7 CYBERSECURITY TIPS

you can use to help protect your businesses

FIREWALL SECURITY

Monitor incoming and outgoing traffic on your network. Set security standards to prevent outsiders from accessing your data.

BACKUP BUSINESS DATA

Ensure all critical data is backed up daily and stored offsite (databases, accounts payable/receivable files, human resource files, spreadsheets) in the event of a ransomware attack.

LIMIT AUTHORITY

Employees should only be given access to the systems and data they need to perform their jobs. Don't allow software installation without permission.

PASSWORD MANAGEMENT

Change passwords every 3 months, require unique passwords over 8 characters long, and consider implementing multi-factor authentication to gain entry to systems.

EMPLOYEE TRAINING

Establish security protocols for identifying and reporting possible security threats. Provide education and protocols for handling customer and sensitive data.

ASSET PROTECTION

Install updates as soon as they are available. The latest security software, web browser, and operating system are the best defense against viruses, malware, and online threats.

CONTROL PHYSICAL ACCESS

Prevent the use of company devices by unauthorized personnel. Create separate accounts for each employee and lock unattended devices.

PROTECT YOUR BUSINESS AND STRENGTHEN YOUR SECURITY POSTURE