

Ransomware....Can You Afford It?

March 2013



ON CYBER PATROL

ciog6.army.mil/OnCyberPatrol.aspx



Scammers are using a form of malware called Ransomware to terrorize computer users. This type of malware prevents a user from using his or her computer or accessing any data until a payment (the ransom) is made. The user is asked to pay a ransom -- that ranges anywhere from hundreds to thousands of dollars -- through wire transfer, online payment vouchers or premium rate text messages. Users could feel forced to pay in order to have access to their system again.

The system is held hostage in several ways. Lockscreen Ransomware displays a full-screen image or webpage that prevents access to anything on your computer. Whereas, encryption based Ransomware encrypts the files with a password, and this takes away your ability to open or copy files.

Some instances of Ransomware display a notification, saying the local authorities have detected illegal activity in your computer. Some users are told their computers contain pornography, illegally obtained software, illegally downloaded music or something else linked to illegal activity. Other users are told the version of their operating system is counterfeit and they must purchase a good, clean copy before their computer can be used again.

This virus is presenting so many problems because it appears to come from actual law enforcement officials with very real looking web pages and official seals and logos. This scam is not only directed at the home user with one or two computers, but also at large corporations and hospitals that can afford to pay higher ransoms.

How do criminals install Ransomware on your computer? Ransomware is usually installed when you open a malicious email attachment or when you click a malicious link in an email message, instant message, or on a social networking site.

The Microsoft Safety & Security Center recommends several ways to avoid becoming a victim of Ransomware:

- * Keep all of the software on your computer up to date.
- * Keep your firewall turned on.
- * Don't open spam email messages or click links on suspicious websites.
- * Download Microsoft Security Essentials, or Anti-Virus software
- * Scan your computer with the Microsoft Safety Scanner, or Anti-Virus software

Under no circumstance should you pay the ransom in order to regain access to your computer or files. If you pay, that does not guarantee you will be given access to your files. The scammers could continue to ask for more money. What you should do is immediately report the incident to: <http://www.onguardonline.gov/>.

If you find out your computer has Ransomware on it, you should immediately take steps to remove it. This link will help you remove it: <http://www.microsoft.com/security/portal/shared/ransomware.aspx#recover>

Remember, never visit questionable websites or download suspicious attachments. Make sure you only open emails from people you know and be vigilant when doing online transactions.

More OnCyberPatrol comics and articles can be found at: <https://ciog6.army.mil/OnCyberPatrol.aspx>