Cyber Security — Best Practices Checklist

Hackers increasingly target small- and mid-sized businesses with fewer data security resources. Complete the following checklist for a quick assessment of critical cyber security best practices for your business.

Topic	Assessment
Cyber Event Preparation	☐ Written cyber security and incident response plan reviewed with all employees
Multi-Factor Authorization (MFA)	☐ Required for remote network access ☐ Required for any key financial and customer information access
Employee Training	☐ Active and consistent employee cyber security awareness training
Secure Email/Encryption	☐ Using secure email when sending sensitive information, billing and/or contracts.
Money Transfer and Banking	☐ Confirms all emailed invoices against previous statements and contacts accounts payable to confirm changes ☐ Does not accept any emailed changes to bank or routing numbers without verbal confirmation
Data Backup	☐ Off network backup of key financial and customer data ☐ Minimum once per week, preferably every day
Firewall	☐ Using network firewall to prevent malicious network traffic
Passwords	☐ Using password manager for any computer network access
Website Security	☐ "Bookmarks" commonly used financial (i.e. banking, credit card) and vendor websites ☐ Employees recognize/use only Hypertext Transfer Protocol Secure (HTTPS) sites
Information Security	☐ Limits gathering of unnecessary customer information (e.g. SSN) or keeping customer credit card information ☐ Limits employee access to financial/customer information
Wireless Security	☐ Using WPA2 encryption ☐ Not using company name for network ID (SSID) ☐ Wireless router set to automatically take software updates
Software Security	☐ Using anti-virus software, spam/phishing filters ☐ Computers set to automatically take updates
Physical Security	☐ Sensitive documents, thumb drives and backups stored in secure filing cabinet/safe ☐ Encryption enabled on mobile devices ☐ Remote "wipe" of mobile devices enabled