A Four-Step Plan to Prevent Ransomware Attacks

Hackers are holding hospitals for ransom. Here's your four-step plan to stop them.

> Ransomware attacks encrypt your files and demand ransom for the decryption key. In some cases, hospitals have paid thousands of dollars to regain access to their data. To protect your data, Advisory Board experts recommend these common-sense steps.

STEP 1 >

Back up your data

Attackers are counting on your not having access to your data so you pay the ransom. Prove them wrong. Offline backups will allow you to make a quick recovery.

STEP 2 >

Limit system access

Cut down on your network's access points—such as servers and workstations. Ransomware can slip through any of these entry points to execute a successful attack.

STEP 3 >

Filter your email

Most ransomware arrives via email, so you should screen as many malicious messages as possible with special software designed to safely remove threats. Block attachment types that malware exploits, such as JavaScript extensions.

STEP 4 >

Keep a whitelist of websites and apps

A more radical option: Permit your computers to access only certain applications and websites that are known to be safe and secure.

The Advisory Board Company

Take the next step to protect your data: Check out our webconference, How to Discuss Cybersecurity with Your C-Suite and Board of Directors.