CYBER SECURITY CHECKLIST

KEY: NO Haven't Started Yet OK Started But Not Finished YES Yes, It's Finished & Done!

Using the table below and overleaf, tick the column that best represents the work you have done in each area...

	QUESTION	NO	OK	YES
1	Turn on automatic updates on all staff devices, browsers, and business software.			
2	Enable MFA (Multi-Factor Authentication) on key accounts like email, banking, file storage, and CRMs			
3	Install and set up a password manager (e.g. Bitwarden, LastPass) and train staff to use unique, strong passwords.			
4	Schedule automatic backups to both cloud storage and a separate offline device			
5	Review and update device security settings — ensure screen locks, encryption, and secure remote access are enabled.			
6	Print or distribute the '7 Red Flags of a Scam Email' as a visual guide or poster in the office.			
7	Add a recurring 10-minute cyber briefing to team meetings (monthly or quarterly) to keep awareness fresh.			
8	Create or update your payment verification policy — require verbal confirmation of any changes to bank details using trusted contact info.			
9	Write down your cyber incident response steps — who to call, where to report, what to lock down — and save it where your team can access it.			

BusinessBlueprint®