# 2- GENERIC REACTIVE PROCEDURE FOR RESOLVING A MALWARE INFECTION IN A "WINDOWS.." COMPUTER

by Francis Chao
fchao2@yahoo.com

# Web location for this presentation:

http://aztcs.apcug.org

Click on

"Meeting Notes"

# SUMMARY

Here is a tried-and-trusted generic procedure for removing malware from a "Windows.." computer

# GENERIC PROCEDURE FOR REMOVING MALWARE INFECTIONS IN "WINDOWS.."

- BIG STEP 100:

  Use a camera or your cell phone to take a photo of the monitor screen in your computer.
  (Later on, you can use this photo in a search engine to gain insights about the type and name of malware that your computer was infected with.)

# GENERIC PROCEDURE FOR REMOVING MALWARE INFECTIONS IN "WINDOWS.."

- BIG STEP 200:

  **If your mouse cursor does not move OR your keyboard is not working (try pressing Ctrl + Shift + Esc), then press down on the Power button of your computer until the computer turns off;** wait 30 seconds and make sure that the fans of the computer have stopped spinning; then turn the computer back on.

# GENERIC PROCEDURE FOR REMOVING MALWARE INFECTIONS IN "WINDOWS.."

- BIG STEP 300:

  Disconnect the network connection of the computer.

# GENERIC PROCEDURE FOR REMOVING MALWARE INFECTIONS IN "WINDOWS.."

- BIG STEP 400:
  Power the computer back up.

# GENERIC PROCEDURE FOR REMOVING MALWARE INFECTIONS IN "WINDOWS.."

- BIG STEP 500:
  Run a "Quick Scan" with "Windows Security" or any other antivirus program that is installed in your computer

# GENERIC PROCEDURE FOR REMOVING MALWARE INFECTIONS IN "WINDOWS.." (continued)

- BIG STEP 600:
  Use the bundled "Task Manager" to see if the malware "task" can be identified:
  If you see anything that is suspicious, try to close it with a right-click.
  If it closes successfully, reboot the computer.
  If it resumes itself, use another computer to search "Google", "Bing", or "duckduckgo" for advice.

# GENERIC PROCEDURE FOR REMOVING MALWARE INFECTIONS IN "WINDOWS.." (continued)

- BIG STEP 700:
  Use "Revo Uninstaller Portable" to remove any possibly infected "apps".
  (See https://aztcs.apcug.org/meeting_notes/winhardsig/uninstaller/RevoUninstallerPortable.pdf )

# GENERIC PROCEDURE FOR REMOVING MALWARE INFECTIONS IN "WINDOWS.." (continued)

- BIG STEP 800 (continued):
  If "Revo Uninstaller Portable" is used to remove a possibly infected "app", reboot the computer to see if the malware problem is still there.

# GENERIC PROCEDURE FOR REMOVING MALWARE INFECTIONS IN "WINDOWS.." (continued)

- BIG STEP 900:
  If the problem no longer exists, reconnect the computer to the network.

# GENERIC PROCEDURE FOR REMOVING MALWARE INFECTIONS IN "WINDOWS.." (continued)

- BIG STEP 1000:
  Power up the computer.

# GENERIC PROCEDURE FOR REMOVING MALWARE INFECTIONS IN "WINDOWS.." (continued)

- BIG STEP 1100:
  Then use the "Microsoft Store" or the Web sites of software providers to re-install the apps that you removed in "BIG STEP 700"