CryptoLocker Virus Holds Your Data for Ransom

CryptoLocker is a virus program released earlier this fall. It targets Windows computers (Windows XP, Windows Vista, Windows 7, and Windows 8). The virus will encrypt (lock with a code) your business documents, pictures, and other files. Once your files are locked, you will get a ransom notice to pay up to $300 to unlock them. If you don't pay the ransom within 72 hours, the code is destroyed and your files can never be restored.

The good news—if you pay the money, your files will probably be unlocked. (If you consider paying $300 good news). At least they're 'honest' thieves.

The bad news—if you don't pay, your data is gone. As I mentioned last month, you'll know how devastating that can be to a business.

Minimize your chances of infection

- Don't open emails, email attachments, or links in emails from people you don't know.

- If you have to send an email with an attachment, let the recipient know it's coming before you send it.

- Don't download random files from the internet. (Be especially suspicious if you're asked to download a file to be able to watch a video)

- Maintain OFFSITE backups of your important files and make sure that the backups are working.

    - Backups are working when they run on a consistent, regular schedule and can be restored!

    - Backups are OFFSITE if you store them on the cloud or on an external drive that is stored someplace other than next to your computer.

- Make sure your Anti-Virus and Firewall protection software is up-to-date

Your IT provider/department and your Internet service probably scan and filter your email, and have some firewall protection, but you still need to be vigilant.

What gets infected?

CryptoLocker mainly infects photo and video files plus most types of Office documents (Word, Excel, PowerPoint, etc.) Even if you use a free program (StarOffice, OpenOffice) CryptoLocker will infect those files. The writers of the CryptoLocker virus know that the bulk of the data you need is probably stored in an office type document, whether it's Microsoft, Corel, or OpenOffice.

If you do get infected...

Disconnect your computer from your wireless or wired network. If you leave it connected, the virus will encrypt other files on your network instead of just your local files. If you elect to pay the ransom, DON'T use a personal credit card. Get a pre-paid cash card so you don't add identity theft to the situation. If you don't pay the ransom (because you have a good backup system in place), leave the computer alone and contact your network administrator (or IT provider/department). The virus should be cleaned off the computer, then the files can be restored from a previous backup.

Four Tips for Online Backup

I know some of you saw this last month, but it's important enough that it bears repeating. From a business standpoint, backing up your data is a necessity—and for more than the inconvenience of losing the data. Offline backups are most likely a standard practice rather than an extra these days.

If you haven't begun using an online backup service, here some things you'll maybe want to consider before you do:

Plan. What data needs to be protected with offsite backup and recovery tools?

Adhere to a schedule. Your data is only as secure as your last backup. It needs to be protected on a predictable, repeatable schedule.

Offsite storage issues. Transmitting the data requires a reliable and repeatable software program. Encryption should also be present when transmitting or storing your data offsite.

Vendor selection. K² provides the needed pre-sale consulting advice and after-sale support. Plus, we're not across the country or thousands of miles away.

A well thought out offsite backup and recovery solution helps you get back in business fast, should the need arise. Call us here for information about the **K² Ambassador Basic Backup Services**

Like our Facebook page for computer tips and tricks!

http://www.facebook.com/ K2Technologies.Wyoming

Do you have a specific software training need? K2 can create a custom training event just for you and your company!

Call Karen for more information on this and to discuss any other software training needs you might have. 307-686-3025.