

Re: System Recovery?

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2007-05/msg07488.html>

- *From:* pikespeak <pikespeaklosangeles@xxxxxxxxxx>
 - *Date:* Mon, 28 May 2007 02:13:00 -0700
-

First of all, Rock:

Thank you for the stern advice.

You are absolutely correct. I should have never put myself in such a position.

I am more surprised than you were when I saw all the files here. It was really strange. Everything is here.

There wasn't court documents or anything, just music, pictures, and my website links. Nothing dire.

When I upgraded my Norton—and I did a final scan about 12 hours ago, you wouldn't believe what I found: 3 Trojan Horse, 2 W32 Beagles, and 8 other worms and viruses. It was like a roach infestation.

I will do as I'm advised and get make a report.

Thank you for all your advice, Rock.

And to you too, Andrew.

Regards,
Marcus

"Rock" wrote:

"pikespeak" wrote

Hello,
Hopefully I am succinct, and clear on what I am about to say.

Today, my system crashed, or I thought it did. I tried to boot my computer in safe mode, because I wanted to remove a virus and reinstall Norton Anti-Virus. Apparently, the worm or trojan disables Norton and renders it unusable. On the Symantec website, I was told I had to

Re: System Recovery?

reboot in safe mode and turn off system restore until I removed the virus with a removal tool provided by their website.

But when I tried to reboot, it didn't work, it wouldn't even let me go into windows. The computer informed me, in a command prompt setting, to either boot normally or go to last workable configuration. But Windows wouldn't boot—AT ALL. Nor would it let me go into safe mode—NOTHING.

I went ahead and did a system recovery by pressing F10 before I boot. I was informed that all my files would be deleted...especially since I couldn't get into windows and I turned system restore off. Before I rebooted. :(

The system restore worked and was able to get back into windows and I thought everything was gone—all 50+GB of files and data...apparently not. Most of the stuff is still here. I think all of it is. Even the amount of space available is still the same number as before the system recovery. I had two separate user profiles, and there is a folder with my name

on it, but it says: "C:\Documents and Settings\ Marcus Young is not accessible. Access is denied." I did a Norton Scan and I can see the names of my files in that folder, that I cannot access. I see my favourites and everything, plus it's still taking up the 30GB of memory as it did before recovery. Those are my files. When I tried to set up another profile to log in—I typed in my name and the icon that I had put in there 2 months ago automatically came up.

Everything else is here and accessible—even my Emule programme and the files I downloaded from that software that very morning.

How can I access my folder: Marcus Young? All my projects are in there.

You need to take ownership of the files and folders. See this link.

HOW TO: Take Ownership of a File or Folder in Windows XP

<http://support.microsoft.com/?id=308421>

At this point you are lucky. Normally a system recovery with an OEM recovery process is a destructive one, and all data/programs are lost. It even cautioned you about this, so it's surprising you can still see files. Might be a good time to read up on exactly how the recovery process works for your system

More importantly though, if the data is so important, why don't you have a backup? You suffered a malware problem but there are any number of things that can happen which lead to data loss. For example what if the hard drive died?

Always have a full and complete backup of important data. This should be on

Re: System Recovery?

media external to the system. A 3 1/2 inch hard drive in an external hard drive enclosure connected by USB, Firewire or eSata is a low cost backup medium.

There are a variety of tools for backup. I suggest you get a drive imaging program such as Acronis True Image Home, version 10 to image the drive(s) to his external hard drive.

You should never have to face permanent data loss.

—

Rock [MS-MVP User/Shell]