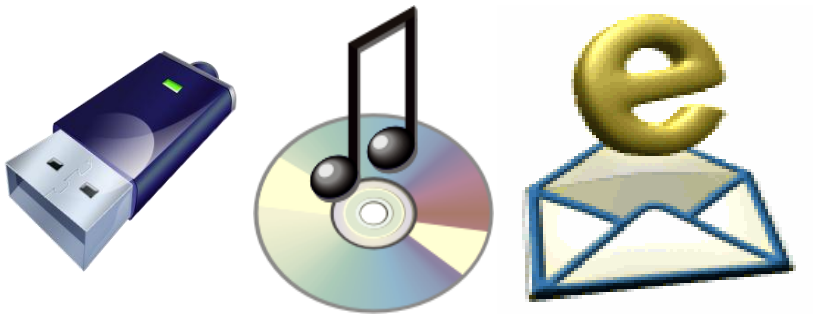
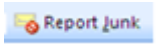
Security Awareness Message

Removable Media, Malware and Phishing Scams



Help prevent a malware outbreak on the Human Services Enterprise Network (HSEN). Malware attempts to make changes to the infected workstation's operating system. Since most OCFS and Local District and Voluntary Agency workstations store or transmit confidential information, when machines are affected, workstations require re-imaging.

Malware is most likely introduced through a removable media device, such as a USB flash drive **or** through a phishing scam designed to get a user to click on a link.

Never open a suspicious email or click on a suspicious link. Do not give out personal information or log-on and password! Report spam by using the 

report junk icon on your toolbar.

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.