Ransomware

What is Ransomware?

Ransomware is malicious software used by an attacker to encrypt files, an entire computer, or an entire company or university network. The attacker will then demand payment to decrypt the files. The decision to pay or not to pay is a regular topic of debate within IT Security communities.

Tips to protect yourself against Ransomware

- Backup your critical files regularly. Store at least two copies in different locations if possible
- Keep your computer operating systems up to date
- Allow software patches to be installed when prompted
- Keep software on your computer up to date. Uninstall unused programs
- Reboot your machine on a regular basis to ensure updates are fully processed
- Install antivirus, keep it up to date and scan your computer for viruses regularly
- Learn to identify phishing emails. Tips at http://phishing.fairfield.edu
- Report suspicious emails to phishing@fairfield.edu

What to do if you think you're infected with Ransomware

- Immediately unplug your computer's network cable and turn off the wireless on your computer
- Immediately shut your computer down
- Do not make any immediate payments
- If this incident occurs on the Fairfield University network contact the Help Desk as soon as possible

Videos:

A short training video about Ransomware: