DATALINE

Published by Santa Clarita Valley Computer Club … We're User Friendly
Serving the Santa Clarita Valley, CA since 1988

Volume XXVIX, Issue 3
Editor: Judy Taylour

Meetings
SCV Senior Center
22900 Market Street
Newhall CA 91321
www.scvcomputerclub.org

In This Issue

Wednesday, March 8, 2017

Is Amazon Prime Worth It?
Difference Between Office 2016 and Office 365 – Which one is best for you?
New Tools in Word 2016

6:00 pm – Are you an Amazon Prime member? If so, are you taking advantage of its many benefits? If not, perhaps you will find it will be a benefit for you to become a member.

7:00 pm – We'll learn about the difference between Office 2016 and Office 365. Which one is best for you? We'll also take a look at some of the new tools in Word 2016 you might not be using.

Please bring one of your favorite Word or Excel tools to share that you can't do without. We'll all go home with new tools that will make us more productive.

Recover, restore, backup, clone, image?
By Carol Picard, Editor / Webmaster, Midland Computer Club, MI
February 2017 issue, Bits and Bytes
www.mcc.apcug.org / capmidmi (at) yahoo.com

At our January club meeting we discussed how to recover in case of hard drive failure, virus, or if Windows won't start.

The most important steps for recovery need to be completed before a problem occurs. First step is to create a recovery drive. Depending on the computer, this could require a 16Gb or 32Gb flash drive. My suggestion is to use a 32 Gb flash drive. Everything on the flash drive will be deleted and you cannot use the drive for anything else. Well-known brands, 32 Gb flash drives, were recently on sale for less than $10.00.

To create a recovery drive on a Windows 10 computer, connect the flash drive to the computer, search for recovery, click Create a recovery drive. Follow the prompts to create the drive. Make sure "Back up system files to the recovery drive" is selected. The minimum size of flash drive needed will be indicated.

A flash drive has less usable space than the amount of space indicated on the label, so, if it indicates 16Gb needed, you will actually need a 32Gb flash drive. It could take an hour or more to create the recovery drive. During the process, you will see a prompt to "Delete the recovery partition from your PC".

Do not click that option, so you still have the ability to run recovery from the hard drive. Make sure you get the message that the recovery drive was successfully created. If not, try again. After safely removing the flash drive, label it and store it in a safe place. The flash drive is bootable. When you need to use it, insert it in the computer, turn on the computer, and it should automatically boot from the flash drive. However, depending on the computer, you may have to access startup or bios options to boot from the flash drive.

The recovery drive offers more than one recovery option. Depending on what is wrong with the computer, you may be able to save personal files, or may only be able to reinstall the Windows operating system and any programs that were installed by the manufacturer, which is why it is important to have a good backup.

The next step is to back up personal data, e.g., documents, photos, videos, etc. If you are using an email client installed on your computer, such as Outlook or Thunderbird, find out how to back up contacts and emails. Other software programs may store data in special locations, so you will need to find those as well.

Backing up personal data is not a one-time event. Develop a backup plan and follow it because the time that you miss creating a couple backups is when you are going to need them. One of our members mentioned he uses five flash drives for backing up data, backing up once a week, rotating through the flash drives. Based on your use of the computer, you may decide to back up more or less often. Why have more than one or two backups? If you accidentally delete a file, you may not realize it right away and, if you only have a couple backups, by the time you realize the file is missing, you may have written over the last backup that contained that file. Store backup drives in a safe place, e.g., fireproof safe, or at least in another area in your house, away from the computer. For pictures, videos, really important documents, you might want to copy them to an additional flash drive and store that drive at another location.

Most software programs are downloaded directly to our computers so we don't have CD/DVD drives to reinstall from. Generally, if you need to reinstall the software, you can go to the vendor's website and download it again. However, there may be restrictions on downloading the software more than once, or there may be a charge to upgrade to a more current version. After downloading new software, copy the installation files to a flash drive or external hard drive. When software comes with activation codes, I print that information to a pdf file and save the pdf file on the same drive as the installation files.

You can manually back up files by copying them from your computer to your flash or external drive. Or you may decide to use a software program to manage the backup process. Both free and paid backup programs are available, although some free ones have limited functionality. When purchasing a new external hard drive , it may include backup software. Backup software lets you specify what to back up and to set a schedule for automatic backups. Some have the option to schedule an initial full backup and subsequent smaller backups, called incremental backups, backing up files that have changed since the last full backup. One caution is that viruses can spread to attached drives. Instead of automatic backup, which requires the backup drive be connected at all times, you can run manual backups, connecting the drive only while running the backup.

Online backup and cloud storage are other options to consider. There is generally a charge for online backup service and may be a charge for cloud storage, depending on how much data you have. An advantage is that you can generally access your data from another device, e.g., computer, tablet, smartphone. Onliine/Cloud storage may not prevent loss of data if your computer is locked by ransomware.

With any backup solution, you should occasionally check to make sure the backups are running successfully and that you can recover files. Consider using a program that allows you to restore select files without using the software that was used to create the backup. You may find you need a file while your computer is out of commission and you want to be able to connect the backup drive to another computer and access files

without having to install software on that computer. Also, if you only need one or two files, you don't want to have to restore the entire backup.

Whatever backup strategy you use, make sure it is backing up everything you need. I installed a new hard drive for someone whose hard drive had failed. He was using online backup so was confident he would recover all of his data but, the default settings for the service he was using did not include videos, so they were not being backed up and we were unable to recover the videos from the failed hard drive.

Another backup/recovery option we discussed was creating an image (also called system image) of the hard drive. If necessary to wipe/format a hard drive, an image can restore the entire contents of a hard drive; the operating system, programs, and personal files. Some backup programs also provide the option to create an image.

While the terms image and clone are often used interchangeably, the exact definition of clone is when two hard drives are installed in a computer and data is copied from old to new, which requires that the original hard drive is still working. The last time I purchased a new hard drive, it came with a version of True Image software that provided this capability and I was up and running in a short period of time with all of my user ids, programs, data and settings.

When creating a system image most flash drives will be too small so you will need an external hard drive. Depending on the size of the external hard drive, multiple images can be saved to the same drive. Name the image (or the folder you save it in) so you can identify when it was created and, if you have multiple computers, which computer it was created from. The program used to create the image prompts you to create a bootable flash drive, which only has to be done once. You boot the computer from the flash drive and it contains the software to restore the image from the external drive. If you have multiple computers, you may need to create a bootable flash drive for each computer. In most cases, an image or clone can't be used to restore to a different computer, although some software may support this.

Another term discussed was System Restore. This option usually requires being able to boot into Windows. System Restore can be used if the computer isn't working correctly and you suspect recent changes caused the problem, or as an initial troubleshooting step, before resorting to recovery. Make sure system restore is turned on. After upgrading from Windows 7 to Windows 10, I discovered that system restore had been turned off. Windows automatically creates restore points before performing certain actions. You can manually create a restore point, e.g., before installing new software.

To access system restore, search for system and click create a restore point. It should open System Protection under System Properties. Under Protection Settings, it will list the drives on the computer and whether protection is on or off. Normally, you just want protection on for (C:). If it is not on, click Configure and turn it on. Make sure the percentage of disk space available for system restore is set to something other than 0, 10% should be good in most cases.

To create a restore point, click Create and follow the prompts. To revert to a previous restore point, click System Restore… , click Next. To see more restore points, click to place checkmark in box to left of “Show more restore points”. Click the restore point you want to use and click Next. If you know when the problem started, chose the restore point just before that date/time. If you don’t know which restore point to use, start with the most recent and, if that doesn’t fix the problem, run System restore again and choose a different restore point. System restore is not supposed to affect your personal files, but make sure your backup is current, just in case.

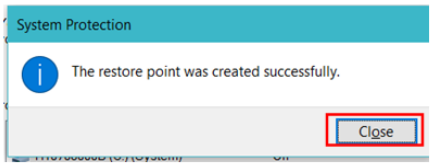


Figure 1 – Insert key

In some cases, system restore fails and Windows automatically returns the computer to how it was before system restore ran. There is also an option to undo a system restore. After restoring to a date prior to a Windows update or a software installation, it may be necessary to reinstall the update or software.

If you suspect you have a virus on your computer, and don’t know whether any of the images/backups contain the virus, it is probably best to use the Windows recovery drive to reinstall Windows and then manually restore personal files. If you don’t have a recovery drive, but have access to another computer, you can create recovery media for Windows 10. (https://www.microsoft.com/en-us/software-download/windows10). Previous versions of Windows required entering a code to activate. However, once Windows 10 has been installed and activated, you don’t need to enter a code when reinstalling Windows 10 on that computer. When restoring from a backup that may contain infected files, don’t restore executable files (.exe) as they are more likely to contain viruses.

With the recovery drive and good backups, you will be prepared when a problem occurs.

What Happened to Word’s Overtype Mode?

By Nancy DeMarte, 2nd Vice President,
Sarasota Technology Users Group
February 2017, Sarasota Monitor
www.thestug.org / ndemarte (at) verizon.net

If you used versions of Word before 2007, you probably encountered an editing feature called Overtype mode. This feature was introduced to save time when you needed to change some text in a document. To turn on Overtype mode, you pressed the Insert key on the keyboard. With Overtype enabled, every character you typed replaced the one to its right. It eliminated the step of deleting a group of text and inserting new text in its place.

Figure 2 – Insert key

If you were an Overtype user, you might have wondered why it doesn't work anymore. Beginning with Word 2007, Overtype mode has been disabled. Why? One reason is that it was hard for the user to tell if Overdrive were enabled. With no light or indicator on the screen, you didn't know whether Overdrive was active or not until you began typing. Non-professional typists like me would occasionally press the Insert key by accident, engaging Overtype and find ourselves deleting text we wanted to keep. Figure 1 shows how close the Insert key is to the common Backspace and Delete keys.

Although Overtype mode is disabled in recent versions, you can make it accessible using one these two methods. First, with a Word document open, click File, then Options. (In Word 2007, click the Office button, then Word Options.) Then click Advanced from the left menu, and under Editing Options, click the checkbox which says, "Use Overtype mode."(Figure 2) If you want the Insert key to control whether Overtype is on or off, click the checkbox next to "Use the Insert key to control Overtype mode." Then click OK.

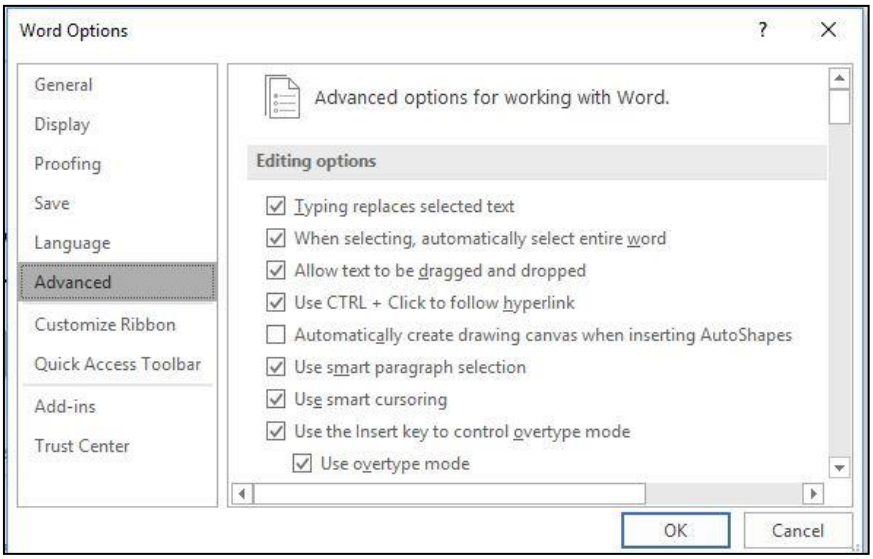


Figure 3 - Overtype settings in Word Options

An easier way to enable Overtype and know whether it is on or off is to add it to the Status bar. This bar runs along the bottom of every Word Window above the Taskbar (That's the one with the Zoom slider on its right end.) Right click in an empty space on the Status bar. The list which appears shows you the tools you can add to this bar, one of which is Overtype. When you click it, the word Overtype appears near the left end of the status bar, showing that it is enabled. To disable it, click the word again and it becomes Insert. You don't need to change the checkboxes in Word Options, and you don't have to touch the Insert key. Just a glance at the status bar will tell you what editing mode you're using, Insert or Overtype.

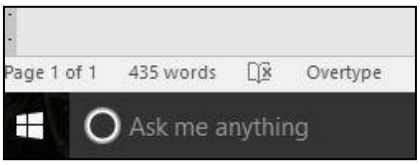


Figure 4 - Overtype on the status bar in Windows 10

Watch out for this convincing fake
By Cynthia
March 7, 2017
http:// bit.ly/2mH0sXa

A reader forwarded a recently received email that purported to be from Microsoft and wanted to know if it was real.

From: Microsoft.com security team <no-reply-adm-6@outlook.com>
Sent: March 1, 2017 1:19 AM
To: Microsoft.com security team
Subject: Verify your email address to avoid service interruption. (Do not ignore!)

Outlook.com

Dear Outlook User.

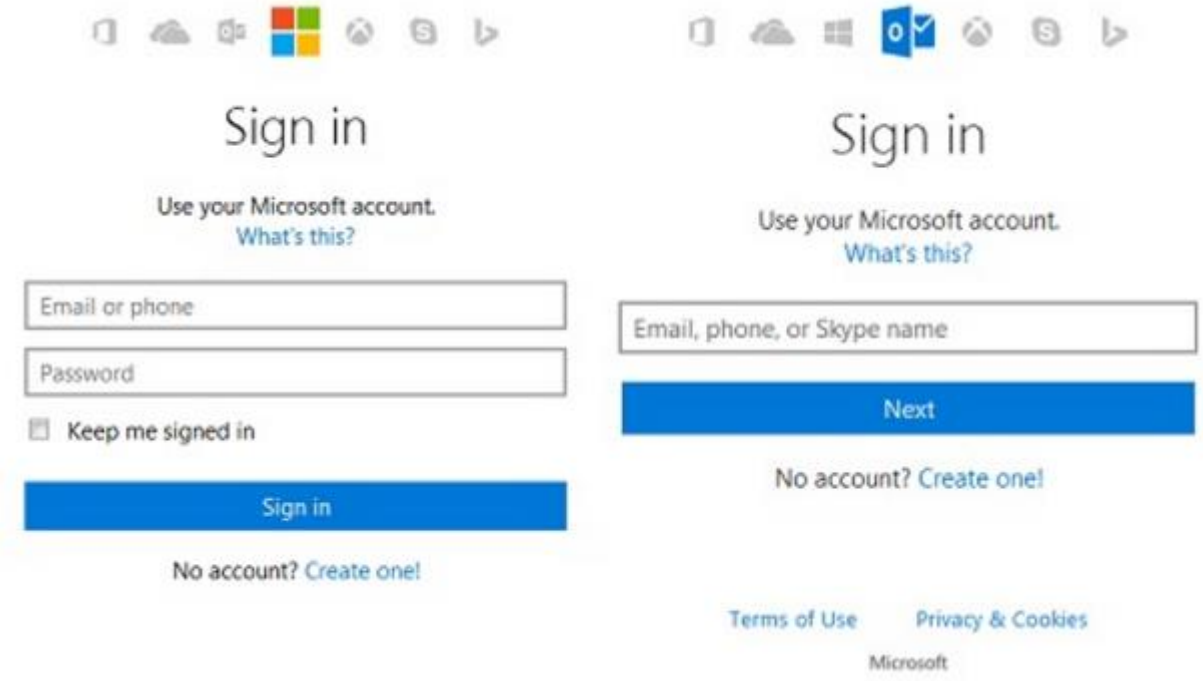
As part of our effort to improve your experience across our consumer services, we're updating the Microsoft Services Agreement and the Microsoft Privacy Statement.

If you do not verify your Microsoft account within 24 hours your account will be deactivated and deleted from our server and you will no longer have access to many of the features for improved Conversations, contac ts and attachments.

Take a minute to verify your account for a faster, safer and full-featured Microsoft Outlook experience and to avoid your account being De-Activated.

While this email is fairly professional-looking compared to some scams, there are red flags. First, I've never received a privacy policy update from Microsoft where they threatened to shut down and delete everything in my account if I didn't respond within 24 hours. I tested this out (don't try this at home) and it takes you to a nearly exact duplicate of the actual Outlook sign-in page. Fake site on the left. Actual Outlook.com on the right.

If you entered your info on the site on the left, the crooks would have your Outlook ID and your password.



If you think a notice like this is legitimate, just go to Outlook.com. Don't click on a link. Type that actual address into your browser. If there are some terms you need to accept, you'll be notified before you log in.

The Sky Isn't Falling. Yet.

By Rod Scher, The Geekly Weekly
www.thegeeklyweekly.com / rod3041@gmail.com

I really love the Internet. I get a kick out of technology in general, of course, but I'm crazy about the Internet in particular. When you think about what it's given us—communication, information, empowerment, and more—it's difficult to come up with too many other technologies that have had this great an impact. To a great extent, the Internet has truly democratized information.

And yet . . . When I stop and think about it, I kind of freak out. I mean, I don't want to sound alarmist or anything, and I generally like to stay calm about the issues, but I THINK WE'RE ALL TOTALLY SCREWED!!

OK, there. I feel better now. I'm calm. But here's what I mean…

Let's start with ransomware: This is malware that, when accidentally downloaded (generally by people who have ignored the basic security rules that tech people keep trying to get them to follow), encrypts your files, which it then holds for ransom. (The ransom varies, but $300 to $500 or so is a typical ballpark: enough to make it worthwhile for the bad guys, and just barely cheap enough for most of us to at least consider paying the ransom.) In most cases, the encryption is done very well and very

quickly; you are not getting those files back unless you pay the ransom. (Or unless you have a good backup and know how to restore your files from that backup.)

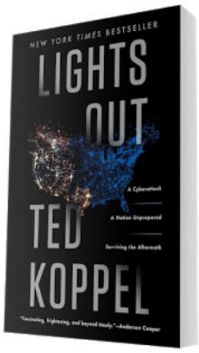
Businesses and individuals have been getting hit with ransomware regularly, but more recently, the bad guys have discovered other tempting targets: municipal entities, law enforcement agencies, and hospitals, for instance. Think about it: A small police department or hospital has data that is very important, sometimes literally a matter of life and death, including such things as patient records, info from medical devices (sometimes from various implants), evidence stored for court cases, and more. This is critical stuff. The data should have been backed up and the organization should have a relatively bulletproof backup-and-restore process in place, but many such entities do not. That's why the combination is almost irresistible to bad guys: These organizations have critical data they cannot afford to lose, and crappy (or sometimes non-existent) IT departments. The result? These are big, juicy targets; crooks can easily mount an attack, and the payoff can be big.

How big? Last year, bad guys encrypted data from the Hollywood Presbyterian Medical Center, and demanded $3.4 million (in untraceable Bitcoin, a digital cryptocurrency) to give it back. Hospital executives declared a state of emergency and employees reverted to paper and faxes. (Ironically, it's sometimes possible to negotiate with the thieves; in this case, the hospital eventually paid about $17,000 to get its files back. Still, $17,000 is a pretty good chunk of change)

Of course, there are other attacks, and other types of attacks.

Last December 23rd, unknown intruders (possibly state-sponsored actors under Russian control, though this remains unproven) hacked into the computers of the Ukraine's (please do not ask me to pronounce this) Prykarpattyaoblenergo electrical control center. Operators watched, dumbfounded and helpless, as the intruder simply navigated through onscreen menus, shutting down some 30 electrical substations, one mouse-click at a time. The hacker then disabled backup power supplies in two of the region’s three electrical distribution centers, leaving all concerned literally and figuratively in the dark.

About 230,000 people were suddenly without electricity in an area where the temperature that evening dropped to around 14 degrees Fahrenheit. (Lest you think that the U.S. power grid is more secure and sophisticated than a control center in Ukraine, note that many experts said that the Ukrainian station was better secured than many U.S. stations.)



This is the first known hack of a power grid that resulted in a power outage of that size, but it's probably not the last. (For a sensational—some reviewers said sensationalist—read on the subject, see Ted Koppel's Lights Out.) The reality is that, as unsecure as our private

infrastructures (see the hospitals and corporations mentioned above) are, many government and quasi-government infrastructures are even more disorganized and less secure. (If this surprises you, then you haven't been paying attention to news of the DNC—and now RNC and other—hacks. Also, you've never been in the Army.)

Here's the problem in a nutshell: We took an inherently unsecure technology, the Internet (which was created to share, not hide, information), and made it into the backbone of both our infrastructure and our economy. We've taken steps to make it more robust and mitigate its weaknesses, but the reality is that just about everything—from our power grid to our banking industry and from hospitals to law enforcement—now runs on what turns out to be a vulnerable and easily crippled technology.

And it's going to get worse as the Internet of Things takes hold. The IoT involves connecting literally billions of things to the Internet, everything from your toothbrush to your thermostat and from your doorbell to your dog's water bowl. Those connections will, for the most part, make your life much easier. Until suddenly they don't.

Take baby monitors, for instance. It's comforting to know that your child is safe and snug in his bed; being able to hear the cooing sounds your toddler makes as he sleeps is soothing. Hearing the voice of some stranger speaking to your child through the monitor is definitely not soothing, but it has happened on occasion. Why? Well, the baby monitor is on your wireless network, and is probably not very well protected. Neither you nor the manufacturer took steps to secure that device.

This is just one of several brands of baby monitor that has been hacked.

But the technology itself is not the only major problem. The other weakness is . . . well, us. Any security pro will tell you that the biggest vulnerability is human, the people standing between the palace door and the storeroom in which the crown jewels are held. Basically, people are not very good at security, because we're lazy, naïve, and entirely too nice. We really, really want to be helpful, so when we get an email asking for information, we're all too ready to part with that information. When someone claiming to be a hardware tech or copier repair person shows up at a place of business with a clipboard, a baseball cap with a company logo, and a good story, people are almost always willing to "help" him by parting with names, phone numbers, even passwords.

Almost without exception, we are the weak link in the security chain. We click links in phishing emails, visit sketchy websites, download suspicious files, and answer the (seemingly innocent) questions of people who wander into our places of business. We place all our very personal information on the Internet for anyone to see: between Facebook, LinkedIn, and Twitter, anyone looking for information about you or your business has all he needs.

Chris Hadnagy is a security expert and a penetration tester; companies pay him to break into their networks in order to uncover flaws. Chris says that he can "social engineer" (read: schmooze, lie, or finagle) his way onto any corporate network well over 90% of the time. Years ago, says Chris, the difficult part of his job was uncovering enough information to be able to mount a convincing deception. Now, he says, with all the information floating around on the Internet, his biggest problem is sifting through the tons of data available to decide which pieces are most useful.

Still, a hacked baby monitor or an individual who's fallen victim to ransomware is not what worries me. We can learn to protect ourselves; if we don't, then we have only ourselves to blame.

But state-sponsored attacks on infrastructure are another story. Weapons are rarely made without someone wanting to find an excuse to use them, and the Internet is, among other things, a weapon. It's simply too terrifyingly easy to conduct an attack that could turn into a full-blown cyber war. A digital attacker risks nothing, really. It's a form of warfare that, unlike all other forms, is cheap, fast, simple, and deniable. That's a temptation too alluring to ignore. You can engage an enemy anonymously from half a world away, and there's absolutely no risk that you or any of your fellow "soldiers" will get hurt. You can cripple a region—or possibly an entire country—with just a few well-placed strikes. Whether the attacker is a state actor (or someone who operates at the behest of such actors) or an independent guerilla operator, the technology is too available, the risk is too small, and the payoff too big to ignore.

And that is what worries me. I do believe that we will eventually address many or even most of these security issues, but I suspect that our actions will be reactive in nature: nothing will be done until something very bad happens, and then suddenly security will be on everyone's mind, from our legislators to our law enforcement people, and from infrastructure developers to IoT manufacturers.

We should probably be thinking about such matters before the sky starts falling.

Drones

By George Harding, Treasurer
www.aztcs.org
georgehardingsbd (at) earthlink.net

I am amazed at the rapid development of the drone industry and the uses to which drones are being put.

Here are a few of the uses so far:

- **Package delivery:** UPS has stated that their plan is substantially complete and will be introduced soon. It has limits for weight, distance delivery address.
- **Weddings and other similar events:** Drones make it easy to record events that are important to family and friends. Viewpoints can include those that an individual cannot do.

- **News gathering:** Many TV channels now use drones to access accident sites and other events of interest to a broadcast.
- **Site inspection:** Viewing construction as it is occurring is valuable to identify problems that may not otherwise be seen. Checking electric and other similar supports can be done with drones without the necessity of having a human climb up a tall tower to inspect.
- **Agriculture:** Drones are used to check field sizes, crop progress and limited spraying, without the dangers associated with crop duster planes.
- **Police and Fire observation of sites:** This saves the need for a human to be in danger.
- **Security:** Drones can inspect premises to identify risks that would be difficult for a human to do quickly and economically.
- **Safety:** Australia has started using drones to survey beach areas for sharks.
- **Photography:** Drones can deliver video and photographs in high resolution of just about anything: Nature, colorful situations, traffic, events and more.
- **Search and rescue:** Drones can access locations that are difficult or dangerous during severe storms, earthquakes, and hurricanes to find survivors and help with rescue.

With the FAA promulgation of Rule 107, individuals and business can operate drones with assurance that they will not fun afoul of government oversight. Some of the rules are:

- Line of sight. The operator must keep the drone in sight at all times.
- Night operations not allowed.
- Maximum ground speed of 100mph and maximum altitude of 400 feet.
- Drone must be lighter than 55 pounds
- Operations in commercial airspace (airports, etc.) only with ATC permission.
- Preflight inspection of drone required.
- Remote pilot airman certificate required. Pilot aeronautical knowledge required, unless the operator of the drone already has a pilot license.
- Registration of drone required. Over 500,000 drones have been registered already.

Intel has made some interesting innovations in drone technology. They have available a ready-to-fly drone that incorporates their Real Sense technology. It allows the drone to see conflicts ahead and move to avoid them. So, instead of flying into a tree, its drone can see the tree and maneuver around it to keep on track for the target. See intel.com/aero for more info.

Intel is also working on the ability to control more than one drone at a time. At **Interdrone 2016,** a video was shown of a demonstration of controlling 100 drones at a time over the opera house in Sydney, Australia. It showed the drones circling around in what appeared to be a random pattern and ended with an oval of drones in the sky with “Intel” in blue drones in the center. Most amazing!

The drone market is exploding as to usage. There are many uses today for drones, but the future will open up many more, things we have not even thought of today.

Back to Basics
Copying Photos from Your iPhone to Your PC
By Jim Cerny, Forum Leader, Sarasota Technology User's Group, FL
www.thestug.org / jimcerny123 (at) gmail.com

Using your iPhone to take photos is easy, convenient, and fun. I always have my iPhone with me everywhere I go and it has become my only camera for taking pictures. After taking a few hundred photos, however, what do I do with them? For me, I simply COPY them to my Windows PC and then delete them from my iPhone so that I free up that memory. Perhaps this can be helpful to you if you use your iPhone as your camera.

Actually, connecting your iPhone to your computer is not much different than connecting a portable drive. Once successfully connected to your Windows computer, you just need to access the iPhone's memory that contains your photos. Fortunately, this is not difficult, here are the steps to follow:

1. Turn on your computer and go to the desktop screen. It is usually best not to have any windows open or programs running.
2. It is usually a great idea to DELETE photos you do not want from your iPhone before you copy them to your PC. Why copy photos you do not want to keep?
3. Connect your iPhone to your computer using the cable from the phone to a USB port on your computer.
4. You may hear a "tone" (or several tones) as your phone turns itself on and establishes the connection. If your phone does not come on, turn it on. These "tones" are indicating that your iPhone has been detected by Windows and your iPhone may be "syncing" to your computer. For example, if you have iTunes for Windows installed on your computer, your iPhone will update and "sync" with that program. Just wait until this is completed and the tones stop.
5. You should see a text box on your phone that says: "Allow this device to access photos and videos?" Please select "ALLOW", otherwise it will not work.
6. If it is not yet open, <u>OPEN Windows File Explorer</u> (which is called Windows Explorer in older versions of Windows).
7. In the File Explorer window, on the left side, look for a NEW FOLDER listed called "Apple iPhone". Think of this folder as you would as if it was a portable drive you connected to your computer.
8. Click on the small arrowhead to the left of "Apple iPhone" to open the FOLDER that is in it. You should now see the folder "Internal Storage" listed.
9. In the "Internal Storage" folder is a folder called "DCIM" (Digital Camera Images). It seems that ALL image capable devices have a DCIM folder to hold photos. Open that folder and you will see a folder called "100APPLE".
10. Open the "100APPLE" folder to see your photos! Your iPhone has many memory areas and this is the folder (in the DCIM folder) that has your photos,
11. You can now copy or "drag" any photos you wish from there to any folder on your "C" drive or anyplace else. You can also DELETE photos from this folder and thus they will be deleted from your iPhone. This works no differently than if you were working with any files on any device using File Explorer!
12. When you are finished, simply unplug your phone from your PC. [NOTE that in most cases when you have connected another memory device to your computer,

you should open the “Safely remove hardware and eject media” icon on the lower right corner of your desktop screen (near the clock and date) and then click on the device displayed to disconnect it. With my iPhone on Windows 10 this icon does not show the iPhone connected, so you can just unplug it.]

13. Check your iPhone to make sure it has the photos you want on it or deleted.

Once you have done this once or twice it will be easy for you to control where your photos are stored and free up your iPhone for more photos!

Now you can go take as many pictures with your iPhone as you want and you will not have to worry about using up all your iPhone memory. If you take videos, remember they take up much more memory than photos. Now get your iPhone and ask a friend to SMILE!

Windows 10 Tip
Use the Magnifier tool to zoom in on text or objects
Ed Bott, The Ed Bott Report - http://www.zdnet.com/blog/bott/ zd.net/2m3aDSA

Like its predecessors, Windows 10 is filled with accessibility tools. One of my favorites is the Magnifier app, a handy system utility that allows you to zoom in on a portion of the display so you can read the fine print on a web page, distinguish between confusing characters in a product key, or take a closer look at detail in an image.

You can run the Magnifier app by finding its executable file, Magnify.exe. But it's much easier to use the built-in keyboard shortcuts:

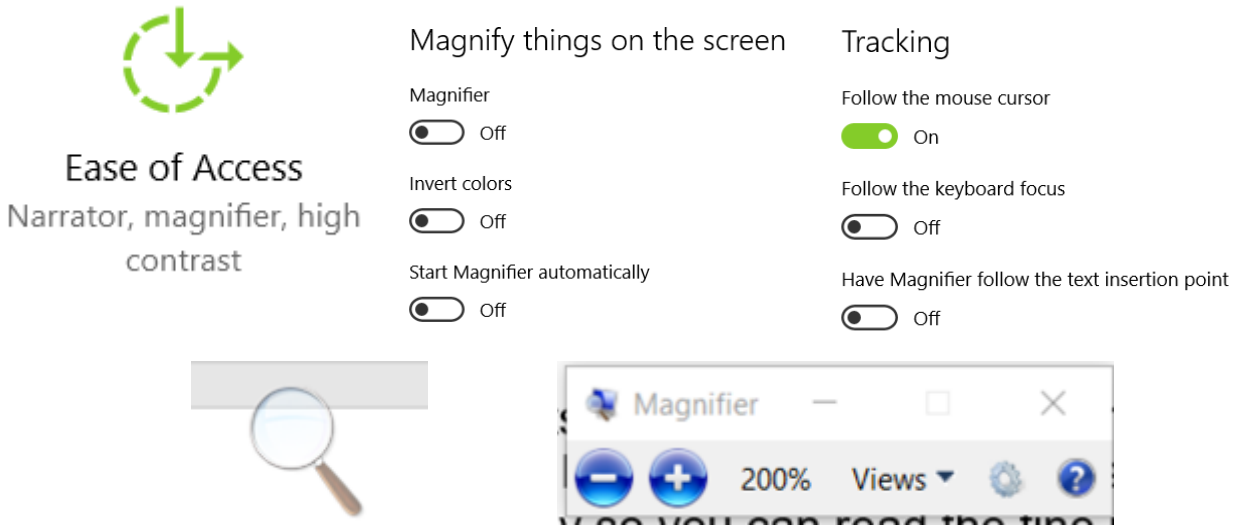
- Press the Windows key and then tap the plus sign to turn Magnifier on and zoom the current display to 200 percent. If Magnifier is already running, that key combination zooms the display in 100-percent increments all the way to 1600 percent.
- Press the Windows key and then tap the minus sign to zoom back out, again in 100-percent increments, until you return to normal magnification.
- Press the Windows key and tap Esc to close Magnifier and return to the normal display.
- After zooming the screen, you can use the mouse to pan to portions of the screen that aren't currently visible.

Four additional options on the View menu, shown here, allow you to change the Magnifier view.

- Ctrl+Alt+F: This is the default, full-screen view.
- Ctrl+Alt+L: Press this combination to turn the Magnifier into a lens that zooms only the portion of the screen directly under the mouse pointer.
- Ctrl+Alt+D: Use this option to dock the magnifier window to the top of the screen.

- Ctrl+Alt+Spacebar: Pressing this combination when you're zoomed in temporarily shows you the entire display, with the zoomed portion highlighted.

The Magnifier control is always visible on the screen when it's running, although it backs off to a dim icon of a magnifying glass when you're focused on a different portion of the screen. To see the full set of Magnifier controls, move the mouse pointer back over the magnifying glass icon and click once. When the full Magnifier interface is visible, click the red X in the upper-right corner to close it.



Press the Windows key and then tap the plus sign to turn current display to 200 percent.

The Meeting that Was...February

By Judy

Attendees were asked to bring a tech question so they could be forwarded to Toby Scott, Channel Islands PCUG tech guru, to answer on his weekly podcast. Several of the attendees brought one or more questions and Toby answered them on two podcasts. We also answered some of them at the meeting but I sent themall to Toby in case he had a different answer.

https://youtu.be/Ru4Afpqt0rk
http://mercurybroadcasting.net/qa-cipcug-session-34/
http://mercurybroadcasting.net/qa-with-cipcug-session-35/

We had a fun, interesting, and informative very unstructured Windows 10 Creator Studio update presentation by Bill James, VP, OK City Computer Club. In addition to some of the upcoming updates, he showed us how he is using Windows 10. I hope others got as much out of the presentation as I did – I found different ways of doing things that makes Win 10 even better. Thanks to a question by Helen Blanchard, we also got to take a look at his genealogy 'stuff.' Genealogy is obviously something he really enjoys.

We're waiting online with Zoom for Bill to click on the link to join us.

And, here he is – along with his two dogs.

He's been a Windows OS beta tester for years. Microsoft does pay attention to their feedback.

Agnes won everything in the raffle. Flash drive & USB to Android phone/tablet expandable cord.
Don't forget to thank her for bringing the cookies.

2016/2017 SCV CC OFFICERS

President Judy Taylour
scvcomputerclub(at)gmail.com

Information Line 661.513.4612

Snail Mail 18727 Nadal Street
Santa Clarita, CA 91351

General Meeting 2nd Wednesday / month

SCV Senior Center
22900 Market Street
Newhall CA 91321

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@Lefty.Tech
65+ = $10 discount on Onsite support
In-your-house support also available

Rogers System Specialist
HAS MOVED
(Various Discounts)
24621 Arch St. Newhall CA 91321
Turn on 13th street off Railroad
800.366.0579
Give Judy's telephone number for the discount 661.252.8852

The SCV Computer Club is dedicated to supporting the needs of its members and to the exchange of information about computers, peripherals, services, hardware and software through meetings, its web page, and the distribution of this newsletter.

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

The SCV Computer Club 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

Contact Judy for Discount Info

PEACHPIT USER GROUP
PROGRAM MEMBER
35% Discount

O'REILLY PARTNER PROGRAM MEMBER
O'Reilly Partner Program
50% off most ebooks / videos
40% off most print books from O'Reilly.com

webucator
customized INSTRUCTOR-LED training services
One free class / member
See Judy for Free Voucher #

Focal Press User Groups
learn · master · create www.focalpress.com
40% Discount

USER GROUP MEMBER
que PEARSON
35% Discount

Wrox User Group Members
Click here and save!
wrox.com
40% Discount

no starch press
30% Discount

Apress THE EXPERT'S VOICE
eBooks – 50% discount