General

Compromised Systems - Policies and procedures for handling malware on campus.

The following document pertains to computers which have been identified by the network team as being compromised and/or infected with malware.

First steps:

If you have discovered your computer is infected, immediately disconnect it from all networks to prevent it spreading from device to device. Secondly, ensure you have changed your passwords for online accounts on a separate device such as a mobile phone or lab computer. If the device is infected and you attempt to update your password on it, they have the ability to get the new password.

For student and personally-owned PCs:

The PC will be disabled from network access if we detect malicious activity until it has been formatted/reloaded. Once this has been done, please bring proof to the Technology Support Center. They can determine the Operating System install date to verify the system has been reloaded.

For university-owned PCs:

The PC will also be disabled from the network until the Virus has been removed. The system can be brought into Tech Support so we can attempt to remove the virus. If we are unsuccessful, we will be required to format the system and reload it. In case of this, we can back up all the necessary data if possible. We can also reinstall most University Software that was previously on the system. If you think your system is infected, please call the Technology Support Center at (321) 674-7284.

Unique solution ID: #1099
Author: Tech Support
Last update: 2020-04-09 10:16