Cryptolocker

ITS has been made aware of a **RansomWare Virus** called **‘CryptoLocker’**, that is currently infecting Windows computers.

What does this virus do?

When this virus infects a system, it immediately encrypts the users data, and the data on any network shared drives that user has access to. Once the data has been encrypted, the virus prompts the user with a red background that requires the user to pay a fee to un-encrypt the data. The user has 72 hours from the start of the message to pay before the virus deletes the decryption keys. Once the files are encrypted there are no other alternatives EXCEPT to recover the data from an offline backup. Online backup solutions (like Box, Carbonite, Mozy, Backblaze, and Dropbox, etc...) are affected by the virus, and will copy encrypted files to their repositories.

Will McAfee protect you?

At this time, antivirus vendors (such as McAfee) are still working on a solution to successfully detect this virus, and prevent its infection, but they do not have one yet. They also do not have a way to un-encrypt the files once they’ve been encrypted.

What you can do to protect your computer and your data?

- Do NOT open attachments from people you’re not expecting to get attachments from. This includes emails from printers saying they’ve sent you a scanned document, or from shipping companies stating there is a customer support issue.
- Take regular backups of your data and store them offline. If you backup your files to an external HDD, do not leave it connected to your computer. Disconnect it after you have backed up your files.

What should I do if I’m infected?

- Immediately turn off your computer
- Do not attempt to move files or circumvent the problem
- Immediately contact the IT Service Center to place a work order, and have your computer rebuilt.