Protecting Yourself from Ransomware

Ransomware is software that infects a computer system and then through pop-up messages, demands that you pay to have your information restored. If your computer is infected, it may appear frozen and you will see a big message in red informing you that your files have been encrypted! There will be a demand to pay a fee online via a bitcoin payment. (Bitcoin in a type of digital currency widely used online.) The fee will rise quickly over time, threatening to destroy your files if you do not pay.

Cybersecurity experts say the virus affects computers using Microsoft operating systems and takes advantage of known vulnerabilities in the software to spread the infection. All it takes to become infected is just one click on a link or email attachment to cause the virus to spread to your computer and other computers connected to your network. If you use Apple computing products, you are safe for now. There have been no known infections of Macintosh computers.

There are several measures you can take to protect your computer and its data.

- PC users should update their computers with maintenance updates from Microsoft as they are made available. This can be set up as an automatic feature in Windows.
- If you are using older versions of operating systems such as Windows XP, stop! Old versions of software not supported by Microsoft anymore and are vulnerable to ransomware.
- Use virus software that will monitor your emails for both links and attachments. Good virus protection software will help reduce your risks. Ransomware is typically contracted by either opening an email attachment or clicking on a link in an email.
    - Most importantly, don't open emails from senders you don't know.
    - Always be on the lookout for suspicious emails with attachments that you did not request, and never click on links from questionable sources.
- Remember you are also taking a risk every time you download and/or install a file from the Internet. Be very warry of FREE SOFTWARE. Ransomware and other malicious software are commonly distributed by this method.
- Make backups regularly. The only sure way to recover is to re-install your software to a version that you obtained prior to the infection.

Would-be extortionists can launch a global campaign with little effort, yet authorities can do little because it's very difficult to investigate. Because criminals are responsible, not governments, even paying a ransom does not necessarily assure you can get your data and computers operational. Your best protection is to become savvy with spotting bogus emails and solicitations.

Don't think any of this pertains to you? If one looks at a typical household right now, a general household, it's not unusual for it to have 20 or maybe 30 IoT (Internet of Things) devices. While these are typically Wi Fi enabled, they are all part of your home's "private network." An attack

on any device can expose the home computing devices connected to the home network. Those home devices such as door bells, locks, thermostats, appliances, and cameras are made with no secure backend to protect against intrusion. Because we forget about them, people are not updating them when the manufacturers provide security updates. These are the vulnerabilities that can expose you to ransomware. And don't forget that the passwords you use for these home devices are just as vulnerable to hacking. Learn how to create complex passwords and change them occasionally.

Central Florida Crime Prevention Association

http://www.cfcpa.org/