Fraudulent Telephone Call: Computer Virus

This scam works because many people understand that computer viruses exist, but do not understand how to prevent or repair from a computer virus.

The scam goes like this: The victim gets a telephone call from a person "who works for Microsoft" and tells the victim that his/her "computer has a virus." In order to "fix the problem" the victim is told to "pay a fee/service charge" by giving his/her "credit card/bank account information." The victim will then get "an email from Microsoft with a link to remove the virus" or similar directions.

What Really Happens: The victim either pays for something that they do not get, or in the worst case has their credit card information or bank account information stolen and the funds raided.

Sometimes the "Microsoft employee" may tell the victim that "I need to take remote control of your computer to fix the virus." The victim may be told that "there is no charge for this."

What Really Happens: The "employee" installs software to capture key strokes made when the computer is used, thereby gaining access to all of the victim's user names and passwords for online banking and credit card transactions. In some cases, the installed software also gives the "employee" access to all of the information on the victim's computer, including personal identifying information as well as online banking and credit card information.

How To Protect Yourself: Recognize that these types of calls are attempts to defraud you. Understand that Microsoft, AVG, Norton Anti-virus, etc., do not call to tell you that you have a computer virus. Do not let anyone have remote access to your computer. Do not make payment to "repair your computer" when someone calls you.