Adlumin

www.adlumin.com

6 QUICK TIPS TO PROTECT AGAINST RANSOMWARE

ADLUMIN, INC.

The cost of cybercrime damages is predicted to reach **$6 trillion** this year. One contributing factor? Ransomware. These attacks are increasing in frequency, victim losses are through the roof, and hackers target a wide variety of industries. In our latest blog **post**, we explored the basics and strengths of ransomware attacks, proving just how dangerous they can be to an individual or business. Going one step further, below are six quick tips to help your organization avoid the devastation that accompanies ransomware.

USE CAUTION WITH LINKS

When opening emails or scrolling through websites, beware of suspicious links. If the sender is not someone you are familiar with, or if the website appears to be untrustworthy, do not randomly start clicking. Malware is often hidden behind links or embedded within an attachment, which may direct you to a malicious site or infect your system.

VERIFY EMAIL / SENDERS

As stated by the **Cybersecurity & Infrastructure Security Agency (CISA)**, “if you are unsure whether or not an email is legitimate, try to verify the email’s legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.”

SAFEGUARD PERSONAL INFORMATION

Keep your data off unsecured websites. Make sure you include strong passwords and multi-step authentication factors to protect your information. This will give potential intruders more hurdles to jump through, making it harder to find an entry point to attack your network.

STAY INFORMED

Ransomware news and attacks are everywhere. Make sure that your organization is up to date with what’s happening inside the world of ransomware, so you can prepare and defend yourself appropriately.

INVEST IN DARK WEB MONITORING

Most ransomware attacks stem from stolen information leaked on the dark web. Investing in a security tool with a **Darknet Exposure Module** will allow your organization to extend defensive capabilities beyond your firewalls, endpoints, and security devices into Russian ID theft forums and the criminal underground. A module protects all domain accounts with automatic notifications and password resets if a business account is compromised.

TRAIN YOUR IT TEAM / EMPLOYEES

Organizations should provide cybersecurity **awareness training** to all employees, shining a more prominent light on ransomware. Your organization should consider incorporating mandatory cybersecurity awareness training into your IT team’s yearly roadmaps to improve workforce preparedness.

Often the underlining roadblock of staying steps ahead of cybercriminals is that you don’t know what you don’t know. These quick tips are significant indicators of protection and a blueprint to keeping your networks illuminated. Together, we can end this cyberwar with proper planning, protocol, and execution.