Midland Computer Club

Midland Michigan

BITS AND BYTES

JUNE 2018

http://mcc.apcug.org/

ARTICLE INDEX

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

Wednesday, June 27, 2018
6:00 P.M.

Educational, Fun, and Interesting Web Sites (submitted by Carol Picard)

How-to Geek

What Does CCleaner Do, and Should You Use It?
https://www.howtogeek.com/172820/beginner-geek-what-does-ccleaner-do-and-should-you-use-it/

How to Choose the Best VPN Service for Your Needs
https://www.howtogeek.com/221929/how-to-choose-the-best-vpn-service-for-your-needs/

Headlines About "The Dark Web" Are Usually Nonsense
https://www.howtogeek.com/fyi/headlines-about-the-dark-web-are-usually-nonsense/

The Best Free Screenshot Apps for Windows
https://www.howtogeek.com/349652/the-best-free-screenshot-apps-for-windows/

Standard Ebooks Offers Public Domain Downloads That Aren't Ugly
https://www.howtogeek.com/fyi/standard-ebooks-offers-public-domain-downloads-that-arent-ugly/

How to See What Data Windows 10 is Sending to Microsoft
https://www.howtogeek.com/348699/how-to-see-what-data-windows-10-is-sending-to-microsoft/

How to Disable the Timeline on Windows 10
https://www.howtogeek.com/348138/how-to-disable-the-timeline-on-windows-10/

Duck-Duck-Go

Protect Your Privacy on Windows 10
https://spreadprivacy.com/windows-10-privacy-tips/

Protect Your Privacy on Android
https://spreadprivacy.com/android-privacy-tips/

Duck Duck Go Blog
https://spreadprivacy.com/

Power Strip Versus Surge Protector—Which Do You Need?

By Tim Elder, Treasurer, Canton Alliance Massillon User Group, OH
February 2018 issue, The Memory Map -- www.camug.com -- treasurer (at) camug.com

These two devices are quite similar in appearance, but they are definitely not the same. If what you need is an extension cord with multiple outlets, a power strip will work fine because it acts as an extension of the wall outlet but does not add any protection capabilities. It will have multiple outlets, probably an on-off switch, which can disconnect all outlets at once, and maybe a circuit breaker or fuse. But if you are connecting to a computer, TV, home theater, or other electronics, a power strip will NOT be fine, because it cannot protect your expensive electronics from power line surges; for this you need a surge protector, sometimes called a surge suppressor or surge diverter.

An electrical surge is an intense very short duration voltage spike.

A surge protector does its “magic” by means of built-in electronic components which quickly cut the power when an electrical surge comes through the mains (this is a British term which works well for the electrical distribution grid—the system bringing electrical power into the building) or from electric motors within the

house which can reflect surges back through the wiring. In order to work properly, a surge protector must be connected to a grounded outlet. A surge protector will cost more than a similar-appearing power strip.

The difference in capabilities of the two devices will be found on the packaging, and on the back of the device if the packaging has already been removed. Power strips and surge protectors will often be placed near each other on the store shelves; so, make sure you read the readin' to make sure you get what you need. A surge protector is generally, clearly labeled as such, but its capabilities can vary considerably.

Surge protectors are rated by the amount of electrical energy they can absorb, either all at once or bit-by-bit; this will certainly be advertised on the packaging. Suggested specifications to look for, which can be misleading if you are not paying attention, include: 2000 joules where more is better; and, sometimes listed, response time which is usually in nanoseconds, shorter is better.

How do you know how much of this protection is left? The number of joules is like a reservoir, but you can't tell how much has been used already. Thus, a surge protector should be replaced, say, after 5 years; after this it can serve as a power strip. Since our memories are fickle, put a self-adhesive note on it saying when it was installed. A surge protector will likely have a pilot light to tell you when the connected items are protected from line surges. If this light goes out or changes color, the surge protector has given its life to protect whatever was connected. It will have to be replaced. But this pilot light is not foolproof, meaning that it can give false assurance.

When purchasing a surge protector, be sure to get more outlets than you think you need and remember that transformer plugs can block adjacent outlets. Also remember that a surge can come in over phone or cable wires; look for connections for these if your setup uses them.

Many surge protectors also have USB charging ports. Labeling should also include a United Laboratories seal. When I was checking the stores, the price varied from $10 to $60 depending on the number of outlets, the number of USB charging ports, and the joule capacity which ranged from 500 to 4350. The selection at Staples was much better than at Walmart.

As with the protection pilot light, a surge protector is not foolproof, and you probably do not want to gamble with Mother Nature. If an electrical storm is approaching, you should shut down the computer, then turn off the surge protector switch or unplug it. Anytime the power goes off suddenly for any reason, your first move should be to turn off the surge protector switch to stop the risk of a surge when the power comes back on.

If you want even more protection than a surge protector offers, consider a UPS (Uninterruptible Power Supply.) These offer a battery backup which provides a few minutes to properly save files and shut down the computer. They can also smooth any bumps in the incoming electrical supply; this capability is called AVR, Automatic Voltage Regulation. A surge protector can be purchased to protect the whole house from external surges, but these must be installed at the service entrance with the supply disconnected. An electrician is recommended.

Securing Android

By Dick Maybach, Member, Brookdale Computer Users' Group, NJ
January 2018 issue, BUG Bytes - www.bcug.com - n2nd (at) att.net

Your PC remains at home behind locked doors, accesses the Internet through a firewall, and has its software updated regularly, but none of this is true of your Android device. If you haven't thought about its security, you are overdue to begin. We obtain PC software updates directly from the software vendors, e.g. Microsoft issues these for Windows. Google releases monthly security updates for Android, but the only end users that get them are owners of Google Nexus and Pixel devices. All others receive them through their device vendors and usually get them much later, if at all. To see the date of your last security update, go to Settings, then About phone (probably the last item). Figure 1 shows the lower part of the resulting screen. (This is for a Motorola G[4] using Android 7; screens on other configurations may differ.)

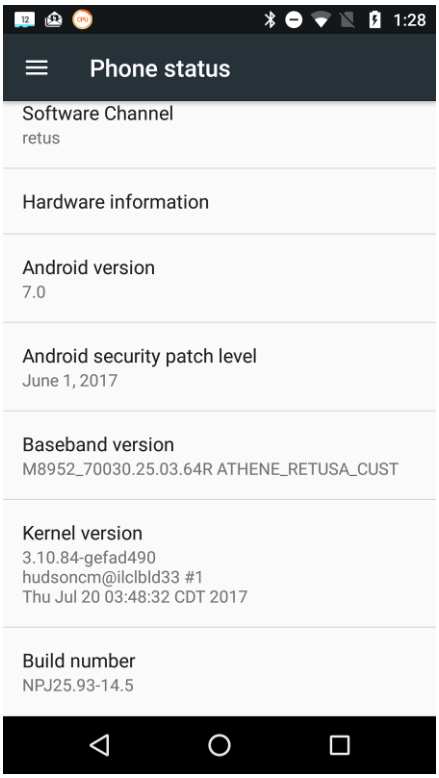


Figure 1. About Phone Screen

This shot was taken in November and shows that the latest security update had been made in June, which was not reassuring (although I did receive the September update later in November). Many security professionals believe that keeping software up to date is the most important security measure, more so than using anti-malware software.

That your Android phone is subject to damage and loss, probably runs on software with known vulnerabilities, and lacks protection from Internet aggressors are beyond your control, but there are things you can do to reduce your risk.

Be sure your phone is protected by going to Settings then Security and enabling screen lock; a password here is more secure but less convenient than a PIN. Don't use None or Swipe, as these make your device fully accessible to anyone who picks it up. I don't care for the Smart Lock features as they unlock your phone for extended periods. Making passwords visible isn't as dangerous as it sounds, as it displays only the last character you enter and only for only a short time. I find it greatly reduces errors when entering passwords. I haven't encrypted my entire device because all my sensitive data is encrypted separately. Figure 2 shows the upper portion of the security screen.

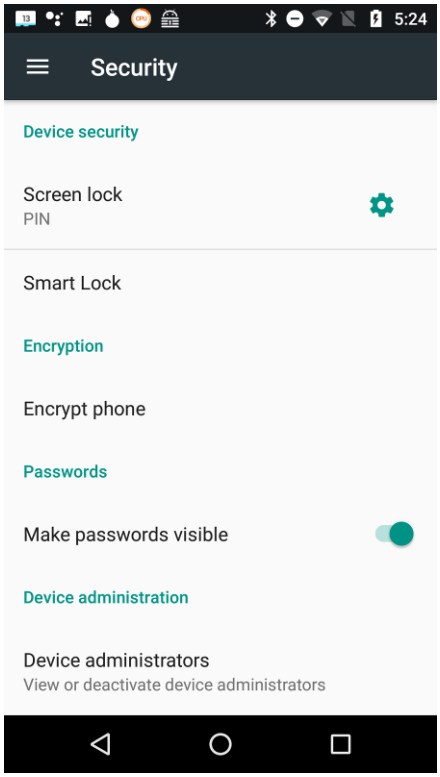


Figure 2. Settings/Security Screen

Sanitize your browser favorites, especially if you sync them with your PC over the Internet. Review all your favorites. (With Firefox, open the menu, select Preferences, then Security, and finally Saved Logins…; for other browsers check the Internet.) Delete any, such as banks, that are sensitive, and the next time you log into one with a password, your browser will offer to save it. Select “Never for this site,” or the equivalent

Use a password manager that stores its data in an encrypted database and use a non-trivial password for it. I like Keepass2Android Password Safe by Croco Apps, as it uses the same database as KeePass, KeePassX, and KeePassXC, which are available for Linux, OS X, and Windows. You can transfer the database file among all your devices. Because it’s encrypted, you could sync it using a cloud service, but I prefer not to so expose it. Keep all your sensitive information here, passwords, PINs, account numbers, passport numbers, etc. Figure 3 shows Firefox on a site’s login page with KeePass2Android active.

To get to Figure 3, I opened KeePass2 and selected the Adafruit entry. Then when I launched Firefox and opened the Adafruit location, it displayed a keyboard icon in the bottom menu bar. I selected this and then selected the KeePass keyboard, which added a second lower-menu bar. Now placing the cursor in the Username box and tapping the User button (in the second lower-menu bar) causes KeePass to enter the name in that box. Then placing the cursor in the password box and tapping the Password button does the same for the password. (Of course, I had previously entered the Adafruit information, its URL, my username, and my password, in KeePass.) All this takes longer to describe than to do.

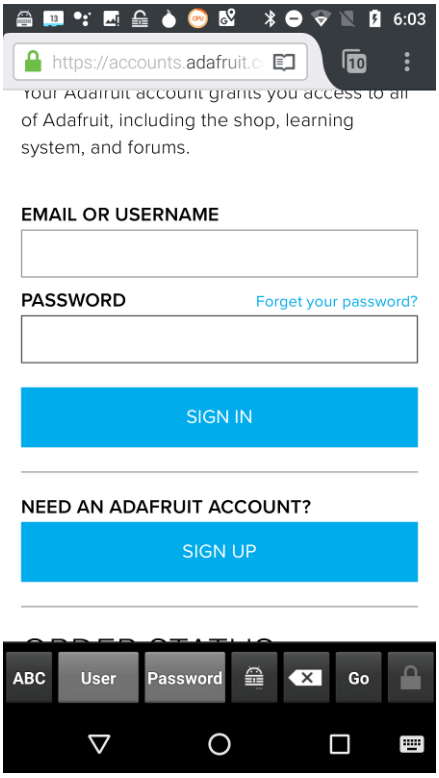
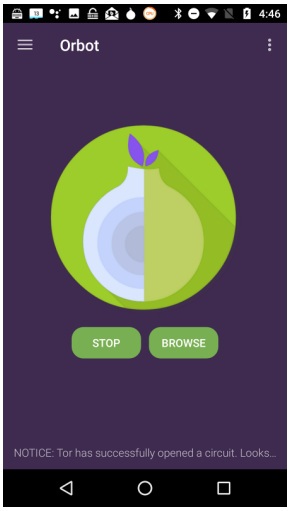


Figure 3. Web Login Page with KeePass2Android Running



Be careful when using public wi-fi, as with readily-available software anyone on the same network can view every packet you send and receive. Fortunately, Tor is available for Android, and you should use it whenever you access the Internet using a public wi-fi hot spot. Install the app “Orbot: Proxy with Tor” from Everyone, which will ask that you install “Orfox; Tor Browser for Android, “also from Everyone. Orbot is a proxy that enables access to the Tor network, and Orfox a secure browser that uses Tor. When you use these, a wi-fi snoop will see only encrypted packets and won’t know where they are going or from where they are coming. Figure 4 shows the opening Orbot screen. (While we’re considering networks, don’t ever set your device up as a portable hotspot, which makes it a server.)

Figure 4. Orbot Opening Screen

Because of its vulnerability, an Android device is not a safe place to store data. Don't keep anything in it, unless its encrypted, that you wouldn't write on a post-it stuck to the roof of your car. Encrypt anything sensitive, such as passwords and banking information, and as soon as it's convenient, copy your new data to a PC. Although it's not a security issue, be cautious about purchasing copyrighted items encumbered with Digital Rights Management (DRM) features. Some can be used only on a single device, which means if your phone is lost or damaged, you also lose these. See my December 2017 article (available at http://www.bcug.com) for sharing data among Android devices and computers.

Every app you install adds potential security vulnerabilities, and many consume resources even when they appear not to be running. Their icons clutter your screen, making it difficult to find other apps, and their files fill your storage space. Your device can become less usable with each visit to the Play Store. Google is a large, technically competent organization, with procedures that ensure that Android is a high-quality, secure product. However, this isn't necessarily true of app developers, whose competence is unknown. Google performs security audits on all Playstore apps, and your risk of installing malware is just 0.05 per cent if download apps from only there, compared to an overall infection rate of 0.71 per cent. That an app is popular doesn't mean it's well-designed or safe. Take a disciplined look at your app collection and remove all you don't use regularly. This is one of the most important security measures you can take.

Some apps add considerable risk. For example, some checkbook programs require linking to a bank account, and anyone now accessing your phone could potentially also access your bank account. If you really need this feature, you must secure your phone with a secure password, e.g. one that is long and difficult to guess, which of course will make using the device less convenient.

If you keep your Android data synced with your home computer, you can be casual about backing it up. Nevertheless, backing up may be good insurance if it also backs up your installed apps, since if you lose your phone, you could reinstall them on a new one.

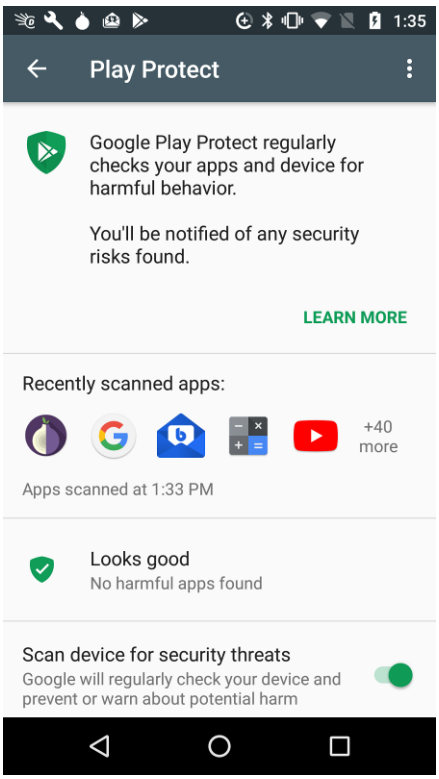


Figure 5. Google Play Protect Screen

Be sure Google Play Protect is operating by going to the Google Play Store app, selecting the menu (the icon at the left of the menu bar), and then Play Protect; the Scan device for security threats item should be turned on. See Figure 5.

This checks apps as you download them and periodically scans your device for threats. I don't think other anti-virus programs are needed. Android is less vulnerable than Windows, although "less vulnerable" is not the same as "invulnerable." If you keep your device synced with your home PC, and protect any sensitive data with encryption, you haven't much at risk. That an anti-virus vendor would like to sell you an app doesn't mean you need one.

If your device is lost, you can use Google's Android Device Manager service to help you find it and to safeguard its data. Go to http://www.google.com/android/devicemanager and log in with your Google password. The eventual result will be the screen in Figure 6.

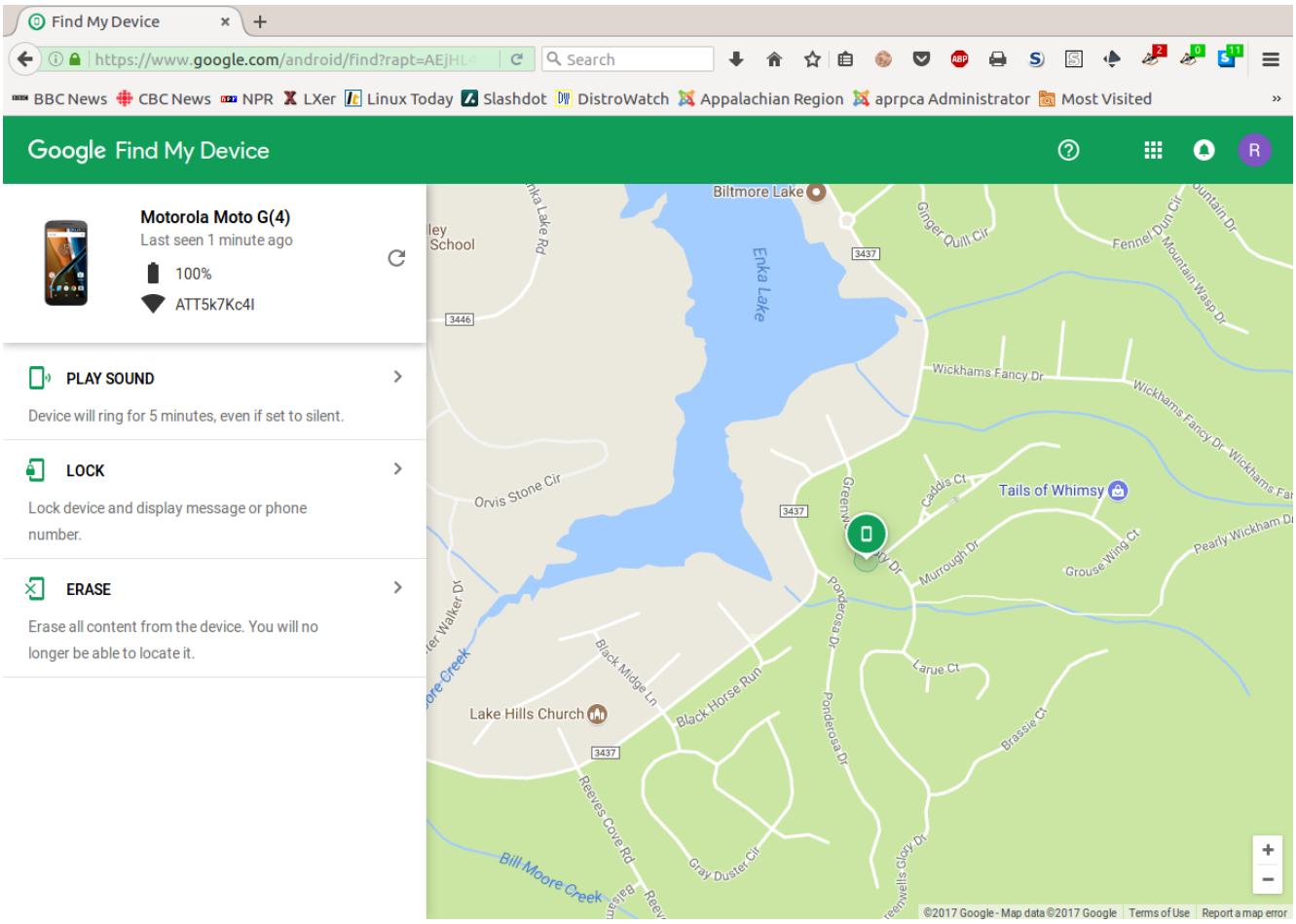


Figure 6. Google Android Device Manager

This shows you the location of your lost device and gives you the options to have it make some noise (in case its misplaced), lock itself (if you expect to get it back), or wipe its memory (if you think it's gone forever), The last two won't get your phone back, but they will prevent whoever has it from using it or accessing your data. Note however, there is no way to undue the last.

With these few simple precautions you can significantly reduce the risks of using your Android device. For more information on Android security see http://source.android.com/security/.

Mobile Highway
Items of interest to Mobile Device Users

One Dongle to Rule Them and In the Darkness, Bind Them

By Chris Woods, Member, Under the Computer Hood UG
February 2018 issue, Drive Light -- www.uchug.org -- 1editor101 (at) uchug.org

When you get a wireless mouse, keyboard or any other of a myriad of wireless devices, what is common is that they all come with their own dongle. Most operate within the 2.4 GHz range and are mated to that device. Lose the dongle and you might as well kiss it goodbye. Ever noticed, on some of these devices, a tiny orange asterisk tattooed upon its surface?

The orange asterisk symbol stands for Unifying Receiver, one of the dirty little secrets of peripheral manufacturers. Why have all your USB ports taken up with dongles when only one is required, the Unifying Receiver?

Logitech introduced its Unifying Receiver back in 2009. At first, it was only for Logitech's line of devices, and it was limited to keyboards and mice. Many manufacturers have quietly included the same function on their peripherals. One of the pieces that make this magic work is the Logitech Unifying Software (http://support.logitech.com/en_us/software/unifying).

The software acts the same as a Bluetooth pairing, mating the device to the receiver. To set up this paring you first download the software. Then plug in the Unifying Receiver to a USB port and allow its driver to load. Finally, you run the software. When you run the software, there is a prompt that will ask you to turn each device (mouse, keyboard, etc.) off and on. If the device is compatible it is paired to that one receiver. To add other devices later you run the software again and follow the prompts. Right now, it's still limited to six devices per receiver. A space saver for systems that are port limited, provided the device is recognized as compatible. As of this writing, according to Toms Hardware:

"A Logitech Receiver will pair up to 6 Logitech and non-Logitech peripherals, provided they both have the symbol. A Microsoft Receiver will pair most devices...but not Logitech."

I have not seen any compatibility lists, but I can confirm from a tech standpoint that most peripherals that have the symbol pair without issue. I have a user at work that has a Logitech Unifying Receiver with an Asus keyboard, a Logitech mouse, and a Wacom drawing tablet. The limiting factor seems to be if your OS sees the device as an HID (Human Interface Device). For someone using many wired HID's and wanting to switch to wireless to open USB ports the Unifying Receiver can come in very handy.

OneDrive Files on Demand

By Nancy DeMarte, 2nd Vice President, The Sarasota Technology Users Group, FL
March 2018 issue, Sarasota Monitor -- www.thestug.org / ndemarte (at) verizon.net

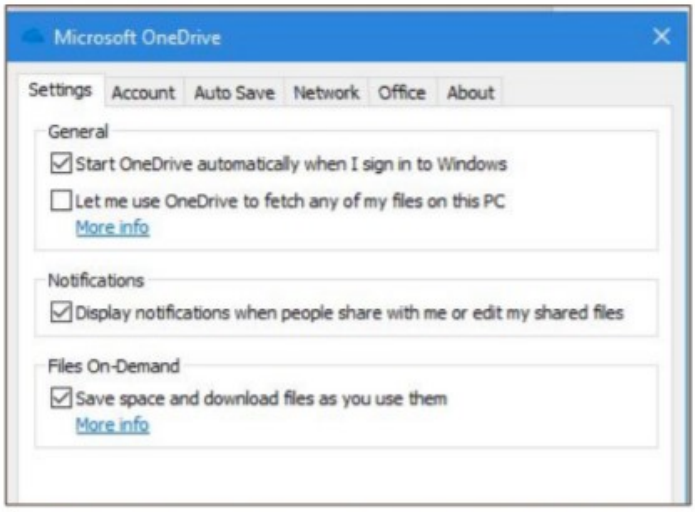
The 2017 Creators update (1709) to Windows 10 included several changes. One of my favorites is "Files on Demand," a new process to make files stored on OneDrive, the Microsoft cloud, available on your PC and other devices.

Anyone with a Windows 10 computer and a Microsoft account automatically has 5GB of free storage on OneDrive. If more space is needed, $1.99 a month will provide 50GB of storage. Office 365 subscribers have 1TB (1000 GBs) of OneDrive storage. If you have files stored on OneDrive, you might want to consider Files-on-Demand to manage them.

To set up Files-on-Demand, you must enable it in OneDrive. First, locate the OneDrive icon on your computer. It may be listed in the File Explorer left column, or it may be an icon in the notification area of the taskbar. If it isn't visible in that area, click the upside-down V and look for it in the group of hidden

icons that opens. The OneDrive icon resembles two white or blue clouds overlapping. If you still can't find it, try using the Cortana search box or get it from the Microsoft store or Apple store.

OneDrive icon



Files-on-Demand option on the settings tab in OneDrive

Right-click the OneDrive icon and click the Settings tab. Under Files-on-Demand, click next to "Save space and download files as you use them." and click OK. The feature in now enabled. If you want to use Files-on-Demand in OneDrive on other devices besides your computer, you need to enable it on each device.

The goal of Files-on-Demand is to save space on your computer or device by storing files on the Internet but making them easily available and up to date on your computer and other devices.

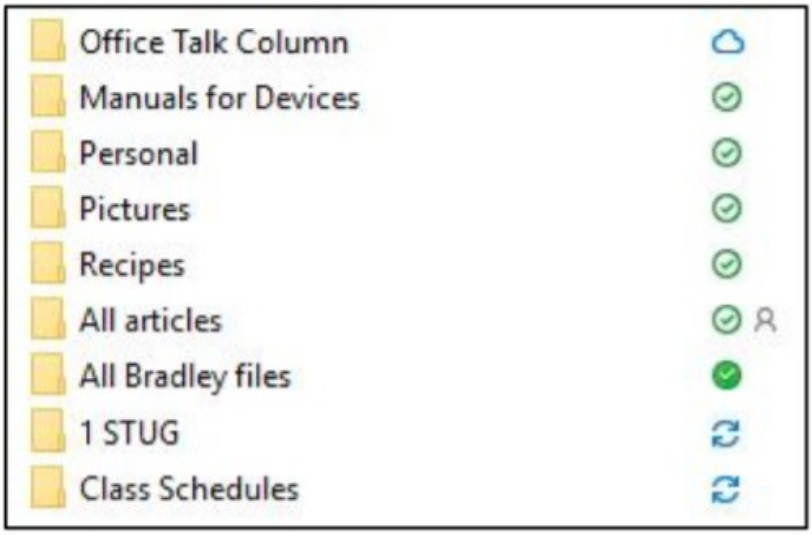
- If you double-click a file in OneDrive, it downloads to your computer or device while remaining stored on OneDrive.
- If you right-click one or more OneDrive files and select "Always keep on this device," files will be available on both your device and OneDrive but will use hard drive space.
- If you want to save space on your computer, right click a file or folder in OneDrive and click "Free up space." This makes new files created on other devices sync to your computer. If you do not click this command, these new files will appear as online-only.

To help you remember what the status is of files and folders saved in OneDrive, a new status column has been added that contains an icon next to each file. The screen shot below shows how they look and what the icons mean.

The folder next to the white cloud with a blue outline is stored only on OneDrive. The folders with a checkmark in a white circle outlined in green will download to the computer when opened. The small people icon means that folder is shared.

The folder with the solid green circle and checkmark has been marked "Always keep on this device." It will use hard drive space.

Although stored in OneDrive, the two folders with blue circular arrows are synced between OneDrive and one or more computers and devices.



Folders stored in OneDrive with status icons

Tips:

- If you delete a file from OneDrive using File Explorer, it will also be deleted from your device.
- If you want to disable Files-on-Demand, go to One Drive Settings tab and remove the checkmark next to “Save space and download files as you use them.” When the feature is turned off, all your files which are synced to OneDrive will download to your computer and will no longer sync.
- For more information about Files-on-Demand, here is a useful website. Copy and paste it into the address bar on your browser: http://bit.ly/2p8KJAc

It takes a little practice to get used to this new system, but its options make it an improvement over the old one.

TECH TALK

Should you leave your computer on 24 HOURS A DAY?

By Joe Isaac, Member, Central Kentucky Computer Society
March 2018 issue, CKCS newsletter -- www.ckcs.org -- newsletter (at) ckcs.org

NO! I shut my computer down every night. If I'm going to be gone several days I not only shut it down, I unplug the computer from the wall and unplug the phone line from the wall.

You are wearing your fan motor out and pulling dust thru your computer. Your hard drive may be running more. If you get a big surge of electricity that jumps your surge protector, it may save your computer by having it turned off.

Your surge protector is passive and works whether it is turned off or on. When it is off, the surge must jump the switch and the surge protector to get to your computer.

The only good thing about leaving your computer on is that you can get rid of the dust bunnies, the fan will pull them into your computer and your utility company will love you.

With the increased use of always on – DSL and Cable Internet and with the growing threat of hackers and worms, it makes even more sense to shut your computer down when not in use.

A computer not running and not connected cannot be hacked.

OTHER GREAT REASON TO CUT YOUR COMPUTER OFF AT NIGHT.

- It's not unusual to get low on system resources after you use Windows for a long stretch, especially if you open and close programs frequently. Adding a bunch of RAM doesn't help. System resources are stored in fixed memory blocks that reside in your System RAM.

- Programs store certain routines inside your system resources. Some programs don't reallocate or release the memory, so after a while your machine gets full. You must restart Windows to free up memory again.

That's why Windows feels more reliable if you start it up fresh every day.

TeamViewer

By Joel Ewing, President, Bella Vista Computer Club, AR
February 2018 issue, Bits & Bytes -- http://bvcompclub.org -- president (at) bvcompclub.org

One way to get help with a computer problem or with a problem using a particular application on your computer is to physically take the computer to an expert or get an expert to make a house call.

If the computer is sufficiently functional and is connected to the Internet, another alternative may be to allow an expert to remotely connect with your computer to diagnose and fix the problem by controlling your computer remotely. One utility that may be used for this purpose is TeamViewer, free for personal use and available from https://www.teamviewer.us/solutions/remote-access/

Some of the BVCC personnel who provide help at our Help Clinics are also willing to provide help remotely via TeamViewer.

TeamViewer allows one computer to remotely view and control a remote computer using a secure encrypted connection over the Internet or over a local network: it's as if the remote operator were sitting in front of your computer viewing your display and with access to your keyboard and mouse. You run an appropriate version of TeamViewer on both the controlling system and the target system. There are versions that run on many different platforms and environment types: Windows PC, Linux PC, Mac, and Mobile Devices are all supported. The Windows version is compatible with Windows versions XP (SP3 level), Vista, 7, 8, 8.1, and 10. The Windows XP and Vista support does additionally require IE8 or later to be installed. The Linux version in some cases may support outbound connections (to control a remote system) but not inbound connections (to be controlled).

There are several ways in which TeamViewer may be used. The way we are recommending requires users at both machines to start TeamViewer when a specific remote diagnostic session is to be established with a known party. When started, TeamViewer will display a 9-digit numeric ID unique to that machine and a numeric password that should be different each time TeamViewer is started. The user at the machine that is to be remotely controlled communicates by phone his ID and password to the other user to give access to his machine. When the remote user enters the ID and password, a session with the remote computer is established. The connection creation requires use of an Internet server operated by TeamViewer, which uses the ID to link to the target machine, and then the target machine verifies the password. If possible, a direct encrypted connection between the controlling and controlled systems will be established; otherwise, the TeamViewer server will serve as a relay point, passing encrypted data between the two machines.

Another way in which TeamViewer may be used is to configure it for unattended operation: have TeamViewer start up with Windows and run with a known password so it may be accessed without a person present. The intent is that you would be able to access your own computer from a remote mobile device, but it also means that anyone else who might discover your ID and password could connect to your system and compromise it without you being aware. We are not recommending that type of usage, because it is possible to choose options that may unnecessarily put your system at risk for abuse over the Internet.

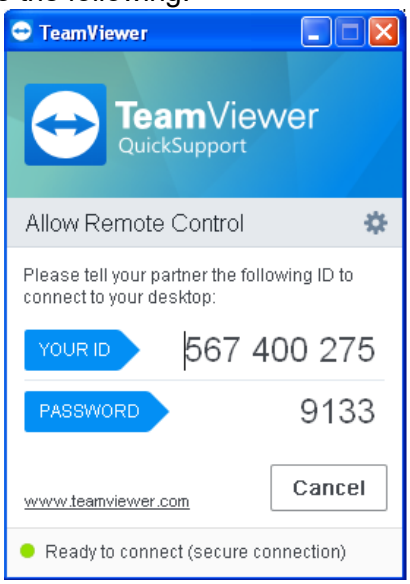
If you are sitting in front of your computer, you can see when someone has access via TeamViewer and act to terminate the connection if you did not authorize it. If the connection is by someone you didn't intend or expect to have access and it occurs when the computer is unattended, it would be trivial for that person to install any variety of malware on your system without your knowledge.

Although TeamViewer's security protocol appears technically sound and they are clearly a security-conscious business, their server platform must somehow store the ID codes for millions of TeamViewer users, making that server an attractive target for hackers, and no site is guaranteed 100% secure 100% of the time when humans are involved. Should your ID become known, a 4-digit password will not keep your system secure for long if your system is always up, with TeamViewer always active, and with a short, fixed password. Your own usage of TeamViewer to access your home site from a remote mobile device could also become an exposure. Should that mobile device become infected with malware and compromised,

your TeamViewer ID and password could also be compromised, making it easy then to compromise your home system as well.

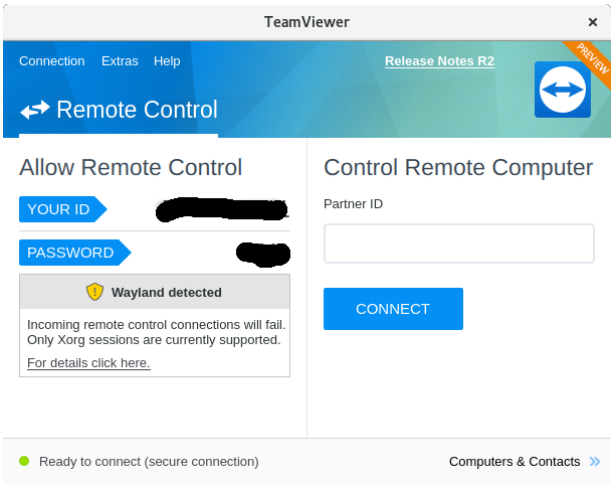
So how do you install free TeamViewer for personal use? Go to the TeamViewer site given earlier, select "Download Now", indicate when asked that your intent is "To access my personal computer at home" (personal, rather than business use). You should be taken to the download page appropriate for your Operating system type. In the case of Windows, you can choose the "Download TeamViewer" button to download a full version of the program that can be installed on your system, or you can choose the "Download QuickSupport" button to download a smaller version that can be executed without installing to allow your system to be remotely controlled for diagnostic assistance only. Alternatively, you can use versions supplied by BVCC Help Clinic personnel.

The simplest and most secure way to execute TeamViewer for a remote diagnostic session is to just download and execute the TeamViewer Quick Support version, which does not support the always-up options that could be mis-configured to make your system more vulnerable. If you execute the TeamViewer QuickSupport version, when it starts you will see a screen like the following:



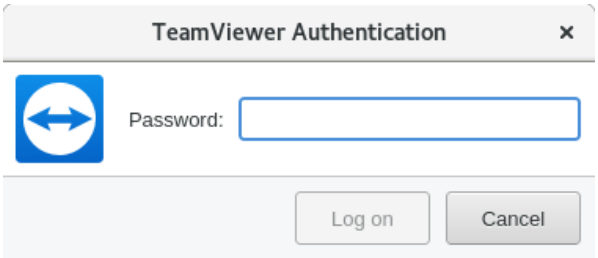
(This is from a virtual Windows system that will be destroyed after writing this article, so it doesn't matter that ID & Password are revealed.)

On a second system that will be used to control the first and where the TeamViewer application is installed, executing TeamViewer displays:

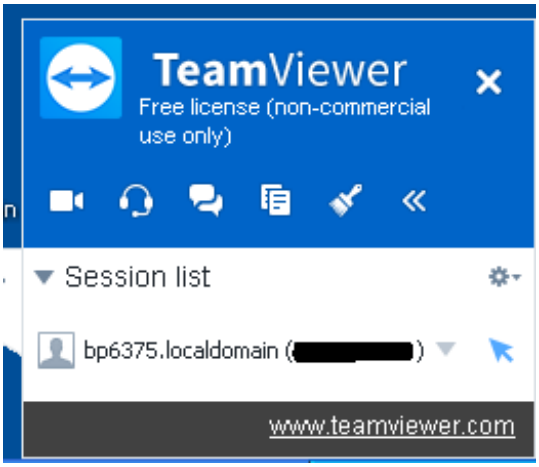


If on that machine you key into the Remote Computer "PartnerID" field the ID of the first machine, you will next be asked for the password.

and if the password of the first machine is correctly entered, the second machine will now display the desktop of the first machine and will be able to control that machine. The first machine will show that it is being remotely controlled by displaying a desktop window on the bottom right including the name and ID of the controlling machine.



(I blacked out the 9-digit ID). Closing that window on the controlled machine is one way to break the controlling connection. While a connection is in effect, it is possible for the users at the controlling and controlled computers to text via a Chat feature in TeamViewer and mark on the controlled desktop as a means of communication, but in most cases, it would be more efficient to communicate by phone on a speaker phone.



There also appears to be support for handling video conferencing between the computers, but this presumes both systems have a functional microphone and camera, which mine do not.

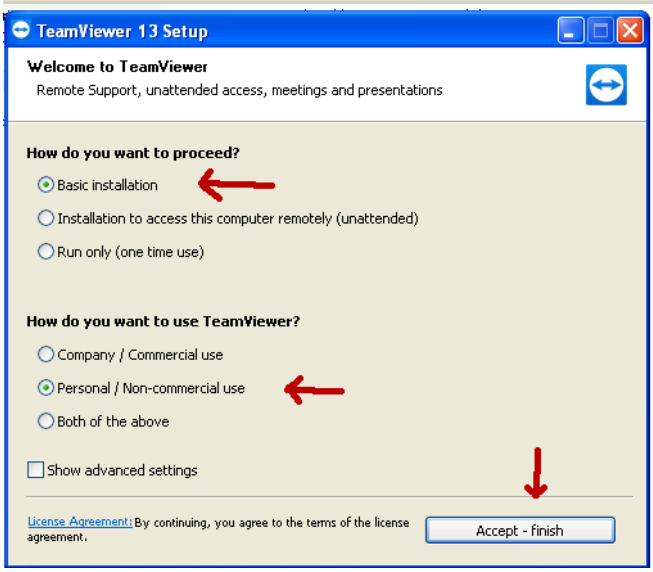
When the TeamViewer session is terminated, you will get a window reminding that you are using a free version for personal use only. If you are not using it to support a business, the correct response is “OK”.

After closing that window, you will get one more advertisement for purchasing a business license, which should be ignored for personal usage.

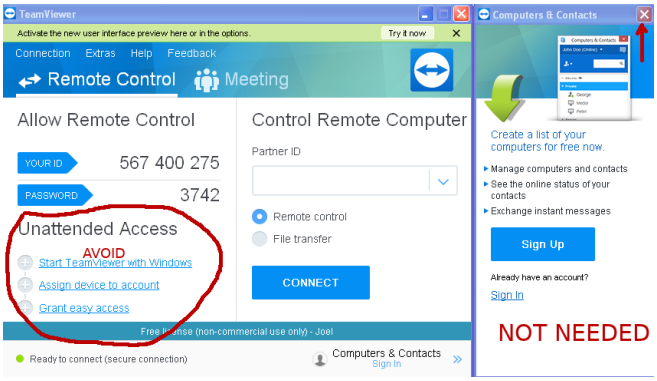
Another useful feature, which is available if both operating systems are some variety of Windows, is to initiate a File Transfer session rather than a Desktop Control session, so files can be moved between the two computers. When running in this mode, the controlling system displays a window similar to those of FTP client applications, where the left half is local machine files, the right half is remote machine files, and you can search directories and drag-drop files from one machine into the directory structure of the other. Unfortunately, if you are primarily a Linux user, this feature isn’t functional with release 13 when one of the machines is running Linux instead of Windows (at least in the case where the Linux system doesn’t support in-bound TeamViewer connections). There are other TeamViewer features related to meetings and conferencing that I didn’t explore, because they weren’t relevant to its remote diagnostic capabilities.

If you choose in install the full TeamViewer version rather than just run the QuickSupport version., there are install options you need to avoid.

Specify “Basic” (not unattended access) and that installation is for “Personal” use, and “Accept”.
The first time the program is opened, at least on the Windows install pictured here.



You will also have a Computers & Contacts window as shown. If you only plan to use TeamViewer to allow a technician to remotely control your system for problem diagnosis, then you don't need an account with TeamViewer and the Computers & Contacts window can be ignored and closed.



The main window also enables you to turn on various features that support unattended access. Unless you have a really good reason why you need this capability, don't activate it, because it increases the risk that your computer might be exposed to malicious damage over the Internet should your ID and password become compromised.

If you must have TeamViewer configured for unattended connections, there are recommended option combinations that should be researched and observed. Option settings may be found under Extras → Options. It's probable that installing with "Installation… (unattended)" rather than "Basic Installation" will set a combination of options that are within recommended guidelines for unattended access, provided adequate passwords are used, but I have not attempted to verify this.

Back to Basics

E-mail Basic Review

By Jim Cerny, Forum Leader, Sarasota Technology User Group, Florida
December 2017 issue, Sarasota Monitor -- www.thestug.org -- jimcerny123 (at) yahoo.com

I am going to assume you already have an email address and are enjoying sending and receiving emails. But perhaps you are not aware of the fun and helpful options available in all email applications. Hopefully something in this article will push your curiosity button and encourage you to "ask google" for more information. Although each email provider (app or program) may look different on your device (and even the SAME provider can look quite different on a Windows computer than on an iPad, etc.) all are capable of doing the following:

Entering people in your "TO:" box – If you just start typing the name of someone, your email will search your "contact list" or "address book" to find a match and list what it finds. Just click on the name you want. Be sure to keep your contact list of email addresses current. It is easy to click on a name which may have an OLD email address. If no name matches, you have to enter the email address yourself. Why not add that person to your contact list for next time?

Learn to use "group" email addresses. You can use your contact list to create a "group" email such as for a club or family group. This means you only have to enter the group name, and ALL the email addresses in that group will be placed in the "TO:" box for you. This is a great time saver. Of course, you need to keep the group current. It is easy to learn how to "add" or "delete" people from a group.

Clean out your "inbox" by deleting old emails or keeping only the emails you want by moving them to a folder. Your "inbox", "deleted emails", "drafts", etc., are all folders or places – you can add your own folders to this list and move the emails you want to keep to them. I have a folder for STUG emails and for another club I belong to. This keeps the emails in my inbox to a minimum.

Learn to SEARCH for emails in any or all folders. You can search and find words in the subject line or in the emails themselves. You can search for all emails to or from a specific address too. This is helpful if you forget where you put an email.

Emails you delete will go to the “deleted emails” folder and they need to be deleted again from that folder to be deleted forever. Check to see if your email has an automatic delete setting for this folder. I have my email set to delete emails older than 90 days from my “deleted emails” folder. Do NOT keep thousands of emails! (Yes, there are people who like to keep everything, they call them “hoarders” and they have their own television show!).

Sharing photos using email is easy. You just “attach” the photo (or ANY file) to your email before you send it. Yes, you can attach more than one, but don’t go crazy and attach too many, usually three or four is plenty. Photos take a lot more time to send than text.

Learn to access your email on another device. This is very helpful when you are traveling or need to use another computer to get to your email. You should always be able to access your email by going to your email internet webpage and entering your email account and password there. I highly recommend that you try this to be sure you can do it when you need to.

All emails provide many tools and options to help you. Most of them are easy to use, too. Please “ask Google” or use YouTube and watch a short video about your email and the possibilities it provides. There is always more to learn, and I hope this information will be helpful for you to find and use the tools you need for better emailing!

Interesting Internet Finds – January

By Steve Costello, Boca Raton Computer Society -- http://ctublog.sefcug.com / editor (at) brcs.org

Can You Use Any Charger With Any Device?
https://www.howtogeek.com/175734/htg-explains-can-you-use-any-charger-with-any-device/
With so many devices needing to be recharged this is a post that is a must read.

Charging Your Phone Overnight: Battery Myths Debunked
https://www.pcmag.com/news/357987/charging-your-phone-overnight-battery-myths-debunked
Do you? Should you? Check out this PC Magazine post for some answers.

Should You Get A Cat6 Or Cat7 Ethernet Cable For Your Network?
https://www.ghacks.net/2018/01/30/should-you-get-a-cat6-or-cat7-ethernet-cable-for-your-network/
Need some new cables for your wired network? If so this post has some advice for you.

My Five Favorite Services For Streaming Free Music Online
https://www.thesimpledollar.com/five-best-streaming-sites-for-free-music-online/
When I am working on my blogs, or the user group newsletter, I like stream music while online or through my smartphone. If you like to do that too, check out this post for some ideas on what to use.

How To Prioritize Wi-Fi Networks On Your Android Phone
https://www.guidingtech.com/prioritize-wifi-networks-android/
This post explains how to use the WiFi Prioritizer app to prioritize your w-fi networks. (I have been using this app for some time now and it works.)

How To Stop A USB Mouse From Constantly Disconnecting And Reconnecting
https://www.simplehelp.net/2018/01/04/how-to-stop-a-usb-mouse-from-constantly-disconnecting-and-reconnecting/
This was a timely post for me. The day before this post my USB mouse started disconnecting and reconnecting. I did what is suggested here, and the problem has gone away. I really didn't want to go trying to update drivers.

****

Most Fridays, more interesting finds will be posted on the Computers, Technology, and User Groups Blog:

http://ctublog.sefcug.com/tag/interesting-internet-finds/

The posts are under Creative Commons licensing.

NOTES FROM THE EDITOR

New Column on the APCUG website - Judy Taylour

For all you Linux lovers and those who want to learn about it, “Free John” Kennedy, Advisor for Regions 3 and 6/7, suggested we have a Linux column along with the *Tech Tips* and *Apple Tech Tips* by Jere Minich.

Credit Jim Evans, Tech Tips & Apple Tech Tips graphics; John Kennedy, Linux avatar

The *Penguin Platform* went live today – check it out as well as the other tip columns. When I visit member group websites I see that several link to one or more of the Tips columns, include some of the tips on their site or in their group’s newsletter.

It was a group effort putting the column together; among others, John worked with Orv Beach, the training chair for SCALE in Los Angeles. He also gives Linux presentations at our VTCs.

Gust Kookootsedes

Gust J. Kookootsedes, 88, passed away on the evening of June 1, 2018 at his home in The Woodlands, Texas.

He is survived by Mary, his wife of 66 years and their children, Penny (Tod) Bradley, Jean (TJ) Hare, and Christine (Jeff) Wolverton; 11 grandchildren, their spouses; seven great-grandchildren; siblings, George (Marina) Kookootsedes, Mary Jannides; and sister-in-law, Nancy Christy. He was preceded in death by his parents, John and Penelope Kookootsedes; his brother, Chris Christy; and brother -in-law, Spiros Jannides.

Born in Brooklyn, N.Y., July 12, 1929, Gust moved to Sidney, Ohio in 1932 where he spent his childhood. When he wasn't in school, playing tennis and/or football, he worked at The Purity confectionery owned by his father, where his passion for candy making began. He attended Ohio Wesleyan and earned his degree in chemistry. After graduating in 1951, he was hired as a research chemist for Dow Corning Corp in Midland where he worked for 40 years. While employed there, he was awarded several patents - one discovery was even named after him (KP Fluid).

He and Mary were wed on Oct. 7, 1951 and moved to Midland to start their life together. In 1954, they left for Baltimore, Md. while Gust served in the U.S. Army for two years. They returned to Midland and lived there until the fall of 2016 when they moved to Texas to be close to their daughter, Penny.

Gust always put God and his family first. He was proud of his Greek heritage and was much happier being the giver than the receiver in all of his relationships. He had many interests and hobbies including tennis, music, gardening, candy making and photography. He was an incredible man and will be missed by not only his family but many friends as well.

Please join us for his viewing on Monday, June 18, 2018 from 5-7 p.m. at Case Funeral Home in Saginaw, and/or funeral services on June 19 at 11 a.m. at St. Demetrios Greek Orthodox Church. In lieu of flowers, the family requests memorial contributions be sent to St. Demetrios Greek Orthodox Church, 4970 Mackinaw Road, Saginaw, MI 48603.

Funeral Home
W. L. Case and Company Funeral Home
4480 Mackinaw Rd. Saginaw, MI 48603
(989)793-9700

Published in Midland Daily News on June 13, 2018

ALTERNATE ROUTES TO MIDLAND PUBLIC SCHOOLS ADMINISTRATION BUILDING