

# Ransomware

## YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America (Article I, Section 8, Clause 8; Article 202; Article 228 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years).

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, sexploit and child abuse, your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist notices were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through

To pay the fine, you should enter the digits resulting code, which is located on the back of your  in the payment form and press OK (if you have several codes, enter them one after the other and press OK).



Ransomware is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. Ransomware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again. Ransomware stops you from using your PC. It holds your PC or files for ransom. Some versions of ransomware are called "FBI Moneypak" or the "FBI virus" because they use the FBI's logos.



Ransomware is usually installed when you open a malicious email attachment or when you click a malicious link in an email message or instant message or on a social networking site or other website. Ransomware can even be installed when you visit a malicious website. The simplest type of ransomware, aka scareware, consists of bogus antivirus or clean-up tools that claim they've detected umpteen issues, and demand that you pay in order to fix them. Some specimens of this variety of ransomware may allow you to use your PC but bombard you with alerts and pop-ups, while others might prevent you from running any programs at all. Typically these invaders are the easiest type of ransomware to remove.



## How to avoid Ransomware:

- ✓ Keep all of the software on your computer up to date. Make sure automatic updating is turned on to get all the latest Microsoft security updates.
- ✓ Keep your firewall turned on.
- ✓ Don't open spam email messages or click links on suspicious websites.
- ✓ Scan your computer with the Microsoft Safety Scanner.

## REFERENCES

-  <http://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx>
-  <http://www.microsoft.com/security/resources/ransomware-what-is.aspx>