EYONIC
SYSTEMS

Ransomware

- What is it?
    - Malicious software that encrypts all of the files on the infected device
    - AND any attached USB drives
    - AND any mapped network drives
    - Distribution increased 267% between June – November 2016
- How does it work?
    - A malicious piece of software gets installed on the local device which starts encrypting files
    - The software can come from a link on a website, in an email, as an attachment, from a USB drive, etc.
    - Later you are asked to pay the "Ransomware" in bitcoin because it is untraceable
    - If paid, you should get an encryption key to unlock your life
    - Honor amongst thieves – consider the source you are working with
- First steps if you think you have been affected
    - Remove it from the network
        - Unplug the network cable (looks like a phone cord)
        - Disable the wireless
    - Shut the device off
- What's next?
    - Assess the damage
    - Find a trusted source to help you if necessary
    - Decide how to recover
        - Wipe the machine, reinstall the OS, and copy backed up files onto the machine
        - Pay the ransom
            - Enter the encryption key and hope it works
            - Recommend copying all files to another location, wiping the machine and copying files back because there is no guarantee the malicious software does not still exist on the machine
- How can you protect yourself?
    - Be cautious about what you download and what links you click
    - Keep backup copies of any important files!
        - Remember the backup rule of 3:
            - 3 copies of anything important
            - 2 different types of storage media
            - 1 offsite storage location
    - Create secondary logins for children and other family members on devices
        - This is especially important when these device are used for business purposes
- Questions? Check out https://eyonic.com/ransomware or feel free to ask us!