# Email Deliverability: 4-Week Warm-Up Protocol

Successfully scaling email campaigns requires a methodical approach to IP and domain warming. This protocol guides you through progressive volume increases while maintaining strong engagement metrics and sender reputation.

Follow these benchmarks to achieve optimal inbox placement and minimize deliverability issues.

# Progressive Volume Scaling: Your 4-Week Roadmap

Building sender reputation requires patience and precision. This warm-up schedule balances aggressive scaling with engagement quality, ensuring ISPs recognize your domain as a legitimate sender. Each week targets specific engagement thresholds before advancing to the next tier.

| Week | Daily Volume | Open Rate Target | Recipient Tier |
|---|---|---|---|
| Week 1 | 50-100/day | >30% | Tier 1 only |
| Week 2 | 400-800/day | >25% | + Tier 2 |
| Week 3 | 2,000-4,000/day | >22% | + Tier 3 |
| Week 4 | 8,000-10,000/day | >20% | Full scale |

**Critical Success Factor:** Only advance to the next week if you meet or exceed the open rate target for three consecutive days. Tier 1 should consist of your most engaged subscribers, those who have opened or clicked within the past 30 days. This ensures strong early signals to ISPs that your mail is wanted.

# Daily Monitoring & Emergency Response

## Daily Health Metrics

Monitor these KPIs every morning before sending. Any metric falling outside acceptable ranges requires immediate investigation and potential volume reduction.

- **Open rate:** Must maintain >20%
- **Click rate:** Target >2%
- **Hard bounce rate:** Keep <0.5%
- **Spam complaints:** Critical threshold <0.10%
- **Mail-Tester score:** Minimum 8/10
- **Google Postmaster:** GREEN status required
- **DMARC alignment:** Maintain >95%

## Emergency Protocols

### ⚠️ High Spam Complaints (>0.3%)

1. Stop all sending immediately
2. Check Google Postmaster for domain reputation issues
3. Review recent campaign content for spam triggers
4. Resume at 50% volume after 48-hour cooldown

### ⚠️ Elevated Hard Bounces (>0.5%)

1. Verify entire list using ZeroBounce or NeverBounce
2. Remove ALL invalid addresses immediately
3. Reduce volume by 70% for 5-7 days
4. Investigate list hygiene practices

Quick action on these red flags prevents long-term reputation damage. A single day of poor metrics can take weeks to recover from, so err on the side of caution when you see warning signs.

# Authentication Foundation: Pre-Launch Checklist

Proper authentication is non-negotiable for modern email deliverability. ISPs like Gmail and Yahoo require these protocols to even consider inbox placement. Complete every item before sending your first campaign.

1

### SPF Record Configuration

Authorizes specific mail servers to send on behalf of your domain. Include all sending IPs and ESP servers in your DNS record.

2

### DKIM Signature Active

Cryptographically signs your emails to prove they haven't been tampered with in transit. Configure through your ESP and verify with a test send.

3

### DMARC Policy Established

Set policy to `p=quarantine` minimum (not `p=none`). This tells ISPs how to handle unauthenticated mail claiming to be from your domain.

4

### List-Unsubscribe Headers

Implement both List-Unsubscribe and List-Unsubscribe-Post headers. These enable one-click unsubscribe in Gmail and other major ISPs—now mandatory for bulk senders.

5

### Dedicated Campaign Subdomain

Use a subdomain like `mail.yourdomain.com` for all marketing emails. This isolates campaign reputation from your primary domain and transactional mail.

**Verification Tip:** Use tools like MXToolbox, Mail-Tester.com, and Google's CheckMX to validate your authentication setup before launching. All three protocols (SPF, DKIM, DMARC) must pass for optimal deliverability.

novaexpress.ai

**NovaExpress Email Templates**

Professional, responsive email templates for newsletters and campaigns