# Computer Assistance Scam

by Shawn Mosch of Scam Victims United

January 20, 2012 - Most of us use our computers on a daily basis, and the idea of a virus in our computer is something that no one wants to deal with.  So what if a computer technical support service called you and warned you that they had detected a virus on your computer, and they were able to help you to rid your computer of that virus BEFORE it corrupted all of your files and documents?

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
  var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
  po.src = 'https://apis.google.com/js/plusone.js';
  var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

This is one of the phone scams that is going around right now, and I know about it because they called my house twice this week.  When I answered the phone the person on the other end identified themselves as a Tech Support Specialist from Microsoft.  They knew my name and address, and they told me that they had detected a problem with my computer.  It just seemed strange to me that a company like Microsoft would be calling me to alert me to a virus on my computer, but I listened to what they had to say because I knew it had to be a scam and wanted to get some more information from them.  They wanted me to go to my computer and go to a website and that is when I told them that I knew that there was no problem with my computer.

After hanging up, I jumped on my computer and started doing some Google Research.  I found that this scam has been hitting people in the UK, Australia, South Africa and now it seems to have made it's way to the United States.  Had I stayed on the phone, the phony Tech Support caller would have directed me to look at some files on my computer that would have "proven" that I had the virus that they were calling about.  They would have then directed me to a website where I could download a file that would fix the issue, but what that file really does is allow them access to your computer!  Now they have all of your information!  And to top it off they will ask you to pay them for this service.

Microsoft has information about this scam on their website . . .

Once they have access to your computer, they can do the following:

Trick you into installing malicious software that could capture sensitive data, such as online banking user names and passwords. They might also then charge you to remove this software.

Take control of your computer remotely and adjust settings to leave your computer vulnerable.

Request credit card information so they can bill you for phony services.

Direct you to fraudulent websites and ask you to enter credit card and other personal or financial information there.

Neither Microsoft nor our partners make unsolicited phone calls (also known as cold calls) to charge you for computer security or software fixes.

 As with anything, do your research first.  One intended victim indicated that when they spoke with the phone Tech Support person they indicated that they had 4 computers in their home, and asked which computer had the problem . . . the phony Tech responded that they could turn on any one of their computers to fix this problem.  This was a dead giveaway that it was a scam.

If you have been hit by this scam you should change your passwords, use a trusted malware scanner to remove any unwanted software from your computer and contact your bank and credit card companies.

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS