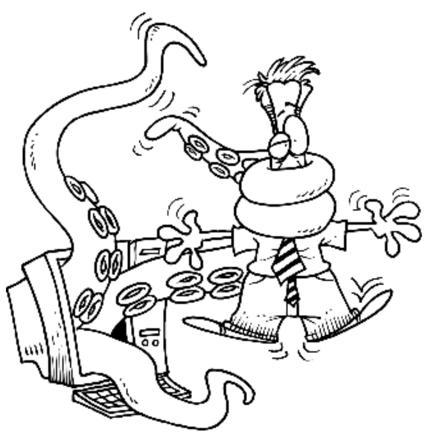
KEEP IT *Up&Running*

Dedicated to Keeping Your Computers *Up&Running*

Regular Backups Are Even More Critical

You have probably heard of the **Cryptolocker** virus



by now. Not only will it destroy all the files on the computer it first enters, it will also destroy the files on a network server that is connected to that computer. Once it has destroyed (encrypted) all of the data files, you'll get a pop-up: "Your personal files are encrypted!" The user is then instructed to pay a ransom in order to get the key to unencrypt the files.

You may be one of the "lucky" few who pay the ransom and have their files unencrypted by the criminal who has extorted the money. Most people are not so fortunate and end up losing their money and their files. It's never a good idea to reward criminals anyway.

Usually the virus comes in as a link in a phishing message. It may be one that says it's from Xerox and is delivering a PDF of a scanned image. It will even look like it has a PDF extension. Unfortunately, there is a hidden ".exe" extension which makes it a dangerous executable file. Or it may say it is from UPS or FedEx offering tracking information. It may be from a bank confirming a wire or money transfer. It has also come in as a notice of a voice mail message that you can hear if you click on a link. Obviously, you should never click on a link in an email that you weren't expecting, even if it looks like it's from a reliable company. Instead, go to the actual website for the company using your web browser.

At this time, anti-virus and malware programs have been completely unsuccessful in stopping the **Cryptolocker** virus. If you become infected,

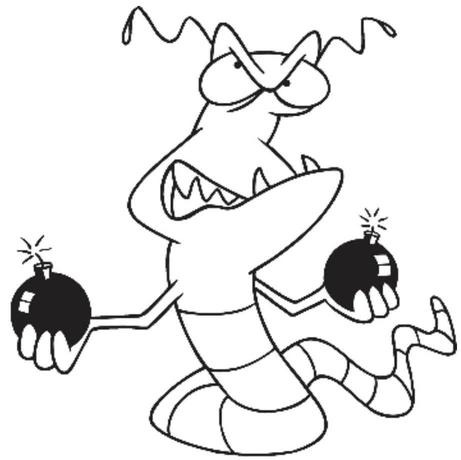
you will probably notice unusual activity on the hard drive, or the computer acting sluggish. If you see the hard drive light on the computer case blinking more rapidly than usual when you aren't doing anything, you should be suspicious. If you know you have also clicked on a link in a recent email, it's best to turn off the computer sooner, rather than later. Then call ***Up&Running*** for

assistance. We have been able to save most of the files on a computer when it was shut down soon enough.
First we copy the data off and then reformat the hard drive and reinstall Windows and the rest of the software programs. Then the data is moved back to the hard drive.

If you don't discover the virus until the pop-up appears, only a backup will save your data. The hard drive will have to be reformatted and everything will be lost.

So a word to the wise: Do regular backups to an external media device. An easy way to make sure that your files are safely backed up each night is to take advantage of our remote backup service. For a small monthly fee, depending on the amount of data that is being backed up, all of your files can be backed up to a secure cloud site every night. If one or more of your files need to be restored, it is an easy process for you to restore the files yourself. Of course, we're always available if you would like assistance with that process.

Now is the time to take the necessary precautions against the **Crytolocker**



virus and any other nasty new ones that are sure to start creating havoc in the future.

Call today:
(949) 859-9880

- **Networks and Servers**
- **Remote Backups**
- **Data and System Backups**
- **Custom-Built Computers**
- **System Conflicts**
- **Hardware Diagnostics**
- **Upgrades**

Up&Running

(949) 859-9880