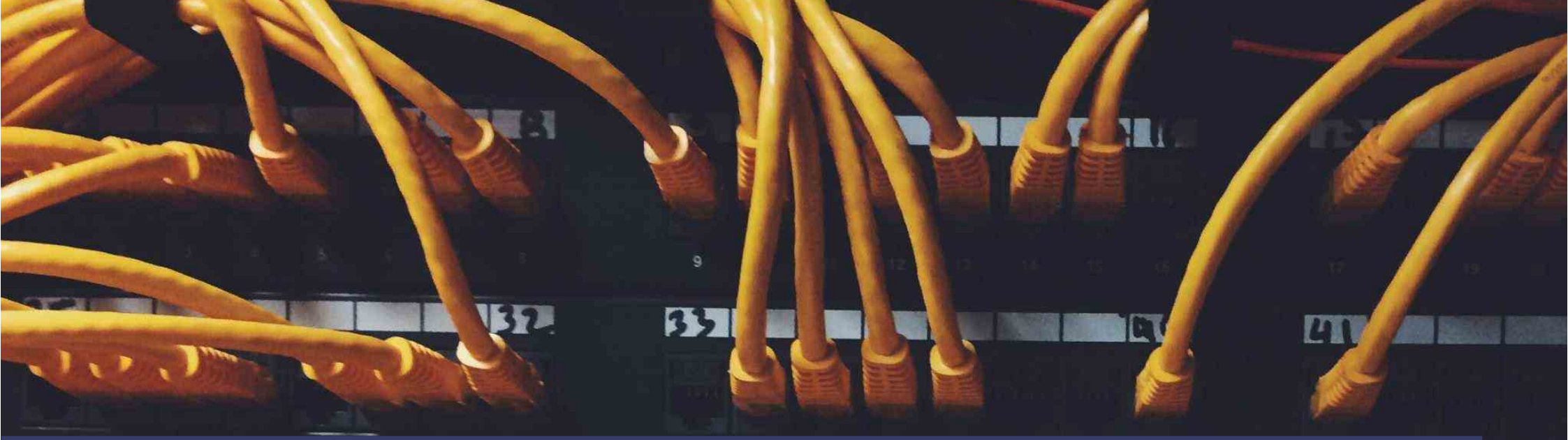


Cybersecurity onderzoek Alert Online 2024

Deelrapport bedrijfsleven

Ipsos i&O

Ministerie van Economische Zaken

www.ipsos-publiek.nl

Colofon

Uitgave
Ipsos I&O
Piet Heinkade 55
1019 GM Amsterdam

Rapportnummer
2024/198

Datum
september 2024

Opdrachtgever
Ministerie van Economische Zaken

Auteurs
Sara Kellij
Bram Doms

Inhoudsopgave

Colofon 2

Inhoudsopgave 3

1. Managementsamenvatting 4

2. Inleiding en achtergrond 7

3. Kennis en ervaring online risico's 10

4. Zorgen en online gedrag op het werk 12

5. Slachtofferschap en aangiftebereidheid 24

Contactgegevens 33

1. Managementsamenvatting

Samenvatting | 1/2

Medewerkers schatten eigen kennis over online veiligheid hoger in dan in 2023
Ruim een kwart (27%) van de medewerkers schat hun eigen kennis over online veiligheid in als (zeer) goed. In 2023 lag dit percentage op 21 procent. ICT-verantwoordelijken schatten hun kennis hoger in dan andere medewerkers. Het aandeel ICT-verantwoordelijken dat zijn kennis als (zeer) goed beoordeelt is 53 procent.

ICT-verantwoordelijken schatten risico cybercrime hoger in
ICT-verantwoordelijken zijn beter bekend met de betekenis van de verschillende vormen van cybercrime dan andere medewerkers. Van de vormen van cybercrime die men kent, acht men het meemaken in de werksituatie van hacking (52%) en phishing het meest waarschijnlijk (48%). Van de ICT-verantwoordelijken vindt 68 procent het waarschijnlijk dat ze phishing op het werk meemaken. Ook alle andere voorgelegde vormen van cybercrime worden door ICT-verantwoordelijken aannemelijker geacht om op het werk mee te maken te krijgen dan door andere medewerkers.

ICT-verantwoordelijken maken zich meer zorgen over online veiligheid dan medewerkers
Vier op de tien ICT-verantwoordelijken (40%) maken zich (zeer) veel of enige zorgen over de eigen online veiligheid op het werk. Voor andere medewerkers is dit percentage significant lager (23%). Wel geven ICT-verantwoordelijken zichzelf een hoger cijfer (7,4) als het gaat om het veilig omgaan met online risico's dan andere medewerkers (7,0).

Een derde van kleine bedrijven onderneemt geen actie om veilig online te zijn
Twee-staps-inloggen is de meest genomen actie ten behoeve van online veilig gedrag bij bedrijven (medewerkers: 38%). Ook door ICT-verantwoordelijken (54%) en medewerkers van grote bedrijven (50%) wordt deze maatregel het vaakst genoemd. Kleine bedrijven ondernemen minder acties. Bovendien onderneemt een derde van deze bedrijven (32%) geen enkele actie ten behoeve van veilig online gedrag. Wanneer we kijken naar medewerkers, dan geeft 9 procent aan dat er binnen hun bedrijf geen maatregelen worden genomen. Grote bedrijven ondernemen naar verhouding juist meer acties. Bij bedrijven waar afspraken zijn gemaakt over veilig online gedrag, vinden vier op de vijf medewerkers het gemakkelijk om zich aan die afspraken te houden.

Samenvatting | 2/2

ICT-verantwoordelijken zijn het vaakst op de hoogte van NIS2

Een derde (33%) van de ICT-verantwoordelijken heeft wel eens van de NIS2-richtlijn gehoord of is goed op de hoogte. In de sectoren die onder de NIS2-richtlijn vallen, is 45 procent van de ICT-verantwoordelijken bekend met de richtlijn. Medewerkers binnen alle andere typen bedrijven zijn minder goed op de hoogte; 85 procent heeft nog nooit van NIS2 gehoord. Negen op de tien zijn er niet van op de hoogte dat hun bedrijf (waarschijnlijk) onder de richtlijn gaat vallen.

Phishing komt het vaakst voor

Zes op de tien (58%) medewerkers ontvingen in de afgelopen twaalf maanden een phishingmail. Onder ICT-verantwoordelijken was dit zelfs 72 procent. Bij beide groepen is dit de vorm van cybercrime die men het meest meemaakt. Net zoals in 2023 hebben ICT-verantwoordelijken vaker te maken met verschillende voorgelegde vormen van cybercrime dan andere medewerkers.

Meerderheid onderneemt geen actie op cybercrime

De helft (47%) van de medewerkers die te maken kregen met cybercrime deed hier geen melding of aangifte van. Doet men dit wel, dan is de ICT-afdeling van het bedrijf de plek waar men dit het vaakst meldt (39%). De belangrijkste redenen om aangifte of melding te doen zijn het creëren van een veiligere online omgeving (70%) en voorkomen dat de dader opnieuw slachtoffers maakt (46%). Een derde van de medewerkers die geen aangifte doet, geeft aan dat ze geen of weinig schade ondervonden. Een vijfde (21%) vindt het (daarnaast) niet zo belangrijk. Achttien procent zegt dat het geen zin heeft om aangifte of melding te doen.

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 online veiligheid, op het vergroten van kennis over online veiligheid en op het stimuleren van en helpen bij veilig digitaal gedrag. Dit wordt gedaan door kennisoverdracht via veiliginternetten.nl, het Digital Trust Center en met een specifiek partnernetwerk van organisaties in Nederland. Een onderdeel van de campagne is dit jaarlijks terugkerende bewustwordingsonderzoek waarmee de cybersecuritymaand in oktober wordt afgetrapt.

In opdracht van het ministerie van Economische Zaken voerde Ipsos I&O onderzoek uit naar de kennis en beleving van de digitale veiligheid onder Nederlanders.

Onderzoeksdoel

Het doel van dit onderzoek is het monitoren van het digitaal bewustzijn, de kennis en vaardigheden van Nederlanders op het gebied van digitale veiligheid door de jaren heen. Aanvullend beoogt dit onderzoek om aanknopingspunten voor beleidsvorming over dit onderwerp te vergaren.

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 werknemers in het bedrijfsleven.

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

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

Leeswijzer

Dit deelrapport bevat de resultaten van medewerkers en ICT-verantwoordelijken in het bedrijfsleven. Medewerkers worden in het rapport uitgesplitst naar verschillende grootteklassen:

1 minder dan 10 medewerkers (n=62);
2 10 t/m 199 medewerkers (n=247);
3 200 of meer medewerkers (n=429).

Daarnaast is uitgesplitst of men al dan niet werkzaam is in de vitale infrastructuur.[1] ICT-verantwoordelijken zijn in sommige figuren afgekort tot 'ICT', ten behoeve van de leesbaarheid. In deze rapportage is ervan uitgegaan dat zzp'ers per definitie ICT-verantwoordelijk voor hun bedrijf zijn. Waar de resultaten van deze groep afwijken van de andere ICT-verantwoordelijken, wordt dit in de tekst benoemd.

Hoofdstukken 3 t/m 5 van dit rapport behandelen de onderzoeksresultaten voor de drie onderzoeksvragen. Hoofdstuk 3 gaat in op kennis en ervaring over 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 over het bedrijfsleven is er ook een hoofdrapport over de Nederlandse bevolking en een deelrapport over de overheid.

Verantwoording

In totaal deden 738 medewerkers mee aan dit onderzoek en 417 ICT-verantwoordelijken. De respondenten zijn afkomstig uit het I&O Research Panel. Het online veldwerk vond plaats van 25 juni t/m 7 juli 2024. De resultaten zijn gewogen naar bedrijfsgrootte. Daarmee zijn de resultaten representatief voor dit kenmerk.

---

[1] *Op basis van zelfopgave. Het gaat om mensen die bij een bedrijf met minimaal 10 werknemers werken in een van de volgende sectoren: Transport en distributie elektriciteit, Gasproductie en distributie gas, Internettoegang (Internetproviders), Drinkwatervoorziening, Keren en beheren waterkwantiteit, Vlucht- en vliegtuigafhandeling (bijv. op Schiphol), Scheepvaartafwikkeling (bijv. in de haven van Rotterdam), Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen, Opslag, productie en verwerking nucleair materiaal, Toonbankbetalingsverkeer, Massaal giraal betalingsverkeer, Betalingsverkeer tussen banken, Effectenverkeer, Digitale overheidsprocessen.*

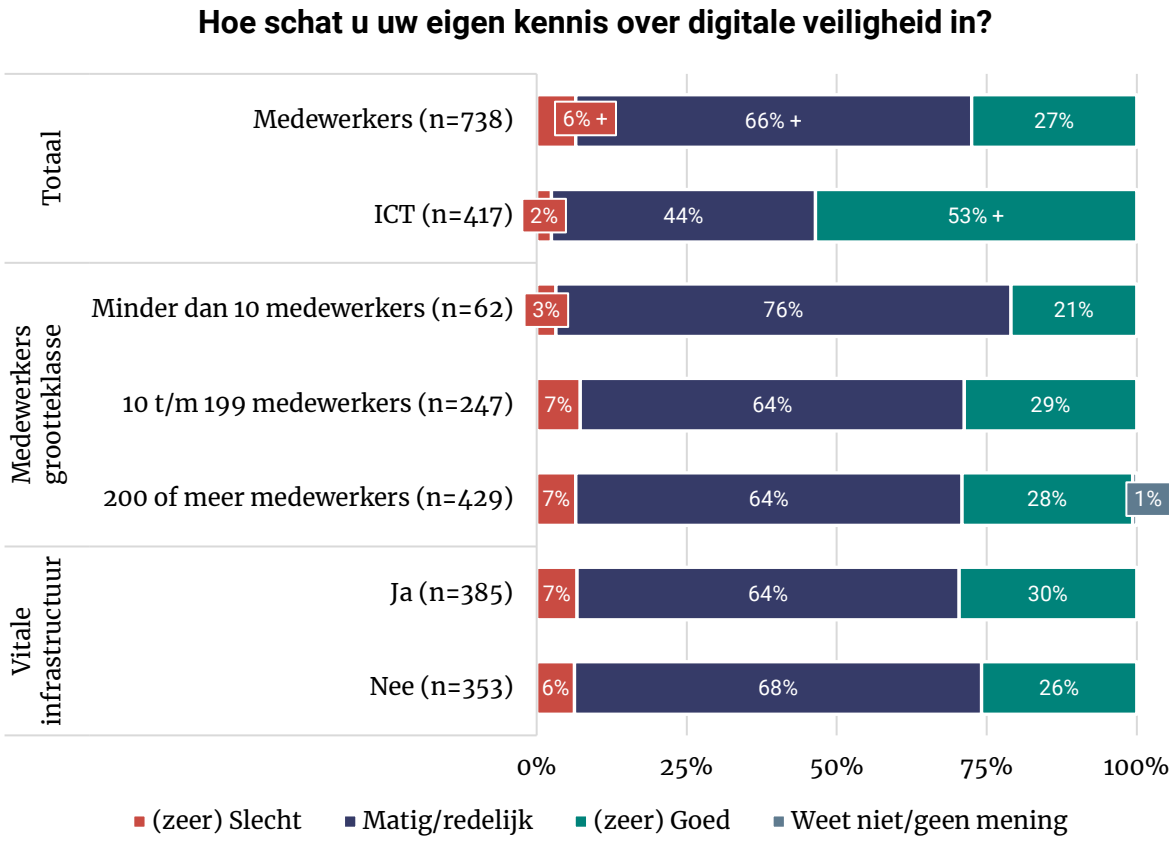
3. Kennis en ervaring online risico’s

Een kwart van de medewerkers vindt eigen kennis over digitale veiligheid (zeer) goed

- Medewerkers schatten hun kennis over digitale veiligheid lager in dan ICT-verantwoordelijken.
- Ruim de helft van de ICT-verantwoordelijken schat hun kennis in als (zeer) goed.
- Er zijn geen verschillen tussen medewerkers die in vitale sectoren en in niet vitale sectoren werkzaam zijn.

Vergelijking met 2023

- Medewerkers schatten hun eigen kennis vaker als (zeer) goed in dan in 2023. In 2023 was dit 21 procent tegenover 27 procent nu.



Meeste vormen van cybercrime bij ruime meerderheid bekend

- Het grootste deel van de medewerkers heeft wel eens van de voorgelegde vormen van cybercrime gehoord. Alleen social engineering en CEO-fraude zijn minder bekend.
- ICT-verantwoordelijken kennen de verschillende vormen van cybercrime vaker dan medewerkers. Ook schatten ze de kans om ermee te maken te krijgen voor alle voorgelegde vormen groter in.
- Het meest aannemelijk acht men het om met hacking, phishing en malware te maken te krijgen.

Vergelijking met 2023

- Ten opzichte van 2023 is de bekendheid met ransomware, helpdeskfraude en hacking toegenomen.
- Verschillende vormen van cybercrime acht men – als men ze kent – waarschijnlijker om mee te maken dan in 2023.

In deze tabel staan 10 voorgelegde vormen van cybercrime	Is er bekend mee/weet wat het is		Denkt in werksituatie te maken te kunnen krijgen met deze vormen van cybercriminaliteit?**	
	Medewerkers (n=738)	ICT-verantwoordelijk (n=417)	Medewerkers	ICT-verantwoordelijk
Malware	76%	92%	43% n=575	61% n=381
Phishing	94%	98%	48% n=706	68% n=409
Ransomware	70% +	89%	43% + n=536	62% n=369
Helpdeskfraude	80% +	92%	20% n=605	28% - n=377
DDoS-aanval	72%	90%	47% + n=541	55% n=370
Hacking	98% +	98%	52% - n=718	71% n=407
QR-codefraude	61%	73%	16% n=458	23% n=291
Bankhelpdeskfraude	87%	95%	12% n=644	25% n=395
Social engineering	26%	52%	31% + n=204	51% + n=210
CEO-fraude	31%	60%	42% n=247	47% n=237
Misbruik van bedrijfsgegevens/bedrijfsnaam, online aankopen (alleen voorgelegd aan ondernemers)	93% n=27*	94% n=195	36% n=25*	58% n=181
Aankoopfraude	80%	88%		

Significante verschillen tussen medewerkers en ICT-verantwoordelijken zijn aangegeven met groen (hoger)
Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).
*Laag aantal waarnemingen. Indicatieve uitkomsten.
**Alle begrippen voorgelegd waarvan men de betekenis zegt te kennen | percentage zeker + waarschijnlijk wel.

4. Zorgen en online gedrag op het werk

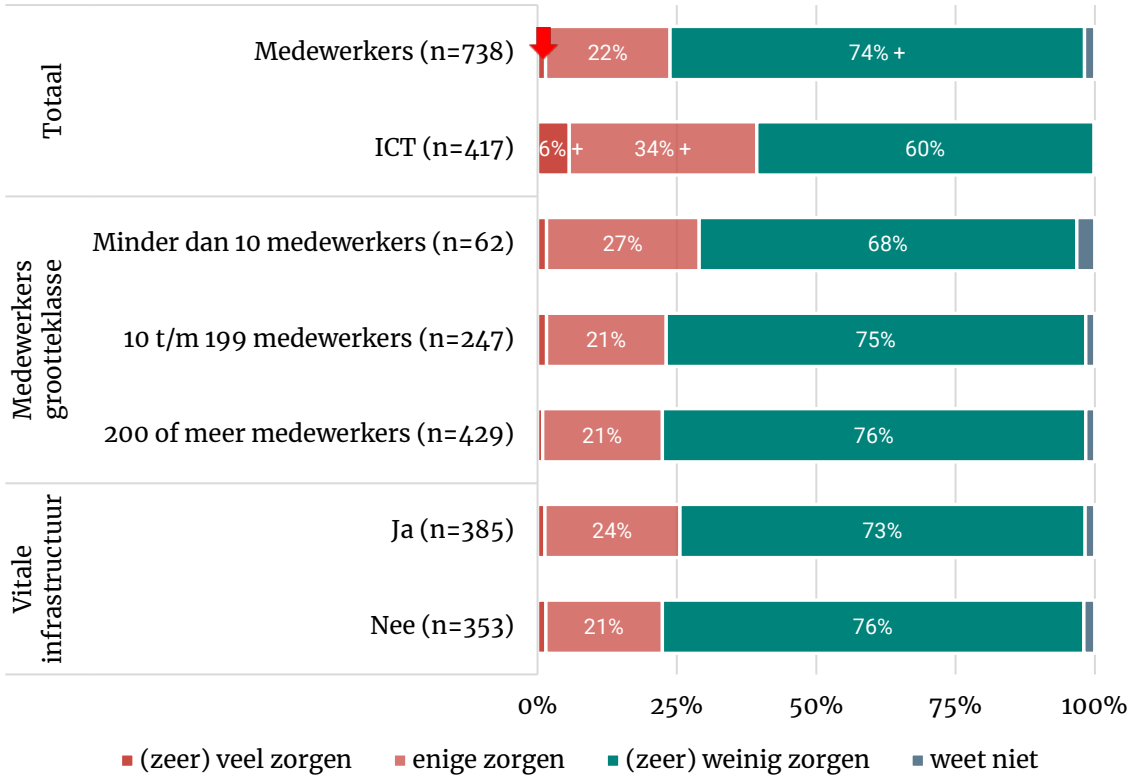
Driekwart medewerkers heeft weinig zorgen over digitale veiligheid in werksituatie

- Vier op de tien ICT-verantwoordelijken (40%) maken zich (veel of enige) zorgen over de eigen online veiligheid op het werk. Voor medewerkers is dit percentage significant lager: 23 procent zegt zich zorgen te maken.
- Medewerkers zeggen vaker dan ICT-verantwoordelijken zich weinig of geen zorgen te maken (74%).

Vergelijking met 2023

- Medewerkers maken zich minder vaak (zeer) veel zorgen in vergelijking met 2023. In 2024 gaat het om 1,4 procent en in 2023 was dit 2,4 procent.

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



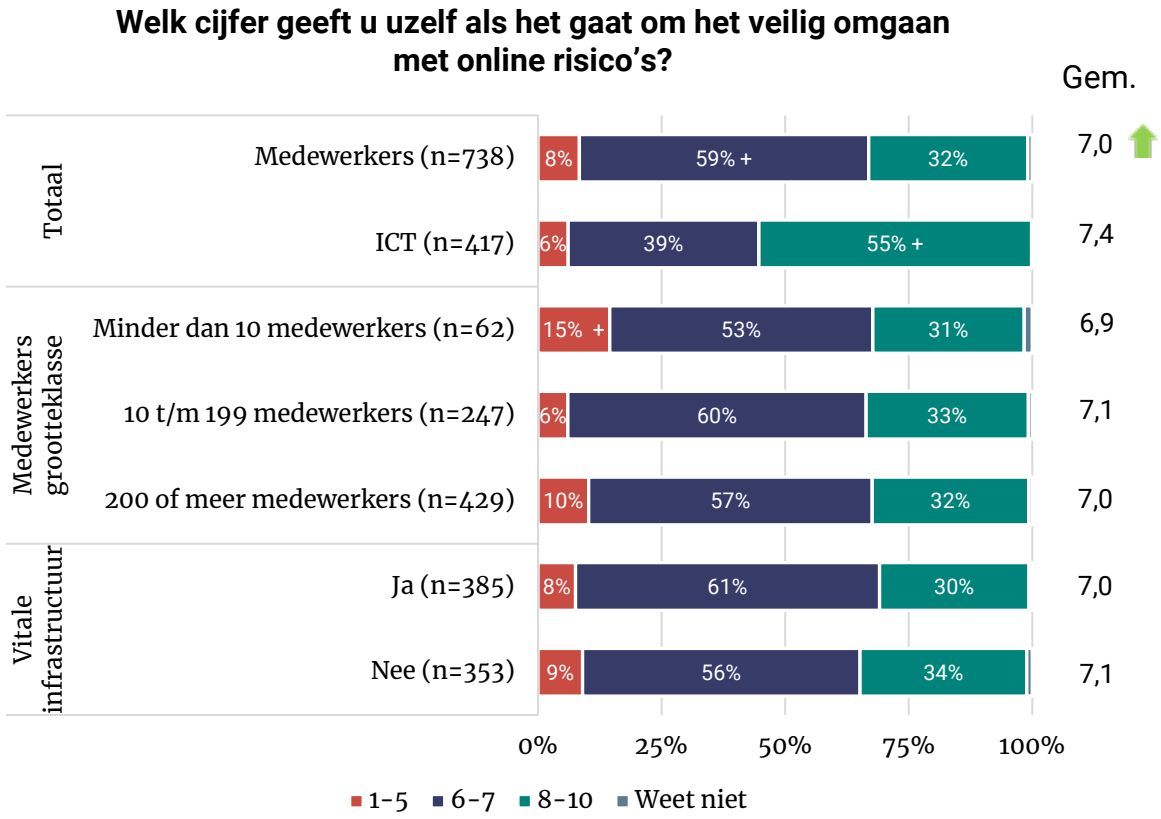
Significantie verschillen ten opzichte van 2023 zijn aangegeven met een ↓ (afname) of ↑ (toename). Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).

ICT-verantwoordelijken beoordelen eigen omgang met online risico's beter dan andere medewerkers

- Gemiddeld geven medewerkers zichzelf een 7,0 als het gaat om het omgaan met online risico's. Dat is lager dan de 7,4 die ICT-verantwoordelijken zichzelf geven. Meer dan de helft van de ICT-verantwoordelijken (55%) geeft zichzelf het cijfer 8 of hoger.
- Medewerkers van bedrijven met minder dan 10 werknemers geven zichzelf vaker een onvoldoende dan medewerkers van grotere bedrijven.

Vergelijking met 2023

- Medewerkers geven zichzelf dit jaar gemiddeld een hoger cijfer dan in 2023 (6,8).



Significantie verschillen ten opzichte van 2023 zijn aangegeven met een (afname) of (toename). Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).

Een derde kleine bedrijven neemt geen acties om veilig online te zijn (1)

- Twee-staps-inloggen is de meest genomen actie ten behoeve van online veilig gedrag bij bedrijven (tabel op volgende pagina). De helft van de ICT-verantwoordelijken (54%) en medewerkers van grote bedrijven (50%) noemt dat deze maatregel wordt toegepast.
- Bij 35 procent van de bedrijven wordt ook de mogelijkheid om zelf software te installeren beperkt tot alleen systeembeheerders.
- Het afsluiten van een verzekering tegen cybercrime komt het minst voor.
- Een kwart (26%) weet niet welke acties zijn of haar organisatie heeft genomen.
- Een op de drie (32%) medewerkers van kleine bedrijven zegt dat geen enkele maatregel genomen wordt.

Vergelijking met 2023

- Een aantal maatregelen worden door meer medewerkers genoemd dan een jaar eerder. Het gaat om verplicht twee-staps-inloggen, afspraken over uitwisselen bestanden en gebruik usb-sticks of harde schijven, adviezen over online thuiswerken en testmails om te testen op het herkennen van phishing.
- Bij kleine bedrijven met minder dan 10 werknemers valt op dat ze vaker dan in 2023 aangeven dat ze geen acties nemen ten behoeve van veilig online gedrag. In 2023 nam 19 procent van de kleine bedrijven geen actie, nu is dat 32 procent.

Een derde kleine bedrijven neemt geen acties om veilig online te zijn (2)

Welke acties zijn er binnen uw bedrijf/organisatie ondernomen ten behoeve van online veilig gedrag?	Medewerkers (n=738)	ICT verantwoordelijken (n=417)	Minder dan 10 medewerkers (n=62)	10 t/m 199 medewerkers (n=247)	200 of meer medewerkers (n=429)	Vitaal (n=385)	Niet vitaal (n=347)
Er zijn adviezen/richtlijnen over het gebruikmaken van websites/of e-mail/sociale media*	18%	31%	10%	17%	28%	22%	16%
Er zijn regels over het gebruikmaken van websites/of e-mail/sociale media*	17%	27%	5%	15%	29%	18%	16%
Er is binnen mijn organisatie/bedrijf een digitale hulpverlener waar je terecht kunt	19%	28% +	6%	17%	33%	25%	15%
Er worden op willekeurige momenten testmails verstuurd om medewerkers te testen op de herkenning van phishing	18% +	28% +	3%	13%	38% +	21%	15%
Er zijn adviezen/richtlijnen over hoe je veilig online thuiswerkt	23% +	32%	11%	20%	36%	28%	18%
Er zijn regels over hoe je veilig online thuiswerkt	20%	30%	10%	17%	34%	27%	15%
Er zijn afspraken gemaakt over het gebruikmaken van opslagmedia als usb-sticks of externe harde schijven	17% +	32% +	6%	15%	25%	21%	13%
Er zijn afspraken gemaakt over het versturen/uitwisselen van bestanden en/of persoonsgegevens	25% +	35%	13%	24%	35%	34%	18%
Er zijn afspraken gemaakt over het gebruik van zakelijke smartphones, laptops en/of tablets voor privé en/of zakelijk gebruik	23%	33%	6%	21%	38%	30%	18%
De toegang tot bepaalde websites en/of socialmediakanalen is geblokkeerd	19% +	23%	8%	15%	34%	22%	16%
Het gebruik van USB-sticks in onze organisatie is onmogelijk gemaakt	10%	14%	3%	9%	17%	17%	5%
Alleen de systeembeheerders kunnen software installeren	35%	41% +	19%	32%	51%	37%	33%
Er is een verzekering afgesloten tegen de financiële gevolgen van cybercrime	4%	10%	5%	4%	4%	4%	5% +
Er is twee-staps-inloggen verplicht voor toegang	38% +	54%	19%	38%	50%	45% +	32%
Er worden trainingen gegeven binnen mijn organisatie over online veiligheid*	24%	35%	6%	21%	41%	31%	19%
Anders	1% -	7%	5%	0% -	2%	1% -	2%
Weet ik niet	26%	7%	26%	28%	22%	23%	29%
In mijn bedrijf of organisatie is geen enkele actie ondernomen ten behoeve van veilig online gedrag	9%	13%	32% +	6%	1%	5%	12%

Significantieverschillen ($p<.05$) tussen (sub)groepen zijn aangegeven met groen (hoger).

Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

*Stelling is nieuw of anders geformuleerd in 2024. Daarom is vergelijking met eerdere jaren niet mogelijk.

Meerderheid vindt het makkelijk om zich aan afspraken over online veiligheid binnen organisatie te houden

- Vier op de vijf medewerkers vinden het gemakkelijk om zich aan de afspraken over online veilig gedrag te houden. Hetzelfde aandeel vindt het goed wanneer men wordt aangesproken op het niet naleven hiervan.
- Zeven op de tien (72%) medewerkers vinden de afspraken over veilig online gedrag duidelijk. Acht op de tien zeggen toegang te hebben tot de juiste tools om veilig online te kunnen werken en ruim zes op de tien vinden dat afspraken voldoende worden toegepast. De resultaten voor ICT-verantwoordelijken en medewerkers zijn vergelijkbaar.
- Medewerkers van grotere bedrijven ervaren vaker dat de afspraken binnen de organisatie goed worden toegepast.

Vergelijking met 2023

- In 2024 zeggen medewerkers vaker dat ze goede tools en instrumenten krijgen om online veilig gedrag te bevorderen.
- ICT-verantwoordelijken zeggen vaker dat afspraken over online veilig gedrag voldoende worden toegepast.

In hoeverre bent u het eens of oneens met de volgende stellingen? % (zeer) eens. (gesteld indien er werkafspraken zijn over veilig online gedrag)	Medewerkers (n=517)	ICT verantwoordelijken (n=324)	Minder dan 10 medewerkers (n=26)*	10 t/m 199 medewerkers (n=161)	200 of meer medewerkers (n=330)	Vitaal (n=287)	Niet vitaal (n=230)
Het is gemakkelijk om mij aan de afspraken te houden over online veilig gedrag binnen mijn bedrijf/organisatie	84%	82%	73%	85%	87%	84%	85%
Ik vind het goed als collega's mij erop aanspreken als ik me niet houd aan de werkafspraken over online veilig gedrag	83%	82%	77%	83%	85%	84%	82%
De afspraken over hoe ik me online veilig moet gedragen op mijn werk vind ik duidelijk	72%	74%	65%	68%	82%	72%	73%
Ik krijg toegang tot goede tools en instrumenten (bijvoorbeeld tweestapsverificatie of een wachtwoordmanager) om online veilig gedrag te bevorderen	78% +	78%	69%	77%	82% +	78% +	77% +
De afspraken over online veilig gedrag die binnen mijn organisatie/bedrijf zijn gemaakt, worden voldoende toegepast	64%	66% +	46%	65%	68%	62%	66%

Significantieverschillen ($p<.05$) tussen (sub)groepen zijn aangegeven met groen (hoger).

Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

* = Indicatief i.v.m. laag aantal waarnemingen.

Zes op de tien ICT-verantwoordelijken spreken collega's aan op niet naleven werkafspraken

- De helft van de medewerkers wordt aangesproken op het niet naleven van werkafspraken.
- Bijna de helft spreekt zelf collega's aan als zij zich niet aan de afspraken houden. Van de ICT-verantwoordelijken doen ruim zes op de tien dit.
- Volgens vier op de tien medewerkers geeft hun leidinggevende het goede voorbeeld.
- Driekwart van de ICT-verantwoordelijken past veiligheidsmaatregelen op het werk ook in de privésituatie toe, bij medewerkers is dit aandeel kleiner (59%).
- In de vitale sectoren spreken werknemers collega's er meer op aan als ze zich niet aan werkafspraken voor veilig gedrag houden (51%). Bij bedrijven in niet-vitale sectoren doet 41 procent van de medewerkers dit.

Vergelijking met 2023

- Er zijn geen significante verschillen in vergelijking met de vorige meting.

In hoeverre bent u het eens of oneens met de volgende stellingen? % (zeer) eens.	Medewerkers (n=517)	ICT verantwoordelijken (n=324)	Minder dan 10 medewerkers (n=26)*	10 t/m 199 medewerkers (n=161)	200 of meer medewerkers (n=330)	Vitaal (n=287)	Niet vitaal (n=230)
Ik word er op mijn werk op aangesproken als ik me niet aan de werkafspraken houd over online veilig gedrag	50%	52%	46%	49%	55%	49%	52%
Ik spreek collega's er op aan als zij zich niet houden aan de werkafspraken over online veilig gedrag	46%	63%	31%	47%	49%	51%	41%
Mijn leidinggevende geeft het goede voorbeeld als het gaat om online veilig gedrag	43%	44%	31%	45%	43%	42%	44%
Ik pas de veiligheidsmaatregelen die ik voor werk moet nemen ook toe in mijn privé-situatie	59%	74%	65%	57%	60%	58%	59%

Significantieverschillen (p<.05) tussen (sub)groepen zijn aangegeven met groen (hoger).* = Indicatief i.v.m. laag aantal waarnemingen.

Bij meeste bedrijven worden automatische backups gemaakt

- Bij drie op de vijf medewerkers maakt de werkgever automatische back-ups van alle bestanden. Een derde maakt thuis ook back-ups.
- Ruim de helft (58%) checkt of er een ‘slotje’ bij websites staat.
- Net zoveel medewerkers (59%) hebben de privacy-instellingen van sociale media accounts verhoogd.

Vergelijking ICT

- ICT-verantwoordelijken zeggen vaker dat hun werkgever volledige back-ups uitvoert. Bovendien maken ze ook zelf vaker back-ups.
- Ook letten ze vaker op dan andere medewerkers op een slotje of https in de webbrowser.

Vergelijking met 2023

- Medewerkers maken in 2024 thuis of op hun werklaptop minder back-ups van bestanden. Ook versturen ze minder werkbestanden naar hun privémail.

In hoeverre zijn de volgende uitspraken van toepassing op uw gedrag? % meestal wel + altijd (exclusief ‘niet van toepassing’)	Medewerkers (n=738)	ICT-verantwoordelijk (n=417)
Mijn werkgever maakt automatisch back-ups van alle bestanden (volledige back-ups)	62%	86% +
Ik let op of er een slotje en/of https bij het webadres staat	58%	72% -
Ik heb de privacy instellingen van mijn social media accounts verhoogd ten opzichte van de standaardinstellingen	59%	69%
Als ik een openbare computer heb gebruikt dan log ik na gebruik al mijn accounts uit (bijv. bank, social media en e-mail)	85%	87%
Ik maak thuis regelmatig back-ups van mijn bestanden	40% -	68%
Ik maak op mijn werk regelmatig back-ups van de bestanden op mijn werklaptop	32% -	60% -
Ik maak thuis gebruik van een extern opslagapparaat dat continu online is	13%	30%
Ik verstuur werkbestanden van mijn werk e-mailadres naar mijn privé e-mail	4% -	11%

Significantie verschillen (p<.05) tussen (sub)groepen zijn aangegeven met groen (hoger). Significante verschillen tussen 2024 en 2023 zijn aangegeven met ‘+’ (toename) en ‘-’ (afname).

Meer dan helft zou zich schamen na het aanklikken van phishinglink

- Driekwart zou het meteen aan anderen of aan de ICT-afdeling vertellen wanneer men een virus heeft gedownload.
- Zes op de tien medewerkers zeggen dat de werkgever back-ups maakt.
- Ruim de helft zou zich schamen wanneer men op een phishinglink heeft geklikt.

Vergelijking ICT

- Er zijn geen significante verschillen tussen medewerkers en ICT-verantwoordelijken.

Vergelijking met 2023

- In 2023 kon men antwoorden op een schaal van *altijd* tot *nooit*. De rode lijn van de uitkomsten was wel hetzelfde. De meeste medewerkers dachten het te zeggen als ze een virus zouden downloaden. Iets meer dan de helft van de medewerkers verwachtte zich te schamen als ze in phishing zouden trappen.

In hoeverre zijn de volgende uitspraken van toepassing op uw gedrag? % Zeer waarschijnlijk + waarschijnlijk	Medewerkers (n=738)	ICT-verantwoordelijk (n=417)
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	76%	80%
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	75%	80%
Als ik op een link in een phishing e-mail zou klikken dan zou ik mij daarvoor schamen	54%	54%
Als ik getroffen word door ransomware (gijzelsoftware), dan zou ik betalen als ik daardoor weer toegang krijg tot mijn persoonlijke bestanden	4%	6%
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%	5%

Meerderheid gebruikt bij thuiswerken wifi-netwerk met wachtwoord

- De meeste medewerkers maken bij het thuiswerken gebruik van wifi met een wachtwoord (90%).
- Medewerkers werkzaam in grotere bedrijven gebruiken relatief vaker een VPN-verbinding.
- Meer dan de helft (57%) heeft een zelfverzonnen wachtwoord op de router. Een derde (36%) gebruikt het standaard met de router meegeleverde wachtwoord.

Vergelijking met 2023

- Meer medewerkers dan in 2023 maken gebruik van een wifi-netwerk met wachtwoord (2024: 90%; 2023: 85%).
- Tegelijkertijd gebruiken mindere medewerkers een hotspot (2024: 6%; 2023: 10%).

Van wat voor netwerkverbinding maakt u thuis gebruik? Voorgelegd aan medewerkers die weleens thuis werken	Totaal		Medewerkers grootteklasse			Vitale infrastructuur	
	Medewerkers (n=343)	ICT (n=333)	Minder dan 10 medewerkers (n=38)	10 t/m 199 medewerkers (n=100)	200 of meer medewerkers (n=205)	Ja (n=182)	Nee (n=161)
Een wifi-netwerkverbinding met wachtwoord	90% +	90%	84%	92%	90% +	94% +	87%
Een VPN verbinding	31%	45%	18%	31%	42%	35% -	29%
Via een internetkabel (niet draadloos; LAN)	21%	36%	26%	19%	22%	20%	22%
Een hotspot verbinding (3G/4G/5G) via mijn smartphone of tablet	6% -	14%	13%	3% +	7%	5%	7%
Een wifi-netwerkverbinding zonder wachtwoord (bv openbaar (wifi-)netwerk)	1% +	1%	3%	1%	0%	0%	2%

Significantie verschillen (p<.05) tussen (sub)groepen zijn aangegeven met groen (hoger). Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

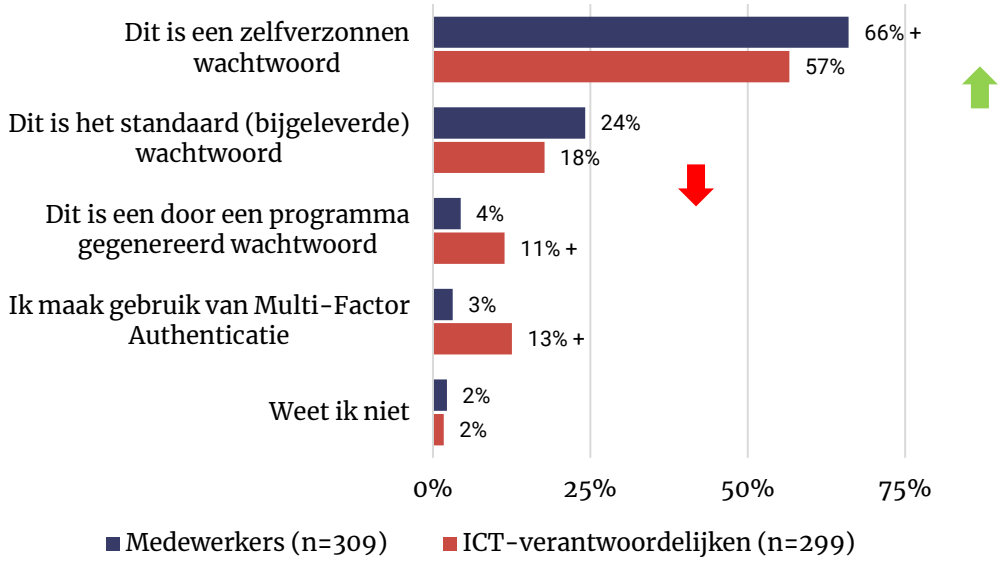
Twee derde van medewerkers gebruikt een zelfverzonnen wachtwoord voor netwerkverbinding thuis

- Twee derde van de medewerkers gebruikt een zelfverzonnen wachtwoord thuis. Onder ICT-verantwoordelijken is dit 57 procent.
- Een kwart (24%) gebruikt het standaard met de router meegeleverde wachtwoord.
- ICT-verantwoordelijken gebruiken vaker dan andere medewerkers een door een programma gegenereerd wachtwoord en multi-factor authenticatie.
- Kleine letters, hoofdletters en cijfers worden in ruim vier op de vijf zelfverzonnen wachtwoorden gebruikt. Zes op de tien gebruiken leestekens en speciale tekens. Vier op de tien (39%) hebben een wachtwoord van 12 tekens of langer.
- Onder ICT-verantwoordelijken is dit aandeel groter (54%).

Vergelijking met 2023

- Het aandeel met zelfverzonnen wachtwoord is dit jaar gestegen (2024: 66%; 2023: 57%). Minder medewerkers gebruiken het standaardwachtwoord dan een jaar eerder.

U geeft aan dat u thuis gebruikmaakt van een netwerkverbinding met wachtwoord. Kunt u aangeven wat voor soort wachtwoord dat is?
(gesteld aan mensen die thuis gebruikmaken van een netwerkverbinding met wachtwoord)

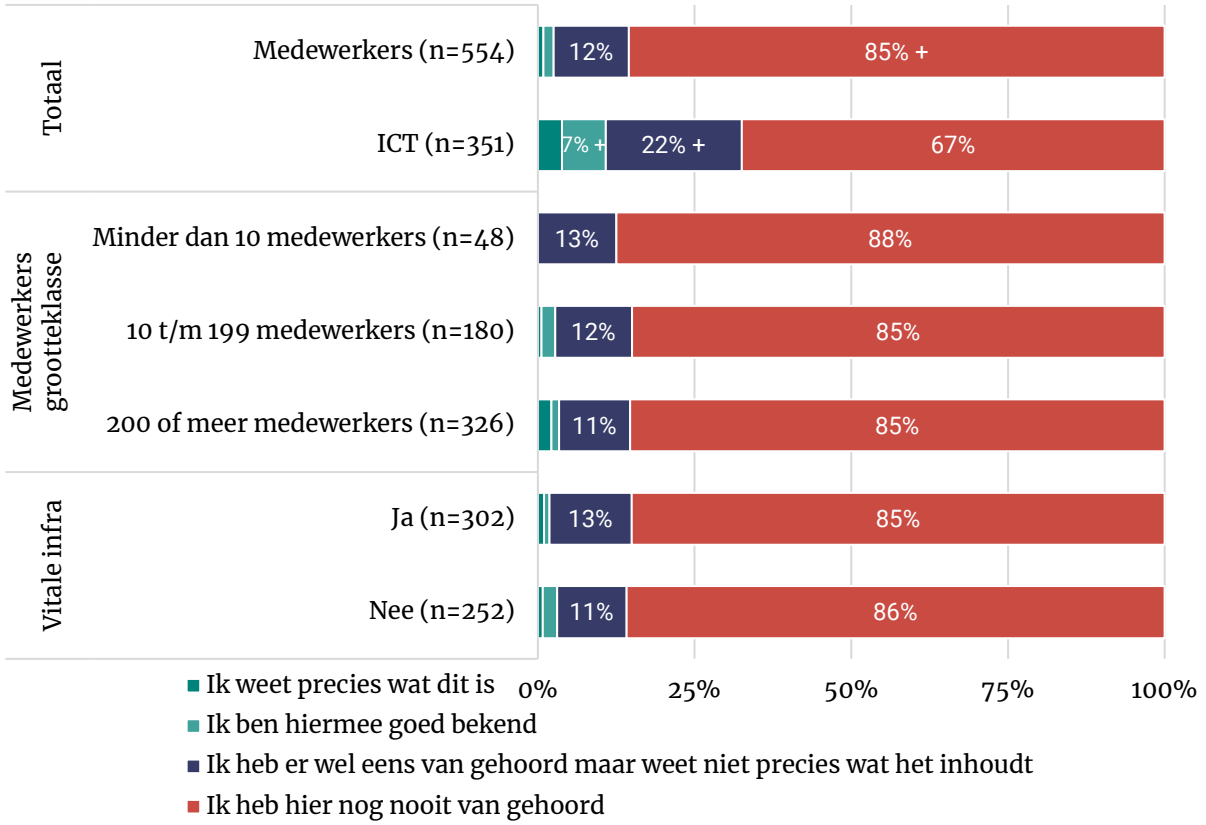


Significantie verschillen (p<.05) tussen medewerkers en ICT-verantwoordelijken zijn aangegeven met '+' hoger en '-' lager. Verschillen tussen 2024 en 2023 zijn met groen (hoger) of rood (lager) aangegeven.

NIS2-richtlijn nog onbekend onder gros van de medewerkers

- De NIS2-richtlijn voor informatiebeveiliging gaat vanaf oktober 2024 in.
- Ongeveer een op tien medewerkers heeft wel eens van NIS2 gehoord, maar weet niet precies wat het inhoudt.
- Onder ICT-verantwoordelijken is de richtlijn bekender: een op de drie (33%) heeft ervan gehoord. Bij bedrijven die onder de richtlijn vallen is dat 45 procent.
- Het aandeel dat nog nooit van NIS2 heeft gehoord is 85 procent. Onder medewerkers die bij bedrijven werken die onder de richtlijn vallen, is dit aandeel vergelijkbaar (83%).
- Ook bij ICT-verantwoordelijken is voor twee derde de richtlijn volledig onbekend.

In hoeverre bent u bekend met de NIS2-richtlijn?

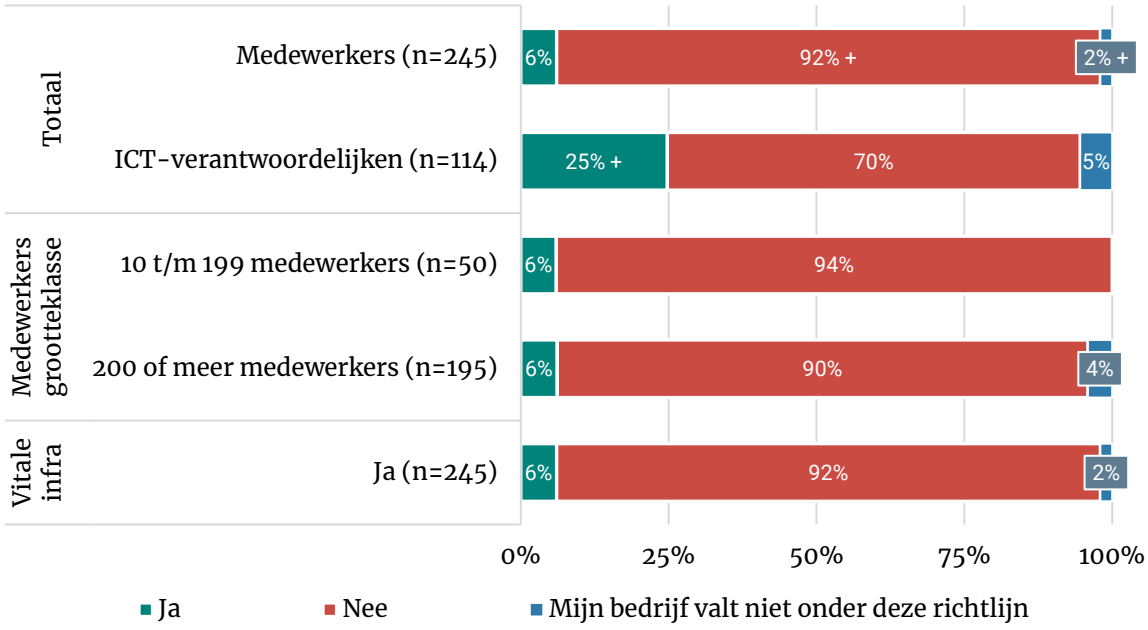


Significante verschillen (p<0.05) tussen (sub)groepen zijn aangegeven met + (hoger) en –(lager).

Negen op tien wisten niet dat bedrijf waarschijnlijk onder NIS2-richtlijn gaat vallen

- Ruim negen op de tien zijn er niet van op de hoogte dat het bedrijf waar men werkt (waarschijnlijk) aan de NIS2-richtlijn moet gaan voldoen.
- Onder ICT-verantwoordelijken is het aandeel dat hiervan wel op de hoogte is het grootst (25%).

Uw bedrijf valt waarschijnlijk onder de NIS2-richtlijn. Was u hiervan op de hoogte? (gesteld aan werkenden die waarschijnlijk onder de NIS2-richtlijn vallen)

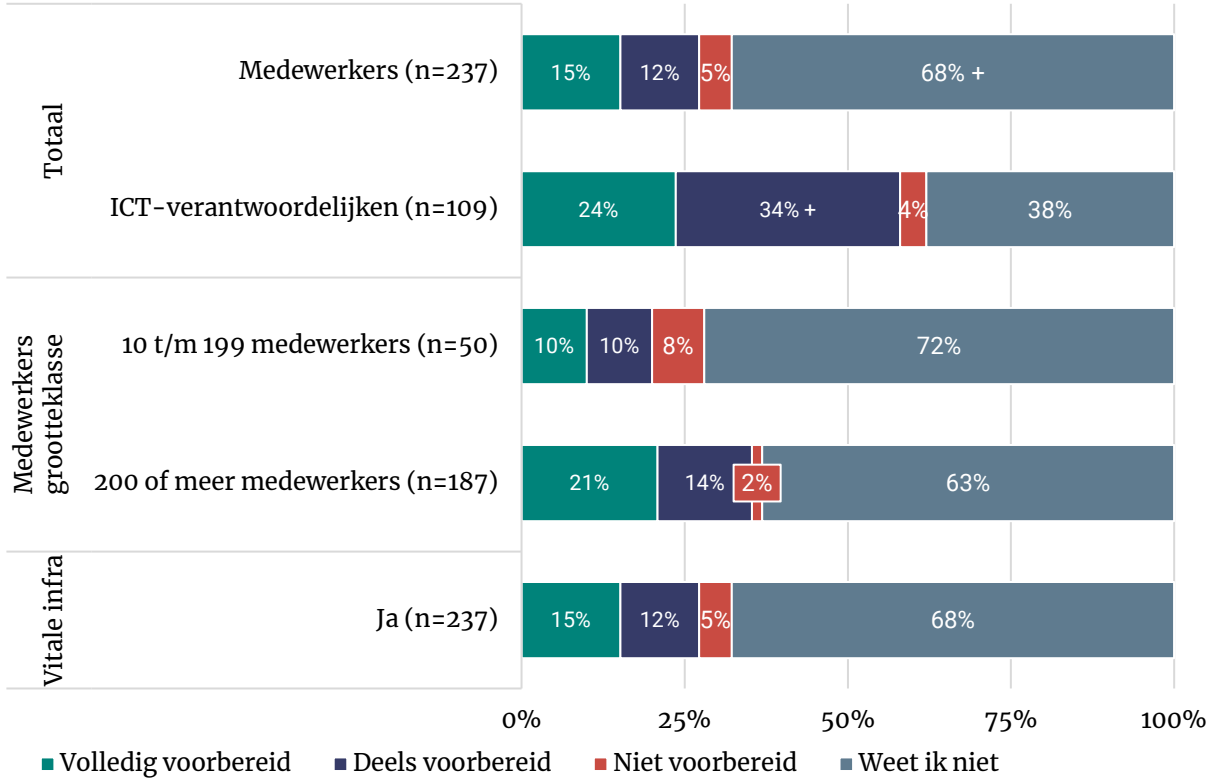


Significante verschillen (p<0.05) tussen (sub)groepen zijn aangegeven met + (hoger) en –(lager).

Twee derde weet niet in hoeverre bedrijf is voorbereid op NIS2

- In lijn met voorgaande vragen over NIS2, zegt een ruime meerderheid (68%) niet te weten in hoeverre hun bedrijf voorbereid is op NIS2.
- Onder ICT-verantwoordelijken is dit aandeel kleiner (38%).
- ICT-verantwoordelijken zeggen vaker dat hun bedrijf deels is voorbereid.

In hoeverre denkt u dat uw bedrijf voorbereid is op de invoering van NIS2? (gesteld aan werkenden die waarschijnlijk onder de NIS2-richtlijn vallen en bij de vorige vraag niet aangaven dat dit niet zo is)



Significante verschillen (p<0.05) tussen (sub)groepen zijn aangegeven met + (hoger) en –(lager).

5. Slachtofferschap en aangiftebereidheid

Kwart medewerkers maakte op werk poging tot phishing mee (1)

- Een kwart van de werkenden (25%), maakte phishing op werk mee (tabel op volgende pagina). Onder ICT-verantwoordelijken is dit aandeel groter (44%).
- ICT-verantwoordelijken hebben vaker te maken met cybercrime dan andere medewerkers. Het herkennen van cybercrime kan daarin een rol spelen.
- Zeven op de tien medewerkers zeggen met geen van de voorgelegde voorvallen op het werk te maken gehad te hebben in de afgelopen twaalf maanden. Bij ICT-verantwoordelijken is dit de helft.

Vergelijking met 2023

- Waar in 2023 een vijfde (21%) van de medewerkers phishingmails ontving, is dit nu een kwart (25%). Acquisitiefraude, inloggen op apparaten zonder toestemming en ervaringen met malware namen af.

Kwart medewerkers maakte op werk poging tot phishing mee (2)

Heeft u in de afgelopen 12 maanden zelf weleens te maken gehad met een van de onderstaande voorvallen in uw werksituatie?	Medewerkers (n=738)	ICT verantwoordelijken (n=417)	Minder dan 10 medewerkers (n=62)	10 t/m 199 medewerkers (n=247)	200 of meer medewerkers (n=429)	Vitaal (n=385)
Mails ontvangen met poging tot phishing	25% +	44%	21%	24% +	29%	36% +
Acquisitiefraude	1% -	4% -	3%	1%	1%	2%
Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik die bijna niet van echt te onderscheiden is	2%	7%	3%	2%	3%	3%
Gebeld door iemand die zich voordeed als bedrijf of officiële instantie om geld of gegevens te bemachtigen	3%	8%	3%	2%	3%	4%
Benaderd op social media met een vraag om een onbekende link aan te klikken	3%	7%	3%	2%	3%	3%
Dat iemand dreigde mijn bestanden te openbaren of dit ook echt deed	1%	4%	2%	2%	1%	1%
Benaderd via WhatsApp door iemand die zich voordeed als een bekende die probeerde geld te ontvangen	4%	7% +	2%	4%	6% +	5% +
Dat iemand in een apparaat heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	0,5% -	0.3%	2%	0,4%	0,0%	0,0%
Ransomware	0,1%	1%	0,0%	0,0%	0,2%	0,1%
Dat iemand in een account heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	0,0%	1%	0,0%	0,0%	0,0%	0,5%
Identiteitsdiefstal	0,0%	0,5%	0,0%	0,0%	0,0%	0,4%
Een foute link ook daadwerkelijk hebben aangeklikt in de zin dat deze een virus, spam, phishing of andere ongewenste poging tot cybercrime bevatte	1%	2%	0,0%	2%	0,7%	2%
Dat een computer tijdelijk niet werkte door malware zoals bijvoorbeeld een virus	0,0% -	1%	0,0%	0,0% -	0,0%	0,4%
Dat door het downloaden van geïnfecteerde software/bestanden malware verspreid werd (o.a. via een e-mail)	0,0% -	1%	0,0%	0,0%	0,0%	0,4%
Geen van deze voorvallen	71%	49%	74%	71%	67%	60% -

Significantie verschillen (p<.05) tussen (sub)groepen zijn aangegeven met groen (hoger).
Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

Meeste meldingen bij ICT-afdeling bedrijf

- De meerderheid van ICT-verantwoordelijken (53%) onderneemt geen actie nadat men te maken kreeg met cybercrime in de werksituatie.
- Iets minder dan de helft van de medewerkers onderneemt geen actie.
- Medewerkers die wel actie ondernemen doen dit door een melding te maken bij de ICT-afdeling.
- Er zijn geen significante verschillen met 2023.

Heeft u of uw werkgever toen een aangifte of melding gedaan? (gesteld indien men in de afgelopen 12 maanden een voorval van cybercrime meemaakte)	Medewerkers (n=229)	ICT-verantwoordelijken (n=221)	Minder dan 10 medewerkers (n=16)*	10 t/m 199 medewerkers (n=70)	200 of meer medewerkers (n=143)	Vitaal (n=133)
Aangifte bij de politie	2%	2%	0%	3%	2%	2%
Melding bij de politie	2%	0%	0%	3%	1%	2%
Melding bij de fraudehelpdesk	7%	8%	0%	10%	5%	5%
Bij een bank	1%	4%	6%	0%	0%	0%
Bij de autoriteit persoonsgegevens	1%	0%	0%	1%	0%	2%
Melding bij de ICT-afdeling van mijn bedrijf	39%	30%	25%	37%	50%	42%
Bij mijn leidinggevende	7%	8%	6%	9%	5%	7%
Melding bij het nationaal cyber security centrum (NCSC)	1%	0%	0%	1%	1%	0%
Bij een andere organisatie	1%	4%	0%	0%	2%	1%
Ik heb hier niks mee gedaan	47%	53%	63%	47%	39%	47%

Significante verschillen tussen medewerkers en ICT-verantwoordelijken zijn aangegeven met groen (hoger).
*Laag aantal waarnemingen. Indicatieve uitkomsten.

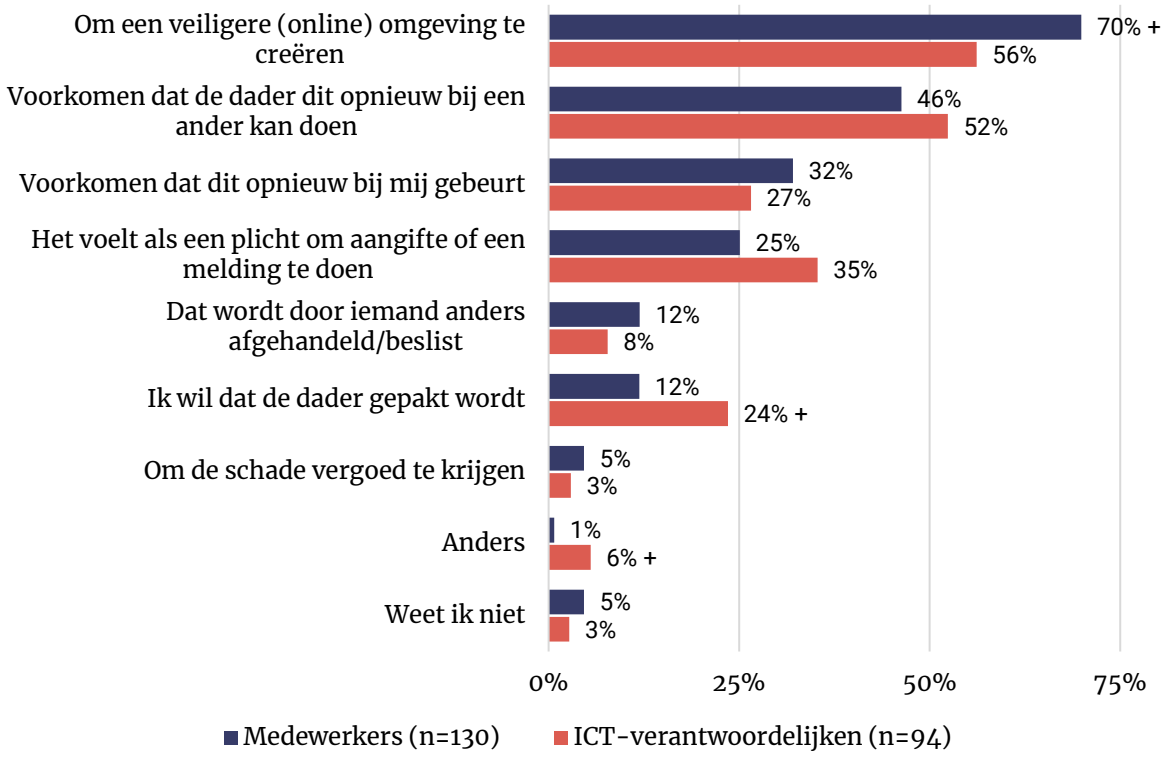
Veiligere omgeving en voorkomen herhaling belangrijkste redenen voor melding of aangifte

- Zeven op de tien medewerkers die een melding of aangifte doen willen een veiligere online omgeving creëren. Voor medewerkers is dit vaker een reden dan voor ICT-verantwoordelijken.
- De helft wil met de melding of aangifte voorkomen dat de dader andere slachtoffers kan maken.
- ICT-verantwoordelijken willen vaker dat de dader gepakt wordt.
- De minst belangrijke reden om melding of aangifte te doen is om de schade vergoed te krijgen.

Vergelijking met 2023

- Minder medewerkers doen aangifte omdat men wil dat de dader gepakt wordt (2024: 12%; 2023: 29%). Het creëren van een veiligere online omgeving is dit jaar echter belangrijker geworden (2024: 70%; 2023: 47%).

Wat zijn de belangrijkste redenen om geen aangifte of melding te doen? (gesteld als men aangifte of melding van de meegemaakte voorval(len) deed)



Significantie verschillen (p<.05) tussen (sub)groepen zijn aangegeven met '+' (hoger).

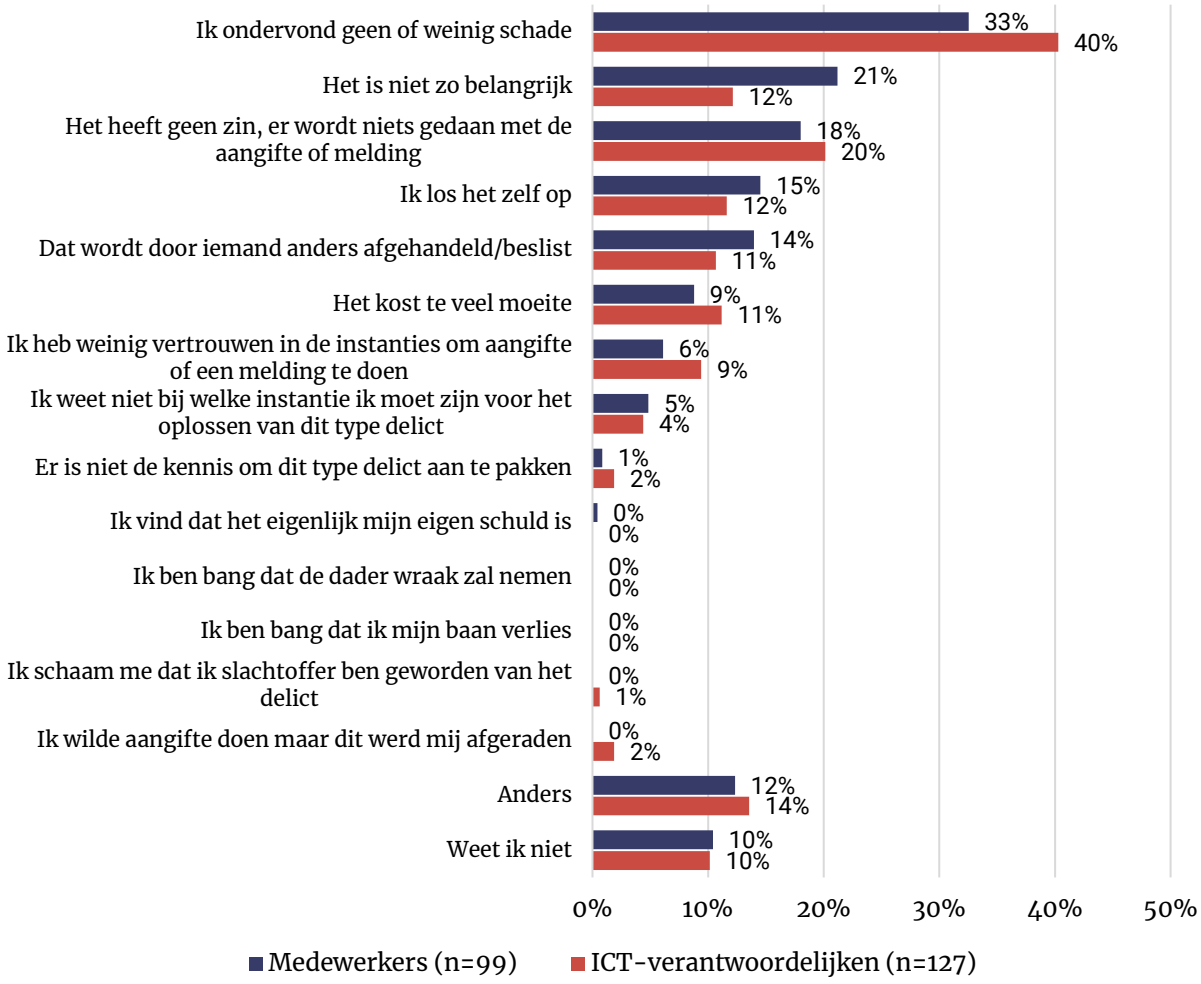
Een op vijf ICT-verantwoordelijken denkt dat melding/aangifte geen zin heeft

- De voornaamste reden om geen melding of aangifte te doen is omdat men geen schade ondervond.
- Een vijfde van de medewerkers vindt het niet zo belangrijk, bij ICT-verantwoordelijken is dit 12 procent.
- Ook denkt een vijfde dat het geen zin heeft.
- Een op de tien ICT-verantwoordelijken heeft weinig vertrouwen in instanties waar men aangifte of melding kan doen.

Vergelijking met 2023

- Er zijn geen significante verschillen in vergelijking met 2023.

Wat zijn de belangrijkste redenen om geen aangifte of melding te doen? (gesteld als men geen aangifte of melding van de meegemaakte voorval(len) deed)



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