How to add SPF records in Microsoft 365

- Access Microsoft 365 Admin Center.
- Navigate to your DNS hosting provider (e.g., GoDaddy).
- Add a TXT record with `v=spf1 include:spf.protection.outlook.com -all`.
- Save and verify the record in Microsoft 365.

How to configure DKIM (generate public/private keys and add records)

- In Microsoft 365 Defender, go to **Email & collaboration** → **Policies & rules** → **Threat policies** → **DKIM**.
- Enable DKIM for your domain; Microsoft automatically generates selectors.
- Add two CNAME records in your DNS pointing to Microsoft's DKIM selectors.
- Once DNS propagates, enable DKIM signing.

How to add DMARC records in Microsoft 365

- Create a TXT record in DNS: `v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@yourdomain.com; ruf=mailto:dmarc-failure@yourdomain.com; fo=1`.
- Save and verify DMARC policies using Microsoft 365 message headers or external tools.

How to set up SPF, DKIM, and DMARC using Microsoft Defender

- Use the **Email Authentication Settings** in Microsoft Defender.
- Validate SPF, enable DKIM signing, and configure DMARC enforcement.
- Monitor mail flow and adjust policies to tighten security.

What spoofed emails are and how they work

- Spoofed emails forge the "From" address to trick recipients.
- Attackers impersonate trusted domains to bypass weak security.
- SPF, DKIM, and DMARC prevent spoofing by authenticating senders.

How to change SOA values in DNS

- Access DNS management in your domain registrar.
- Locate the SOA (Start of Authority) record.
- Adjust parameters such as TTL, refresh, retry, and expire values.

How to update SOA records in GoDaddy using Zone File Editor

- Log in to GoDaddy → Domain → DNS → Advanced Settings → Zone File Editor.
- Edit SOA record fields and save changes.

How to view and manage DNS records in GoDaddy

- Use the DNS Management page to view existing records.
- Add, edit, or delete records like A, MX, TXT, or CNAME.
- Save and verify changes using Microsoft 365 admin tools.

How to block access to company resources (files, network, apps) using Microsoft 365 tools

- Use Conditional Access policies to restrict logins.
- Apply Data Loss Prevention (DLP) to monitor sensitive files.
- Use Information Rights Management (IRM) to encrypt content.
- Deploy Intune to control device access and compliance.

Full step-by-step path to secure company data and restrict unauthorized access

1. Implement SPF, DKIM, and DMARC.
2. Enforce MFA and Conditional Access.
3. Apply DLP and IRM policies to sensitive content.
4. Monitor user activity with Microsoft Defender.
5. Use Intune for device management and compliance enforcement.