CryptoLocker and Ransomware

John Stevenson - 2023-03-03 - Comments (0) - Security

What is CryptoLocker?

CryptoLocker is malicious software that encrypts your data files (Word, PowerPoint, pictures, music, videos, etc.), including your files on removable media and network storage. You are then asked to pay for the decryption key to restore access to your data.

What computers are at risk?

All computers that run Windows, including virtualized machines and Bootcamp partitions.

What is dangerous about this malware?

Once infected, your data files are encrypted with a unique key that only the people responsible for the malware are able to provide. Once encrypted, there is no way to recover the data without paying the ransom. If the key is lost or the ransomers refuse to provide it, the data is lost forever.

How can I protect my data?

Backup your data to another location (network drive, external hard drive, cloud storage, etc.)

How can I avoid the malware infection?

Never open attachments from email addresses that you don't know or trust. Be careful which web advertisements you click on and if an unfamiliar application asks for elevated privileges, click no.

How can I protect my computer?

Make sure to regularly connect your work computer to the network to receive regular and important updates for your operating system and anti-virus software.

For a personally owned computers, make sure you are regularly connecting to Windows Update and have an up-to-date anti-virus program. Most modern Windows computers have Windows Defender, which is a built in anti-virus software—this is why it is imperative that you keep your device update and routinely check for optional security updates as well. In addition, you should consider paying for an online backup solution or backup your documents regularly to external storage.

I think my computer may be infected with CryptoLocker, what do I do?

Turn off your computer immediately and, if this is a university-owned computer, contact your Computing Coordinator or the IT Help Desk immediately.

For personally-owned computers, you should take your machine to a qualified technician for help.