7 september 2023

Standaardistatieraad Onderwijs & Forum Standaardisatie

Forum Standaardisatie

Standaard Samenwerken

Forum Standaardisatie

Standaard Samenwerken

Waarom ook al weer?

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*.

rtlnieuws

Groot datalek bij Jeugdriagg: medische dossiers kwetsbare kinderen gelekt

01 oktober 2020 12:56
Aangepast: 01 oktober 2020 13:45

5 VRAGEN OVER PHISHING

Phishingmails worden steeds echter

Afgelopen jaar maakten criminelen bijna 4 miljoen euro buit met phishingfraude bij internetbankieren. In 2017 was dat nog iets meer dan een miljoen. Vooral 'speervissen', gericht op een specifieke persoon, is lucratief.

Waardoor is phishing toegenomen?
Fraudeurs gaan steeds geraffineerder te werk. Volgens Betaalvereniging Nederland wordt de kwaliteit van valse e-mails en websites beter. Hier worden slachtoffers naartoe gelokt waar ze, in de veronderstelling dat ze op de site van hun eigen bank zijn, inloggen met hun wachtwoord en hun rekeningnummer of creditcardnummer prijsgeven.
Vluchtig opgestelde teksten in slecht Nederlands maken plaats voor keurig ogende documenten met minder taalfouten en betere vormgeving en opmaak. Daarnaast kunnen criminelen tegenwoordig eenvoudig software kopen waarmee ze zonder diepgaande programmeerkennis snel een valse website of e-mail kunnen maken. Zo kunnen aanvallen snakkelijker, vaker en grootschaliger worden uitgevoerd.

Gebeurt phishing alleen via e-mail?
Criminelen benaderen slachtoffers vaker via sociale media, zoals Facebook en WhatsApp. Whatsappfraude is een vorm van 'spearphishing', Engels voor speervissen. Met speervissen wil een oplichter niet met een 'visnet' zo veel mogelijk slachtoffers maken, maar richt hij zich specifiek op een individu. Dat gaat zo: de oplichter stuurt een appje naar het slachtoffer en doet zich voor als familielid of vriend, door een profielfoto te kopiëren van bijvoorbeeld Facebook. De oplichter vindt de telefoonnummers van zijn doelwit op sites zoals Marktplaats. Daar vindt hij ook namen van familieleden en gesprekken die hij kan gebruiken om zich in zijn rol in te leven. De 'bekende' zegt in dringende geldnood te zitten en vraagt het slachtoffer om geld over te maken.

De campagne Veilig bankieren: 'Hang op, klik weg, bel uw bank!'

Hoe is speervissen te herkennen?
Het taalgebruik van het appje verraadt vaak de fraudeur. Een oplichter die zich voordoet als een vriend of kennis van wie je weet dat die gruwt van taalfouten, valt door de mand als hij appt: 'Hey. Dit is me nieuwe nummer, me oude telefoon is kapot'. Ook is het bij twijfel een goed idee om te bellen met de betreffende vriend of kennis om te vragen of het verhaal klopt. Bellen met de fraudeur schept ook snel duidelijkheid. Dat wil hij namelijk niet. Hij beweert dat dit niet kan of lukt, vanwege bijvoorbeeld een kapotte microfoon of slechte ontvangst.

De fraude met betaalpassen is daarentegen juist afgenomen. Hoe komt dat?
Nederlanders gaan zorgvuldiger om met hun bankpasjes en pincodes, vermoedt een woordvoerder van Betaalvereniging Nederland. Een tweede oorzaak ligt bij de toename van contactloos betalen. 'De vorm van betaalpasfraude die verreweg het meest gemeld wordt, is het afkijken van de pincode gevolgd door het rollen van de betaalpas. Door contactloos te betalen hoef je veel minder vaak je pincode in te tikken. Een fraudeur heeft dan ook geen gelegenheid om de pincode af te kijken.'

Heeft de anti-phishingcampagne van de banken dan niets opgeleverd?
Zeker wel, stelt de Betaalvereniging Nederland. Met de slogan 'Hang op, klik weg, bel uw bank!', voeren de brancheverenging en de Nederlandse Vereniging van Banken (NVB) al jarenlang campagne voor veilig bankieren. Hoewel de schade door phishing is toegenomen, denkt de brancheverenging dat de campagne wel effectief is. 'Als we geen campagne zouden voeren, zou de schade nóg groter zijn', aldus de woordvoerder.

Kirsten Zwanenburg

Advertentie

dossiers
sychische
ningen

Forum Standaardisatie

Standaard Samenwerken

Waarom ook al weer?

Forum Standaardisatie

Standaard Samenwerken

Waarom ook al weer?

Forum Standaardisatie
Standaard Samenwerken

Forum Standaardisatie

overheidsbrede samenstelling, met beleid & uitvoering, wetenschap & bedrijfsleven:

Larissa Zegveld, voorzitter (Kennisnet)
Rudi Bekkers (Universiteit Eindhoven)
Renate de Vree (Betaalvereniging)
Tom Kok, secretaris (Logius)
Cor Franke (Franke Interim Management)
Olivier van der Post (namens CIO Rijk)
Floor Jas (Surfnet)
Lindy van de Westelaken (BZK/DO)
Peter den Held (Gemeente Rotterdam)
Jolien van Zetten (NEN)

Thomas Faber (EZK/DE)
Benno Overeinder (NLnet Labs)
Friso Penninga (Geonovum)
Theo Peters (VNG Realisatie)
Geert-Jan van de Ven (Manifestgroep/CIP)
Marc van Hilvoorde (FIN/Belastingdienst)
Gerard Smits (Waterschapshuis)
Hans Tijl (IPO)
Michiel Steltman (DINL)
Gino Laan (Manifestgroep/Rinis)

Forum Standaardisatie

In 2006 opgericht om interoperabiliteit van de digitale overheid en de digitale economie te vergroten. Opdrachtgevers zijn BZK en EZK.

1. Forum adviseert overheidsbrede OBDO (voorheen Nationaal Beraad & College Standaardisatie). OBDO beslist.

2. Belangrijkste middel is de ‘Pas toe of leg uit’-lijst, met bestaande **open standaarden**. Deze zijn niet leveranciersgebonden & helpen vendor-lockin beperken.
   https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht

3. Ze helpen overheidsorganisaties (met verschillende leveranciers) digitaal te kunnen samenwerken in ketens, gegevens te kunnen hergebruiken en eenduidig met bedrijven & burgers te communiceren.

4. Doen verkenningen naar ‘bovensectorale problemen/kansen zonder eigenaar’

Forum Standaardisatie
Standaard Samenwerken

Forum Standaardisatie

In 2006 opgericht om inter van de digitale overheid en de digitale economie te vergroten. Op BZK en EZK.

1. Forum adviseert ove rheen Nationaal Beraad & College Standaardisatie). O

2. Belangrijkste mid uit lijst, met bestaande **open standaarden**. D sgebonden & helpen vendor-lockin te beperken.
   https://www.fo open-standaarden/lijst/verplicht

3. Ze helpen ove et verschillende leveranciers) digitaal te kunnen samenwerk gegevens te kunnen hergebruiken, en eenduidig met bedrijven e s te communiceren.

4. Doen verkenningen naar ‘bovensectorale problemen/kansen zonder eigenaar’

Forum Standaardisatie

Standaard Samenwerken

Waarom ook al weer?

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*.

rtlnieuws

Groot datalek bij Jeugdriagg: medische dossiers kwetsbare kinderen gelekt

01 oktober 2020 12:56
Aangepast: 01 oktober 2020 13:45

...e dossiers
...sychische
...ningen

OVER PHISHING

Phishingmails worden steeds echter

Afgelopen jaar maakten criminelen bijna 4 miljoen euro buit met phishingfraude bij internetbankieren. In 2017 was dat nog iets meer dan een miljoen. Vooral 'speervissen', gericht op een specifieke persoon, is lucratief.

Waardoor is phishing toegenomen?
Fraudeurs gaan steeds geraffineerder te werk. Volgens Betaalvereniging Nederland wordt de kwaliteit van valse e-mails en websites beter. Hier worden slachtoffers naartoe gelokt waar ze, in de veronderstelling dat ze op de site van hun eigen bank zijn, inloggen met hun wachtwoord en hun rekeningnummer of creditcardnummer prijsgeven.
Vluchtig opgestelde teksten in slecht Nederlands maken plaats voor keurig ogende documenten met minder taalfouten en betere vormgeving en opmaak. Daarnaast kunnen criminelen tegenwoordig eenvoudig software kopen waarmee ze zonder diepgaande programmeerkennis snel een valse website of e-mail kunnen maken. Zo kunnen aanvallen snakkelijker, vaker en grootschaliger worden uitgevoerd.

Gebeurt phishing alleen via e-mail?
Criminelen benaderen slachtoffers vaker via sociale media, zoals Facebook en WhatsApp. Whatsappfraude is een vorm van 'spearphishing', Engels voor speervissen. Met speervissen wil een oplichter niet met een 'visnet' zo veel mogelijk slachtoffers maken, maar richt hij zich specifiek op een individu. Dat gaat zo: de oplichter stuurt een appje naar het slachtoffer en doet zich voor als familielid of vriend, door een profielfoto te kopiëren van bijvoorbeeld Facebook. De oplichter vindt de telefoonnummers van zijn doelwit op sites zoals Marktplaats. Daar vindt hij ook namen van familieleden en gesprekken die hij kan gebruiken om zich in zijn rol in te leven. De 'bekende' zegt in dringende geldnood te zitten en vraagt het slachtoffer om geld over te maken.

De campagne Veilig bankieren: 'Hang op, klik weg, bel uw bank!'

Hoe is speervissen te herkennen?
Het taalgebruik van het appje verraadt vaak de fraudeur. Een oplichter die zich voordoet als een vriend of kennis van wie je weet dat die gruwt van taalfouten, valt door de mand als hij appt: 'Hey. Dit is me nieuwe nummer, me oude telefoon is kapot'. Ook is het bij twijfel een goed idee om te bellen met de betreffende vriend of kennis om te vragen of het verhaal klopt. Bellen met de fraudeur schept ook snel duidelijkheid. Dat wil hij namelijk niet. Hij beweert dat dit niet kan of lukt, vanwege bijvoorbeeld een kapotte microfoon of slechte ontvangst.

De fraude met betaalpassen is daarentegen juist afgenomen. Hoe komt dat?
Nederlanders gaan zorgvuldiger om met hun bankpasjes en pincodes, vermoedt een woordvoerder van Betaalvereniging Nederland. Een tweede oorzaak ligt bij de toename van contactloos betalen. 'De vorm van betaalpasfraude die verreweg het meest gemeld wordt, is het afkijken van de pincode gevolgd door het rollen van de betaalpas. Door contactloos te betalen hoef je veel minder vaak je pincode in te tikken. Een fraudeur heeft dan ook geen gelegenheid om de pincode af te kijken.'

Heeft de anti-phishingcampagne van de banken dan niets opgeleverd?
Zeker wel, stelt de Betaalvereniging Nederland. Met de slogan 'Hang op, klik weg, bel uw bank!', voeren de brancheverenging en de Nederlandse Vereniging van Banken (NVB) al jarenlang campagne voor veilig bankieren. Hoewel de schade door phishing is toegenomen, denkt de brancheverenging dat de campagne wel effectief is. 'Als we geen campagne zouden voeren, zou de schade nóg groter zijn', aldus de woordvoerder.

Kirsten Zwanenburg

Forum Standaardisatie

Standaard Samenwerken

Waarom ook al weer?

Forum Standaardisatie

Standaard Samenwerken

Waarom ook al weer?

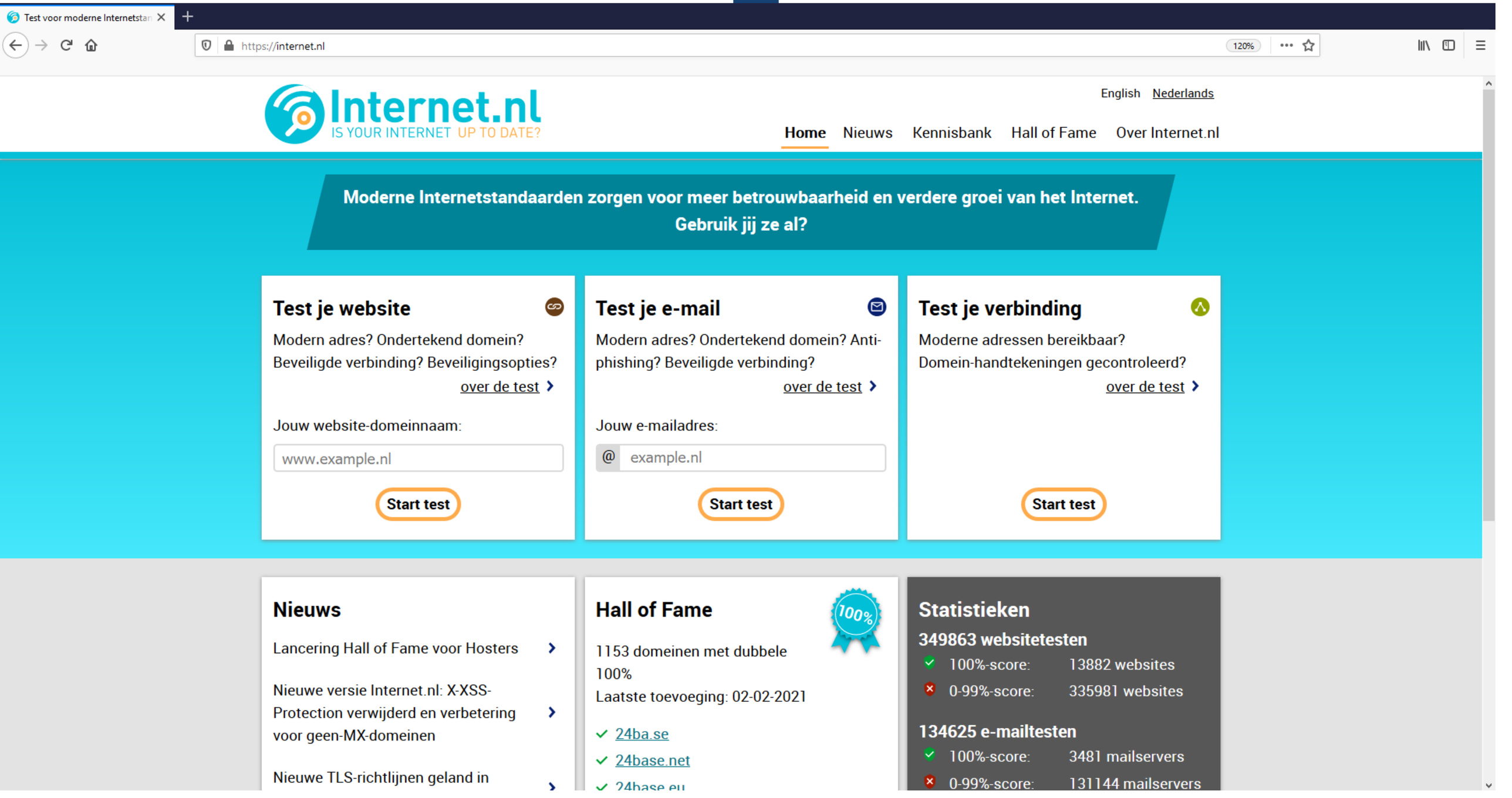
Forum Standaardisatie

Standaard Samenwerken

80% van werk Forum =

‘Pas toe of leg uit’-lijst

- Afspreken / Status geven
- Stimuleren
- Meten


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
24base.eu
Statistieken
349863 websitetesten
100%-score: 13882 websites
0-99%-score: 335981 websites
134625 e-mailtesten
100%-score: 3481 mailservers
0-99%-score: 131144 mailservers

Forum Standaardisatie
Standaard Samenwerken

Nieuwe kansen

- Signaleren
- Agenderen
- Adresseren
- Operationaliseren

Synergie Standaardisatie-raad onderwijs & Forum Standaardisatie?

- Onderwijs gebruiker van ’Pas toe of leg uit - standaarden, zoals informatieveiligheid standaarden:

  Edustandaard: Uniforme Beveiligings Voorschriften (UBV)

  (toelichting Jordy van den Elshout van Kennisnet)

Synergie Standaardisatie-raad onderwijs & Forum Standaardisatie?

- Onderwijs gebruiker van ’Pas toe of leg uit - standaarden, zoals informatieveiligheid standaarden
- Onderwijs zou ‘Pas toe of leg uit’ lijst als boven sectoraal instrument kunnen gebruiken
- Leren van elkaar (proces, handreikingen, adoptie)
- Link met/in Forum?
- Suggesties leden raad?

Vragen?

Forum Standaardisatie is bereikbaar via:

1. www.forumstandaardisatie.nl
2. info@forumstandaardisatie.nl
3. 070 - 888 7776
4. Twitter: @openstandaarden
   Youtube
   Linkedin
   Mastodon:
   https://social.overheid.nl/@forumstandaardisatie

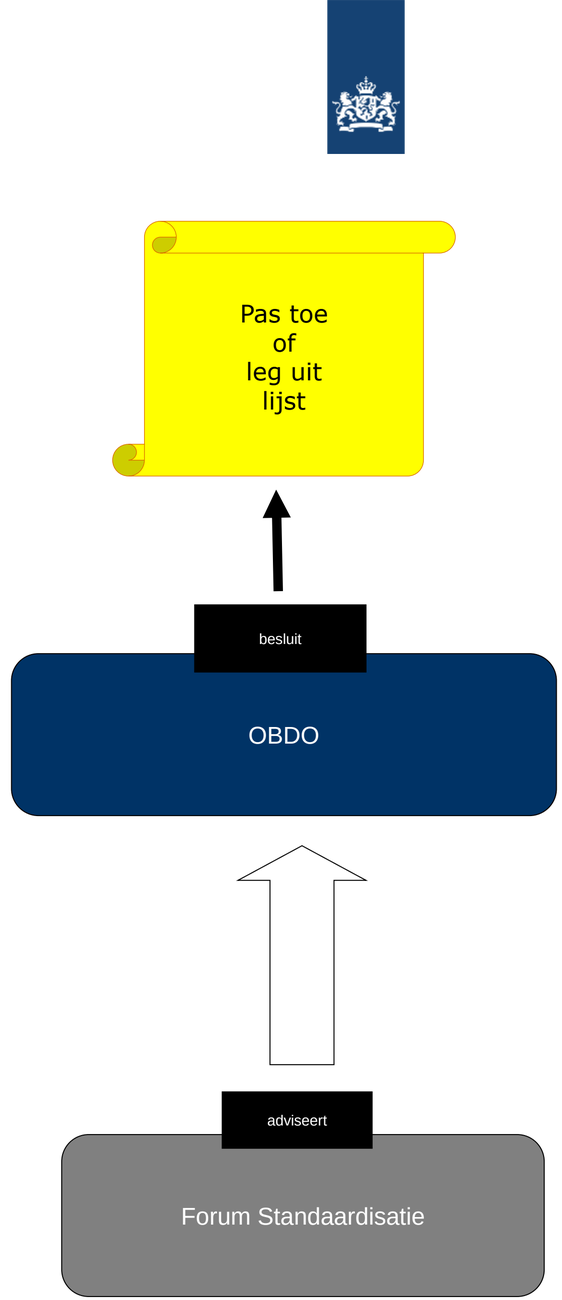
Forum Standaardisatie

Standaard Samenwerken

Sheets voor achter de hand

Forum Standaardisatie

Standaard Samenwerken



Forum Standaardisatie
Standaard Samenwerken

23 maart 2023

80% van werk Forum =

‘pas toe of leg uit’-lijst

Forum standaardisatie ontwikkelt zelf geen standaarden

- Afspreken / Status geven door oa expert advies, Internetconsultatie
- Stimuleren
- Meten

Forum Standaardisatie

Standaard Samenwerken

8 september 2023

c) inhoudelijke inbreng te leveren bij het aanwijzen van wettelijk verplicht toe te passen open standaarden;

d) het periodiek toetsen en het publiceren van de naleving van overheidsbrede afspraken over het gebruik van open standaarden, onder meer aan de hand van een jaarlijkse monitor en een halfjaarlijkse meting van het gebruik van informatieveiligheidsstandaarden en het aanspreken van achterblijvende partijen, onder meer via het OBDO, op het gebruik van de ‘pas toe of leg uit’-standaarden en het naleven van het ‘pas toe of leg uit’-beleid;

e) het doen van voorstellen voor het verweven van standaardisatie- en open

Forum Standaardisatie

Standaard Samenwerken

ICTU

Rapport

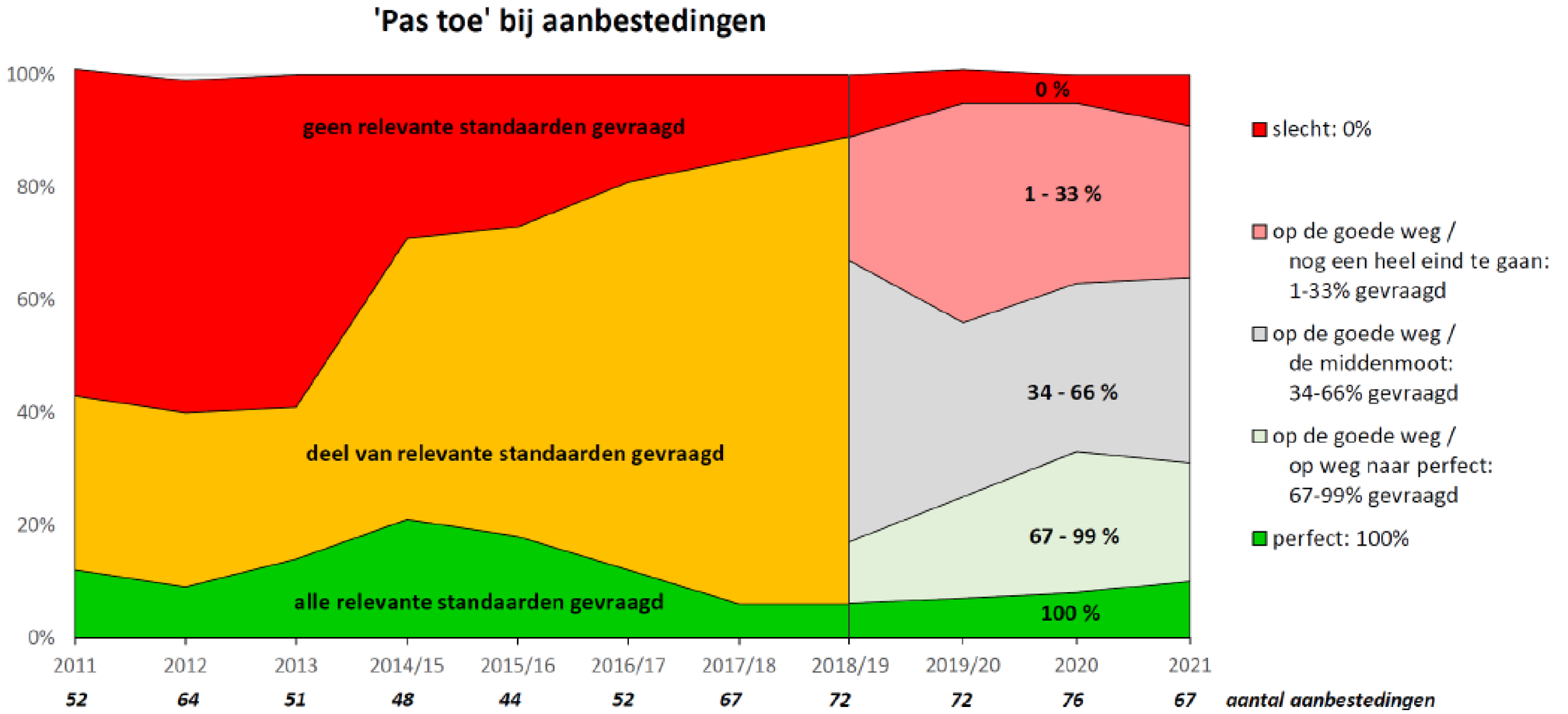
Monitor Open standaarden 2022

Onderzoek naar het gebruik van open standaarden van de 'pas toe of leg uit'-lijst van het Forum Standaardisatie: bij aanbestedingen, in voorzieningen en per standaard

Forum Standaardisatie
Standaard Samenwerken

'Pas toe' bij aanbestedingen, 2011 – 2021

Rond de 50%

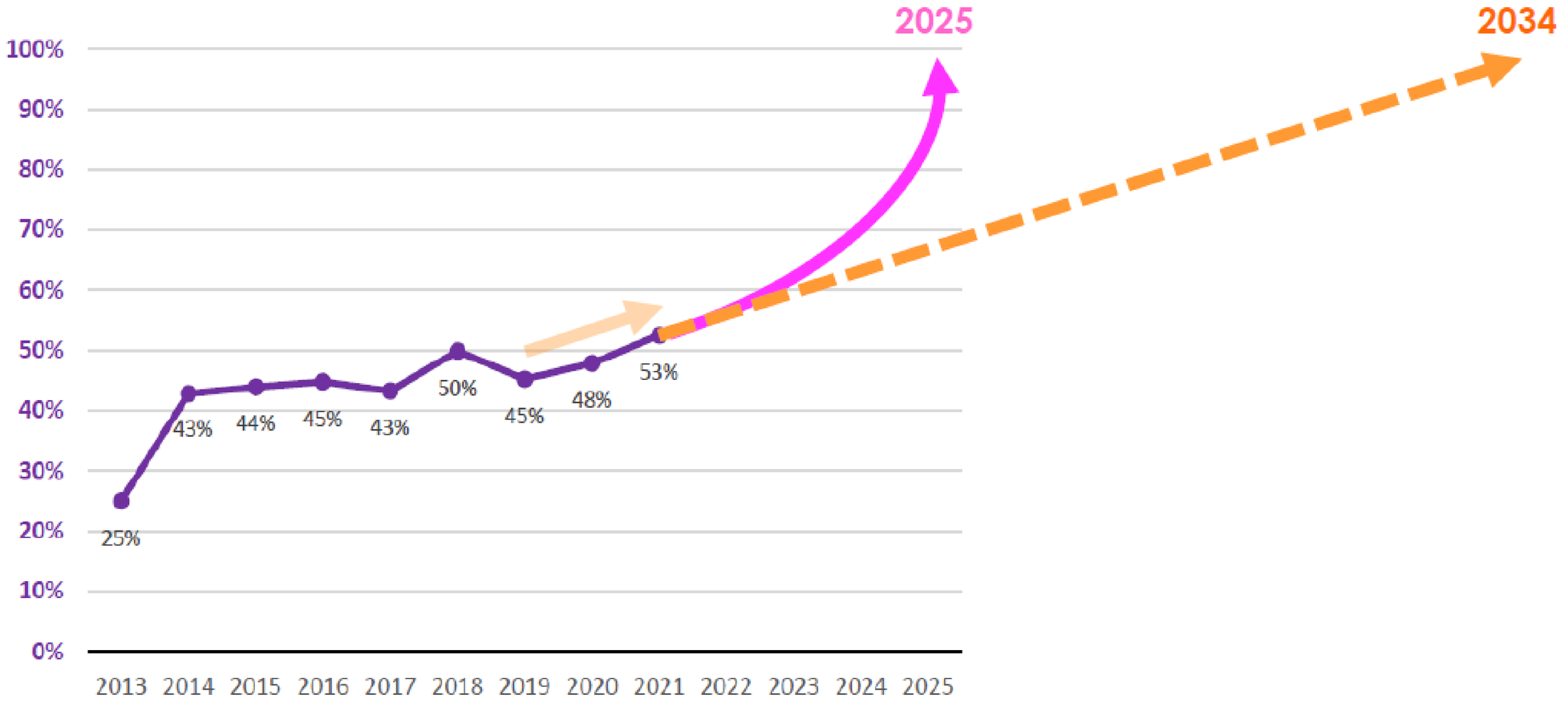


Bron: Monitor open standaarden 2022

Forum Standaardisatie

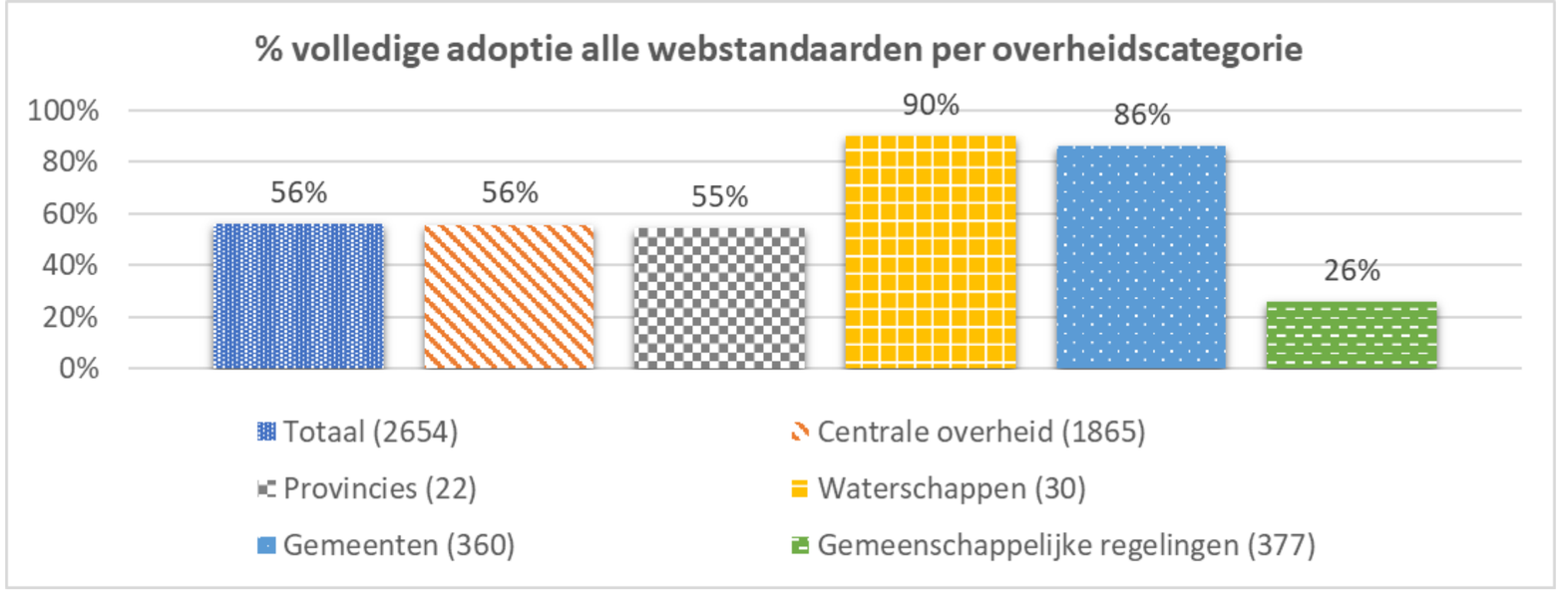
Standaard Samenwerken

Extrapolatie van 'Pas toe' bij aanbestedingen: wanneer wordt 100% bereikt?

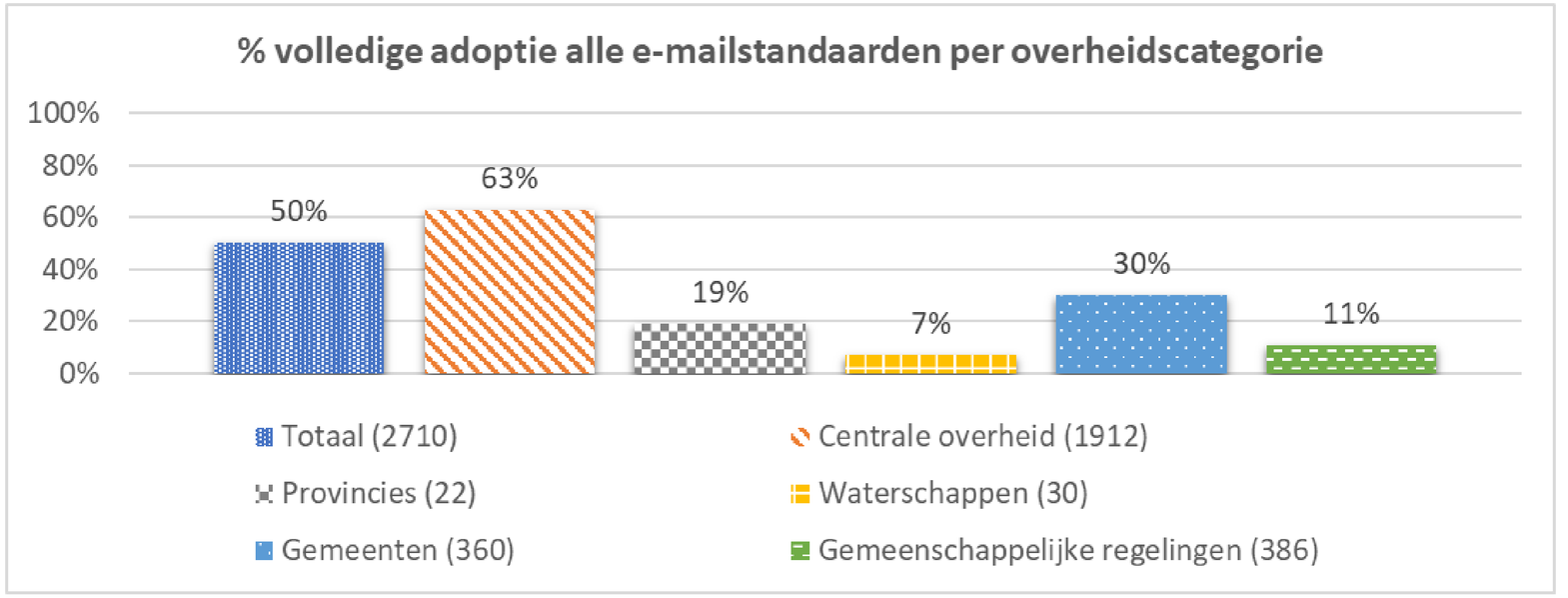


Bron: Monitor open standaarden 2022

Forum Standaardisatie
Standaard Samenwerken



56%



50%

Bron: meting informatieveiligheidstandaarden voorjaar 2023

Forum en Gemeenschappelijke Digitale Infrastructuur

1. Standaarden zitten overal in GDI:
   Basisregistraties, Federatief Stelsel Berichtenbox, PKIoverheid, eHerkenning e-Factureren etc. etc.

2. Adagium MIDO
   “Afspraken boven Standaarden boven Voorzieningen”

3. Synergy MIDO en Forum (voorzitter Forum in Architectuurraad):
   -Achterblijvers over de streep helpen (traditionele rol)
   -Burger centraal (herkenbare en gebruiksvriendelijke digitale overheid)
   -Harmonisatie & standaardisatie kansen Signaleren Agenderen Adresseren (ook internationaal)