

# DMARC záznam

Poslední aktualizace 12 září, 2024

Domain Message Authentication Reporting and Conformance, zkráceně DMARC. Tento prvek z oblasti e-mailové komunikace je navazující částí na již existující technologie SPF a DKIM.

Pokud DKIM a SPF vůbec nemáte, tak těmi musíte začít. Bez těchto technologií nemá cenu DMARC řešit.

Přečtěte si, jak nastavit:

- [DKIM záznamy](#)
- [SPF záznamy](#)

## Co DMARC dělá/umí?

- Vychází z adresy odesílatele uvedené v hlavičce **From** dopisu a snaží se **ověřit, jestli dopis byl skutečně odeslán z uvedené domény.**
- **Navazuje na využití SPF a DKIM** – pokud bylo splněno SPF odesílatele domény nebo dopis nese její ověřený DKIM podpis, považuje ji za důvěryhodnou.
- **Definujte politiku pro neúspěšné dopisy** – jak se zachovat k těm, které DMARC ověřením neprojdou.
- **Umožňuje nastavit zpětnou vazbu** – kam a jak posílat reporty o výsledku DMARC pro dopisy odeslané z dané domény.
- Lze nastavit, že se má uplatňovat jen pro část dopisů a nasazovat je postupně.

DMARC zveřejňuje držitel odesílající domény a ověřuje příjemce dopisu.

## Jak splnit potřebné minimum pro validaci DMARC záznamu?

př. Vlastníte doménu **mojedomena.cz**

Do DNS přidejte následující TXT záznam:

název záznamu: **\_dmarc.mojedomena.cz**

**obsah záznamu:** v=DMARC1; p=none;

Tímto záznamem splníte potřebnou část pro validaci výskytu DMARC záznamu.