are in a remote area that doesn't have cell coverage, maps on your phone will likely not work.

Other interesting considerations:

GPS devices are more accurate—to within 15 feet your location— because they are using satellite technology.

Smartphone locations are accurate to about 164 feet. Your location is determined by triangulating signals from several cell towers.

A Smartphone app uses your phone's battery (though you may be able to charge it in your car via USB). Beware, however, that on a recent trip, my Android phone was plugged in. During the half-hour trip, the phone's battery level dropped by 4% because the power used by the app was greater than the rate of charging.
A GPS device will plug into your car's cigarette lighter or USB port.

Using a GPS device will leave your Smartphone available for other purposes (though not when you are driving, of course!).

A Smartphone app will use up mobile data, which may be of concern if your phone service doesn't include an unlimited data plan.

GPS devices often come with a way to mount them to your dashboard, which makes it easier to check your route.

The Google Maps Smartphone app gives you up-to-the-minute accident reports. It even prompts you to respond as to whether the accident someone reported earlier is still there. It provides an estimated time delay, as well as alternate routes.
Some GPS devices offer traffic alerts as well.

Using the Google Maps Smartphone app, I was surprised one time when I entered the address of my destination, which was a store. I got immediate feedback that the store had already closed for the day. Very useful information to know (and saved me a stop).

Many GPS devices include lifetime map updates. This can be handy, as new housing developments are constructed. You can also download (or purchase) maps for foreign countries. You can likely use your Smartphone app abroad, but I haven't tried that.

Some GPS devices can store your trip data, which you can then download to a map, where it displays your route. This is particularly interesting if you are hiking or on a boat.

If you are car-shopping, you may be offered a package that includes a built-in GPS system. However, that option is likely to cost much more than the price of a hand-held separate device.

Articles on the subject:

- Do I need a dedicated GPS device if I have a smartphone?
-
- Can you trust your phone's GPS driving directions?
- Smartphone vs. Dedicated Car GPS (PND)
- The 7 Best Traffic Apps of 2019
- 44 Google Maps Tricks You Need to Try

5G is Coming
Author: Jeff Wilkinson, President,
Sun City Summerlin Computer Club, NV
October 2019 issue, The Gigabyte Gazette
www.scscc.club / clearmeadows11 (at) gmail.com

5G is the designation for the upcoming fifth-generation cellular network technology. This technology, which had the standards set at the end of 2017, promises to bring faster speeds than the current 4G technology in use by most cell phones today. This technology will not only affect your cell phones, tablets and laptops, but also the myriad of other connected devices such as door locks, autonomous vehicles, security cameras, home appliances, and many more devices included in the IoT space – Internet of Things!

It's estimated that over 20 billion devices will be connected to the internet by the end of 2020 up from the 6 Billion plus currently connected. The promised latency (the delay in sending data from one point to the next) reduction of 5G is critical to the growth of driverless vehicles and many other applications.

Shipments of 5G smartphones will surge to more than 100 million units by the end of 2020 as the coverage of 5G networks grows and the premium prices of today's handsets come down, according to a report by International Data Corporation. IDC said that next year 5G handsets could account for close to 10% of global volumes, which have been hammered in recent years by consumers taking longer and longer to upgrade to new models.

Driverless Cars and 5G Technology
For autonomous car technology to be unlocked, many experts agree that large-scale adoption of 5G is required.

If you've been following the news about 5G, you know that it has the potential to significantly boost bandwidth up to 10 Gbits/sec. It also has sub-1-millisecond system latency paired with a considerable reduction in power consumption over existing

networks. 5G will enable a host of new applications in the Industrial Internet of Things (IoT), vehicle-to-vehicle communication, virtual reality and artificial intelligence applications.

Said Nokia's Jane Rygaard in a recent interview with the BBC : "*We need to look at how long it takes for the message to be transmitted between sensors and then get to the computer in each car, and then how long it takes for the computer to make a decision, and all of this has to be in less time than a human would take to make a decision—2 milliseconds. We need a network supporting this, and 5G is that network*."

New to the Library
Google Apps Made Easy – Learn to Work in the Cloud
Author: Terry Flanagan, Club Librarian, GVR Computer Club, AZ
October 2019 issue, Greenbytes
www.ccgvaz.org / Newsletter (at) ccgvaz.org

Just added to the club library is *GOOGLE APPS MADE EASY – Learn To Work In The Cloud*. Google Apps is Google's response to Microsoft Office and LibreOffice. The table below lists the various functions and the names used.

FUNCTION	GOOGLE APPS	M/S OFFICE	LibreOffice
Word Processing	Docs	Word	Writer
Spreadsheet	Sheets	Excel	Calc
Presentation	Slides	PowerPoint	Impress
Database	N.A.	Access	Base
Forms	Forms	N.A.	N.A.
Note Taking	Keep	OneNote	N.A.
Photo Organizing	Photos	N.A.	N.A.
Vector Graphics	N.A.	N.A.	Draw
Email	Gmail	Outlook	Thunderbird
COST	Free	$100/yr.	Free

What makes Google Apps different? First and foremost Google Apps are web based. You do not download and install a program on your computer. You use your web browser, preferably Google Chrome, to go to www.google.com and log into your account and there they are. You do not have to be concerned with updates, maintenance, and backup issues. They are also platform or operating system independent. It does not matter if you are using a M/S Windows, Apple MAC or Linux computer, an Android smart phone, iPhone or iPad. The applications and your files are there in the cloud for you to access from wherever you are.

There are several advantage and disadvantages to working in the cloud. Being on the cloud makes it easier to share your files with others, which makes collaboration easier. There is no need to send email attachments back and forth or copy files onto flash drives. Also, all of your data will be consistent between your devices. If you make changes in Google Docs on your PC and later open the file on your iPad the changes are there. Even if you save the file locally to your computer it will be synchronized to the cloud version. The disadvantages are that you must have an internet connection since most of the things you will do with these apps are cloud-based and done online. The applications do not have as many features as the other office suites and some may have security concerns about their data being on the cloud.

From the chart above, you will note that each office suite has applications that the other does not. Google Apps does not have a database module, but this is not a frequently used application by home users. Many common database functions can be handled by a spreadsheet. M/S Office and LibreOffice do not have a photo editing module, but there are a number of good stand-alone programs to perform those tasks.

Google Forms stands out as a unique application. Forms does what the name implies. You can easily create forms to gather information or take surveys. The data is automatically transferred to a spreadsheet and reports created to summarize the results and display them in easy to understand charts.

One final point to mention – notice the bottom line in the chart above. Google Apps are free along with 15 gigabytes of cloud file storage. More space is available for a fee.

Computer History
Author: Leah Clark, President / Editor,
Los Angeles Computer Society
October 2019 issue, User Friendly
www.lacspc.org / editor (at) lacspc.org

Recently I was in Washington D.C. While there, I visited the Smithsonian Museum of American History. They had a special exhibit on computer history. There was a sign that read, “Unless you know the road you’ve come down, you cannot know where you are going.” I wonder where computer and other technologies are going? Here is some information from the exhibit.

Both corporate researchers and self-trained hobbyists played crucial roles in the invention of the personal computer. Robert Noyce, Gordon Moore and Andy Grove used their doctoral training in physics and chemistry to found Intel, a leading manufacturer of integrated circuits. Alan Kay and others at Xerox advanced computer graphics, networking, and printing. The Homebrew Computer Club in Menlo Park, California, gave hobbyists a place to share knowledge. Homebrew members Steve Jobs and Steve Wozniak founded Apple Computer after demonstrating their Apple I kit at the club.

Early computers were big and expensive and required technically trained specialists to run them. Not surprisingly, only universities, big businesses, and government agencies had access to these behemoths. In the 1970s and ‘80s, Silicon Valley inventors

changed the face of computing with the first “personal computers” small enough to fit on a desk. They created revolutionary features that we take for granted today — a hand-held input device called a mouse, a graphical user interface with overlapping “windows,” and clickable pictures called “icons” — and made computers less expensive and more “user-friendly.”

Douglas Engelbart and his colleagues at the Stanford Research Institute were pioneers in the field of “human - computer interaction.” In 1964, they built a hand-held pointing device to manipulate images and text on a monitor’s screen. The prototype was a simple wooden box with two perpendicular metal wheels, a selection button, and a wire connection to the processor. Engelbart’s “mouse” was subsequently refined by researchers at Xerox PARC and made popular with the release of the Apple Macintosh in 1984. Engelbart later noted, “It just looked like a mouse with a tail, and we called it that.”

Tech Humor One-liners - http://www.jokes4us.com/peoplejokes/technologyjokes.html

Why was the computer tired when it got home? It had a "hard drive"

How do trees use a computer? They log in!

"When I die, I want my tombstone to be a Wi-Fi hotspot.....that way people visit more often."

https://www.invisionapp.com/inside-design/tech-industry-halloween-costumes/

Working at Home

Rabid Prototype

Mad Data Scientist

Back in the 5-1/4” disk days, I glued tech stuff of the day to a felt tunic I made; I wore it, with jeans and a long-sleeved t-shirt, to work as well as for the trick or treaters.

The Meeting that Was…September
By Judy

The SCVCC's goal is to keep its members informed about what's new in technology. Hopefully, members learn something new about technology at each meeting.

I showed how I use bit.ly to shorten very long website addresses to something that is easier and more reliable to click on – how many times has someone sent you a long URL in an email that is 3 lines long. It's free and you can see how many clicks you have gotten.
https://www.groovypost.com/unplugged/what-is-windows-10x/?utm_source=newsletter&utm_medium=email&utm_campaign=daily
or
http://bit.ly/2VGbZFA

We also looked at the Reader View (Chrome, Firefox and Edge) where you can read and print an article without ads, etc. I'm using it as a way to easily create presentations. I hope everyone took time to learn how to use it with their favorite browser.

Thanks to member Mark Thomas, lefty.tech, for bringing his streaming media gadgets and mini router to the meeting. He has the router set up to match the one in his home; he uses it when doing on-site tech support so he doesn't need to ask for the client's passwords. He focused on Roku, Fire Stick, Chrome Cast and Plex. Some members were already using one or two of the devices. Cutting the cord are relatively new buzz words and using one of the devices is a way to do that.

I liked the Amazon Fire TV Stick the best. You can use the voice remote with or without Alexa. ($49.99 – Black Friday will be here soon ;-).

2019/2020 SCV CC OFFICERS

President Judy Taylour
scvcomputerclub(at)gmail.com

Snail Mail 18727 Nadal Street
Santa Clarita, CA
91351

General Meeting 1st Monday of the month
6:30-9:00pm

Bella Vida
27180 Golden Valley Rd.
Santa Clarita 91350

Membership Application
(Please Print)

_____
Name

_____
Address

_____
City/State/Zip

_____
Home Phone

_____
E-mail

_____
Areas of Interest

Level of computer skills (please circle)

Novice Average Expert

Mail to: SCV CC, 18727 Nadal Street,
Canyon Country CA 91351

Membership Benefits Around Town

Lefty.tech
aka Mark Thomas Computer Support
26117 Rainbow Glen Drive
Newhall 91321
661.250.7440 / Lefty (at) Lefty.Tech
65+ = $10 discount on Onsite support
In-your-house support also available

The SCV Computer Club (SCVCC) has been serving technology enthusiasts from novice to the professional in the Santa Clarita Valley, California since 1988.

The information appearing in this newsletter is distributed solely for use by SCVCC members. Permission is enthusiastically granted to reprint all or any part by similar non-commercial publications *provided the attribution included with the article is included with the article.*

Publication of information in this newsletter constitutes no guarantee of accuracy and its use by readers is discretionary. All opinions expressed are those of the authors and not necessarily those of the SCVCC.

The SCVCC is dedicated to supporting the needs of its members and to the exchange of information about technology (computers, devices, services, software and hardware) through meetings, its web page, and the distribution of this newsletter.

Member of apcug An International Association of Technology & Computer User Groups

The SCVCC is a member of SCRUGS and APCUG
(Southern California Regional User Group Summit)
(Association of Personal Computer User Groups)

Annual membership Dues	$30.00
Annual Family	$54.00
Senior (55)	$27.00
Senior Family (55)	$48.00
Student Membership	$25.00