



CITY OF GLENDORA

For Immediate Release

October 3, 2013
For Immediate Release
For further information contact
Glendora Police Department (626) 914-8274

GLENDORA POLICE DEPARTMENT WARNS RESIDENTS ABOUT A NEW COMPUTER VIRUS THAT DESTROYS YOUR FILES IF YOU DO NOT PAY A "RANSOM"

The Glendora Police Department has recently taken a report from a resident regarding a computer virus that corrupted their computer remotely and then demanded a ransom.

A local businessman received an email from what he thought was his bank, addressed to his business, only to find that after he clicked on the zip file attachment, a malware virus encrypted his files, rendering them useless. Two windows then popped up, one with the word "Crypto Locker" in the title, requesting that he pay \$300 via a pre-paid money card and once done, he would receive a "key" to unlock his files. The message continued to tell him that he only had a certain amount of time to pay the money, and if he did not send the money, his files would then become useless and he would not be able to retrieve his photos, files and other documents. According to the victim's computer expert, the data was lost because of the encryption. The Glendora Police Department investigated the origin of the email and found that the account asking for the ransom came from overseas and there is no guarantee that the key will be sent even if the money was paid.

"These types of sophisticated crimes are becoming more prevalent and it is my hope that by informing the public we can reduce the chances of our community members falling victim to these types of cyber-crimes being perpetrated from across the world," said Chief of Police Rob Castro.

Unfortunately, the new ransomware is a growing trend, according to a website called Boxaid. Boxaid, along with the Glendora Police Department, wishes to pass along these tips to computer users in order to help avoid receiving these computer viruses:

1. Don't click on anything unless you know what it is and who it is from. In the case of Crypto Locker, it disguises itself as a legitimate source such as the US Postal Service, your local

more



CITY OF GLENDORA

For Immediate Release

- bank, etc. If you are not expecting anything from these sources, don't open the email.
2. If you get an email from anyone with an attachment, do not open it unless you trust the sender.
 3. Don't click on links that seem too good to be true, such as "How to Make Money" or "How to Speed up your Computer," etc.
 4. Don't trust cold calls. Do not give your information to anyone who calls you. If they say that they are from tech support and have found a virus on your computer, it could be a scam. If you give them access, they will control your computer remotely and use your personal information to open new charge accounts or charge on your existing accounts. If the caller claims there is a security threat to your computer, hang up and call your computer company directly.

To read the article on this malware virus from Boxaid, go to <http://www.boxaid.com/word/cryptolocker-ransomware-encrypts-files-permanently/>

Please share this information with your friends and family so that you do not become a victim of this crime trend.

For more information, please contact the Glendora Police Department at 626-914-8250.

###



CITY OF GLENDORA

For Immediate Release