“My computer is infected. Now what?”

Ransomware encrypts files and/or denies access to a computer system or its data until money is paid—typically using bitcoin or other untraceable currency. It happens to both large and small businesses across all industries. Hackers aim for an amount that you are willing to pay and that makes for a quick turnaround.

So what should you do if you’re hit by ransomware?

- **Shutdown infected systems immediately.**

  Disconnect the infected device from any network it is on and turn off any wireless capabilities such as Wi-Fi or Bluetooth. Unplug any storage devices such as USB or external hard drives.

- **Determine the strain and the scope.**

  Ransomware usually identifies itself, so understanding which one it is can help in deciding how to remove it. Also, determine how many devices are infected, as well as what kind of data is encrypted.

- **Report the incident.**

  Your organization should know about the attack so it can be reported to the FBI or local authorities depending on your situation.

- **Evaluate your options.**

  No backup solution? Your other options are to lose your data or decrypt your files using third party decryption. Be aware that paying the ransom increases the chances that you will be targeted again.

- **Prevent ransomware attacks.**

  The first step in preventing ransomware attacks is to educate your employees on cybersecurity awareness. Also, invest in endpoint security with a firewall or third party service that protects against ransomware. Finally, get a business continuity plan. It can’t prevent an attack, but it can prevent it from succeeding!

Call JigsawTek to learn more!

JigsawTek
Big IT for Your Business