

"Local Support • Personal Service • Since 1976"

www.ccstech.net

"Relax...we're on IT"

300 Main Street, Coopersville, MI 49404
616.997.TECH(8324)
Fax 616.997.9317

206 Washington, Grand Haven, MI 49417
616.842.TECH(8324)

3489 Kelly Street, Hudsonville, MI 49426
616.669.TECH(8324)

Beware of Fake Tech Support Scams

By Eric Ruzek

A problem many computer users face today are scammers looking to take your money by claiming to be from Microsoft, the IRS or some other entity that you are familiar with. You probably know someone that has fallen victim to a fake tech support call and they've given them access to their computer. Very often it comes from pop-ups on a webpage or even the whole page itself that indicates false problems and asks the user to call a phone number. They try and trick you into believing your computer has big problems or infections by giving you false information. Then they con you into purchasing software protection and services for hundreds of dollars and tell you it will last the rest of your life. The best thing to do at this point is to hang up your phone and turn off your computer! I've heard of some people asking them if their mother knows they are stealing, but that is just an option before you hang up. The key point is to NOT let them get remote access to your computer.

Here are some tips to avoid falling prey to a scam:

- Don't click on any links in emails you weren't expecting. Emails can be disguised to get your attention and make you want to click on it. They use tactics to make you want to click on those links which lead to problems.
- Verify emails from your bank that have links to click on. Even if it looks official it very possibly could be a scammer trying to get access. Scammers are very good at what they do.
- Be careful of unknown sites you visit. If you are doing a search for something, take a quick look at the link and make sure the word "Ad" isn't in front of it. This will lead to an undesirable site and problems.
- Make sure you are running anti-virus protection and you keep it up to date. *CCS Technologies* can help ensure your current product works properly or recommend a good anti-virus solution if you need one.

If you do fall victim to a scam here are some steps to take:

Call your financial institution and tell them about it.

There is a good chance they have already had others in the same situation. If so, there probably is a game plan in place to handle it. They can help keep your accounts safe, take care of fraudulent charges and issue new credit cards if they were used.

Turn off the computer and have it checked out.

Our policy at *CCS Technologies* is to wipe and reload the system after a scammer has gained remote access to your computer. We just don't know what software or other special "gifts" they left behind. There could be further problems because of keylogging software or remote access software. The best policy is to back up the data and reload from scratch. The computer will be clean of anything they did at the point. Our experienced technicians at *CCS Technologies* can assist you with that.

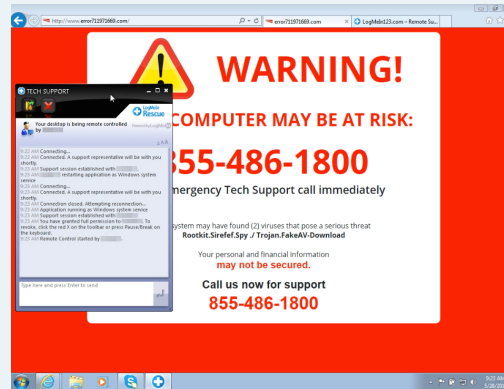
Keep an eye on all your accounts.

This is something you should be doing anyway. There are lots of savvy people looking at diverse ways to get your identity, steal your money and in general just cause you harm. You want to make sure your personal information is protected.

Change your passwords.

We know that there can be a lot of passwords to remember with all the different on-line services offered. This is a crucial step when you know your system is clean because you do not want to leave any door open for possible reinfection. You can get some helpful tips from our previous articles at <http://ccstech.net> under News and Newsletters regarding password management (see September 2017 Newsletter).

If at any time you are not sure if you've been hacked, PLEASE take the time to find out! You can call us, and we will be happy to help you. Stay safe!



Contact Information

Information	Info@ccstech.net
Tech Support	Support@ccstech.net
Sales	Sales@ccstech.net
Greg Slater	Gslater@ccstech.net
Ellen Slater	Eslater@ccstech.net
Drew Rowe	Drowe@ccstech.net
Jeff Verry	Jverry@ccstech.net
Joe Halstead	Jhalstead@ccstech.net
Jorge Arias	Jarias@ccstech.net
Karen Strickland	Kstrickland@ccstech.net
Mark Kowitz	Mkowitz@ccstech.net
Ryan McMillen	Rmcmillen@ccstech.net
Eric Ruzek	Eruzek@ccstech.net
Seth Johnson	Sjohnson@ccstech.net
Nick Dykstra	Ndykstra@ccstech.net

CCS Technologies Store Hours

Coopersville Store

Mon-Fri 8 - 5:30 & Sat 9:30 - 12:00

Grand Haven Store

Mon-Thu 9 - 6 & Fri 10 - 6
Sat 10 - 3

Hudsonville Store

Mon-Thu 9 - 6 & Fri 10 - 6
Sat 10 - 1

Lenovo ThinkCentre Tiny



- 2.7 Ghz Intel Quad-Core i5 CPU
- 8 GB DDR4 RAM
- 256 GB SSD Hard Drive
- Gigabit Ethernet & Dual Band Wireless A/C
- 6 USB ports and 3 DisplayPorts
- Windows 10 Professional 64-bit
- 12 Month Mfr Warranty

Setup and Ready to Use!

Prices good through 1/31/2018

While supplies last

Happy New Year!

From all of us at *CCS Technologies* we hope you have a good and prosperous 2018. It has been our privilege to serve you in 2017 and we look forward to helping you this year. We know technology changes very quickly and the cyber world can be very scary, but with great products and superior support we are committed to keeping you safe!

"Relax...we're on IT"