Should My Business Be Concerned About Ransomware or Cryptolocker Malware?

Few things strike fear in the hearts of millions of computer users quite like the possibility of their computer becoming infected by ransomware or other malware such as Cryptolocker. While ransomware may be little more than an inconvenience for individual home computer users, it be can catastrophic for a business.

Malware, or malicious software, is a broad term used to describe computer viruses that can compromise a computer's security – many of them turn off antivirus software and download additional malware – or hold the computer or the data on the computer for ransom. Often a malware will claim that your computer is infected with a virus which the malware's creator will helpfully remove for you if you pay them. Some versions of malware claim to have found illegal files on your computer, such has the infamous FBI Virus, and demand that you pay a 'fine' before you will be allowed access to your files.

Generally, this type of malware blocks your access to the internet, locks you out of your computer, or disables access to your files or programs until you pay the virus creator to release your computer.

Although these types of infections generally come from infected e-mail or websites, once a single machine in a business is infected, the virus can spread quickly through the network, file shares on the network, or by simply e-mailing itself to other workers in the company's e-mail directory.

The impact of workers suddenly losing the ability to access their computers or to access the data on their computers can be devastating.

More importantly, the financial impact can be crippling to a small business, whether through lost productivity or the cost associated with bringing in outside IT support, if needed, to clean up your computers.

However, the cost of a basic malware infection pales in comparison to the cost of a Cryptolocker infection.

Continue on Page 2

Cryptolocker works by encrypting your files using a secret encryption key. The only way to regain access to those files is to pay a ransom to the virus creator for the matching decryption key so that you can unencrypt the files.

Cryptolocker is an extremely dangerous virus that will quickly encrypt every file the computer hosting the virus has access to. On a shared computer network, this means that not only will the individual user's files be encrypted, but any shared files on the network, such as a workgroup share or a common public share, will be quickly – and potentially irrecoverably – encrypted.

Paying the ransom is no guarantee that you will recover your files.

One Charlotte, NC law firm learned this the hard way. A 2014 Cryptlocker infection at the law offices of Paul Goodson resulted in the loss of thousands of stored legal documents, many of which contained confidential client information, when his firm was struck by a virus masquerading as an e-mail from the firm's automated phone system.

Preventing such infections is the job of every employee. A good antivirus solution will stop many infections, but a more important weapon is as simple as user education.

Contact us for more information on how to protect your business, **515-270-5300.**