Are You **Ready** for Ransomware?

CYBER SECURITY AUGUST 2018

What is Ransomware?

Ransomware is a type of malicious software that encrypts your files. Often, the only way to decrypt and gain access to the files is by paying a "ransom" or fee to the attackers. The attackers might provide the decryption key allowing you to regain access to your files. Ransomware may spread to any shared networks or drives to which your devices are connected. We are continuing to see ransomware attacks and expect their frequency to increase.

How Can I Get Infected with Ransomware?

Common vectors for ransomware attacks include e-mails with malicious attachments or links to malicious websites. It's also possible to get an infection through instant messaging or texts with malicious links. Antivirus may or may not detect a malicious attachment, so it's important for you to be vigilant.

How Can I Get Infected with Ransomware?

There are two steps to protection against ransomware:

- Preparation
  Back up your information regularly. Once a ransomware infection occurs, it's often too late to recover the encrypted information. Your research project or other important information may be lost permanently. For more information on backups, visit RIT's best practices web page.

- Identification
  Ransomware typically appears as phishing e-mails, either with links to malicious websites or infected files attached. You might also see a ransomware attack perpetrated through a pop-up telling you that your computer is infected and asking you to click for a free scan. Another possible vector is malvertising, malicious advertising on an otherwise legitimate website.

What Are the Most Important Steps I Can Take to Prepare?

- Ensure that your information is backed up regularly and properly. Because ransomware can encrypt the files on your computer and any connected drives (potentially including connected cloud drives such as Dropbox), it's important to back up your files regularly to a location that you're not continuously connected to. To determine the backup capabilities available to you contact your IT service desk.

- Ensure that you're able to restore files from your backups. Again, work with your IT support personnel to discuss how to test restore capabilities.

- Ensure that antivirus/anti-malware is up to date and functioning. Antivirus may detect malicious attachments.

- Ensure that you're keeping your system (and mobile devices) up to date with patches. If you're prompted by your computer or mobile device to accept updates, accept them at your earliest convenience.

- Don't do day-to-day work using an administrator account. A successful ransomware attack will have the same permissions that you have when working. (If you're not using an account with administrator privileges, the initial attack may be foiled.)

What Do I Do If I Think I'm Infected?

- Report the ransomware attack to your service desk immediately.

- Isolate or shut down the infected computer. (If you're on Wi-Fi, turn off the Wi-Fi. If you're plugged into the network, unplug the computer. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or shared drives.)