To: UMass Dartmouth Faculty and Staff

From: Donna R. Massano, CIO & Associate Vice Chancellor for Information Technology

Re: Important Virus Alert - CryptoLocker Ransomware

CryptoLocker is the generic name for an increasingly prevalent and nasty strain of malicious software (malware) that encrypts all the files on your computer, any connected external hard drives or flash drives and even your online accounts like Dropbox. Remember to store important business files on your UMass Dartmouth U: drive share to ensure that they are protected from this type of damage.

According to reports from security firms, CryptoLocker is most often spread through email attachments, but the malware also can be deployed by hacked and malicious web sites by exploiting outdated browser plugins. Currently, there are no anti-virus programs that detect this malware prior to its activation.

CITS has implemented a number of security measures including blocking .exe, .zip, and .bat attachments. Should you need to send or receive an attachment of this nature, please contact the IT Service Center at 508-999-8790 or via email at ITSCenter@umassd.edu.

It is also important to remember that files like this can be sent to your personal email accounts, so NEVER open an attachment that you are not expecting.

Additionally, CITS is pleased to offer Sophos Anti-Virus protection for faculty and staff to install on their personal computers. Although it won't currently protect you from Cryptolocker, we are hopeful that Sophos will soon find a resolution to this problem. Sophos will help protect you from other viruses, spyware, and malware.

You can access the download by logging into the Portal and selecting "Downloads" from Campus Tools. Once you log in with your UMassD logon, you will have access to any software provided by CITS for your use. Please select and install the version of Sophos that is appropriate for your computer.

You can learn more about how to avoid this threat from a ComputerWorld article which has been linked from the UMass Dartmouth website: http://www.umassd.edu/cryptolocker

CITS will never ask you for your password or other confidential information via email. Beware of phishing scams where email and/or malicious web sites try to trick users into entering their username and password. For more information about password security please visit: http://www.umassd.edu/cits/security/