

MEMORANDUM

TO: All Locations

FROM: Information Technology Services (ITS)

SUBJECT: **** CRITICAL ** VIRUS/WORM THREAT**

ITS has identified the presence of a "replicating virus/worm" threat that is appearing within the school site networks on the MDCPS Network. This worm/virus is a member of the "sober" virus family. The effect of this worm is massive e-mails being transmitted to network users. The worm uses different subjects and the sender information will vary. The message may appear to come from someone you know when in fact that person has not sent the message. These messages may come with an attachment. These attachments are being cleaned by the District's antivirus software. If you receive one of these messages, **delete** the message without opening the attachment or clicking on any links contained in the message.

To prevent your site from becoming infected, it is critical that the steps below are followed:

1. Keep ALL site computers turned on 24/7.
2. Set all computers to "automatically update" Microsoft Operating System patches.
3. Insure that **ALL** computers have McAfee EPO client software installed and functioning.
4. Insure that Big Fix is installed on all computers.

All locations are reminded that it is the responsibility of each user to update their VirusScan software. Each user should set their VirusScan software to update DAT files on a weekly basis. Instructions for scheduling the Virus Scan software to update automatically are available from the following website:

<http://its.dadeschools.net/virus.htm>

If you do not have McAfee installed on your computer, information for obtaining the District's free McAfee Antivirus software is available at the following website:

<http://datasecurity.dadeschools.net/>

If you have any questions regarding this memo, please call Support Services at 305-995-3705.