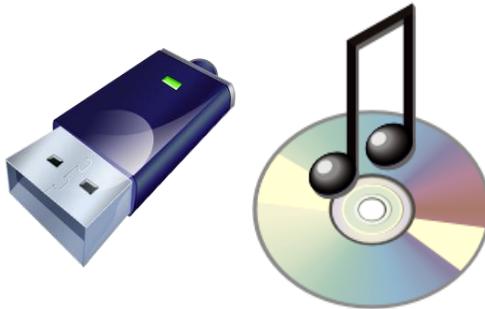


Security Awareness Message

Removable Media



Recently there was an active malware outbreak at multiple sites on the Chief Information Officer/Office for Technology's (CIO/ OFT) Human Services Enterprise Network (HSEN). This malware attempts to make changes to the infected workstation's operating system. Since most OCFS and Local District workstations store or transmit confidential information, the affected workstations required re-imaging.

OFT analysis indicated that this outbreak was most likely introduced through a removable media device, such as a USB flash drive.

REMINDER: Users must not place ANY personal removable media into a USB port, CD drive, DVD drive or in any other port on a state-owned workstation, laptop or other device. Only State issued removable media devices should be used on State-owned assets. State issued removable media should not be used on personal equipment. Users are also reminded not to upload or store any non-work related music, video, or digital images on state-owned workstations, laptops, other devices, or networked servers.