SUPERCOM COMPUTER CLUB TECH TIMES

Volume 11 May 15, 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)

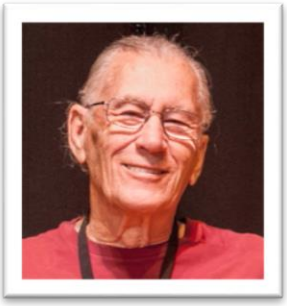
Ben Tarbell, Mike Gerkin, Jim Oliver, Peggy Bullock, Jim Mills, Rick Heesen, Lowell Lee, Steve Andreasen (Apple/Mac), Dick Strong and Art Rice.



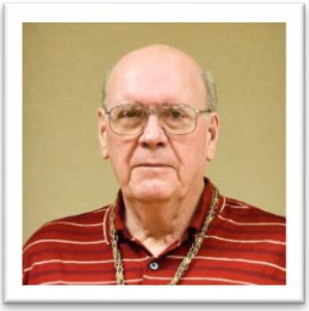








Dick Strong is on “time off” for season 2016-2017.



Greetings

We are back in our summer campground in the 5th wheel! A good flight home, a few minor medical equipment issues, but off and running. I even managed to bring a little AZ sunshine home with me. There has been a lot of rain, but this week is looking fantastic! 80's and an AZ blue sky!!

Your Tech Committee is busy keeping me on my toes! I no more get one Tech Times done and the next day's email has another article.

Just a friendly reminder-----
Make these two things priorities!!!
WINDOWS UPDATES
And
Remember your maintenance schedule!!

****

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

http://www.supercomcc.org

Last month, a couple members emailed me that they couldn't access the newsletter with the link I inserted in the email. I'm sorry about that. I tried something new from my browser and apparently it didn't work for everyone. BUT, the above link will get you to the Website, then click on the Tech Times and Tips. You can access the newsletter there if the link in your email does not work.

****

Submitted by Mike Gerkin:

Many of our SuperCom Club members have updated their devices to the Windows 10 operating system (OS).

Last month Microsoft released the Creators Update for Windows 10 and although not all users have been offered the updated version of the OS on Windows Update, many did manually install it so this month's Patch Tuesday will move their current PC build forward to 15063.296 from 15063.250 or 15063.138.

In the latest updates there is also a security update for Adobe Flash Player for Windows 10 Version 1703 (KB4020821) and the standard monthly release of the updated Windows Malicious Software Removal Tool (KB890830).

If you do not have your Update setting set to Automatic, you may want to go to Settings now and check for available updates. This link 1703 15063.296 Update to Microsoft will explain what is in the latest Windows update.

While it is important to keep windows current, it is just one of the programs that works best when updated regularly. In my case, I make certain that Malwarebytes, SuperAntiSpyware, and Glary5 are always up to date to provide maximum security protection. How about you? Are you regularly updating your programs?

****

Submitted by Rick Heesen:

Are You Locked Out of Facebook?

It's time for a Facebook reality check. Is your Facebook account safe from hackers? If your account gets hacked, have you set it up in such a way that you can regain control? These are both pretty important questions, right? My daughter, who some of you may know, is competing in American Ninja Warrior events and has been using her Facebook account as her data base for storing her videos, photos, followers, event information etc. A few days ago she opened her account only to find she had been hacked and her password had been changed. No problem, right? Just sign in and when it says "I've forgotten my password" access the account with the emergency phone number and/or email listed in the Account section.

Problem, her emergency access phone number was an old number no longer in service and the same was true for her emergency email address. Although some accounts will give you the option of identifying tagged photos in your account, some won't, and hers didn't. Still no problem, just contact Facebook and have them walk you through an identification process to get the account back. Nice thought, but there's no way to talk to an actual person about your Facebook account. So, how can she get her account back?

As it turns out she probably can't, which begs the question, "How can I keep this from happening to me?" Well, the most obvious answer is keep your emergency access phone numbers and email addresses up to date at all times. But there's another option that takes a little pre-planning but works very well, and that's "trusted friends". Facebook allows you to identify three friends, also members of Facebook, as trusted friends. This means that if you get locked out of your Facebook account for any reason, when you get to the dreaded "I've forgotten my password" screen and your phone number and/or email address won't work you can choose to have one of your trusted friends to use as a safety net. Facebook will send him/her an unlock code that he/she can then give to you to unlock your account.

Here's how to set it up:
Log into Facebook. On the top of the Facebook home page where the "Find Friends" search bar lives you will find a downward pointing triangle located at the far right, click on this triangle.
Then choose "Settings" > "Security and Login" and scroll down to "Setting Up Extra Security" and click on the "Edit" button next to "Choose 3 to 5 friends to contact if you get locked out".
Here you will have the option to type in the names of 3-5 trusted friends in case all other emergency account access options fail. These people won't have access to your account but they will be listed on your account as people you trust enough to receive the unlock access code in case of a lock-out. This would also be a good time to update your email and phone number if they have changed.

For Email:
Log into Facebook. On the top of the Facebook home page where the “Find Friends” search bar lives you will find a downward pointing triangle located at the far right, click on this triangle. Then choose “Settings”. In the center of the page will be “General Account Settings”. If the email next to “contact” is incorrect click on the “edit” button and change it.

For Phone Number:
Log into Facebook. On the top of the Facebook home page where the “Find Friends” search bar lives you will find a downward pointing triangle located at the far right, click on this triangle. Then choose “Settings” > “Mobile”. If the phone number under “your phones” is incorrect, click “Remove”, then click “Add Another Mobile Phone Number” and follow the prompts to update your phone number.

Now you have several options for recovering a locked Facebook account. Happy Facebooking.

Thanks Rick! I wish we would have stressed this better in our Facebook SIG!!

****

Submitted by Peggy Bullock:

Have one of these smartphones? Your bank details, passwords and photos could be stolen

By Mark Jones, Komando.com

Your smartphone is a very valuable piece of technology. I'm not talking about the price you pay to upgrade to a new gadget either. No, I'm referring to all of the sensitive data these amazing devices hold.

Imagine if a hacker was able to get into your phone to steal banking information and passwords to all of your accounts. Scary! A vulnerability has been recently discovered that allows cybercriminals to do just that and millions of smartphone users are at risk.

Why millions of Android users are at risk

Researchers at Check Point have discovered a major security flaw that puts almost half of all Android users at risk of having their gadget "hijacked." The bug is in Android's software and it allows hackers to steal banking information, passwords and photos. Nearly 45 percent of Android users worldwide are affected by this vulnerability.

What's happening is, malicious apps found in the Google Play Store are taking advantage of the security flaw. It has to do with Google's permissions policy that allows apps to pop-up on your gadget's screen. The vulnerability is found in Android's operating system, version 6.0.1 and newer.

Detailing the bug, Check Point researchers said, "Based on Google's policy which grants extensive permissions to apps installed directly from Google Play, this flaw exposes Android users to several types of attacks, including ransomware, banking malware and adware. Check Point reported this flaw to Google, which responded that this issue is already being dealt with in the upcoming version of Android, currently dubbed 'Android O.'"

The problem with waiting for Android O is it's not expected to be released until August. That's just too long to have an exposed gadget without taking precautions.

In the meantime, you really need to be careful downloading apps. Make sure you read the app's reviews before downloading it. If the app is malicious, there's a good chance an affected user will mention it in the comment section of the app store.

Continue reading for more suggestions on how to avoid malicious apps.

How to stay protected from malicious apps

- **Reviews** - Most of the popular apps will have reviews by other users in the app store. You can sometimes find reviews by experts online. These are helpful at pointing out malicious or faulty apps. If you find a review warning the app is malicious, do NOT download it.
- **App stores** - Stay away from third-party app stores because they do little vetting of apps, making it easier for scammers to spread malware there. FalseGuide malware slipping past Google's security and making it into the Play Store is somewhat rare. Google Play and Apple's App Store are the most secure way to download apps.
- **Check the apps' developer** - Verifying the name of the app developer is important. Copycat apps will have a different developer's name than the actual one. Before downloading an app, do a Google search to find the original developer.
- **Update your gadget** - Make sure that you have downloaded the latest security and operating system updates. These updates usually include patches to help protect your device from the most recent threats.

If you do think that your Android device has been infected with a virus, don't worry, we've got you covered. Click here to find out how to detect and remove a virus on your Android gadget.

Note: I like the above suggestion of checking to see who the apps' developer is. I'm always leery about downloading apps when I don't recognize a well known name.

****

Submitted by Bob King (EVACC) and Peggy Bullock (Kim Komando):

The following articles all relate to a WanaCrypt Ransomware attack

Submitted by Bob King (EVACC – East Valley Association of Computer Clubs):

Many of you have probably heard about the Ransomware attacks that occurred worldwide this past week. Here is an article explaining the attacks and Microsoft's response. I suspect many are not still running Windows 8 nor Windows 8.1 or XP. But it will not hurt to pass this information along.

Microsoft Issues WanaCrypt Patch for Windows 8, XP

(Taken from: https://krebsonsecurity.com/2017/05/microsoft-issues-wanacrypt-patch-for-windows-8-xp/)

On Saturday May 13 the **Microsoft Corp.** today took the unusual step of issuing security updates to address flaws in older, unsupported versions of Windows — including **Windows XP** and **Windows 8**. The move is a bid to slow the spread of the **WanaCrypt** ransomware strain that infected tens of thousands of Windows computers virtually overnight this week.

On Friday, May 12, countless organizations around the world began fending off attacks from a ransomware strain variously known as WannaCrypt, WanaDecrypt and Wanna.Cry. Ransomware encrypts a victim's documents, images, music and other files unless the victim pays for a key to unlock them.

It quickly became apparent that Wanna was spreading with the help of a file-sharing vulnerability in Windows.

Microsoft issued a patch to fix this flaw back in March 2017, but organizations running older, unsupported versions of Windows (such as Windows XP) were unable to apply the update because Microsoft no longer supplies security patches for those versions of Windows.

The software giant today made an exception to that policy after it became clear that many organizations hit hardest by Wanna were those still running older, unsupported versions of Windows.

Another from Kim Komando's site by Mark Jones:

Worldwide ransomware attack spreading like wildfire - More than 100 countries hit!

By Mark Jones, Komando.com

We've been warning you for quite some time that ransomware attacks are nasty. This, of course, is when cybercriminals encrypt important files on your gadget and demand a ransom to give you access to them again.

In most cases, the victim clicks on a malicious link, which leads to their device being infected. However, the largest known attack to date is happening right now worldwide, and you don't even have to click a link to be impacted.

What you need to know about the world's largest ransomware attack

What we're talking about is a massive ransomware attack dubbed **WannaCry**, or **WanaCrypt0r 2.0**. It started spreading Friday, May 12 and has already locked computer systems in at least 150 countries worldwide. The attack has targeted private companies and public organizations, but it's spreading so fast no one is safe.

As we said earlier, typically a ransomware victim clicks a malicious link before their gadget is infected. This attack is different. It is being deployed via a worm and spreads itself between vulnerable computers connected to the same network.

Once a gadget is infected with WannaCry, its files are encrypted and a ransom note appears on the screen. The criminal behind the attack is demanding $300 in Bitcoin payments to decrypt the victim's device. Following is an example of what the ransom note looks like:

Image: Example of WannaCry ransom note.

This attack has actually endangered the lives of people. Hospitals in England were victimized by WannaCry ransomware Friday and had to turn patients scheduled for surgery away and cancel appointments.

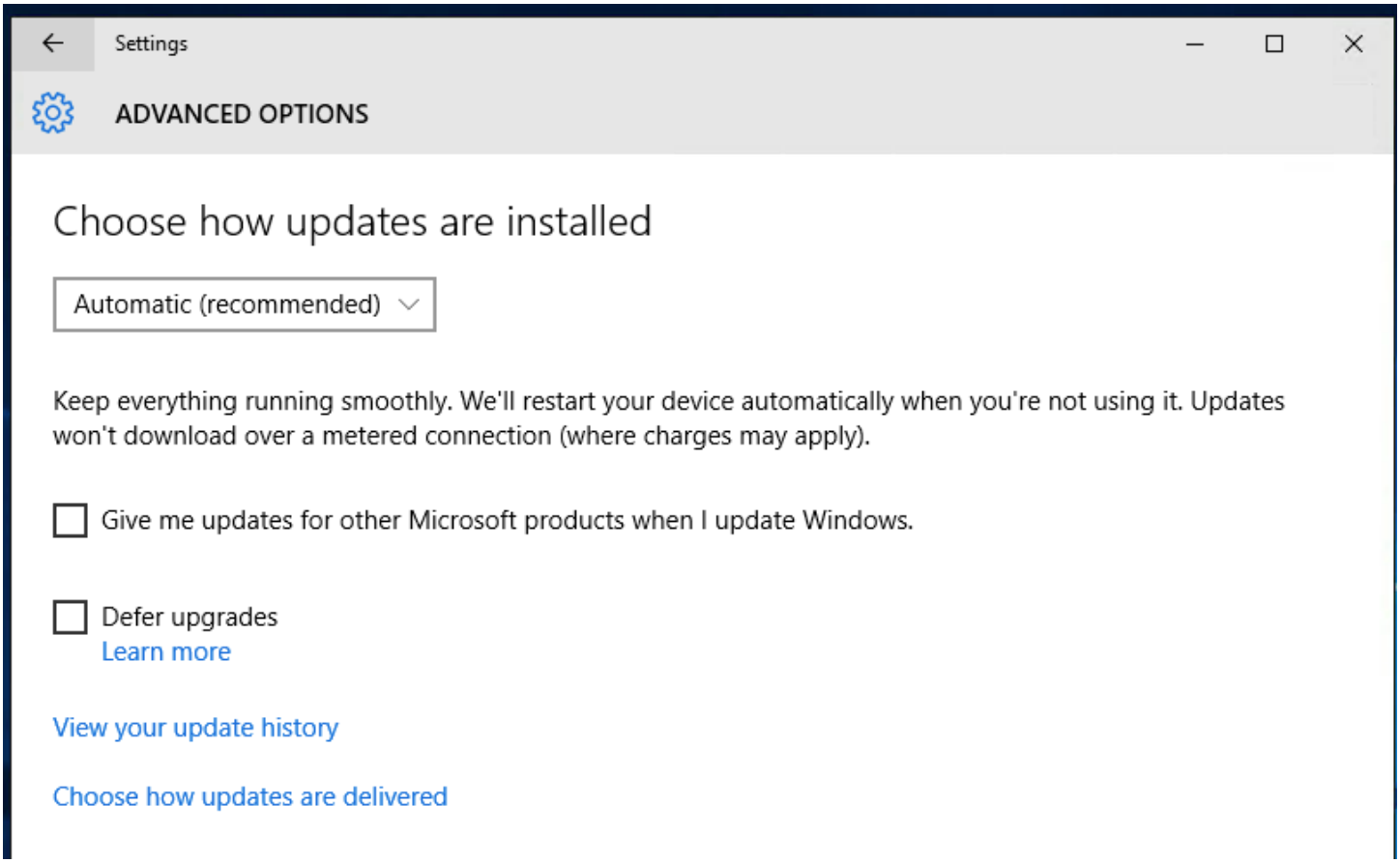
How to protect yourself from WannaCry ransomware

Reports say the criminals behind WannaCry ransomware are exploiting the **Eternal Blue** flaw in Windows operating systems. [This flaw is an NSA tool leaked by Shadow Brokers earlier this year](#).

Microsoft knew of this vulnerability months ago and sent a patch for it in an update back in March. So it is ***CRITICAL*** to make sure your Windows OS is up to date.

Most Windows machines are set to download and install updates automatically by default. If you haven't changed your automatic update settings then you should be fine.

But if you want to check, here's how:



On Windows 10, click **Start** (Windows logo), choose "**Settings**," select "**Update & Security**," then on the "**Windows Update**" section, click on "**Advanced Options**." (Note: the "Windows Update" section is also handy for showing you updates that are currently being downloaded or applied.) Under "Advanced Options," just make sure the drop down box is set to "Automatic."

If you have an older Vista or Windows 7 system, check out our tips on how to set up and check Windows Updates.

Backing up your critical data is also an important safety precaution in the fight against ransomware. It's the best way to recover encrypted files without paying a ransom.

****

Submitted by Steve Andreasen:

HMMMMMM, be cautious of what you buy……..

All New Windows 10 Has a Serious, Unfixable Problem

Gordon Kelly, Contributor, I write about technology's biggest companies.

Opinions expressed by Forbes Contributors are their own.

Microsoft MSFT +0.07% has an all new version of Windows 10, confusingly called 'Windows 10 S' which promises to be a faster, cheaper and more secure version of Windows 10. But Microsoft has now confirmed not only does Windows 10S have a serious problem, it is one that cannot be fixed…

The problem stems from Microsoft's decision to only allow software installation on Windows 10S if it comes via the official Windows Store. Right now the Store is a wasteland and avoided by both Apple and Google among many others. But it's about to get worse.

Microsoft's Surface Laptop is the Windows 10 S launch device, but it is severely compromised by the new platform

Whereas many thought the solution would simply right itself as customer pressure pushed companies to publish through the Windows Store, it turns out there's a bigger issue and one that hits web browsers in particular because Windows Store policy states:

"Apps that browse the web must use the appropriate HTML and JavaScript engines provided by the Windows Platform."

This is not the language Chrome is written in (nor Opera) so in order for Google to make the world's most popular web browser available on Windows 10S it wouldn't just have to repackage and list it in the Windows Store, it would have to completely rewrite the core code of the browser. Even then Windows 10S does not allow users to change the default browser from Microsoft Edge and the search engine from Bing.

In a statement Microsoft told MSPoweruser:

"Windows Store apps that browse the web must use HTML and JavaScript engines provided by the Windows Platform. All Windows Store content is certified by Microsoft to help ensure a quality experience and keep your devices safer...If people would like to access apps from other stores and services, they can switch to Windows 10 Pro at any time."

Upgrading to Windows 10 Pro from Windows 10 S will cost $50, though there's a free upgrade promotion until the end of 2017.

Windows 10 S is Microsoft's newest operating system, but it is likely to confuse a lot of users fitting in between Windows 10 Home and Windows 10 Pro

Of course Microsoft isn't the first to lockdown browser control. iOS has the same browser coding restrictions forcing Google to use WebKit as the base for Chrome on iOS rather than its own Blink engine which it uses on Android. But there's far more pressure for Google to be on iPhones and iPads than PCs running a new niche Windows operating system - especially one designed to compete directly with Google's own burgeoning Chrome OS.

But the tech world is nothing if not hypocritical.

Technically Chrome OS doesn't allow for an alternative browser to be installed, though there is a workaround using the Google Play store which is Chrome OS-compatible. Furthermore I suspect customers will be a lot more resistant to being locked into Edge and Bing than Chrome and Google search.

So far Microsoft has yet to specify what the 'S' in Windows 10 S stands for. If the operating system doesn't become more flexible in its restrictions, customers are going to pick their own word…

****

Remember to visit the website with the NEW address for more Tech Tips and club announcements over the summer. (www.supercomcc.org).

From: Mike Gerkin, Rick Heesen, Steve Andreasen and Peggy Bullock