Cybersecurity onderzoek Alert Online 2025

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
2025/174

Datum
augustus 2025

Opdrachtgever
Ministerie van Economische Zaken

Auteurs
Bram Doms
Melle Conradie

Inhoudsopgave

1. Managementsamenvatting

Samenvatting | 1/3

Medewerkers schatten kennis over online veiligheid hoger in dan in 2024
Een derde (34%) van de medewerkers schat hun eigen kennis over online veiligheid in als (zeer) goed. In 2024 lag dit percentage op 27 procent. ICT-verantwoordelijken schatten hun kennis hoger in dan andere medewerkers. Het aandeel ICT-verantwoordelijken dat zijn kennis als (zeer) goed beoordeelt is 61 procent.
Drie op de vijf medewerkers (60%) denken dat de eigen organisatie voldoet aan de huidige wet- en regelgeving en de helft (49%) denkt dat hun organisatie ook voorbereid is voor toekomstige regelgeving. Zelf zijn medewerkers niet altijd goed op de hoogte van de wet- en regelgeving. Tien procent zegt (zeer) goed op de hoogte te zijn en de helft (52%) juist (zeer) slecht.

ICT-verantwoordelijken schatten risico cybercrime hoger in
ICT-verantwoordelijken zijn naar eigen zeggen beter bekend met de betekenis van de elf voorgelegde verschillende vormen van cybercrime dan andere medewerkers. Van de vormen van cybercrime die men kent, achten medewerkers het meemaken van phishing in de werksituatie van (61%) het meest waarschijnlijk. Van de ICT-verantwoordelijken vindt 70 procent het waarschijnlijk dat ze phishing op het werk meemaken. Ook van alle andere voorgelegde vormen van cybercrime wordt het door ICT-verantwoordelijken aannemelijker geacht om er op het werk mee te maken te krijgen dan door andere medewerkers.

ICT-verantwoordelijken maken zich vaker zorgen over online veiligheid dan medewerkers
Ruim vier op de tien ICT-verantwoordelijken (43%) maken zich (zeer) veel of enige zorgen over hun eigen online veiligheid op het werk. Onder medewerkers is dit percentage lager (27%). ICT-verantwoordelijken geven zichzelf een hoger cijfer (7,4) als het gaat om het veilig omgaan met online risico's dan andere medewerkers (6,9).

Samenvatting | 2/3

Een vijfde van kleine bedrijven onderneemt geen actie om veilig online te zijn
Twee-staps-inloggen is de meest genomen actie ten behoeve van online veilig zijn bij bedrijven (55% noemt dat dit binnen hun organisatie verplicht is). Ook door ICT-verantwoordelijken (64%) en medewerkers van grote bedrijven (64%) wordt deze maatregel (net zoals in 2024) het vaakst genoemd. Kleine bedrijven (minder dan 10 medewerkers) ondernemen minder acties. Een vijfde van deze bedrijven (20%) onderneemt zelfs geen enkele actie ten behoeve van veilig online zijn. De meeste werknemers (80%) voelen zich comfortabel om cyberincidenten te melden binnen hun organisatie.

In werksituatie komt phishing het vaakst voor
Drie op de tien medewerkers (31%) ontvingen in de afgelopen twaalf maanden een phishingmail op hun werk. Onder ICT-verantwoordelijken was dit 44 procent. Het aandeel medewerkers dat phishing meemaakte nam toe van 25% in 2024 naar 31% in 2025. Ook het gebeld worden door een zogenaamde officiële instantie nam toe (2024: 3%; 2025: 7%). Net zoals in 2024 zeggen ICT-verantwoordelijken vaker te maken te hebben met de verschillende voorgelegde vormen van cybercrime dan andere medewerkers.

Helft onderneemt geen actie na cybercrime
In de helft (47%) van de gevallen dat een medewerker te maken kreeg met cybercrime deed men geen melding of aangifte. Medewerkers die wel actie ondernamen deden dat overwegend door melding te maken bij de ICT-afdeling van hun bedrijf (45%). De belangrijkste reden van medewerkers om aangifte of melding te doen is het creëren van een veiligere online omgeving (60%). Twee op de vijf medewerkers die geen aangifte deden, geven aan dat ze geen of weinig schade ondervonden (41%). Een derde (35%) vond het (daarnaast) niet zo belangrijk. Vijf procent zegt dat het geen zin heeft om aangifte of melding te doen, onder ICT-verantwoordelijken is dit aandeel een vijfde (22%).

Samenvatting | 3/3

Meer dan helft medewerkers gebruik generatieve AI

Een op de drie medewerkers (36%) zegt uitstekend of zeer goed bekend te zijn met generatieve AI, zoals ChatGPT of beeld- en tekstgenererende AI-modellen. Een kwart weet er weinig (14%) of zeer weinig van (9%). Medewerkers van kleinere bedrijven (minder dan 10 werknemers) geven relatief vaker aan hiermee zeer weinig bekend te zijn.

De helft van de medewerkers zegt dat zijn of haar organisatie soms (35%) of structureel (14%) generatieve AI gebruikt. Een kwart van de medewerkers weet niet of dit gebeurt. Een kwart van de medewerkers (26%) vindt dat hun organisatie duidelijke richtlijnen heeft voor het gebruik van generatieve AI om potentiële risico's (bijvoorbeeld op het gebied van dataveiligheid) te beheersen. Een kwart (23%) is het hier juist niet mee eens. Twee op de vijf (38%) kunnen het niet goed beoordelen.

ICT-verantwoordelijken schatten hun kennis over AI groter in dan andere medewerkers. Ook weten ze beter wat binnen de organisatie gebeurt op het gebied van AI en zijn ze positiever over de richtlijnen voor AI in de organisatie. Bijna de helft van de ICT-verantwoordelijken (45%) vindt dat er goede richtlijnen zijn en een vijfde (22%) is het daar niet mee eens.

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. Onderdeel van de campagne is het jaarlijks terugkerende Cybersecurityonderzoek Alert Online waarmee de cybersecuritymaand 29 september wordt 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 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=54);
2 10 t/m 199 medewerkers (n=225);
3 200 of meer medewerkers (n=455).

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 734 medewerkers mee aan dit onderzoek en 754 ICT-verantwoordelijken. De respondenten zijn afkomstig uit het I&O Research Panel. Het online veldwerk vond plaats van 23 juni t/m 6 juli 2025. 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

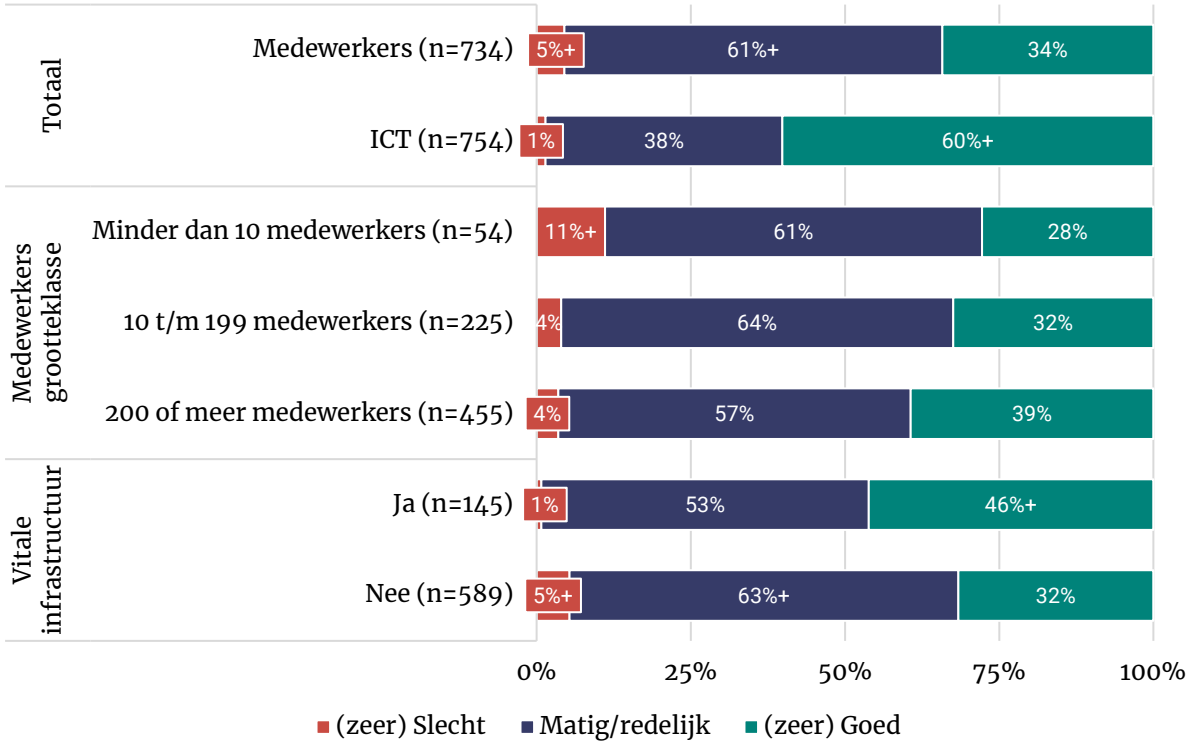
Een derde van de medewerkers vindt eigen kennis over digitale veiligheid (zeer) goed

- Medewerkers schatten hun kennis over digitale veiligheid lager in dan ICT-verantwoordelijken.
- Zes op de tien ICT-verantwoordelijken schatten hun kennis in als (zeer) goed.
- Medewerkers die in vitale sectoren werkzaam zijn schatten hun kennis als beter in dan medewerkers die dat niet zijn.

Vergelijking met 2024

- Medewerkers schatten hun eigen kennis in 2025 vaker als (zeer) goed. In 2024 was dit 27 procent tegenover 34 procent nu.

Hoe schat u uw eigen kennis over digitale veiligheid in?



Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).

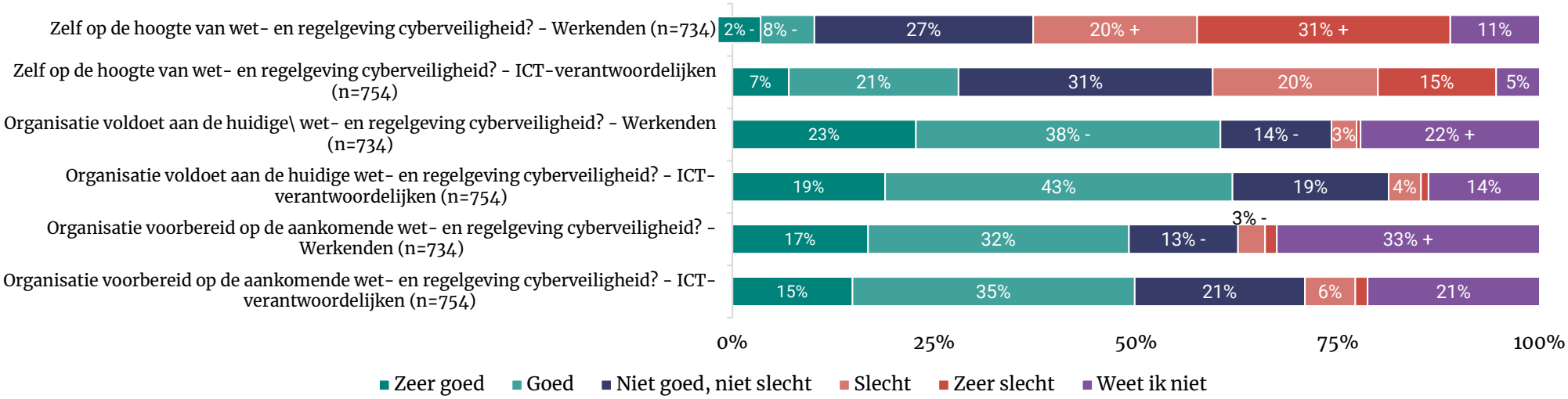
Twee derde denkt dat bedrijf voldoet aan regelgeving cyberveiligheid

- Drie op de vijf medewerkers (60%) denken dat hun organisatie voldoet aan de huidige wet- en regelgeving op het gebied van cyberveiligheid.
- De helft (49%) denkt dat hun organisatie ook voorbereid is op toekomstige regelgeving. Een derde (33%) weet dit niet.
- Zelf zijn medewerkers niet altijd goed op de hoogte van de wet- en regelgeving. Tien procent zegt (zeer) goed op de hoogte te zijn en de helft (52%) juist (zeer) slecht.
- ICT-verantwoordelijken zijn beter op de hoogte, maar ook zij zeggen vaker dat de kennis (zeer) slecht is (35%) dan (zeer) goed (28%).

Vergelijking met 2024

- Deze vraag is in 2025 voor het eerst gesteld. Vergelijking met 2024 is daarom niet mogelijk.

Vragen met betrekking tot wet- en regelgeving op het gebied van cyberveiligheid.



Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).

Helpdeskfraude is de meest bekende vorm van cybercrime

- De meerderheid van de medewerkers kent de elf voorgelegde vormen van cybercrime. Helpdeskfraude is hierbij het vaakst bekend.
- CEO fraude en QR-codefraude zijn het minst bekend onder medewerkers.
- ICT-verantwoordelijken kennen alle voorgelegde vormen van cybercrime vaker dan andere medewerkers.
- Minder dan de helft van de medewerkers denkt te maken te kunnen krijgen met de voorgelegde vormen van cybercrime, maar hacking en phishing vormen hierbij een uitzondering.
- ICT-verantwoordelijken schatten de kans om met de vormen van cybercrime te maken te krijgen consequent groter in.

Vergelijking met 2024

- DDoS-aanvallen (2025: 82%; 2024: 72%) en CEO-fraude (2025: 42%; 2024: 31%) zijn onder medewerkers bekender geworden ten opzichte van 2024.
- Ook achten meer medewerkers dan in 2024 het waarschijnlijk met veel vormen van cybercrime vaker te maken te kunnen krijgen.

In deze tabel staan 11 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=734)	ICT-verantwoordelijk (n=754)	Medewerkers	ICT-verantwoordelijk
Helpdeskfraude*	97%	100%	29%	41%
Hacking	96% -	99%	57%	69%
Identiteitsfraude*	96%	99%	30%	35%
Phishing	95%	99%	61% +	70%
Misbruik van bedrijfsgegevens/bedrijfsnaam online aankopen*	86%	93%	39%	46%
DDoS-aanval	82% +	95% +	55% +	63% +
Aankoopfraude	82%	88%	16%	21%
Malware	78%	93%	56%	63%
Ransomware	71%	92%	56% +	65%
QR-codefraude	58%	76%	24% +	29%
CEO-fraude	42% +	62%	55% +	47%

Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).
* Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

4. Zorgen en online gedrag op het werk

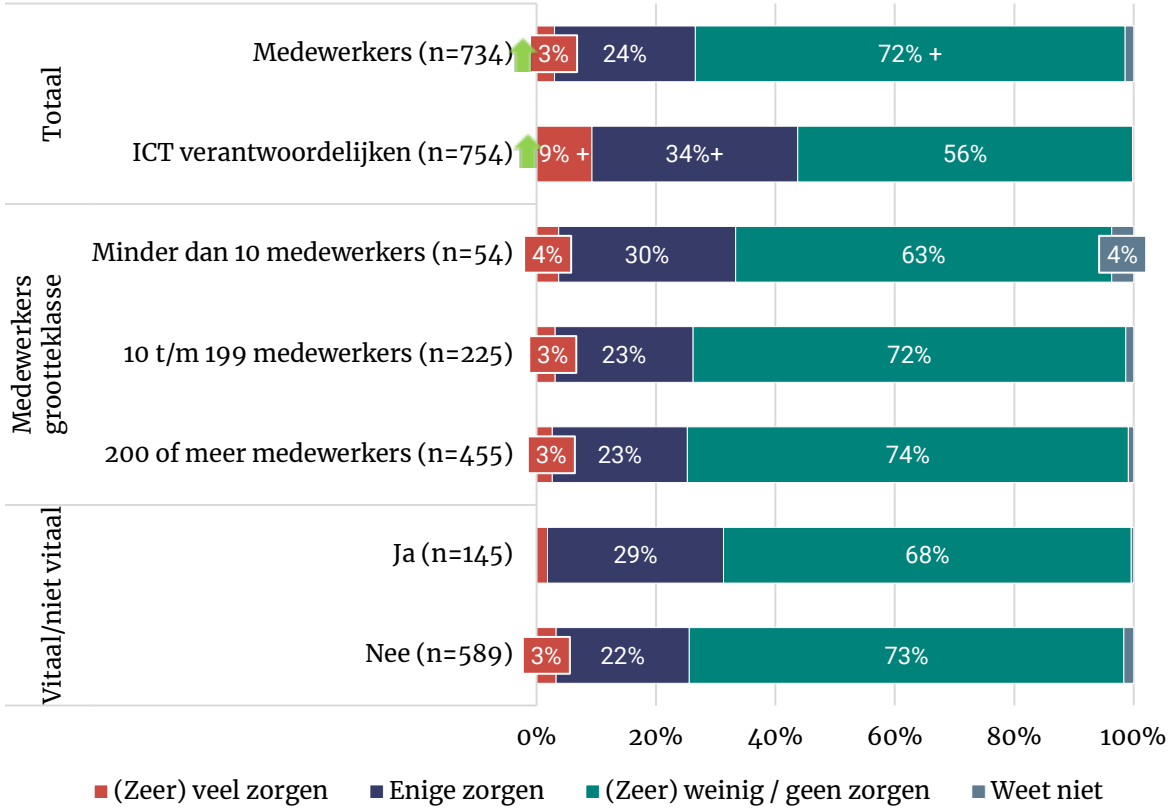
Driekwart medewerkers heeft weinig zorgen over digitale veiligheid in werksituatie

- Vier op de tien ICT-verantwoordelijken (43%) maken zich veel of enige zorgen over hun eigen online veiligheid op het werk. Voor medewerkers is dit percentage significant lager: 27 procent zegt zich zorgen te maken.
- Medewerkers zeggen vaker dan ICT-verantwoordelijken zich weinig of geen zorgen te maken (72%).

Vergelijking met 2024

- Medewerkers maken zich vaker (zeer) veel zorgen in vergelijking met 2024. In 2025 gaat het om 3 procent en in 2024 was dit 1 procent. Ook bij ICT verantwoordelijken is een stijging te zien, van 6 naar 9 procent.

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



Significantie verschillen ten opzichte van 2024 zijn aangegeven met een (afname) of (toename). Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).

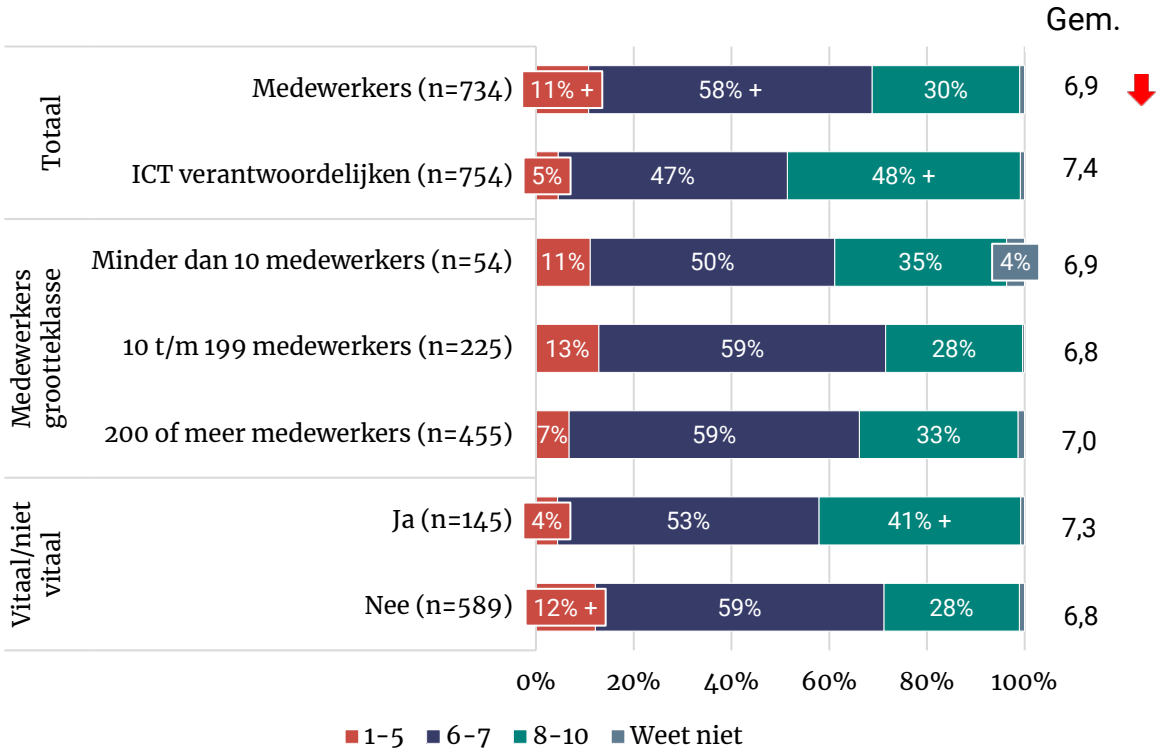
ICT-verantwoordelijken beoordelen hun omgang met online risico's beter dan andere medewerkers

- Gemiddeld geven medewerkers zichzelf een 6,9 als het gaat om het omgaan met online risico's. Dat is lager dan de 7,4 die ICT-verantwoordelijken zichzelf geven. De helft van de ICT-verantwoordelijken (48%) geeft zichzelf het cijfer 8 of hoger.
- Medewerkers van bedrijven tot 200 werknemers geven zichzelf vaker een onvoldoende dan medewerkers van grotere bedrijven.

Vergelijking met 2024

- Medewerkers geven zichzelf dit jaar gemiddeld een 6,9, dat is lager dan in 2024 (7,0).

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



Significantie verschillen ten opzichte van 2024 zijn aangegeven met een ↓ (afname) of ↑ (toename). Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).

Een vijfde van de kleine bedrijven onderneemt geen acties om veilig online te zijn (1)

- Twee-staps-inloggen is net zoals in 2024 de meest genomen actie ten behoeve van het online veilig zijn bij bedrijven (zie de tabel op de volgende pagina). Zes op de tien (64%) ICT-verantwoordelijken en een even groot aandeel van medewerkers van grote bedrijven (200+ medewerkers) noemt dat deze maatregel binnen hun organisatie wordt toegepast.
- Bij de helft van de bedrijven kan alleen software geïnstalleerd worden door de systeembeheerders. Onder de kleinere bedrijven (minder dan 10 medewerkers) is dit aandeel significant lager (28%).
- Het blokkeren van de toegang tot bepaalde websites komt volgens medewerkers het minst voor (28%).
- Een vijfde (17%) van de medewerkers zegt niet te weten welke acties zijn of haar organisatie heeft genomen.
- Een op de vijf (20%) medewerkers van bedrijven met minder dan 10 medewerkers zegt dat geen enkele maatregel genomen wordt.

Vergelijking met 2024

- Alle voorgelegde acties worden dit jaar door meer medewerkers genoemd dan in 2024. Bovendien geven minder medewerkers aan dat er geen enkele actie wordt ondernomen of dat ze niet weten welke acties er genomen worden.

Een vijfde van de kleine bedrijven onderneemt geen acties om veilig online te zijn (2)

Welke acties zijn er binnen uw bedrijf of organisatie ondernomen ten behoeve van veilig online gedrag?	Medewerkers (n=734)	ICT-verantwoordelijk (n=754)	Minder dan 10 medewerkers (n=54)	10 t/m 199 medewerkers (n=225)	200 of meer medewerkers (n=455)	Wel vitaal (n=145)	Niet vitaal (n=589)
Er zijn adviezen/richtlijnen/regels over online veilig gedrag van medewerkers*	50%	59%	13%	46%	68%	66%	47%
De toegang tot bepaalde websites en/of socialmediakanalen is geblokkeerd	28% +	39% +	2%	21%	47%	42%	24%
Er is binnen mijn organisatie/bedrijf een digitale hulpverlener waar je terechtkunt	37% +	38% +	9%	34%	49%	49%	34%
Er wordt getoetst op veilig online gedrag door bijvoorbeeld op willekeurige momenten nep phishingmails te sturen	35% +	44% +	6%	28%	58%	56%	31%
Er zijn afspraken gemaakt over het gebruik van zakelijke apparaten smartphones, laptops en/of tablets voor privé en/of zakelijk gebruik	41% +	53% +	19%	37%	55%	63%	36%
Alleen de systeembeheerders kunnen software installeren	50% +	50% +	28%	50%	55%	53%	49%
Twee-staps-inloggen is verplicht voor toegang	55% +	64% +	30%	55%	64%	71%	52%
Er worden trainingen gegeven binnen mijn organisatie over online veiligheid	40% +	49% +	7%	34%	60%	60%	36%
Anders	2%	8%	7%	1%	2%	1%	2%
Weet ik niet	17% -	7%	24%	19%	12%	6%	20%
In mijn bedrijf of organisatie is geen enkele actie ondernomen ten behoeve van veilig online gedrag	4% -	7% -	20%	3%	0%	3%	4%

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

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

* Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

Meesten vinden het makkelijk om zich aan de afspraken te houden

- Negen op de tien medewerkers (86%) vinden het gemakkelijk om zich aan de afspraken over online veilig gedrag te houden.
- Acht op de tien (83%) zeggen toegang te hebben tot de juiste tools om veilig online te kunnen werken en zeven op de tien (71%) 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 2024

- In 2025 zeggen medewerkers (83%) en ICT-verantwoordelijken (87%) vaker dat ze goede tools en instrumenten krijgen om online veilig gedrag te bevorderen (was voor beide groepen 78% in 2024).
- ICT-verantwoordelijken ervaren dit jaar vaker dat het makkelijk is om zich aan afspraken voor online veilig gedrag te houden (2025: 87%; 2024: 82%).
- Medewerkers vinden vaker (71%) dan in 2024 (64%) 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=605)	ICT verantwoordelijken (n=662)	Minder dan 10 medewerkers (n=30)*	10 t/m 199 medewerkers (n=177)	200 of meer medewerkers (n=398)	Vitaal (n=135)	Niet vitaal (n=470)
Het is gemakkelijk om mij aan de afspraken te houden over online veilig gedrag binnen mijn bedrijf/organisatie	86%	87% +	83%	85%	89%	87%	86%
Ik krijg toegang tot goede tools en instrumenten (bijvoorbeeld tweestapsverificatie of een wachtwoordmanager) om online veilig gedrag te bevorderen	83% +	87% +	77%	80%	90%	86%	82%
De afspraken over online veilig gedrag die binnen mijn organisatie/bedrijf zijn gemaakt, worden voldoende toegepast	71% +	71%	70%	66%	80%	81%	69%

Significantieverschillen (p<.05) tussen (sub)groepen zijn aangegeven met groen (hoger).
Significante Verschillen tussen 2024 en 2025 zijn aangegeven met '+' (toename) en '-' (afname).
* = Indicatief i.v.m. laag aantal waarnemingen.

Melden bedreigingen wordt binnen meeste organisaties gewaardeerd

- Negen op de tien medewerkers (86%) vinden het gemakkelijk om zich aan de afspraken over online veilig gedrag te houden.
- De helft (49%) van de medewerkers wordt erop aangesproken als werkafspraken niet nageleefd worden.
- Twee op de vijf medewerkers (41%) spreken collega's aan als deze zich niet aan werkafspraken houden, onder ICT-verantwoordelijken is dit aandeel met 58 procent hoger.
- Driekwart (72%) van de ICT-verantwoordelijken past veiligheidsmaatregelen op het werk ook in de privésituatie toe, onder medewerkers gebeurt dit minder (56%).
- In de vitale sectoren worden medewerkers er vaker op aan gesproken als ze zich niet aan werkafspraken voor veilig gedrag houden (60%). Bij bedrijven in niet-vitale sectoren is dit 46 procent.

Vergelijking met 2024

- ICT-verantwoordelijken zeggen dit jaar vaker aangesproken te worden op het niet houden aan werkafspraken (2025: 59%; 2024: 52%).

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=605)	ICT verantwoordelijken (n=662)	Minder dan 10 medewerkers (n=30)*	10 t/m 199 medewerkers (n=177)	200 of meer medewerkers (n=398)	Vitaal (n=135)	Niet vitaal (n=470)
Ik word er op mijn werk op aangesproken als ik me niet aan de werkafspraken houd over online veilig gedrag	49%	59% +	40%	44%	58%	60%	46%
Ik spreek collega's er op aan als zij zich niet houden aan de werkafspraken over online veilig gedrag	41%	58%	43%	37%	48%	46%	40%
Ik pas de veiligheidsmaatregelen die ik voor werk moet nemen ook toe in mijn privé-situatie	56%	72%	67%	54%	57%	60%	55%
Het melden van mogelijke bedreigingen wordt gewaardeerd op mijn werk*	86%	83%	83%	84%	90%	89%	85%
Digitale veiligheid staat hoog op de agenda bij het bestuur / de directie van mijn werk*	66%	74%	57%	57%	82%	75%	64%

Significantieverschillen (p<.05) tussen (sub)groepen zijn aangegeven met groen (hoger).
Significante Verschillen tussen 2024 en 2025 zijn aangegeven met '+' (toename) en '-' (afname).
* = Indicatief i.v.m. laag aantal waarnemingen.

Twee derde van medewerkers update slimme apparaten altijd

- Bij twee op de drie medewerkers maakt de werkgever automatische back-ups van alle bestanden (68%). Bijna de helft (45%) maakt thuis ook back-ups.
- Twee derde van de werknemers zorgt dat hun slimme apparaten altijd de laatste updates gebruiken (66%) en controleren of mobiele apps veilig zijn voordat ze deze installeren (69%).
- ICT-verantwoordelijken zeggen vaker dat hun werkgever volledige back-ups uitvoert (82%). Bovendien maken ze ook zelf vaker back-ups thuis (65%).
- Ook andere maatregelen worden door ICT-verantwoordelijken vaker genomen dan door medewerkers.

Vergelijking met 2024

- ICT-verantwoordelijken versturen minder vaak dan in 2024 werkbestanden naar hun privémail (2025: 5%; 2024: 11%).

In hoeverre zijn de volgende uitspraken van toepassing op uw gedrag? % meestal wel + altijd / (Zeer) waarschijnlijk	Medewerkers (n=734)	ICT-verantwoordelijk (n=754)
Ik maak thuis regelmatig back-ups van mijn bestanden	45% +	65%
Mijn werkgever maakt automatisch back-ups van alle bestanden (volledige back-ups)	68% +	82%
Ik verstuur werkbestanden van mijn werk e-mailadres naar mijn privé e-mail	6% +	5% +
Ik zorg dat al mijn slimme apparaten altijd de laatste updates gebruiken*	66%	75%
Ik controleer of mobiele apps veilig en betrouwbaar zijn voordat ik deze installeer*	69%	80%

Significantie verschillen (p<.05) tussen (sub)groepen zijn aangegeven met groen (hoger).
Significante verschillen tussen 2024 en 2025 zijn aangegeven met '+' (toename) en '-' (afname).
* Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

Meer dan helft zou zich schamen na het aanklikken van phishinglink

- Vier op de vijf werknemers denkt het meteen te zullen melden aan anderen of aan de ICT-afdeling wanneer ze een virus downloaden.
- Ruim de helft verwacht zich te schamen wanneer ze op een phishinglink klikken. ICT-verantwoordelijken vaker (63%) dan medewerkers (58%).
- Zeven procent van de medewerkers verwacht te betalen om weer toegang tot bestanden te krijgen na slachtofferschap van gijzelsoftware. Dit is vaker dan ICT-verantwoordelijken (4%).

Vergelijking met 2024

- Ten opzichte van 2024 verwachten medewerkers nu vaker te betalen voor toegang tot hun bestanden na een ransomware aanval (2025: 7%; 2024: 4%).
- Ook meldt men het downloaden van een virus vaker aan iemand of de ICT-afdeling op het werk dan in 2024 (toen respectievelijk 75% en 76%; 2025: 81% en 84%).

In hoeverre zijn de volgende uitspraken van toepassing op uw gedrag? % Zeer waarschijnlijk + waarschijnlijk	Medewerkers (n=734)	ICT-verantwoordelijk (n=754)
Als ik getroffen wordt door ransomware (gijzelsoftware), dan zou ik betalen als ik daardoor weer toegang krijg tot mijn persoonlijke bestanden'	7% +	4%
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.	81% +	84%
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.	84% +	84%
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%	3%
Als ik op een link in een phishing e-mail zou klikken dan zou ik mij daarvoor schamen	58%	63% +
Als er een update beschikbaar is voor mijn werkcomputer voer ik deze meteen uit*	75%	86%

Significantie verschillen (p<.05) tussen (sub)groepen zijn aangegeven met groen (hoger).
Significante Verschillen tussen 2024 en 2025 zijn aangegeven met '+' (toename) en '-' (afname).
* Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

Meerderheid gebruikt bij thuiswerken wifi-netwerk met wachtwoord

- De meeste medewerkers maken bij het thuiswerken gebruik van wifi met een wachtwoord (87%).
- Medewerkers werkzaam bij grotere bedrijven (200 of meer medewerkers) gebruiken relatief vaak een VPN-verbinding (48%).

Vergelijking met 2024

- Er zijn geen verschillen met 2024.

Als u thuiswerkt: van wat voor netwerkverbinding maakt u gebruik?	Medewerkers (n=454)	ICT - verantwoordelijk (n=660)	Minder dan 10 medewerkers (n=31)	10 t/m 199 medewerkers (n=138)	200 of meer medewerkers (n=285)	Wel vitaal (n=108)	Niet vitaal (n=346)
Een wifi-netwerkverbinding met wachtwoord	87%	85% -	90%	88%	85%	86%	88%
Een wifi-netwerkverbinding zonder wachtwoord (bv openbaar (wifi-) netwerk	1%	1%	6%	1%	1%	1%	1%
Een VPN-verbinding	37%	47%	16%	33%	48%	40%	36%
Een hotspotverbinding (3G/4G/5G) via mijn smartphone of tablet	9%	12%	13%	9%	9%	8%	9%
Via een internetkabel (niet draadloos; LAN)	20%	33%	29%	20%	19%	20%	21%

Significantie verschillen (p<.05) tussen (sub)groepen zijn aangegeven met groen (hoger).
Significante Verschillen tussen 2024 en 2025 zijn aangegeven met '+' (toename) en '-' (afname).

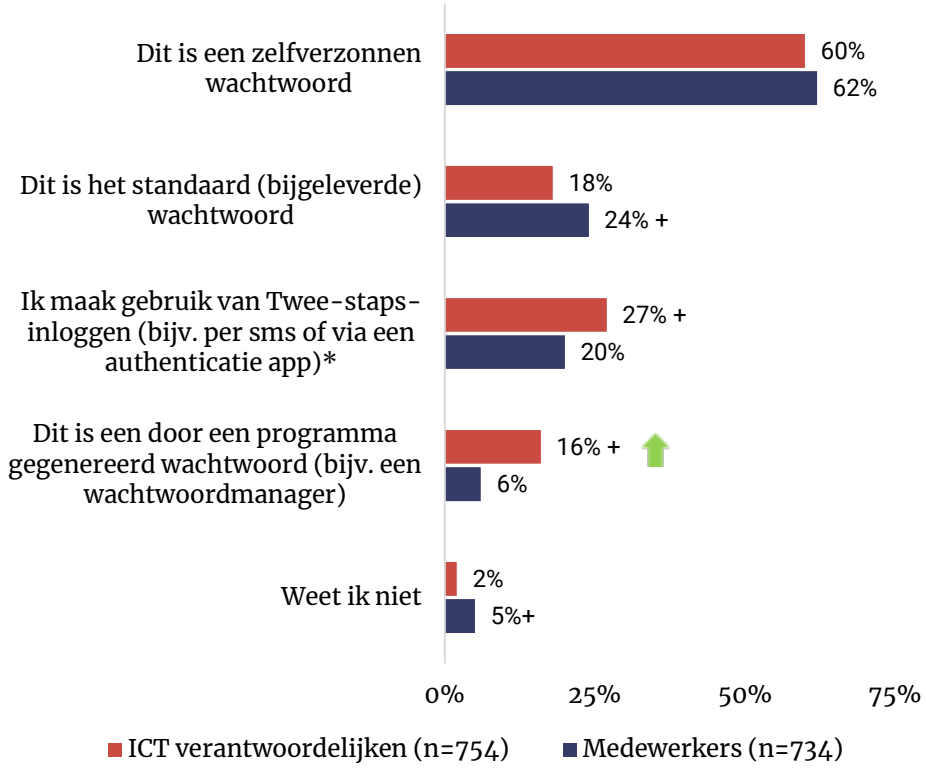
Zes op de tien gebruiken een zelfverzonnen wachtwoord voor netwerkverbinding thuis

- Zes op tien medewerkers gebruiken een zelfverzonnen wachtwoord thuis (62%).
- Een kwart (24%) gebruikt het standaard met de router meegeleverde wachtwoord. Onder ICT-verantwoordelijken is dit 18 procent.
- ICT-verantwoordelijken gebruiken vaker dan andere medewerkers een door een programma gegenereerd wachtwoord en twee-staps-inloggen.

Vergelijking met 2024

- Het aandeel ICT-verantwoordelijken dat een door een programma gegenereerd wachtwoord gebruikt, is toegenomen (2025: 16%; 2024: 11%).

U geeft aan dat u thuis gebruikmaakt van een netwerkverbinding met wachtwoord. Kunt u aangeven wat voor soort wachtwoord dat is?



Significantie verschillen (p<.05) tussen medewerkers en ICT-verantwoordelijken zijn aangegeven met '+' hoger en '-' lager. Verschillen tussen 2024 en 2025 zijn met groen (hoger) of rood (lager) aangegeven.
* Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

5. Slachtofferschap en aangiftebereidheid

Drie op de tien medewerkers maakten op werk poging tot phishing mee (1)

- Drie op de tien medewerkers (31%), maakte phishing op het werk mee (tabel op volgende pagina). Onder ICT-verantwoordelijken is dit aandeel groter (44%).
- Veel vormen van cybercrime zeggen ICT-verantwoordelijken vaker mee te maken dan andere medewerkers.
- Twee derde (64%) van de medewerkers zegt 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 (49%).

Vergelijking met 2024

- Waar in 2024 een kwart (25%) van de medewerkers phishingmails ontving, is dit nu een drie op de tien (31%). Ook het gebeld worden door een zogenaamde officiële instantie nam toe (2024: 3%; 2025: 7%).

Drie op de tien medewerkers maakten op werk poging tot phishing mee (2)

Heeft u in de afgelopen 12 maanden zelf weleens te maken gehad met één van de onderstaande voorvallen? Gesteld indien meegemaakt: percentages meegemaakt in *werksituatie*.	Medewerkers (n=734)	ICT-verantwoordelijken (n=754)	Minder dan 10 medewerkers (n=54)	10 t/m 199 medewerkers (n=225)	200 of meer medewerkers (n=455)	vitaal (n=145)	Niet vitaal (n=589)
Benaderd op Whatsapp door iemand die zich voordeed als een bekende die probeerde geld te ontvangen	4%	7%	2%	4%	4%	5%	3%
Geïnfecteerde software/bestanden gedownload waardoor malware werd verspreid	0%	1%	0%	0%	0%	0%	0%
Computer werkte tijdelijk niet door malware/virus	1%	1%	2%	1%	0%	1%	1%
Identiteitsdiefstal	0%	0%	0%	0%	0%	0%	0%
Mails ontvangen met poging tot phishing	31% +	44%	20%	31%	33%	36%	29% +
Benaderd op social media met een vraag om een onbekende link aan te klikken	3%	7%	2%	4%	3%	7%	2%
Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik die echt leek	3%	7%	4%	3%	3%	3% +	3%
Ransomware	0%	1%	0%	0%	0%	0%	0%
Acquisitiefraude	1%	4%	2%	0%	1%	2%	0%
Dat iemand in een apparaat (computer, telefoon) heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	0%	0%	0%	1%	0%	0%	1%
Dat iemand dreigde uw bestanden te openbaren of dit ook echt deed	1%	4%	2%	2%	1%	2%	1%
Dat iemand in een account heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	1%	1%	0%	1%	0%	2%	0%
Gebeld door iemand die zich voordeed als bedrijf of officiële instantie (bijv. bank, belasting) om geld of gegevens te bemachtigen	7% +	8%	7%	8% +	6% +	9%	7% +
Aankoopfraude	1%	1%	0%	1%	0%	0%	1%
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%	1%	2%	4%	1%
Geen van deze voorvallen	64% -	49%	78%	63%	62%	56%	66%

Significantie verschillen (p<.05) tussen (sub)groepen zijn aangegeven met groen (hoger).
Significante Verschillen tussen 2024 en 2025 zijn aangegeven met '+' (toename) en '-' (afname).

Wanneer melding gemaakt wordt, is dat meestal bij de ICT-afdeling

- 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 (47%) onderneemt geen actie.
- Medewerkers die wel actie ondernemen, doen dit vaak door een melding te maken bij de ICT-afdeling (45%).
- ICT-medewerkers maken vaker dan andere medewerkers melding bij de Autoriteit Persoonsgegevens of de bij een bank. Medewerkers in vitale sectoren maken vaker melding bij de fraudehelpdesk.

Vergelijking met 2024

- Vergeleken met 2024 maken ICT-medewerkers vaker melding bij de Autoriteit Persoonsgegevens (2024: 0%; 2025: 5%).

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=265)	ICT verantwoordelijken (n=406)	Minder dan 10 medewerkers (n=12*)	10 t/m 199 medewerkers (n=82)	200 of meer medewerkers (n=171)	Vitaal (n=69)	Niet vitaal (n=196)
Ja, aangifte bij de politie	2%	4%	8%	1%	1%	1%	2%
Ja, melding bij de politie	1%	2%	0%	1%	2%	2%	1%
Ja, melding bij de Fraudehelpdesk	5%	8%	8%	4%	6%	12%	3%
Ja, bij een bank	0%	6%	0%	0%	1%	2%	0%
Ja, bij de Autoriteit Persoonsgegevens	1%	5% +	0%	0%	3%	3%	1%
Ja, melding bij de ICT-afdeling van mijn bedrijf	45%	31%	17%	45%	49%	45%	44%
Ja, bij mijn leidinggevende	7%	7%	0%	7%	8%	6%	8%
Ja, melding bij het Nationaal Cyber Security Centrum (NCSC)	2%	2%	0%	1%	3%	7%	0%
Ja, bij een andere organisatie namelijk	1%	4%	8%	0%	2%	2%	1%
Nee, ik/mijn werkgever hebben hier niks mee gedaan	47%	53%	58%	48%	43%	42%	48%

Significante verschillen tussen groepen zijn aangegeven met groen (hoger).
*Laag aantal waarnemingen: Indicatieve uitkomsten.

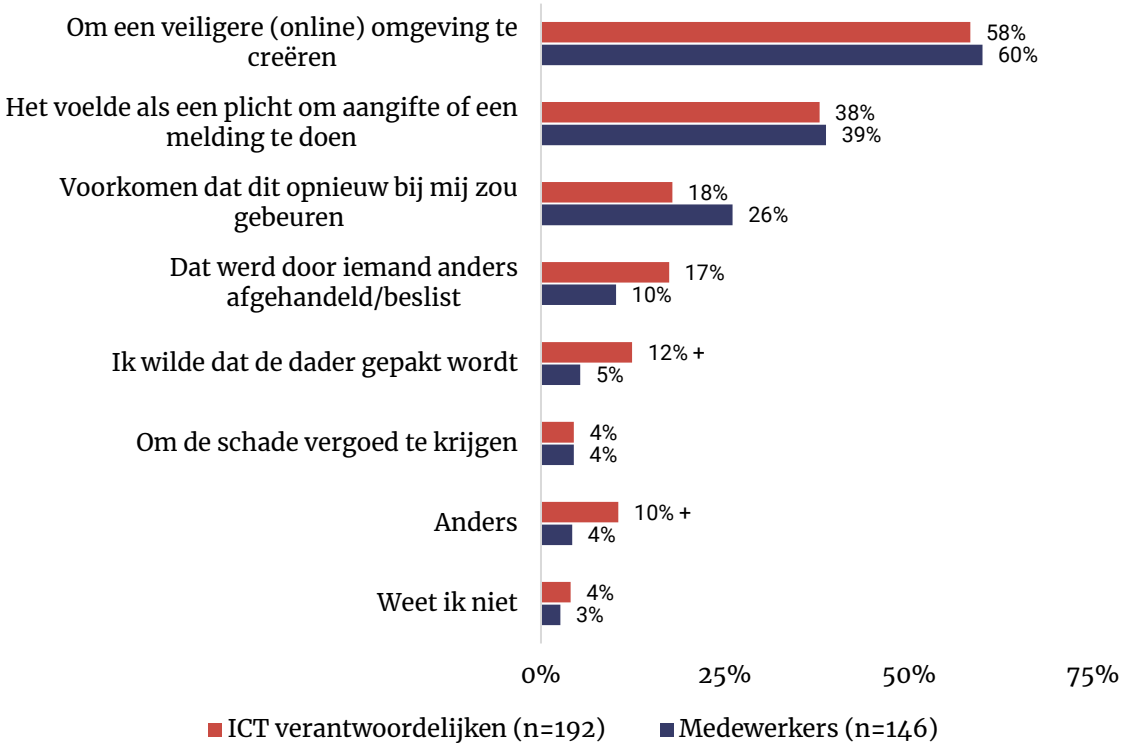
Veiligere omgeving belangrijkste redenen voor melding of aangifte

- Drie op de vijf medewerkers die een melding of aangifte doen, willen een veiligere online omgeving creëren.
- Twee op de vijf medewerkers zien het als een plicht om aangifte te doen.
- Vijf procent wil met de melding of aangifte zorgen dat de dader gepakt wordt. ICT-verantwoordelijken willen dit nog vaker (12%).
- De minst belangrijke reden om melding of aangifte te doen is om de schade vergoed te krijgen.

Vergelijking met 2024

- Meer medewerkers dan een jaar eerder doen aangifte omdat ze het als een plicht zien (2024: 25%; 2025: 39%).
- ICT-verantwoordelijken noemen minder vaak als reden dat ze willen dat de dader wordt gepakt (2024: 24%; 2025: 12%). Vaker zeggen ze dit jaar dat het door anderen wordt beslist (2024: 8%; 2025: 17%).

Wat zijn de belangrijkste redenen om wel 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).

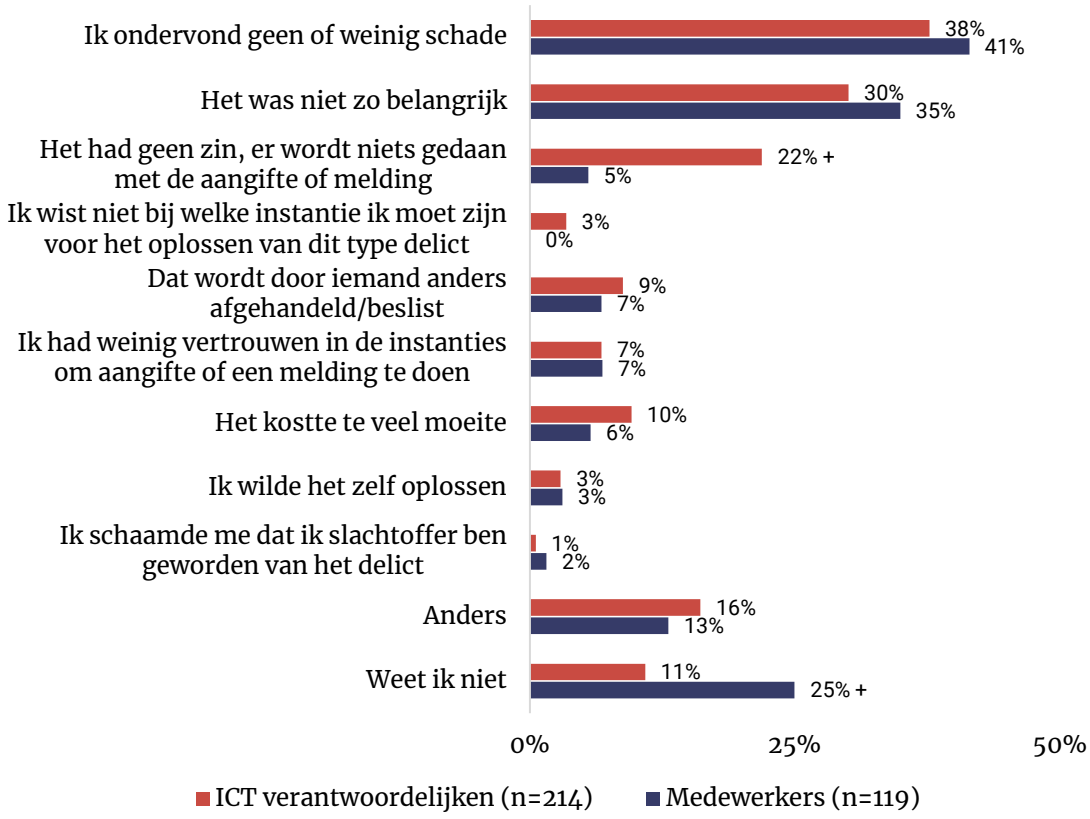
Een vijfde van de ICT-verantwoordelijken denkt dat melding/aangifte geen zin heeft

- De voornaamste reden om geen melding of aangifte te doen is omdat men geen schade ondervond.
- Drie op de tien (30%) vonden het niet zo belangrijk om aangifte of melding te doen.
- Ook denkt een vijfde van de ICT verantwoordelijken dat het geen zin heeft. Onder andere medewerkers is dit percentage met 5 procent lager.
- Een kwart van de medewerkers heeft geen reden waarom geen aangifte of melding is gedaan. Dit is meer dan bij de ICT-verantwoordelijken (11%).

Vergelijking met 2024

- Medewerkers noemen minder dan in 2024 dat aangifte geen zin heeft (2024: 18%; 2025: 5%). Wel zegt men vaker dat het niet zo belangrijk is (2024: 21%; 2025: 35%).
- Onder ICT-verantwoordelijken zijn vergelijkbare verschillen.

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)



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

Meerderheid voelt zich comfortabel om cyberincident te melden

- De meerderheid van medewerkers (80%) en ICT-verantwoordelijken (83%) voelt zich comfortabel om cyberincidenten te melden.
- Driekwart van de ICT-verantwoordelijken (74%) zegt dat hun organisatie open communicatie over kwetsbaarheden en incidenten aanmoedigt, van de werknemers zegt 61 procent dit.
- Het overgrote deel is het er niet mee eens dat melders van incidenten negatieve gevolgen van hun melding ondervinden. Drie procent is het hier eens met deze stelling.

Vergelijking met 2024

- Deze vraag is in 2025 voor het eerst gesteld. Vergelijking met 2024 is daarom niet mogelijk.

Bent u het eens of oneens met de onderstaande stellingen? % (helemaal) mee eens.	Medewerkers (n=734)	ICT verantwoordelijken (n=754)	Minder dan 10 medewerkers (n=54)	10 t/m 199 medewerkers (n=225)	200 of meer medewerkers (n=455)	Vitaal (n=145)	Niet vitaal (n=589)
Mijn organisatie moedigt open communicatie aan over kwetsbaarheden en incidenten op het gebied van cyberveiligheid	61%	74%	46%	58%	70%	76%	58%
Als ik een cyberincident mee zou maken op het werk, zou ik me comfortabel voelen om dit te melden'	80%	83%	69%	79%	86%	89%	78%
Mijn organisatie waardeert medewerkers die cyberveiligheidsincidenten melden	72%	78%	61%	68%	82%	89%	69%
Binnen mijn organisatie ondervinden melders van cyberveiligheidsincidenten negatieve gevolgen	3%	3%	4%	3%	4%	4%	3%

Significante verschillen tussen groepen zijn aangegeven met groen (hoger).

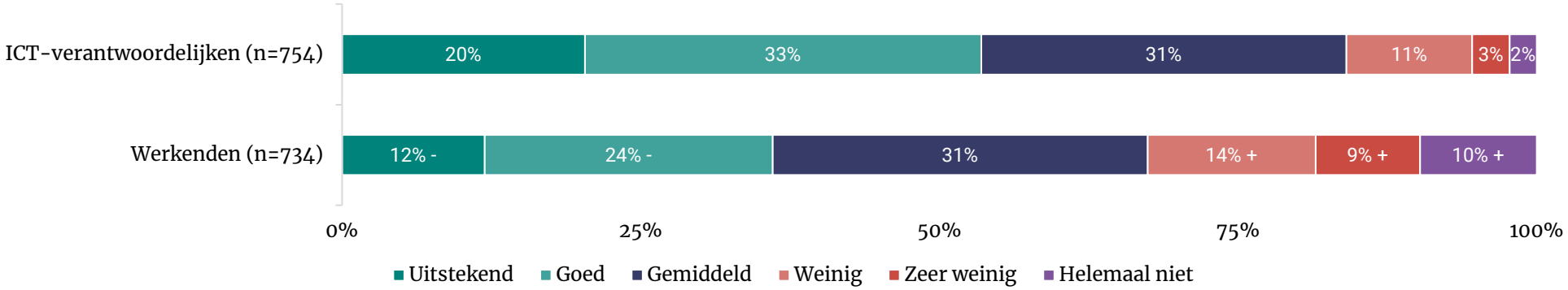
Wisselende kennis van generatieve AI

- Een op de drie medewerkers (36%) zegt uitstekend of zeer goed bekend te zijn met generatieve AI, zoals ChatGPT of beeld- en tekstgenererende AI-modellen.
- Een kwart weet er juist weinig (14%) of zeer weinig van (9%).
- Drie op de tien (31%) beoordelen de eigen kennis als gemiddeld.
- ICT-verantwoordelijken schatten hun kennis hoger in dan andere medewerkers.
- Medewerkers van bedrijven met minder dan 10 werknemers geven vaker dan bij grotere bedrijven aan zeer weinig bekend te zijn (19%).
- Medewerkers van middelgrote bedrijven (10-199 medewerkers) geven relatief vaker aan weinig bekend te zijn met generatieve AI (16%).

Vergelijking met 2024

- Deze vraag is in 2025 voor het eerst gesteld. Vergelijking met 2024 is daarom niet mogelijk.

In hoeverre bent u bekend met toepassingen van generatieve AI, zoals ChatGPT of beeld- en tekst genererende AI-modellen?



Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).

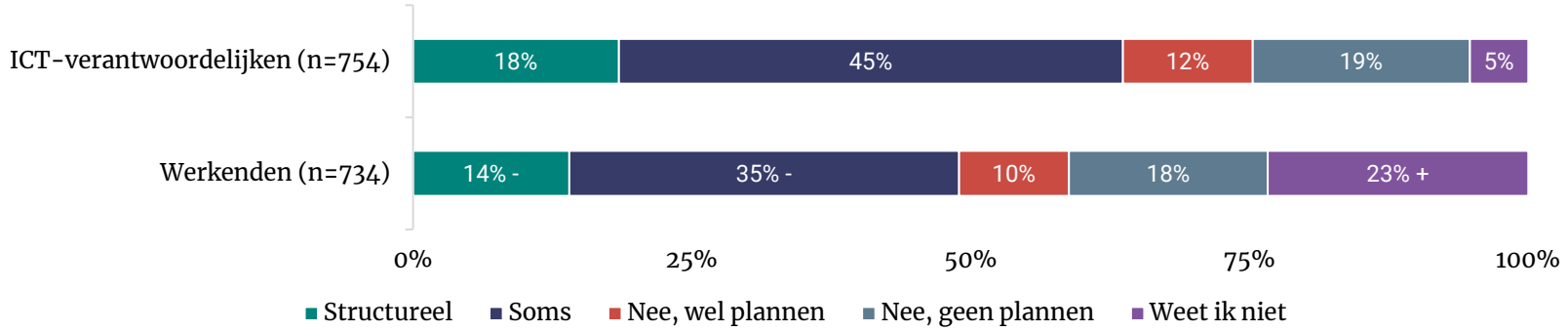
Meer dan de helft gebruikt generatieve AI

- De helft van de medewerkers zegt dat zijn of haar organisatie soms (35%) of structureel (14%) generatieve AI gebruikt. ICT-verantwoordelijken weten vaker of AI gebruikt wordt en geven ook vaker aan dat dit binnen de organisatie in gebruik is.
- Bij 10 procent van de medewerkers zijn plannen voor gebruik van generatieve AI binnen hun organisatie.
- Een kwart van de medewerkers weet niet of dit gebeurt.
- Binnen grote bedrijven (200+ medewerkers) weet men relatief vaak niet (28%) of de organisatie generatieve AI gebruikt. Medewerkers van kleinere bedrijven (minder dan 10 medewerkers) geven vaker aan dat hun bedrijf geen generatieve AI gebruikt en dat daar ook nog geen plannen voor zijn (41%).

Vergelijking met 2024

- Deze vraag is in 2025 voor het eerst gesteld. Vergelijking met 2024 is daarom niet mogelijk.

Gebruikt uw organisatie generatieve AI?



Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).

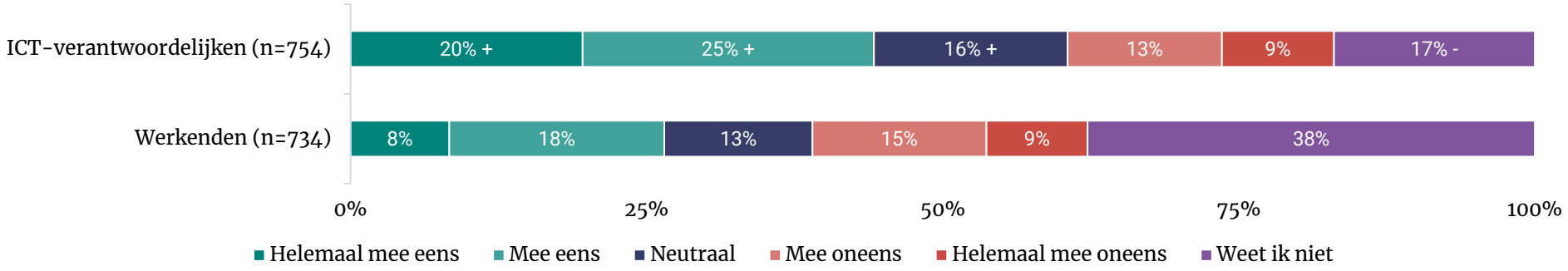
Een derde heeft duidelijke richtlijnen voor het gebruik van AI

- Een kwart van de medewerkers (26%) vindt dat hun organisatie duidelijke richtlijnen heeft voor het gebruik van generatieve AI om potentiële risico's (bijvoorbeeld op het gebied van dataveiligheid) te beheersen. Een kwart (23%) is het hier juist niet mee eens. Twee op de vijf (38%) kunnen het niet goed beoordelen.
- ICT-verantwoordelijken zijn positiever. Bijna de helft (45%) vindt dat er goede richtlijnen zijn en een vijfde (22%) is het daar niet mee eens.

Vergelijking met 2024

- Deze vraag is in 2025 voor het eerst gesteld. Vergelijking met 2024 is daarom niet mogelijk.

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



Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).

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