Basic Spyware Scanning and Troubleshooting

Computers are complicated enough that they don't always do precisely what we expect. Sometimes an unexpected behavior is just a fluke; other times, it's an outward and visible sign of an inward and terrible malware infestation. If you notice any of the security warning signs below your system may well be compromised.

1. **Popup ads appear even when no browser is open.** While not as common as they used to be, adware programs bombard their victims with advertisements. Sometimes they're ads for legitimate products; other times they contain links to malicious websites, sites that will attempt to drop more malware on your PC.

2. **Browser navigation gets redirected.** Not every site redirect is malicious, but if you find that trying to reach Google takes you to an unfamiliar search site, you've almost certainly got a problem. Sometimes the redirection is more subtle. For example, a banking Trojan might divert your browser to a fraudulent site that looks just like your bank's real site. In that case your only clue is the unfamiliar URL in the Address bar.

3. **A security program you never installed pops up scary warnings.** Creating and distributing fake antivirus programs is a lucrative business. The perpetrators use drive-by downloads or other sneaky techniques to get the fake antivirus onto your system, then display scary warnings about made-up threats. Naturally you have to register a payment before the fraudulent tool will "fix" the problem. And of course scanning for malware with the fake AV is super-fast, since it's not actually doing anything.

4. **Posts you didn't write appear on your social media pages.** Malware focused on Facebook and other social media sites propagates by generating fake posts. Typically these posts include an inflammatory statement of some kind, like "OMG were you really that drunk? Look at this picture!" Anyone who falls for the fake and clicks the link will become the next victim.

5. **A program holds your PC for ransom.** Some malware programs literally hold your PC or data for ransom. Overt threats may encrypt all your pictures and documents and demand that you pay to get them back. Others try to obscure what they're doing. For example, they may display a warning supposedly from the FBI stating that your computer was used to send spam and demanding that you pay a fine before you're allowed to use it again. Of course, even if you do pay, you may not get your system back.

6. **Suddenly you can't use common system tools.** A smart user, suspecting the presence of malware, might launch Task Manager to investigate, or check settings using Registry Editor. If you suddenly find that trying to use these or other system tools triggers a message saying your Administrator has disabled them, it may well be an attempt at self-defense by malware on your system.
7. Everything seems perfectly normal. That's right. Some types of malware do their best to hide all activity, leaving no visible traces. Even when you don’t notice anything unusual, it's possible that a 'bot on your system may be quietly awaiting instruction from its command and control system, or a Remote Access Trojan may be harvesting your personal information.

If you think that malware has taken up residence in your PC, install a powerful antivirus utility or security suite immediately. Already got one? Then apparently the malware got past its protection. Make sure your antivirus is fully up to date, and run a full scan. Also get a second opinion from a free cleanup-only antivirus like Malwarebytes or Spybot. You definitely want to get that nasty, malicious program out of your system as soon as possible, before it invites "friends" to make your security problem even worse. (Reprinted from PC Magazine online article http://www.pcmag.com/article2/0,2817,2416788,00.asp)

Below are instructions for installation of the spyware programs Spybot, Malwarebytes, and many more. If you have issues after downloading, installing, updating, and running the spyware applications contact the helpdesk with your questions or concerns. To start killing that pesky spyware please follow the directions below.

I. Map a network drive to \sh-csrv1\guest and browse through the folders as follows:

   a. Utilities -> Spyware detector and you will find 3 folders called Boot-up Cleaning Tools, Rootkit Cleaners, and Spyware

   b. Install the applications from the different folders depending on your needs. During the installation, follow the on screen prompts and accept all defaults.

   c. Always make sure to first update the programs first before running them. All of these software applications can be accessed using VPN or your work computer.

II. If you need additional assistance email shvservicedesk@lsuhsc.edu or call the helpdesk at (318) 675-5470. Please include a specific description of the problem, your contact information, and computer name.