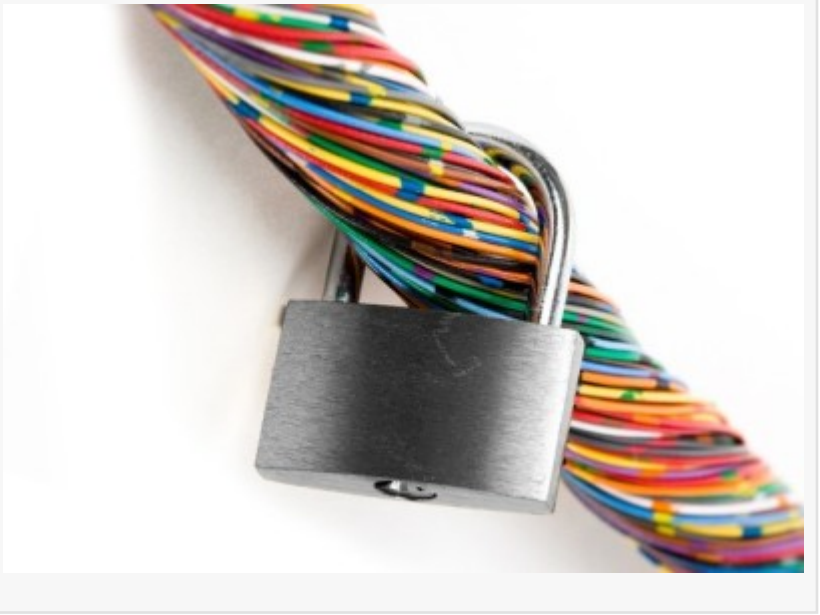
Quikteks Tech Support Offers Ransomware Mitigation Techniques

Quikteks Tech Support Offers Ransomware Mitigation Techniques



FAIRFIELD, NEW JERSEY, USA, April 24, 2019 /EINPresswire.com/ -- Quikteks Tech Support has seen an increasing number of ransomware cases over the past few years. According to the FBI's 2017 Internet Crime Report, the Internet Crime Complaint Center (IC3), received 1,783 ransomware complaints with losses exceeding $2.3 million. In the past, ransomware targeted random individuals; however, recent ransomware iterations have begun targeting specific organizations and their employees.

According to Quikteks Tech Support owner and CEO Andrew Rich, "In either case, employee education and ransomware mitigation is more important than ever."

With that in mind, Rich offers the following 5 ransomware mitigation techniques.

> If someone sends you a file you're not expecting, think twice about opening it."
>
> *Andrew Rich, CEO*

1. Raise Employee Awareness -- Ransomware often arrives via email attachments. infected websites, and downloads, making it crucial to educate employees about safe Internet practices. "If someone sends you a file you're not expecting, think twice about opening it," Rich said. "Always be suspicious."

2. Back Up Your Systems Regularly -- Having a good, current backup can get you out of a lot of binds. This is by far your best insurance against ransomware as having a bulletproof backup means you can get your data back without being extorted. Rich stresses the importance of disconnecting the backup from your systems so that ransomware can't infect the backup as well.

3. Put Up Code Execution Roadblocks -- One way to ensure that ransomware cannot encrypt your data is to put obstacles in its way. For example, if you use access control to restrict code execution, any ransomware that executes from temporary or data folders will not have appropriate access control, and thus, can't execute data encryption.

4. Terminate Default Admin Accounts and Restrict System Access -- Are you still using the default admin account to administer your system? According to Rich, that's just asking for trouble, especially because some ransomware carries out its mission by using the default system administrator account. If you don't have that account, the ransomware will have a much more

difficult time taking over your system.

5. Keep Your Computer Security Software Current -- Computer security and anti-malware software is a must, but keeping it current with the latest updates is essential. After all, as new ransomware variants are discovered, patches are released, protecting your system from new threats. However, if you don't update your software, you won't benefit from that protection.

For more complex malware mitigation efforts, please contact Quikteks Tech Support by visiting Quikteks.com or calling 973-882-4644.

About Quikteks Tech Support

Based in Fairfield, New Jersey, Quikteks Tech Support delivers cutting-edge, reliable and cost-effective business technology solutions to small and medium-sized businesses in the Tri-State area. The company's computer solutions include 24-hour tech support, help desk support, computer support, advising, and storing valuable and confidential data in a secure cloud.

For More Information:

Email: info@quikteks.com

Phone (973) 882-4644

Web: https://www.quikteks.com

Andrew Rich
Quikteks
9738824644x315
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
