7 Steps to Protect Against Ransomware

STEP 1

Ensure All Systems are Up to Date and Properly Patched

- Make sure that all of your operating systems (for backend servers, desktops, laptops, cell phones, and other devices) are current and fully patched, as are all of your applications and related utilities—including things as innocuous seeming as printers, monitors, and any other devices that connect in any way to your network, including the full realm of the Internet of Things (IoT).

STEP 2

Restrict Remote Access

- Use Virtual Private Network (VPN) for remote access. A VPN enables users to create a secure connection between home devices and network resources. A VPN is especially important when using Wi-Fi connections.

STEP 3

Implement a Robust Backup & Disaster Recovery System

- There should be multiple backups, at multiple locations—including cloud-based resources, that cannot be touched by a ransomware attack. Backups should include a complete image of your infrastructure, to include all your applications.

STEP 4

Enforce Strong Password Policies

- Cannot reuse the last 12 passwords
- User's must change password every 60-90 days
- Minimum password length of 10 Characters
- Accounts will be locked for 5-miuntes if their password is entered incorrectly 5-times in a row
- Complex passwords require:
  - Cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters
  - Must contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Numbers (0 through 9)
    - Non-alphabetic characters
    - ` ~ ! @ # $ % ^ & *

STEP 5

Encrypt Your Data in Motion and At Rest

- Data should be encrypted before it is transmitted to each backup resource and remain encrypted until needed. That way, if it is intercepted en route, or hacked into while in storage, there is nothing for the hacker to steal.

STEP 6

Educate All Employees on Social Engineering Attacks (aka Don't click that link)

- All it takes is one user clicking on an e-mail link or on a phony pop-up screen telling them they have been attacked by a virus and instructing them to click a button to undo it . . . or instructing them to click to update software, or for a spectrum of other reasons. Phishing, and the more finely tuned spear phishing, attacks can also come via text messages, or through phone calls.

STEP 7

Find a Business Partner for Your IT Security Needs

CALL US

COMPUTER BUSINESS CONSULTANTS, INC.

407-654-5600

www.computerbusiness.com