

48.3%

The number of users attacked by encryption ransomware increased by 48.3% in 2015.*



HOW CAN YOU PREVENT A RANSOMWARE ATTACK?

Ransomware is the digital version of extortion. It's as simple as that. It uses age-old tactics to carry out a modern day crime, but the elements behind it are as old as human criminal activity itself.

* The Kaspersky Lab Security Bulletin Overall Statistics Report for 2015

10

SIMPLE TIPS TO PROTECT YOUR DATA FROM RANSOMWARE.

1

BACK UP YOUR FILES REGULARLY.

The only way to ensure that you can immediately handle a ransomware attack is to implement a regular backup schedule so that your company can get access to the files it needs without dealing with the cybercriminals. Your backup should have certain restrictions, such as read/write permissions without an opportunity to modify or delete the files.



CHECK YOUR BACKUPS.

There are times when something can damage your files. Be sure to check regularly that your backups are in good shape.

2

3

PROTECT AGAINST PHISHING ATTACKS.

Cybercriminals often distribute fake email messages that look like an official message from a vendor or bank, luring a user to click on a malicious link and download malware. Teach employees that they must never open attachments from an unknown sender or even suspicious attachments from a friend in case they have been hacked.



TRUST BUT VERIFY.

Malicious links can be sent by your friends or your colleagues whose accounts have been hacked. Let employees know that if they receive something out of the ordinary from a friend, they should call that person directly to verify that they sent it and find out if their accounts have been compromised.

4

5

ENABLE 'SHOW FILE EXTENSIONS' OPTION IN THE WINDOWS SETTINGS.

This will make it much easier to distinguish potentially malicious files. Because Trojans are programs, employees should be warned to stay away from file extensions like ".exe", ".vbs" and ".scr." Scammers could use several extensions to masquerade a malicious file as a video, photo, or a document.



REGULARLY UPDATE YOUR OPERATING SYSTEM

Cybercriminals tend to exploit vulnerabilities in software to compromise systems. With Kaspersky Lab's automated Vulnerability Assessment and Patch Management tools, you can rest assured that your system will be scanned and that patches will be distributed regularly in order to keep your system updated.

6

7

USE A ROBUST ANTIVIRUS PROGRAM

Protect your system from ransomware. Our Kaspersky Lab products employ a multi-layered system of defense that checks malware from many different angles to ensure that it does not corrupt your system.



BUT IF RANSOMWARE HITS...



CUT OFF YOUR INTERNET CONNECTION IMMEDIATELY.

If you discover ransomware, shut off your internet connection right away. If the ransomware did not manage to erase the encryption key from the computers in question, then there is still a chance you can restore your files.

8

9

DON'T PAY THE RANSOM.

If your files become encrypted, we do not recommend paying the ransom unless instant access to some of your files is critical. Each payment made helps the criminals to prosper and thrive to go on to build new strains of ransomware.



TRY TO IDENTIFY THE MALWARE

If you are hit by ransomware, try to find out the name of the malware. Older versions of ransomware used to be less advanced, so if it is an earlier version, you may be able to restore the files. Moreover, cybersecurity experts, including Kaspersky Lab experts, collaborate with law enforcement to provide file restoration tools and, hopefully, detain the adversaries. Some victims are able to decrypt the files without having to pay the ransom. To check whether that's possible, visit kaspersky.com

10