There is a gun pointed at your data!!

And it is waiting for you to pull the trigger!

CRYPTOLOCKER! *A brief on data disaster*

Eddie Winecoff – President, Computer Connections Inc.

Cryptolocker – the Miscreants newest threat to your data. Yes, the threat is real! Yes, your data is under severe threat if your computer is infected with the virus. Yes, you have to pay the ransom to "unlock" your data. Yes, you **can** prevent it from happening!

How real is the threat?

When we look at this latest threat, we are seeing two different kinds of "ransomware". One is by far the most common and the least destructive. It is known more commonly as the "FBI Virus". This infection will lock your computer up, but your data is not in complete jeopardy. It is known by its signature split screen, an FBI shield on one side and instructions for paying the ransom on the other. Your computer will have to be "cleaned" by a professional but your data typically can be rescued. **Computer Connections** technicians typically fix 2-3 PC's with this infection a day.

The far more sinister infection is the actual "CRYPTOLOCKER" Trojan infection. This virus WILL encrypt and lock your data. The ONLY way to recover your data is to pay the ransom. If you do not pay the ransom, the data that has been infected on your computer is irretrievably lost. Hopefully you have a good backup routine. We have only seen one or two of these actual infections. We may not be seeing these as much due to people actually paying the ransom.

We do know that the infection is active and being delivered to PC's in our area, due to the phone calls we get where their anti-virus has successfully blocked the delivery of the virus.

How do I keep from getting it?

The best way to prevent your computer from being infected with any virus is twofold. One, be aware and vigilant about the email links you open, the videos you click on in social media (Facebook, Twitter, etc.) and the web sites you visit. Most of the ransomeware infections are delivered through fake emails from UPS, FEDEX, DHL or your utility company, that say something to the effect that "your package has not been delivered" or "your account is delinquent" . These typically will have a link embedded for you to click on for more information. We also see the infection being spread in a most unusual way and that is through customers using a remote 3rd party service company, which they allow to "logon" to their computer remotely to fix a problem. NEVER let someone on your computer remotely that you do not know. Even if you have been communicating with what you think is a reputable computer or printer company. They typically hand off their online service to a 3rd party company and this is where the problem starts. The first thing they will want is your credit card information. Best practice is to only allow someone you know to get on your computer remotely.

The second best preventative is to have a good solid anti-virus program running on your computer. The free programs just do not do the job in preventing most brute force viruses. Keep in mind though, that any anti-virus program is not 100%. You must still be vigilant and aware of what you are doing.

I have the infection, now what do I do?

First thing you should do if your computer gets infected is turn it off immediately and remove it from your network. This will keep the infection from spreading to other PC's on your network. Once off your network, you can turn your computer back on. Be aware that at this point you are probably past the point of no return. If you have the true Cryptolocker infection the damage is probably done to your data. At this point you have to decide if you are going to pay the ransom or not. If you have the lesser "FBI" type virus, you may still be able to do some things, but your computer will eventually lock. Your data is probably still available.

You will want to get some professional help with either virus at this point. Computer Connections has the knowledge and expertise to help you make your decision going forward.