Secure A Small Business Email System

Plain-English how-to. ~45 minutes. Covers Google Workspace, Microsoft 365, and your own domain.

Lock down Google Workspace / Microsoft 365 with MFA, SPF/DKIM/DMARC, anti-phishing, and audit.
Print, share, and re-run quarterly.

Do This Right Now

#	STEP
1.	Enforce MFA on every account, no exceptions.
2.	Set up SPF, DKIM, and DMARC.
3.	Move DMARC from p=quarantine to p=reject over a month.
4.	Enable anti-phishing on the email platform.
5.	Publish an out-of-band payment verification policy.
6.	Turn on mailbox audit logging.
7.	Test SPF/DKIM/DMARC with MXToolbox.
8.	Quarterly phishing training + DNS audit.

Why This Matters

- Email is the most common entry point for attacks on small businesses. The FBI reports BEC accounts for the largest financial loss cat
- Common BEC patterns: attacker compromises a vendor's email, then sends 'updated wire instructions' to your AP team. The money g
- The good news: nearly every BEC attack is preventable with the standard email security stack — MFA, SPF/DKIM/DMARC, training, a