SUPERCOM COMPUTER CLUB TECH TIMES

Volume 12   June 8, 2017

Objective:

To bring the latest technology news to you, our members. Tips and suggestions will help you to keep your device(s) running smoothly and help you be aware of threats. Technical tips will be coming to you through our Technical Committee.

Committee Members: (Pictured Below)

Ben Tarbell, Mike Gerkin, Jim Oliver, Peggy Bullock, Jim Mills, Rick Heesen, Lowell Lee, Steve Andreasen (Apple/Mac), Dick Strong and Art Rice.
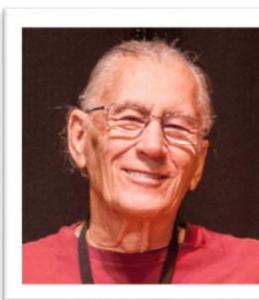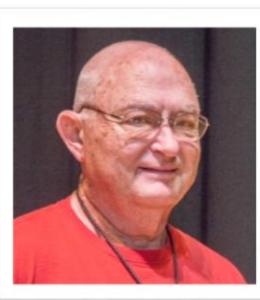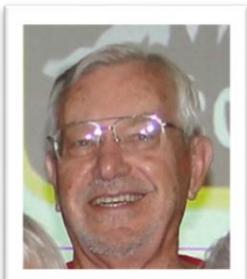
Dick Strong is on "time off" for season 2016-2017.
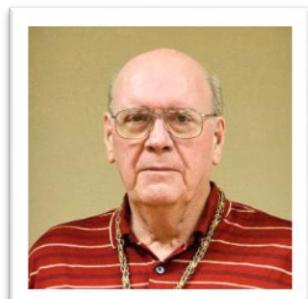
Greetings

From the emails I have received, many of you are enjoying your summer activities, families and some computer activities. Our membership should be very glad our Tech Committee doesn't really take the summers off. We are always being diligent in keeping up on recent threats, virus and ransomware. We hope you all are being as diligent in doing the following:

<div align="center" style="color:red">

WINDOWS UPDATES
And
Your maintenance schedule!!

</div>

****

Did you make the following a favorite in your bookmarks yet? If not, you should!

http://www.supercomcc.org

****

Submitted by Ben Tarbell:

What Happened to Solitaire and Minesweeper in Windows 8 and 10?

The classic desktop versions of Solitaire and Minesweeper are gone in Windows 8 and 10. Instead, you'll find shiny new versions with advertisements, Xbox integration, and optional subscription fees. But you can still play Solitaire and Minesweeper without ads, and without paying a cent.

How to Launch Solitaire on Windows 10

Solitaire is installed by default on Windows 10. You can just open the Start menu and launch the "Microsoft Solitaire Collection" application to open it.

If the Microsoft Solitaire Collection isn't installed—perhaps you've uninstalled it in the past—you can get it from the Windows Store.

Please go the actual article to read the rest and see the specifics of how to do it.

https://www.howtogeek.com/122145/what-happened-to-solitaire-and-minesweeper-in-windows-8/

****

This is an excellent article that summarizes how you can check to see that you are protected from these really nasty recent Ransomware Attacks.

Ransomware was once again in the news. This time it was due to WannaCry, an attack that stretched across 150 countries and nearly 57,000 countries. The attackers used a Windows vulnerability only recently patched (March 2017), formerly used by the National Security Agency to secretly take control of computers.

Determine If You Are Protected

First off, check and make sure you are protected.

If you are running Windows 10, >>>>>>

Please click on article to read the rest of the write-up for yourself.
http://windowssecrets.com/windows-secrets/what-you-need-to-know-to-protect-yourself-from-ransomware/

Credit to: **Susan Bradley** is a Small Business Server and Security MVP, a title awarded by Microsoft to independent experts

****

Submitted by Ben Tarbell:

How to Check for Windows Updates

Annoying as they might be, it's important to keep Windows updated...just ask the victims of the latest ransomware attack. If you haven't used your PC for a while or you just want to make sure you're updated with the latest software, it's easy to manually check and make sure in Windows.

Press the Windows button or Search button, and type "check for updates" in the box. Then, hit Enter or click on the first result. This will take you to the dedicated Windows Update page in the Windows 10 Settings application (or, if you're using Windows 7, the Control Panel).
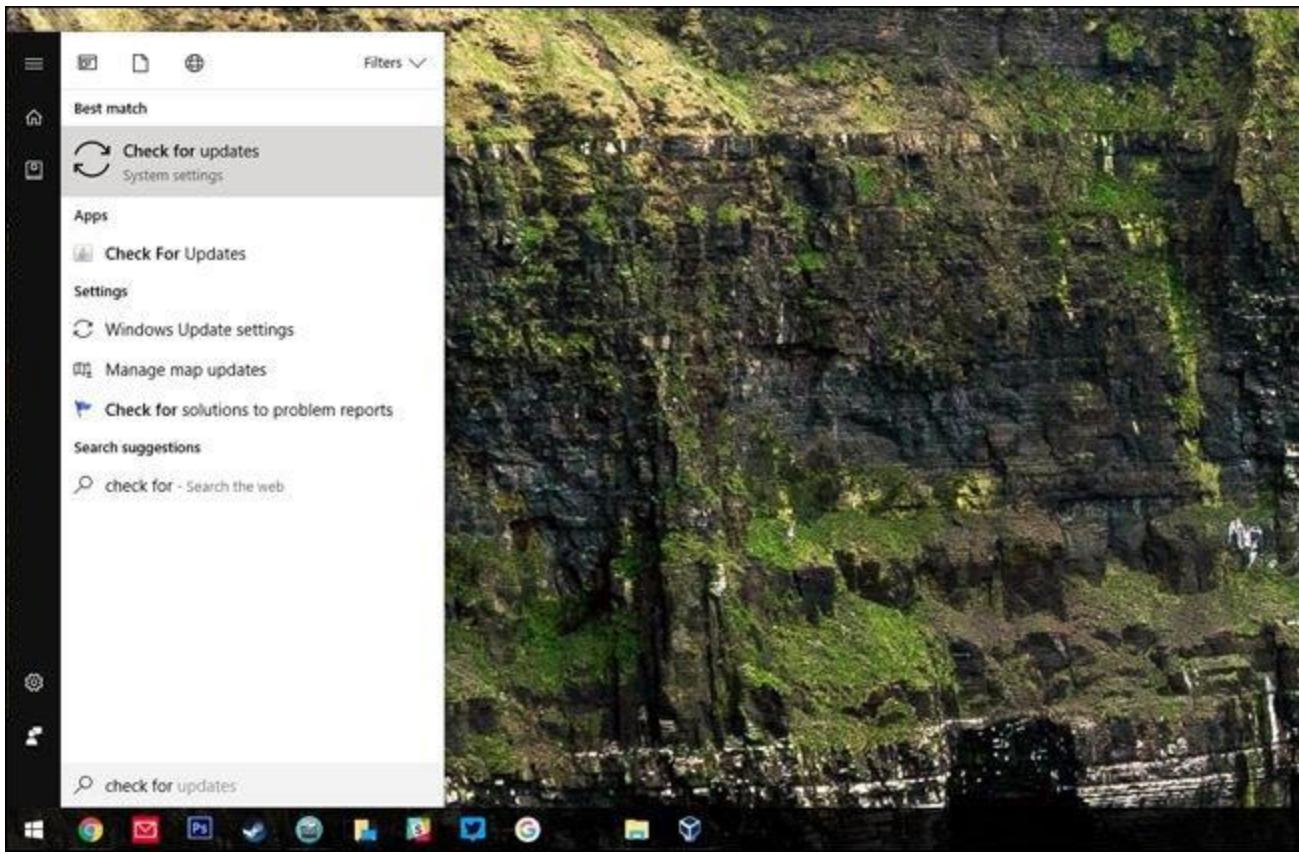
The display will show you the last time Windows connected to a Microsoft server to check for the latest updates. Click the "Check for updates" button. After a few seconds you'll know if you're running the very latest version of Windows or not.
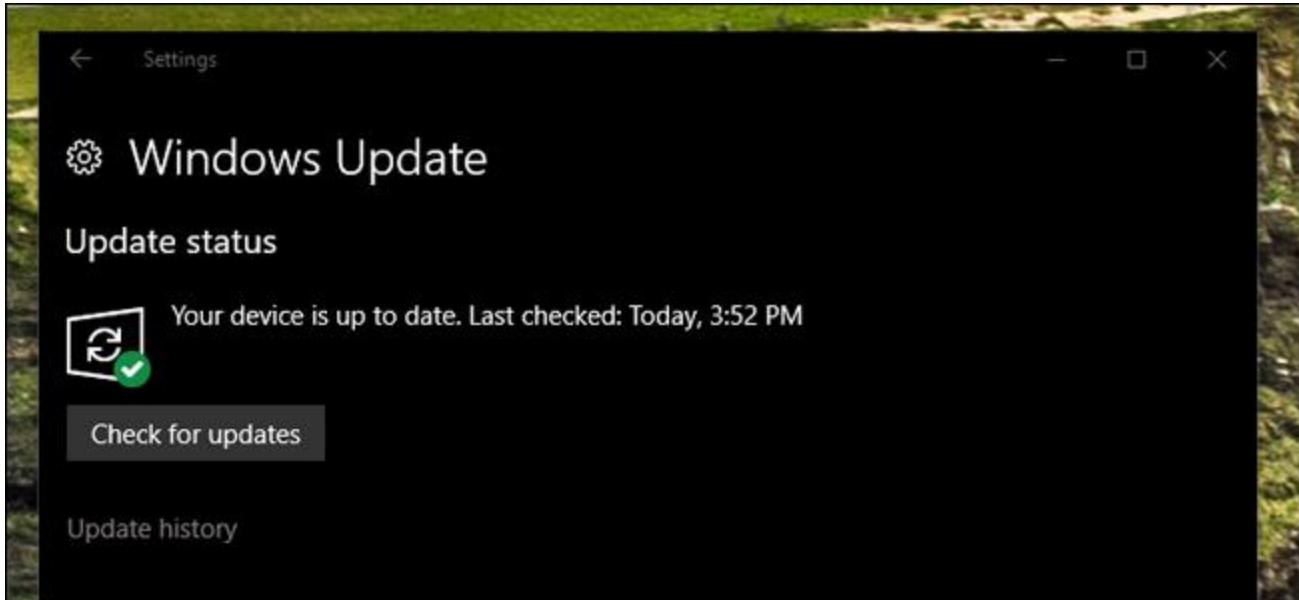
Windows 7 users will see a slightly different window, but with the same options. Just click "Check for Updates" to see if updates are available.
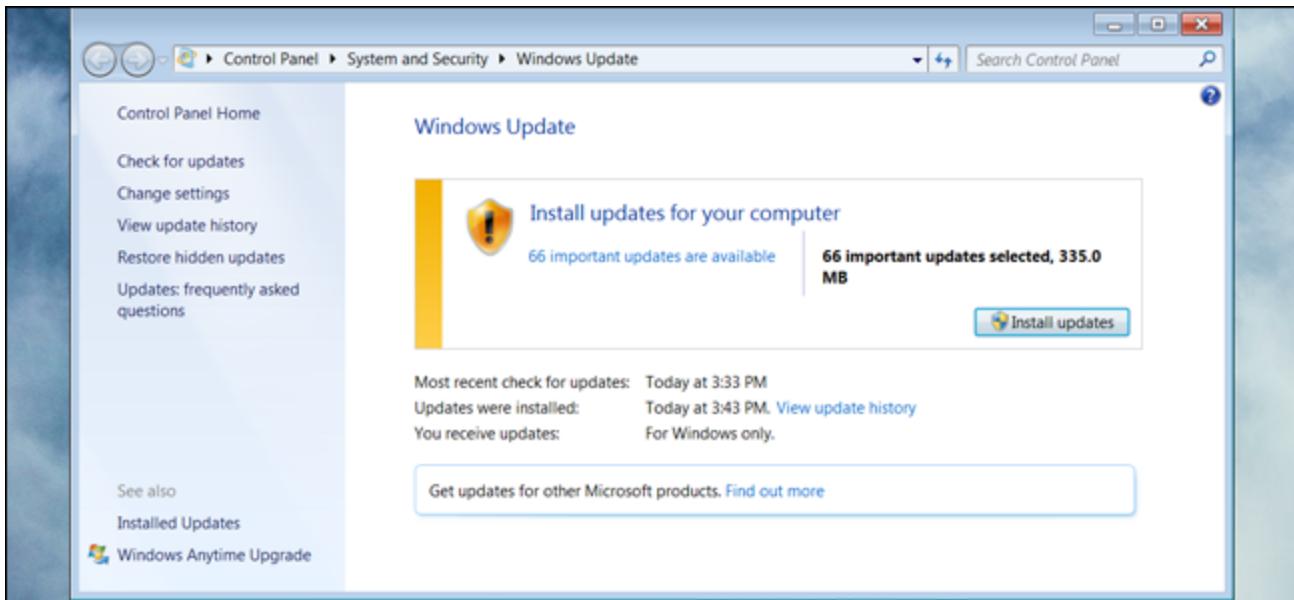
If you're up to date, congrats. If not, just click "Install updates" follow the on-screen instructions to download and install what you need. You may be prompted to restart your computer once the update process starts, so save any open work.

Normally, you shouldn't have to manually check for updates. By default, all versions of Windows will download and install updates automatically. If you've turned this feature off, you should really turn it back on (Under "Change settings" in Windows 7 and "Choose how updates are installed" in Windows 8). These automatic updates keep your computer safe, and as annoying as they can be, they're very important.

Windows 10 doesn't allow users to disable updates completely, but if you're concerned with being forced to restart and lose saved work, there's a way to schedule your "Active Hours" and make sure that happens when you won't be inconvenienced.

Credit to: By Michael Crider on May 25th, 2017

<div align="center">*****************************</div>

<u>Submitted by Rick Heesen</u>:

How many times have you, as a member of the computer club, heard the Tech People, or even other members, talk about something and you have no idea what they are talking about??? Well, I (Peggy) for one, as a member and a Tech member, really enjoy the articles the other members turn up! I always learn something. Have you ever heard the phrase Zero-Day Attack ? Click on the link and you will be informed about vulnerabilities and how they are found and fixed.

Credit: Ask Leo

<div align="center">*****************************</div>

Submitted by Rick Heesen:

Information about Windows 10 S:

Windows 10 S is Microsofts newest version of Windows 10 aimed squarely at the education market and, although designed specifically for student use, it will also be available to the general public.
Windows 10 S is Microsofts answer to Chrome OS, the operating system used in Chromebooks and, like Chrome OS, primarily supports web based programs, programs that live on and are accessed through the web and not downloaded onto your PC. However, unlike Chrome OS, which supports apps found in Googles Play Store as well as most Android apps, Windows 10 S has been restricted by Microsoft to support only apps found in the Windows Store. That doesn't mean that desktop apps won't run on this version of Windows 10, but it does mean they'll need to be specially packaged by their developer and listed in the Windows Store to be useable. For example, although Microsoft states Windows 10 S will run on any browser in the Windows Store, the only browser currently in the store is Edge. Microsoft has invited both Google and Mozilla to repackage their browsers for the Store but will only accept browsers designed around the Edge browser engine. This would require Google and Mozilla to essentially redesign their browsers from the ground up. There is a precedent for this however, as this is exactly what Google has done to make Chrome available in Apples App Store. But even if Google and Mozilla do redesign their browsers in compliance with Microsoft, since there is currently no mechanism in 10 S to change the default browser, Edge will remain your only option for default browser. Also, although Microsoft states you can use any search engine accessible from your browser, there is no option to change the default search engine from Bing to whatever your favorite might be. And just because an app can be found in the Windows Store doesn't mean it will run in 10 S. There are some apps in the Store that are not compatible with the new OS, including all command line apps, as well as shells and consoles.

For those who wish to have more control over what apps they download, Microsoft has included the option to upgrade from Windows 10 S to Windows 10 Pro for $50. However, this is a one way upgrade and once you switch to Windows 10 Pro you'll be unable to revert back to Windows 10 S.

Pros and cons of Windows 10 S

Pros:
-All apps are pre-screened by Microsoft prior to being made available in the Windows Store and are run in a secure container. This means they can't make changes to your registry or leave behind files on your PC such as viruses or malware.

-Windows 10 S PC's come with none of the usual manufacturer installed bloat ware so often found on non-S PC's and therefore boot faster than their non-S counterparts. And since nothing is installed on your PC, boot times and sign-in times shouldn't change over time.

-New PC set-up is faster and simpler.

-Since Windows 10 S is built around Windows 10 Pro it supports many of the advanced features found in Windows 10 Pro, such as mobile device management, Bitlocker encryption, Azure active directory domain join, and Windows Update for Business, which allows administrators to fine-tune when they want feature updates to roll out, and defer normal updates for up to 30 days.

-Microsoft projects extended battery life with charges lasting significantly longer than comparable Windows10 Pro PC's.

-If you find you don't like Windows 10 S you have the ability to upgrade to Windows 10 Pro for the current up-charge of $50.

-Since Windows 10 S is a streamlined and less resource demanding OS it can be offered on lower-end budget PC's thereby saving you money at time of purchase. This could potentially be a negative if you later decide to upgrade to Windows 10 Pro.

Cons:

-Windows 10 S can only run apps pre-approved by Microsoft and found in the Windows Store. Although the Store is sparse on app offerings as of now, the hope is that as Windows 10 S gains in popularity software designers will choose to repackage their apps to qualify for the Store. Only time will tell.

-Currently the only browser available in the new OS is Edge. As stated above, this may change in the future.

-There is currently no provision to change the default browser in Windows 10 S so even if other browsers become available in the Store, your default browser will remain Edge.

-Although you can access any search engine through Edge, you can't change the default search engine from Bing to anything else.

-There is no ability to launch command line environments.

-Since the only drivers available to Windows 10 S PC's are those already in the Windows 10 driver database, there may be hardware connectivity problems leading to decreased functionality or complete inability to connect, especially with older hardware.

So what does this all mean for you? If your PC use is restricted primarily to checking email, browsing the web and working with Microsoft Office apps, and you don't have a burning desire to play the latest and greatest game app, then Windows 10 S may be a good fit, provided that Microsoft does indeed make their Office Suite available in their Store, which is currently their plan. If however the above use pattern fits for you but you DO want the latest and greatest game app available, than you might want to consider a Chromebook powered by Chrome OS, since many of these PC's are capable of running Android apps as well as Google Play Store apps. If, on the other hand, you have a need or desire to run traditional desktop apps then a Windows 10 Home or Windows 10 Pro is what you're looking for.

All in all, there are some very attractive aspects to Windows 10 S but there are some obvious drawbacks as well. Hopefully this helps sort out some of the issues. Happy shopping.

Sources:
"What is Windows 10 S, and how is it different", How-To-Geek, May 30, 2017, by Chris Hoffman, https://www.howtogeek.com/305363/what-is-windows-s-and-how-is-it-different/

****

A note from Mike Gerkin & Peggy Bullock:

Type in your search bar "winver" and you should be able to see the latest version of Windows 10. It is 1703 and the OS Build is 15063.332. Make sure you keep your Windows Updates current!

****

Submitted by Mike Gerkin:

By now, you've heard all about those ransomware attacks that crippled Britain's hospitals and businesses and organizations in 150 countries.

The worst part is that this round of attacks was entirely preventable if good, basic security rules had been followed. And I'm not even talking about teaching employees not to click on suspicious links or unexpected attachments.

If the people in charge of keeping these systems safe had been serious about security, this never would have happened.

The flaw that allowed these attacks to go down was identified months ago by Microsoft and a patch was issued back in March to protect systems against this exploit.

The problem is that many places are still running the old unprotected XP operating system or just not bothering to do security updates for their newer systems.

I know some of you love XP. But Microsoft ended security and bug updates THREE years ago. And even if you're running Norton or any other third-party security system, they can't properly patch or protect XP. XP systems are especially vulnerable because when patches are issued, hackers analyze the security patch to figure out what it's patching and then write up a bit of malware to take advantage of that flaw in unprotected systems. That means Windows XP (and now Vista) AND Windows systems that haven't had recent security updates are at risk. Your PC is a sitting duck. Don't fall victim.

Big entities with money to pay for ransom are the preferred targets — for now. Keep in mind that the ransomware landscape is changing. You don't need to have any real tech knowledge these days to be a cybercriminal. Crooks can purchase ransomware packages all ready to go. There are even services to collect their payments for them. Expect home users to be targeted more and more as more criminals enter the ransomware game and need more victims.

Here's what you (and companies and other organizations) must do to protect themselves.

1. Use an up-to-date operating system. If you're using Windows XP, Vista, or a version of Mac OS that is no longer supported – stay offline with that computer. Also be careful about loading files onto that PC.

2. Run those security updates ASAP. This refers to both Windows and Mac updates and to any updates from third-party security software. If your device isn't already set for automatic updates, set it now.

3. Be cautious about any links or attachments you receive.

As a consumer, be proactive. If you are providing personal and valuable information to others such as your doctor, lawyer, financial advisor, bank etc… find out what operating system is being used and if

security is updated regularly. If they can't answer, ask them to find out who can insure your information at their site is secure.

Check in with your church, club, or any other organization you belong to and make sure they are safeguarding your information.

Check with your friends and relatives to make sure they are up-to-date. Remember, someone who gets into their information, might be able to find out quite a bit about you.

****

If any of our members have questions or comments during the summer, please don't hesitate to shoot us an email. We will pass it on to someone of the Techs who most likely would have the knowledge to answer you. We know just because it is "summer", our computer problems don't take a "summer vacation"! Keep in touch, we would love to hear what you all are doing over the summer too!

Until next time…………..Have a Beautiful Day!

From: Ben Tarbell, Rick Heesen, Mike Gerkin and Peggy Bullock