Your computer has been infected with malware, now what?

The following software packages will help you remove the unwanted software from your computer. Most of the free versions of this software are limited however and you may want to pay for the added protection if you continue to become infected.

- Malwarebytes is a great malware removal tool, but the free version does not provide active protection. It can be found at https://www.malwarebytes.org/.
- SUPERAntiSpyware is an antivirus suite. This program provides active protection as well as malware removal. Find this program at http://www.superantispyware.com/.
- avast! Antivirus has consistently been one of the best performing free antivirus software suites. It is available for PC, Mac, and your smartphone, provides active protection and malware removal. Go to http://www.avast.com/en-us/index to get your copy today.

The most common ways for computers to become infected are from:

- Opening email attachments which contain malware
- Downloading files off of the internet
- Visiting a malicious website or
- Clicking on malicious advertisements displayed on websites

These tips can help prevent malware from infecting your machine:

- Run Anti-Virus and keep it up to date
- Update your computer's operating system regularly.
  - The second Tuesday of every month is referred to as "Patch Tuesday" because that is when software vendors like Apple and Microsoft release updates for their software
- Regularly update important applications such as:
  - Your web browser of choice
  - Adobe Flash
  - Java
- Be careful where you click! Many reputable sites have been known to host malware in their banner advertisements
  - Adblock Plus can be found at https://adblockplus.org/ and is a great way to block those pesky ads that might contain malware
- Think before you act; communications and pop-ups imploring you to act immediately or that sound too good to be true are most likely malicious
- Delete suspicious emails, tweets, posts and other suspicious digital communications
  - These communications are counting on you to make a mistake!
  - Look for misspelled words, links, or threats
  - These communications often look like they are sent from a legitimate source
- Be wary of unprotected Wi-Fi connections; information sent over unsecured wireless networks is visible to everyone!

If you have any questions you may contact the Student Technology Help Desk by email at sth@csusm.edu or by phone at (760) 750-6505.