CYBERTECH360
SECURITY · MONITORING · MANAGEMENT

Ransomware

Keep thieves out of your pockets. Protect from ransomware attacks!

Ransomware attacks are among the most expensive and disruptive (and all-to-common) cyber threats today. When your system is infected by ransomware, malware encrypts your files making them inaccessible. Once compromised, cybercriminals demand payment in exchange for providing you the decryption key, freezing your systems until the ransom is paid. Production is lost and costing you until your files are recovered.

At CyberTech360, our first line of defense is prevention. Adding to that is our ransomware detection. With our Ransomware Detection feature. Our ransomware detection will alert us to take proactive steps that will minimize the ransomware impact.

Upon detection, Datto RMM notifies us immediately of the detection and attempts to terminate the ransomware process and isolate the infected device to prevent the ransomware from spreading. Ransomware detection within Datto RMM offers us the ability to isolate devices automatically, allowing technicians to take effective action to resolve the issue.

With Datto RMM's ransomware notifications, network isolation and rapid recovery through Datto Continuity, you'll be able to withstand a ransomware attack.

Follow us to the next page to learn how Cybertech360 can help you protect yourself from Ransomware, and how we can help you remediate your business if you have been ransomed.

Alleviate Your Aggravations

1-833-362-9237

CYBERTECH360

To protect against ransomware, businesses can take several preventative measures:

Regularly backing up data can help to ensure that critical data can be recovered in the event of a ransomware attack. Utilizing BCDR Backup solutions through Cybertech360 will help to keep that data safe.

Implementing security software: This can include firewalls, antivirus software, and intrusion detection systems. It's important to keep security software up to date and to regularly run scans to detect any potential threats. Cybertech360 can assist your business with our world-class partners in Security Software

Employees should be educated about the risks of ransomware and how to identify potential threats. They should also be trained on best practices for security, such as avoiding suspicious emails and websites. Cybertech360 has shared resources to keep you and your employees safe in a modern online world.

Enforcing access controls: Limiting access to sensitive data and systems can help to prevent unauthorized access by attackers. Cybertech360 checks privileged accounts and employee's security systems such as Threatlocker that keep the data available to only those who need it.

Regularly updating software and operating systems can help to prevent vulnerabilities that can be exploited by attackers.

Developing an incident response plan: In the event of a ransomware attack, having an incident response plan in place can help to ensure a quick and effective response to mitigate damage and restore operations.

Overall, preventing ransomware attacks requires a multi-layered approach - Cybertech360 can help you build these layers and implement these technologies into your business.

Alleviate Your Aggravations

1-833-362-9237

CYBERTECH360