Business Email Setup and Configuration

Choosing a platform, setting up mailboxes, connecting devices, SPF, DKIM and DMARC, and fixing email that lands in spam.

Updated November 2026 · for small businesses

1. Choosing a platform

	Email with web hosting (cPanel)	Microsoft 365	Google Workspace
Best for	One to ten people who mainly need mailboxes, on a low budget.	Offices that live in Word, Excel and Outlook, or need Teams and shared calendars.	Teams that like Gmail, Docs and Meet, or work mostly in a browser.
Delivery	Good when set up correctly, but the server is shared, so its reputation matters.	Very good.	Very good.
Security	Strong passwords only. No built-in two-step login for mailboxes.	Two-step login, admin and device controls.	Two-step login, admin and device controls.
Cost	Included with hosting. Contact us for pricing.	Per user, per month. Contact us for pricing.	Per user, per month. Contact us for pricing.

Rule for all three: a domain delivers its mail to one place. When you change platform, the MX records change and old mail must be copied across. Plan the switch for a quiet time and keep the old mailboxes until the new ones are checked. Your email addresses do not change.

2. Mailboxes, aliases and forwarding

- **One mailbox per person.** Shared logins hide who did what and make leavers hard to remove.
- **Use aliases for roles.** info@, sales@ and accounts@ can deliver into one or two real mailboxes.
- **Be careful with forwarding** to personal Gmail or Outlook.com addresses: it can break authentication and send mail to spam.
- **Set mailbox size limits** and archive old mail every year. A full mailbox bounces mail.

3. Connecting phones and computers

Use **IMAP**: mail stays on the server and every device shows the same folders. POP downloads to one device and is only worth using when one computer is the only place mail is read.

Setting	Value (check your own control panel)
Username	The full address, e.g. name@yourbusiness.co.za
Incoming (IMAP)	mail.yourbusiness.co.za, port **993**, SSL/TLS
Outgoing (SMTP)	mail.yourbusiness.co.za, port **465** SSL/TLS, or **587** STARTTLS
Outgoing authentication	Required, same username and password
POP3 (only if needed)	Port **995**, SSL/TLS

If a device will not connect

- Username is not the full address.
- Wrong port or security type (993 needs SSL/TLS).
- Outgoing fails but incoming works: authentication is off, or port 25 is blocked. Use 465 or 587.
- Certificate warning: use the server name your host gives you, not the bare domain.
- Worked yesterday: check for a changed password, a full mailbox or a lapsed domain.

Gmail: Google is removing Gmail's "Check mail from other accounts" (POP) feature. Existing setups keep working for now, but new ones are no longer supported. Add the mailbox to the Gmail app on your phone (IMAP) or use a mail program such as Thunderbird or Outlook.

4. SPF, DKIM and DMARC in plain English

These three DNS records let Gmail, Outlook.com and others check that mail really came from you.

Record	What it does	Comparison
SPF	Lists the servers allowed to send mail for your domain.	A guest list at the door.
DKIM	Signs each message so it cannot be changed unseen.	A tamper-proof seal.
DMARC	Says what to do when SPF and DKIM fail, and sends you reports.	Instructions to the doorman.

Gmail expects everyone who sends mail to Gmail addresses to authenticate it, and larger senders (about 5,000 messages a day or more) must have SPF, DKIM and DMARC. Outlook.com has had similar rules for large senders since May 2025. Having all three in place protects your genuine mail and stops others forging your address.

Checking in cPanel

Open **Email** → **Email Deliverability**. Each domain shows the state of its mail records. **Repair** installs a suggested record; **Manage** shows DKIM, SPF, DMARC and reverse DNS. If your DNS is held elsewhere (your registrar or Cloudflare), Repair will not work: copy the suggested records to where the DNS is managed. Install DMARC last. With Microsoft 365 or Google Workspace, use their own instructions and switch DKIM on in their admin portal.

Examples only: use the values from your own control panel

```
SPF  (TXT on the domain):  v=spf1 +mx +a ~all
```

```
DMARC (TXT named _dmarc):  v=DMARC1; p=none; rua=mailto:dmarc@yourbusiness.co.za
```

- A domain can have **only one** SPF record; two make SPF fail. Several services are combined with include: entries.
- ~all means treat other senders as suspicious; -all means reject them. Start with ~all.
- SPF allows at most ten DNS lookups. Many mail services can quietly exceed that.

Rolling out DMARC safely

- ☐ Confirm SPF and DKIM pass for your own mail first.
- ☐ Start with p=none. Nothing is blocked and you receive reports.
- ☐ List every genuine sender: newsletter tools, invoicing software, website forms and voicemail-to-email.
- ☐ After a few weeks of clean reports, move to p=quarantine, then p=reject.

5. Why email lands in spam

Work through these in order. The first three fix most cases.

Check	What to look for	What to do
Authentication	Send a test to Gmail, choose Show original: SPF, DKIM and DMARC should all say PASS.	Fix the failing record. SPF fail: a sender is missing. DKIM fail: DKIM is not switched on.
Reverse DNS (PTR)	The sending IP should resolve to a sensible matching name.	Set by whoever controls the IP, usually your host.
Blacklists	On shared hosting, another customer’s abuse can list the whole server.	Check the IP on a blacklist checker; contact your host.
Content	Image-only messages, shortened links, .zip or .exe attachments.	Send normal text with links to your real site.
Volume	A new or quiet domain suddenly sending a lot.	Build up gradually; use a newsletter service for bulk mail.
Hacked mailbox	Bounces for mail you never sent, or a host warning.	Change the password, remove unknown forwarders, ask us to check.

6. Security and housekeeping

- ☐ Long, unique passwords for every mailbox (a password manager helps).
- ☐ Two-step login on Microsoft 365 and Google Workspace, starting with the owner and accounts.
- ☐ Confirm bank-detail changes by phone. Most email fraud is a convincing message, not a technical attack.
- ☐ Check forwarders and filters now and then; attackers add hidden forwarders.

- ☐ When staff leave: change the password, forward their mail for a while, then close the mailbox.
- ☐ Email is not a backup. Keep a separate copy of important mail.
- ☐ Keep the domain renewed, with a contact email you can reach.

7. How we set it up

- ☐ **Talk it through:** people, devices, what you use today.
- ☐ **Choose the platform** and agree it. Contact us for pricing.
- ☐ **Prepare:** we need access to your domain’s DNS, a list of mailboxes and aliases, and access to old mailboxes if moving.
- ☐ **Build and migrate:** mailboxes, old mail and DNS records including SPF, DKIM and DMARC.
- ☐ **Connect devices** and test, including a test to Gmail and Outlook.com.
- ☐ **Check and hand over:** confirm authentication passes and leave a one-page summary.

> **Email in trouble?** Mail in spam, devices that will not connect or a mailbox that keeps filling up: send us a short description and a screenshot of the error. Afridyne Systems helps Helderberg businesses with email setup, migration and clean-up. Call or WhatsApp 062 509 8065, or visit afridyne.co.za.