A QUICK GUIDE TO STOPPING RANSOMWARE

1. Deploya Reputable, Multi-Vector Endpoint Security
   - Protects against threats from multiple vectors.
   - Includes next-generation endpoint protection, anti-malware, anti-ransomware, and more.

2. Deploy Backup and Business Continuity Recovery
   - Back up important data regularly to minimize data loss.
   - Test your backup and recovery processes to ensure they are working effectively.

3. Disable Macros and AutoRun
   - Many ransomware attacks are delivered through macros in Microsoft Office documents.
   - Disable AutoRun for removable drives to prevent ransomware from spreading.

4. Create Strong Windows Policies
   - Implement strong password policies, including complexity and expiration requirements.
   - Use multi-factor authentication for added security.

5. Centralized Management
   - Use centralized management solutions to remotely manage and secure networked devices.
   - Ensure that all devices are up-to-date with the latest security patches.

6. Have a Second Browser
   - Use a second browser, such as Firefox, when accessing sensitive information.
   - This can help prevent ransomware from infecting your primary browser.

7. Use Policies to Block Volume Shadow Copy Service
   - Block the Volume Shadow Copy Service to prevent ransomware from creating hidden copies of data.
   - This can help prevent ransomware from encrypting your data.

8. Disable Windows Script Hosting
   - Disable Windows Script Hosting to prevent the execution of scripts that could be used by ransomware.
   - This can help prevent ransomware from being able to execute scripts on your system.

9. Educate Users
   - Train employees on recognizing and avoiding common ransomware techniques.
   - Encourage employees to report suspicious activity immediately.

FIVE GENERAL TIPS

- Keep your software and systems up-to-date with the latest security patches.
- Use strong, unique passwords and enable two-factor authentication.
- Regularly back up important data to prevent data loss.
- Educate yourself and your employees on the latest ransomware threats.
- Test your disaster recovery and business continuity plans regularly.