Cybersecurity Plan Checklist

Component	Considerations	Notes
Secured network	• Encrypt your information. • Use a firewall. • Make your Wi-Fi network secure and hidden. • Password-protect access to the router. • Use a Virtual Private Network (VPN) for employees to use working remotely.	
Antivirus program	• Use a reputable, paid antivirus program. Free programs can be unreliable and may not be regularly updated. • Configure to automatically install updates.	
Multi-factor authentication (MFA)	• MFA requires a unique, time-sensitive action or code after the user enters their username and password. • Take advantage of vendor-provided MFAs for different services such as banks, payroll processing, etc. • Retain an MFA service provider for your systems.	
Secured payment processing	• Work with your bank and card processors to ensure you're using highly-validated tools and anti-fraud services. • Isolate payment systems from other systems, i.e., use a dedicated computer that is only used to process payments.	
Controlled physical access	• Provide each employee with a unique user account. • Require strong passwords for account access. • Limit administrative access to IT staff and/or key personnel. • Make sure all digital devices are secured when not in use, whether in or away from the office. • Promptly deactivate the user accounts of exiting employees, and make sure they relinquish all company devices before departing.	
Controlled data access	• Store sensitive data on an external hard drive that is maintained in a secure, restricted-access location. • Designate an administrator for cloud storage platforms used, such as Google Drive, DropBox, etc. • Promptly deactivate access to cloud platforms by exiting employees.	
Up-to-date digital tools	• Routinely monitor and update operating systems, web browsers, antivirus software, firewalls, and all other systems used in your business. • Set systems and programs to auto-update.	