# SUPERCOM COMPUTER CLUB TECH TIMES

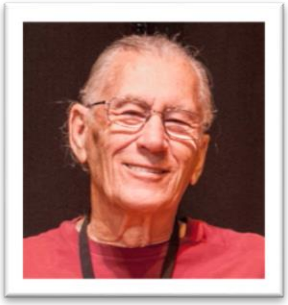
Volume 16 October 25, 2017

## Objective:

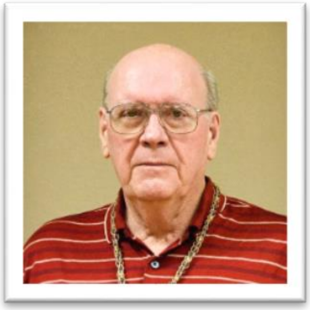
To bring the latest technology news to you, our members. Tips and suggestions will help you to keep your device(s) running smoothly and help you be aware of threats. Technical tips will be coming to you through our Technical Committee.

## 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

This will be the last Tech Times Newsletter before the beginning of our 2017-2018 season – unless, of course, there is a major issue that we feel you really need to know about!  You can count on us to let you know and not keep you in the dark until November 3rd!!

## A note from our incoming Chairperson, Bev Hooper

Summer has come to an end, and now we look forward to our winter homes in the park.  Some of you are there all year long while we others are preparing for departure from our summer homes.

Our first meeting will be on the 3th of November, 2017, and due to the timing, we will only have two meetings in that month.  There will be no open labs in November, they will start in December.

I hope you have looked at our new web site, www.supercomcc.org. It's great, and Peggy & Mike have done a great job in setting this up.   There is even a place for computer tips!!  If these fail to help you, then consult with the geeks who are of great assistance to all of us members.

Looking forward to seeing you all on the 3rd of November at 9:00am in the Ballroom.  Have a safe trip, and don't forget all those necessary cords for your electronic systems.

Bev Hooper, Chair.

******************************

**Submitted by Rick Heesen:**

In last month's Tech Times, Rick addressed the CCleaner hack and some issues.  But we all know we have to be vigilant with our updates – keep your software programs up-to-date.  Here is another follow-up article from Ask Leo:

### What the CCleaner Hack Means to You

CCleaner, a popular Windows utility, accidentally included malware in its download for a time. Here's my take on what to be concerned about and what to do.

How about a word on CCleaner. Do you still recommend?

I do.

I don't believe in "one strike and you're out". CCleaner remains a valuable tool for your computer maintenance needs…

… regardless of what is being said by some click-bait headlines.

**What happened**

For one month, downloads of CCleaner version 5.33.6162 included malicious software.

It's a company's worst nightmare. I'm constantly telling people to download software from the official download site to avoid unexpected add-ons in the form of PUPs and malware. When the official site itself is compromised, even that advice doesn't help.

Avast (the new owners of Piriform's CCleaner) has updated the product to remove the malware, and current downloads are safe. They're also in the process of determining the exact scope of the attack, who was vulnerable and to what degree, and what safeguards they need to avoid this type of thing happening again.

Initial indications are that while the malware has affected over two million machines, it's effectively been neutered. The malware itself did nothing malicious, other than act as a gateway for the potential backdoor installation of additional malware. The command-and-control servers used to make that delivery have been taken down. The current understanding is that this was a targeted attack on "select large technology and telecommunication companies", according to Avast. Consumer machines were characterized as "uninteresting" to the malware.

**What seems to have gone well**

In my opinion, Avast has done a good job of publicly reporting the issues, and continuing to report on the progress of their investigation.

Of course this should never have happened, but as I've said before: there's no such thing as perfect security. What's arguably at least as important as good security is the quality, speed, and honesty in response to security issues that are discovered.

So far, Avast appears to be handling it well.

**Disappointing headlines**

I wish I could say the same for some of their competitors.

In recent days, I've seen at least two cases of companies I would characterize as being in competition with either Avast or CCleaner publishing headlines and "analysis" I can only characterize as hyperbole. Rather than addressing the specific issues encountered, and perhaps contrasting their own product in comparison, they seem to be using this event as an excuse to use the worst possible terms and impacts to characterize CCleaner (or Avast) as no longer trustworthy and something that should be immediately abandoned.

I don't agree. Not at all. So much so that my opinion of those other products has been somewhat diminished.

**The worst-case scenario**

One thing I've seen referenced is what I often refer to as the "nuclear option" when it comes to malware.

Specifically, some competitors have recommended that you completely reformat your machine and reinstall Windows from scratch if you happened to install the affected version of CCleaner.

In an absolute sense, that option is valid. Once you have malware on your machine, you have no idea what it might have done. *But that's true for any and all malware, at any time and from any source.* Why they happened to make that recommendation in response to this specific situation becomes highly suspect if they're not making it any other time.

At a more practical level, its gross overkill, and in my opinion, unwarranted.

At worst, you might restore from a backup image taken prior to CCleaner's installation. Honestly, even that is overkill, and not something I recommend or will do myself.

**What I recommend**

My response to this is pretty simple, actually:

- Update your copy of CCleaner, if you plan to use it, or simply uninstall your current copy. You can always reinstall later when you need the tool again.
- Run up-to-date anti-malware scans. Your automated scans and updates may be enough, but to be on the safe side, have your security tool run a complete scan manually.
- Stay alert to more news. If something more troubling is discovered, then take action in proportion to its severity. Right now, I'm not expecting anything major at all.

Most of all, I'm *not* recommending that you abandon CCleaner. It remains a good and useful tool.

As long as Avast's response continues to be appropriate, I see no reason to bail.

Article by Ask Leo.

******************************

**Submitted by Mike Gerkin:**

Since Verizon has acquired Yahoo more information has been released regarding some significant breaches of Yahoo security occurring several years ago. See Yahoo Breach . We now know that apparently over 3 billion accounts were affected. Although Yahoo eventually forced users to change their passwords and security questions because of the 2013 hack, it would be advisable to change them again because of subsequent breaches occurring in 2014 and 2016 if you have ignored our previous suggestions to do so.

Just because you haven't yet been a victim because of these hacks does not mean your exposed data will not be used in the future if you do not make changes to your account.

******************************

**Submitted by Peggy Bullock:**

# This security setting will stop thieves from emptying your bank account

By Francis Navarro, Komando.com

© Chad Mcdermott | Dreamstime

The massive Equifax data breach has dominated the digital security landscape for weeks now. It is now estimated that over 145 million American adults are affected by this incident, now considered as the largest credit data breach in history.

Click here to check if your personal data was exposed in the Equifax data breach.

The amount of personal information stolen is staggering. It includes names, Social Security numbers, birth dates, addresses, and even driver's license numbers. You might as well assume the hackers have your personal data.

Just think about this for a second - all your critical financial information, including your Social Security number, driver's license number, and credit card data may now be in the hands of cybercriminals, waiting to be used for whatever purpose they see fit. That's scary!

Bet you never thought of this. Click here to learn how the Equifax breach lets ID thieves have surgery on your dime.

**What this means for your money**

With all this critical information floating around, this means most of our financial lives will be disrupted for years to come.

Think bank accounts, savings accounts, retirement money, investments, credit accounts, Social Security benefits, even medical care - everything that is tied to your identity! Most of these accounts are set up and can be accessed with the information that was stolen in the Equifax breach. Just imagine all the security and identity risks we will be facing from now on.

We've told you about this one essential step you must take to stop criminals from opening credit card accounts under your name. Now I'm going to tell you about another equally important security tool you can use to protect your bank accounts and prevent thieves from stealing your money.

**You need to take this one step now**

I'm talking about turning on two-factor authentication (2FA) for your accounts. Two-factor identification is a fancy name for adding an extra verification step to the login process of your most critical accounts.

With the 2FA setting enabled, instead of just providing your username or password to log in to an account, a secondary form of verification is required to prove your identity.

The most popular form of 2FA right now is a special one-time code that's texted to your cellphone.

The idea is that even though hackers may have figured out your credentials, without the special code, they still won't be able to access your account.

This gives you an extra strong layer of security because it's unlikely that hackers have physical access to your smartphone too. Click here to read more about two-factor authentication.

**Important links to your bank account's settings**

Not all banks support two-factor authentication, but if yours does, set it up as soon as you can. It will definitely add another hurdle for hackers to go through. You can usually set up two-factor authentication either on your online banking account page or within the bank’s official app.

We've done the work for you.

Here are the links to some of the more popular banks or financial institutions' two-factor authentication setup page:

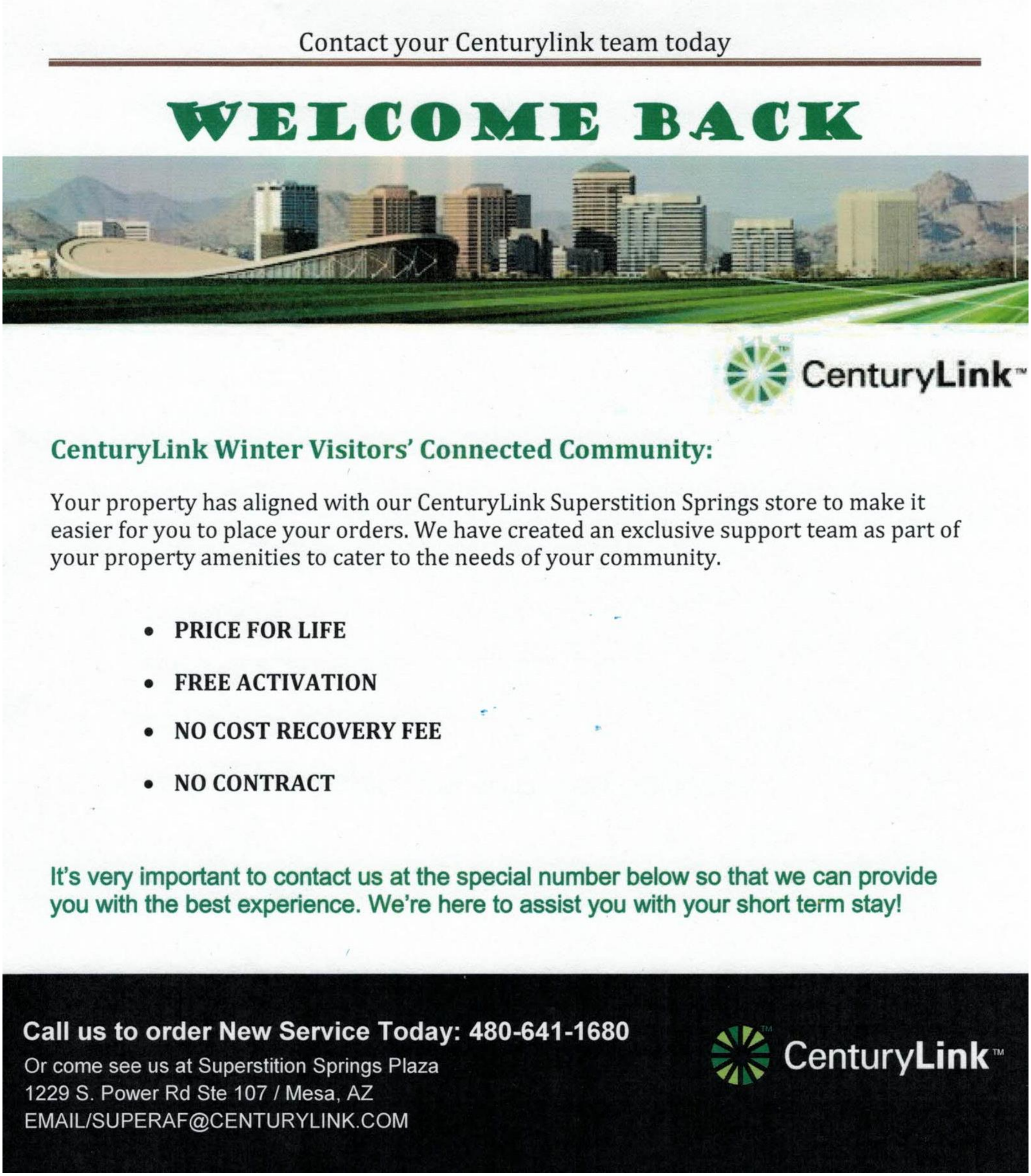
- Bank of America
- Capital One
- Chase
- Discover
- HSBC
- USAA
- Wells Fargo

If your bank is not on the list above, call or visit your bank. This useful site, twofactorauth.org, also lists services that use 2FA. It includes not just banks or financial institutions, but other online services, too.

******************************

**Submitted by Mike Gerkin through Alyson Stroup**:

**The following is the information regarding Century Link service for our winter residents and was in the last issue of Tech Times.  Just in case you deleted it and you need the phone numbers here it is again:**



Contact your Centurylink team today

# WELCOME BACK

CenturyLink™

## CenturyLink Winter Visitors' Connected Community:

Your property has aligned with our CenturyLink Superstition Springs store to make it easier for you to place your orders. We have created an exclusive support team as part of your property amenities to cater to the needs of your community.

- **PRICE FOR LIFE**
- **FREE ACTIVATION**
- **NO COST RECOVERY FEE**
- **NO CONTRACT**

It's very important to contact us at the special number below so that we can provide you with the best experience. We're here to assist you with your short term stay!

**Call us to order New Service Today: 480-641-1680**

Or come see us at Superstition Springs Plaza
1229 S. Power Rd Ste 107 / Mesa, AZ
EMAIL/SUPERAF@CENTURYLINK.COM

CenturyLink™

*******************************

**<u>REMEMBER – This is your computer club, here to help, but we are run by volunteers – and that means you!! If you are interested in teaching a class this season, please send your class suggestion, your name, phone number and email to</u>:** judith101345@gmail.com

**<u>Submitted by Steve Andreasen</u>:**

Steve says he gets asked this question a lot in his MAC SIG about Apple products – Read more:

### Do iPhones Need Malware Protection?

Unsure as to whether you need virus protection on your iPhone or whether you can get viruses on iOS? We have the answers.

By Joshua Rotter
June 01, 2017
Last Updated: August 03, 2017

### Apps in this Guide

Trend Micro Mobile Security

Avast SecureMe

McAfee Mobile Security, Vault, Backup and Locate

Apple's favor, its unique hardware, firmware, and software architecture; data encryption; and Touch ID, six-digit PIN codes, app store, and Find My iPhone features safeguard against most attacks. If you want even more protection and privacy, consider adding these recommended security apps above.

*******************************

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

Rick really keeps us on our toes! He is always the bearer of "good, scary" news! This article is a little involved for the novice. I even had to call Rick for help! But,,,,,,,,we do need to be aware of all these vulnerabilities!! Read the How to Geek article here: Your wi-fi Network is Vulnerable-How to Protect Yourself Against KRACK

*******************************

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

**HOPE TO SEE YOU NOVEMBER 3rd at 9:00AM in the BALLROOM**