Jay Trent
Your friendly neighborhood IT Guy!

I just had a call from one of my users at the office who told me they were contacted by a company to be acting on behalf of Microsoft and that their computer was infested with viruses and that they were instructed to help.

The caller had my user do something in the DOS prompt, from what I gather it was just to do a dir listing to make it look as if those files were infected.

They then wanted him to download a remote access client from ammyy.com and this is where he became suspicious and said he did not have time and would have to call back.

The company acting on behalf of Microsoft gave my user a bogus 800 number and an MS employee id.

They're using social engineering techniques to scare people and then gain access to the user's pc and network. I can see a lot of vulnerable people being caught by this. This technique of social engineering is a technique I myself have practiced for years to help others protect themselves from scammers. I can go on, on how easy it is for me to talk to a user for less than 5 minutes and be able to gain full access to the user's pc. This is a serious problem and most corporate networks are hacked and destroyed by social engineering.

Beware that this scam is out there and if you have friends or family who may not be completely technically savvy it may bite them in the rear.

Remember:

1. Anyone can dial a number and claim to be someone else;
2. The real Microsoft doesn't call their customers to report virus infections;
3. Never run any unknown program or install any remote access tool for someone unless you are 100% certain of their identity and trustworthiness.
4. Never give out your password
5. Never use passwords that are in the dictionary… password, god, love, money
6. Use upper and lower case letters, number and special characters… 1mL337, p@s5w0Rd!