



ALL ABOUT RANSOMWARE



Presented by: Maria kopaka

What is ransomware



Ransomware is a type of malware (malicious software) used by cybercriminals. If a computer or network has been infected with ransomware, the ransomware blocks access to the system or encrypts its data. Cybercriminals demand ransom money from their victims in exchange for releasing the data.



For example

A ransomware attack is a type of malware attack that encrypts a victim's data and prevents access until a ransom payment is made. Ransomware attackers often use social engineering techniques, such as phishing, to gain access to a victim's environment. There are two main types of ransomware crypto ransomware and locker ransomware

The screenshot shows a ransomware payment screen with a red background and white text. The main heading is "Oops, your files have been encrypted!". Below this, there is a white padlock icon. The screen is divided into several sections:

- What Happened to My Computer?**

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
- Can I Recover My Files?**

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.
- How Do I Pay?**

On the left side, there are two boxes with a white background and red text:

- Payment will be raised on**
1/4/1970 05:30:00
Time Left
00:00:00:00
- Your files will be lost on**
1/8/1970 05:30:00

At the top right, there is a language dropdown menu set to "English".

On the far left, there is a black vertical bar with red text: "Oops, If you see th then your ant it from your". There are also two small icons of hands shaking and a document icon.

On the far right, there is a black vertical bar with red text: "indow, leted".

Can ransomware be removed

RANSOMWARE SOMETIMES DELETES ITSELF AFTER IT HAS INFECTED A SYSTEM; OTHER TIMES, IT STAYS ON A DEVICE TO INFECT OTHER DEVICES OR FILES. USE ANTIMALWARE/ANTI-RANSOMWARE. MOST ANTIMALWARE AND ANTI-RANSOMWARE SOFTWARE CAN QUARANTINE AND REMOVE THE MALICIOUS SOFTWARE. FOR THE FASTEST WAY TO RECOVER FROM RANSOMWARE IS TO SIMPLY RESTORE YOUR SYSTEMS FROM BACKUPS. FOR THIS METHOD TO WORK, YOU MUST HAVE A RECENT VERSION OF YOUR DATA AND APPLICATIONS THAT DO NOT CONTAIN THE RANSOMWARE YOU ARE CURRENTLY INFECTED WITH. BEFORE RESTORATION, MAKE SURE TO ELIMINATE THE RANSOMWARE FIRST.

HOW TO REMOVE RANSOMWARE?

RANSOMWARE: A TYPE OF MALICIOUS SOFTWARE DESIGNED TO BLOCK ACCESS TO A SYSTEM UNTIL A SUM OF MONEY IS PAID.

THERE ARE THREE LEVELS OF RANSOMWARE AND YOUR REMOVAL SOLUTION DEPENDS ON IT.

- Scare-ware - Fake Antivirus or PC Cleanup tools pretending to detect issues on computer and demanding money to clean them up.**
- Screen / Browser Locker - Fake FBI / U.S. Department messages to claim they've detected illegal activity on computer for which you need to pay fine.**
- Data Encrypter - Pop-up messages say your files are encrypted and demand ransom money be paid in order to return them.**

HOW TO REMOVE SCAREWARE AND SCREEN LOCKERS?

- 01** Usually, these can be found in the list of Software programs installed on your computer. You can uninstall them manually from the list.
- 02** In case, name is not listed, you should use proven anti-malware solution.
- 03** It will detect and remove such nuisance programs and also look up for any other infection on system.

3 WAYS TO REMOVE