Protecting Your Email Domain from Phishing and Scams

A Step-by-Step Guide to SPF, DKIM, and DMARC

What Is This?

Every day, scammers send emails pretending to be from organizations like yours. They use your organization's name and email domain to trick your staff, donors, and community members into clicking malicious links or handing over sensitive information. This is called **email spoofing**, and it's one of the most common ways phishing attacks succeed.

However, there are three email security tools - SPF, DKIM, and DMARC - that work together to make it much harder for attackers to impersonate your organization. Enabling these tools tells email systems: "*Only emails that come from us are really from us.*"

> **What This Protects Against**
>
> Scammers sending emails that appear to come from your domain (e.g., yourname@yourorg.org) to trick staff, donors, or community members. These tools also protect your organization's reputation: if your domain is used to send spam, it can get blacklisted, meaning your legitimate emails stop being delivered.

The Three Tools Explained

Here's a simple way to think about each one:

Protocol	What It Does	Who Sets It Up

SPF	Verifies which mail servers can send email from your domain	Your IT provider or domain registrar
DKIM	Adds a digital signature to emails so recipients know they're genuine	Your IT provider or email platform (Google/Microsoft)
DMARC	Tells email providers what to do with messages that fail SPF or DKIM checks	Your IT provider or domain registrar

SPF

Think of SPF like a guest list at the door of your event. It tells email providers: "Here is the list of mail servers allowed to send email on behalf of our organization." If an email arrives claiming to be from you, but it's not on the list, the receiving server knows something is wrong and can reject or flag it.

DKIM

DKIM works like a seal on an old-fashioned letter. When your organization sends an email, DKIM adds an invisible digital signature. The receiving email server checks that seal to confirm the message genuinely came from you and wasn't tampered with along the way.

DMARC

DMARC is the set of instructions you give to the email that says: "If an email claims to be from us but fails the SPF or DKIM checks, here's what to do with it — quarantine it, reject it, or just let us know." DMARC also sends you regular reports so you can see if anyone is attempting to misuse your domain.

> **Note**
>
> Setting up these tools requires access to your organization's domain settings (DNS records). This is typically managed by your IT provider or whoever hosts your domain. We strongly recommend working with your IT provider to implement these. The steps below are provided so you understand what to ask for, or to follow along if you're doing this yourself.

Step-by-Step Setup: Google Workspace (Gmail)

If your organization uses Google Workspace for email, follow these steps. You'll need to be a Google Workspace Admin to complete them.

Step 1: Set Up SPF

SPF for Google Workspace is a single record you add to your domain's DNS settings.

1. Log in to your domain registrar (e.g., GoDaddy, Namecheap, Google Domains, Squarespace). If you're not sure who your registrar is, ask your IT provider.
2. Find the DNS settings. This is usually labeled "DNS Management," "Advanced DNS," or "Manage Domain."
3. Look for existing TXT records. If you already have a record starting with "v=spf1" you'll need to edit it rather than add a new one (having two SPF records breaks things).
4. Add or update the TXT record with this value exactly:

   ```
   v=spf1 include:_spf.google.com ~all
   ```

5. Save the record. DNS changes can take up to 48 hours to take effect, though usually it's much faster.

> **What the record means**
>
> The "~all" at the end means "soft fail" — emails from unlisted servers are flagged but not immediately rejected. This is the safest starting point. Your IT provider can later change it to "-all" (hard fail) once everything is confirmed working.

Step 2: Set Up DKIM

Google Workspace generates your DKIM key for you. You just need to activate it and add it to your DNS.

1. Go to your Google Workspace Admin Console at admin.google.com.
2. Navigate to: **Apps → Google Workspace → Gmail → Authenticate email.**
3. Select your domain from the dropdown.
4. Click "Generate New Record." Leave the default settings as they are and click Generate.
5. Google will display a TXT record value. Copy this entire value — it will be a long string of letters and numbers.
6. Go back to your domain registrar's DNS settings and add a new TXT record:
   - **Name/Host:** `google._domainkey` (followed by your domain)
   - **Value:** Paste the long string Google gave you
7. Save the record, then return to the Google Admin Console and click "Start Authentication."

> **Not seeing the option?**
>
> The DKIM setup wizard is only available to Google Workspace admins. If you don't see it, confirm that you're logged in with your admin account, not your regular staff account.

Step 3: Set Up DMARC

DMARC is added as a TXT record in your DNS settings, just like SPF and DKIM. We recommend starting in "monitor only" mode before enforcing rejections.

1. Go back to your domain registrar's DNS settings.
2. Add a new TXT record:
   - **Name/Host:** `_dmarc`
   - **Value:** `v=DMARC1; p=none; rua=mailto:it@yourorg.org`

   Replace `it@yourorg.org` with a real email address where you'd like to receive DMARC reports. This can be your IT provider's address.
3. Save the record.
4. After a few weeks of reviewing reports, your IT provider can update "p=none" to "p=quarantine" (suspicious emails go to spam) and eventually "p=reject" (suspicious emails are blocked entirely).

Step-by-Step Setup: Microsoft 365 (Outlook)

If your organization uses Microsoft 365 for email, the process is similar. You'll need to be a Microsoft 365 Global Admin and have access to your domain registrar.

Step 1: Set Up SPF

Microsoft 365 uses a different SPF value than Google Workspace.

1. Log in to your domain registrar and navigate to your DNS settings.
2. Look for any existing TXT record starting with "v=spf1." If one exists, edit it. Do not add a second SPF record.
3. Add or update the TXT record with this value:

   ```
   v=spf1 include:spf.protection.outlook.com ~all
   ```

4. Save the record and allow up to 48 hours for it to take effect.

Step 2: Set Up DKIM

Microsoft 365 also generates your DKIM keys for you through the Defender portal.

1. Log in to the Microsoft 365 Defender portal at security.microsoft.com.
2. In the left navigation, go to: **Email & Collaboration → Policies & Rules → Threat Policies → Email Authentication Settings.**
3. Select the **DKIM** tab.
4. Choose your domain and click "Enable."
5. Microsoft will display two CNAME records you need to add to your DNS. Copy both values exactly.
6. Go to your domain registrar's DNS settings and add both CNAME records as provided.
7. Return to the Defender portal and verify the status shows "Enabled." This may take up to 72 hours.

Step 3: Set Up DMARC

DMARC setup is identical regardless of whether you use Google Workspace or Microsoft 365.

1. Go to your domain registrar's DNS settings.
2. Add a new TXT record:
   - **Name/Host:** `_dmarc`
   - **Value:** `v=DMARC1; p=none; rua=mailto:it@yourorg.org`

   Replace `it@yourorg.org` with a real email address where you'd like to receive DMARC reports.
3. Save the record.
4. After 4–6 weeks, review the DMARC reports with your IT provider and tighten the policy to "p=quarantine" and then "p=reject."

How to Verify It's Working

Once your IT provider has set everything up, you can verify the settings are active using a free tool called MXToolbox. No technical knowledge required.

1. Go to mxtoolbox.com in your web browser.
2. In the search bar, type your organization's domain name (e.g., yourorg.org) and select "SPF Record Lookup" from the dropdown. A green result means it's working.
3. Repeat the search selecting "DKIM Lookup" — you will need to enter your domain and the selector (for Google it's "google"; for Microsoft it's "selector1").

4. Finally, select "DMARC Lookup" and enter your domain. A valid policy will be displayed.

> **See something red or an error?**
>
> Don't panic — just share the screenshot with your IT provider. It will help them quickly identify what needs to be fixed.

What to Do Next

Here is a simple checklist to share with your IT provider:

☐ Ask your IT provider to confirm whether SPF, DKIM, and DMARC are already set up for your domain.

☐ If not, share this guide with them and ask them to set all three up.

☐ Request that DMARC start in monitoring mode (p=none) and that they review the reports after 4–6 weeks.

☐ Once monitoring confirms no legitimate email is being blocked, ask them to update DMARC to p=quarantine, then eventually p=reject.

☐ Verify everything is working using MXToolbox (mxtoolbox.com).

> **Remember: Technology Is Just One Layer**
>
> SPF, DKIM, and DMARC significantly reduce the risk of your domain being spoofed, but they don't make your organization immune to phishing. Attackers can still send phishing emails from other domains that look convincing. Staff training, simulated phishing tests, and a culture of "when in doubt, report it" remain just as important.

Revision #3
Created 9 June 2026 15:20:43 by Josh
Updated 12 August 2026 21:49:24 by Josh