DATALINE

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

In This Issue

Wednesday, April 13, 2016
Spring Clean Your Devices
Xth-Weekday-of-a-Month-Alternate-Formula
Denny Fuerst's Potpourri of Photos
SCV Photo ID Game

6:00 pm – The NCSA and BBB encourage everyone to make a thorough "digital spring cleaning" an annual ritual. The National Cyber Security Alliance (NCSA) and Better Business Bureau (BBB) are encouraging consumers (that's us) to put cybersecurity at the top of our mind by making digital devices an additional target of our spring cleaning activities. We'll go through their suggestions during this presentation.

David Nix will show us how to set up the Xth-Weekday-of-a-Month-Alternate-Formula in Excel. His example is the club's 2016 meeting dates.

7:00 pm - Denny Fuerst for two interesting photographic presentations. Denny has had a life-long interest in photography and will present a great variety of photos - some old and some newer - that he has taken during his lifetime with a focus (no pun intended) on interesting, entertaining and, perhaps, enlightening photos. Denny's collection of photos was initially taken with traditional film cameras (black & white and color), beginning with a Kodak Brownie and moving on to Nikon 35mm slide and APS (Advanced Photo System) cameras. More recently, his photos have been taken with a Canon point-and-shoot digital camera and a Nikon SLR digital camera with interchangeable lenses. With the great improvement in cell phone cameras, more of his photographic pursuits are likely to come from this option. After seeing Denny's potpourri of photos, you just may be inspired to pull out your camera or cell phone more often to record the world around you.

Following this photo presentation, everyone will be asked to participate in what Denny calls his "SCV Photo ID Game." A total of 30 photos of local SVC buildings and sites will be shown - one at a time - with the identity of the photo in question. You will be given an answer sheet to use to identify each photo. After all photos have been displayed, there will be a reveal session where the identity of each photo will be given. Some of the photos may be fairly easy for you to identify while others will be more challenging. Denny will award prizes - from his time serving as a vice president at Princess Cruises and Uniworld Boutique River Cruises - to club members who correctly identify the most photos. So, if you think you know the SCV, here's your chance to shine and impress your fellow club members and take home some cruise line swag as well.
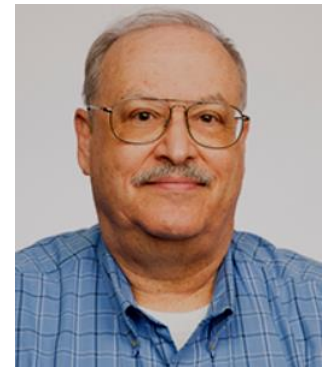
We'll also have popcorn!

Secure Your Accounts with Two-Factor Authentication
By Ira Wilsker

Ira is a member of the Golden Triangle PC Club and an Associate Professor at Lamar Institute of Technology; he is also a deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.

What does iTunes, Yahoo!, Gmail, Outlook, Twitter, Facebook, Bank of America, Chase, Discover, E*Trade, Vanguard, PayPal. eBay, and Etsy have in common with thousands of other secured online services? They all offer their users a secure supplementary method to prevent illicit access to their online accounts, with a level of protection much greater than the traditional password, that method known as "Two Factor Authentication". While it may increase the time necessary to logon to websites by a few seconds, it also greatly reduces the risk of an unauthorized person gaining access to those websites, even if the users' passwords have been compromised.

I recently presented two sessions on Password Security for the public event hosted by the city of Port Arthur, Texas. Judging from the questions and responses of those attending these sessions, too many people are still using insecure passwords. Several participants stated that their email accounts had been hacked, and unknown "hackers" had sent spam and other illicit emails from their email accounts. Others had mentioned that an assortment of shopping and financial websites, including online banking, had been accessed by unauthorized individuals, sometimes resulting in substantial financial losses. What many of the participants were blissfully unaware of is the fact that "crackers", people who can "crack" others' passwords, can easily crack simple passwords in just a few seconds, and moderately complex passwords may take several minutes or hours to crack. Cyber crooks can obtain passwords and usernames by compromising the servers of popular websites and servers, such as the "alleged" theft of five million Gmail passwords, over a million from CNet, and countless other successful hack attacks on servers all over the world. Often these usernames and passwords are posted online, many times on the "Dark Web," where illicit information and data is often bought, sold, traded, or given away.

While these cyber heists of millions of usernames and passwords sometimes get the attention of the media, the quiet work of thousands of crackers using simple guessing based on password tables, or a myriad of software utilities that can try hundreds of passwords a minute, continues to this day. The primary reason why the majority of victims who have had their passwords compromised and taken advantage of is their own doing, in that millions of people still use simple, easy to guess passwords to access secure websites and services. What is even more shocking is that most users who use these simple passwords also use the same simple password on multiple websites, meaning that if one is cracked, the cracker now has access to all of the user's online accounts. The number of Americans using the same password for all of their online access is a staggering 61%, according to a report published by CSID (csid.com) in September 2012, but still considered by many as a somewhat accurate reflection of the risks currently faced by the majority of computer (and smart phone or tablet) users.

According to the most recent surveys performed by several cyber security organizations, the majority of users still continue to use very common and easy to guess passwords. The security firm SplashData performs an annual study of the stolen password files published online by the hackers, and has found that over the past several years, there has been little change in the most widely used passwords, with the "Top 10" list of most widely used passwords in 2014 being (in rank order from 1 to 10) 123456, password (used by 4% of users), 12345, 12345678, qwerty, 123456789, 1234, baseball, dragon, and football. Among some of the next 15 most commonly used passwords, completing the "Top 25" list are 1234567, monkey, letmein, abc123, 111111, 123123, master, and access, along with the current crop of contemporary superheroes including superman and batman being in the top 25. My personal favorite, which was #25 in the list is "trustno1". In its report, SplashData urges that users follow three simple tips in order to make more secure passwords. Those three recommendations are: 1. Use passwords of eight characters or more with mixed types of characters; 2. Avoid using the same username/password combination for multiple websites; and 3. Use a password manager ... to organize and protect passwords, generate random passwords, and automatically log into websites."

Some users try to outsmart crackers by thinking that they are creating complex passwords by using a simple alpha numeric substitution for some letters that appear similar, such as replacing the letter "E' with a "3", the letter "O (oh)" with a "0 (zero)", the lower case "l (el)" with a "1 (one)", and the letter "S" with a "5". In reality, this simple substitution will not slow down even the most juvenile and inexperienced password cracker, as almost all of the readily available password cracking tools that utilize a "brute force dictionary attack" automatically make those substitutions when cracking passwords. I have one old and very primitive password cracking utility that incorporates the top 100 most widely used passwords as its first line of attack, followed by those same 100 passwords substituting numbers for letters, and then using an open source dictionary to crack passwords; this utility can try 1200 logons per minute (20 per second), and I can crack most users' passwords in a matter of seconds, my personal best being under five seconds, and the longest it ever took me to crack a non-complex password was about six minutes; good complex passwords are difficult (but not impossible) to crack using the most readily available cracker tools. Since a reported 25% of users in aggregate use the "Top 20" passwords to access their accounts, just manually entering each of the top 20 in order will give access to about one in four accounts, unless the website detects an attempted intrusion and locks the user out.

According to a study done by the password manager publisher LastPass (lastpass.com), 42.5% of users use passwords consisting of lowercase letters and numbers only; 39.8% use lower case letters only; 15.7% user numbers only; and only

1% use a reasonably secure and hard to crack combination of upper case and lower case letters, numbers, and characters (such as !, @, #, $, %, &). The same survey found that the average password is only six characters in length, and all lower case letters, which is an open invitation for a cracker to access that user's accounts. In creating complex passwords, users should never use family member or pets' names, birthdates, anniversaries, addresses, or other readily available personal information, as crackers often "data mine" social networking services such as Facebook profiles, gathering such information. Likewise, users should not use complete words as these are easy to crack with a simple "dictionary attack", and should never record passwords in an insecure way such as on a "Post It Note" on the monitor, unencrypted spreadsheet, text file on a phone or computer, or any other mode that can be easily purloined. Likewise, keep passwords absolutely private, and do not share them with anyone. Passwords can be easily captured by cyber crooks when the users access public Wi-Fi in coffee shops, airports, and other public places, with the same cyber thieves often setting up bogus but official looking hotspots in public places (airports are a favorite for this ruse) in order to steal login information including usernames and passwords for the explicit purpose of committing identity theft.

4%	**25%**	**3 min**
of people use the word "password" as their password	of the top 20 most common passwords, are first names	An expert hacker can crack the average password in under 3 minutes

Fortunately for us users, there is an easy way to provide an additional layer of security which will make it nearly impossible for a hacker or cracker to access our most important online accounts, regardless of the complexity of our passwords, and even if our passwords had been compromised in a previous hack. This method of security is referred to in the industry as "Two Factor Authentication", and is offered as an additional, free level of security by thousands of financial institutions, online retailers, email services, online gaming sites, government agencies, and other web based services that have password based access. The process itself is very simple, takes a few seconds to set up once on each participating website visited, and then a few more seconds when actually implemented. The website turnon2fa.com/tutorials offers simple but site specific instructions on how to implement Two Factor Authentication on hundreds of participating websites; generally it is as easy as checking a "Two Factor Authentication" or similar box on the target website's user configuration or profile page, and then entering a preferred method of contact, preferably a mobile phone number. That website will now display a third line for a key code, following the traditional username and password boxes.

The White House Wants YOU to Turn on 2FA: Learn More

Turn It On

Many of the world's largest online and mobile properties offer 2FA to help prevent fraudulent activity and protect your accounts. To see if the sites and apps you use offer 2FA, and to get detailed step-by-step instructions on how to Turn It On, start here.

I have Two Factor Authentication implemented on several of my most sensitive and personal web accounts; if I access those websites from a computer, smart phone, or other device not previously recognized and confirmed as mine, the website will send a verification code as a text message to my phone. Even if I entered a valid username and password (which could have been stolen by a hacker or cracker), the website will also require that the validation code sent to my phone also be entered in a finite number of seconds in order to access the account. Unless the cyber crook also has my smart phone, they will be unable to access my account even if they have my valid user name and password. Many people are unaware that each device on the internet has a unique code number attached to it, which is also sent to websites to help verify the source of an inquiry; if the website does not recognize the unique hardware code previously verified for my computer, smart phone, or tablet, it will demand that I also promptly enter the unique access code that the website sends to my phone; no code, no access, it is that simple.

While there are many websites that explain how to implement Two Factor Authentication on their particular websites, and the process is inheritably simple, as well as similar on most participating websites, my personal favorite is still the directory at turnon2fa.com/tutorials. All of the information that anyone might need, including a 90 second video explaining the process, is available from the "Turn It On" website at www.turnon2fa.com. If you are worried about someone accessing your accounts or hacking into your email (and you should be!), you need to enable the Two Factor Authentication offered for free by many of the websites that we access.

If offered by online services, such as your email provider, and you do not implement Two Factor Authentication (or some similar technology such as the uncommon digital dongles), please do not come running to me if your email or other account is accessed by disreputable individuals. I would hate to say it, but, "I told you so!"

Websites

https://en.wikipedia.org/wiki/Two-factor_authentication
http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/
http://www.cnet.com/how-to/how-to-enable-two-factor-authentication-on-popular-sites/
http://searchsecurity.techtarget.com/definition/two-factor-authentication
http://www.pcmag.com/article2/0,2817,2456400,00.asp
https://www.turnon2fa.com
https://www.turnon2fa.com/tutorials
http://splashdata.com/press/worst-passwords-of-2014.htm
https://www.turnon2fa.com/tutorials/how-to-turn-on-2fa-for-gmail-2/
https://www.turnon2fa.com/tutorials/how-to-turn-on-2fa-for-facebook/
https://www.turnon2fa.com/tutorials/how-to-turn-on-2fa-for-apple-itunes/

Backing Up Using Windows File History
Tom Burt, Vice President,
Sun City Summerlin Computer Club, NV
January 2016 issue, Gigabyte Gazette
http://www.scscc.club/
**tomburt89134 (at) cox.net**

It can't be stressed enough that computer users need to back up their PC's data files regularly. Without backups, the inevitable failure of a PC's disk drive means that all that data becomes lost permanently. A backup regimen usually includes some kind of full clone or image process that makes a complete backup of everything on the hard drive. However, full backups are time-consuming and so are not convenient to perform every day or even every week. Also, in a full backup, probably 95% of the data being backed up has not changed since the last backup.

To complement the full backup process, it would be nice to have a facility that automatically backs up just those files that have changed within a designated set of folders. Enter Windows File History. File History appeared in Windows 8 and has been improved in Windows 10. Its ancestry goes back to Windows XP's little known or used Volume Shadow Copy feature. File History makes regular backup copies of files in a designated set of folders to a designated backup drive. Commonly, the backup drive is an external hard drive, a USB flash drive or a folder on another PC on your network. Generally, you will want to leave this backup drive plugged in continually.

File History has to be turned on and a backup location has to be designated. To get started, go to the File History Settings via the Control Panel. The screen below is from Windows 8.1, but the screen from Windows 10 is similar. Plug in the desired external hard drive or flash drive, or create a Mapped drive to a network share on another PC. In my case, I am using a 64GB USB 3 flash drive as the backup drive.

Click the "Turn On" button and specify the drive letter of your backup drive. Then click the "Advanced Settings" button and review the detailed settings for how often the backup runs, the size of the offline cache (space on the
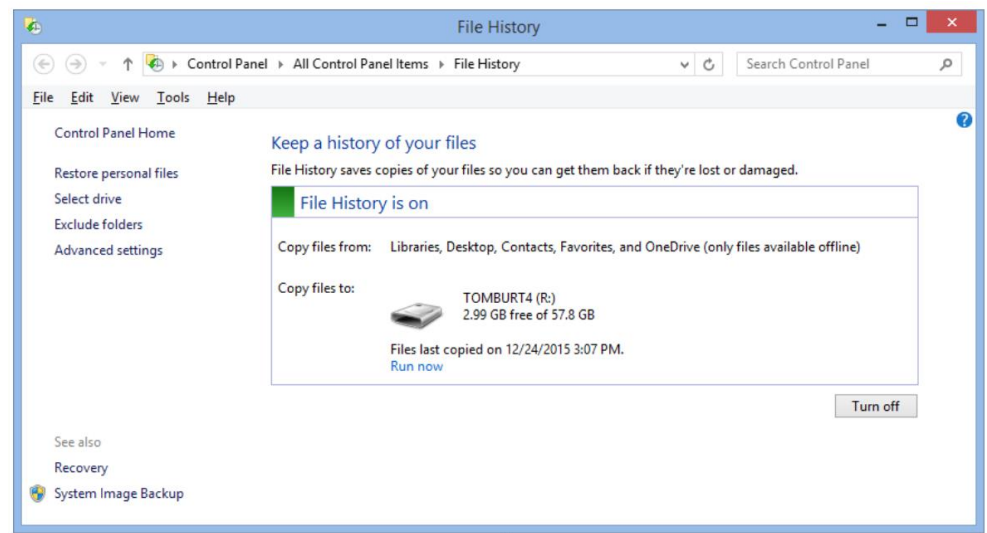
regular PC hard drive used to save copies if the backup drive is not plugged in) and conditions on how long to keep backup versions of files.
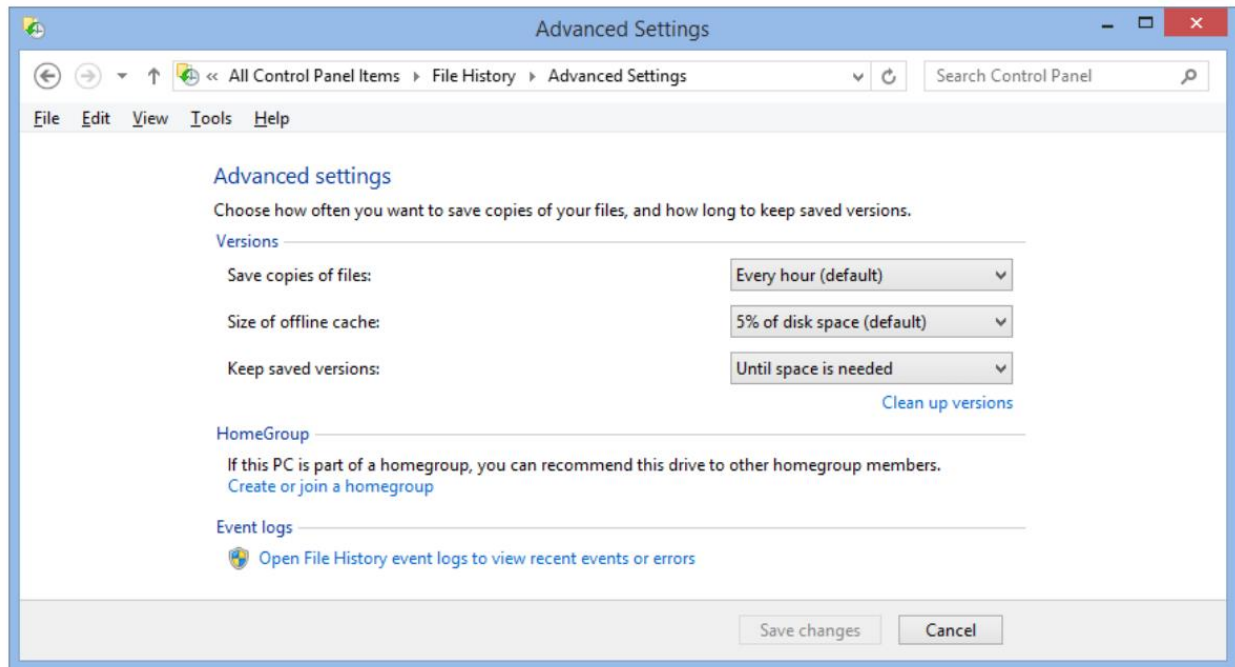
File History takes care of backing up files in my "profile folder" that change frequently, such as saved emails, Internet favorites, contents of "My Documents" and other libraries. In Windows 8.1, you can add other folders as libraries and they will then get backed up. In Windows 10, File History was improved to allow you to specify an open-ended list of folders to include in the backup.

Each time a file in one of my "profile folders" changes, File History will create a new backup version of that file, also keeping previous backup versions. I set File History to keep saved versions until the backup drive gets full. File History will then automatically delete the oldest versions to make room for new backups.

The File History backup drive is visible in the File Explorer, just like any other drive. Let's say you've accidentally deleted a file within one of the folders File History is backing up and then you also emptied the recycle bin. You can start File History and then click "Restore personal files" (see the first screen shot above) to find that file on the File History drive and copy it back to the original location. You might want to restore an earlier version of a file if the live version of the file gets damaged in some way (maybe you accidentally deleted a large paragraph in a Word document and saved it before you noticed).

This has been just a quick overview of File History. So far, I've been very happy with File History as an ongoing complement to my full system image backups. Once it's set up, it just quietly works in the background and I can be confident that ALL my data files are backed up to within the last hour.

BACK TO BASICS
Your Internet Connection
By Jim Cerny, Chairman, Forums Committee,
Sarasota Technology UG, Florida
February 2016 issue, Sarasota Technology Monitor
www.thestug.org / jimcerny123 (at) gmail.com

Today most people have and use more than one computer device that can connect to the internet. Smart phones (such as the iPhone), tablets, laptops, and desktops all LOVE the internet. In fact, most of these devices try to connect to the internet automatically. In this article we will look at how you can easily determine the answer to that all important question: Am I connected to the internet?

In the old days of ancient history, people connected their computers to a network (which could have been a private network) with a wire connection (telephone or private lines) perhaps using a telephone modem. Do you remember those telephone modems with the two rubber cups to hold the handset? Ah, those were the days when carrier pigeons were faster! But enough of days gone by.

Today the access to the internet is mostly wireless and devices can be connected to it in different ways. One easy way to see if you have internet access regardless of the device you are using is to try to go to a web page. If you can, the web page will display and you know you have access. If not, you should see a message on your screen that tells you there was a problem.

If you are using a smart phone or a tablet device, you may have a model that can use the cellular phone network to access the internet. This may work just fine, but be aware that you will be using your "minutes" or "bits" which will be billed to your cellular phone bill. I recommend that you only use the cellular network to access the internet when no other means are available.

There are two icons that seem to be universal for indicating that you are connected to the internet – a small bar graph or an "eyebrow" icon. In either case, the more "bars" you have on the bar graph or the more "eyebrows" you have, the stronger the internet signal. You should know where to find these small icons on the screen of your device, usually in a corner. You should know how to get to the "settings" option on your device and there will probably be a setting option that deals with the internet and will show you if you are connected.

Many portable devices (laptops, tablets, smart-phones) are constantly searching for a wireless internet connection. Say you went to a restaurant and wanted to get on the internet. You would look at your device's icon and see that you had no internet signal or a "not connected" message. So you would ask an employee of the restaurant for instructions on how to get connected. They would reply with the NAME of their Wi-Fi network and a PASSWORD (if required). Go to the "settings" option on your device and select the wireless network option. You will probably see a list of all the Wi-Fi networks

within range of your device. Although you could try to connect using any of the networks found, you probably want to use the network name given to you by the employee.

Naturally that network should have the strongest signal and be at the top of your list. Select that network and you will be prompted for the password (if needed). Entering the password should get your connection. The nice thing about this is that the next time you return to that restaurant your device may connect automatically without you having to do anything. That is unless, of course, they changed their password.

If you have a problem understanding this for your device, go to Google (on the internet, of course) and ask Google "How do I connect my iPhone to a Wi-Fi network", or "How do I know I am connected to the internet on my Toshiba laptop?" etc. Try to be as specific with your device name as possible. It's nice to know if you are connected and what to do if you are not.

Document Your Life with Photo-Graphic Memory
By Phil Sorrentino, Contributing Writer,
The Computer Club, Florida
http://scccomputerclub.org
Philsorr.wordpress.com / philsorr (at) yahoo.com

A photographic memory is probably something we all would like. And, just think, you can have at least the effect of a photographic memory just by using your camera and your computer to document your activities… your life.

It is amazing how much paper we collect along the way. Most of it goes neatly into file folders and then those folders go neatly into multi-draw filing cases or boxes. Before you know it you have multiple multi-draw filing cases in the den, the home office and/or the bedroom closet. Have you ever looked at the pile of paper you have collected over these many years? It's not a pretty picture. Now there are some things that we just have to hang on to, like licenses, automobile registrations, titles of any sort, and certain special papers that might have an emotional or historical attachment. But the rest of the pile might be eliminated or at least pared down. (And how about old tax forms? How many years do you have to keep the paper? Or is an electronic copy good enough for taxes paid 10 years ago?)

What I'm suggesting is that with your computer, and a scanner and a camera, you can probably cut the paper you need to save down to a very manageable size, and even eliminate some of those storage cases. The scanner is really the key here. The camera

is for unusually large items, or those things that just can't be copied with a scanner. Consider this, review the contents of some of those folders and if you need to know that something occurred, and is relevant, like an award you were given from your last employment. If you have not looked at it since you received it, then you can probably scan it in and throw away the original. I know how difficult this will be for some people, but after a little practice it will get a lot easier. (A very important thing here is that you have adequate "backup" to guarantee that you will never lose the scanned in files. If you don't have adequate backup, which means multiple copies of the data files of the scanned objects, than this is not going to be a good idea. So before you commit to this, make sure you have a good backup plan in place. Make sure that you can guarantee at least two if not three copies of the scanned in files. The first two copies could be an external or portable disk drive and the cloud and the third might be on DVD or a flash memory device.) Once the backup plan is in place and you are really using it, the fun begins. Gather your papers, separate the ones that you have to keep and make a pile of those that can be shredded after they are scanned. Do you really need those greeting cards you received 15 years ago?

In order to make sure that you can retrieve any of these "documents", it is good to establish a naming convention before you start to scan the paper documents; after all, it is no use to have all the data if you can't access it quickly. As you collect your scanned documents, you will be creating a database. Two popular ways of organizing your database are 1- by date, and 2- by event. If every file that you want to keep has a name starting with "yyyy-mm-dd" and is followed by a descriptive name, then when the digital files are put in a digital folder, they will organize in a chronological fashion. yyyy represents the year, like 2015, mm represents the numerical value of the month like 04 for April, and dd represents the day of the month like 01 for April 1. (For some databases only the year and month may be adequate.) Now, when you go looking for a document, all you have to know is the date associated with the item, and you can just look in the chronological order to find it. Let's say that if you scanned in an award that you received in June 1986, then you would look in the area of 1976-06, to find that document. Windows/File Explorer makes it easy to find scanned documents because it shows a thumbnail photo of the file, while you are searching for the file. This is especially helpful because a scanned file is usually saved as a .jpg file, a picture file.

If you do use this naming convention, then you can organize your folders to represent either years (or groups of years), or events. If you choose to be completely chronological, then the folders will be named 1980, 1981, 1982,… you get the idea. Then you could put the 1970s folders into a folder named 1980s, and you could do the same with all other decades. If you choose to organize around events, then the folders might have names like "awards," "house info," "car info," "career",.. – really, any collection of events or things that makes sense to you and any others who will use the database.

Besides your scanned in documents, you can include photos from your digital camera. If you use the same naming convention with your photos, then you can mix them in with the documents and they all will organize in chronological order. Sometimes that makes a lot of sense when you have both pictures and documents that are part of the same

event. This combination sometimes helps tell the complete story of the activities of the specific event.

Another way to organize your database is to organize your folders around events; then you might name your folders "birthdays," "anniversaries," "parties," "weddings,"… you get this idea too. So these would represent those types of events throughout the years. The fact that the files are chronologically named means they would organize chronologically inside the folders, making it easy to find a specific event within an event folder. And you can mix the two types of database folders. You could have your basic folders chronologically named, but inside a year you might have a series of events like "a vacation trip to the Grand Canyon" where the pictures from the trip would show what you saw and the documents you collected like maps and brochures from the particular destinations. As long as each file is chronologically named, the files will organize in a way that will make it easy for you to find a specific document, or group of pictures.

Not only do you save storage space, but once your pictures and documents are in your database, they are immediately available because they are literally at your fingertips (if your fingers are on the keyboard). I bet you'll be able to impress your friends how fast you can find those awards you received from your first employer. Of course there are always a few items that just can't be committed to electronic files and there are always a few pictures of the grandchildren that just must be made into an 8 by 10 for the wall. But, just think, with a lot of those paper documents shredded, and all of your photos committed to digital files, you won't need all of that paper and picture storage. It will probably free up some valuable storage space and maybe you can even make a few bucks by selling those filing cabinets.

Should I Buy a Chromebook?
By John Moss, Member, Green Valley Computer Club, AZ
Summer 2016 Issue, Green Bytes
www.ccgvaz.org / dmfitch (at) cox.net

What is a Chromebook?

Chromebooks are lightweight laptops that run an operating system called Chrome OS; Chromebooks are made by computer manufacturers like Dell, HP, Acer, Samsung, Toshiba, and Lenovo. These computers are designed to be used primarily while connected to the Internet, with most applications and documents living in the cloud. As a result, these laptops don't have a lot of onboard memory, but they don't have very large price tags, either.

Chromebooks are optimized for Google's apps, such as Gmail, Google Calendar and Google Drive. Getting set up on a Chromebook will be easy if you already use Google's services for your email, calendar and documents. However, if you use other popular services--such as Microsoft Outlook, AIM or Yahoo Mail--it might take some time to get adjusted to Google's OS.

If you use your computer primarily for email, Facebook, and general Internet surfing, you will get along just fine with a Chromebook. After all, that is exactly what Chromebooks were designed for.

Key Advantages of a Chromebook
So, are Chromebooks good enough for what you do with your laptop? Here are some of the features that draw people to a Chromebook as opposed to a Windows or Mac computer.

1. Price: The majority of Chromebooks cost significantly less than your average laptop. Chromebooks can be had for as little as $140 with mid-range models in the $200-250 range.
2. Speed: Chromebooks can power on and be ready to use in around eight seconds.
3. Battery: Chromebooks last a longer time on battery than most laptops.
4. Security: The Chrome OS has built-in virus and malware protection.
5. Sync: Chromebooks sync all your apps and passwords with Chrome browsers on other computers. This also means that you will never lose your work, as all of your data is saved on Google Drive (in the cloud).
6. Cloud Storage: You get 100GB of Google Drive storage free for two years with all new Chromebooks.
7. Updates: Chromebooks update themselves silently, automatically, and in the background.
8. Weight: Most Chromebooks are lightweight.

Disadvantages of a Chromebook
Like anything, Chromebooks, too, have their own shortcomings. It is necessary to be aware of some of the limitations and disadvantages of Chromebooks before making your final decision.

1. If you are married to Microsoft Office products, a Chromebook is not for you. Google encourages you to use its own free online suite of Office-like services.
2. Chromebooks, while startup is quick, can be slow while performing tasks such as working with spreadsheets or retrieving or saving files. This is due mainly to the fact that most of the processing is being done in the cloud.
3. Chromebooks typically only have 16 to 32GB of on-board storage. Limiting storage helps keep the price down because component costs are cheaper. Google wants you to store your data in the cloud, and that is why it includes 100GB of online storage for free for two years.
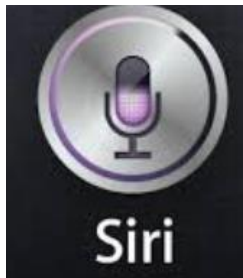4. Chromebooks have no optical drive for CDs and DVDs.

Having Fun with Siri
By Bill Crowe, Director, Sarasota Technology User Group
March 2016 issue, Sarasota Technology Monitor
www.thestug.org

Siri, Apple's voice assistant for iPhone and iPad that was first introduced with the iPhone 4S in 2011, is one funny virtual guy (or gal, depending on which Voice Gender you've chosen). Here is a list of 50 questions that you should try asking Siri. You might be surprised by some of the answers. Don't forget to ask him or her more than once for different results.

Source and courtesy of Mac World
For more Apple tutorials visit http://www.macworld.co.uk/how-to/

1. Star Wars fan? Say: "Siri, I am your father."
2. What is zero divided by zero?
3. When is the world going to end?
4. What does the fox say? (If you remember the irritatingly popular song, you can probably guess Siri's answer.)
5. Read me a haiku
6. Tell me a story
7. What came first, the chicken or the egg?
8. OK Glass
9. What are you wearing?
10. What do you think about Google Now?
11. I'm naked
12. What are you doing later?
13. Where is Elvis Presley?
14. I'm drunk
15. What is the meaning of life?
16. What does Siri mean?
17. I'm sleepy
18. If you've watched the movie Her, you should ask Siri "Are you Her?"
19. Another movie related question with a funny response: What is Inception about?
20. Do you follow the three laws of robotics?
21. Open the pod bay door
22. What's your favorite animal?
23. What is the best smartphone?
24. Stop it, Siri
25. Mirror, Mirror on the wall, who is the fairest of them all?
26. I love you
27. On rare occasions, setting early alarms can be quite amusing. Siri might say "I set an alarm for 6am; don't wake me up."
28. Roll a die
29. Who's your daddy?
30. Make me a sandwich.
31. Does Santa Claus exist?
32. What's better, Windows or Mac?
33. Where did I put my keys?
34. What's the best computer?
35. Sing me a song, Siri.
36. Is God real?
37. Will pigs fly?
38. Can I borrow some money?
39. Beam me up, Scotty.
40. Guess what
41. Talk dirty to me
42. Do you have any pets?
43. Blah, blah, blah, blah, blah
44. Why did the chicken cross the road?
45. Why do you vibrate?
46. How much wood could a woodchuck chuck if woodchuck could chuck wood?
47. How do I look?
48. How many Apple Store Geniuses does it take to screw in a lightbulb?
49. How old are you?
50. Testing, testing

Stu's Media Column
How to Take Better Photos with Your Smartphone
By Stu Gershon, Digital Photo SIG
Sun City Summerlin Computer Club, Nevada
www.scscc.club / tomburt89134 (at) cox.net

1. Hold camera HORIZONTALLY (Landscape). If you take a photo horizontally, you get a wider field of view. This "fills the screen." When you see cell phone photos on TV, they have large blank bars on the side because a phone photo has a different aspect ratio than your TV (or computer screen). If you take a landscape photo, you can always zoom in or crop to make the picture vertical and closer. You cannot do that if you've taken the photo vertically.

2. Hold the camera firmly which will keep the photo steady. Most pictures are blurry because people naturally seem to push downward when they press the shutter button, and this movement causes blur. Also, just lightly tap the shutter button - the less the movement the steadier the shot and the clearer the final photo.

3. Light - the natural light (outdoors) should always be behind or to the side of the photographer. This will eliminate "backlight" which often causes your subject to be in silhouette or look like little black stick figures.

5. Rule of thirds - if you imagine a tic-tac-toe board (with nine boxes), try to keep your subject at one of the corners of the center box, NOT IN THE CENTER BOX. This gives the picture some "movement" with either more foreground (what's in front), or more background (what's behind).

Is there software that will allow me to keep all the software on my machine up to date?
Reprinted via Creative Commons License
By Leo Notenboom, AskLeo!
www.askleo.com

It's important to keep software up to date, and there are several ways to do it. But when it comes to drivers... be careful!

The answer really depends on what you mean by program updater. If you mean a third party program that will somehow keep track of all the various versions of all the various software that you have installed and try to manage updates for you, there are a couple to try. But it's an incredibly difficult problem to solve and solve well.

Relying on the software itself

My personal approach is to use no additional software.

If software installed on my machine updates on its own or notifies me of available updates, I let it. I use Windows/Microsoft Update to update Windows itself automatically, as well as any additional software like Microsoft Office that it might keep track of at the same time.

Ultimately, I just let everything update itself if it can, automatically if possible. Everything else, I pretty much ignore until I have some reason to care. And when you think about it, most of the major software these days, and particularly the software that has major impact on security, is already updating itself one way or another.

Updaters
Downloading PatchNow at the other end of the spectrum, there are programs that will do the installs for you or inventory your system and tell you what's out of date.

Ninite is a program that I keep hearing about that automates the install of a number of very common programs, and at the same time apparently also keeps them up to date.

Ninite makes the installation easier by essentially just letting you choose from a menu of possible programs. When you click on "ok," it then just installs them all without you having to do them one at a time, avoiding most foistware in the process. One of my assistants is a real big fan, and it's on my list to look at more closely some day. See his article on Ninite at: https://goo.gl/IsgBTe

> Foistware is additional software "foisted" on an unsuspecting user when some other software is installed.
> The most common example of foistware might be additional toolbars and search add-ons that often accompany free software downloads. Foistware may, or may not, include an option to be installed, but often installs without asking.
>
> Aka shovelware   crapware   craplet

The Secunia (Now FLEXERA) Personal Software Inspector is a tool that examines the software installed on your machine with an eye towards security.

You download it, you run it, it tells you what's out of date, and then it gives you the option to update those things that need updating. I have it, but it's been a while since I last ran it, so I just now ran it on my Windows 8 machine preparing for this article. It told me about 12 programs on my machine that needed updating; all of which I understood and expected (it's a kind of side effect of how I manage my utility software). And it also told me that there are 103 programs that are up to date.

If I was going to recommend one program for most people with already-installed software, it would probably be Secunia's free tool. It does install software that then keeps running, presumably to keep monitoring what tools are out of date and need updating – so there will be a little icon that will show up in the notification area after you've run the free tool. You can turn on this off, but it is there by default.

Update scanners to avoid
I do have to point out one area where free update scanners can often cause much more harm than good, and that's with respect to drivers. There are tons of ads out there for utilities that will scan your computers for updates and a large number that are specifically targeted at updating drivers.

I avoid them all.

Don't do it. Aside from the usual scams that actually do nothing in exchange for your money, automated driver updates by these utilities often result in systems that end up with more problems, not fewer. When it comes to drivers, I recommend only updating them when offered or recommended by Windows Update; when offered or recommended by the software already on your machine for that specific hardware; or when you are diagnosing a specific problem.

So, in summary Ninite sounds very promising; Secunia is a good tool that I can recommend; and when it comes to drivers, just don't. And also, make sure to enable automatic updates that are offered by the software on your machine already, including Windows itself.

HELPING OLD PEOPLE FEEL MORE AT HOME WITH COMPUTERS

The Meeting that Was...March
By Judy

We took a look at a few more Internet of Things devices that I included in the La Verne Computer Club presentation.

7:00 pm brought us OneNote vs. Evernote. Mark Thomas (lefty.tech) uses Microsoft's OneNote as an electronic version of a paper notebook. OneNote collects and organizes the information, making it available for searching as well as sharing with others. He uses it to keep track of his customer's individual set-ups, records of when he did what to customers' devices, etc. It's a valuable resource that helps him make sure he is meeting his customer's needs when it comes to their technology. You can search by word as well as text in an image. Mark gave us a demonstration of his OneNote account (everything is in the Cloud).

Evernote is a free App (they also have a paid version) that is very similar to OneNote. I use it to keep track of what we would have, back-in-the-day, put on a post-it note. After I put my PowerPoint presentation together on the Evernote program accessed directly from my laptop, I found I like the Web version view of the program. I have been using it almost daily for a month and I've found it extremely useful for having one place where I can find info for future computer club meetings, APCUG virtual technology conferences, etc. etc. It saves me time since I don't have to remember which folder / subfolder, etc. I saved information in – it's just all in one place and makes it very easy to copy the information to my hard drive when I'm actively working on a project; i.e. APCUG's May 7 VTC. I'm always finding information in user group newsletters that I want to look at later – easy to find the URL to the newsletter in Evernote.

We also took a look at the LA County Library website where, with a library card, you can take a free Lynda.com class. We quickly looked at the Evernote and OneNote training videos. And, then we took a tour of the website with Helen Blanchard telling us that's where she does some of her genealogy research, John Metcalf had us look at the videos/movies you can 'check out'. When we looked at the magazines, we found the old program (Zinio) Dick Beekman used to read PCWorld (he now uses Texture).

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

And, the Winners were:

David Nix, Evernote for Dummies ($22)
Agnes Chaney – ream of copy paper ($5.00)

Membership Benefits Around Town

Mark Thomas Computer Support
26117 Rainbow Glen Drive
Newhall 91321
661.250.7440 / mark@marktcs.com
65+ = $10 discount on Onsite support
In-your-house support also available
iPhone / iPad screen repair

ROGERS HAS MOVED!!!
Rogers System Specialist
(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

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