Telephone Scams

Microsoft Impersonation Scam

snopes
updated From the archive

SHARE 14.3K

Scam: Scammers pretending to be Microsoft techs call victims to gain access to their computers and/or bank accounts.

Example: [Collected on the Internet, August 2009]

I have just received a phone call form someone claiming to be from Microsoft, who says that I have a virus which is sending information from my computer.

It sounds like a bit of a scam, but is there any chance that it could be genuine?

Origins: This Microsoft impersonation scam has been around since at least 2009 and has been run on computer users in numerous countries, including the U.S., Canada, Australia, New Zealand, Ireland, and England. The usual setup is for the scammers to call you and identify themselves as technicians from Microsoft (or some Microsoft-related company), then tell you that your Windows-based computer has a virus (or other problem) that is causing it to generate all sorts of error messages on the Internet and many bad things will happen if you don't correct the issue immediately. And the handy techs who just called you are ready to step in and solve your problem — for a fee, of course.

In short, Microsoft does not contact people out of the blue to tell them there's something wrong with their computers. Ergo, unless you've initiated contact with Microsoft about a computer problem you're having, you should dismiss as frauds any phone calls, e-mails, online chat dialogues, and the like from folks who claim they work for Microsoft and have spotted something wrong with your computer.

The scammers running this type of fraud pretend they're from the software company's technical support department when they telephone to inform householders that their computers have been infected with a virus. Often the scam pitch begins "I'm calling for Microsoft. We've had a report from your internet service provider of serious virus problems from your computer." The caller warns that if the problem is not solved the computer will become unusable and then offers to repair the problem.

The ultimate goal of the fraud varies depending upon which con artists are running it. Some crossroaders set up the confused householders to buy overpriced (and worthless) anti-virus protection. Others, under the guise of selling a solution to the victim's computer virus "problem," go after their pigeons' bank account info, then make hefty withdrawals once they have it. Yet others look to take remote control of the computers belonging to those they dupe. The last of these appears to be the most common form of the scam; in that iteration, con artists direct their intended victims to access a particular website and download a program from it. By doing so, those users enable remote access to their computers.

These scammers are known for being tenacious. I once received a call from one such scammer, and even after I identified myself, informed the caller that I knew he was running a scam, pointed out that I write about scams like these for a living, threatened to call the FTC and report him, and told him I knew he was lying because I had no Windows-based PC at home, he still wouldn't give up on trying to sell me his "service" or acknowledge he was a scammer.

Microsoft says about this fraud that:

> Microsoft does not make unsolicited phone calls to help you fix your computer
>
> In this scam cybercriminals call you and claim to be from Microsoft Tech Support. They offer to help solve your computer problems. Once the crooks have gained your trust, they attempt to steal from you and

damage your computer with malware including viruses and spyware.

Although law enforcement can trace phone numbers, perpetrators often use pay phones, disposable cellular phones, or stolen cellular phone numbers. It's better to avoid being conned rather than try to repair damage afterwards.

Treat all unsolicited phone calls with skepticism. Do not provide any personal information.

If you receive an unsolicited call from someone claiming to be from Microsoft Tech Support, hang up. We do not make these kinds of calls.

In August 2010, Microsoft Australia issued a press release about the scam:

Microsoft today warned Australians to be wary of a phone scam that has left some victims hundreds of dollars out of pocket.

Scammers are using several well-known brands, including Microsoft, to fool people into believing that something is wrong with their computers. The scam typically unfolds in the following manner:

- A cold caller, claiming to be a representative of Microsoft, one of its brands or a third party contracted by Microsoft, tells the victim they are checking into a computer problem, infection or virus that has been detected by Microsoft.
- They tell the victim they can help and direct them to a website that then allows the scammers to take remote control of the computer.
- The cold caller will then spend some time on the computer trying to demonstrate where the 'problems' are and in the process convinces the victim to pay a fee for a service that will fix the computer.

"In reality, there is nothing wrong with their computer but the scammer has tricked the consumer into believing there is a problem and that paying the fee is the best way to get it fixed. Often they will also push the customer to buy a one year computer maintenance subscription. They are just trying to scam innocent Australians out of money," said Stuart Strathdee, Microsoft Australia's chief security advisor.

Strathdee also said that the callers presented themselves in a professional manner and sounded genuine.

"Don't be fooled, Microsoft is not cold calling consumers in regards to malfunctioning PCs, viruses or any other matter," he said.

"We strongly advise Australians to simply hang up if they receive a call of this nature and not to respond to any communications from these scammers."

"If you're not sure, contact Microsoft on 13 20 58 or the Police," he said.

Barbara "call centered" Mikkelson

Last updated: 18 July 2014

Sources:

CBC News. "Phone Scam Warns of Microsoft Virus."
8 December 2010.

East Kent Mercury. "Warning Over Computer Virus Phone Call Scam."
6 January 2011.

Irish Examiner. "Public Urged to Be Aware of Microsoft 'Cyberscam.'"
14 December 2010.

[Victoria] Times Colonist. "BBB Warns of Microsoft Scam."
19 January 2011 (p. B4).