EMAIL MARKETING CHANGES

The New Rules & Getting Your Records Setup

1

WHAT WE'RE COVERING

WICKED *marvelous*

1. Agenda
2. Who Am I?
3. The New Rules
4. Access Controls
5. Helpful Resources
6. SPF Records
7. DKIM Records
8. DMARC Records
9. Cleaning Your List
10. Questions + Next Steps

WHO AM I?

Anna Addoms

I love to talk about how to build a sustainable business, so you love what you do and make money, how to use technology and automation without overwhelm, and how to gain visibility and growth in your business without spending a lot of money while making your business work for you, the way you work, so you can focus on what you do best.

Anna is on a mission to make small business owners build their dreams through sustainable business growth and automation without tech overwhelm.

3 THE NEW RULES

WICKED *marvelous*

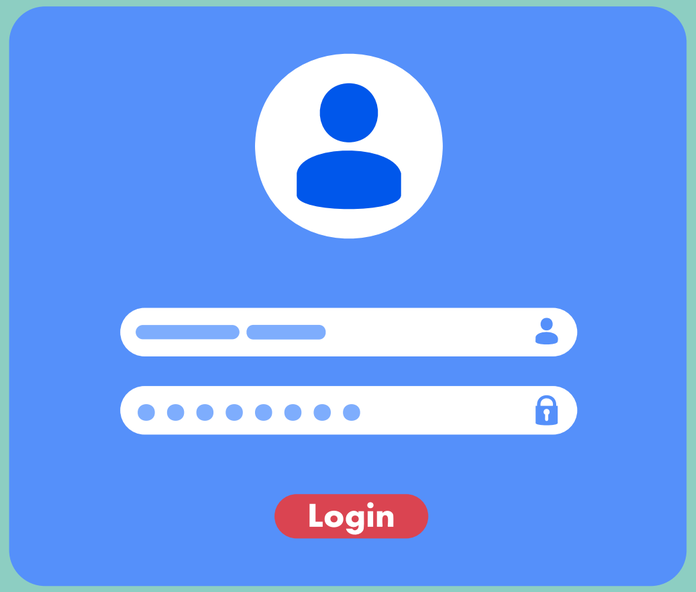
1. Email Authentication
    a. DNS Records Setup
2. Easy Unsubscribe Links
    a. Part of Your Email Marketing Provider
3. New Spam Complaint Threshold
    a. Keeping Your List Healthy
4. Sending Email Accounts

4 ACCESS CONTROLS

WICKED *marvelous*

You Need Access to:

- Your Email Admin Dashboard
  - Google Workspace, Microsoft 365, etc
- DNS Records Management
  - usually where you host your website, sometimes where you purchased your domain
- Account/Admin Settings for Your Email Marketing Provider
  - Convertkit, MailerLite, Mailchimp, etc



HELPFUL RESOURCES

Resources for Generating Records

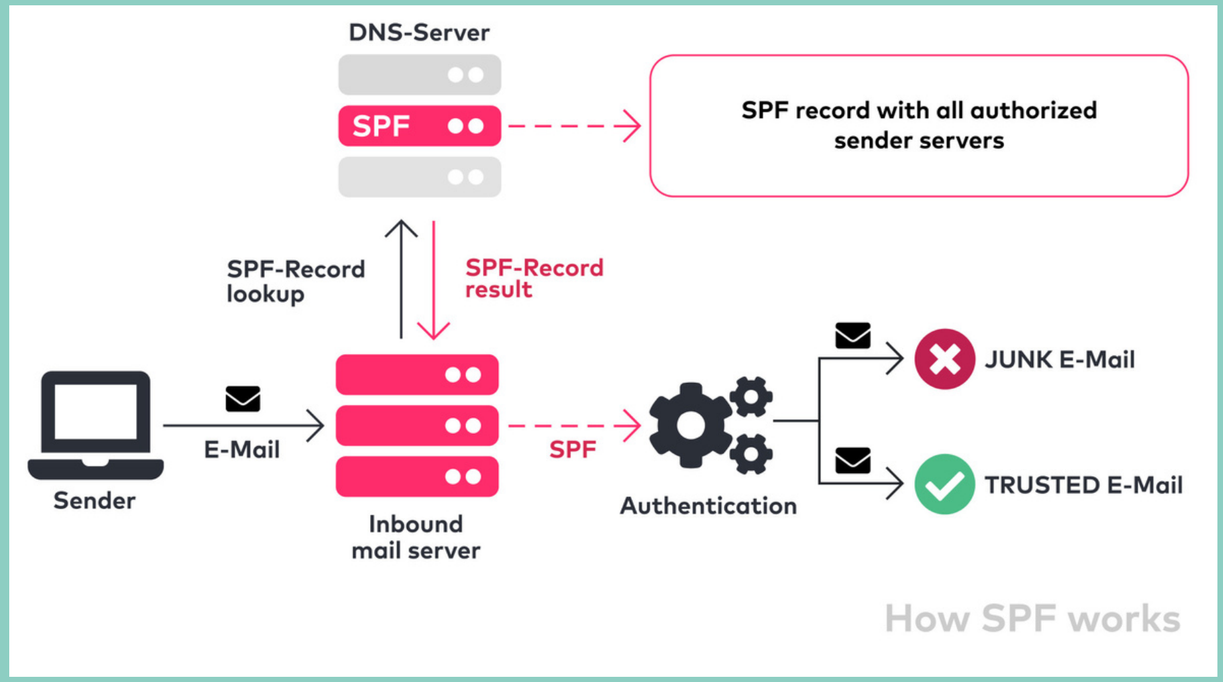
- Valid Bot: https://www.validbot.com/tools/spf-dkim-dmarc-wizard.php

Tools for Checking Records

- Valid Bot
- Mail Tester: https://www.mail-tester.com/
- Experte.com: https://www.experte.com/spam-checker

SPF RECORDS

- Identifies the mail servers and domains that are allowed to send email on behalf of your domain
- Receiving servers check your SPF record to verify that incoming messages that appear to be from your organization are sent from servers allowed by you



DKIM RECORDS

- A specially formatted DNS TXT record that stores the public key the receiving mail server will use to verify a message's signature.
- Generated by Your Email Provider

If you're using a domain email through your hosting provider, the records are generally automatically setup

DMARC RECORDS

Domain-based Message Authentication, Reporting, and Conformance (DMARC) policy

- Shouldn’t be setup until you’ve completed setup of SPF and DKIM records
- It enables:
  - **Visibility** - Monitor emails sent using your domain to ensure they are properly authenticated using SPF and/or DKIM.
  - **Brand Protection** - Block spoofed messages that might damage your brand‘s reputation with customers.
  - **Security** - Prevent users from falling victim to phishing scams that could compromise your organization‘s security.

CLEANING YOUR LIST

As part of the new **0.3%** spam rate threshold (as defined by Google) you'll want to review re-engage, and ultimately clean any "cold" subscribers from your list each month.

You can do this by resending parts of your welcome sequence, using a re-engagement sequence, or a cold-scrub sequence.

QUESTIONS + NEXT STEPS

What questions do you have?

Want a second set of eyes on your setup?

- book a 15-minute review check ($50)
- https://tidycal.com/anna/email-records-check

Overwhelmed? Looking for a DFY option?

- purchase a record setup package ($125)
- https://tc.wickedmarvelous.com/email-marketing-records-setup/