**SIDN** | Campagnetoolkit veilige e-mailstandaarden | social posts & mailings

**Social post 1**

**Facebook & LinkedIn**

*Direct zichtbare tekst:*

Zo’n 96% van de Nederlandse bedrijven heeft het e-maildomein onvoldoende beveiligd.

*Description (niet direct zichtbaar):*

Dat is zorgelijk, want cyberaanvallen komen regelmatig voor. E-mail is de belangrijkste ingang voor internetcriminelen. Zij gebruiken phishing, malware en spoofing om persoonsgegevens of andere informatie te achterhalen en geld afhandig te maken. Organisaties als Artis en MediaMarkt werden slachtoffer van zo’n aanval.

In dit artikel lees je meer over het belang van massale implementatie van veilige e-mailstandaarden: [link naar artikel 1].

**Instagram**

Zo’n 96% van de Nederlandse bedrijven heeft het e-maildomein onvoldoende beveiligd.

Dat is zorgelijk, want cyberaanvallen komen regelmatig voor. E-mail is de belangrijkste ingang voor internetcriminelen. Zij gebruiken phishing, malware en spoofing om persoonsgegevens of andere informatie te achterhalen en geld afhandig te maken. Organisaties als Artis en MediaMarkt werden slachtoffer van zo’n aanval.

Meer over het belang van massale implementatie van veilige e-mailstandaarden lees je via de link in de biografie.

#veiligmailen #cybersecurity #digitaleveiligheid #onlineveiligheid #cyberaanvallen #emailstandaarden

**Social post 2**

**Facebook & LinkedIn**

*Direct zichtbare tekst:*

De schade door phishing naar beveiligingscodes van bankrekeningen liep in 2022 op tot € 3,6 miljoen.

*Description (niet direct zichtbaar):*

Toch zijn phishing, malware, spoofing en andere vormen van cybercriminaliteit relatief gemakkelijk aan te pakken, door massaal veilige e-mailstandaarden te implementeren. Dat houdt in dat veilige e-mailstandaarden op alle domeinen en alle verzendende en ontvangende mailservers worden geïmplementeerd.

Lees hier hoe je veilige e-mailstandaarden direct toepast en de continuïteit van je bedrijf waarborgt: [link naar artikel 2].

**Instagram**

De schade door phishing naar beveiligingscodes van bankrekeningen liep in 2022 op tot € 3,6 miljoen.

Toch zijn phishing, malware, spoofing en andere vormen van cybercriminaliteit relatief gemakkelijk aan te pakken, door massaal veilige e-mailstandaarden te implementeren. Dat houdt in dat veilige e-mailstandaarden op alle domeinen en alle verzendende en ontvangende mailservers worden geïmplementeerd.

Via de link in de biografie lees je hoe jij direct veilige e-mailstandaarden toepast.

#cybersecurity #digitaleveiligheid #onlineveiligheid #cyberaanvallen #emailstandaarden #spam #phishing

**Social post 3**

**Facebook & LinkedIn**

*Direct zichtbare tekst:*

In 2022 kreeg 32% van alle Nederlanders te maken met phishing.

*Description (niet direct zichtbaar):*   
Bij phishing proberen internetcriminelen via e-mails achter persoonlijke informatie of je bankrekening te komen. Deze vorm van cybercriminaliteit is nog steeds een groot probleem in Nederland. Zo blijkt uit recent onderzoek van SIDN dat 25,3% van de ondernemers en bedrijven de afgelopen 3 jaar te maken kreeg met een veiligheidsincident rondom de website of zakelijke mail van de organisatie.

Is jouw mailverkeer goed beveiligd? Lees meer via [eigen link of link naar [SIDN](https://www.sidn.nl/moderne-internetstandaarden/e-mailbeveiliging)] en neem contact op met je hostingpartij om te starten met de implementatie van veilige e-mailstandaarden.

**Instagram**

In 2022 kreeg 32% van alle Nederlanders te maken met phishing.

Bij phishing proberen internetcriminelen via e-mails achter persoonlijke informatie of je bankrekening te komen. Deze vorm van cybercriminaliteit is nog steeds een groot probleem in Nederland. Zo blijkt uit recent onderzoek van SIDN dat 25,3% van de ondernemers en bedrijven de afgelopen 3 jaar te maken had met een veiligheidsincident rondom de website of zakelijke mail van de organisatie.

Is jouw mailverkeer goed beveiligd? Lees meer via [eigen link of link naar [SIDN](https://www.sidn.nl/moderne-internetstandaarden/e-mailbeveiliging)] en neem contact op met je hostingpartij om te starten met de implementatie van veilige e-mailstandaarden.

#phishing #veiligmailen #cybersecurity #digitaleveiligheid #onlineveiligheid #ondernemer

**Social post 4**

**Facebook & LinkedIn**

*Direct zichtbare tekst:*

Phishing veroorzaakt 90% van het online misbruik in Nederland.

*Description (niet direct zichtbaar):*

Het is belangrijk om je zakelijke mail goed te beveiligen om phishing te voorkomen en de continuïteit van je bedrijf te bewaken. Je wilt natuurlijk voorkomen dat gegevens op straat komen te liggen of belangrijke bedrijfsprocessen worden stilgelegd.

Neem contact op met je hostingpartij en start direct met de implementatie van veilige e-mailstandaarden. Lees meer via [eigen link of link naar [SIDN](https://www.sidn.nl/moderne-internetstandaarden/e-mailbeveiliging)].

**Instagram**

Phishing veroorzaakt 90% van het online misbruik in Nederland.

Het is belangrijk om je zakelijke mail goed te beveiligen om phishing te voorkomen en de continuïteit van je bedrijf te bewaken. Je wilt natuurlijk voorkomen dat gegevens op straat komen te liggen of belangrijke bedrijfsprocessen worden stilgelegd.

Neem contact op met je hostingpartij en start direct met de implementatie van veilige e-mailstandaarden. Lees meer via de link in onze biografie.

#phishing #veiligmailen #cybersecurity #digitaleveiligheid #onlineveiligheid #ondernemer

**Mail 1 - Belang van veilige e-mailstandaarden**

Subject: Implementeer veilige e-mailstandaarden en voorkom cyberaanvallen.

Beste [voornaam ontvanger],

Mailen doen we dagelijks. Vooral binnen organisaties is e-mail een van de meestgebruikte communicatiemiddelen.

Toch kent het e-mailprotocol nog steeds kwetsbaarheden en is e-mail de belangrijkste ingang voor cybercriminelen. Het is daarom belangrijk dat je jouw zakelijke mailverkeer optimaal beveiligt.

E-mailstandaarden als DANE, SPF, DKIM en DMARC gaan phishing, spam en malware tegen. Dit doen ze door de afzender, het mailsysteem en de inhoud van een e-mail te beveiligen.

Lees meer over het belang van veilige e-mailstandaarden: [link naar artikel 1].

Heb je vragen over online veiligheid? Neem dan gerust contact met ons op via [contactgegevens].

**Mail 2 - Direct aan de slag met de implementatie van veilige e-mailstandaarden**

Subject: Start direct met de implementatie van veilige e-mailstandaarden.

Beste [voornaam ontvanger],

Internetcriminelen maken gebruik van phishing en spoofing om achter persoonsgegevens of andere informatie te komen, malware op een computer te installeren en een bedrijf geld afhandig te maken. 2022 een recordjaar als het gaat om phishing. Sinds begin 2019 steeg het aantal phishingaanvallen met meer dan 150% tot 4,7 miljoen ([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..)).

Deze en andere vormen van cybercriminaliteit zijn relatief gemakkelijk aan te pakken door veilige e-mailstandaarden te implementeren. Alleen als we veilige e-mailstandaarden massaal toepassen, is de bestrijding van phishing, spoofing en malware effectief.

In ons artikel lees je meer over de implementatie van veilige e-mailstandaarden: [link naar artikel 2].

Heb je vragen over online veiligheid? Neem dan gerust contact met ons op via [contactgegevens].