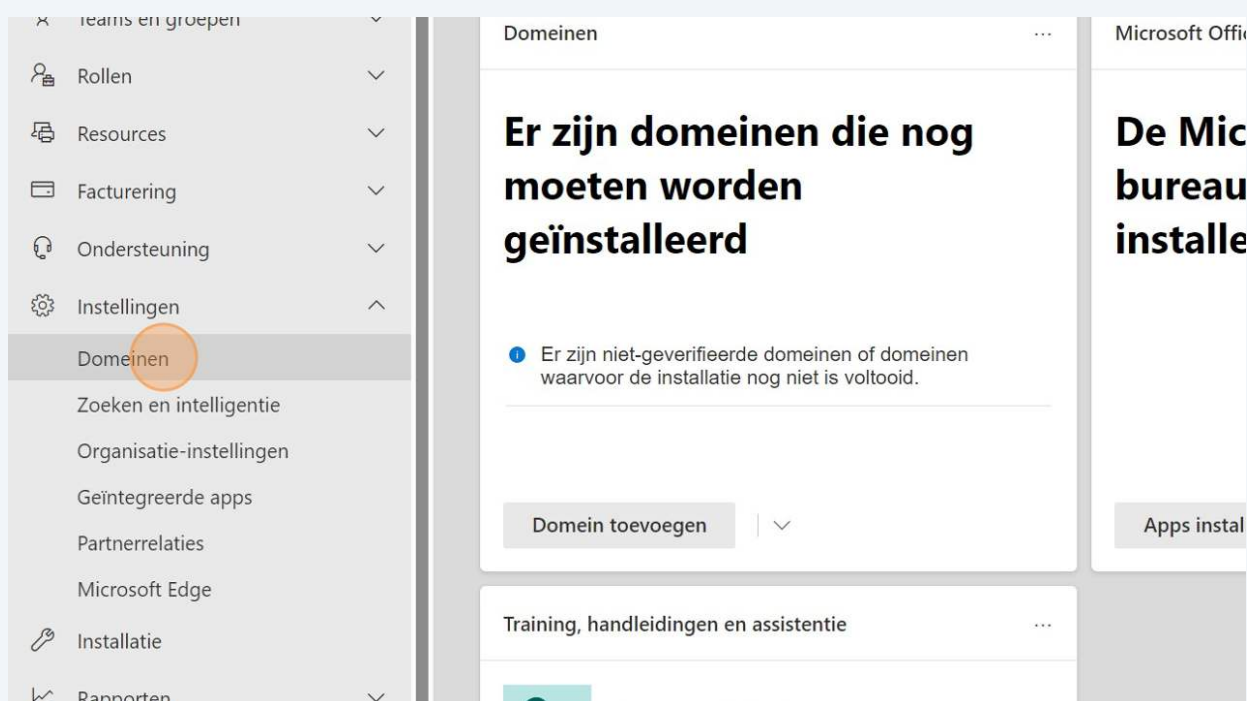


Voorkom SPAM behandeling door het instellen van SPF, DKIM en DMARC

We ontvangen veel mails. Maar hierdoor worden veel belangrijke mails vaak ook in de ongewenste mailbox afgeleverd. Als je niets doet, zal ook jij hiervan slachtoffer worden. Voorkom dat je mails in SPAM terecht komen door enkele domeinnaam instellingen uit te voeren. Je moet hiervoor je domeinnaam DNS beheer openen en enkele waarden uit Microsoft Admin center ophalen en verifiëren. (A1, A3, A5)

1

Open het beheerderspaneel <https://admin.microsoft.com>
Onder "Instellingen" kies je voor "Domeinen"



2

Klik op één van de domeinnamen (niet de [.onmicrosoft.com](https://onmicrosoft.com)) en kies vervolgens bovenaan voor "DNS-records"

Gebruikers

Apparaten

Teams en groepen

Rollen

Resources

Facturering

Ondersteuning

Instellingen

Domeinen

Zoeken en intelligentie

Organisatie-instellingen

Geïntegreerde apps

Partnerrelaties

Extern beheerd

Als standaard instellen

Domein verwijderen

Vernieuwen

Overzicht

DNS-records

Gebruikers

Teams en groepen

Apps

Domeinstatus

In orde

Alles ziet er goed uit en er zijn geen items die uw aandacht nodig hebben.

3

Klik bovenaan op DNS beheer en bevestig met "doorgaan".

Overzicht

DNS-records

Gebruikers

Teams en groepen

Apps

Ga naar de DNS-hostingprovider om **DNS-records te beheren voor veggivino.com: Overige.**

Verbind uw services met uw domein door deze DNS-records toe te voegen aan uw domeinregistrar of DNS-hostingprovider. Selecteer een record om alle details ervan te bekijken, en kopieer en plak de verwachte waarden naar de registrar. [Meer informatie over DNS- en recordtypen.](#)

Status controleren

DNS beheer

CSV-bestand downloaden

Zonebestand downloaden

Microsoft Exchange

Type	Status	Naam
☐ MX		@
☐ TXT		@

4

Open het DNS record onder "Microsoft Exchange" van het type TXT en klik om de TXT waarde te kopiëren.

> CNAME-records (1)

✓ **TXT-records (1)**
[Instructies voor TXT-records weergeven](#)

Opnemen	TXT-naam	TXT-waarde	TTL
Verwacht	@	v=spf1 include:spf.protection.outlook.com -all	1 uur

Geavanceerde opties

Vorige Doorgaan

5

Bewerk of maak in je DNS beeer van de domeinnaam (extern!) een nieuw record aan van het type TXT, laat de naam leeg en plak de inhoud. Bewaar en wacht enkele minuten/uren.

Je SPF record is nu ingesteld.

Naam

Inhoud
v=spf1 include:spf.protection.outlook.com -all

Beschrijving

BEWAAR ANNULEER

6

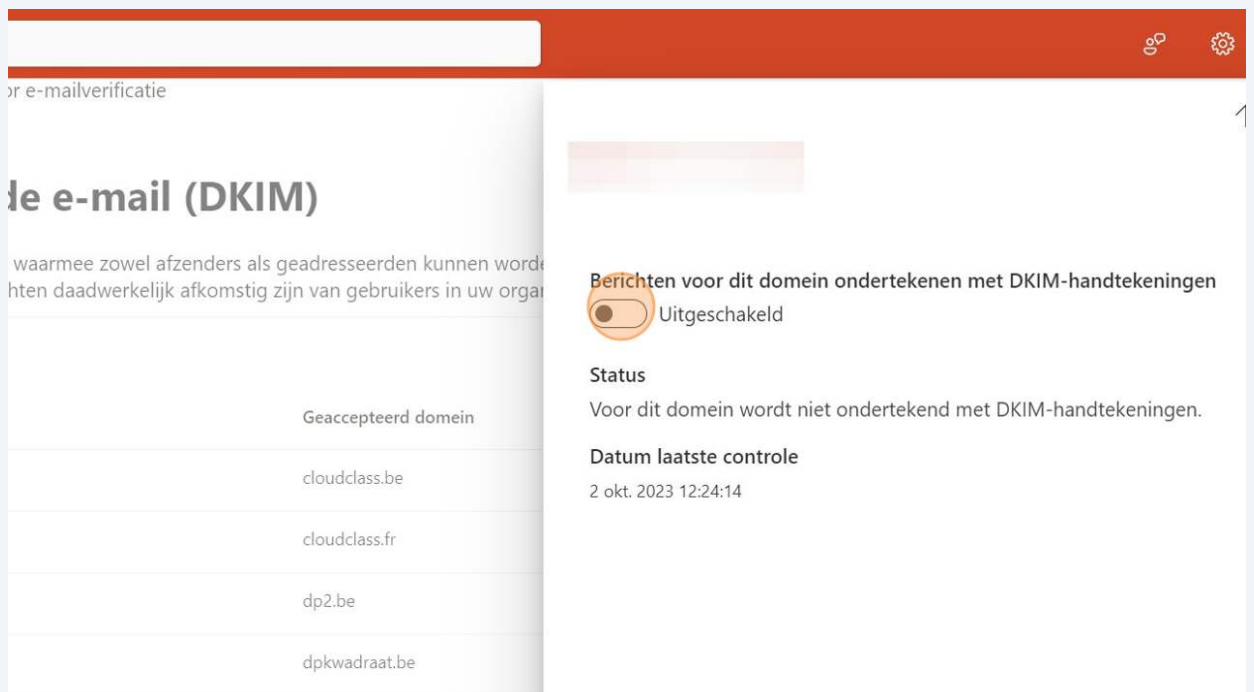
Navigeer naar <https://security.microsoft.com/dkimv2> en klik op de domeinnaam die je wenst te activeren (klik er op, niet aanvinken).



The screenshot shows the Microsoft 365 Defender interface. The left sidebar contains navigation options: Start, Incidenten en meldingen, Opsporing, Acties & ingediende items, Threat intelligence, and Secure score. The main content area is titled 'DomainKeys geïdentificeerde e-mail (DKIM)' and includes a breadcrumb trail: 'Beleid en regels > Bedreigingsbeleid > Instellingen voor e-mailverificatie'. Below the title, there is a description of DKIM and two buttons: 'Exporteren' and 'Vernieuwen'. A table with the header 'Naam' is partially visible at the bottom.

7

Kies ervoor om DKIM in te schakelen.



The screenshot shows the Microsoft 365 Defender interface for DKIM settings. The left sidebar is partially visible. The main content area is titled 'De e-mail (DKIM)' and includes a description of DKIM. A toggle switch labeled 'Berichten voor dit domein ondertekenen met DKIM-handtekeningen' is currently turned off, with the text 'Uitgeschakeld' next to it. Below this, the 'Status' section states 'Voor dit domein wordt niet ondertekend met DKIM-handtekeningen.' and the 'Datum laatste controle' is '2 okt. 2023 12:24:14'. A table with the header 'Geaccepteerd domein' is partially visible at the bottom, showing domain names like cloudclass.be, cloudclass.fr, dp2.be, and dpkwadraat.be.

8

Kopieer in de melding die je krijgt de Host name en de Value om de CNAME voor selector1 alsook selector2 aan te maken.

The screenshot shows a DNS management interface with a table of domains. A modal dialog titled 'Clientfout' is open, displaying an error message:

[Microsoft.Exchange.Management.Tasks.ValidationException]CNAME record does not exist for this config. Please publish the following two CNAME records first. Domain Name : veggivino.com Host Name : selector1._domainkey Points to address or value: selector1-veggivino-com._domainkey.educationtech.onmicrosoft.com Host Name : selector2._domainkey Points to address or value: selector2-veggivino-com._domainkey.educationtech.onmicrosoft.com . If you have already published the CNAME records, sync will take a few minutes to as many as 4 days based on your specific DNS. Return and retry this step later.

The background table lists domains such as cloudclass.be, cloudclass.fr, dp2.be, dpkwadmaat.be, edu-teach.be, edu-teach.com, edu-tech.be, educationtech.mail.onm, and educationtech.onmicrosoft.com (standaard domein voor ondertekening).

9

Maak de CNAME aan met de gekopieerde informatie. Dit doe je tweemaal (Selector1 en Selector2)

Voeg een nieuw CNAME-record toe

Voeg een nieuw CNAME-record toe door de hostnaam en de doelhostnaam op te geven. Klik op 'Opslaan'.

Vanwege DNS-caching kan het enige tijd duren vooraleer deze wijziging zichtbaar is op internet.

Hostnaam

selector1._domainkey

Verwijst naar

selector1- n._domainkey. .onmicrosoft.com

Beschrijving

BEWAAR

ANNULEER

10

Wacht enkele uren/dagen en schakel het DKIM record opnieuw in (opnieuw testen).

Je DKIM record is nu ingesteld.



11

Navigeer naar <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-dmarc-configure>

Kopieer de DMARC instelling die je wenst te configureren.

the receiving server to follow if DMARC fails. You can set the policy

become familiar with the concepts in Best practices for

```
"v=DMARC1; p=none"
```

 Copy

```
"v=DMARC1; p=quarantine"
```

 Copy

Training

Module

[Manage anti-malware and anti-spam policies - Training](#)

Manage anti-malware and anti-spam policies

Documentation

[How to use DKIM for email in your custom domain](#)

Learn how to use DomainKeys Identified Mail (DKIM) with Microsoft 365 to ensure messages sent from your custom domain are trusted by the destination email systems.

[Set up SPF to help prevent spoofing](#)

Learn how to update a Domain Name Service (DNS) record to use Sender Policy Framework (SPF) with your custom domain in Office 365.

[How to enable DMARC Reporting for Microsoft Online Email Routing Address \(MOERA\) and parked Domains](#)

12 Maak bij je DNS Domeinnaam hosting een nieuw TXT record aan.

Stel als Hostname "_dmarc" in en pas de gekopieerde inhoud aan om alleen de inhoud tussen de "-tekens te bevatten.

Je DMARC record is nu ingesteld.

Voeg een nieuw TXT-record toe

Voeg een nieuw TXT-record toe door een hostnaam en de inhoud van het record op te geven. Een TXT-record kan elke tekstuele inhoud bevatten. Klik op 'Opslaan'.
Vanwege DNS-caching kan het enige tijd duren vooraleer deze wijziging zichtbaar is op internet.

Naam

_dmarc

Inhoud

v=DMARC1; p=none

Beschrijving

 **BEWAAR**

ANNULEER

13

Wil je DMARC rapportagemails ontvangen dan plak je de geavanceerde DMARC inhoud en pas je de rapportage mailboxen aan naar een monitoring e-mail account.

Je DMARC record is nu ingesteld.

Voeg een nieuw TXT-record toe



Voeg een nieuw TXT-record toe door een hostnaam en de inhoud van het record op te geven. Een TXT-record kan elke tekstuele inhoud bevatten. Klik op 'Opslaan'. Vanwege DNS-caching kan het enige tijd duren vooraleer deze wijziging zichtbaar is op internet.

Naam

_dmarc

Inhoud

v=DMARC1; p=none; pct=100; rua=mailto:d@rua.example.com;
ruf=mailto:d@ruf.example.com; fo=1

Beschrijving

 **BEWAAR**

ANNULEER