What is Ransomware? How to Protect Your Device from Ransomware

Ransomware is becoming one of the biggest threats to internet users. This type of malware can encrypt data and force victims to pay a ransom to recover it. Understanding how it works will help you protect your devices from being attacked.

Ransomware can paralyze entire systems and cause serious data loss. Understanding how it works and taking preventative measures is the best way to protect personal and business information.

History of Ransomware

Ransomware first appeared in 2005-2006, developed by criminal groups in Russia. Initially, it was widely spread in Russia, Belarus, Ukraine and Kazakhstan with variants such as Archievus and **Troj_Cryzip.A** .

Early versions worked quite simply: files in the My Documents folder were encrypted and then transferred to a password-protected Zip file. To retrieve the data, victims had to pay through **E-Gold** , a popular exchange platform at the time. However, after the platform was shut down in 2009 due to its involvement in money laundering, attackers began using Bitcoin and prepaid debit cards to collect ransoms.

By the late 2000s, the malware had become more sophisticated. Some variants, such as Reveton, impersonated law enforcement agencies to intimidate users. When infected, a fake warning would appear on the screen, accusing the victim of copyright infringement and demanding a 'fine.' This helped the ransomware spread across Europe, the United States, Australia, Canada, and New Zealand.

In 2012, ransomware continued to thrive, targeting the Windows Master Boot Record (MBR) – the component that helps the operating system boot. When the system is infected, the malware replaces the MBR with a ransom note, forcing the victim to pay through QIWI, a Russian online payment platform, to regain access to the device.

Common variations

- Crypto malware: Encrypts files and demands ransom to unlock them.
- Locker malware: Locks the entire system, making the user unable to use the device.
- Scareware: Displays fake warnings about system errors or viruses to trick users into buying useless software.

How does ransomware spread?

1. Via phishing email

- Emails containing malicious attachments or links to phishing websites.

- When the user opens the file, the malware is activated and begins encrypting the data.

2. Attack via insecure software

- Cracked apps or software may contain ransomware.

- Incomplete system updates increase the risk of attack.

3. Exploiting security holes

- Attacks through unpatched vulnerabilities in operating systems and software.
- Some ransomware exploits the RDP (Remote Desktop Protocol) protocol to infiltrate devices.

Signs of a Ransomware Infected Device

1. Ransomware warning appears

The screen displays a message asking for payment in Bitcoin or other cryptocurrencies.

2. Unable to open file or access system

- Files are renamed or have strange extensions.
- Computer is locked, only showing payment instructions.

3. System performance is significantly reduced

- Computer is running abnormally slow due to malware running in the background.
- CPU and hard drive processes suddenly increase.

How to protect your device from ransomware

1. Update software and operating system

- Always install the latest updates to patch security holes.
- Use licensed operating systems and software.

2. Use powerful antivirus software

- Install and enable anti-ransomware features on security software.
- Some software such as Windows Defender, Avast, Kaspersky provide anti-ransomware tools.

3. Do not download files from untrusted sources

- Avoid opening emails from unknown senders or with suspicious content.
Do not download and install software from unofficial websites.

4. Back up your data regularly

- Use an external hard drive or cloud storage service for regular backups.
- Keep at least one backup offline to avoid being encrypted by ransomware.

What to do when infected with ransomware?

When you discover that your device **is infected with ransomware** , the most important thing is **not to panic** and take the following steps:

1. Disconnect from the internet immediately

This helps prevent the malware from spreading to other devices or downloading additional malicious data from the attacker's server.

2. Do not pay ransom

Paying does not guarantee that you will get your data back. At the same time, it encourages hackers to continue their attacks.

3. Use a free decryption tool

Some programs like Avast Ransomware Decryption Tool or Kaspersky Ransomware Decryptor can help recover data without paying the ransom.

4. Reinstall the system if necessary

If you cannot decrypt the files, reinstalling the operating system from a backup is the best option to completely remove the malware.

To reduce the risk of being attacked, it is important to install security software. Free Download recommends that you use reputable **antivirus software** such as Avast, Kaspersky or Windows Defender, which can detect and prevent threats from the beginning.

You finished reading the article "**What is Ransomware? How to Protect Your Device from Ransomware**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.