

- Perform a risk assessment to identify any high-level easy targets
- Perform a network vulnerability test
- Train your users how to identify malware in email and links
- Control your administrative access accounts and passwords
- Use antivirus to scan at regular intervals
- Use patch management to keep computers up to date
- Review the benefits of new firewalls and blocking traffic
- Put spam filters in place and review them
- Restrict the use of personal software not approved by the company
- Disable RDP
- Setup Whitelists:
 - Application
 - Protocol
 - Endpoints
 - Destinations
- Make a plan to review and update the security plan to keep up with new threats



For a FREE consultation with InclusiveTech's I.T. Ninjas

CALL (424) 258-0288

www.inclusivetech.net