RANSOMWARE

More about it

01

What is ransomware

A type of malicious software designed to block access to a computer system until a sum of money is paid.

02

Give examples of ransomware

If a computer or network has been infected with ransomware, the ransomware blocksaccess to the system or encrypts its data. Cybercriminals demand ransom money from their victims in exchange for releasing the data.

03

Is ransomware a virus

While some people might think it is a virus, ransomware would be recognized as a different form of malware than a virus.

04

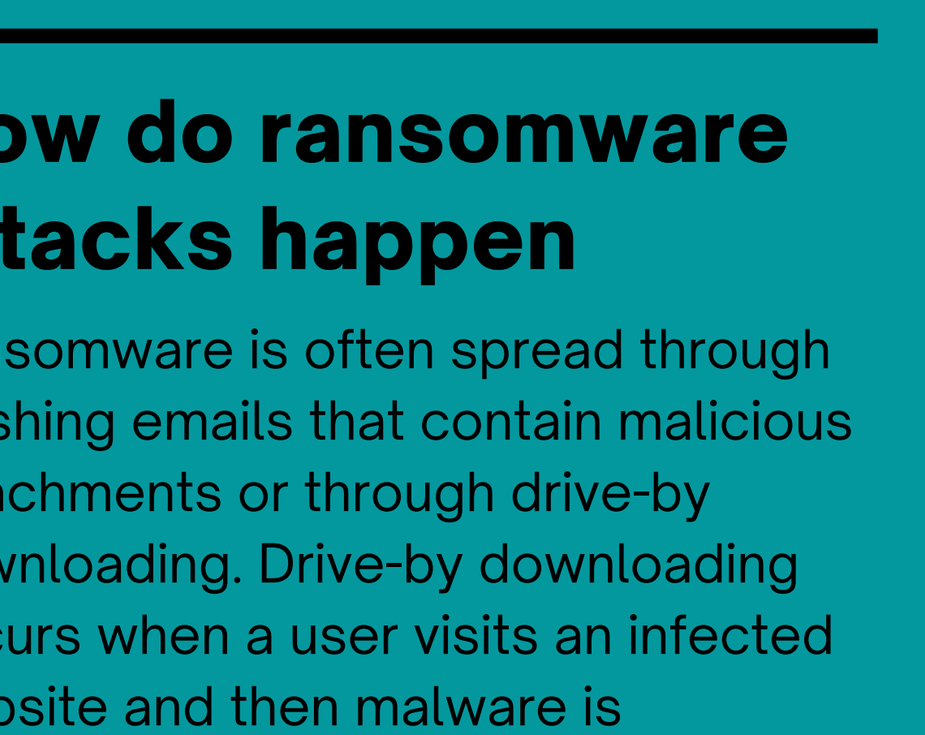
How do ransomware attacks happen

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user visits an infected website and then malware is downloaded and installed without the user's knowledge.

05

Can ransomware steal data

Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.



Protection Tips

Can ransomware be removed

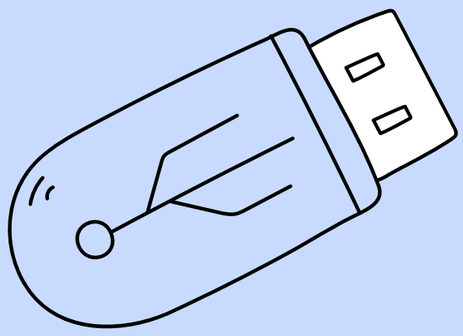
Ransomware sometimes deletes itself after it has infected a system. Other times, it stays on a device to infect other devices or files. Most antimalware and antiransomware software can quarantine and remove the malicious software.

Can antivirus detect ransomware

The best antivirus companies keep a catalog of all the known threats, so they can identify ransomware quickly and effectively. Some antivirus apps also provide a free ransomware decryption tool for malware with low-level encryption

How can ransomware attacks be prevented

Effective ransomware prevention requires a combination of good monitoring applications, frequent file backups, anti-malware software, and user training. Although no cyber-defenses reduce risk completely, you can greatly limit the chance attackers will be successful.



Stay safe

2022/23