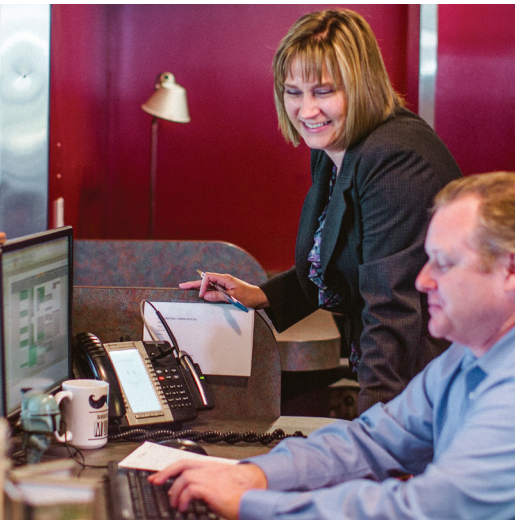
Tips to Stay Protected from CryptoLocker Ransomware



PAVELCOMM

Tips to Stay Protected from CryptoLocker Ransomware

Are Your Files Protected from Ransomware?

Imagine sitting at your work desk checking your emails like you do every morning – when suddenly, you're kicked out from accessing your personal files and data. CryptoLocker is a type of ransomware that encrypts users' files via email attachments and links. When activated, the malware prevents you from accessing your data until a "ransom," usually made through a wire transfer or digital currency like Bitcoin, is given to the attacker.

According to an analysis by Dell SecureWorks, the feared Cryptolocker ransomware has infected at least a quarter

of a million PCs worldwide. Based on Bitcoin payments connected to the ransoms, the sums estimated to have been extorted in the first 100 days of CryptoLocker's activation were between $380,000 and $980,000 in value. The security threat landscape has never been so unstable than it is now. Is your business protected from the latest threats and ransomware attacks? We'll share a few tips to help keep your personal data better protected.

Tips to Protect Your Data from CryptoLocker Ransomware

Execute a Robust BDR Plan

A comprehensive Backup and Disaster Recovery (BDR) plan can be the best defense against CryptoLocker ransomware. Because CryptoLocker can also encrypt any attached networks, it's best to do offsite backups as well. By securing your business with a strong BDR plan, you can avoid having to pay a ransom to access to your critical files and data.

Implement Employee Security Awareness Training

Human errors are by far the most common and most frequent causes of business disasters. Training your employees on best email practices and security policies is a crucial step to securing your business.

Install Antivirus Software on All Work Computers

Always make sure you've got a reputable and updated antivirus program installed on your work computers to monitor and detect threats. An effective antivirus software package can help keep you safe from CryptoLocker and other harmful types of malware.

"By securing your business with a strong BDR plan, you can avoid having to pay a ransom to access to your critical files and data."

Avoid Clicking on Suspicious Links/Email Attachments

CryptoLocker is most commonly activated via email. That is the reason why you should always be wary of suspicious email links and attachments, especially when you're dealing with sensitive corporate data. By staying alert when going through your emails, you can prevent a deadly attack from striking and affecting your organization.

Regularly Update & Patch Your PCs

Don't ignore those notifications telling you that it's time for a Windows security update. These updates patch system vulnerabilities that could allow your computer to be compromised. Always be sure to update your PCs regularly!

"By staying alert when going through your emails, you can prevent a deadly attack from striking and affecting your organization."

Don't Let Ransomware Interrupt Your Business

Here at Pavelcomm, your security is our number one priority. We hope that these tips helped you gain a better understanding of CryptoLocker and what you can do to prevent falling victim to the next ransomware attack. If you need a technology partner to help you backup your systems, restore your data, or keep you updated with the latest antivirus and anti-malware programs, contact us today! We'd be happy to meet with you for a free consultation.

PAVELCOMM

Get In Touch

info@pavelcomm.com
(503) 223 5008

1640 NW 14th Ave
Portland, Oregon 97209