Ransomware - What is it? How Can we Protect Ourselves

Ransomware is a form of malicious software that threatens you with harm, usually by denying you access to your data. Ransomware attacks are often deployed via social engineering tactics.

You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware.

Most of the time, you don’t know your computer has been infected. You usually discover it when you can no longer access your data or you see computer messages letting you know about the attack and demanding ransom payments.

Ransomware attacks doubled in frequency in 2021 according to the Verizon Data Breach Investigation Report and from January to July 2021 the FBI reported a 62% increase in Ransomware complaints made to them.

Cybercriminals typically target businesses and governments in hopes they'll pay big bounties to release files and restore critical systems. But ransomware attacks happen to regular computer users, too.

- More than 90% of ransoms were paid in Bitcoin
- 3.4 Billion phishing emails are sent out every day !
- A new organization will fall victim to ransomware every 11 seconds
- 90% of Ransomware attacks come via email

What options do you have to recover your files other than paying?

Do you have duplicate files somewhere else, such as on a hard drive not connected to your computer?

Do you need the hijacked files or care if they are revealed?

Protection against ransomware – How to prevent an infection

- Never click on unsafe links
- Avoid disclosing personal information
- Do not open suspicious email attachments
- Never use unknown USB sticks
- Keep your programs and operating system up to date
- Use only known download sources
- Use VPN services on public Wi-Fi networks:

For more detailed information on this topic click on the button to visit our webpage dedicated to Ransomware

ransomware info