CICADA | RESOURCES

IDENTITY · 10 MIN · ESSENTIAL · UPDATED NOVEMBER 2026

Turn on MFA for the accounts that matter

Multi-factor authentication is the highest-value ten minutes in small business security. Start with email, then money, then admin.

The short version

- ✓ MFA stops most account takeover even after a password leaks.
- ✓ Email first: it is the reset route for almost everything else.
- ✓ An authenticator app or passkey beats SMS; SMS still beats nothing.
- ✓ Save recovery codes offline and nominate a second admin.

Why email comes first

Your email address is the master key. Password resets for banking, accounting, payroll, social media and your domain all arrive there. If someone can read your inbox, they can usually take over everything else without ever guessing another password.

MFA means a password alone is no longer enough. After the password, the service asks for a second proof: a code from an app, a passkey, a hardware key, or a prompt on your phone.

Do it in this order

01 **Email.** Microsoft 365, Google Workspace, or your hosting provider. Enforce MFA for every user, not just the owner.

02 **Money.** Online banking, accounting software, payroll and payment platforms.

03 **Admin.** Domain registrar, website, social accounts, password manager and remote access.

04 **Everything else.** Any tool that holds customer data or can send email as your business.

Most providers have a bulk switch: Microsoft 365 has Security Defaults or per-user MFA; Google Workspace has 2-Step Verification enforcement. Turn it on for the whole tenant rather than asking people nicely.

Choose the right second factor

Best to worst, in practice:

- **Passkeys**: phishing-resistant, tied to the device, no code to read out.
- **Authenticator app**: a rotating code in Microsoft Authenticator, Google Authenticator, 1Password or similar.
- **Hardware security key**: excellent for owners and admins; keep one spare.
- **SMS**: better than nothing, but vulnerable to SIM swap and interception.

Turn on **number matching** if your provider offers it. It defeats MFA fatigue, where an attacker spams prompts until someone taps approve.

Roll it out without locking yourself out

Before enforcing, make sure at least two people can administer the account. Save recovery codes somewhere offline. A printed sheet in the safe is fine. Register a second device for the owner. Then enforce, and check the sign-in logs for anyone still using a password alone.

> NEVER
>
> No legitimate IT person, bank or software provider will ask you to read out a code or approve a login you didn't start. Make that a rule everyone knows.

Action checklist

- [ ] MFA enforced for every email account
- [ ] MFA on banking, accounting and payroll
- [ ] MFA on domain, website and social admin
- [ ] Recovery codes printed and stored offline
- [ ] Two people can administer each critical service
- [ ] Staff know never to share a code or approve an unexpected prompt

0 of 6 done