

An employee publication of the  
Texas Department of Criminal Justice

## Information Security: CryptoLocker ransomware warning

A newly developed ransomware program called CryptoLocker poses a serious threat to anyone using email on Microsoft Windows. In 2013, security software experts named CryptoLocker “Menace of the Year” when it infected more than 12,000 computers in a single week. Data files on CryptoLocker-infected computers are at risk of being lost forever.

CryptoLocker spreads through email attachments, and often targets companies through phishing attempts. Infection often spreads through an email which can look like a tracking notification from UPS or FedEx, or anything hackers can come up with to tempt you to click the link. CryptoLocker targets dozens of common files, including Word documents and JPEG images. An especially dangerous aspect of CryptoLocker is that it not only attacks data on the PC which was used to open the infected file, but also goes after any devices, drives and networks connected to that PC. One business in Australia was shut down for five days with staff sent home on leave. Every network share’s data was encrypted, more than 64,000 files, after a staff member clicked on an attachment, despite telltale suspicious signs.



CryptoLocker currently requests individuals pay \$300 to have their files unencrypted, and ransom payment does not guarantee restoration of your data.

To help prevent the spread of malware such as CryptoLocker, Information Technology Division (ITD) restricts administrative privileges and limits user access to software control settings. Other tips you can follow to help protect yourself from CryptoLocker and malware in general include:

- Use an anti-virus, and keep it up to date: While TDCJ’s ITD maintains anti-virus software on agency computers, it is important to notify the help desk if anti-virus is not on your computer, not updating properly, or if you think that

you may have already been infected. ITD has noted that many current victims of CryptoLocker were already infected with malware that should have been removed, preventing not only the CryptoLocker attack, but also any damage due to the malware infection.

- Keep your operating system and software up to date with patches: This helps prevent malware from sneaking unnoticed onto your computer. CryptoLocker doesn’t use sophisticated intrusion techniques because their malware uses malware already on the victim’s computer to open the door. While ITD maintains system patching, you should notify the help desk if the system is not updating properly.

*Continued on page 2*

*Continued from page 1*

ITD works diligently to protect our data from threats such as CryptoLocker, but security relies on the individual users. Learn how to recognize malware and prevent spreading infection by computer virus. If you have any questions about data protection, call the Information Security Department at 936-437-1800. ●