From: HELPDESK
Sent: Friday, February 26, 2016 7:05 PM
Subject: Email Ransom Virus Alert ** IMPORTANT **

The email in the screenshot below appears to have been sent out to members of the College Community. The example email below has an attachment that will download a very dangerous new type of Ransomware Virus (Locky) which will **encrypt & lock** your files and personal data, including files on network shares (N: Drive) to which you have access. This means that your files will no longer be accessible.

How to Avoid Getting a Virus Through Email

1. Be aware that viruses and malware are often sent in Word, Excel and PDF files attached to email messages.
2. Avoid opening an email that came from an unknown person, or if its subject is something suspicious.
3. Avoid downloading or opening attachments that you did not expect to get in the first place.
4. Be careful when clicking links in suspicious email messages. Links may direct you to websites that will automatically install viruses and other malware.
5. If you should receive an email like the one below, please immediately delete it and contact the Helpdesk, or forward the email to helpdesk@mercy.edu.

If you have already clicked on a link or opened an attachment, please immediately shutdown your computer and contact the helpdesk.

Mercy College Helpdesk
helpdesk@mercy.edu
914-674-7526

Protect your ID, and never provide your username and password in response to an Email telling you that they are needed. IT Services would never send a request for this information via Email. Official IT announcements will have the Mercy College logo at the top.