Tech Training: Malware

Below are links to our client tutorials covering malware and its removal. We provide more specific malware help than just recommending removal programs. There is a malware removal checklist that we run through each time a client comes in with malware.

This checklist lists different steps depending on whether the computer is Windows or Mac, and if it is personally-owned or Taylor-owned. Often you will have to start the malware removal process and then pass it on to the next worker, or have to pick up in the middle of the malware removal process. So initial each completed step on the checklist so we know each step has been completed.

The general malware removal programs that we run are: Endpoint Protection, Malwarebytes, Super AntiSpyware, and various AV programs for Mac. Due to licensing restrictions, Endpoint Protection is only run on Taylor owned PCs, Super AntiSpyware is never run on Taylor owned PCs, and Taylor owns 2 Malwarebytes licenses. This is why Malwarebytes always has to be uninstalled from Taylor owned PCs after use. Specific notes about these programs are found on the Malware Removal Checklist.

Always start at the top of the checklist and work down. And make sure that you are using the correct column for the client's computer. Only initial a step once that step is complete.

The tutorials listed below provide definitions for the various types of malware along with malware prevention, detection, and removal instructions.

Malware & SPAM Intro: http://4040.taylor.edu/Tutorials/Malware/MalwareIntro.pdf
Malware Removal (Win): http://4040.taylor.edu/Tutorials/Malware/MalwareRemoval_Win.pdf
Malware Removal (Mac): http://4040.taylor.edu/tutorials/Malware/MalwareRemoval_Mac.pdf
HijackThis Tutorial: http://4040.taylor.edu/tutorials/techtraining/tt_hijackthis.pdf
Anti-Malware vs. Anti-virus: https://www.youtube.com/watch?v=67-5bzc_GKE

At IT's request, we attempts to reduce the risk of spreading malware by reducing the amount of time an infected device is connected to TUCAN. Steps:

1. Disconnect device from TUCAN
2. Gather tools required for malware removal process using a CS computer
    - CCleaner installer from https://www.piriform.com/ccleaner/download
    - Malwarebytes installer from https://www.malwarebytes.com/mwb-download/
    - Malwarebytes updater from http://www.majorgeeks.com/mg/get/malwarebytes_anti_malware_database,1.html
3. Transfer tools to client device via USB drive
4. Install CCleaner, and install/update Malwarebytes
5. Complete malware removal process with device disconnected from TUCAN
6. Connect device, and test

Notes:
SuperAntiSpyware installer is available at http://www.superantispyware.com/superantispywarefreevspro.html. Updating Super requires internet access. At this writing, there is no manual update process. If the infection is severe and you feel you need to run Super, temporarily connect to TUCAN in order to update Super. Then disconnect.

If a client device will not recognize your USB drive, a cache of tools is available at http://4040.taylor.edu/utilities-all.aspx?folder=ThumbDriveUtilities. However, these copies may be out of date. If so, update them manually, and then copy to USB drive.