# SUPERCOM COMPUTER CLUB TECH TIMES

Volume 01   November 4, 2016

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 and Steve Andreasen (Apple/Mac).
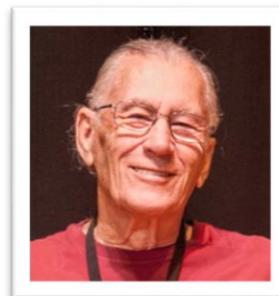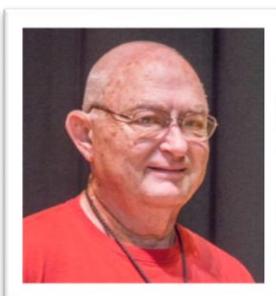
Dick Strong is on "time off" for season 2016-2017.

Greetings

WOW!! What a great start to the new season! Congratulations to our new officers and to all those volunteers that keep the gears moving. That is the ⌕ to a successful club!

Ben Tarbell and Jim Oliver did a great job on their Windows 10 Anniversary Update presentation along with the overview of Windows 10. Watch for their SIG and Windows 10 classes.

Among some of the questions that were asked this morning, one very important one that Mike Gerkin will address in the following tip –

Virus Alert: Real or Rogue

Just a few days ago when I was browsing on the Internet and also recently when I received an unusual email, I saw a message that told me I had a virus on my computer and to immediately call the number on the screen. I knew something was wrong.

But sometimes it may not be easy to simply close that message that is on the screen. If this happens to you, it could mean that you have picked up a real virus in your computer, but more likely than not you may simply be looking at a simulated virus that is nothing more than a web page that a scammer has made difficult to close. If the message is contained in an email, it likely is a trap waiting for you to spring it.

Either way, **do not call** that phone number! You will surely be connected to a fake "tech support rep" who will try to initiate a remote session with you. He'll also try to con you out of one or more credit card numbers with a comment like "Oops, that card was declined. Got another?" He may also try to get your bank account numbers, Social Security Number, driver's license number, and other data that can be used to steal your identity.

If you were to call, the most likely result is that you **WILL** have a virus after dutifully following the instructions of the person on the other end of the phone. Adding insult to injury, new credit card charges will be rung up, leaving you to sort things out with the card issuer. It has happened in our park. So **do not** call that phone number.

If this "virus alert" pops up only when you are browsing the Web, it is probably a fake Web page. Your computer does not have a virus. Just close your browser. But the fake page can be designed to take over your entire screen, leaving scant clues that a browser is even open. The page may also include code that makes it very difficult to close the page, and which re-opens the page if you do manage to close it. Your first step to get out of this trap is to close your browser without clicking anywhere on the page including the red X.

I suggest pressing the Ctl-Alt-Del keys simultaneously and hold them down until a Windows screen appears that bears the line, "Start Task Manager" or just "Task Manager". (Your screen may go blank for a few seconds.) Click on that to open the Task Manager utility. In the Applications tab or Apps section you will see the name of your browser (Internet Explorer, Google Chrome, Firefox etc.). Highlight that name and then click the "End Task" button at the bottom of Task Manager to force the browser to safely close.

If that doesn't work, you could choose to shut the computer the normal way by selecting the shutdown options from your start menu. Just pressing the power button to shut down a computer to get rid of a pop-up is always the very **last** option and should be saved for when the PC is completely locked up.

Shutting down your computer in this manner can sometimes cause bits of data to become corrupted and place junk in your registry. It's very important when things like this pop-up scam happen not to panic. Ask we discussed above, one panicked reaction might be to call the number for the fake tech support. Another could be to yank the power cord out of the wall or immediately push the power button. Take a breath and do the right thing, simply close the browser.

But what if I have been infected

If you suspect a virus infection, run the fullest, most in-depth scan that your antivirus software can perform. Then run another intense scan using another antivirus program, just to be sure. We have recommended several free anti-virus and anti-spyware programs in past newsletters for you to use. See our previous articles or talk to one of the SuperCom Tech Geeks for help finding and using free security tools.

If the "virus alert" message went away when you closed your browser, then the problem is almost certainly browser-related. The alert may simply be a page on a shady web site that you visited; the solution is to close that site's tab or window and never go there again.

But it's also possible that malware has infected your browser via an extension or add-on that you installed. A free utility from Malwarebytes named [ADWCleaner](#) will scan your computer, browser, and Windows registry for extensions and other programs that may harbor this "tech support" scam. It's also a good idea to run a full scan using the free or paid version of [MalwareBytes Anti-Malware](#) to catch malware your regular anti-virus may have missed. I have no interest in Malwarebytes but believe it makes some excellent free and subscription products. Again, your SuperCom Tech Geeks may be able to assist you.

Another option is System Restore which will roll back your Windows system to an earlier time before you started getting the "virus alert." We have previously described how to use this built-in Windows feature in past newsletters too.

Viruses generally don't throw up "alerts" to let you know something is wrong. Most malware prefers to operate in secret, so you won't find and remove it. They certainly don't proclaim "I am a fraud and I am just trying to get you to give me your valuable information". But there may be other clues. Just being aware of the unusual is a good start. A computer that suddenly runs sluggishly is another clue you may be infected with a virus. Whatever mischief the virus does in the background consumes resources and slows everything.

If your antivirus software is disabled and you didn't do it, a virus may have. If you cannot visit certain Web sites, especially sites that deal with security and antivirus programs, then you may well have a virus. See my instructions above to scan your computer for viruses if something doesn't seem right, or just as a precautionary measure.

Your thoughts or experiences on this topic are welcome.

The underlined highlights in blue are safe links to additional information.

Mike Gerkin

Peggy Bullock