Asigra.

Recovery is Everything™

Eight Surefire Ways to Prevent Ransomware From Damaging Your Business

Ransomware has compromised many organizations data by preventing access to encrypted critical business information, which directly impacts the business and its brand credibility. While backup and restoration services are essential elements to safeguard your data, it is just one of several safeguards within a multi-faceted approach needed to effectively mitigate the risk of ransomware. Below are eight tips to stay safe.

Keep abreast of the latest security threats and trends in the industry. Subscribe to blogs, join online communities, follow technical support sites and ensure staff is trained on privacy policies and procedures while keeping them up to date about generic do's and don'ts to stay safe.

Don't pay the ransom. Ransomware is very serious. The authorities should be notified (FBI, RCMP) immediately before any ransom is paid to the cybercriminal.

Use a good antivirus software. (Such as Norton, PCmatic, MacAfee, etc.) and enable firewall protections.

Make sure to have a pop-up blocker, or enable this feature in all browsers. That way, if a popup appears, click on the X in the right-hand corner, not the buttons within a popup. These have most likely been reprogrammed by the criminals.

Always air on the side of caution when doing things online. Security experts warn key attack vectors include: JavaScript attachments sent in spam email; unsolicited links; unexpected email attachments; and malware infected websites. Don't open email from unknown sources without first virus scanning. Don't click on unknown links or attachments, and use browsers that warn of malware infected websites.

Disconnect from the internet right away. Once ransomware is detected on a system, turn off/ disconnect from the internet and shut down the system preventing data from being sent back to the perpetrators. Assuming the system is backed up and the infection has not been, then the system can be recovered ransomware free.

Ensure that access and privileges to networks, files, drives and folders are limited to the bare minimum. Enables simpler permissions management while providing visibility into which users are accessing information and data at any given time.

Most importantly, always securely backup all systems! That means ensuring backups are free from ransomware infections, ransomware is prevented from deleting any backups, and passwords cannot be compromised.

Request a Demo: www.asigra.com