RANSOMWARE

Ransomware is malicious software that cyber criminals use to hold your computer or computer files for ransom, demanding payment from you to get them back. Sadly, ransomware is becoming an increasingly popular way for malware authors to extort money from companies and consumers alike. There is a variety of ransomware can get onto a person's machine, but as always, those techniques either boil down to social engineering tactics or using software vulnerabilities to silently install on a victim's machine.

(Often comes through an e-mail you don't recognize)

What can you do to protect against ransomware?

On the one hand, ransomware can be very scary – the encrypted files can essentially be considered damaged beyond repair. But if you have properly prepared your system, it is really nothing more than a nuisance. Here are a few tips that will help you keep ransomware from wrecking your day:

1. Back up your data

The **single biggest thing** that will defeat ransomware is **having a regularly updated backup**. If you are attacked with ransomware you may lose that document you started earlier this morning, but if you can restore your system to an earlier snapshot or clean up your machine and restore your other lost documents from backup, you can rest easy. Remember that Cryptolocker will also encrypt files on drives that are mapped. This includes any external drives such as a USB thumb drive, as well as any network or cloud file stores that you have assigned a drive letter. So, what you need is a regular backup regimen, to an external drive or backup service, one that is not assigned a drive letter or is disconnected when it is not doing backup.

9. Disconnect from WiFi or unplug from the network immediately

If you run a file that you suspect may be ransomware, but you have not yet seen the characteristic ransomware screen, if you act *very* quickly you might be able to stop communication with the C&C server before it finish encrypting your files. If you disconnect yourself from the network *immediately*(have I stressed enough that this must be done *right away*?), you might mitigate the damage. It takes some time to encrypt all your files, so you may be able to stop it before it succeeds in garbling them all. This technique is definitely not foolproof, and you might not be sufficiently lucky or be able to move more quickly than the malware, but disconnecting from the network may be better than doing nothing.

(After disconnecting, contact your district technician for assistance)

Additional tips and information at the source page/link below.

Source: http://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against-ransomware-including-cryptolocker/