All,

This is to inform you of recent issues that we are seeing with “Ransomware” types of malware infections.

Note that ransomware is different than a typical virus as it currently does not propagate from one PC to another. Instead, it attacks only a single PC and renders the data files stored on that PC completely useless. We have recently had several PCs infected with CryptorBit, like CryptoLocker before it, is an infection that can activate when a user clicks on a link in a spam message or malicious email, clicks on a malicious link while browsing the web, or opens an attachment in an email from a malicious source. Emails may appear to be sent from people you know, but it’s important to read carefully – if it doesn’t look right it’s probably not.

Once inside your computer, Ransomware takes your files and encrypts them so that you can’t read them. Then it holds your files hostage for a monetary ransom of several hundred dollars or more. If you don’t pay the ransom, the files remain unusable and are essentially destroyed. This not only applies to files on your computer, but also files on any attached shared drives as well (thumb drives, home drive, departmental shares, dropbox). The encryption process is able to corrupt pretty much ALL types of data files, including Word, Excel, Pictures, Music, etc.

Even when antivirus programs and other security policies and procedures are in place, it will not prevent a Ransomware infection. Everyone should be especially careful with emails and web browsing. The latest variation, Cryptorbit, seems to be widely distributed in the guise of an Adobe Flash update. Everyone has seen the “Adobe Flash needs an update – Click here to do that” dialog box – even to the point of irritation as Adobe seems to need never ending updates. The suggestion for these types of situations is – If you receive a dialog box telling you that you need to update something – Do Not Click on the Update Button. Instead – go to the appropriate Website, for the application, and download & Install the update from the official website.

If you think you have a Ransomware infection:

1. **DO NOT CLICK ON IT!** Clicking on an infection alert is often the method by which the infection tricks you into activating it.

2. **SHUT DOWN YOUR COMPUTER** – in order to prevent further damage to your files, shut down your computer right away. If you don’t see your start menu because it is hidden by the infection, hold down the power button on your computer until it shuts off. **Unplugging your Ethernet cable is also a good thing to do as this may save some of the files that you have residing on a network shared drive.**

3. **CALL iTech HELP DESK RIGHT AWAY** – do not attempt to continue working on your computer – the longer you wait, the easier it is for infections to embed.

The best protection against these infections is a good backup. **We strongly advise that people keep their important files on their servers**, and not their desktops or local folders. The reason
for this is that files on the server are typically backed up, and files on the local computer are generally not. If your files are encrypted, we can restore them from a backup.

**HOWEVER** – if your files are not backed up, they will not be able to be recovered without paying the ransom, which is an expensive process. In either case, **PLEASE DO NOT ATTEMPT TO TAKE ANY ACTION ON YOUR OWN!**

Please call the Help Desk if you think you have infections of any kind.

Please be vigilant! iTech offers short classes on phishing and protecting your computer. Check out the articles on the Information Security channel.