

Emerging IT Threat Advisory: Ransomware

January 11, 2016

We are writing to remind the Lehman community of the importance of IT security and steps we all need to take to protect computers and mobile devices from malware and unauthorized access.

We also want to alert you to an emerging threat – **ransomware** – that renders files unusable until a “ransom” is paid. Ransomware scrambles data including documents, images, videos, and spreadsheets, using encryption technology. The victim is then prompted to pay the attacker a fee to obtain the decryption key to restore files to their original form. Like many forms of malware, ransomware is typically installed on the victim’s computer as a result of clicking a link in a malicious email message, opening an infected attachment, or visiting a compromised website. For additional information on ransomware, see <http://www.cuny.edu/about/administration/offices/CIS/security/advisories/Ransomware-Advisory.pdf>

For additional information on cyber threats to universities and the public sector, see <http://fedscoop.com/cybersecurity-nonprofit-addresses-2016-threats-for-states-localities>

The Lehman community shares responsibility in maintaining a safe and effective technology environment. Sound practices include maintaining up-to-date anti-virus software and being cautious when clicking on links or opening email attachments.

Finally, the potential threat of ransomware and data loss due to other reasons underscores the need to regularly back up your data to an external drive and to verify that the backups are usable.

If you need more information or are the victim of a ransomware attack, please contact the IT Help Desk at (718) 960-1111 or by email at help.desk@lehman.cuny.edu.