

Cleaning and Securing Your Windows PC

This document is designed for multiple scenarios including situations where network access is unavailable. Due to the difficulties in keeping a distribution CD current and issues involving software licensing, ITS cannot distribute CDs. If network access is unavailable on your computer, use a friend's computer or a lab computer to download the necessary tools discussed in this document and burn them onto a CD. If you use a lab computer, consult Windows XP's built-in help system for information on how to burn a CD.

If you do not have a network connection, start here; if you have a network connection proceed to Step 1.

If you have to use a friend's computer or a lab computer, start by collecting all of the necessary tools and burn them onto a CD.

- 1) Create a folder on the desktop and label it "Removal Tools"
- 2) Download the following tools and place them in the "Removal Tools" folder.
 - a) Stinger virus removal tool: <http://us.mcafee.com/virusInfo/default.asp?id=stinger>
 - b) Spybot S&D: <http://www.safer-networking.org/en/download/index.html>
 - c) Spybot Detection List: <http://www.safer-networking.org/en/download/index.html>
- 3) Burn the "Removal Tools" folder to a CD for use on the infected computer

Step 1: Activate Firewall Software

Windows XP has a built-in firewall. For information on how to activate it, use the Windows XP help system located in the Start menu. Prior versions of Windows do not have a built-in firewall. This is not an issue for Windows 9x and ME users who can skip this step; however, if you use Windows 2000 it is an issue and you will need to contact the Help Desk.

Note: If you use the Windows XP firewall without having Service Pack 2 installed or you use a third party firewall, you will not be able to access network file servers. This problem can be solved by installing Service Pack 2 on XP and by disabling third party firewalls. **DO NOT** turn off the firewall until all critical Windows Updates are installed on your computer or your computer will quickly become reinfected. For information about updating Windows, follow the link in Step 4.

Step 2: Remove the Malicious Software

In most cases an infected computer has multiple infections involving viruses, worms and spyware. To clear the malicious software from your computer you need to use a stand-alone virus removal tool and a spyware removal tool.

Stand-alone Virus Removal Tool

If you have not already done so, download and install a stand-alone virus removal tool and perform a scan with it. McAfee provides a comprehensive stand-alone virus removal tool, free of charge, called Stinger that is capable of removing many common viruses and worms. Stinger is very intuitive and easy to use. Current versions of Stinger and information on using it are available at: <http://us.mcafee.com/virusInfo/default.asp?id=stinger>

Spyware Removal Tool

If you have not already done so download and install a spyware removal program and perform a scan with it.

A highly rated spyware remover is Spybot Search and Destroy and it is available free of charge at:

<http://www.safer-networking.org/en/download/index.html>

Important: Spyware removers will only work correctly if they have a current detection list.

If you have a network connection, after installing Spybot, click on the "Update" link to get the latest detection list.

Then begin the scan. If you do not have a network connection, you will need to install the current detection list. If you have not already downloaded the detection list it is available at: <http://www.safer-networking.org/en/download/index.html>

Before installing the current detection list, you must first install Spybot. After the detection list is installed begin the scan.

Step 3: Get Back on the Network if You Were Black Holed

If your computer was removed from the network (Black Holed), call the Help Desk at x6500 and indicate you have cleared the viruses and/or spyware from your computer. If your computer is not properly cleaned and secured, it will become infected again in a short amount of time.

Step 4: Secure Your Computer to Prevent Reinfection.

Learn how to prevent future infections and/or to get antivirus software, visit:

<http://helpdesk.its.bethel.edu/students/security/security.jsp>

Taking some time to learn about prevention now will pay off greatly in the future in immeasurable ways.