

I'm pretty sure that my computer has a virus, what...

My computer has been compromised, what do I do?¹

If you are not a computer expert, you should probably consult with one as soon as possible. The reason for this advice is that we believe that a compromised system can **not** be patched. [If you really think that you are up to the task, please read [this](#) first.] Therefore, the quickest and easiest way to secure a compromised system is by taking drastic measures. Measures which are much more easily understood and performed by a computer expert. Think of it like this: when your car breaks down, do you try to fix it yourself? or do you take it to a mechanic.

The steps:

- Disconnect the computer from the internet as soon as possible.
- Backup or image the computer's hard drive (so as to recover the important data later).
- Perform a clean install of Windows - a format of the drive **should** be completed.
- Immediately update that installation with all of the latest patches.
- Use the latest anti-spyware, anti-virus, and event rootkit detection to scan and clean any data that you want to recover from the backups.

To keep your computer from being compromised, you should take a layered approach to security:

- Firewall software
- Intrusion detection / prevention software
- Anti-virus software
- Anti-spyware software
- Anti-spam software

You should keep your computer up to date with the latest patches - Automatic Updates for Windows can be set to download and install all critical patches. You should also consider disabling the Administrator account, as most malware takes advantage of the full access to the system which the administrator account provides.

Again, our rationale behind these steps and ideas are due to evidence and experience that a compromised system cannot be patched. Microsoft's Security Program Manager expressed it quite well [here](#).

From Business UX's experience, there is no one security vendor can provide 100% protection against virus's, spyware and spam. Computers can still be compromised even with the latest security software.

¹ From the ClamWin Free Anti-virus website <http://www.clamwin.com/>