Fake Tech Support Scam

Fake Tech Support Scam | Tech Tips Video by PcCG

Fake Tech Support Video by PC Computer Guy Demonstrating what they do.

Several times a week we get calls about a virus on the computer. The caller explains that it says the computer is going to blow up in a nuclear explosion if it isn't fixed right away. Ok, maybe that's a bit of an exaggeration, but it warns your passwords, bank accounts and everything you have has been compromised. It says your network is infected, your browser hijacked, and says call some random 800 number to fix it immediately. They often say do not restart your computer or everything may be lost.

This is almost certainly a scam.

Let's start with the fix.

Most of the time simply restarting your computer resolves the issue (despite their warning that your computer will break if you restart it). They are telling you not to restart it, because they KNOW that will likely remove the "issue". If you can't restart for whatever reason, then simply hold down the power button for 10 seconds. This will FORCE the computer to shut off. Continue to hold it for the full 10 seconds. After it goes COMPLETELY off, you can then turn it back on. If you get a window saying "start in safe mode, or windows normally", choose windows normally. That's it. It's that simple.

Details about the scam.

This warning you may have received is simply a website. It did NOT scan your computer, it knows nothing about the state of the computer, it is not Microsoft. These are fake images, pictures that show these scary, legit looking messages to goad you into rashly calling them and forking over money to them.

FakeTechSupport.jpg [1]

Fake Tech Support Scam Published on PC Computer Guy (https://www.pccomputerguy.com)

Action Required Threats Detected	Confirm Navigatio Avast Detected Securit Found On Your Compu Technicians 1 €77-788 Are you sure you want	y Error, Due to Susp iter. Contact Avast ((Toll Free)	nline Scan		
Title		11000	e-surface -	Action	
SONAR.Heuristic.130 has been det	ected.	Critical	Infected	Contact Support	
SONAR.Heuristic.130 has been det	ected.	Critical	Infected	Contact Support	
SYSTEM CRITICA	LLY INFECTED			IMMEDIATELY	
Removed files are quarantined. To restore, click here			* Recommended Actions		
DO NOT TRY TO MANUALLY HARD-DRIVE MIGHT FAIL*	REMOVE THE VI	RUS,	AVAST TE	CHNICAL SUPPORT	

For example, if you went to the exact same website on a different computer, you'd receive the same message. If you do it on your smart phone, same message. If you take a brand new computer and go to that website, guess what? – Same Message! This because it's not really scanning and detecting things on your computer.

The goal is to allow a "tech" (aka scammer) to remote into your system. They then show you all these scary looking things on your computer. For example they'll bring up the command prompt (black old dos window) and type a couple commands and tell you that infections have been found. The funny thing is, they are just running normal commands... commands such as "show me all the directories and files", or "show me network connections". If you know what these are, you know that's how any computer should react. But if you have no clue what's going on, it looks scary. It's not. It's a scam.

NetStat.jpg [2]

Fake Tech Support Scam

Published on PC Computer Guy (https://www.pccomputerguy.com)

TCP	127.0.0.1:62998	photodex:62997	ESTABLISHED	
TCP	192.168.1.250:445	PC-Ronin:63647	ESTABLISHED	
TCP	192.168.1.250:3389	unknown : 62613	ESTABLISHED	
TCP	192.168.1.250:49156	a23-207-22-3:https	CLOSE_WAIT	
TCP	192.168.1.250:49157	a23-207-22-3:https	CLOSE_WAIT	
TCP	192.168.1.250:49171	207.244.67.199:https	CLOSE_WAIT	
TCP	192.168.1.250:49181	142:https	CLOSE_WAIT	
TCP	192.168.1.250:51202	in-in-f188:5228	ESTABLISHED	
TCP	192.168.1.250:51465	111.221.77.146:33033	ESTABLISHED	
TCP	192.168.1.250:51468	65.52.108.74:https	ESTABLISHED	
TCP	192.168.1.250:51516	bos-1009c:https	ESTABLISHED	
TCP	192.168.1.250:51548	91.190.216.55:12350	ESTABLISHED	
TCP	192.168.1.250:51554	li1021-206:https	ESTABLISHED	
TCP	192.168.1.250:51570	msnbot-65-52-108-190:)	https ESTABLISHED	
TCP	192.168.1.250:52185	a104-72-36-195:https	CLOSE_WAIT	
TCP	192.168.1.250:52190	a104-72-36-195:https	CLOSE_WAIT	
TCP	192.168.1.250:52366	f0:https	ESTABLISHED	
TCP	192.168.1.250:52412	a104-72-36-195:https	CLOSE_WAIT	
TCP	192.168.1.250:52413	a104-72-36-195:https	CLOSE_WAIT	
ICP	192.168.1.250:54349	server3302:5938	ESTABLISHED	
TCP	192.168.1.250:54788	f0:https	ESTABLISHED	
FCP	192.168.1.250:55026	168.63.140.76:https	ESTABLISHED	
TCP	192.168.1.250:55088	pccg-exchange:1467	ESTABLISHED	
TCP	192.168.1.250:55090	pccg-exchange:1467	ESTABLISHED	

They then show you the "event viewer" which is a big log of most things that go on in the computer. They will show you errors in the event viewer. The secret? Practically EVERY SINGLE COMPUTER will have many errors. Most of these errors are nothing to worry about. If you notice the date on most of the errors are old, and your computer continued to operate just fine. Again, they are simply showing you things to scare you into giving them your money. My own computer has plenty of errors at this very moment, none of which I am going to lift a finger to resolve because there's no need to. The computer works fine.

EventViewer.jpg [3]

Fake Tech Support Scam

Published on PC Computer Guy (https://www.pccomputerguy.com)

 Event Viewer (Local) Custom Views Windows Logs Application Security Setup System Forwarded Ever Applications and S Subscriptions 	System Number of events: 63,416 (!) N	Actions		
	Level Error Error Error Error Information Error Error Error Error Error Error Error	Date and Time 9/28/2016 2:19:37 PM 9/28/2016 2:19:37 PM 9/28/2016 2:19:35 PM 9/28/2016 2:19:35 PM 9/28/2016 2:10:00 PM 9/28/2016 2:05:39 PM 9/28/2016 2:04:07 PM 9/28/2016 2:04:07 PM	System Open Saved Log Create Custom Vie Import Custom Vi Clear Log Filter Current Log Properties ODE Find	
	Event 56, TermDD General Details The Terminal Server security layer details the client. Client IP: 190.10.8.98.	Save All Events As Attach a Task To t View Refresh Help	•	
< ,	Log Name: System Source: TermDD Fvent ID: 56 III	Logge <u>d</u> : 9/28/20 Task Category: None	Event 56, TermDD Event Properties Attach Task To Thi Copy	•

It is a scam! Again, just restart your computer and odds are you will be fine. If you continue to experience issues, then give us a call and we can give it a look over for you. 317-883-PCCG (7224)

The Catch

The difficult part is knowing what is a legitimate message you need to respond to and which is a scam. Generally speaking, if the message is NOT present when your web browser is closed (Chrome, Firefox, Internet Explorer), then it's a scam. If the message is STILL THERE with the web browsers closed, then it's possibly a legit message.

Another way to tell if it's a scam, is if the message is prompting you to call some phone number. Normal error messages in your system won't provide a number for you to call, it will simply tell you of a problem and it's up to you to get it resolved.

It's a bad habit to ignore all messages on your system about problems, and I don't want to encourage that. I simply want to help with the basics in terms of a legit warning, and a fake warning.

So now you know! Pass this information around to your friends and family so that they are informed as well and don't fall for this scam. You'll be saving them hundreds of dollars.

Knowing is half the battle!

Tags:Tech Tips[4]Tech Tips Videos[5]

Links

[1] https://www.pccomputerguy.com/file/211 [2] https://www.pccomputerguy.com/file/212 [3] https://www.pccomputerguy.com/file/213 [4] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips [5] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Videos