“This is Microsoft Support” ***Really?***

A trend of the past couple of years has been for scammers to contact computer owners *directly via telephone* in the United States in an effort to convince them that there is a problem with their PC and they'll need to pay to have it fixed. In general, these people cannot fix anything, and instead they merely charge exorbitant fees for absolutely nothing. In other words, they scam you.

The call generally goes something like this:

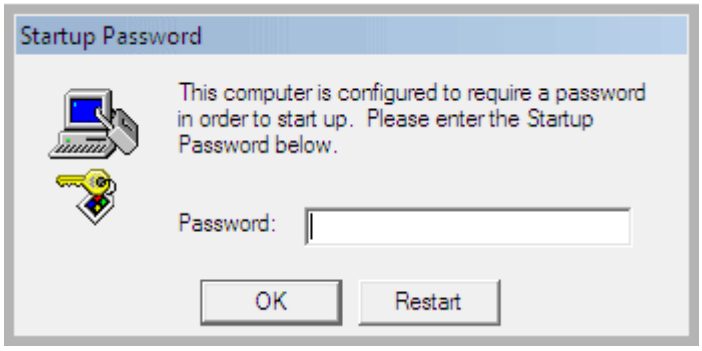
1. A foreigner with a thick Indian accent identifies himself as a member of Microsoft Support or similar.
2. He informs you that you have a number of critical problems with your PC and that you will need to have it fixed.
3. To convince you, he offers to connect remotely and pulls up your Event Log (eventvwr.msc). He then filters for Warnings, Errors, and Critical events and uses that as evidence that your PC will soon fail to work correctly if you do not pay him to correct it.

The astute among you have probably already sensed that something here is seriously wrong, and it's not your PC. It's the fact that someone is *calling you* to tell you there is a problem with your computer. **No one will ever do that. The only way they could possibly know there is a problem is by hacking or guessing.**

In this case, it's mere guesswork, and it's not even correct most of the time. The Event Log is *supposed* to log warnings and errors, and even on the healthiest of PCs there are plenty of Error Events that can be safely ignored, as they often don't amount to anything. The important thing to remember is to **never trust someone** who calls you about a problem with your PC, and **never, EVER** let them connect remotely to your PC.

If you ***do*** make the mistake of letting them connect, but then you happen to get cold feet and refuse to pay the $180+ they request via credit card, the next thing that happens isn't pretty. This scammer proceeded to actually follow through on his promise of the PC “not working” if they don't agree to have him fix it, and so in a few quick steps, behind the user's back, he enacted what is known as SysKey encryption on the SAM registry hive.

SysKey encryption is a little-known feature of Windows which allows administrators to lock out access to the Security Accounts Manager (SAM) registry hive so that login specifics cannot be stolen and the PC cannot be accessed without knowing the proper credentials. The problem is, unlike other scams, there is no way around the problem; you can't simply remove the password, as the actual SAM hive has been encrypted entirely by the process. If your Windows installation has had SysKey activated, you'll see the following message:



The ONLY solution is to find a clean copy of the registry hives from before this occurred. This scammer knew this, however, and as such, he took an extra step to block any repair or recovery attempts: he **deleted all System Restore points on the machine**, which normally house backup copies of the registry hives.

All you can do now is reformat the computer with a complete loss of all your files that haven't been backed up.

Originally Posted on **April 10, 2013** by **Steve Schardein**

Webspinner Computers
604-217-0302
Webspinner@me.com