SUPERCOM COMPUTER CLUB TECH TIMES

Volume 18 May 1, 2018

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)

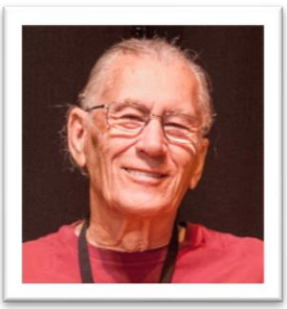
Ben Tarbell, Mike Gerkin, Peggy Bullock, Jim Mills, Rick Heesen, Lowell Lee, Steve Andreasen (Apple/Mac) and Mike Smith. Jim Oliver and Dick Strong.









Dick Strong and Jim Oliver are on "time off" for season 2017-2018.

Greetings

IS IT SPRING WHERE YOU ARE????

AZ SPRING

I know a lot of you have had to face snow when returning to the north or and east, but I am hoping you are starting to see the beauty of Spring in your neighborhoods soon! Nothing better than a new season with new life.

And since we like to keep up to date on new things, we are beginning the Spring/Summer season with new Tech Times articles for you to read. Because some of the articles are long and the newsletter would be up to 20+ pages, I have included links for you to click on so that you can continue reading the entire article on the webpage from which it came. Please take the time to click and read the information that our Tech people have researched out to share with you.

Remember – Our Club Website is: www.supercomcc.org. We try to keep it up to date too. I have a few more meetings/pictures to add that I became slack on towards the end of the season. I promise to get it updated too!

All links in our newsletter are safe to click on.

Submitted by Rick Heesen:

What Is a Port-Out Scam?

If you want to switch cellphone carriers, you can typically bring your existing phone number with you—because who wants to get a new phone number if they don't *have* to? No one, that's who.

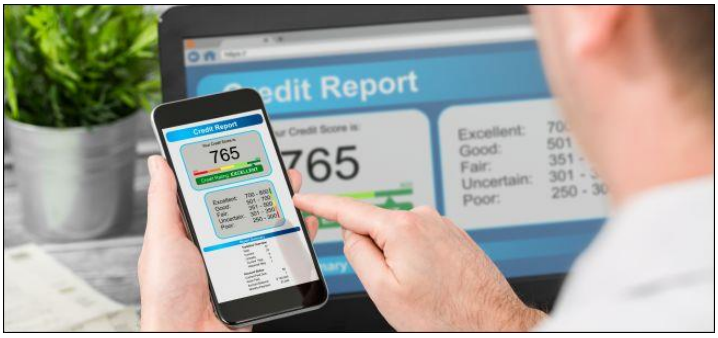
Now, imagine someone walking into a carrier store (or calling them) and pretending to be you. Without the proper security measures in place, this person could pretty easily steal your phone number and take it to a new carrier, effectively shutting off your phone service and taking control of your number. That's pretty scary.

And that's not the only type of porting scam in the wild today— TO READ THE REST OF THE ARTICLE, CTRL + CLICK on the following link: What is a Phone Port-Out Scam.

Submitted by Rick Heesen:

How to View (and Monitor) Your Credit Report for Free

By Chris Hoffman, March 18th, 2018



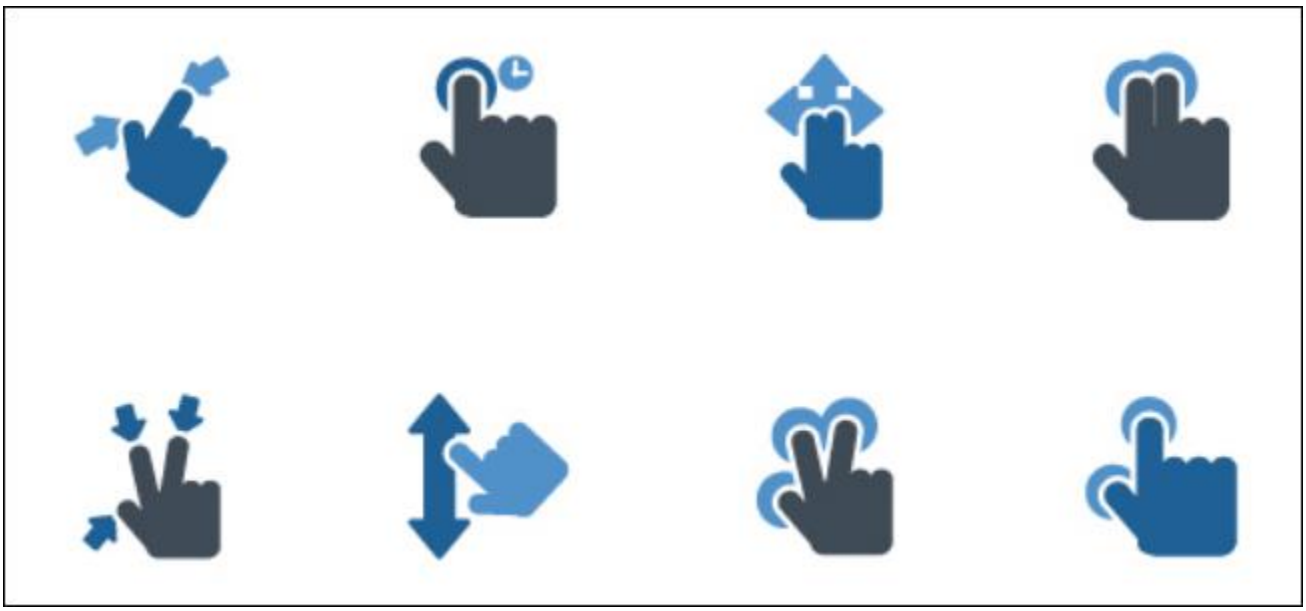
If you keep a regular eye on your credit report, you'll notice when identity thieves open accounts in your name and when errors are listed that might cause you problems in the future. Here's how to do it for free.

To read this article, CTRL+CLICK this link: How to View and Monitor Your Credit Report for Free.

Submitted by Rick Heesen:

Seven Android Gestures You May Not Know About

By Cameron Summerson, April 13th, 2018



Gestures make using your phone faster and more efficient—but only if you know the gestures in the first place. Here's a collection of some of the best ones for Android that you may not already be using.

CTRL+CLICK on the blue title above to read the full article.

Quite interesting!! Might have to try them a few times to get the hang of it, but they work. (Peggy)

Submitted by Mike Gerkin:

SHUT DOWN/SLEEP/HIBERNATE

Through the years I have had several SuperCom members ask me if they should regularly shut down their computers, or if the sleep or hibernation modes are worth using. While the answer may vary based on the members actual usage, I see that Ask Leo has a very good article on just that topic. It is worth reading to learn more about just how your computer works in different conditions.

CTRL + CLICK here: Ask Leo Article

Along with Mike's article, the following was shared from APCUG (Association of Personal Computer User Groups):

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 (Central Kentucky Computer Society)

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

Submitted by Ben Tarbell: (I have included the complete article in the Tech Times for this one. Lots of good information I don't want you to miss!!)

7 Sudden Signs You Have Been Hacked

Source: https://www.komando.com/tips/452528/7-signs-youve-been-hacked-that-you-need-to-know-now

7 signs you've been hacked that you need to know now

By Francis Navarro, Komando.com

In this digital age where everyone everywhere is interconnected via the magic of the internet, there will always be groups of cybercriminals looking to take advantage of us. We hear of data breaches, malware attacks, ransomware and phishing scams constantly - it seems like we are under attack around the clock.

And it's true, online threats never stop. They are lurking in every corner of the web, waiting for that inadvertent click, that hasty install, or that vulnerable gadget that can be exploited. Don't be shocked, but an unpatched and unprotected PC can get hacked in less than five minutes when connected to the internet!

This means knowing the signs that your gadget is hacked or compromised is critical. Why? Time is of the essence when you're dealing with malware and data breaches and detecting them early enough is key.

Here are the top seven signs that you've been hacked:

1. Your gadget suddenly slows down
2. You're using more data than usual
3. Videos are suddenly buffering and webpages take forever to load
4. Programs and apps start crashing
5. You start seeing pop-up ads
6. Your gadget suddenly restarts
7. Things are happening you had no part of

WHAT CAN YOU DO?

EASY STEPS TO PROTECT YOURSELF

1. **Install security software**
2. **Keep software up to date**
3. **Create strong passwords and security questions**
4. **Slow Down - Pause before you click**
5. **Freeze your credit**

Now – if you are interested in the detailed information, keep reading on the following pages.

Please note - there are clickable links within the article.

1. Your gadget suddenly slows down

Have you ever wondered if you have hidden malicious software lurking within your computer? Maybe at times it is abnormally sluggish, constantly freezing, or you feel that something just doesn't feel right. If you start noticing some of these symptoms, your gadget may very well be infected with viruses, trojans or worms.

Malicious software usually run in the background, secretly eating up your gadget's resources while it's active.

If your gadget starts struggling to do the most basic tasks and lags or freezes even without any open apps you know of, then hidden malicious software may be churning along quietly, using your device memory and processor resources.

What can you do?

Here are tools you can use to pinpoint those nasty applications. If an application that you don't recognize is hogging your computer resources, it's likely a virus!

PC: Use Task Manager

There are a few ways to see what processes your computer is running. The easiest is to bring up Windows' built-in Task Manager. Just use the keyboard shortcut CTRL + SHIFT + ESC and go to the Processes tab.

Note: *Windows 10 and 8 present process information in a much friendlier way than Windows 7 or Vista. If you're on Windows 7 or Vista, you'll probably want to pick up the program Process Explorer.*

You'll see the process name, how much of your computer's processing power it's using, how much memory it's hogging and - sometimes - which programs use it.

So where do processes come in handy? Well, your computer might be feeling sluggish on a regular basis. Open up Task Manager and check the CPU and memory columns for each process.

You might find one process is using 100 percent - or close to it - of your CPU for a long period of time. Open up the program associated with the process and see what it's doing.

If it doesn't appear to be doing anything, restart it and keep an eye on it for a while to see if it starts hogging your processor again.

Click here to learn 7 secrets of Windows Task Manager every computer user should know.

Mac: Use Activity Monitor

To view open processes and computer resources usage on a Mac, use the Activity Monitor.

To quickest way to access the Activity Monitor is by using Spotlight Search.

Click the magnifying glass on the right side of the menu bar at the top of your screen or press Command + Spacebar to open a Spotlight window and start typing the first few letters to auto-complete "Activity Monitor." Just press enter to access the tool.

Another way of accessing the Activity Monitor is through the Launchpad. The Activity Monitor is in the "Other" folder. Optionally, you could then drag its icon to the dock for easy access in the future.

Similar to Window's Task Manager, Mac's Activity Monitor displays a list of all your open processes with tabs for CPU, Threads, Idle Wake Ups and Network usage.

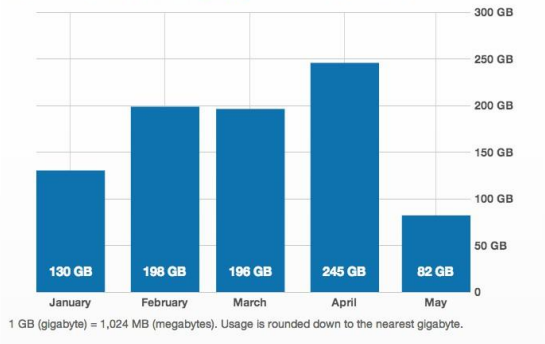
Learn these three troubleshooting shortcuts every Mac user should know.

If this happens when you are on an iPhone, try a soft reset by holding the power and the home button until it reboots with the Apple logo. This can clear out frozen apps that can be hogging your memory.

On Android, try rebooting as well, or better yet, boot into safe mode to troubleshoot any errant apps.

If resetting your device doesn't resolve the high resource usage, then there's a high probability that your phone is infected.

2. You're using more data than usual



One thing you will notice if your gadget has been hacked is an unexpected increase in data usage. Every internet provider has tools that can keep track of your monthly bandwidth consumption.

Look under Data Usage Meter or Data Monitor, depending on your provider.

Now, compare the amount of data used for data usage from the prior months and if you notice sudden spikes in your data activity even though you haven't really changed your patterns, then chances are you are infected.

For example, adware infected gadgets usually perform unsolicited clicks in the background to generate profit for cybercriminals.

All of these stealthy tactics use up bandwidth and the unauthorized data they consume should be fairly easy to spot.

Do you want to save on your data consumption? Here are 5 steps to cut your data usage in half.

3. Videos are suddenly buffering and webpages take forever to load

We've all seen this happen one way or another - we're tucked cozily on our favorite sofa, hoping to binge-watch a show on our favorite streaming service.

Then it happens...the dreaded buffering circle rears its ugly head again.

So, you check your internet speeds. Uh oh. Webpages are slow to load, surfing the net comes to a crawl. What's wrong? The problem could be with your internet service or maybe your router simply needs a reboot.

However, it might be something more malicious. Your neighbors or another unknown party could be on your network using your bandwidth.

Click here for steps on how to check for Wi-Fi thieves.

Or maybe a virus is redirecting your web traffic or hogging your internet connection. One way malware can slow down your internet traffic is by DNS hijacking.

What these clever hackers do is insert rogue DNS servers so your traffic is directed to unsafe servers instead of the secure servers your internet service provider gives you. This will not only slow down your browsing experience, it's a serious security risk, as well.

For example, if your router's DNS settings have been hijacked, each time you visit your online bank's website, you'll be redirected to a phishing website instead.

To check your router's DNS settings, you can use an online tool like F-Secure Router. For more security, consider changing your DNS server to one with advanced hijacking protection like CloudFlare or Quad9.

Do you want to make your router hack-proof? Click here for more tips.

4. Programs and apps start crashing

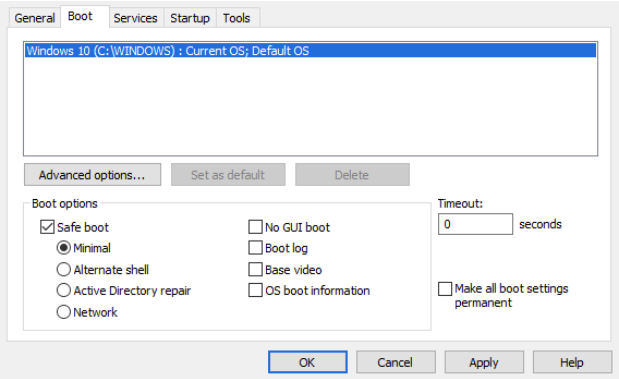
Now, here is a definite symptom that your system has been severely infected. If your antivirus software and task manager are either crashing or disabled, then a nasty virus has already taken hold of your critical system files.

If your gadget is compromised, you may not be able to click on the apps that you rely on every day. Or, if you've been hit by ransomware, you may not be able to open files you regularly use. It's frustrating and a little scary.

You can try and fix the problem by booting your gadget in Safe Mode. With Safe Mode, your computer will be running with just the bare essentials.

This way, you can safely delete and uninstall any programs and files that you can't during normal operation.

Windows:



On Windows, search for System Configuration then open it >> select Boot tab then tick off Safe Boot >>check Minimal (this is enough for most cases) >> click on OK to confirm >> Restart your computer.

Click here for detailed steps on how to boot into Windows Safe Mode.

macOS:

On a Mac, press and hold down the Shift key while restarting your computer. Keep holding the key through the Apple logo and release when you see the login screen.

Android:

Android also has its own version of Safe Mode but there are different ways to activate it, depending on your phone model. Click here to learn how.

iOS:

Stock iOS doesn't have a Safe Mode but you can try a soft reset to fix most issues. To do this, press and hold both your iPhone's Home button and the Sleep button at the same time, wait for it to restart then let go of the buttons when the Apple logo is displayed.

The iPhone X doesn't have a Home button so the process is a bit different.

Press and quickly release the volume up button, press and quickly release the volume down button then press and hold the side button and release when the Apple logo appears.

If attempts to fix the issues in Safe Mode fail, it may be time for a complete restore so you can start fresh. If you're recovering from a serious malware infection, starting from scratch is the only way to go.

5. You start seeing pop-up ads

If you're starting to get annoying pop-up ads and notifications, unwanted reminders and nagging "system" warnings that just won't go away, then your gadget may have been compromised.

Malware can also add bookmarks that you don't want, website shortcuts to your home screen that you didn't create and spammy messages that entice you to click through.

Apart from slowing down your gadget and eating away at your data, these intrusive notifications can also install more malware on your system.

Criminals can also use DNS hijacking to modify the ads that you see while browsing. Instead of the regular ads that you should be getting, they can be replaced with inappropriate or malicious ones.

This opens you up to a whole world where all your personal information is vulnerable and your system's chances of getting infected with malware go up.

On Windows, clean out adware with SpyBot Search & Destroy. On a Mac, use Malwarebytes for Mac.

6. Your gadget suddenly restarts

Automatic restarts are part of normal computer life. For example, software updates and new application installs can prompt you to reboot your computer. Your system will always warn you when these happen, though, and you can delay or postpone them if you desire.

Sudden restarts are a different story. If your computer randomly shuts down or reboots while you're in the middle of an activity, then it's definitely a sign that something's amiss.

It could be a buggy application that's crashing, faulty hardware or, you guessed it, a virus lurking in the background.

With Windows 10, there's a free malware detection and extraction program called Microsoft Windows Malicious Software Removal Tool.

A Full Scan with this tool is a recommended method if you want to verify that the tool is updated with the latest malware definitions or if you want to have a more thorough system scan.

7. Things are happening you had no part of

This is what hackers covet the most - your usernames and passwords. These, coupled with social engineering tricks, can gain access to your banking accounts, your social media profiles, and your online services.

Keep an eye on your email's "sent" folder and on your social network posts. If you notice emails and posts that you don't remember sending or posting, it's likely that you have been hacked.

Constantly check your accounts for unauthorized activity - movies on your Netflix profile that you don't remember streaming, mystery purchases that you haven't made, songs on your Spotify that you didn't listen to, credit card charges that came from nowhere - if something's amiss, report it immediately.

Did you know that your stolen information can be up for grabs on the Dark Web for cheap? Click here to learn more.

EASY STEPS TO PROTECT YOURSELF

1. Install security software

The most important habit for good online security is to use strong security software. Good security software stops most attacks before they can even start, but great security software goes beyond that with other features that keep you safe.

Of course, while great security software will protect you against most threats, there are still some things you can do to help out. Whether the virus is in a download, email or coming at you online, security software can detect and block it.

Windows already has built-in virus protection with Windows Defender while Google scans malicious files and apps on Android with Google Play Protect. There are plenty of free and paid third-party security software programs for both Mac and Windows, too. Avast and Malwarebytes are popular because, well, they're free.

2. Keep software up to date

If you want to keep your computer safe and get the latest features, which you do, it's important to install the updates as soon as you can especially if they're aiming to fix security bugs and

issues. Keep all your apps, smart appliances and even your router updated with the latest patches and firmware too.

There's an important term in computer security you need to know called a "zero-day exploit."

Zero-day exploits are some of the biggest threats developers face. The term "zero-day exploit" is just a fancy way of describing exploits that are discovered and abused by hackers before the software company has time to issue a patch.

If hackers can find a zero-day flaw in a program, they can use it to attack computers until the software developer finds the flaw and updates the program. These types of flaws pop up regularly in major software like Windows and other Microsoft programs, web browsers, Adobe programs and Java.

Zero-day flaws often let hackers get around your security software with no input from you. Obviously, it's important to update these programs, and any other programs you use, whenever patches are available.

3. Create strong passwords and security questions

Securing your online accounts is just as important as securing your Windows account. The first step is to have a strong password and security question.

When you're creating an online account, you might be in the habit of rushing to get through the process so you can start using the site. That's why many people use weak passwords like "password" or "123456," or reuse passwords from other accounts.

Both of these make you unsafe. Hackers can guess an easy password in minutes. If you reuse passwords and they get your password in a data breach then they can get into all your accounts without a problem.

That's why you need to get into the habit of creating unique, complex passwords. These take more time to create, but they keep your information safe. Of course, you also need a good way to remember them. Here are 5 password mistakes that will likely get you hacked.

We recommend using a password manager. This can store all your passwords behind a single master password. That way you can have dozens of complex passwords and only have to remember one. Most password managers can also help you create strong passwords.

4. Pause before you click

One of the biggest threats out there is phishing scams. These are deceptive emails and text messages that trick you into clicking on a link to a malicious site or downloading malicious attachments.

There are many phishing scam tactics, but they all rely on you clicking before you have a chance to really think things through. A phishing scam might say there's a problem with your Amazon account and you need to click fast to clear it up. Or maybe it says you can win a free iPad if you sign up immediately.

Taking a second to think is usually enough time to unravel the scam. You might notice a fishy email address or horrible spelling and grammar, or just remember our advice to never click on links in unsolicited emails.

That's why you should make a habit of waiting a second or two before clicking any link. Use that second to confirm that nothing is out of the ordinary. And if you click the link and are presented with something else to click, take another second to really look at that as well.

While this will add a few seconds to each email, it's worth it when you easily avoid the next phishing email to roll around. Learn more about spotting and avoiding phishing emails.

5. Freeze your credit

If you suspect that your identity has been compromised, here's one essential step you must take to stop criminals from opening credit card accounts under your name.

A credit freeze, also known as a security freeze, allows you to restrict access to your credit reports and scores provided by the three major credit bureaus (Equifax, Experian, TransUnion).

Locking up your credit reports will prevent identity thieves from opening new accounts under your name even when they have managed to steal your personal information. Since lenders are required to check your credit report before they can approve a new application, a credit freeze can stop fraudulent accounts from being made at your expense. Learn more about how to set up a credit freeze.

As always, we ask you to be vigilant in keeping your Windows Updates up-to-date, especially if you have a Windows 7 Operating System. Problems with updates are one of our biggest challenges. If you need help with any of these, feel free to contact one of our Tech Geeks. Our email addresses are available on the website. During the summer, we will try to help as best we can. For those of you in the park during the summer, we are sure Rick Heesen would be still willing to help if you can't figure it out.

Your Techs for this time:

Rick Heesen, Mike Gerkin, Ben Tarbell & Peggy Bullock