February 2017
Newsletter Volume 1,
Issue 1

California Community Colleges Chancellor's Office

Ransomware

Ransomware is a type of malware that users inadvertently install on their computers by opening malicious email attachments, clicking links, or downloading files that appear to be harmless but actually contain malware. Ransomware, once installed on a computer, encrypts and blocks access to computer files and network. The only way to get access to the files is by paying money to the criminals who installed the ransomware.

Tips to Help Avoid Ransomware Attacks

1. ***Don't click.*** Visiting unsafe, suspicious or fake websites can lead to the intrusion of malware.
2. ***Always back up your files.*** By maintaining offline copies of your information, ransomware scams will have a limited impact on you.
3. ***Keep your computers and mobile devices up to date.*** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.
4. ***Enable popup blockers.*** To prevent pop-ups, turn on popup blockers to avert unwanted ads, popups or browser malware from constantly appearing on your computer screen.
5. ***Don't fall prey to social engineering or phishing.*** Attackers will attempt to get you to reveal sensitive information to them. If you receive a suspicious email from a family member or work colleagues, ask yourself whether it's unusual before you click. If you're not sure, contact the sender via a different medium, such as giving them a phone call, to cross-check.
6. ***Don't install unapproved software, plugins, or extensions.*** If in doubt, ask your IT System Administrator if the software is safe to use.

Symptoms of Infection

- Multiple pop-ups on your computer.
- Ransom message on your screen.
- Locked out of your computer.
- Can't open your files.
- Odd or missing file extensions.
- You've received instructions for paying the ransom.

My Computer is Infected, Now What?

1. Immediately, notify your line manager and your IT System Administrator.
2. Remain available for interviews.
3. If you have any questions contact Infosec@ccco.edu.

Special Points of Interest

- *Ransomware Symantec*
- *HHS Ransomware and Breach*
- *NIST Cyber Attacks*
- *SANS Survival Guide for Ransomware Attacks*
- *FBI Ransomware attacks skyrocketing*
- *FBI Public Service Announcement*