CYBERSECURITY BEST PRACTICES

Regardless of your business size, cybersecurity should always be top of mind.
Cyber threats can come from any level of your organization and can be devastating to unprotected businesses.
To help you avoid becoming another cybercrime statistic, we've gathered our top cybersecurity best practices.

- Passwords and usernames for business account logins (logins for computers, websites, and software) should never be shared.
- Require employees to use unique passwords with a mix of numbers, symbols, and capital and lower-case letters. Employees should also be required to change passwords at least every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry.
- Wi-Fi network should be password protected and the router password should be updated from the default.
- Employee accounts should be periodically reviewed for accuracy and immediately disabled upon employee termination.
- Reduce vulnerability by ensuring that networks are protected by up-to-date firewall and antivirus.
- Outdated computer hardware may not support the most recent software security upgrades and old hardware makes it slower to respond to cyber-attacks. Make sure to use computer hardware that's more up-to-date.
- Software companies typically provide software updates for three reasons: to add new features, fix known bugs and upgrade security. Always update to the latest version of software to better protect against new or existing security vulnerabilities.
- External storage devices are just as prone to malware as internal storage devices. Always scan external devices for malware before accessing them.
- Perform backups of operationally necessary business data. Hackers thrive on disrupting an organization's activities. An offline backup enables your business to continue while cybersecurity experts deal with damage from a cyberattack.
- Properly shred documents that contain confidential customer/business information.
- If required to retain physical documentation containing confidential customer/business information, it should be stored in a secure location such as a locked filing cabinet.
- If required to retain electronic documentation containing confidential customer information, it should be kept on an encrypted storage device that cannot be accessed by unauthorized users.
- Any sensitive customer/business information being sent to external parties should be sent utilizing an encrypted format.
- The key to making cybersecurity work is to make sure your employees are well trained and are exercising security best practices. Employee Security Awareness Training and Education (SATE) Program is a great way to instill the knowledge and confidence in employees to recognize security threats.