**Artikel 2 |** Bestrijd phishing, spoofing en malware met veilige e-mailstandaarden

*Jaarlijks worden nog steeds veel bedrijven en ondernemers slachtoffer van phishing en andere vormen van cybercriminaliteit. Zo was 2022 een recordjaar als het gaat om phishing. Sinds begin 2019 steeg het aantal phishingaanvallen met meer dan 150% tot 4,7 miljoen in 2022 (*[*APWG, 2022*](https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf?_ga=2.89270299.1205010690.1685603546-440811353.1683116327&_gl=1*2vt685*_ga*NDQwODExMzUzLjE2ODMxMTYzMjc.*_ga_55RF0RHXSR*MTY4NTYwMzU0Ni4yLjEuMTY4NTYwMzU0OS4wLjAuMA..)*). Het is belangrijk dat bedrijven maatregelen nemen om hun mailverkeer te beveiligen. Door veilige e-mailstandaarden als DMARC, DKIM en STARTTLS/DANE massaal te implementeren, kunnen organisaties en ondernemingen samen cybercriminaliteit van e-mail effectief bestrijden. Want hoewel zo’n 95% van de internetgebruikers, houders en ondernemers vindt dat de beveiliging van zakelijke mail onmisbaar is voor de continuïteit van hun bedrijf, valt er nog veel winst te behalen (*[*SIDN, 2023*](https://www.sidn.nl/nieuws-en-blogs/ondernemers-positief-over-aandacht-voor-open-internetstandaarden)*).*

**Veel standaarden voor mailbeveiliging beschikbaar**

Er zijn diverse standaarden beschikbaar om e-mail te beveiligen. Zo gaan SPF, DKIM en DMARC phishing en spoofing tegen. Deze standaarden worden vaak samen ingezet en voorkomen dat een e-mail zomaar namens een andere partij wordt verstuurd. Hierbij worden diverse nieuwe records (DNS-gegevens) in de DNS-informatie opgenomen. Daarnaast gaat STARTTLS in combinatie met DANE het afluisteren van mailverkeer tegen. STARTTLS maakt het mogelijk om transportverbindingen tussen e-mailservers met TLS te beveiligen op basis van certificaten. Met DANE kunnen e-mailservers het gebruik van TLS afdwingen. De vertrouwelijkheid van de berichtenuitwisseling wordt hiermee beveiligd.

SPF, DKIM, DMARC en DANE kun je los van elkaar en op willekeurige volgorde implementeren. Wel is het belangrijk dat je DANE altijd in combinatie met DNSSEC gebruikt. Voor de andere e-mailstandaarden is DNSSEC niet verplicht, maar wel aanbevolen. De afgelopen jaren is de inzet van DANE sterk gegroeid. Een mogelijke reden hiervoor is dat deze beveiligingsstandaard wordt ondersteund in de grote mailserverpakketten. SIDN, het bedrijf dat alle .nl-domeinnamen beheert, stelt bijvoorbeeld een financiële incentive beschikbaar per domein dat een gebruiker beveiligt met e-mailstandaarden. Dit gebeurt via de [Registrar Scorecard](https://www.sidnlabs.nl/nieuws-en-blogs/sidn-gaat-adoptie-van-internetstandaard-dane-stimuleren) waarvoor registrars zich kunnen aanmelden.

**E-mailstandaarden voor Exim en Postfix**

Het is belangrijk om veilige e-mailstandaarden zo snel mogelijk te implementeren voor veilig (zakelijk) mailverkeer. Gelukkig is de implementatie gemakkelijker dan je misschien denkt. Je hoeft hiervoor namelijk alleen de technische mailinfrastructuur aan te raken.

In onderstaande praktische artikelen vind je alles wat je moet weten om veilige e-mailstandaarden te installeren en configureren. Zo kun jij met hulp van je hostingpartij direct aan de slag gaan met de implementatie van SPF, DKIM, DMARC en STARTTLS en DANE voor de meest gebruikte mailservers Postfix en Exim.

* [De implementatie van SPF, DKIM en DMARC in Exim](https://www.sidn.nl/nieuws-en-blogs/hands-on-de-implementatie-van-spf-dkim-en-dmarc-in-exim)
* [De implementatie van SPF, DKIM en DMARC voor Postfix](https://www.sidn.nl/nieuws-en-blogs/hands-on-de-implementatie-van-spf-dkim-en-dmarc-voor-postfix)
* [De implementatie van DANE op Exim](https://www.sidn.nl/nieuws-en-blogs/hands-on-de-implementatie-van-dane-op-exim)
* [De implementatie van DANE voor Postfix](https://www.sidn.nl/nieuws-en-blogs/hands-on-de-implementatie-van-dane-voor-postfix)

**Beveiliging van zakelijke mail**

Houders en ondernemers nemen verschillende maatregelen om de beveiliging van hun zakelijke e-mail te verbeteren. Dat blijkt uit een recent onderzoek van SIDN onder 75 respondenten. Zo hanteert 77,3% een streng beleid met betrekking tot wachtwoorden en gebruikt 73,3% een sterk spamfilter voor e-mail (SIDN, 2023). Het toepassen van veilige e-mailstandaarden is een essentiële stap voor bedrijven om hun bedrijfsgegevens te beschermen en hoge kosten als gevolg van beveiligingsincidenten te voorkomen. En zo effectief phishingaanvallen, malwareverspreiding en andere vormen van cybercriminaliteit via e-mail tegen te gaan.

Via de website [internet.nl](https://internet.nl/test-mail/) kun je je zakelijke mail testen en inzicht krijgen in kwetsbaarheden. Deze mailtest controleert onder meer de beveiliging van de verbinding van je mailserver. De uitslagen in het testrapport kun je gebruiken om met hulp van je hostingpartij je e-mailvoorziening te verbeteren.

*Ga direct aan de slag met de implementatie van de veilige e-mailstandaard aan de hand van* [*deze checklist*](https://www.sidn.nl/downloads/7t8wLafwM4iLXCbW1g9dWw/0c80ad73721c7ad7d154961289c073c0/Checklist_e-mailstandaarden.pdf) *of neem contact met ons op voor meer informatie.*