Midland Computer Club

Midland Michigan

BITS AND BYTES

APRIL 2019

https://mcc.apcug.org/

ARTICLE INDEX

Articles in this Newsletter have been obtained from APCUG with the authors' permission for publication by APCUG member groups. The Midland Computer Club has not verified the information contained in the articles nor tested procedures or hardware/software. Articles do not necessarily reflect the views of the Midland Computer Club.

GENERAL CLUB MEETING

Midland Public Schools Administration Building
600 E Carpenter Street - Room D

Wednesday, April 24, 2019
6:00 P.M.

More Interesting Internet Finds for August 2018

By Steve Costello
scostello (at) sefcug.com

In the course of 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 more items I found interesting during the month of August 2018.

The Dumbest USB Gadgets You Can Buy
https://www.reviewgeek.com/5774/the-dumbest-usb-gadgets-you-can-buy/

This is not the kind of thing I usually share, but I just couldn’t believe some of the things shown. Also, if they are for sale, I assume someone is dumb enough to by one (not you or me, of course).

Here’s What You Should Use Instead of CCleaner
https://www.howtogeek.com/361112/heres-what-you-should-use-instead-of-ccleaner/

I still use CCleaner, but others have concerns lately. For those who no longer use it, this post tells you what you should use instead.

Gmail For Mobile: Disable Conversation View?
https://www.askdavetaylor.com/gmail-for-mobile-android-disable-conversation-view/

Did you know that you can disable conversation view on your mobile (Android only for now)? Dave explains what conversation view actually is, and how to disable it in Android Gmail.

What is Android Bootloader? A Complete Guide
https://joyofandroid.com/android-bootloader/

For those of you who like to know the inner workings of Android, this is a good guide to the bootloader.

OneDrive tips and tricks: How to master Microsoft's free cloud storage
https://www.zdnet.com/article/onedrive-tips-and-tricks-how-to-master-microsofts-free-cloud-storage/

This is a great read for anyone who uses Microsoft OneDrive, especially for those who are using an Office 365 Home or Personal subscription.

When 2FA Goes Bad
https://askbobrankin.com/when_2fa_goes_bad.html

Yes, I know that everyone says you should be using two factor authorization on all you accounts that support it even if SMS messaging is the only option. But, I think you also need to be aware of what can go wrong. Bob Rankin talks about what happened recently to Reddit.

How to Install Minimal Ubuntu on Your Old PC
https://www.maketecheasier.com/install-a-minimal-ubuntu-on-old-laptop/

I recently had a friend ask what he should do with an old x386 laptop with only 2GB of RAM. I told him he should put Linux on it. He did install Ubuntu on it and got everything running with only minor problems. If you have an old PC and want to try installing Ubuntu on it, check out this post. (Note: Other Linux distributions should work in a similar way. I have used both Ubuntu and Mint myself.)
****

Have you taken control of your passwords yet?

By John Fair, Smartphone & Tablet leader, Computer Users of Erie, PA
December 2018 issue, CUE Newsletter www.cuerie.com grimcyber (at) yahoo.com

CUE's April and May 2018 General Meeting Programs addressed passwords, two factor authentication and password managers. More than half of CUE's members missed one or both of these meetings and some who attended may not yet have taken seriously the suggestions made in these presentations. I am so passionate about this subject I wrote this article to give you a second chance.

No one can guarantee you will never be hacked, however there are published guidelines that I'll summarize that can minimize the risk. Only you can decide what to do with these recommendations. First, create strong passwords. This is not easy. We have repeatedly been told to create unique passwords combining numbers, special characters, upper- and lower-case letters. Complexity or randomness is good but you can add strength by making your passwords longer - as long as the site allows. Consider pass phrases or a collection of random words but remember that hackers have access to databases of song and book titles, lyrics, poems, etc. so randomize what you use.

Second, treat your email password with special care. Make it as strong as you can and never use that password or a variation of it for anything else. If hackers gain access to your email they can use it as a key to resetting passwords of your other accounts thus locking you out.

Stop thinking of hackers only as the lonely figure in a hoodie crouched over a laptop in a dimly lit room. Hacking is also done by businesses employing many folks using lots of computing power and large databases to try to separate you from your personal information and hard earned cash. They buy and sell information from data breaches and scour social media and public databases to use in their pursuits. This realization might spur you to take more seriously protecting yourself online.

Never reuse a password! If you do, your security is only as good as the weakest site on which that password is used. It's easy for a hacking program to test one stolen password on all of your sites. And slight variations of that password (add a number) or simple substitutions ($ for s) still make it easy to guess. Don't use as passwords what has become public information because of social media (pet names, birthdays, family names, addresses, phone numbers, etc.) or what can be found in public databases. They are easy guesses for hackers. And, of course, passwords that are user names, simple dictionary words, adjacent keyboard combinations, etc. make it too easy for hacking schemes. Perhaps it should go without saying, don't keep a file containing your passwords on your computer. That list of passwords you keep in writing is a bit safer if inconvenient to update.

Why do we violate good password guidelines? The National Institute for Standards and Technology (NIST) had issued password guidelines we have all been following for the last 15 years. Use at least 8 alphanumeric characters sprinkled with capitals and special characters and change passwords every three months. The unintended result of this complexity was that most people gravitated toward common patterns and hackers exploited these predictable patterns. One author of the original guidelines described the results of imposing these arbitrary rules: "It drives people bananas and they don't pick good passwords no matter what you do."

NIST's newly released password guidelines are more user friendly, requiring only what significantly improves security, putting more burden on the verifier and using 2 factor authentication where possible. Longer passwords are better. Further, they recommend you change passwords only in the event of a data breach. Arbitrary complexity that drives poor practices shouldn't be required. The verifier should screen for and not allow commonly used passwords, eliminate the need for hints and security questions and limit the number of incorrect guesses allowed. You might find that verifiers are a bit slow to adopt their end of these guidelines because of the cost involved.

Because of the number of passwords people (should) use and the complexity of each one, security experts now suggest considering the use of a password manager.

Password managers store your passwords and other information in an encrypted vault, either on your computer or in the cloud, that is accessed by a single VERY STRONG master password that is encrypted and never stored in plain text.

They can generate complex, random passwords of any length for you to use on any site. They work in conjunction with your browser and can autofill username and password for sites you have chosen.

Most have a subscription fee of from $12 to $40 a year, but a few have a limited function version for free. While Wikipedia lists over 30 password managers on the market, most experts suggest staying with one of the top four: LastPass, Dashlane, 1Password or KeePass.

I purchased 1Password before they moved to a subscription-based service and am grandfathered in using it. I found it relatively easy to use, love the excellent security ratings and have it on my Mac, iPad and iPhone. However, if you choose to follow security experts recommendations and give a password manager a try, you might want to avoid paying even a nominal subscription fee in the beginning until you understand what additional features you might need that you must pay for. I suggested giving LastPass a try since the free version does what most folks want from a password manager and, since it is cloud based, can synchronize across computer, smartphone and tablet. It is also very highly rated for security.

If you think LastPass might be of interest, first review their website for information and user forums. That will help you to understand how LastPass might be of value to you. If you want to try out LastPass, STOP!! Don't take any action until you have devised a very strong master password. The LastPass website will offer guidance in how to do that but note that you can use a very long master password and you could take advantage of the security that will offer. One way to generate a long but memorable master password is to use four or more random, unrelated words separated by spaces. To understand the logic behind this just Google "correct horse battery staple."

Really. You want a master password that is easy to remember so that you can access your password manager vault without consulting a written password.

Think this through before you download and try any password manager. You want a master password you will never forget since the password manager company does not store an unencrypted version of your password and thus will not be able to help you recover your vault contents if you should forget your master password.

If you are at all nervous about using a password manager, do not put your banking information or email password in it. I have not. You will see a real benefit from using it for all the rest of your passwords. I have also used 2 factor authentication in LastPass. That gives me the additional convenience of using my fingerprint on my iPhone and iPad to open LastPass since they are identified as trusted devices (the second factor).

Currently there are three authentication factors used to prove your identity in the digital world. One factor is username, password, PIN - something you know.

The second factor is something you have - ID badge, smart card, device (phone, tablet, computer).

And the third factor is something you are - biometric factor such as fingerprint, facial recognition, iris scan.

Using at least two of these factors provides more proof of your identity and is one of the new NIST recommendations for digital security.

Using a password manager requires some setup time. When you log in to a new site LastPass will ask if you want to save the login information (username and password) and that is very convenient. What is not convenient is changing the passwords you currently have to much more secure ones. You will have to go to each site or app and change its password.

LastPass will suggest complex, random passwords you would never remember, but the password manager will. Think about all the passwords you have and the time it will take to log in to each site or app and go through the process to change the password. This effort is what limits most people in the use of a password manager. But if all you do is institutionalize your poor password practices by saving your existing poor or repeated passwords, the password manager will do you no good. You need to make all those passwords stronger - that is the point of having that password manager: to allow you to use individual passwords that are so complex you could never remember them. You don't have to change all your passwords at one time, just start with the most important ones and work on them gradually.

Password managers can also encrypt and store other information that is convenient to have such as passport, drivers license and credit cards. I have entered all this information including the phone numbers of the credit card companies if my cards are lost or stolen. This has replaced the (insecure) scanned paper copies that I used to carry with me when I traveled.

I can't end this article without mentioning that Apple has made using password mangers easer on smartphones and tablets using iOS 12. That mobile device operating system now supports autofill in Safari and third-party apps if you are using LastPass, Dashlane or 1Password. And it makes using password managers very convenient when you are out and about.

No more list of passwords tucked into my iPad case. How insecure was that! Android Oreo and Pie operating systems support autofill with LastPass but older versions do not. Adoption of new Android operating systems is far slower than new versions of Apple iOS so Android users will be limited in their convenient use of autofill. Browser extensions of LastPass on your computer provide autofill as well as the option to fill in forms online including your credit card number. I like and trust password managers but not enough to automatically fill in my credit card number on a form whose origin may not be as trustworthy. 1Password at least requires you to acknowledge you want to fill in a credit card number, an extra step to verify that you are comfortable doing so.

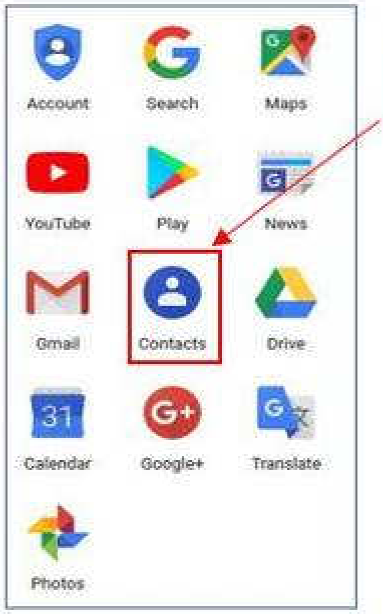
I cannot guarantee your online safety nor can I guarantee your password manager can never be hacked. I don't think you would use "Password123" as your master password but in the event, you do, all bets are off. You can, however, reduce the risk of bad things happening by carefully using a password manager with a strong master password.

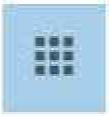
Meet the New Gmail

By Nancy DeMarte, 1st Vice President, Sarasota Technology User Group, FL

October 2018 issue, STUG Monitor - www.thestug.org / ndemarte (at) verizon.net

Gmail is a popular email service for good reason. Located in the cloud, it can be accessed from any computer, smartphone, or tablet. Once you get familiar with the interface, it is simple to use. A few months ago, I began to notice little changes to my Gmail screen. Some things were moved; others were new. After a brief search, I found that Gmail is involved in a big makeover which began in the spring of 2018. Gmail users are getting features as they become available, although everyone is not getting them at the same time. Here are a few of the changes that are included:



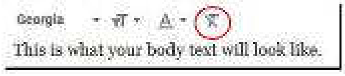


Moves and Changes

1. The Contacts list has been moved from Gmail to the center of the Google app grid. Click the grid (top right of Gmail screen) to open it. This change has frustrated users looking to add or edit a contact. When composing an email, though, Gmail still lists relevant Contacts when you begin to add a name.

2. The Google calendar icon has been added to the right side of the Gmail screen. Now you can add events or reminders to it without leaving Gmail.

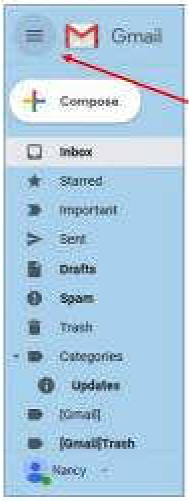
3. When composing a message, you will now find four options for text size: Small, Normal, Large, and Huge. To set your personal font, size, and text color, go to Settings (Gear icon > Settings) and find the "Default Text Style" heading. Click the "Remove Formatting" icon (right end of toolbar), then set your preferences using the down arrows. To save changes in Settings, scroll to the bottom of the page and click "Save Changes.



This is what your body text will look like.

4. If you want to forward or reply to all recipients in the new Gmail, skip the reverse arrow in the top right corner of the message. That sets up a Reply only to the sender. Instead, click the three vertical dots icon next to the arrow and make your choice.

New Gmail Main Menu (left side of screen)

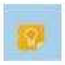


Most of these commands are familiar to anyone who has used Gmail. To save space, however, only the icons are visible until you move your mouse over them. Then the list opens to include the icon names. You can make it stay open by clicking the 3-lined icon in the top left corner of the screen, as shown.

New Gmail Icons & Features (right side of screen)

Google uses a lot of icons. The tiniest of them can have the biggest functions. To see what an icon means, hover your mouse pointer over it without clicking, and its name will appear, sometimes with more information. To use one of the features below, click it, and it opens as a right sidebar.

Google Calendar lets you view or edit your calendar without leaving Gmail.



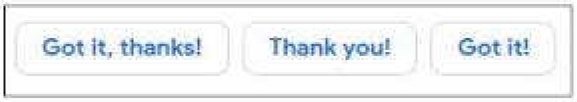
Keep lets you make notes and share them with others.

Use **Tasks** to create a To Do list and check off items as they get done.

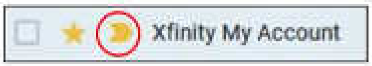
Get Add-ons takes you to the G Suite Marketplace which has add-on features and apps you might like.

Ten New or Updated Gmail Features – Available Now or Coming Soon

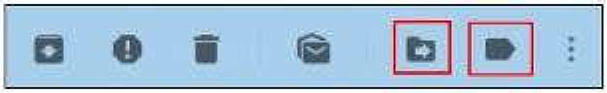
1. Smart Replies: These are canned, informal replies which appear at the bottom of some emails. When in a hurry, click one and send it as your reply.



2. Snooze: Snooze lets you remove an email from the Inbox and return it after a time you set, such as 'tomorrow'. It is useful for emails that you want to answer at a later time.
3. Nudge: When enabled, this function will suggest emails that you should reply to or sent mails to follow up on. Go to Settings to enable or disable it.
4. Confidential Mode: These functions are designed to increase security. You can set a message to self-destruct at a specific time, or you can send an email that requires the recipient to enter a code before opening it.
5. Importance Markers: Google determines which messages are "important" by putting a gold arrow next to them. In this sample from my Inbox, I clicked the star to show that I also considered it important

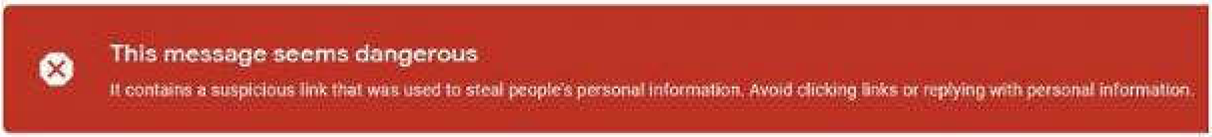


6. Smart Compose: This feature is similar to the tablet or smartphone "auto-complete" function. As you type a message, and a few grayed out words complete the thought. If you like these words, just keep typing over them. If not, type something else. You must enable this feature in Settings.
7. Labels: Labels (much like folders) are found in classic Gmail but now have new icons. You can create labels (travel, personal, etc.) and put emails into them. Just open an email to reveal the icon group shown. Click the 'Label' icon to view the labels list or create a new label. To move an email into a label, click the Label icon, check the box next to a label, and click Apply. Click the 'Move To' icon to get extra labels, like Spam or Trash.



Label Icons outlined in red: 1.Move to 2. Label

8. Offline Support: We know we can't send or receive email without the internet. But Gmail computer users can now compose, open or read Gmail when not on the internet. The Mobile Gmail version already has this capability.
9. Assisted Unsubscribe: This feature targets people who have online subscriptions to newsletters and other regular columns which come via email. If you don't open one of your newsletters often, Gmail will bring up a notice that lets you unsubscribe.
10. Improved Spam Warnings: Gmail has always popped up a notice when you try to open an email known to be unsafe. The new Gmail has larger warnings with colors based on the level of danger. Gray means Suspicious; Red indicates Dangerous.



This message seems dangerous

It contains a suspicious link that was used to steal people's personal information. Avoid clicking links or replying with personal information.

Many of the new features can help you keep your mail organized or save time, but I found a few of them annoying. For example, I'm not sure I want to be "nudged" every time I wait too long to open an email. Fortunately, most features can be enabled, disabled or hidden in Settings. A tip: Don't ignore the little icons which can be crucial to make Gmail function the way you want it to.

To find out if you already have the new Gmail, open Gmail and click the Settings icon. If the top line says, "Go back to classic Gmail," you have the new version. You can click that line and return to the old Gmail. Since you can do this at any time, consider trying out the new version for a while before you decide whether to keep it.

Cell Phone Photography

By Dick Maybach, Member, Brookdale Computer User Group, NJ
www.bcug.com n2nd (at) att.net

Most cell-phone camera photos have little lasting value, making their quality unimportant. However, these cameras are rapidly improving, and more people are using them on vacations and at important events. It now becomes important to take the care to make their pictures worth showing, meaning you must now better understand your camera and its software. The quality of your photos depends more on your photographic skills than on your camera. Good photographers take good pictures regardless of their equipment, and those with limited ability take poor ones regardless of how much money they spend or the tonnage of gear they carry. Dedicated cameras can take better pictures, but they are usually kept safe at home, while our cell phones are almost always with us.

The first step is to recognize the limitations of cell phone cameras.

- Their shapes make them difficult to hold steady, especially while making adjustments.
- They have tiny sensors, making low-light photography difficult at best.
- They reside in pockets and purses, and their exposed lenses quickly become dirty.
- Their lenses are simple with fixed apertures and focal lengths.

Taking good pictures requires learning to compensate for these limitations.

Cell phones' small display screens hide many sins. Develop the habit of transferring every image to a PC, whose large, high-resolution monitor allows you to see what you've captured, warts and all. Moving pictures to a PC also makes them available to image processing software and frees the limited storage space in your phone. Simple changes, such as cropping, exposure correction, and noise reduction, can make large differences.

You hold a conventional camera against your face with both hands. The viewfinder has optics that make the image appear to be about a meter from your eye, and there is an adjustment to compensate for aging vision. Compare this to a cell phone that you hold at arm's length where its screen is often in direct sunlight. Clearly, the latter is subject to a lot more twitching, and using a selfie-stick makes this worse, creating blurry photos, especially in dim light. To minimize this hold your phone with both hands and release the shutter with a dedicated button (often one that controls the volume) rather than jabbing at the screen. Bend your arms so that your elbows are pressed against your waist or are resting on a table if you are sitting. In dim light, rest the phone against a solid object if possible. If your near vision is limited, hold the camera at arm's length to make adjustments, but pull it closer to take the picture.

Tap the screen on the point where you want the camera to set its focus and exposure, otherwise it will make a choice. The result could be a sharply focused, well exposed shrub in the foreground and an overexposed blur in the background barely recognizable as the Leaning Tower of Pisa. If your subject is moving, set the camera to take a sequence of pictures; you'll throw most of them away, but you may capture the moment you want. Also consider a sequence when photographing a group; you'll have a better chance to catch everybody's eyes open. Always squeeze the shutter button rather than jab at it; the latter jerks the camera. Taking a photo sequence means the timing is not important, so even here you can be gentle with the shutter.

The best compensation for a small sensor is to have plenty of light when you take the picture. You can sometimes achieve this by moving so the light source is behind you; certainly try to avoid back-lit subjects. Another approach is to limit the exposure sensitivity, which the camera sets by adjusting its ISO, although not all photo apps and phones allow this. For my phone, ISO values above a few hundred produce very noisy images, which even capable photo processing software can't correct. Once you limit the ISO, you will find you have long exposure times, which means you now must place the camera on a solid support to reduce the shake. You probably also want to delay the exposure, so that it takes place a few seconds after you press the button, giving you time to ensure the camera is steady. Again, not all camera apps have this feature.

Carry a clean, soft cloth or a packet of lens cleaning paper and use it often to clean the lens. Also, keep in mind that the lens is right at the surface of the case and has no shade. You may have to use your hand to keep sunlight from striking it directly. Let's see now, you are holding the phone with one hand, operating the controls with another, and shading the lens with a third, while all the time trying to hold it steady. A shutter delay may help, but some thinking may be better. Perhaps you can stand in the shade or ask someone to cast a shadow on your camera.

The simple lens is always set for wide-angle pictures; it achieves a telephoto effect by throwing away the outer portions of the image. As a result, you should avoid using the camera's zoom feature, instead move closer to your subject. If you can't, then take the picture at wide angle and throw away the unwanted portion of the image with processing software after you move it to your PC. This gives you more flexibility on what you choose to include in the finished photo. Figure 1 shows a picture taken in normal (wide-angle) mode.

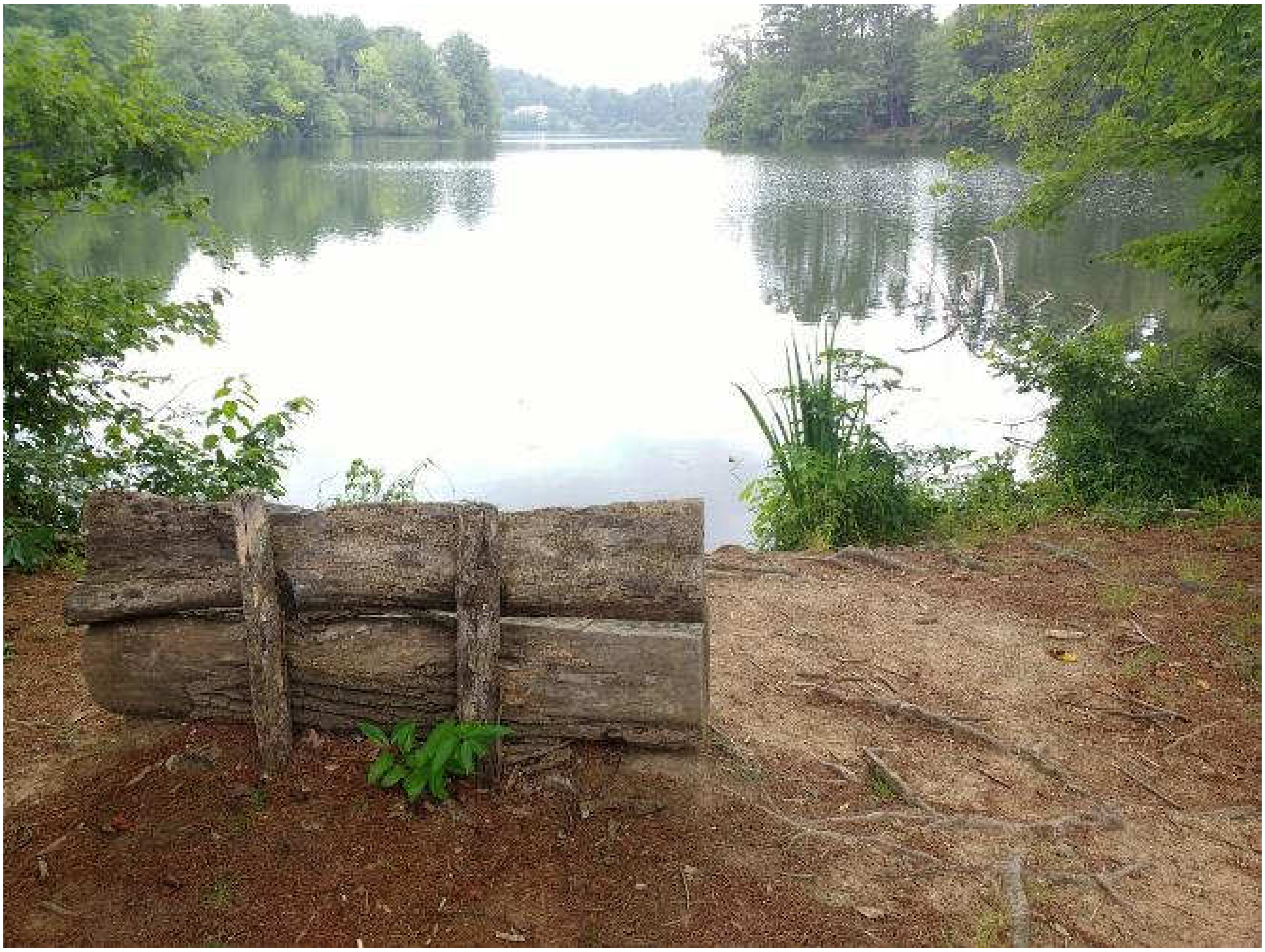


Figure 1. Image in Wide-angle Mode.

Figure 2 shows the same image taken using the zoom feature. The camera throws away the portion of shown in red; however it processes the image so that it has the same number of pixels before it stores the file. If you enlarge two images of the same scene, one wide-angle and one zoomed (you'll of course have to magnify the wide-angle one more), you will see that both have about the same resolution, meaning the added pixels in the zoomed image have not improved its quality. Now do the same experiment, but instead of zooming, move closer to your subject, and you'll find that the latter image does have more detail.

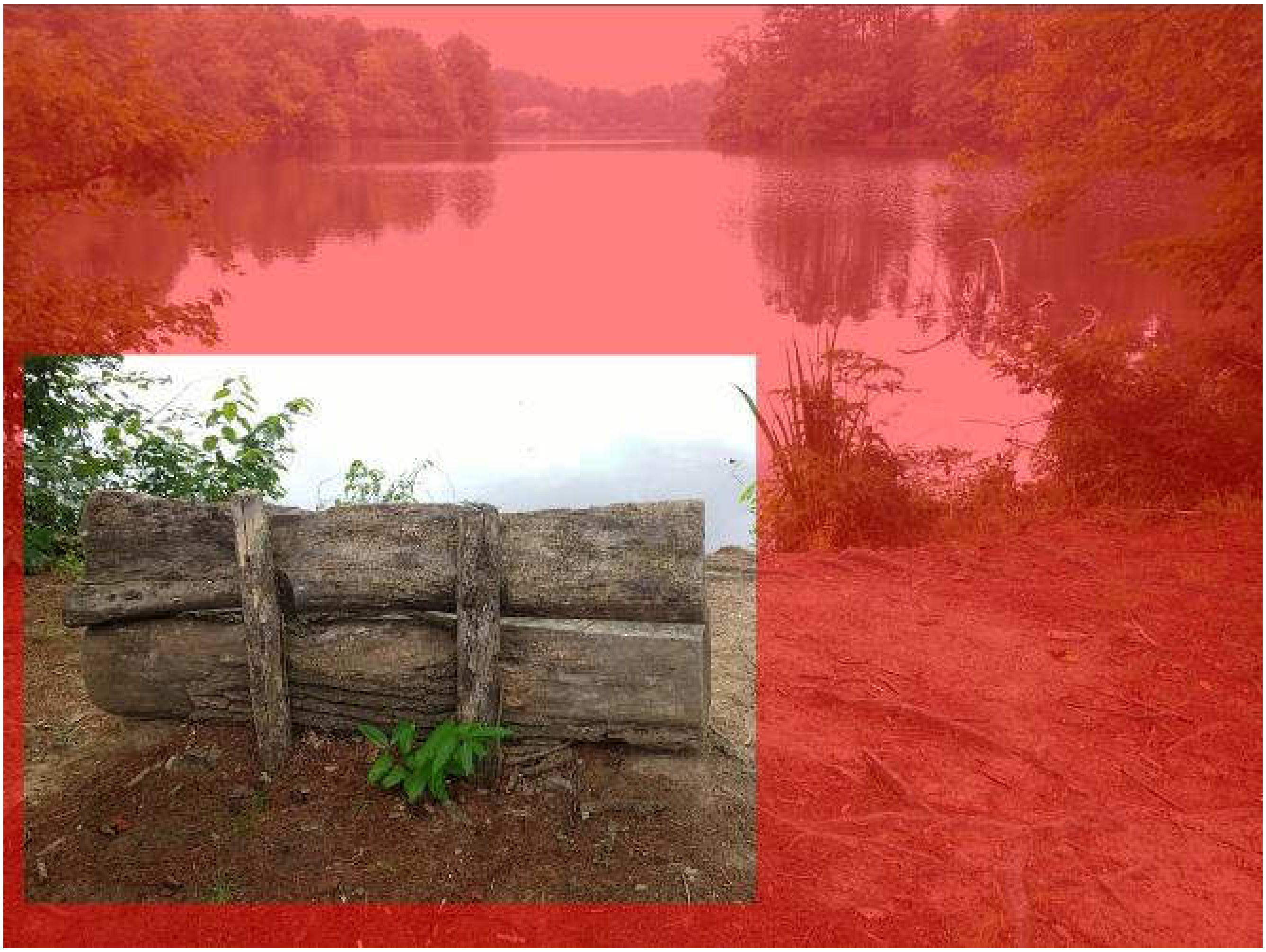


Figure 2. A Zoomed Image.

Finally, be aware that unlike a dedicated camera, a cell phone camera has a fixed aperture; it controls exposure only by adjusting the ISO and exposure time. As a result, you have little control of the depth-of-field. However, because a cell-phone camera has a small sensor, its depth-of-field is large, making it a concern only when you are very close to your subject.

Most photo apps have features you can use to improve your pictures. Figure 3 shows the default display for Moto Camera, the photo app supplied with my Motorola phone. Note the rule-of-thirds guide lines, which help to compose your photo. A common technique is to locate the main subject at one of the intersections. Some apps give you a choice of several such composing aids. Note also the yellow icon around the subject, which appears because I tapped the screen there to create a focus and exposure point. This app also allows you to adjust the exposure by moving the white spot around the icon circle. The other visible controls are (on the left):set manual or automatic mode, set the delay, control the flash, take a high-dynamic-range photo, and (on the right):select movie, still, or panoramic mode, and switch between the front and back cameras. The large white button on the right is the on-screen shutter release.

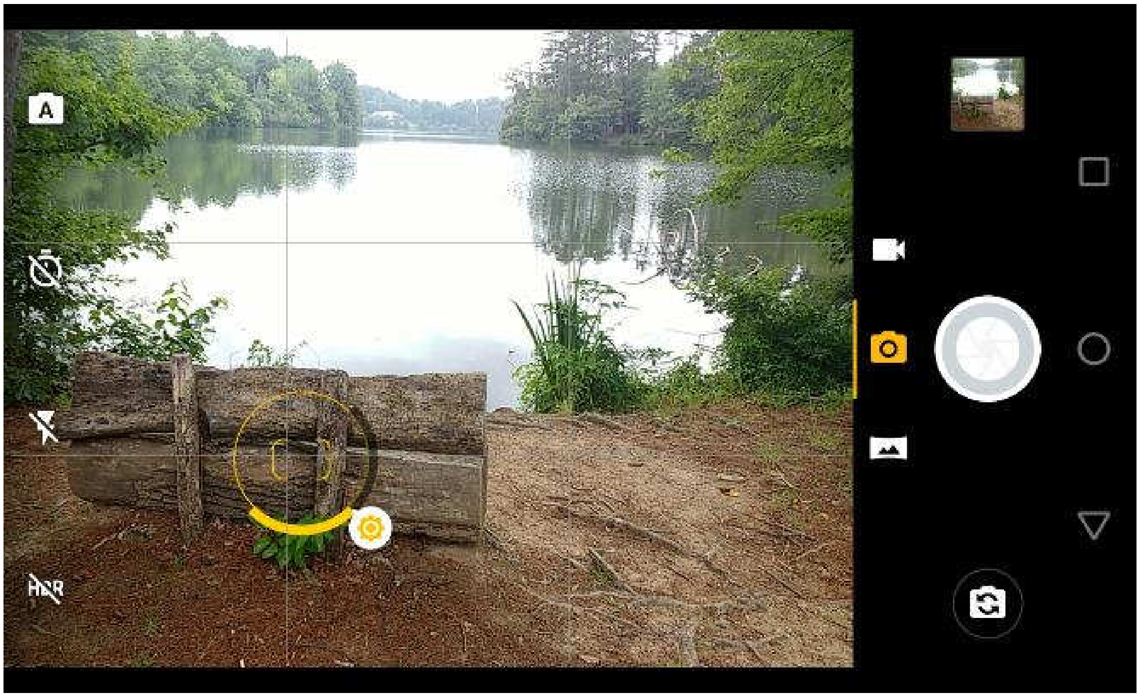


Figure 3. Moto Camera Display.

Surprisingly, I found the photo app supplied with my phone (available from the Play Store as Moto Camera) to be the one I use most often. It allows for adjusting the focus, white balance, shutter speed. ISO, and exposure, includes an exposure delay, high-dynamic-range (HDR), panoramas, and can disable the flash. It doesn't allow photo sequences, and I use Open Camera for this feature.

Figure 4 shows the manual mode of Moto Camera, which allows considerable flexibility. The controls are, from left to right: focus, white balance, shutter speed, ISO, and exposure compensation. You move the white circles to make adjustments. Except for exposure compensation, a white dot at the bottom of its arc means that adjustment is automatic.

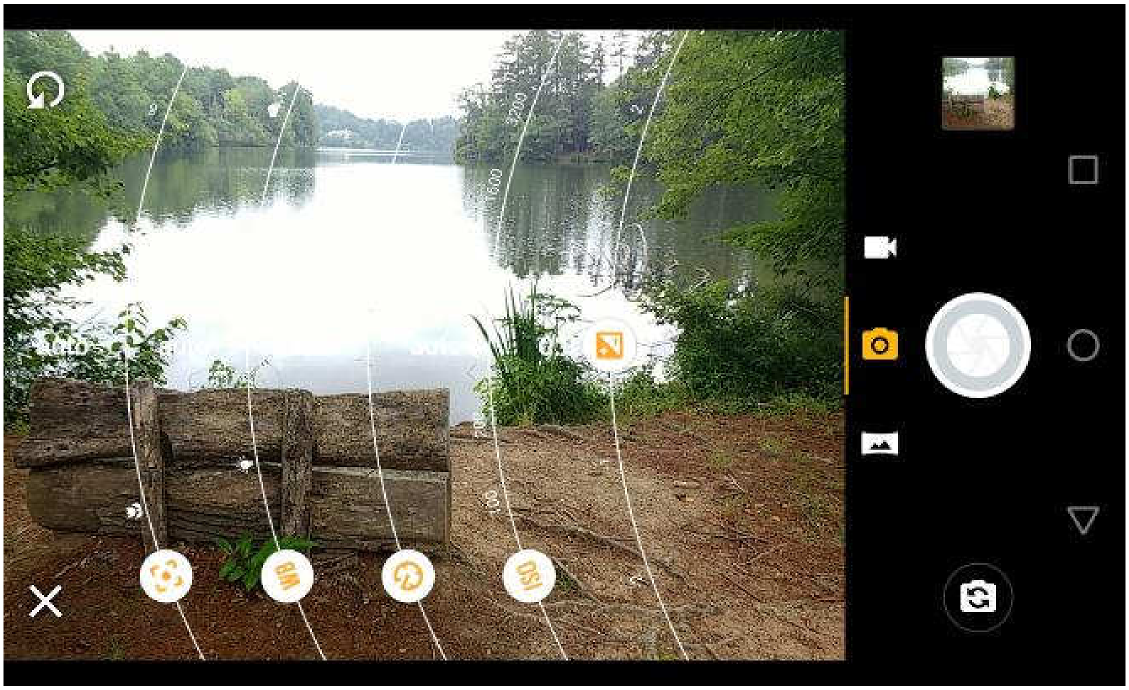


Figure 4. Moto Camera in Manual Mode.

Many apps offer high dynamic range (HDR) where they take several photos at different exposures and combine them with the goal of showing details in both the very bright and the very dim areas. In my experience, it is very difficult to obtain acceptable HDR results, even with a professional camera and high-quality photo processing software. The results with a phone camera and its app software are often disappointing, but you have nothing to lose by trying. The technique won't work on moving subjects; even leaves moving in the background will cause problems. Some apps, for example Open Camera (available from the Play Store), have a dynamic range optimization (DRO), which processes the shadow and highlight areas differently in a single image. This works for moving subjects and I've found the improvement often approaches that using HDR. Open Camera will also save the individual images it combines into an HDR one, which enables you to use your PC processing software and perhaps get better results than with the app's software.

The capabilities of a photo app depend on the version of Android under which it runs and on what features the vendor has enabled. To get everything you need, you will have to experiment and probably install more than one photo app.

We can summarize this discussion as follows.

- Hold the camera firmly with both hands and use a dedicated button to release the shutter and squeeze rather than jab at it.
- Brace your elbows and in low light rest the camera on a firm support. Consider using a shutter delay to reduce camera jiggle.
- Minimize using the zoom feature but take your pictures at wide angle.
- Always select the focus point.
- Keep your lens clean, and shade it from direct sunlight.
- Look at your images on a large, high-resolution monitor.
- Experiment with camera apps to find those that best suit you and your phone.

With a little care and practice you can take surprisingly high-quality photos with your cell-phone camera, often approaching those from dedicated cameras and far surpassing those from cameras of just a few years ago.

How to stay on course when scrolling up & down a web page

By John Krout, Member, Potomac Area Technology and Computer Society, VA
www.patacs.org - krout75 (at) yahoo.com

At a recent PATACS/OLLI meeting in Fairfax City, a question was raised about scrolling up and down a web page: why does the browser sometimes suddenly revert to the top of the page?

This experience, no doubt familiar to many of us, has to do with pointing device behavior. With a normal mouse or track ball, you click and hold the button down on the vertical scroll bar on the far right of the web page, and then drag the scroll bar up and down.

While doing that, often you are intently reading the visible portion of the web page, and not watching the mouse pointer. I run into this a lot when examining the CNN.com home page. It is easy to let the mouse pointer drift slightly right or left. When the pointer moves off the vertical scroll bar, the web page automatically reverts to the top of page. This much I explained at the meeting.

Another member proposed a solution, one that I had not previously thought of, and I think it is a very useful solution: obtain a trackball or mouse with a vertical scroll wheel. Instead of moving the pointer in the familiar way, simply rotate the scroll wheel. Up and down the page goes, very reliably, with no drift.

Now, if the problem described above is unfamiliar to you, then read no further. The rest of this article is a brief survey of products you may wish to know about if the problem is one you would like to solve.

After the meeting, I took a look on the Web at mouse and trackball products including such a wheel. They are not very expensive.

This is not a recommendation or a review. I just want to show you the bottom of the price range and some options.

From here on I focus on products available from Amazon because of the small commission paid to PATACS by Amazon when you use the link to Amazon appearing on the PATACS.org home page and you spend money on Amazon. The sum total of that income to PATACS from Amazon was a few hundred dollars in the last full fiscal year for the club. That is equivalent to 20+ additional dues-paying PATACS members, far more than I expected, and is why the club offers that opportunity.

I used this search on Amazon: *mouse with scroll wheel*. Then I sorted on low price to high price.

On Amazon, I found there are USB scroll wheel mouses for less than $10, and wireless and Bluetooth scroll wheel mouses for less than $20. All provide a wheel on the top of the mouse, equally accessible for right-handed and left-handed use. You will see many such products, even in a choice of colors.

I happen to use a USB trackball for my desktop computer at home, partly because the open space on my desk is often not sufficient for moving a mouse around. So I also looked at trackballs equipped with a scroll wheel.

I used this search on Amazon: *trackball with scroll wheel*. Then I sorted on low price to high price.

It happens that several such trackballs exist. USB trackballs with scroll wheel start at less than $25.

Logitech tends to put the scroll wheel on top and the ball on the side, which means it is difficult for lefties. Maybe they make left handed versions; I did not nose around enough to find out.

I found a very interesting innovation from Kensington, the trackball brand that I have been using. Their trackball scroll wheel is in fact a ring around the centered trackball. Incidentally, in that same set of Amazon search results, I also found keyboards with a trackball and scroll wheel built in. As you might guess, these are more expensive than standalone trackballs, but if your desktop real estate is extremely limited, the all in one keyboard may be of interest to you.

Kensington wired mouse

Logitech wireless trackball with scroll wheel

Kensington trackball mouse with scroll ring

APCUG VIRTUAL TECHNOLOGY CONFERENCE
MAY 4, 2019

TRACK 1

1:00 PM ET

WordPress Introduction for Creating Websites
Mark Zinzow, Member, Rochester WordPress Users Meetup

Mark's presentation will cover:
- Contest Management Systems
- Why choose WordPress, or not?
- Hosting, DNS, and software expenses
- WordPress jargon
- How to create a WordPress site
- WordPress plugins
- WordPress help, tutorials, documentation, etc.
- General Data Protection Regulation (GDPR)

2:00 PM ET

Are Your Bits Flipped?
Joe Kissell, Author and Publisher, Take Control Books

Just as a single "flipped bit" in computer code can bring an otherwise reliable app crashing to a halt, a single misconception in your understanding of personal computing technology can cause all manner of problems—including lost data, wasted time, and frustration as you live and work in today's increasingly digital world. In this presentation based on his book Are Your Bits Flipped?, author and publisher Joe Kissell untangles common confusions surrounding the high-tech products and services we all rely on every day. Find out why conventional wisdom is often wrong, why you might be worried about all the wrong things, and how improved knowledge of topics like privacy, web browsing, email, and encryption can make you smarter and more efficient.

3:00 PM ET

Windows 7 Sunset
Greg Skalka, President, Under the Computer Hood User Group

Windows 7 extended support and consumer security updates will end on January 20, 2020; no more updates or fixes, including security fixes. Greg will discuss options for those who are still fans of Windows 7.

TRACK 2

1:00 PM ET

Google Photos: 7 favorite features
Chris and Jim Guld, Geeks on Tour

Join Chris and Jim as they take us through their 7 favorite Google Photo features: Editing, All your photos in one place and searchable from any device, Shared Library – automatically save partner's photos of you, Shared Albums, Make Movies, Google Lens for reading business cards, and how to Navigate to a Photo's Location.

2:00 PM ET
Youth and Technology
Bill Crowe, 1st Vice President
Sarasota Technology Users Group

What will the world look like in 20 years? It seems that all the youth are so engrossed with their technology that they do not even know how to really socialize or communicate face to face. That is not all together true. They will most likely not have hunched backs and be couch potatoes at the age of 25 from hunching over their smart phones and playing computer games. That said what will happen to our culture. We will learn about how our youth are using technology, how it can have both a positive and negative affect on them and what we as adults can do to encourage the positives and discourage the negatives. Bill has done substantial research on the subject and will be presenting his conclusions.

3:00 PM ET
What's an App?
Jim Glass, President, Glendora's Computer Club

What's an App? Where do I get them? Are they secure? What can I do with them?
Jim's presentation will cover all of the above and more during our exploration of Apps AKA applications, programs …..

4:00 PM ET
ROUNDTABLE DISCUSSION

Let's talk about Websites. Do you use it as a recruiting tool? Or is it just for your members. Will a prospective member find information that will encourage them to attend a meeting? Bring you ideas to share....

For more information: https://apcug2.org/apcug-2019-spring-virtual-technology-conference-vtc32/

APCUG's Virtual Technology Conferences are FREE!

Attend using your computer, tablet or phone with the Zoom.us app.

Download the app for the device you will be using at:
https://zoom.us/download

Sessions are 50 minutes with time for Q&A
Register once via Eventbrite. You do not need an Eventbrite account to attend the conference

Before the event, you will receive an email with directions and links for attending both conference tracks.

Day of conference, after connecting via Zoom, it is very helpful if you sign into each presentation you attend via the Chat Box; first and last name you used to register at Eventbrite. Why? If all of the questions aren't answered during the session, the rest of the answers will be sent to you. Or, there might be a handout.

Register at Eventbrite