BUSINESS EMAIL

How To Secure A Small Business Email System

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

If a single employee email account is compromised in a small business, the damage cascades fast: payroll fraud, fake invoices sent to your customers, wire-transfer redirection, and customer data exposure. Business Email Compromise (BEC) cost US businesses over $2.9 billion in a recent FBI IC3 report — more than ransomware and credit card fraud combined.

Most small businesses run on Google Workspace or Microsoft 365 with default settings. Both platforms include enterprise-grade security tools, but the defaults assume a generic user. Enabling the right settings — MFA on every account, SPF/DKIM/DMARC, anti-phishing rules, and quarterly audits — is what turns 'using Google Workspace' into 'actually secure.'

By the end of this guide your business email will have enforced MFA, properly configured email authentication, anti-phishing rules, and a tested incident-response plan. It takes about 45 minutes and is the single highest-impact security work you can do for a small business.

Quick snapshot

What you'll learn	Lock down Google Workspace / Microsoft 365 with MFA, SPF/DKIM/DMARC, anti-phishing, and audit.
Skill level	Intermediate · Owner / IT lead
Time required	45 minutes
What you'll need	Admin access to your email platform, your domain registrar login
Risk if you skip this	Business email compromise, wire fraud, customer data exposure
PDF kit	■ Download at the bottom of this page

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 category in cybercrime — average loss per incident is over $130,000.

Common BEC patterns: attacker compromises a vendor's email, then sends 'updated wire instructions' to your AP team. The money goes to the attacker's account instead of the real vendor. Without DMARC and MFA, this is alarmingly easy.

The good news: nearly every BEC attack is preventable with the standard email security stack — MFA, SPF/DKIM/DMARC, training, and an out-of-band verification habit for any payment changes.

Before you start

Inventory your accounts. How many active email accounts does your business have? Make a list — admins, employees, shared inboxes, automation accounts. Each needs review.

Have admin access to your email platform (Google Workspace Admin Console or Microsoft 365 Admin Center).

Have access to your domain's DNS settings (where your domain is registered — GoDaddy, Cloudflare, Namecheap, etc.). You'll add SPF/DKIM/DMARC records there.

Step 1 — Enforce MFA on every account (no exceptions)

Google Workspace: **Admin Console** → **Security** → **Authentication** → **2-Step Verification** → **Allow users to turn on 2-Step Verification: ON**, then **Enforcement: ON for everyone**. Microsoft 365: **Admin Center** → **Active Users** → **Multi-factor authentication** → **Service Settings** → **Enable for all users**.

Push everyone to use authenticator app (Microsoft Authenticator or Google Authenticator), not SMS. SMS is fine as a backup, not as primary.

Step 2 — Set up SPF (Sender Policy Framework)

SPF tells receiving servers which IPs are allowed to send mail from your domain. Without it, anyone can spoof your domain. Add a TXT record at your DNS provider:

Google: v=spf1 include:_spf.google.com ~all. Microsoft 365: v=spf1 include:spf.protection.outlook.com -all. Save and wait for DNS propagation (up to 48h).

Step 3 — Set up DKIM (DomainKeys Identified Mail)

DKIM cryptographically signs your outbound emails so receivers can verify they're really from you. Generate the DKIM record in your platform's admin panel, then publish the resulting TXT record at your DNS provider.

Google: **Admin Console** → **Apps** → **Google Workspace** → **Gmail** → **Authenticate email** → **Generate new record** → **Start authentication**. Microsoft 365: **Defender** → **Email & Collaboration** → **Policies** → **DKIM**.

Step 4 — Set up DMARC (final piece)

DMARC tells receiving servers what to do if SPF or DKIM fails — and reports it to you. Add a TXT record at _dmarc.yourdomain.com:

v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@yourdomain.com; sp=quarantine; pct=100. Start with p=quarantine for a month, watch reports, then move to p=reject.

Step 5 — Enable advanced anti-phishing on the platform

Google Workspace: **Admin Console** → **Apps** → **Gmail** → **Safety**. Turn on **Spoofing & authentication** protections (employee name, similar domain, unauthenticated emails). Turn on **Attachments** protections (anomalous attachment scanning).

Microsoft 365: **Defender** → **Email & Collaboration** → **Policies** → **Anti-phishing** → **Office365 anti-phish policy**. Add VIP names (CEO, CFO, etc.) to mailbox impersonation protection.

Step 6 — Set up an out-of-band payment verification rule

Write and publish an internal policy: **'Any wire instructions or payment changes must be verbally confirmed via a known phone number before processing.'** Not via reply email. Not via the number in the email signature.

BEC fraud stops here. This single policy prevents the majority of business email compromise losses. Train every person who handles payments.

Step 7 — Configure mailbox audit logging

Google Workspace: audit logs are on by default. Microsoft 365: **Purview Compliance Portal** → **Audit** → **Start recording user and admin activity**.

Logs let you investigate after the fact — what mail rules an attacker created, which messages were read, which were deleted. Critical for incident response.

Step 8 — Test your setup with a spoofing tool

Use **mxtoolbox.com/SuperTool.aspx** or **dmarcian.com** to verify your SPF, DKIM, and DMARC records are correct. Most issues here are typos in DNS — easy to fix.

Send a test email from your domain to a Gmail account, then click 'Show original' to see SPF/DKIM/DMARC pass status. All three should show 'PASS.'

PRO TIP

DMARC Is The Whole Game.

SPF + DKIM alone don't stop spoofing — only DMARC tells receivers what to do.

Start with p=quarantine for a month, watch reports, then go to p=reject.

Use a dedicated reporting address (dmarc-reports@yourdomain).

Free DMARC report tools: dmarcian, Postmark, MXToolbox.

If you want to go further: power-user upgrades

Power-user upgrade #1 — Issue FIDO2 hardware keys to admins

Owners and IT admins are the highest-value targets. Hardware keys eliminate phishing of these accounts entirely.

Trade-off: ~$30/key plus deployment.

Power-user upgrade #2 — Set up conditional access policies

Google: Context-Aware Access. Microsoft: Conditional Access. Block sign-ins from unexpected countries/devices.

Trade-off: requires planning to avoid blocking legitimate travel.

Power-user upgrade #3 — Enable Mail Routing audit + alert

Both platforms can alert when a user creates an inbox rule that forwards external. Common attacker move.

Trade-off: occasional false-positive alerts.

Power-user upgrade #4 — Implement an SPF flattening tool

Tools like EasyDMARC or Valimail keep your SPF under the 10-lookup limit even with many services.

Trade-off: subscription cost.

Power-user upgrade #5 — Use BIMI for brand-verified email

After DMARC enforcement, BIMI shows your logo next to your messages in supporting clients (Gmail, Apple Mail).

Trade-off: requires Verified Mark Certificate (~$1k/year).

Power-user upgrade #6 — Quarterly phishing simulation

Tools like KnowBe4 send simulated phishing to your team. Tracks who clicks and adjusts training.

Trade-off: subscription cost.

Common mistakes & pitfalls

Mistake — Trusting 'voice authentication' from a known number.

Fix — Voice deepfakes now mimic owners. Out-of-band verbal verification via a previously-known number, every time.

Mistake — Setting DMARC to p=none and forgetting.

Fix — p=none is informational only. Move to quarantine, then reject.

Mistake — Leaving MFA optional.

Fix — One unprotected account is a beachhead. Enforced for all, no exceptions.

Mistake — Skipping audit logs.

Fix — Without them, breach investigation is guesswork.

Mistake — No payment change verification policy.

Fix — BEC fraud relies on this gap. Close it with a written rule.

Mistake — Allowing SMS as primary 2FA on admin accounts.

Fix — SIM-swap attacks bypass SMS. Authenticator app or hardware key for admins.

Mistake — Inheriting an old domain's DNS without auditing.

Fix — Old SPF records from prior services let spoofers slip through.

Pro tips

Pro tip 1. Subscribe to DMARC reports weekly — they show every domain trying to spoof you.

Pro tip 2. Train the team: 'If anyone asks about money via email, verify by phone.' Repeat quarterly.

Pro tip 3. Use group aliases (accounts@) instead of personal addresses for payment communications — easier to monitor.

Pro tip 4. Set up alerts for inbox forwarding rules — most BEC attacks start by setting up a hidden forward.

Pro tip 5. Run a quarterly DNS audit — make sure no stale SPF includes remain.

Frequently asked questions

Will DMARC p=reject block legitimate mail?

Only if you haven't covered every legitimate sender via SPF/DKIM. That's why you start with p=quarantine, watch reports, then move to reject.

Can my domain registrar handle SPF/DKIM/DMARC?

Yes — these are just TXT records in DNS. Every registrar (GoDaddy, Cloudflare, Namecheap, Squarespace) supports adding TXT records.

How long until DMARC reports start coming in?

Within 24 hours of correct setup. You'll get one daily report per receiving domain (Google, Microsoft, Yahoo, etc.) showing how many messages passed/failed.

What if I use a third-party service to send email (Mailchimp, Stripe, HubSpot)?

Add their SPF includes to your record and configure DKIM via their domain verification. They publish setup guides.

Is Microsoft 365 'Defender for Office 365' worth the upgrade?

For most small businesses, yes — Plan 1 ($2/user/month) adds Safe Links and Safe Attachments which catch a lot of phishing.

How do I train employees without buying KnowBe4?

Run a quarterly 30-minute in-house session: real examples of recent phishing, your payment verification policy, and a phishing-report workflow.

What's the difference between BEC and phishing?

BEC is targeted phishing aimed at extracting money from a business. Phishing is broader (any credential theft attempt).

Quick recap — do these in order

DO THIS RIGHT NOW

The 8-step recap.

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.

Mini glossary

SPF: DNS record listing which IPs may send mail from your domain.

DKIM: Cryptographic signature on your outbound mail.

DMARC: Policy that tells receivers what to do if SPF/DKIM fails.

BEC: Business Email Compromise — wire fraud via compromised email.

MFA: Multi-factor authentication.

BIMI: Brand Indicators for Message Identification — your logo in inbox.