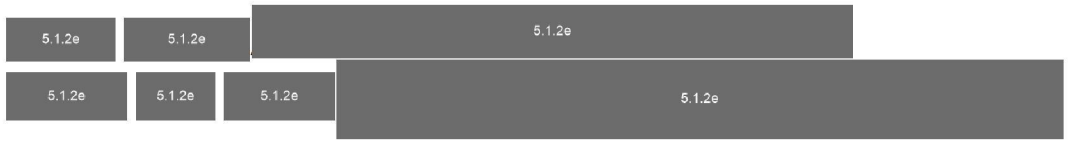
Forum Standaardisatie

Standaard Samenwerken

Internet.nl
IS YOUR INTERNET UP TO DATE?

Van RIVM-spoofing tot GGD-lek: Wat kunnen we ervan leren?

Conferentie Nederland Digitaal 2021

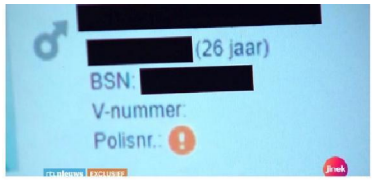


Domeinnaam is vaak startpunt van incident ...

Misbruik via:

1. Opgezegde domeinnaam
2. Onbeschermde domeinnaam (‘spoofing’)
3. Domeinnaam-verwarring

1. Misbruik van opgezegde domeinnaam



GGD case toont aan: let op je domeinnamen

Gepubliceerd op 27 jan. 2021

Michiel Henneke
29 november SIDN Connect: events.sidn.nl | Marketing | Internet | Sp...
+ Volgen

Daniel Verlaan komt regelmatig met scoops over cybersecurity. Ook maandag weer over de GGD. Opvallend detail dat ter sprake kwam in de uitzending van Jinek: het gebruik van oude GGD-domeinnamen om je als GGD'er voor te doen. Voor hem - en zijn hoofdredactie - een stap te ver. Voor echte cybercriminelen niet.

Dit herinnert aan eerdere incidenten bij Jeugdzorg en de Politie: oude domeinnamen op de vrije markt zetten, betekent dat derden deze namen kunnen misbruiken. Daarom adviseer ik altijd twee dingen:

Daniël Verlaan
@danielverlaan

Replying to @danielverlaan

Begin december probeerde ik via een oud, overgenomen GGD-domein per e-mail een account voor CoronIT aan te vragen.

Dat lukte, maar ik moest na twee stappen nóg een stap ondernemen en dat vond ik - samen met de hoofdredactie en Juza - te ver gaan.

Toen heb ik de GGD ingelicht:

Translate Tweet

Daarop kreeg ik een reactie van de servicedesk dat ze nog enkele gegevens moesten krijgen om het CoronIT-account aan te maken. Daarop heb ik samen met de hoofdredactie van RTL Nieuws besloten om het onderzoek stop te zetten, niet verder te gaan dan noodzakelijk, en jullie via de telefoon en per e-mail te informeren.

Omdat het duidelijk is dat de CoronIT Servicedesk niet doorhad dat ik mailde vanaf een oud domein, denk ik dacht het uiteindelijk wel mogelijk was om toegang te krijgen tot CoronIT. Een kwaadwillende zou hier in de toekomst misbruik van kunnen maken. Ik hoop dat de Servicedesk hiervan op de hoogte wordt gesteld, om de beveiligingsmaatregelen verder aan te scherpen. Ondanks dat ben ik blij om te zien dat er wel degelijk vormen van authenticatie in acht werden genomen.

TV-fragment Jinek over Jeugdriagg (1-10-2020)

2. Misbruik van onbeschermde domeinnaam (‘spoofing’)

03 april 2020 14:55
Laatste update: 03 april 2020 17:49

44 NUjij-reacties

Criminelen en anderen kwaadwillenden konden door niet goed ingestelde instellingen e-mailen uit naam van de Rijksoverheid en het Rijksinstituut voor Volksgezondheid en Milieu (RIVM), bevestigen woordvoerders van beide organisaties vrijdag na berichtgeving door *RTL Nieuws*.

TV-fragment RTL Late Night over Tweede Kamer (23-10-2017)

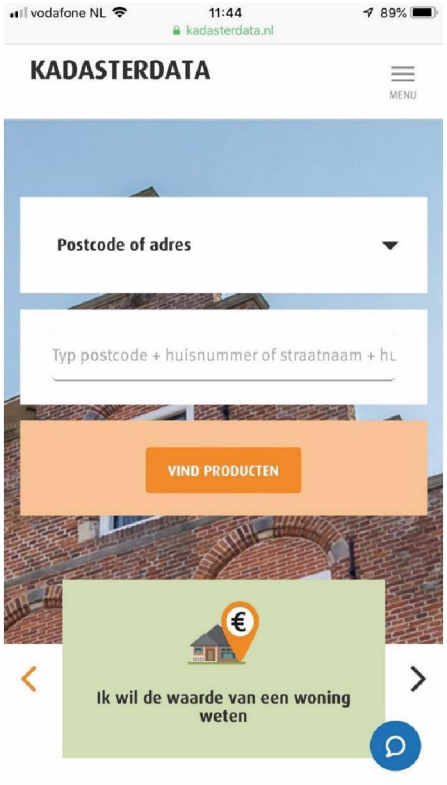
3. Misbruik via domeinnaam-verwarring

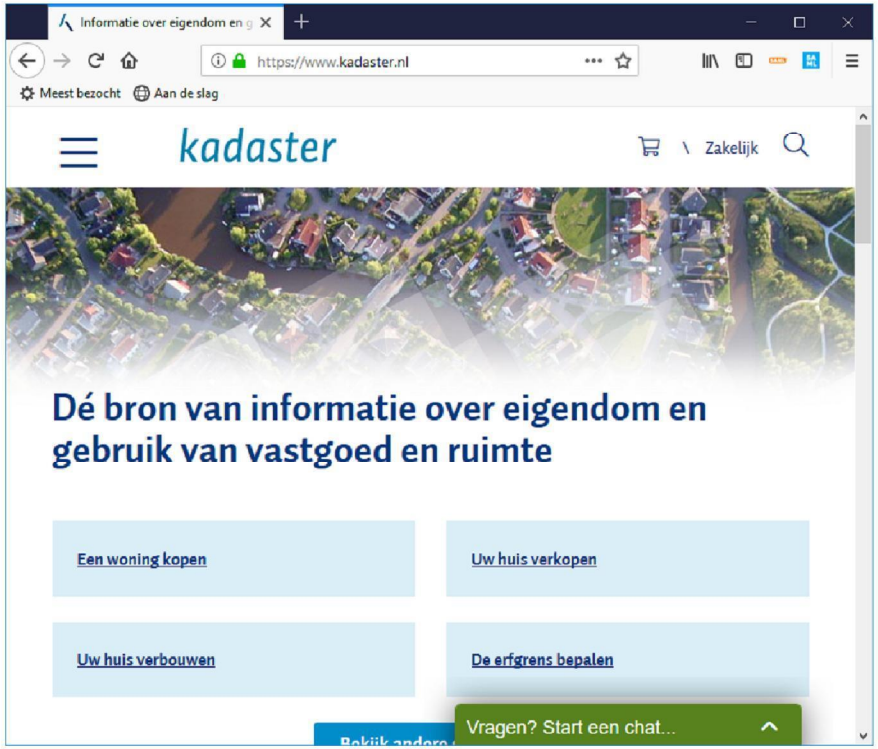
- Ook wel typosquatting of lookalike domeinnamen
- Voorbeelden:
  - Overslaan of verwisselen van letters in de domeinnaam;
  - Vergissingen in de benaming van het domeinnaam;
  - Verkeerd top level domein.

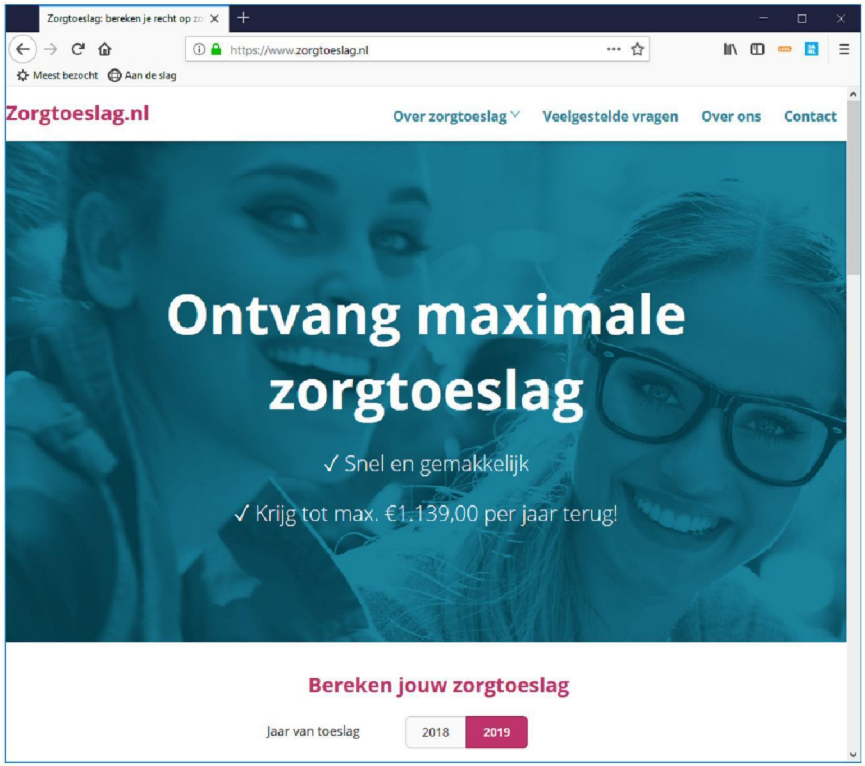
= 5.1.2e 5.1.2e 5.1.2e c.s.

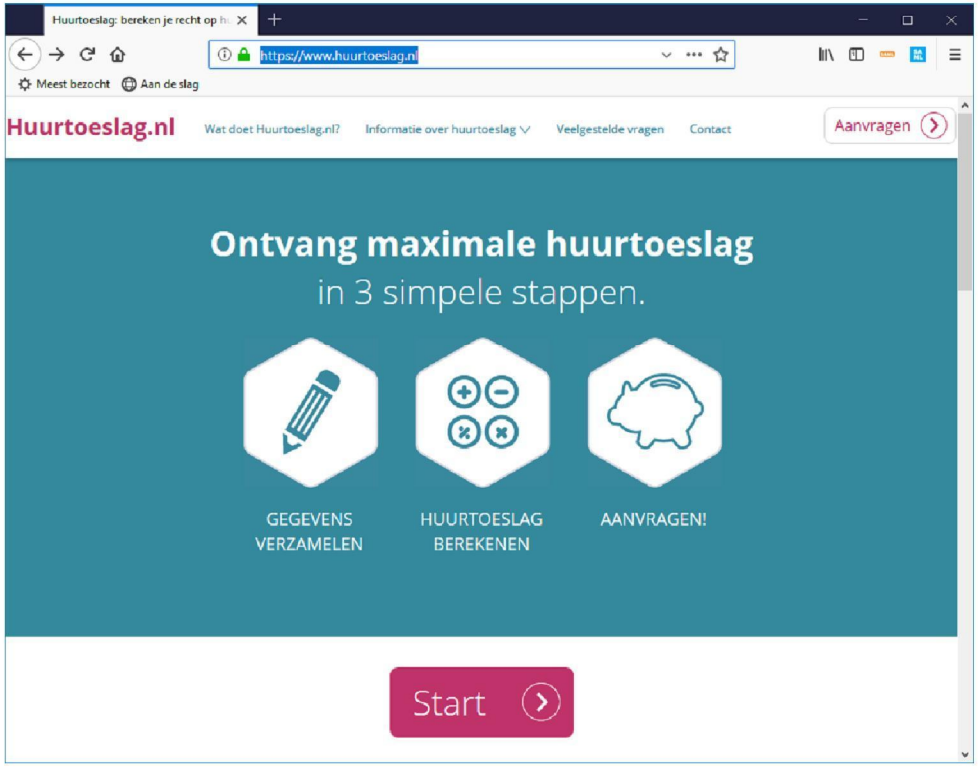
De Cyberonderzoeksraad heeft een groot onderzoek uitgevoerd naar de gevoeligheid van e-mail. Meer dan 70 domeinnamen die op andere domeinen lijken, werden geregistreerd. Vervolgens werd gewacht op binnenkomende berichten. Er bleken ruim 15.000 e-mails binnen te komen. Na het filteren van spam en virussen bleven er zo'n 3.100 relevante berichten over.

Tussen deze berichten zaten gevoelige zaken als processen-verbaal, aangiftes, medische dossiers, rekeningen, kopieën van bankafschriften, kopieën van identiteitspapieren, bestellingen (zelfs voor spionageapparatuur), vorderingen, departementaal vertrouwelijke stukken en meer.

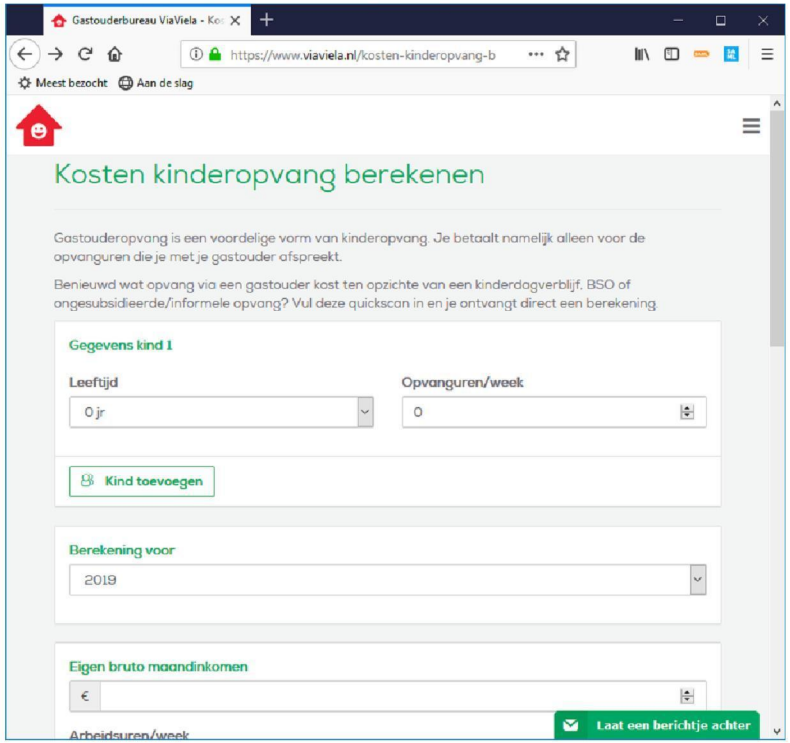

vodafone NL
11:44
89%
kadasterdata.nl
KADASTERDATA
MENU
Postcode of adres
Typ postcode + huisnummer of straatnaam + hu
VIND PRODUCTEN
Ik wil de waarde van een woning weten


Informatie over eigendom en g
https://www.kadaster.nl
Meest bezocht
Aan de slag
kadaster
Zakelijk
Dé bron van informatie over eigendom en gebruik van vastgoed en ruimte
Een woning kopen
Uw huis verkopen
Uw huis verbouwen
De erfgrens bepalen
Vragen? Start een chat...

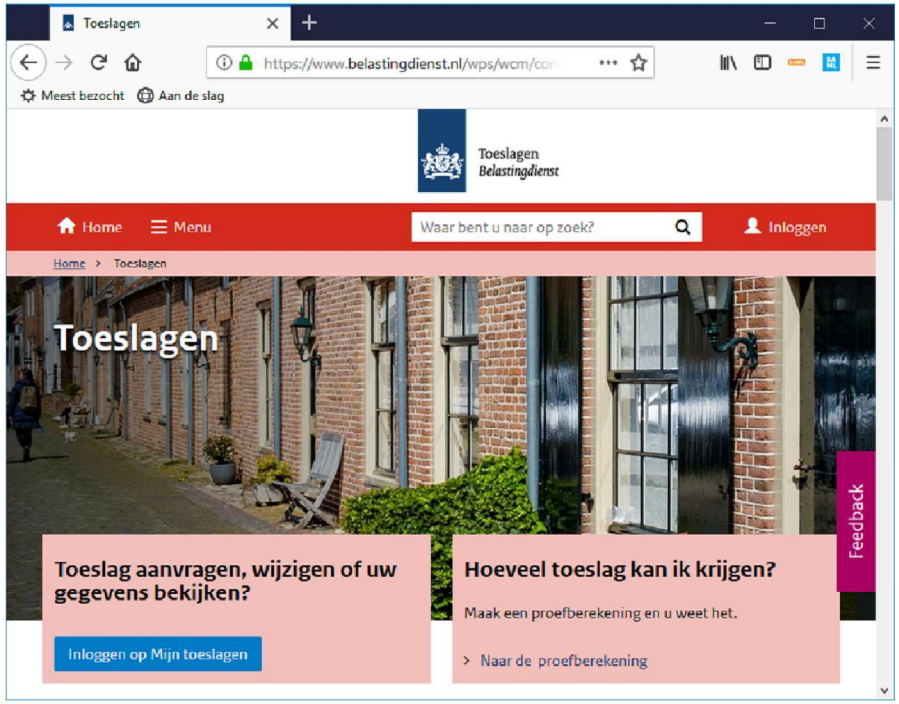

Zorgtoeslag: bereken je recht op zo
https://www.zorgtoeslag.nl
Meest bezocht
Aan de slag
Zorgtoeslag.nl
Over zorgtoeslag
Veelgestelde vragen
Over ons
Contact
Ontvang maximale zorgtoeslag
✓ Snel en gemakkelijk
✓ Krijg tot max. €1.139,00 per jaar terug!
Bereken jouw zorgtoeslag
Jaar van toeslag
2018
2019

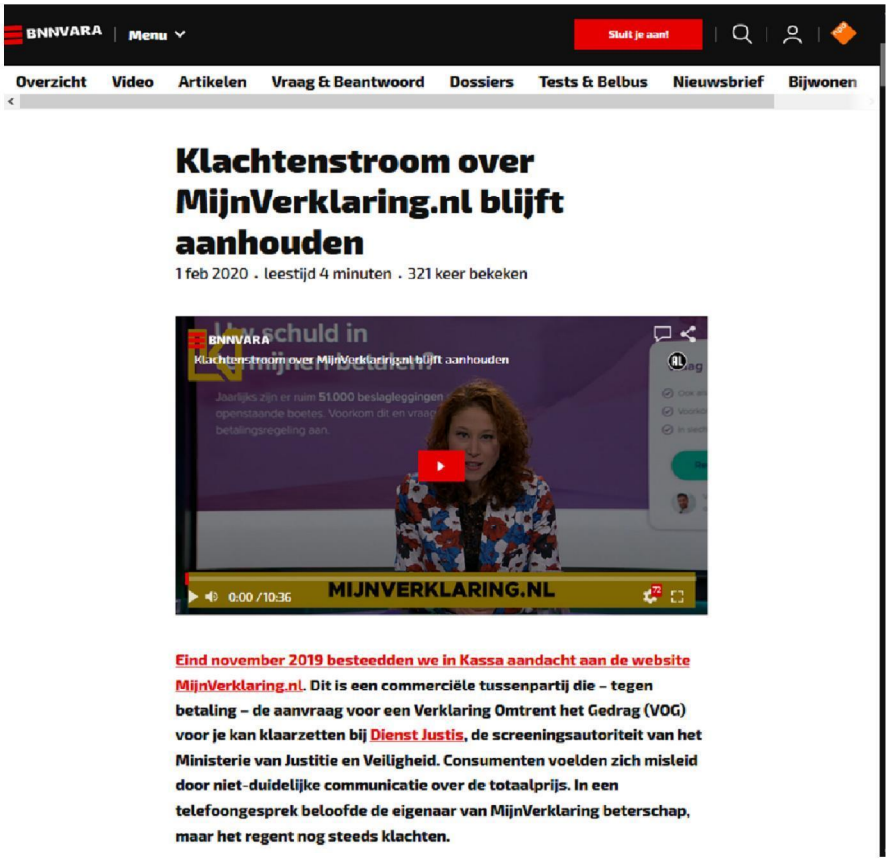

Huurtoeslag: bereken je recht op h
https://www.huurtoeslag.nl
Meest bezocht
Aan de slag
Huurtoeslag.nl
Wat doet Huurtoeslag.nl?
Informatie over huurtoeslag
Veelgestelde vragen
Contact
Aanvragen
Ontvang maximale huurtoeslag
in 3 simpele stappen.
GEGEVENS VERZAMELEN
HUURTOESLAG BEREKENEN
AANVRAGEN!
Start

www.kinderopvangtoeslag.nl



www.toeslagen.nl





BNNVARA | Menu

Sluit je aan!

Overzicht Video Artikelen Vraag & Beantwoord Dossiers Tests & Belbus Nieuwsbrief Bijwonen

Klachtenstroom over MijnVerklaring.nl blijft aanhouden

1 feb 2020 . leestijd 4 minuten . 321 keer bekeken

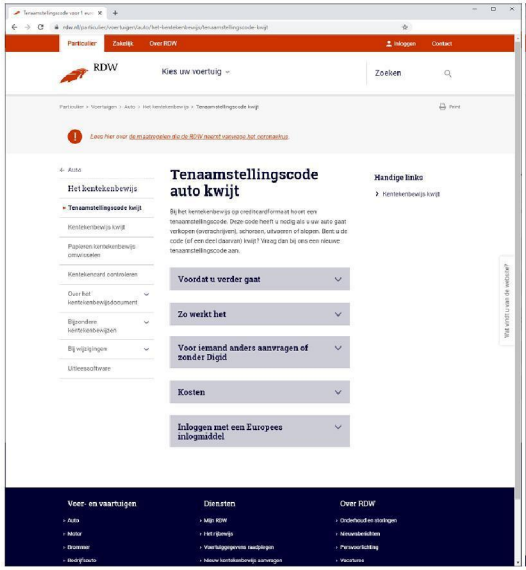
Eind november 2019 besteedden we in Kassa aandacht aan de website MijnVerklaring.nl. Dit is een commerciële tussenpartij die – tegen betaling – de aanvraag voor een Verklaring Omtrent het Gedrag (VOG) voor je kan klaarzetten bij Dienst Justis, de screeningsautoriteit van het Ministerie van Justitie en Veiligheid. Consumenten voelden zich misleid door niet-duidelijke communicatie over de totaalprijs. In een telefoongesprek beloofde de eigenaar van MijnVerklaring beterschap, maar het regent nog steeds klachten.

'Mogelijk malafide'

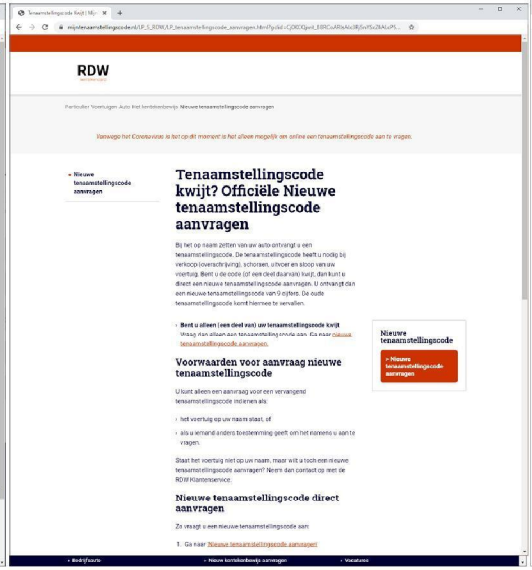
Duizenden mensen gedupeerd bij aanvraag kentekenbewijs: 'Site leek op die van RDW'

05 september 2020 14:01

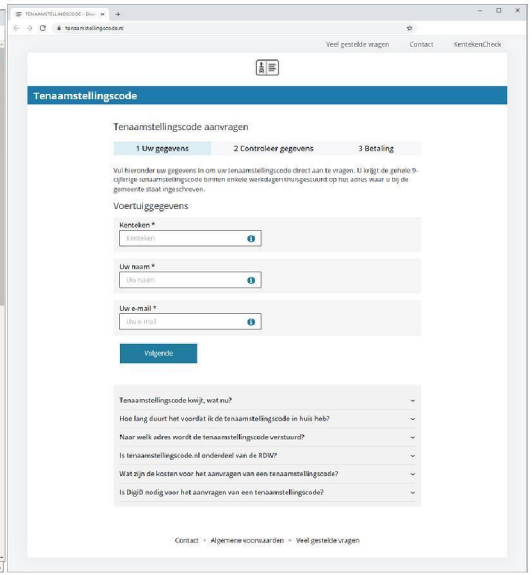
"Het zag er betrouwbaar uit", zegt hij tegen RTL Nieuws. "De site had dezelfde kleuren als de RDW. De verbinding was beveiligd. En als je je kenteken invult, krijg je ook alle gegevens van je motor."



rdw.nl – legitiem – 1 euro
formulieren verstopt achter menu's



mijntenaamstellingscode.nl – niet overheid – 19,95 euro
Gebruikt RDW huisstijl



tenaamstellingscode.nl – niet overheid – 14,95 euro
Gebruikt rijksoverheid stijlen

NIEUWS INFORMATIEWEBSITE

Overheid lanceert site voor onbedoeld zwangeren waarvan adres lijkt op dat van pro life-organisatie

Verwarring dreigt, nu de overheid Onbedoeldzwanger.info heeft gelanceerd. Dit omdat Onbedoeldzwanger.nl al bestaat, een website die verwijst naar hulpverlening van Siriz, een christelijke stichting die voortkomt uit een anti-abortusorganisatie.

Anneke Stoffelen 2 september 2020, 15:53

- **Geen eenduidige naamgeving van (website)domeinen veroorzaakt wantrouwen en/of onduidelijkheid bij burgers. In dit geval door:**
  - Een .info domeinextensie registreren terwijl dit niet gebruikelijk is binnen de overheid.
  - Het in gebruik nemen van een domeinnaam waarvan varianten al geregistreerd (& gevestigd) zijn

Kortom: domeinnaam is vaak startpunt incident ...

Misbruik via:

1. Opgezegde domeinnaam
2. Onbeschermde domeinnaam (‘spoofing’)
3. Domeinnaam-verwarring

Doel van domein-misbruiker...

1. Financieel:
   - Onnodig intermediaire rol (bijv. RDW-tenaamstellingscode, toeslagen en VOG)
     - Misleidend maar niet altijd illegaal
   - Stelen en misbruiken van inloggegevens (bijv. DigiD voor toeslag)
   - Betaling uitlokken (bijv. CJIB-boete of nepfactuur en ook CEO-fraude)
   - Ransomware
   - Verkoop van of chantage via persoonsgegevens

2. Invloed vergroten:
   - Concurrentiepositie verbeteren (bedrijfsspionage)
   - Politieke beïnvloeding (bijv. nepnieuws)

Bijkomende mogelijke gevolgen voor slachtoffer

- Crisissituatie
- Gevolgschade bij klanten (bijv. ‘persoonsgegevens op straat’)
- Reputatieschade
- Minder vertrouwen onder doelgroep
- …

Niet alleen de overheid heeft er last van...

Bioscoopketen Pathé is slachtoffer geworden van ceo-fraude, waarbij meer dan 19 miljoen euro is buitgemaakt. Criminelen deden zich voor als directeuren van het Franse hoofdkantoor en stuurden e-mails naar de Nederlandse directie met het verzoek om geld over te maken, melden Quote en het FD op basis van een vonnis van de rechter deze week over de zaak.

Wat te doen? Zorg goed voor je domeinnamen...

1. Goed domeinnaambeheer
2. Beveiligingsstandaarden toepassen
3. Duidelijke communicatie

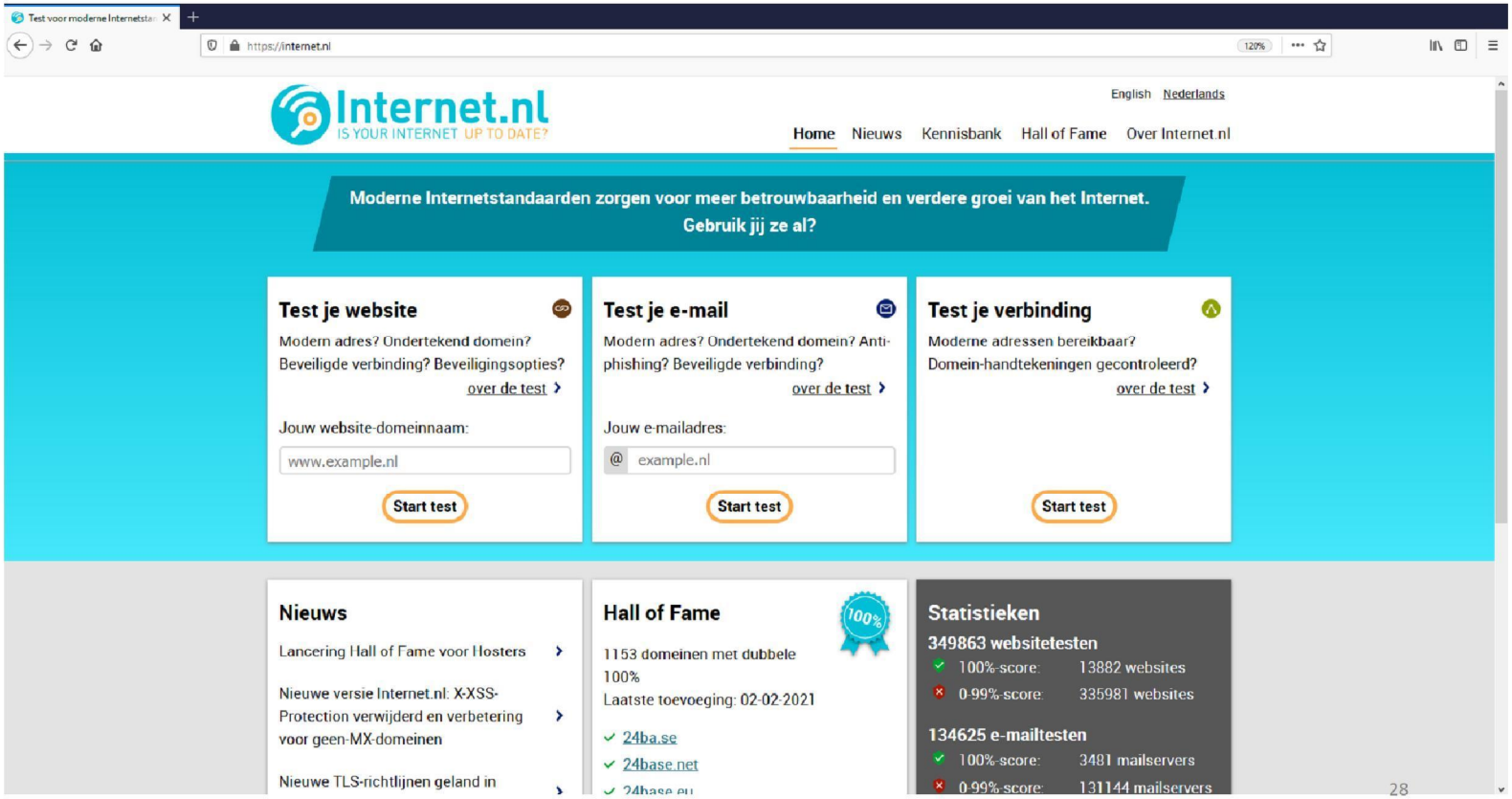
1. Goed domeinnaambeheer

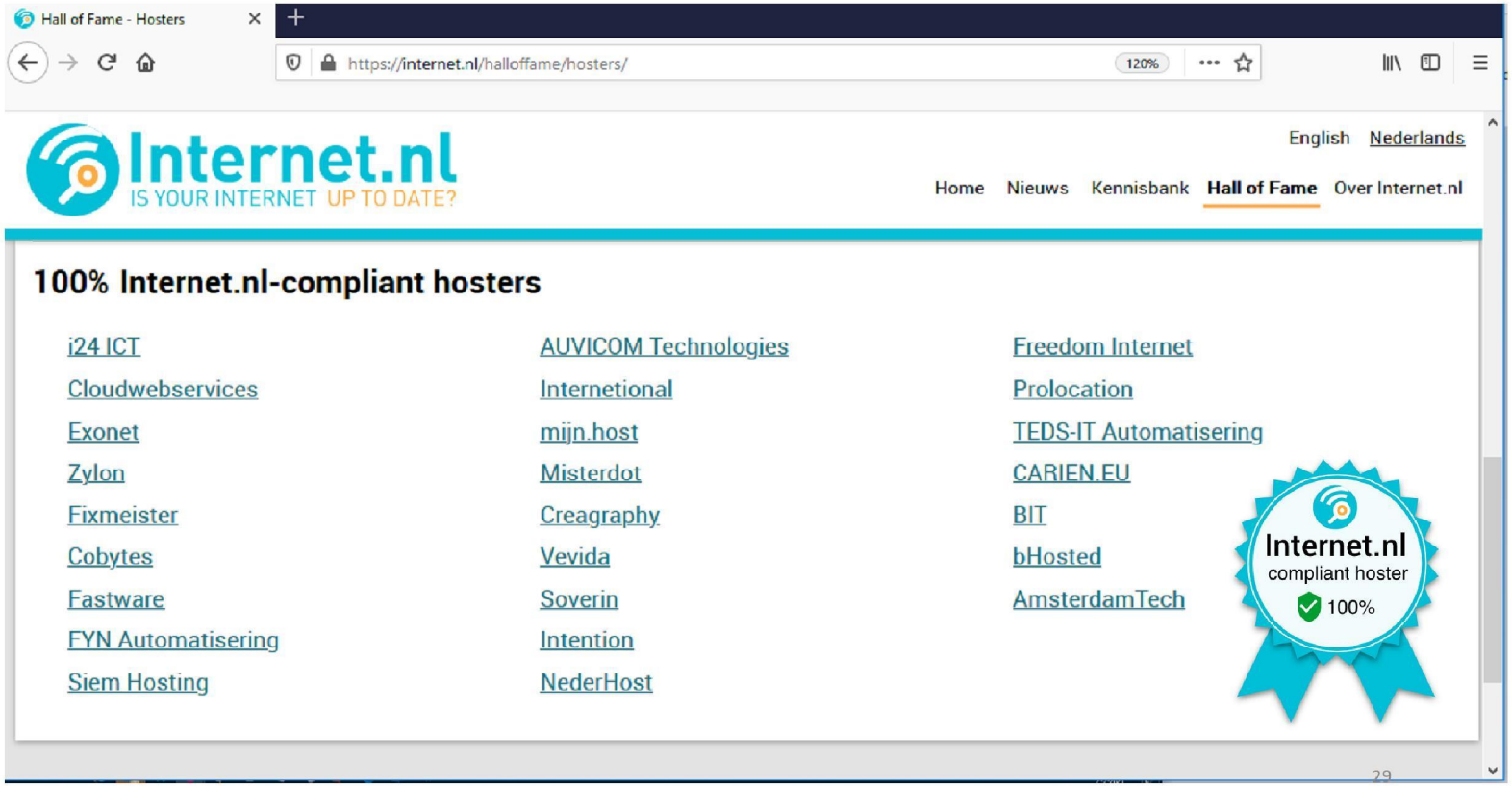
- Welke domeinnamen hebben we?
- Staan alle domeinnamen netjes op onze naam?
- Registreren we sterk ook gelijkende domeinnamen?
- Monitoren we of andere partijen sterk gelijkende domeinnamen registreren? (bijv. via domeinnaambewakingsservice van SIDN)
- Hoe gaan we om met domeinnamen die we niet langer actief gebruiken?
- ...

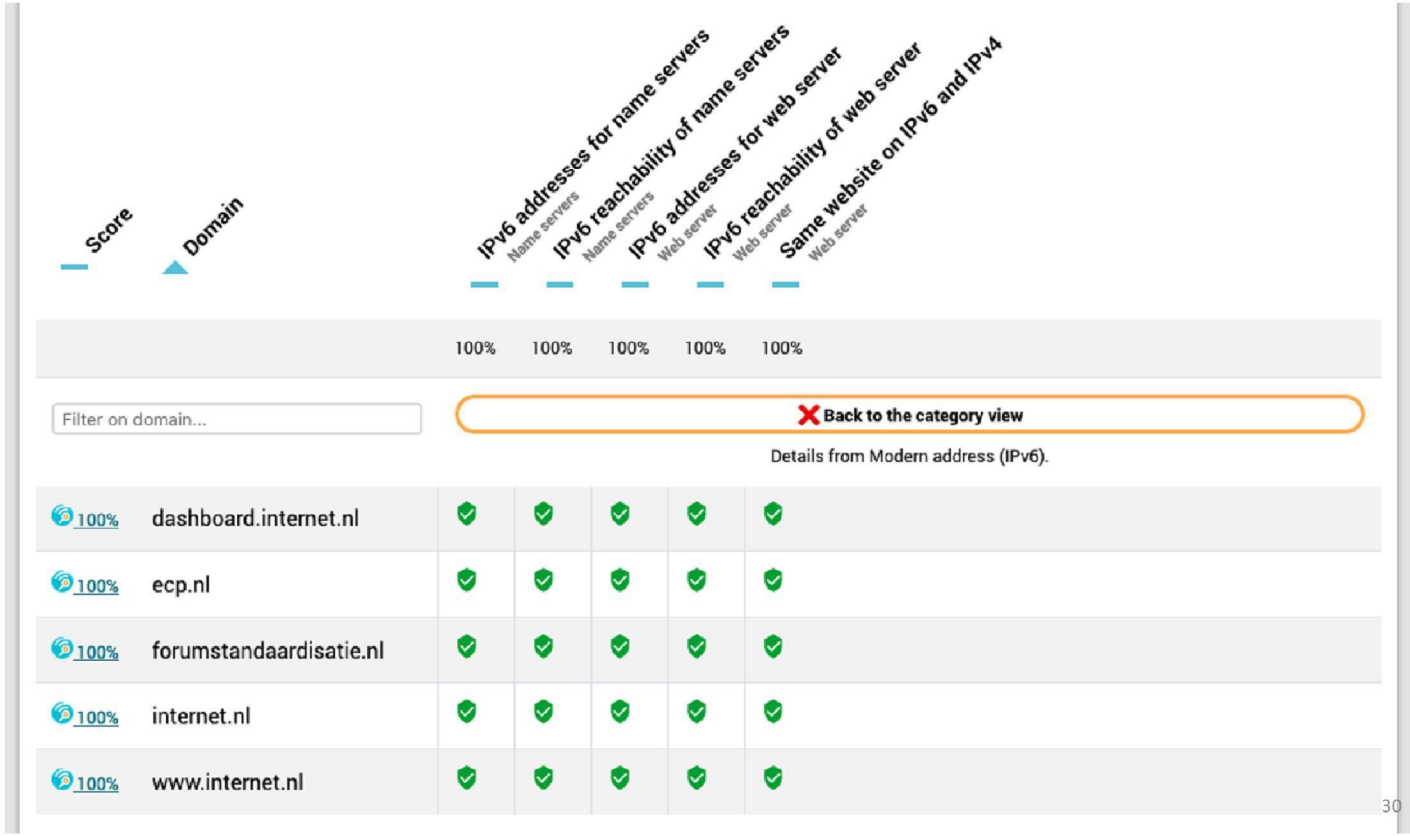
2. Beveiligingsstandaarden toepassen

- E-mail:
  - DMARC, DKIM en SPF: Echtheidswaarmerken ter preventie van spoofing
    STARTTLS en DANE: Encryptie van mailverkeer
- Websites:
  - HTTPS en HSTS: Beveiligde verbinding

- Internet (ook voor email en websites):
  - DNSSEC: integriteit domeinnaam-gegevens
  - RPKI: beveiliging internetroutering
  - IPv6: modern internetadres (duurzame bereikbaarheid)


Test voor moderne Internetstan
https://internet.nl
120%
Internet.nl
IS YOUR INTERNET UP TO DATE?
English Nederlands
Home Nieuws Kennisbank Hall of Fame Over Internet.nl
Moderne Internetstandaarden zorgen voor meer betrouwbaarheid en verdere groei van het Internet.
Gebruik jij ze al?
Test je website
Modern adres? Ondertekend domein? Beveiligde verbinding? Beveiligingsopties?
over de test
Jouw website-domeinnaam:
www.example.nl
Start test
Test je e-mail
Modern adres? Ondertekend domein? Anti-phishing? Beveiligde verbinding?
over de test
Jouw e-mailadres:
@ example.nl
Start test
Test je verbinding
Moderne adressen bereikbaar? Domein-handtekeningen gecontroleerd?
over de test
Start test
Nieuws
Lancering Hall of Fame voor Hosters
Nieuwe versie Internet.nl: X-XSS-Protection verwijderd en verbetering voor geen-MX-domeinen
Nieuwe TLS-richtlijnen geland in
Hall of Fame
100%
1153 domeinen met dubbele 100%
Laatste toevoeging: 02-02-2021
24ba.se
24base.net
Statistieken
349863 websitetesten
100%-score: 13882 websites
0-99%-score: 335981 websites
134625 e-mailtesten
100%-score: 3481 mailservers
0-99%-score: 131144 mailservers
28


Hall of Fame - Hosters
https://internet.nl/halloffame/hosters/
120%
Internet.nl
IS YOUR INTERNET UP TO DATE?
English Nederlands
Home Nieuws Kennisbank Hall of Fame Over Internet.nl
100% Internet.nl-compliant hosters
i24 ICT
Cloudwebservices
Exonet
Zylon
Fixmeister
Cobytes
Fastware
FYN Automatisering
Siem Hosting
AUVICOM Technologies
Internetional
mijn.host
Misterdot
Creagraphy
Vevida
Soverin
Intention
NederHost
Freedom Internet
Prolocation
TEDS-IT Automatisering
CARIEN.EU
BIT
bHosted
AmsterdamTech
Internet.nl
compliant hoster
100%
29


Score
Domain
IPv6 addresses for name servers
Name servers
IPv6 reachability of name servers
Name servers
IPv6 addresses for web server
Web server
IPv6 reachability of web server
Web server
Same website on IPv6 and IPv4
Web server
100%
100%
100%
100%
100%
Filter on domain...
Back to the category view
Details from Modern address (IPv6).
100% dashboard.internet.nl
100% ecp.nl
100% forumstandaardisatie.nl
100% internet.nl
100% www.internet.nl
30

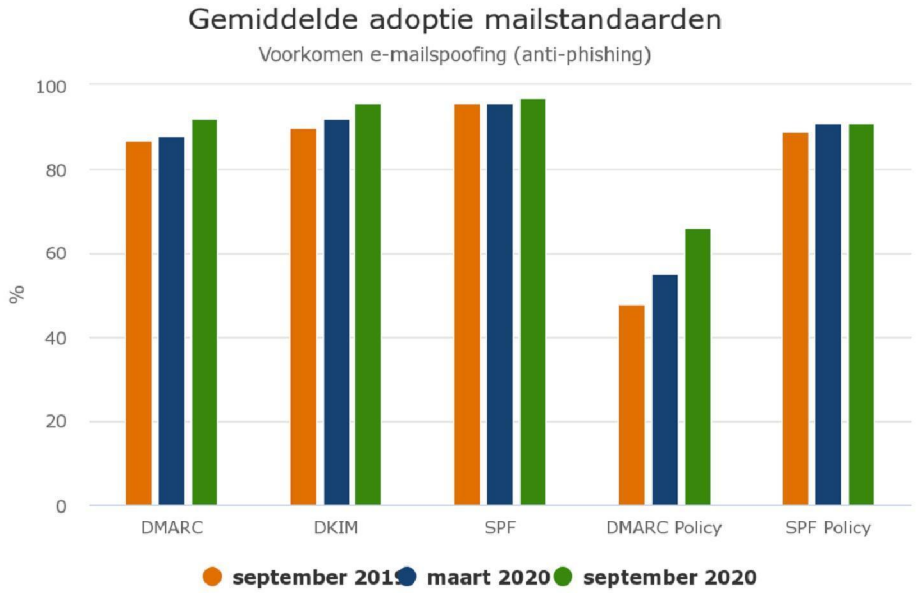
Verplichte open standaarden

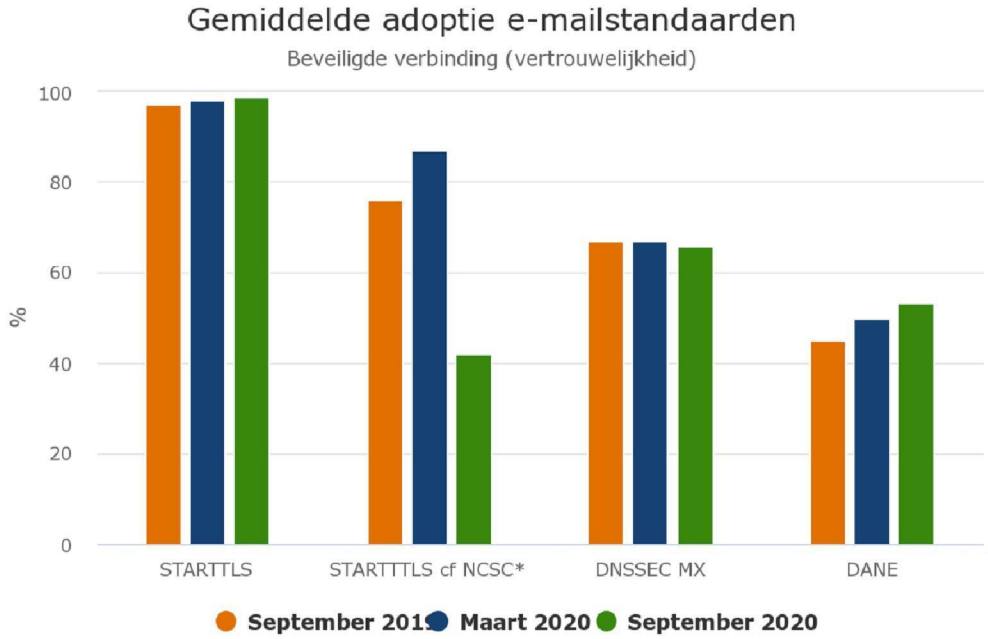
pas toe of leg uit

versie november 2019

Internet en beveiliging	
DKIM	Echtheidskenmerk voor ontvangen mail
DMARC	Beleid bij SPF-/DKIM ongeldige mail
DNSSEC	Controle van echtheid domeinnamen
HTTPS en HSTS	Versleuteling van webverkeer
IPv6 & IPv4	Internetadressering
ISO 27001	Managementsysteem informatiebeveiliging
ISO 27002	Richtlijnen en principes informatiebeveiliging
RPKI	Veilige netwerk routering
SAML	Authenticatie
SPF	Machtiging om mail te verzenden
STARTTLS en DANE	Versleuteling van mailverkeer

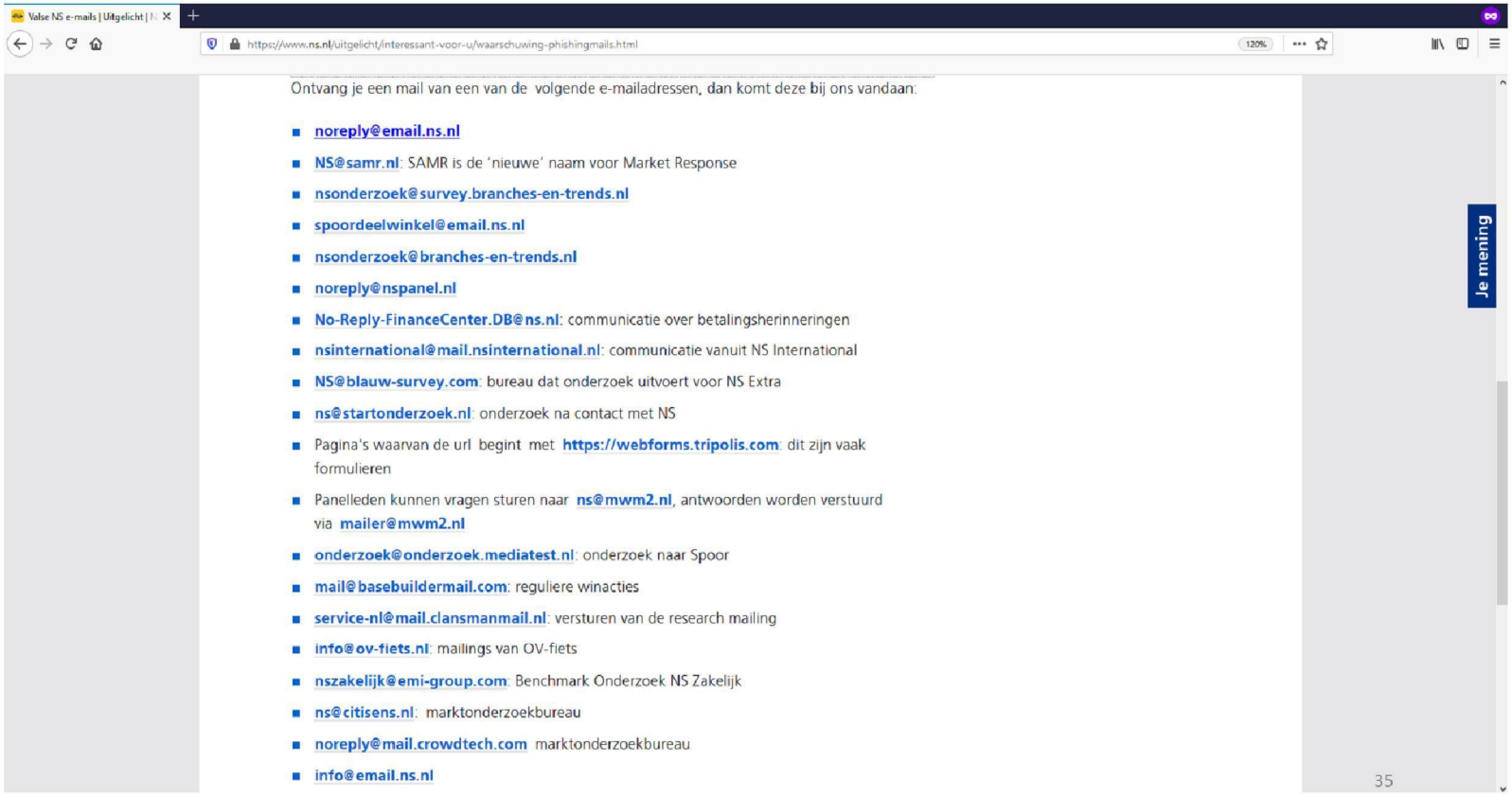
Metingen overheid




Gemiddelde adoptie e-mailstandaarden
Beveiligde verbinding (vertrouwelijkheid)
100
80
60
40
20
0
%
STARTTLS
STARTTTLS cf NCSC*
DNSSEC MX
DANE
September 2019
Maart 2020
September 2020

3. Duidelijke communicatie

- Gebruik één herkenbare domeinnaam.
- Communiceer duidelijk naar je doelgroep wat jouw domeinnaam is.


Valse NS e-mails | Uitgelicht | N
https://www.ns.nl/uitgelicht/interessant-voor-u/waarschuwing-phishingmails.html
120%
Ontvang je een mail van een van de volgende e-mailadressen, dan komt deze bij ons vandaan:
noreply@email.ns.nl
NS@samr.nl: SAMR is de 'nieuwe' naam voor Market Response
nsonderzoek@survey.branches-en-trends.nl
spoordeelwinkel@email.ns.nl
nsonderzoek@branches-en-trends.nl
noreply@nspanel.nl
No-Reply-FinanceCenter.DB@ns.nl: communicatie over betalingsherinneringen
nsinternational@mail.nsinternational.nl: communicatie vanuit NS International
NS@blauw-survey.com: bureau dat onderzoek uitvoert voor NS Extra
ns@startonderzoek.nl: onderzoek na contact met NS
Pagina's waarvan de url begint met https://webforms.tripolis.com: dit zijn vaak formulieren
Panelleden kunnen vragen sturen naar ns@mwm2.nl, antwoorden worden verstuurd via mailer@mwm2.nl
onderzoek@onderzoek.mediatest.nl: onderzoek naar Spoor
mail@basebuildermail.com: reguliere winacties
service-nl@mail.clansmanmail.nl: versturen van de research mailing
info@ov-fiets.nl: mailings van OV-fiets
nszakelijk@emi-group.com: Benchmark Onderzoek NS Zakelijk
ns@citisens.nl: marktonderzoekbureau
noreply@mail.crowdtech.com marktonderzoekbureau
info@email.ns.nl
Je mening
35


Phishing | PostNL
Phishing of fraude melden | Po
https://www.postnl.nl/klantenservice/probleem-klacht/phishing-of-fraude/wat-is-phishing-smishing/
260%
postnl
Inloggen
1. Controleer het e-mailadres van de afzender
Dit doe je door met je muis over de afzender te gaan en op de rechtermuisknop te klikken. Bij sommige e-mail providers is klikken niet nodig. Eindigt het adres op postnl.nl, bijvoorbeeld noreply@postnl.nl, account@postnl.nl, noreply@edm.postnl.nl etc.? Dan is het bericht waarschijnlijk betrouwbaar. Helemaal zeker is dat niet, want op sommige e-mail accounts komen tóch nepberichten binnen die afkomstig lijken van een PostNL adres. Het gaat dan vooral om accounts van Hotmail, Live en Outlook. We hebben hier beveiliging voor gemaakt, maar het is aan je provider om hier juist mee om te gaan.
Geef je mening
Phishing afzenders
36

Dus zorg goed voor je domeinnamen...

1. Goed domeinnaambeheer
2. Beveiligingsstandaarden toepassen
3. Duidelijke communicatie

We helpen graag!

Forum Standaardisatie

Email: info@forumstandaardisatie.nl

Internet.nl
IS YOUR INTERNET UP TO DATE?

Email: 5.1.2e @internet.nl