Email Deliverability Cheatsheet

A comprehensive cheat sheet covering essential aspects of email deliverability, ensuring your emails reach the intended recipients' inboxes.

Authentication & Reputation

Email Authentication Protocols

SPF (Sender Policy Framework)	Specifies which mail servers are authorized to send emails on behalf of your domain. Published in DNS records. Helps prevent spoofing. **Example DNS Record:** `v=spf1 ip4:192.0.2.0/24 include:_spf.example.com -all`
DKIM (DomainKeys Identified Mail)	Adds a digital signature to your email headers, verifying the email's authenticity and integrity. Requires generating a public/private key pair and publishing the public key in DNS. **Example DNS Record:** `example._domainkey.example.com. IN TXT "v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw...."`
DMARC (Domain-based Message Authentication, Reporting & Conformance)	Builds upon SPF and DKIM by specifying how email receivers should handle emails that fail authentication checks. Allows you to request reports on authentication failures. **Example DNS Record:** `_dmarc.example.com. IN TXT "v=DMARC1; p=none; rua=mailto:dmarc@example.com; ruf=mailto:forensic@example.com; adkim=r; aspf=r; fo=1"`
Importance of Implementation	Proper SPF, DKIM, and DMARC implementation significantly improves deliverability by verifying your sender identity and protecting against phishing and spam.

Sender Reputation Factors

IP Address Reputation	The historical behavior of your sending IP address. Blacklists, spam trap hits, and sending volume all impact your IP reputation. Monitor your IP reputation using tools like Google Postmaster Tools.
Domain Reputation	The reputation of your sending domain, influenced by factors like email engagement, spam complaints, and authentication. A strong domain reputation builds trust with ISPs.
Engagement Metrics	Open rates, click-through rates, and positive replies signal good sender behavior. Low engagement and high unsubscribe rates negatively impact reputation.
Spam Complaints	A high spam complaint rate is a major red flag. Actively manage your lists to remove unengaged subscribers and ensure recipients can easily unsubscribe.
Blacklists	Being listed on a blacklist can severely impact deliverability. Regularly check your IP and domain against common blacklists (e.g., Spamhaus, Barracuda) and take immediate action to delist if necessary.

Content & List Management

Email Content Best Practices

Avoid Spam Trigger Words:
Be cautious of using phrases commonly associated with spam, such as “free,” “guarantee,” or excessive use of exclamation points. Use a spam checker tool to analyze your content.

Maintain a Clean HTML Structure: Use well-formed HTML and avoid excessive use of images or large file sizes. Ensure your email renders correctly across different email clients.

Personalization and Relevance:
Tailor your content to your audience's interests and preferences. Personalized emails tend to have higher engagement rates. Segment your list based on demographics, behavior, or purchase history.

Clear Call-to-Action:
Make it easy for recipients to understand what you want them to do. Use clear and concise calls-to-action that stand out visually.

List Hygiene & Segmentation

Double Opt-In	Require subscribers to confirm their email address before adding them to your list. This ensures that you have valid and engaged subscribers.
Regular List Cleaning	Remove inactive or unengaged subscribers from your list. Focus on subscribers who have not opened or clicked on your emails in a while.
Segmentation Strategies	Divide your list into smaller, more targeted segments based on various criteria (e.g., demographics, interests, purchase history). Send tailored content to each segment.
Handling Bounces	Distinguish between hard bounces (permanent delivery failures) and soft bounces (temporary delivery issues). Immediately remove hard bounces from your list.
Feedback Loops	Set up feedback loops with ISPs to receive notifications about spam complaints. Use this data to identify and address any issues with your sending practices.

Infrastructure & Technical Setup

IP Warm-up

Gradual Volume Increase:
When starting with a new IP address, gradually increase your sending volume over time. Start with a small number of recipients and progressively add more. Avoid sending large volumes of emails all at once.

Engagement Monitoring:
Monitor your engagement metrics closely during the warm-up process. Pay attention to open rates, click-through rates, and spam complaints. Adjust your sending volume accordingly.

Consistent Sending:
Maintain a consistent sending schedule during the warm-up period. This helps establish a positive sending reputation with ISPs.

Reverse DNS (rDNS)

What is rDNS?	Reverse DNS maps an IP address back to a domain name. It's the opposite of a standard DNS lookup. It helps verify the legitimacy of your sending server.
Importance of rDNS	ISPs often use rDNS to confirm that the IP address sending emails is associated with the domain it claims to represent. Without proper rDNS, your emails are more likely to be flagged as spam.
Setting up rDNS	Contact your hosting provider or ISP to configure rDNS for your sending IP address. Ensure that the rDNS record matches your sending domain.

Dedicated IP vs. Shared IP

Dedicated IP	An IP address solely used for your email sending. Offers greater control over your sender reputation. Recommended for high-volume senders.
Shared IP	An IP address shared with other senders. Your sending reputation is influenced by the behavior of other users. Suitable for low-volume senders.
Choosing the Right Option	Consider your sending volume and control requirements. If you send a large number of emails, a dedicated IP provides better control and isolation. If you send a small number of emails, a shared IP may be sufficient.

Monitoring & Troubleshooting

Key Metrics to Track

Open Rate	Percentage of recipients who opened your email. Indicates the relevance and appeal of your subject lines.
Click-Through Rate (CTR)	Percentage of recipients who clicked on a link in your email. Measures the effectiveness of your email content and calls-to-action.
Bounce Rate	Percentage of emails that could not be delivered. High bounce rates can negatively impact your sender reputation. Distinguish hard vs. soft bounces.
Spam Complaint Rate	Percentage of recipients who marked your email as spam. A high spam complaint rate is a major red flag and requires immediate attention.
Unsubscribe Rate	Percentage of recipients who unsubscribed from your list. Provides insights into the quality and relevance of your email content.

Troubleshooting Deliverability Issues

Blacklist Checks:
Regularly check your IP address and domain against common blacklists using tools like MXToolbox or Spamhaus. If you are blacklisted, follow the delisting procedures provided by the blacklist operator.

Authentication Verification:
Ensure that SPF, DKIM, and DMARC are properly configured and validated. Use online tools to verify your authentication records.

Content Analysis:
Review your email content for spam trigger words and other potential issues. Use a spam checker tool to analyze your email content.

Feedback Loop Monitoring:
Monitor feedback loops for spam complaints and address any issues promptly. Remove complainants from your list.