Tech Tip – Microsoft "Support"

If you receive a phone call from a security 'expert' at Microsoft offering to fix your PC - it's a scam. Here's how to avoid the Microsoft phone scam, and what to do if you fear you have fallen victim to it.

How It Works

The scammer calls you, and asks for you by name. They say they are a computer security expert from Microsoft (or another legitimate tech company or a Microsoft 'partner'). The 'security expert' is polite, but aggressive. They say that your PC or laptop has been infected with malware, and that they can help you solve the problem.

Some crooks will ask you to give them remote access to your PC or laptop, and then use that access to get hold of your personal data. Others get you to download a tool, which they say is the "fix" for your problem, but is actually malware.

Hang Up

Important To Know

No legitimate IT security company - certainly not Microsoft - is ever going to call you in this way. They can't even tell that your PC is infected. They have your name from the phone book, or any one of the thousands of marketing lists on which your details probably reside. They know nothing about your home computing set up - they're just chancers.

What to do if you're called

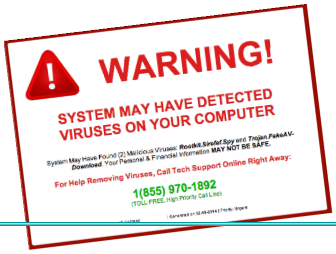
Hang Up

1. Put the phone down. Get rid of the caller and move on with your life. It is not a legitimate call.
2. During your conversation, don't provide any personal information. This is a good rule for any unsolicited call. And certainly never hand over your credit card or bank details.
3. If you've got this far, we can only reiterate point number 1: get off the phone. But whatever you do don't allow a stranger to guide you to a certain webpage, or instruct you to change a setting on your PC or download software
4. Finally, change any passwords and usernames that could possibly have been compromised, and run a scan with up-to-date security software. Then ensure that your firewall and antivirus are up to date and protecting your PC.

If you have been a victim

First of all don't beat yourself up. This could happen to anyone (and does). You need to change all the personal data that you can change. Change all your passwords and usernames, starting with your main email account and any bank and credit card logins. Contact your bank or credit card company if you suspect any financial information was exposed or a fraudulent transaction was done.

Use up-to-date security software to scan and clean your PC, or contact a computer professional to help.



WARNING!

SYSTEM MAY HAVE DETECTED VIRUSES ON YOUR COMPUTER

System May Have Found (2) Malicious Viruses: ***Rootkit.Sirefef.Spy*** and ***Trojan.FakeAV-Download***. Your Personal & Financial Information **MAY NOT BE SAFE.**

For Help Removing Viruses, Call Tech Support Online Right Away:

1(855) 970-1892

(TOLL-FREE, High Priority Call Line)

| Generated on 03-18-2014 | Priority: Urgent

Hang Up