Cybersecurity onderzoek Alert Online 2025

Deelrapport overheid

Ipsos i&O

Ministerie van Economische Zaken

www.ipsos-publiek.nl

Colofon

Uitgave
Ipsos I&O
Piet Heinkade 55
1019 GM Amsterdam

Rapportnummer
2025/157

Datum
augustus 2025

Opdrachtgever
Ministerie van Economische Zaken

Auteurs
Sara Kellij
Bram Doms
Melle Conradie

Inhoudsopgave

1 Samenvatting

Samenvatting | 1/2

Acht op de tien ambtenaren schatten eigen kennis online veiligheid in als redelijk tot goed
Acht op de tien ambtenaren vinden dat de eigen kennis over online veiligheid redelijk tot zeer goed is. Een vijfde vindt het eigen kennisniveau matig of nog minder (17% matig, 3% slecht, 0% zeer slecht). Dat is vergelijkbaar met de inschatting van medewerkers in het grootbedrijf.

Behalve met CEO-fraude, is de meerderheid van de ambtenaren bekend met elf voorgelegde vormen van cybercrime. Phishing, hacking en identiteitsfraude zijn de bekendste vormen van cybercrime, evenals in 2024. DDoS-aanvallen zijn beter bekend onder ambtenaren dan vorig jaar (van 79% naar 84%). Dat geldt ook voor CEO-fraude (van 32% naar 41%). Op het werk zien ambtenaren phishing (61%), DDoS-aanvallen (60%) en hacking (57%) als de meest waarschijnlijke bedreigingen.

Drie op de tien ambtenaren maken zich wel eens zorgen om digitale veiligheid op het werk
Zeven op de tien ambtenaren (71%) zijn relatief zorgeloos over de digitale veiligheid in de werksituatie. Drie op de tien maken zich enige (26%) of veel (3%) zorgen. Het beeld is vergelijkbaar met een jaar eerder. Onder medewerkers van het grootbedrijf is een vergelijkbaar beeld te zien. Ambtenaren beoordelen zichzelf met een 6,9 voor het omgaan met online risico's. Negen procent van de ambtenaren geeft zichzelf een onvoldoende hiervoor. Een kwart van de ambtenaren (25%) geeft zichzelf een 8 of hoger. Dat is minder dan vorig jaar (37% gaf zichzelf toen een 8 of hoger).

Meer acties ondernomen voor online veilig gedrag
Twee-staps-inloggen is de meest genomen maatregel voor online veilig gedrag bij de overheid: bij driekwart van de ambtenaren is dat verplicht. Ten opzichte van 2024 worden er meer acties ondernomen om veilig gedrag te bevorderen. Zo worden er meer trainingen over online veiligheid gegeven (van 48% naar 59%) en is er vaker een digitale hulpverlener (van 42% naar 57%). Ook kunnen vaker alleen systeembeheerders software installeren.

Samenvatting | 2/2

Melden mogelijke bedreigingen wordt in de meeste organisaties gewaardeerd
De meeste ambtenaren vinden dat het gemakkelijk is om zich aan de afspraken over veilig online gedrag te houden (91%). Ook de tools en instrumenten die men daarvoor krijgt, vinden ambtenaren goed (90%). Bij 87 procent van de ambtenaren wordt het gewaardeerd als mogelijke bedreigingen worden gemeld. Driekwart (77%) vindt dat digitale veiligheid hoog op de agenda staat van de directie. Wel vinden ambtenaren minder vaak dan medewerkers van het grootbedrijf dat afspraken voldoende worden toegepast.

Schaamte weerhoudt ambtenaren niet om cyberincidenten te melden
Het overgrote deel van de ambtenaren zou een gedownload virus meteen melden bij de ICT-afdeling (94%), vier procent zou dit uit schaamte niet doen. Twee derde van de ambtenaren (64%) zou zich schamen als ze op een phishinglink zouden klikken. Toch voelen negen op de tien (88%) zich wel comfortabel genoeg om een incident te melden als ze dit zouden meemaken. Bij driekwart van de ambtenaren (74%) wordt open communicatie over cyberincidenten dan ook aangemoedigd.

Bij de helft van de ambtenaren wordt generatieve AI binnen de organisatie gebruikt. Een derde (35%) krijgt vanuit de organisatie ook duidelijke richtlijnen over het gebruik ervan.

Meer meegemaakte voorvallen cybercrime op werk
Vier op de tien ambtenaren (43%) maakten in de afgelopen 12 maanden een of meerdere pogingen tot cybercrime mee op het werk. Dat is meer dan in 2024 (toen: 29%). Vooral phishing (van 22% naar 32%) en telefoontjes van iemand die zich anders voordeed (van 1% naar 10%) kwamen vaker voor.

De helft van de ambtenaren deed geen melding of aangifte van de cybercrime waar ze slachtoffer van werden op het werk. Ambtenaren die wel een melding maakten, deden dit vaak bij de eigen ICT-afdeling. De voornaamste reden om geen actie te ondernemen, is dat het incident niet als belangrijk werd gezien (34%) of dat er weinig schade ondervonden werd (33%). De belangrijkste redenen om wel aangifte te doen, zijn het creëren van een veiligere online omgeving (49%) en voorkomen dat de dader nieuwe slachtoffers maakt (42%).

2 Inleiding en achtergrond

Inleiding

Aanleiding en achtergrond

Alert Online is een gezamenlijk initiatief van overheid, bedrijfsleven en wetenschap, dat zich richt op het creëren van bewustwording rondom digitale veiligheid. Daarnaast beoogt Alert Online onder diverse doelgroepen de kennis over digitale veiligheid te vergroten en cyberveilig gedrag te stimuleren. Dit wordt gedaan door kennisoverdracht via veiliginternetten.nl, het Digital Trust Center en met een specifiek partnernetwerk van organisaties in Nederland. Alert Online bestaat uit de jaarlijkse cybersecuritymaand in oktober. Een onderdeel van deze campagne is het jaarlijks terugkerende Cybersecurityonderzoek Alert Online. Met de resultaten van het onderzoek wordt de cybersecuritymaand op 29 september afgetrapt.

In opdracht van het ministerie van Economische Zaken (EZ) voerde Ipsos I&O dit onderzoek uit naar de beleving van de digitale veiligheid onder Nederlanders.

Onderzoeksdoel

Het onderzoek beoogt aanknopingspunten te bieden voor communicatie en beleidsvorming. Dit doen we door middel van (1) het monitoren van het bewustzijn en de vaardigheden omtrent online veiligheid van Nederlanders door de jaren heen en (2) inzichten te vergaren in de kennis, houding en gedrag van Nederlanders over digitale veiligheid.

Onderzoeksvragen

De hoofdvraag van het onderzoek luidt:
Wat is de kennis, houding en gedrag van verschillende doelgroepen op het gebied van (verbeteren van) online veiligheid?

Dit deelrapport richt zich specifiek op de doelgroep ambtenaren.

De hoofdvraag behandelen we in dit rapport in de volgende drie deelvragen:

1 Wat weten ambtenaren over online veiligheid en het verbeteren van de online veiligheid?
2 Wat vinden ambtenaren van hun eigen online gedrag als het gaat om veiligheid en vaardigheden?
3 Wat doen ambtenaren op het gebied van hun online veiligheid en het verbeteren daarvan?

Leeswijzer

Dit deelrapport behandelt de resultaten van ambtenaren. De resultaten van ambtenaren worden vergeleken met de resultaten van medewerkers van grote bedrijven met meer dan 200 werknemers.

Hoofdstuk 3 t/m 5 van dit rapport behandelen de onderzoeksresultaten voor de drie onderzoeksvragen. Hoofdstuk 3 gaat in op kennis van en ervaring met online risico's. Hoofdstuk 4 behandelt de zorgen die men heeft over online risico's en het online gedrag en regels op het werk. Het rapport sluit af met hoofdstuk 5 over slachtofferschap en aangiftebereidheid.

Naast dit deelrapport is er nog een hoofdrapport dat ingaat op de resultaten voor de Nederlandse bevolking en een deelrapport gericht op het bedrijfsleven.

De percentages in deze rapportage worden afgerond op hele cijfers. Hierdoor tellen de percentages in sommige figuren en tabellen op tot 99 of 101 procent. In de rapportage zijn de uitkomsten waar mogelijk vergeleken met de resultaten van 2023. Significante toenames zijn weergegeven met het symbool "+" en significante afnames met het symbool "-". Daarnaast gaat het bij alle benoemde verschillen om significante verschillen ($p < .05$).

Methode en respons

In totaal vulden 391 ambtenaren een online vragenlijst in. Het gaat om 184 ambtenaren werkzaam bij de overheid (Rijk, provincie, gemeente) en 207 die werkzaam zijn bij de semioverheid.[1] Ambtenaren worden in dit rapport vergeleken met medewerkers van het grootbedrijf (>200 medewerkers). Er zijn 455 medewerkers van een grootbedrijf die hebben meegewerkt aan het onderzoek. Respondenten zijn afkomstig uit het I&O Research Panel[2]. Het online veldwerk vond plaats van 23 juni tot 6 juli 2025.

[1] *Dit is op basis van zelfopgave. Men kon in de vragenlijst de optie "Ik ben werkzaam bij de semioverheid (Waterschappen, Politie, etc.)" selecteren.*
[2] *https://www.ioresearch.nl/onderzoeksmethoden/io-research-panel/*

3 Kennis en ervaring online risico’s

Acht op tien ambtenaren beoordelen eigen kennis als redelijk tot goed

- Acht op de tien (80%) ambtenaren beoordelen de eigen kennis over digitale veiligheid als redelijk tot zeer goed. Een vijfde vindt het eigen kennisniveau matig of slecht (17% matig, 3% slecht, 0% zeer slecht).

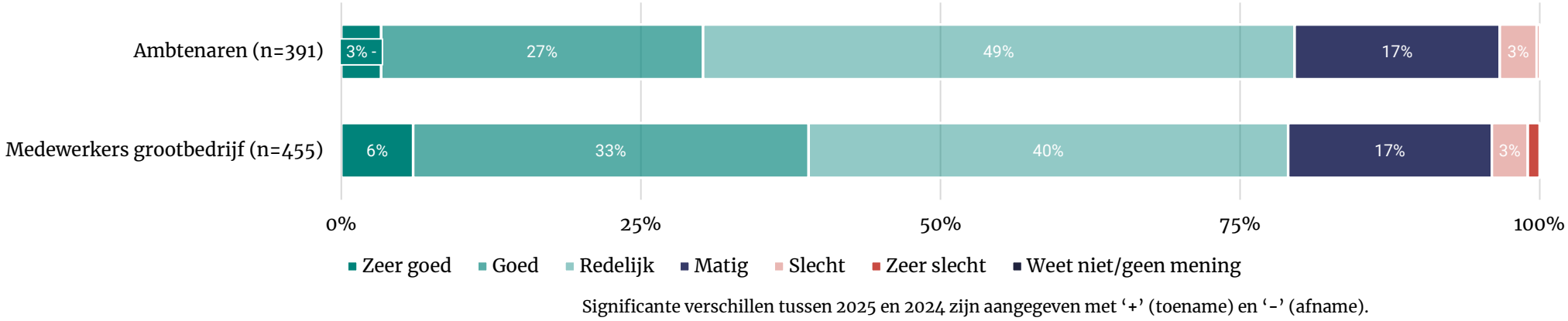
Vergelijking met 2024

- Vergeleken met 2024 beoordelen minder ambtenaren de eigen kennis als zeer goed (toen 9%).

Vergelijking grootbedrijf

- Medewerkers van het grootbedrijf schatten hun kennis over digitale veiligheid vaker in als (zeer) goed terwijl ambtenaren hun kennis hierover vaker als matig of redelijk inschatten.

Hoe schat u uw eigen kennis over digitale veiligheid in?



Significante verschillen tussen 2025 en 2024 zijn aangegeven met '+' (toename) en '-' (afname).

Meerderheid ambtenaren denkt DDoS-aanval, phishing en hacking op werk mee te kunnen maken

- Tien van de elf voorgelegde vormen van cybercrime zijn bij een meerderheid van de ambtenaren bekend.
- Ruim de helft denkt op het werk met phishing, hacking en een DDoS-aanval te maken te kunnen krijgen.

Vergelijking met 2024

- Meer ambtenaren zijn bekend met DDoS-aanvallen en CEO-fraude dan in 2024 (toen resp. 79% en 32%). Men acht de kans om met CEO-fraude te maken te krijgen kleiner (2024: 31%).

Vergelijking grootbedrijf

- De resultaten van het grootbedrijf lijken op die van de overheid. Ambtenaren verwachten vaker te maken te krijgen met DDoS-aanvallen en minder vaak met misbruik van bedrijfsnaam, QR-codefraude en CEO-fraude.

In deze tabel staan 11 voorgelegde vormen van cybercriminaliteit, op volgorde van bekendheid	Kent de betekenis (naar eigen zeggen)		Denkt er in werksituatie mee te maken te kunnen krijgen*	
	Ambtenaren (n=391)	Medewerkers grootbedrijf (n=455)	Ambtenaren	Medewerkers grootbedrijf
Helpdeskfraude (bijvoorbeeld neptelefoontje van bank of softwareaanbieder)***	99% +	98% +	24% + n=386	28% + n=447
Phishing	97%	97%	61% n=379	62% + n=443
Hacking	97%	97%	57% n=378	60% + n=443
Identiteitsfraude**	97%	98%	24% n=375	28% n=445
Misbruik van bedrijfsgegevens/bedrijfsnaam voor online aankopen**	89%	88%	28% n=352	35% n=401
DDoS-aanval	84% +	82% +	60% n=334	48% n=372
Aankoopfraude**	84%	83%	6% n=331	9% n=376
Malware	83%	80%	44% n=330	43% n=366
Ransomware	77%	76%	43% n=306	41% n=344
QR-codefraude (Quishing)	60%	65%	13% n=221	18% n=298
CEO-fraude	41% +	48% +	11% - n=146	24% - n=219

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager).
Significante verschillen tussen 2025 en 2024 zijn aangegeven met '+' (toename) en '–' (afname).
*Alle begrippen voorgelegd waarvan men de betekenis zegt te kennen | percentage zeker + waarschijnlijk wel.
**Vergelijking met voorgaande jaar niet mogelijk door lage responsaantallen of omdat deze niet voorkwam in de vorige meting.
***in 2024 gevraagd als 'helpdeskfraude'

4 Zorgen en online gedrag op het werk

Zeven op tien ambtenaren geen zorgen over digitale veiligheid werk

- Drie op de tien ambtenaren maken zich wel eens zorgen over de digitale veiligheid op het werk. Drie procent maakt zich (zeer) veel zorgen. Zeven op de tien ambtenaren maakt zich weinig of geen zorgen om de digitale veiligheid in de werksituatie.

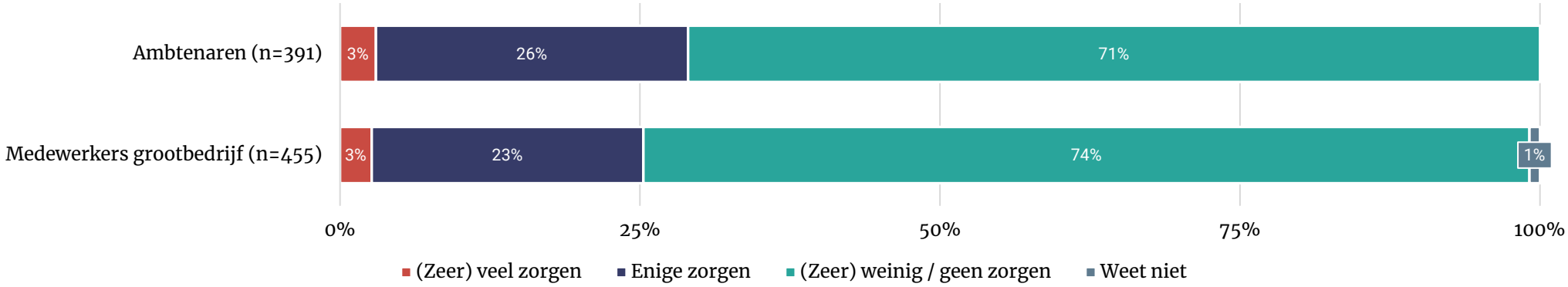
Vergelijking met 2024

- Men maakt zich net zoveel zorgen als in 2024.

Vergelijking grootbedrijf

- Ambtenaren en medewerkers van het grootbedrijf maken zich in vergelijkbare mate zorgen om de digitale veiligheid op het werk.

In hoeverre maakt u zich zorgen over uw digitale veiligheid in uw werksituatie?



Ambtenaren geven zichzelf een 6,9 voor omgaan met online risico's

- Een kwart van de ambtenaren geeft zichzelf een 8 of hoger als het gaat om het veilig omgaan met online risico's. Negen procent geeft zichzelf een onvoldoende. Twee derde beoordeelt de omgang met online risico's als redelijk en geeft zichzelf een 6 of een 7. Ambtenaren geven zichzelf gemiddeld een 6,9.
- Ambtenaren die een hoog cijfer geven, zijn naar eigen zeggen op de hoogte van de online risico's en zijn hier alert op. Ambtenaren die zichzelf gemiddeld in schatten (cijfer 6-7) geven aan wel enigszins kennis te hebben over risico's maar dat dit nog beter zou kunnen. Ambtenaren die een lager cijfer geven, zeggen moeite te hebben om online risico's in te schatten of weinig maatregelen te nemen.

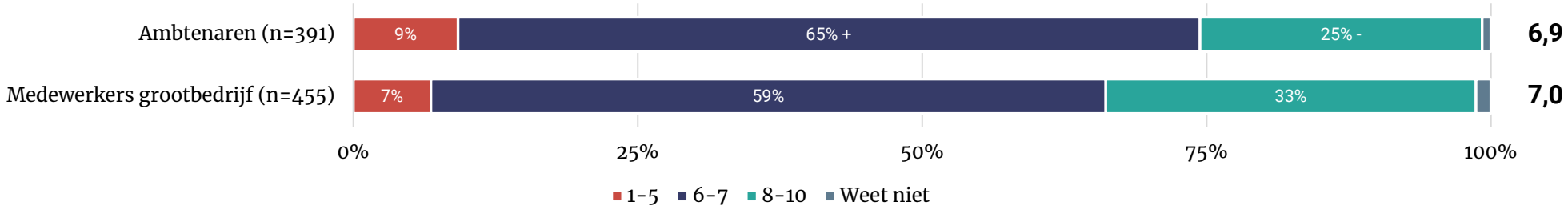
Vergelijking met 2024

- Het aandeel ambtenaren dat zichzelf een 8 of hoger geeft voor het omgaan met online risico's is afgenomen ten opzichte van 2024 (37%). Meer ambtenaren geven zichzelf nu een 6 of 7 in vergelijking met 2024 (2024: 55%, nu: 65%).
- Ten opzichte van 2024 wijkt het gemiddelde cijfer dat men zichzelf geeft niet significant af.

Vergelijking grootbedrijf

- Medewerkers van het grootbedrijf beoordelen hun omgang met online risico's vaker met een 8 of hoger dan ambtenaren.

Welk cijfer geeft u uzelf als het gaat om het veilig omgaan met online risico's?



Twee-staps-inloggen vaker verplicht bij overheid dan grootbedrijf

- Bij de overheid moet driekwart gebruik maken van twee-staps-inloggen.
- Bij zeven op de tien ambtenaren zijn er adviezen/richtlijnen/regels over online veilig gedrag van medewerkers.

Vergelijking met 2024

- Ten opzichte van 2024 worden er meer maatregelen genomen bij overheidsorganisaties. Zo worden er meer trainingen gegeven (2024: 48%) en is er vaker dan in 2024 een digitale hulpverlener (toen: 42%).

Vergelijking grootbedrijf

- Medewerkers van het grootbedrijf hebben minder vaak twee-staps-inloggen en kunnen vaker zelf software installeren op hun werkcomputer. Wel wordt er bij grootbedrijven vaker getoetst op veilig online gedrag door bijvoorbeeld nep phishingmails.

Welke acties zijn er binnen uw bedrijf/organisatie ondernomen ten behoeve van online veilig gedrag?	Ambtenaren (n=391)	Medewerkers grootbedrijf (n=455)
Twee-staps-inloggen is verplicht voor toegang	74%	64% +
Er zijn adviezen/richtlijnen/regels over online veilig gedrag van medewerkers*	71%	68%
Alleen de systeembeheerders kunnen software installeren	68% +	55%
Er worden trainingen gegeven binnen mijn organisatie over online veiligheid	59% +	60% +
Er is binnen mijn organisatie/bedrijf een digitale hulpverlener waar je terechtkunt	57% +	49% +
Er zijn afspraken gemaakt over het gebruik van zakelijke apparaten smartphones, laptops en/of tablets voor privé en/of zakelijk gebruik	55%	55%
Er wordt getoetst op veilig online gedrag door bijvoorbeeld op willekeurige momenten nep phishingmails te sturen**	48% +	58% +
De toegang tot bepaalde websites en/of socialmediakanalen is geblokkeerd	45%	47%
Anders	3%	2%
In mijn bedrijf of organisatie is geen enkele actie ondernomen ten behoeve van veilig online gedrag	0%	0%
Weet ik niet	8%	12% -

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager). Significante verschillen tussen 2025 en 2024 zijn aangegeven met '+' (toename) en '-' (afname).

*niet gevraagd in 2024.
**in 2024: Er worden op willekeurige momenten testmails verstuurt om medewerkers te testen op de herkenning van phishing.

Twee derde ambtenaren vindt dat de afspraken voldoende worden toegepast

- Negen op de tien ambtenaren vinden het makkelijk om zich aan de afspraken voor veilig online gedrag houden.
- De helft van de ambtenaren wordt erop aangesproken als ze zich niet aan de werkafspraken over veilig online gedrag houden.

Vergelijking met 2024

- Meer ambtenaren vinden het gemakkelijk om zich aan afspraken te houden voor online veilig gedrag dan in 2024 (toen: 84%). Ook vinden meer ambtenaren dat ze daar goede tools voor krijgen.
- Minder ambtenaren spreken hun collega's erop aan als ze zich niet houden aan de werkafspraken voor online veilig gedrag.

Vergelijking grootbedrijf

- Ambtenaren vinden minder vaak dat de afspraken over veilig online gedrag voldoende worden toegepast in vergelijking met het grootbedrijf.
- Daarnaast spreken medewerkers van het grootbedrijf hun collega's vaker aan als ze zich niet aan de werkafspraken over veilig gedrag houden.

In hoeverre bent u het eens of oneens met de volgende stellingen? % (zeer) eens. Voorgelegd aan personen waar afspraken op het werk zijn gemaakt.	**Ambtenaren (n=360)**	**Medewerkers grootbedrijf (n=398)**
Het is gemakkelijk om mij aan de afspraken te houden over veilig online gedrag binnen mijn bedrijf of organisatie	91% +	89%
Ik krijg toegang tot goede tools en instrumenten (bijvoorbeeld twee-staps-inloggen of een wachtwoordmanager) om veilig online gedrag te bevorderen	90% +	90% +
Het melden van mogelijke bedreigingen wordt gewaardeerd op mijn werk*	87%	90%
Digitale veiligheid staat hoog op de agenda bij het bestuur / de directie van mijn werk*	77%	82%
De afspraken over veilig online gedrag die binnen mijn organisatie/bedrijf zijn gemaakt, worden voldoende toegepast	66%	80% +
Ik pas de veiligheidsmaatregelen die ik voor werk moet nemen ook toe in mijn privésituatie*	55%	57%
Ik word er op mijn werk op aangesproken als ik me niet aan de werkafspraken houd over veilig online gedrag	51%	58%
Ik spreek collega's er op aan als zij zich niet houden aan de werkafspraken over veilig online gedrag	39% -	48%

*niet gevraagd in 2024.

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager). Significante verschillen tussen 2025 en 2024 zijn aangegeven met '+' (toename) en '-' (afname).

Driekwart checkt mobiele apps voordat ze worden geïnstalleerd

- Bij acht op de tien ambtenaren (78%) worden door hun werkgever back-ups gemaakt. De helft (52%) doet dit ook thuis.
- Driekwart (74%) controleert of mobiele apps veilig en betrouwbaar zijn voordat deze worden geïnstalleerd.

Vergelijking met 2024

- Werkgevers maken in 2025 minder vaak een back-up van alle bestanden (2024: 92%).
- Ambtenaren maken thuis juist vaker back-ups van hun bestanden (2024: 44%).

Vergelijking grootbedrijf

- Tussen ambtenaren en medewerkers van het grootbedrijf zijn geen significante verschillen voor deze stellingen.

In hoeverre zijn de volgende uitspraken van toepassing op u? (% meestal wel + altijd)	Ambtenaren (n=391)	Medewerkers grootbedrijf (n=455)
Mijn werkgever maakt automatisch back-ups van alle bestanden (volledige back-ups)	78% -	74%
Ik controleer of mobiele apps veilig en betrouwbaar zijn voordat ik deze installeer*	74%	72%
Ik zorg dat al mijn slimme apparaten altijd de laatste updates gebruiken*	66%	70%
Ik maak thuis regelmatig back-ups van mijn bestanden	52% +	48%
Ik verstuur werkbestanden van mijn werk e-mailadres naar mijn privé e-mail	4%	3% -

*nieuwe stelling in 2024.

Significante verschillen tussen 2025 en 2024 zijn aangegeven met '+' (toename) en '-' (afname).

Minder ambtenaren zouden een gedownload virus meteen melden

- Het overgrote deel van de ambtenaren meldt (94%) het meteen bij de ICT-afdeling als ze een virus downloaden waardoor ook andere computers binnen het bedrijf besmet (kunnen) raken.
- Twee derde van de ambtenaren zou zich schamen als blijkt dat ze in een phishingmail zijn getrapt. Vier procent zou uit schaamte niet vertellen dat ze een virus hebben gedownload.

Vergelijking met 2024

- Ten opzichte van 2024 is het aantal ambtenaren dat een virus meteen zou melden bij de ICT-afdeling of aan iemand op het werk gedaald (toen resp. 97% en 95%).

Vergelijking grootbedrijf

- Ambtenaren zouden sneller een virus melden dan medewerkers van een grootbedrijf. Ook voeren ze vaker meteen een update uit.

In hoeverre zijn de volgende uitspraken van toepassing op u? (% zeer waarschijnlijk + waarschijnlijk)	Ambtenaren (n=391)	Medewerkers grootbedrijf (n=455)
Als ik door heb dat ik een virus heb gedownload op mijn werkcomputer waardoor ook andere computers binnen mijn bedrijf besmet (kunnen) raken, dan vertel ik de ICT-afdeling meteen wat ik heb gedaan	94% -	88% -
Als ik door heb dat ik een virus heb gedownload op mijn werkcomputer waardoor ook andere computers binnen mijn bedrijf besmet (kunnen) raken, dan vertel ik meteen aan iemand op mijn werk wat ik heb gedaan	88% -	84% -
Als er een update beschikbaar is voor mijn werkcomputer voer ik deze meteen uit*	87%	78%
Als ik op een link in een phishing e-mail zou klikken dan zou ik mij daarvoor schamen	64%	58%
Als ik door heb dat ik een virus heb gedownload op mijn werkcomputer, dan vertel ik uit schaamte niet aan anderen wat ik heb gedaan	4%	4%

*nieuwe stelling in 2025.

Significante verschillen tussen 2025 en 2024 zijn aangegeven met '+' (toename) en '-' (afname).

Negen op tien ambtenaren voelt zich comfortabel cyberincident te melden

- Negen op de tien ambtenaren zouden zich comfortabel voelen om een cyberincident te melden.
- Driekwart van de ambtenaren zegt dat hun organisatie open communicatie over kwetsbaarheden en incidenten aanmoedigt.

Vergelijking met 2024

- Deze vraag is in 2025 voor het eerst gevraagd.

Vergelijking grootbedrijf

- Tussen ambtenaren en medewerkers van het grootbedrijf zijn er geen verschillen.

In hoeverre zijn de volgende uitspraken van toepassing op u? (% (helemaal) mee eens)	Ambtenaren (n=391)	Medewerkers grootbedrijf (n=455)
Als ik een cyberincident mee zou maken op het werk, zou ik me comfortabel voelen om dit te melden	88%	86%
Mijn organisatie waardeert medewerkers die cyberveiligheidsincidenten melden	82%	82%
Mijn organisatie moedigt open communicatie aan over kwetsbaarheden en incidenten op het gebied van cyberveiligheid	74%	70%
Binnen mijn organisatie ondervinden melders van cyberveiligheidsincidenten negatieve gevolgen	3%	4%

Een derde ambtenaren heeft duidelijke richtlijnen voor AI-gebruik

- Bij de helft van de ambtenaren wordt binnen de organisatie soms (45%) of structureel (6%) generatieve AI gebruikt. Een kwart (23%) van de ambtenaren weet niet of dit gebeurt.
- Een derde van de ambtenaren (36%) krijgt vanuit hun organisatie duidelijke richtlijnen voor het gebruik van generatieve AI om potentiële risico's te beheersen. Ruim een derde (37%) weet niet hoe dat in hun organisatie geregeld is.

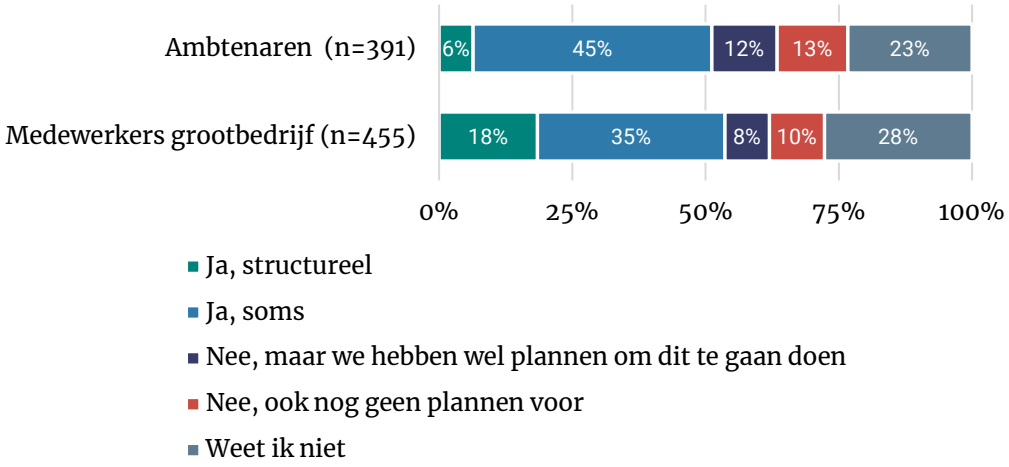
Vergelijking met 2024

- Deze vraag is in 2025 voor het eerst gesteld.

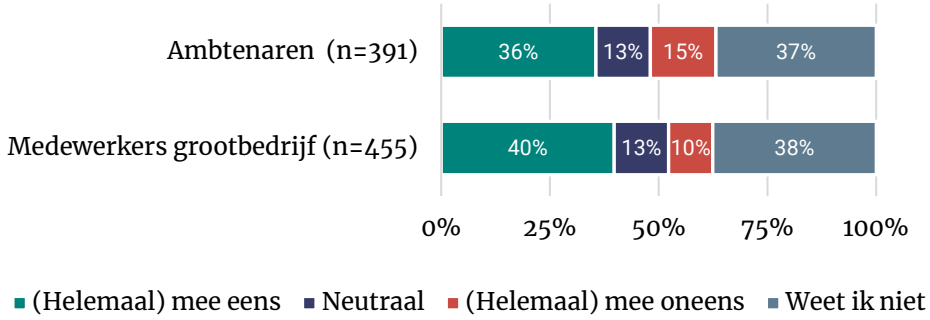
Vergelijking met grootbedrijf

- Bij grootbedrijven wordt generatieve AI vaker structureel ingezet dan bij de overheid.

Gebruikt uw organisatie generatieve AI?



Mijn organisatie heeft duidelijke richtlijnen voor het gebruik van generatieve AI om potentiële risico's (bijvoorbeeld op het gebied van dataveiligheid) te beheersen



5 Slachtofferschap en aangiftebereidheid

Stijging aantal meegemaakte voorvallen cybercrime op werk

- Vier op de tien ambtenaren (43%) maakten in de afgelopen 12 maanden een of meerdere pogingen tot cybercrime mee op het werk.
- Een derde van de ambtenaren maakte een poging tot phishing mee. Een op tien werd gebeld door iemand die zich voordeed als een bedrijf of officiële instantie.

Vergelijking met 2024

- Ambtenaren hebben vaker te maken met cybercrime op het werk (2024: 29%). Vooral phishing (2024: 22%) en neptelefoontjes (2024: 1%) kwamen vaker voor.

Vergelijking grootbedrijf

- Medewerkers van het grootbedrijf hebben minder vaak te maken met cybercrime via Whatsapp.

Heeft u in de afgelopen 12 maanden zelf weleens te maken gehad met een van de onderstaande voorvallen in uw werksituatie?	Ambtenaren (n=391)	Medewerkers grootbedrijf (n=455)
Mails ontvangen met poging tot phishing	32% +	33%
Gebeld door iemand die zich voordeed als bedrijf of officiële instantie (bijv. bank, belasting) om geld of gegevens te bemachtigen	10% +	6% +
Benaderd op Whatsapp door iemand die zich voordeed als een bekende die probeerde geld te ontvangen	8%	4%
Benaderd op social media met een vraag om een onbekende link aan te klikken	3%	3%
Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik die echt leek	2%	3%
Een foute link ook daadwerkelijk hebben aangeklikt in de zin dat deze een virus, spam, phishing of andere ongewenste poging tot cybercrime bevatte	2%	2%
Dat iemand dreigde uw bestanden te openbaren of dit ook echt deed	2%	1%
Computer werkte tijdelijk niet door malware/virus	1%	0%
Acquisitiefraude	1%	1%
Identiteitsdiefstal*	1%	0%
Dat iemand in een account heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	0%	0%
Aankoopfraude	0%	0%
Geïnfecteerde software/bestanden gedownload waardoor malware werd verspreid	0%	0%
Randsomware	0%	0%
Dat iemand in een apparaat (computer, telefoon) heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	0%	0%
Geen van deze voorvallen	57% -	62%

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager). Significante verschillen tussen 2025 en 2024 zijn aangegeven met '+' (toename) en '-' (afname).

* in 2024: identiteitsfraude.

Helft van de ambtenaren doet geen aangifte of melding cybercrime

- De helft van de ambtenaren (47%) die een incident meemaakten, deed een melding of aangifte.
- Vier op de tien ambtenaren die een incident meemaakten, meldden dit bij de ICT-afdeling.

Vergelijking met 2024

- Er zijn geen verschillen tussen 2025 en 2024 in of en waar ambtenaren cybercrime melden.

Vergelijking grootbedrijf

- Tussen medewerkers van het grootbedrijf en ambtenaren zijn er geen significante verschillen in het doen van aangifte of het maken van een melding.

U geeft aan dat u op uw werk te maken heeft gehad met een of meerdere voorvallen van cybercrime. Heeft u of uw werkgever toen een aangifte of melding gedaan?	Ambtenaren (n=166)	Medewerkers grootbedrijf (n=171)
Ja, melding bij de ICT-afdeling van mijn bedrijf	41%	49%
Ja, bij mijn leidinggevende	6%	8%
Ja, melding bij de Fraudehelpdesk	4%	6%
Ja, bij de Autoriteit Persoonsgegevens	3%	3% +
Ja, bij een andere organisatie namelijk	3%	2%
Ja, aangifte bij de politie	2%	1%
Ja, melding bij het Nationaal Cyber Security Centrum (NCSC)	1%	3%
Ja, bij een bank	1%	1%
Ja, melding bij de politie	0%	2%
Nee, ik/mijn werkgever hebben hier niks mee gedaan	53%	43%

Significante verschillen tussen 2025 en 2024 zijn aangegeven met '+' (toename) en '-' (afname).

Helft doet aangifte of melding om veiligere online omgeving te creëren

- De helft van de ambtenaren noemt als belangrijkste reden voor een aangifte of melding, het creëren van een veiligere (online) omgeving. Ook willen vier op de tien voorkomen dat de dader hetzelfde opnieuw bij een ander kan doen.
- Een derde ziet het als plicht om aangifte of melding te doen en een kwart wil voorkomen dat ze het nog eens meemaken.

Vergelijking met 2024

- Minder dan in 2024 doen ambtenaren aangifte om een veiligere omgeving te creëren (toen: 77%).

Vergelijking grootbedrijf

- Tussen medewerkers van het grootbedrijf zijn er geen significante verschillen.

Wat waren de belangrijkste redenen om wel aangifte of melding te doen?* (maximaal 3)	Ambtenaren (n=78)	Medewerkers grootbedrijf (n=91)
Om een veiligere (online) omgeving te creëren	49% -	64%
Voorkomen dat de dader dit opnieuw bij een ander kan doen	42%	43%
Het voelde als een plicht om aangifte of een melding te doen*	33%	40% +
Voorkomen dat dit opnieuw bij mij gebeurt	26%	22%
Dat werd door iemand anders afgehandeld/beslist*	15%	15%
Ik wilde dat de dader gepakt wordt*	10%	7% -
Om de schade vergoed te krijgen	4%	1%
Anders	8%	4%
Weet ik niet	6%	7%

*Vraagstelling en antwoordcategorieën aangepast naar verleden tijd.
Vraagstelling in 2024 was: wat zijn de belangrijkste redenen om geen aangifte of melding te doen?

Significante verschillen tussen 2025 en 2024 zijn aangegeven met '+' (toename) en '-' (afname).

Een derde ambtenaren deed geen melding om het niet zo belangrijk was

- Ambtenaren die geen melding of aangifte deden, vonden het in de meeste gevallen niet zo belangrijk of ondervonden weinig schade.
- Bij een vijfde werd het door iemand anders afgehandeld of beslist.

Vergelijking 2024

- Ten opzichte van 2024 geven meer ambtenaren aan dat het niet zo belangrijk was (toen: 10%) en minder ambtenaren dat ze het zelf wilden oplossen (2024: 15%).

Vergelijking grootbedrijf

- Er zijn geen significante verschillen tussen ambtenaren en medewerkers van het grootbedrijf.

Wat waren de belangrijkste reden om geen aangifte of melding te doen?* (maximaal 3)	Ambtenaren (n=88)	Medewerkers grootbedrijf (n=73)
Het was niet zo belangrijk*	34% +	25% +
Ik ondervond geen of weinig schade	33%	37%
Dat wordt door iemand anders afgehandeld/beslist	19%	16%
Het had geen zin, er wordt niets gedaan met de aangifte of melding*	6%	4% -
Het kostte te veel moeite*	2%	8%
Ik wist niet bij welke instantie ik moet zijn voor het oplossen van dit type delict*	2%	0% -
Ik heb weinig vertrouwen in de instanties om aangifte of een melding te doen	1%	7%
Ik wilde het zelf oplossen*	0% -	1% -
Ik schaamde me dat ik slachtoffer ben geworden van het delict*	0%	0%
Anders, namelijk	14%	18%
Weet ik niet	18%	18%

*Vraagstelling en antwoordcategorieën aangepast naar verleden tijd.
Vraagstelling in 2024 was: wat zijn de belangrijkste redenen om geen aangifte of melding te doen?

Significante verschillen tussen 2025 en 2024 zijn aangegeven met '+' (toename) en '-' (afname).

Contactgegevens

Ipsos I&O Enschede
Zuiderval 70
Postbus 563
7500 AN Enschede
053 - 200 52 00
KVK-nummer 08198802
nl-info-publiek@ipsos.com
www.ipsos-publiek.nl

Ipsos I&O Amsterdam
Piet Heinkade 55
1019 GM Amsterdam
020 – 308 48 00
nl-info-publiek@ipsos.com
www.ipsos-publiek.nl