

Microsoft Scam



A newsletter reader reported several of his customers have been victims of the Microsoft Scam recently and wanted to spread the word about this scam.

The Microsoft impersonation scam has been around since at least 2009 and has been used 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. They describe all the things that will happen if you don't correct the issue immediately. The handy techs who just called you are ready to step in and solve your problem —and give you many more!

Microsoft does not contact people out of the blue to tell them there's something wrong with their 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 scammers set up the victim to buy overpriced (and worthless) anti-virus protection. Others, under the guise of selling a solution to the victim's computer virus obtain bank account info, then make hefty withdrawals once they have it. Yet others look to take remote control of the computers belonging to the victim. **The best course of action is to hang up the phone!**