Small Business Cybersecurity Guide

Account Security

- Use strong, unique passwords for all users.
- Enable multi-factor authentication (MFA) on all critical systems.
- Implement a password manager across the organization.

Device & Network Security

- Ensure all company devices have updated antivirus/EDR software.
- Keep operating systems and apps fully patched.
- Secure office Wi-Fi with WPA3 and a strong password.
- Separate guest Wi-Fi from the internal network.

Data Protection

- Perform and test regular backups.
- Encrypt sensitive data at rest and in transit.
- Implement access controls for cloud accounts (e.g., least privilege).

Employee Awareness

- Conduct security awareness training at least annually.
- Perform regular phishing simulations.
- Establish clear policies for handling sensitive information.

Incident Readiness

- Have an incident response plan in place.
- Ensure staff knows who to contact in case of a breach.
- Log and review security incidents.

Policy & Compliance

- Distribute and have employees sign the Acceptable Use Policy.
- Implement and communicate a data privacy policy.
- Identify regulatory compliance requirements (HIPAA, PCI, etc.).

📍 Based in Wichita, KS — Serving Small Businesses in the Greater Wichita Area