Database and Email List Hygiene and Deliverability Tactics

Your email sending reputation and email deliverability is influenced by the following:
1) Hard bounce rate: bad addresses, undeliverable emails
2) Soft bounce rate: out of office messages
3) Open rate of delivered emails and interval since last open
4) Manual spam marks and complaints

Spam traps are email addresses used to identify unauthorized delivery. Pristine spam traps are emails created to identify spammers or unauthorized reuse of a record. Corporations and email service providers use recycled spam traps, which are departed employees and inactive addresses, to identify senders with poor data hygiene and list practices and either blacklist the domain and IP address or automatically move to spam.

Best practices
1) Control email submission to your database
    i. Use captcha to prevent bot submissions which will bounce when you send
    ii. Filter for correct email syntax, name@company.com/net/org/co etc.
2) If you are B2B, require corporate emails and reject personal emails but not if B2C
3) Use an email send and click verification to increase quality and prevent malicious or intentional database submission and corruption
4) Use a universal exclusion list for unsubscribes across the company
5) Make it easy to unsubscribe to prevent people from marking as spam in retaliation
6) Add all hard bounce responses to your universal unsubscribe list
7) Eliminate records who have not engaged within 12, 9, or 6 months
8) Manage your deliverability to 95% or better
9) Extend the campaign drop times over hours or days and throttle the delivery per hour to keep from triggering spam filters
10) Avoid large and rapid increases in send volume as it suggests list purchase and use
11) Avoid attachment, especially heavy ones as systems are designed to filter them
12) Avoid sending code snippets in the body or an attachment
13) Ask your largest customers to whitelist your IP to prevent mistaken filtering and reputation damage
14) Monitor your spam report in platform to see if anyone has marked your email spam
15) Authenticate your identity to improve security and reputation with ISPs
16) Get your domain and IP added to the whitelists maintained by providers
17) Get your deliverability report from Microsoft SNDS for your verified IP range and use the information on non-deliverability to cull your list