Ransomware

There has been a lot in the news about ransomware lately. Recent ransomware attacks have caused high-profile business shut downs, including FedEx, Under Armor, along with major Health and Financial institutions.

Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network. This article provides some background on what Ransomware is and how to protect yourself.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software (a.k.a malware) that locks the victim out of their computer or files – often by encrypting them – until a ransom is paid. The ransomware typically displays a message letting the victim know that they have been locked out, along with instructions for how much and how to pay.

Ransomware is often spread through use of stolen credentials, malicious links and harmful attachments in email; however, this is not the only mechanism. Other sources include malicious applications and files, and adware/spyware.

It is important to note that paying the ransom doesn't necessarily guarantee that you'll get access to your computer or files back. In fact, a couple of recent, high-profile cyber-attacks, dubbed "WannaCry" and "Petya", even posed as ransomware to distract people from the real attack, but in those cases, there was no way for people to get their files back by paying the ransom. The FBI and law enforcement advise never paying the ransom.

HOW TO PROTECT YOURSELF:

The following good cybersecurity habits will help to protect you from ransomware, and many other cyber threats as well:

1. **Back up critical files, and store the backups in a physically separate location from the originals.** This is probably the best protection against ransomware. If your files are backed up, you can get technical assistance to restore everything back to your computer and you won't lose anything important. Remember to test your backups periodically -- backups are useless if they don't work.
2. **Always think twice before clicking on links or opening attachments**., even if they look like they're from someone you know. Whenever possible, go to web pages by a path you know is legitimate instead of clicking on a link in a message. If an attachment is unexpected, contact the sender by a method you know is legitimate to confirm they sent it. This small extra effort is one of the best ways to keep your devices and information safe.

3. **Keep a clean machine!** Keep your devices, apps and browsers patched and up to date. Recent attacks have taken advantage of unpatched/out-of-date operating systems.
4. **Protect your passwords**, and use multi-factor authentication wherever possible. Also use different passwords for work and non-work activities.
5. **If it’s suspicious, report it!** This is an important habit in general; if something doesn’t seem right, ask. With respect to ransomware, if you think a device or files you use for work have been infected with ransomware, report it to your supervisor and whomever you report security issues to at your location. If this happens to you at home, notify law enforcement.

WHAT SHOULD YOU DO IF YOU GET RANSOMWARE?

Most importantly, don’t panic. If you have good backups, you’re probably OK with some technical assistance. As mentioned above, report the incident so you can get help.