Advice from Middle Aged Female Tech
Hollyecho Montgomery - 812-779-6088
Women's Computer Consulting
http://hollyecho.com

I have been in the industry with my own company since 1994. The entire time I have worked in this field there have been very few times any two techs ever agree completely. The advice I give here is based on my experiences, testing, and what I know works.

Today's Subject: Security alert: Bogus tech-support phone calls

These calls have been a plague on us the American public for now going on 3 years, but, there has been a resurgence. They start out like this**: "Hello. This is Microsoft Tech Support. Your PC has notified us that it has an infection."** Here's how it works and what you need to know to stay out of the trap. Even the **Internet Crime Complaint Center** (a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center) issued a Jan. 7 (http://www.ic3.gov/media/2013/130107.aspx), "New twist to online tech support scam."

This is their report:

"" New Twist to Online Tech Support Scam

The IC3 continues to receive complaints reporting telephone calls from individuals claiming to be with Tech Support from a well-known software company. The callers have very strong accents and use common names such as "Adam" or "Bill." Callers report the user's computer is sending error messages, and a virus has been detected. In order to gain access to the user's computer, the caller claims that only their company can resolve the issue.

The caller convinces the user to grant them the authority to run a program to scan their operating system. Users witness the caller going through their files as the caller claims they are showing how the virus has infected their computer.

Users are told the virus could be removed for a fee and are asked for their credit card details. Those who provide the caller remote access to their computers, whether they paid for the virus to be removed or not, report difficulties with their computer afterwards; either their computers would not turn on or certain programs/files were inaccessible.

Some report taking their computers to local technicians for repair and the technicians confirmed software had been installed. However, no other details were provided.

In a new twist to this scam, it was reported that a user's computer screen turned blue, and eventually black, prior to receiving the call from Tech Support offering to fix their computer. At this time, it has not been determined if this is related to the telephone call or if the user had been experiencing prior computer problems. ""

This puts horrible pressure and undue doubt on legitimate remote support specialists like myself!!! Now, let me inform you (information is power), how to tell a scam call!

1st (and FORMOST) you DID NOT ASK for this call!

2nd Microsoft OR Microsoft partners NEVER EVER call you for ANYTHING, and do not, let me repeat DO NOT ever record, keep, track, or monitor your computer or information.   For you doubters of this, look at it logically -> there are 314 BILLION people in the USA, 293 Thousand of them use Microsoft Products – That is just here in the USA, way too many people to “monitor” infections and personally call you.

3rd If you talk to them and they want to show you how many “infections” you have on your computer, typically they will have you type “.inf” in a search bar (or the search bar just above your start button in windows 7) They, he-and most likely with a heavy accent, will say that ‘.inf’ stands for ***“infected files”*** in windows computers – NO, it these files are INFORMATION txt files for most all windows, Linux, and even MAC computers.

4th They CAN NOT sue you, fine you, or have you arrested for NOT letting them “fix” (steal your hard earned money) your computer.

Cybercriminals often use publicly available phone directories so they might know your name and other personal information when they call you. They might even guess what operating system you're using.

Once they've gained your trust, they might ask for your user name and password or ask you to go to a website to install software that will let them access your computer to fix it. Once you do this, your computer and your personal information is vulnerable.

Do not trust unsolicited calls. Do not provide any personal information.

Here are some of the organizations that cybercriminals claim to be from:

- Windows Helpdesk
- Windows Service Center
- Microsoft Tech Support
- Microsoft Support
- Windows Technical Department Support Group
- Microsoft Research and Development Team (Microsoft R & D Team)

How to protect yourself from telephone tech support scams

If someone claiming to be from Microsoft tech support calls you:

- Do not purchase any software or services.

- Ask if there is a fee or subscription associated with the "service." If there is, hang up.
- Never give control of your computer to a third party unless you can confirm that it is a legitimate representative of a computer support team with whom you are already a customer.
- Take the caller's information down and immediately report it to your local authorities.
- Never provide your credit card or financial information to someone claiming to be from Microsoft tech support.

What to do if you already gave information to a tech support person?

If you think that you might have downloaded malware from a phone tech support scam website or allowed a cybercriminal to access your computer, take these steps:

- Change your computer's password, change the password on your main email account, and change the password for any financial accounts, especially your bank and credit card.
- Scan your computer with the Microsoft Safety Scanner to find out if you have malware installed on your computer.
- Install Microsoft Security Essentials. (Microsoft Security Essentials is a free program. If someone calls you to install this product and then charge you for it, this is also a scam.)

If you ever have any doubts, call a PC tech of your choice, ask for a free evaluation, most of us as legitimate remote specialists will give you a free estimate. You know who you called, where they are located, their name, and even references if you want, business insurance company’s number, anything you ask for upfront. Don’t let the scammers kill your faith in reliable, honorable, legitimate remote computer support techs like myself.

I am always about saving money and not spending it on things you don't need to

Remember ANY questions, email me at: Montgomery@Hollyecho.com. If possible, I will include the answer to your questions in my next article.