Tech Support Scams

Much as most of us like to think we're smart enough not fall for a scam, millions of people are conned every year into giving access to their PCs to tech support imposters. These are the people who claim to be from Microsoft or another computer firm. They tell you they've detected a virus on your PC and need to be given remote access to put it right.

You probably know what "remote access" is, but for those who don't, it's a feature of Windows that enables someone in another location to access your PC via the Internet. But you have to give them permission via your PC first, which is why these scammers make their spoof calls. Once they get access, they can digitally crawl all over your PC, looking for confidential information like passwords and account numbers. And after they're done, they may leave a piece of malware on your PC that enables them to access it at any time or plug it into a botnet — a network of compromised computers that are forced to send out spam.

According to Microsoft's Digital Crime Unit, some 3.3 million people fall victim to the tech support scam every year, costing victims around $1.5 billion.

Once you realize what's happened, you need to take immediate action to minimize the potential damage.

Here's our 10-point plan to deal with it:

1. Shut down and disconnect the affected device/PC from the Internet. That puts an absolute stop on any external meddling. It also often automatically revokes remote access for when you restart.
2. Ideally, you should have a full system backup that would enable you to restore your computer to its previous state, ensuring the scammers no longer have access to your machine. (If you don't know how to back up your system, just do a Google search on your Internet browser – but be careful that you visit a legitimate site).
3. If you don't have a backup, run the Windows "System Restore" feature to remove any unwanted apps. Visit Microsoft Support to learn how to do this.
4. Whether you restored your system or not, ensure your Internet security software is up to date and run a FULL virus scan to remove any lingering malware.
5. If you know how to do it, check your web browser's settings for any newly installed extensions or add-ons you don't recognize and delete them.
6. If you don't know how to do this or you're still not certain your machine is "clean," have it professionally checked.
7. Only when you've done all this should you change all passwords. Yes, all passwords on every account you access via your PC.
8. Alert your bank and credit card companies and monitor all statements online every day, looking for suspicious items.
9. Put a freeze on credit applications via the three credit monitoring agencies — Equifax, Experian and TransUnion. This will cost a few dollars but is worth it. Each of the bureaus has its own "credit lock" service.
10. File a complaint with the Federal Trade Commission (FTC).