Cybersecurity onderzoek Alert Online 2023

Deelrapport bedrijfsleven
Medewerkers en ICT-verantwoordelijken

i&O research

Ministerie van Economische Zaken en Klimaat

Colofon

Uitgave
I&O Research
Piet Heinkade 55
1019 GM Amsterdam

Rapportnummer
2023/171

Datum
september 2023

Opdrachtgever
Ministerie van Economische Zaken en Klimaat

Auteurs
Melle Conradie
Bram Doms

Inhoudsopgave

1. Managementsamenvatting

Samenvatting | 1/2

ICT-verantwoordelijken schatten kennisniveau hoger in dan andere groepen medewerkers
Eén op de vijf (21%) medewerkers schat de eigen kennis over online veiligheid in als (zeer) goed. In 2022 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 48 procent. Medewerkers van grote bedrijven schatten hun kennis gemiddeld hoger in (5% zeer goed) dan medewerkers van kleine bedrijven (1% zeer goed). Ook medewerkers in vitale sectoren zeggen, ten opzichte van anderen, vaker dat hun kennis over digitale veiligheid zeer goed is (5%).

Medewerkers schatten het risico dat zij te maken krijgen met cybercrime lager in dan ICT-verantwoordelijken
ICT-verantwoordelijken zijn beter bekend met de betekenis van de verschillende vormen van cybercrime dan andere medewerkers. Ruim de helft van de medewerkers denkt te maken te kunnen krijgen met phishing en hacking op het werk. Onder ICT-verantwoordelijken is dit aandeel ongeveer driekwart. Ook alle andere voorgelegde vormen van cybercrime worden door ICT-verantwoordelijken aannemelijker geacht dan door andere medewerkers.

ICT-verantwoordelijken maken zich meer zorgen over online veiligheid dan medewerkers
Bijna de helft van de ICT-verantwoordelijken (46%) maakt zich zorgen over de eigen online veiligheid. Voor andere medewerkers is dit percentage significant lager (23%). Wel geven ICT-verantwoordelijken zichzelf een hoger cijfer als het gaat om het veilig omgaan met online risico's (7,1; medewerkers totaal 6,6).

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 gedrag bij bedrijven. De helft van de ICT-verantwoordelijken (49%) en medewerkers van grote bedrijven (47%) noemt deze maatregel. Kleine bedrijven ondernemen minder acties. Bovendien onderneemt een vijfde van deze bedrijven (19%) geen enkele actie ten behoeve van veilig online gedrag. Wanneer we kijken naar alle medewerkers, dan geeft 8 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 hebben vaker zorgen over datalek

Een kwart (24%) van de ICT-verantwoordelijken maakt zich in (zeer) grote mate zorgen om slachtoffer te worden van een datalek. Medewerkers zijn hier minder bezorgd over (44% geen of weinig zorgen). ICT-verantwoordelijken leggen de verantwoordelijkheid voor veilig online gedrag op het werk vooral bij zichzelf.

Phishing komt het vaakst voor in de werksituatie

Een op de vijf (21%) medewerkers ontving in de afgelopen 12 maanden op het werk een phishingmail. Onder ICT-verantwoordelijken was dit zelfs 50 procent. Bij beide groepen is dit de vorm van cybercrime die men het meest meemaakt. Net zoals in 2022 hebben ICT-verantwoordelijken vaker te maken met verschillende voorgelegde vormen van cybercrime dan andere medewerkers.

Meerderheid onderneemt geen actie op cybercrime

Zes op de tien (59%) medewerkers die te maken kregen met cybercrime deden hier geen melding of aangifte van. Doet men dit wel, dan is de ICT-afdeling van het bedrijf de plek waar men zich het vaakste meldt (34%). De belangrijkste redenen om aangifte of melding te doen zijn voorkomen dat de dader opnieuw slachtoffers maakt (56%) en een veiliger online omgeving creëren (47%). Twee op de vijf medewerkers die geen aangifte doen, geven aan dat ze geen of weinig schade ondervonden. Een vijfde (17%) vindt het (daarnaast) te veel moeite. Dertien procent zegt dat het geen zin heeft om aangifte of melding te doen, onder ICT-verantwoordelijken is dit zelfs een kwart.

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, bij diverse doelgroepen. 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 dit jaarlijks terugkerend bewustwordingsonderzoek waarmee de cybersecuritymaand jaarlijks in oktober wordt afgetrapt. In opdracht van het ministerie van Economische Zaken en Klimaat (EZK) voerde I&O Research een onderzoek uit naar de beleving van de digitale veiligheid onder Nederlanders.

Onderzoeksdoel

Het doel van dit onderzoek is het monitoren van het digitaal bewustzijn en cybervaardigheid van Nederlanders door de jaren heen. Aanvullend beoogt dit onderzoek om inzichten te vergaren in kennis, houding en gedrag van Nederlanders met betrekking tot online veiligheid en het bieden van aanknopingspunten voor beleidsvorming.

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 ICT-verantwoordelijken en medewerkers over online veiligheid en het verbeteren van de online veiligheid?
2 Wat vinden ICT-verantwoordelijken en medewerkers van hun eigen online gedrag als het gaat om veiligheid en vaardigheden?
3 Wat doen ICT-verantwoordelijken en medewerkers 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=142);
2 10 t/m 199 medewerkers (n=346);
3 200 of meer medewerkers (n=674).

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.

Hoofdstuk 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 1.162 medewerkers mee aan dit onderzoek en 330 ICT-verantwoordelijken. De respondenten zijn afkomstig uit het I&O Research Panel. Het online veldwerk vond plaats van 10 t/m 24 juli 2023. 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

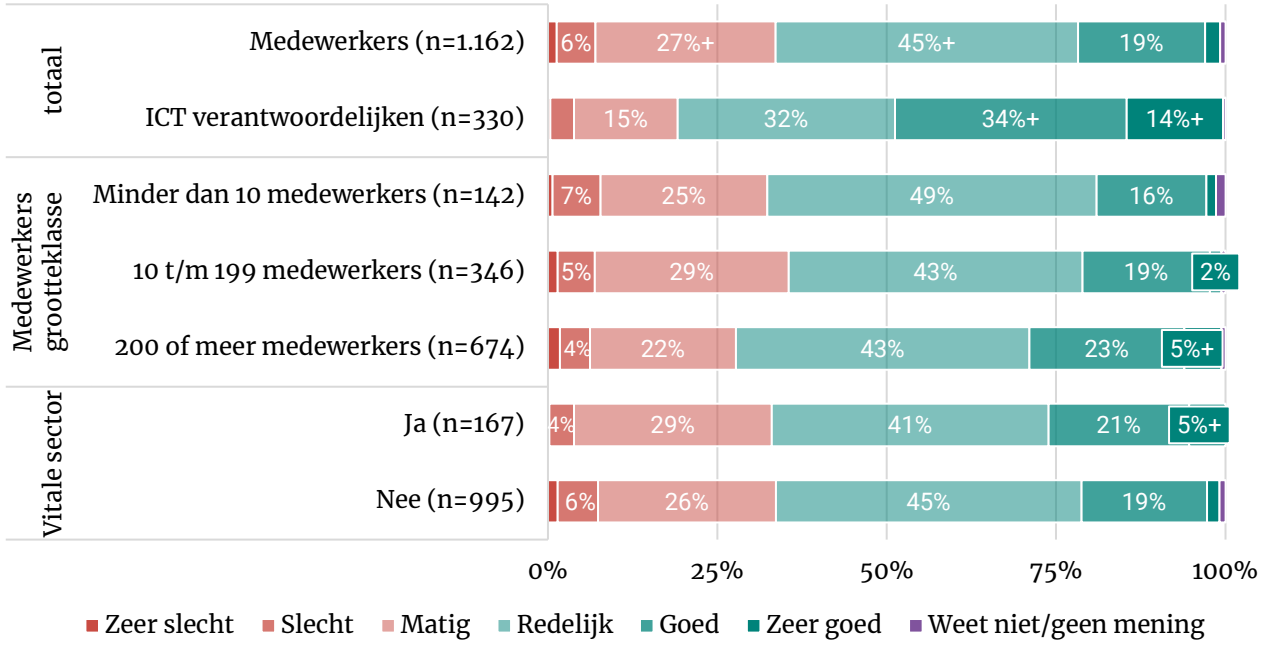
Een vijfde van medewerkers vindt eigen kennis over digitale veiligheid (zeer) goed

- Medewerkers schatten hun eigen kennis over online veiligheid lager in dan ICT-verantwoordelijken.
- De helft van de ICT-verantwoordelijken schatten hun kennis in als (zeer) goed.
- Personeel werkzaam in vitale sectoren beoordeelt zijn kennis beter dan medewerkers die niet in de vitale sectoren werkzaam zijn.

Vergelijking met 2022

- Medewerkers beoordelen hun kennis minder vaak (zeer) goed dan een jaar eerder.

Hoe schat u uw eigen kennis over digitale veiligheid in?



Significante verschillen tussen verschillende groepen en medewerkers zijn aangegeven met '+' (hoger) en '-' (lager).

Meeste vormen van cybercrime bij ruime meerderheid bekend

- Het overgrote deel van de medewerkers en de verschillende subgroepen hierbinnen heeft wel eens van de voorgelegde vormen van cybercrime gehoord.
- Alleen social engineering is 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 van cybercrime groter in.
- Het meest aannemelijk acht men met hacking, phishing en malware te maken te krijgen.
- Ook met ransomware denkt een ruime meerderheid (64%) van de ICT-verantwoordelijken te maken te kunnen krijgen in de werksituatie. Medewerkers schatten deze kans aanzienlijk kleiner in (36%).

Vergelijking met 2022

- zowel medewerkers als ICT-verantwoordelijken achten het vaker aannemelijk om met hacking, helpdeskfraude en QR-code fraude te maken te kunnen krijgen in de werksituatie.

In deze tabel staan 8 voorgelegde vormen van cybercrime	Kent de betekenis (naar eigen zeggen)		Denkt er in werksituatie mee te maken te kunnen krijgen*			
	Medewerkers (n=1.162)	ICT-verantwoordelijk (n=330)	Medewerkers		ICT-verantwoordelijk	
Hacking	95%	98%	59%+	n=878	73%+	n=323
Phishing	94% -	99%	52%	n=1.096	74%	n=325
Malware	73%	93%	41%	n=788	66%+	n=304
DDoS-aanval	74%	92%	37%	n=865	54%	n=296
Ransomware	65% -	93% +	36%	n=788	64%	n=298
Helpdeskfraude	75%	91%	22%+	n=901	40%+	n=289
QR-code fraude	58%	74%	14%+	n=686	26%+	n=232
Social engineering	27%	54%	10%	n=330	25%	n=163

Significante verschillen tussen medewerkers en ICT-verantwoordelijken zijn aangegeven met groen (hoger) en rood (lager).
Significante verschillen tussen 2023 en 2022 zijn aangegeven met '+' (toename) en '-' (afname).
*Alle begrippen voorgelegd waarvan men de betekenis zegt te kennen | percentage zeker + waarschijnlijk wel.

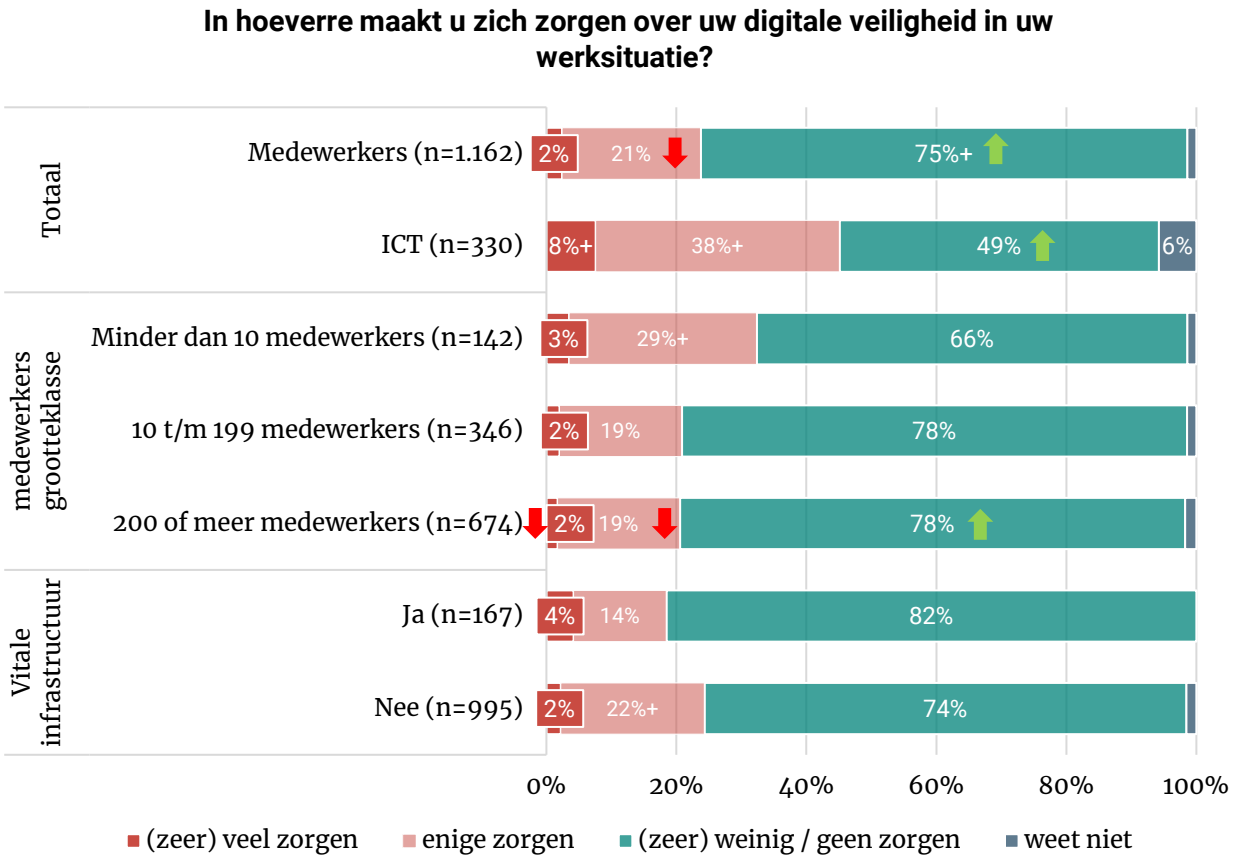
4. Zorgen en online gedrag op het werk

Driekwart medewerkers heeft geen of weinig zorgen over online veiligheid in werksituatie

- Bijna de helft van de ICT-verantwoordelijken (46%) maakt zich zorgen over de eigen online veiligheid. Voor medewerkers is dit percentage significant lager: 23 procent zegt zich (zeer) veel of enige zorgen te maken.

Vergelijking met 2022

- net als in het voorgaande jaar maakt men zich bij kleinere bedrijven (minder dan 10 medewerkers) vaker zorgen dan bij grotere bedrijven. Medewerkers in de vitale sectoren maken zich het minste zorgen (18%).



Significantie verschillen ten opzichte van 2022 zijn aangegeven met een ↓ (minder zorgen) of ↑ (meer zorgen). Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).

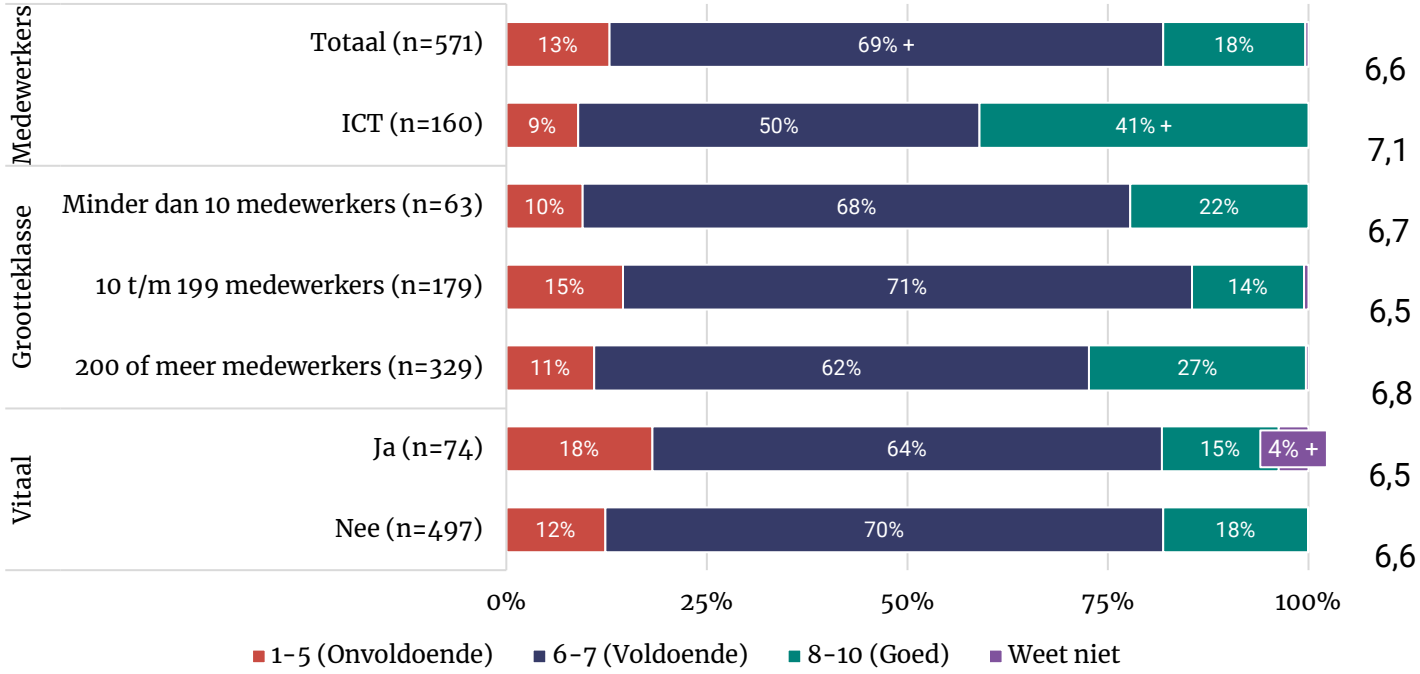
ICT-verantwoordelijken beoordelen eigen omgang met online risico's beter dan medewerkers

- Gemiddeld geven medewerkers zichzelf een 6,6 als het gaat om het omgaan met online risico's. Dat is lager dan de 7,1 die ICT-verantwoordelijken zichzelf geven. ICT-verantwoordelijken geven zichzelf vaker het cijfer 8 of hoger (41%).

Vergelijking met 2022

- Vorig jaar gaven medewerkers zichzelf minder vaak een 8 of hoger (2022: 27%).

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



Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager). Verschillen tussen de subgroepen zijn ook op deze wijze gemarkeerd.

Een vijfde van kleine bedrijven neemt geen acties om veilig online te zijn (1) (toelichting op volgende pagina)

Welke acties zijn er binnen uw bedrijf/organisatie ondernomen ten behoeve van online veilig gedrag?	ICT	Medewerkers				
	Totaal n=330	Totaal n=1.162	Minder dan 10 medewerkers (n=142)	10 t/m 199 medewerkers (n=346)	200 of meer medewerkers (n=674)	Vitaal (n=167)
Er is twee-staps-inloggen verplicht voor toegang	49%	32%	20%	34%	47%	32%
Alleen de systeembeheerders kunnen software installeren	33%	31%	18%	32%	49%	37%
Er zijn afspraken gemaakt over het versturen/uitwisselen van bestanden en/of persoonsgegevens	32%	21%	10%	22%	39%	29%
Er zijn afspraken gemaakt over het gebruik van zakelijke smartphones, laptops en/of tablets voor privé en/of zakelijk gebruik	29%	21%	9%	22%	35%	36%
Er is binnen mijn organisatie/bedrijf een digitale hulpverlener waar je terecht kunt	21%	20%	11%	21%	33%	30%
Er zijn regels over hoe je veilig online thuiswerkt	29%	20%	8%	19%	38%	24%
Er zijn adviezen/richtlijnen over hoe je veilig online thuiswerkt	32%	19%	8%	19%	39%	27%
Er zijn adviezen/richtlijnen over het gebruikmaken van websites/of e-mail	31%	19%	6%	20%	36%	36%
Er zijn regels over het gebruikmaken van websites/of e-mail	27%	17%	7%	17%	33%	27%
De toegang tot bepaalde websites en/of socialmediakanalen is geblokkeerd	21%	13%	5%	12%	33%	29%
Er worden op willekeurige momenten test-emails verstuurd om medewerkers te testen op herkenning van phishing	16%	12%	3%	12%	32%	20%
Er zijn regels over het gebruikmaken van sociale media	17%	12%	8%	10%	24%	20%
Er zijn adviezen/richtlijnen over het gebruikmaken van sociale media	18%	11%	6%	10%	27%	17%
Er zijn afspraken gemaakt over het gebruikmaken van opslagmedia als USB-sticks of externe harde schijven	22%	11%	4%	10%	26%	21%
Het gebruik van USB-sticks in onze organisatie is onmogelijk gemaakt	11%	8%	4%	7%	19%	16%
De toegang tot bepaalde verzendplatforms (zoals WeTransfer) is geblokkeerd	8%	5%	1%	3%	20%	12%
Er is een verzekering afgesloten tegen de financiële gevolgen van cybercrime	9%	3%	1%	3%	5%	7%
Anders	9%	3%	6%	3%	2%	4%
Weet ik niet	8%	30%	36%	31%	18%	16%
In mijn bedrijf of organisatie is geen enkele actie ondernomen ten behoeve van veilig online gedrag	12%	8%	19%	5%	1%	2%

Significantie verschillen (p<.05) tussen medewerkers (Totaal) en ICT-medewerkers zijn aangegeven met groen (hoger). Verschillen tussen de andere groepen zijn ook op deze wijze gemarkeerd.

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

- Twee-staps-inloggen is de meest genomen actie ten behoeve van online veilig gedrag bij bedrijven. De helft van de ICT-verantwoordelijken (49%) en medewerkers van grote bedrijven (47%) noemt dat deze maatregel wordt toepast.
- Ook een restrictie op de mogelijkheid om zelf software te kunnen installeren en dit alleen voor systeembeheerders mogelijk te maken is een veelgenoemde maatregel, met name in het grootbedrijf (49%).
- Het afsluiten van een verzekering tegen cybercrime komt daarentegen weinig voor.
- Drie op de tien medewerkers weten niet welke acties zijn of haar organisatie heeft genomen.
- Een op de vijf (19%) medewerkers van kleine bedrijven zegt dat geen enkele van de genoemde maatregelen genomen wordt.

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

- Vier op de vijf medewerkers vinden het gemakkelijk om zich aan de afspraken over online veilig gedrag te houden. Eenzelfde percentage vindt het goed wanneer men op het niet naleven hiervan aangesproken wordt.
- De helft van de medewerkers wordt aangesproken op het niet naleven van werkafspraken.
- Vier op de tien spreekt zelf collega's aan als zij zich niet aan de afspraken houden. Van de ICT-medewerkers doet twee derde dit.
- Volgens vier op de tien medewerkers geeft hun leidinggevende het goede voorbeeld.

In hoeverre bent u het eens of oneens met de volgende stellingen? % (zeer) eens. Voorgelegd aan personen waar afspraken zijn gemaakt.	ICT	Medewerkers				
	Totaal (n=249)	Totaal (n=828)	Minder dan 10 medewerkers (n=64)	10 t/m 199 medewerkers (n=221)	200 of meer medewerkers (n=543)	Vitaal n=146
Het is gemakkelijk om mij aan de afspraken te houden over online veilig gedrag binnen mijn bedrijf/organisatie	77%	80%	77%	79%	86%	79%
Ik vind het goed als collega's mij erop aanspreken als ik me niet houd aan de werkafspraken over online veilig gedrag.	77%	79%	73%	81%	80%	79%
Ik word er op mijn werk op aangesproken als ik me niet aan de werkafspraken houd over online veilig gedrag	53%	47%	44%	47%	51%	50%
Mijn leidinggevende geeft het goede voorbeeld als het gaat om online veilig gedrag	42%	43%	39%	44%	44%	49%
Ik spreek collega's er op aan als zij zich niet houden aan de werkafspraken over online veilig gedrag	63%	44%	45%	42%	46%	50%

Significantie verschillen (p<.05) tussen medewerkers (Totaal) en ICT-medewerkers zijn aangegeven met groen (hoger). Verschillen tussen de andere groepen zijn ook op deze wijze gemarkeerd.

Driekwart medewerkers vindt afspraken over veilig online gedrag duidelijk

- Driekwart (72%) van de medewerkers vindt de afspraken over veilig online gedrag duidelijk. Zeven op de tien zeggen toegang te hebben tot de juiste tools om veilig online te kunnen werken en zes op de tien vinden dat afspraken voldoende worden toegepast. De resultaten voor ICT-verantwoordelijken en medewerkers zijn vergelijkbaar.
- Medewerkers van het grootbedrijf ervaren vaker dat de afspraken binnen de organisatie goed worden toegepast. In kleine bedrijven heeft men naar verhouding minder toegang tot goede tools en instrumenten.

In hoeverre bent u het eens of oneens met de volgende stellingen? % (zeer) eens. Voorgelegd aan personen waar afspraken zijn gemaakt.	ICT	Medewerkers				
	Totaal n=249	Totaal n=828	Minder dan 10 medewerkers (n=64)	10 t/m 199 medewerkers (n=221)	200 of meer medewerkers (n=543)	Vitaal n=146
De afspraken over hoe ik me online veilig moet gedragen op mijn werk vind ik duidelijk	70%	72%	70%	70%	82%	72%
Ik krijg toegang tot goede tools en instrumenten (bijvoorbeeld twee-stapsverificatie of een wachtwoordmanager) om online veilig gedrag te bevorderen	73%	69%	58%	69%	76%	69%
De afspraken over online veilig gedrag die binnen mijn organisatie/bedrijf zijn gemaakt, worden voldoende toegepast	57%	62%	56%	61%	73%	61%

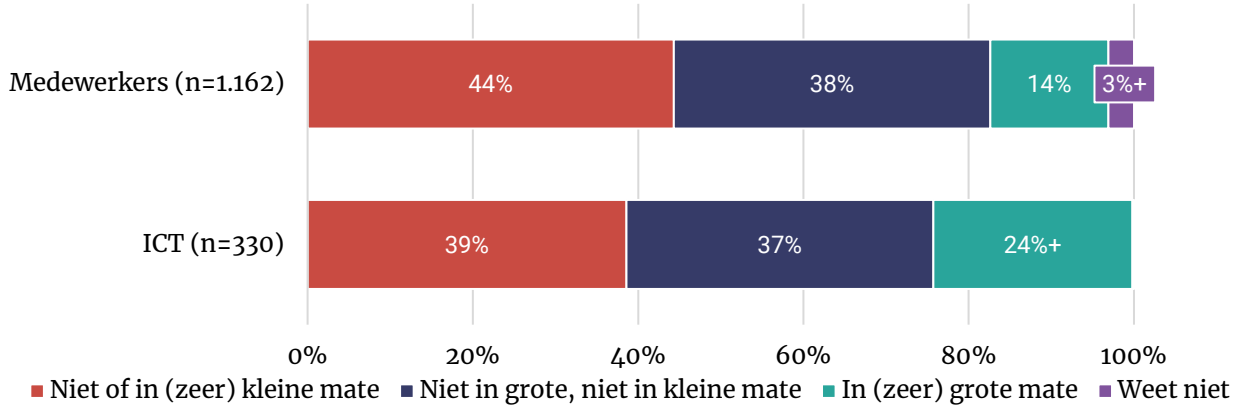
Significantie verschillen (p<.05) tussen medewerkers (Totaal) en ICT-medewerkers zijn aangegeven met groen (hoger) of rood (lager).
Verschillen tussen de andere groepen zijn ook op deze wijze gemarkeerd.

ICT-verantwoordelijken maken zich vaker zorgen over datalek

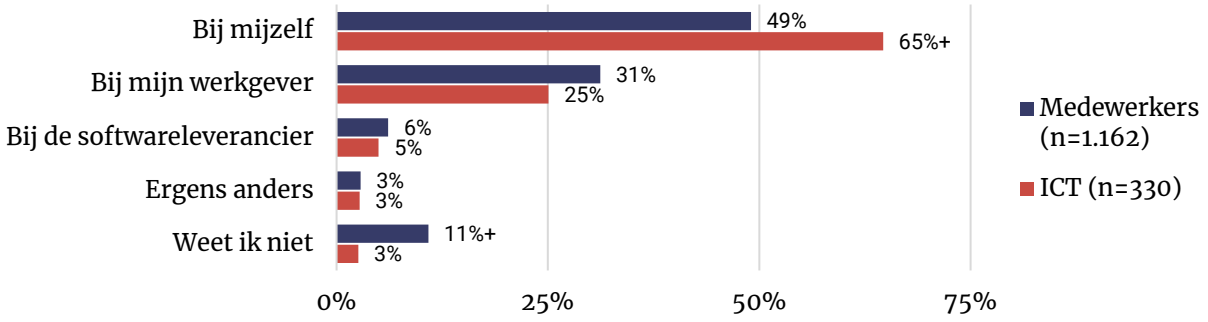
- Vier op de tien medewerkers maakt zich geen of in kleine mate zorgen om slachtoffer te worden van een datalek. Een vergelijkbaar deel antwoordt neutraal.
- ICT-verantwoordelijken maken zich vaker zorgen om slachtoffer te worden (24%) van een datalek dan medewerkers (14%).

- ICT-verantwoordelijken leggen de verantwoordelijkheid voor veilig online gedrag op het werk vaker dan medewerkers bij zichzelf.
- Eén op de tien medewerkers (11%) weet niet waar de verantwoordelijkheid zou moeten liggen. Onder ICT-verantwoordelijken is dit aandeel kleiner (3%).

In maart 2023 was er een datalek waarbij diverse Nederlandse bedrijven en daarmee miljoenen Nederlanders werden getroffen. De gegevens worden vermoedelijk gebruikt voor online oplichting. Doordat bijvoorbeeld een emailadres in combinatie met een naam beke



Bij wie zou wat u betreft de verantwoordelijkheid voor veilig online gedrag op het werk vooral moeten liggen?



Grote meerderheid vertelt het als ze per ongeluk een virus downloaden

- Acht op de tien medewerkers zouden het meteen aan anderen vertellen wanneer men een virus heeft gedownload, negen op de tien zouden het aan de ICT-afdeling vertellen.
- Zes op de tien medewerkers zeggen dat de werkgever back-ups maakt.
- Zes op de tien zouden zich schamen wanneer men op een phishinglink heeft geklikt.

Vergelijking 2022

- Medewerkers zeggen minder vaak (66%) dan een jaar eerder dat de werkgever back-ups van alle bestanden maakt (dit was driekwart).
- Ook ICT-verantwoordelijken geven minder vaak dan in 2022 aan dat de werkgever dit doet.

In hoeverre zijn de volgende uitspraken van toepassing op uw gedrag? % meestal wel + altijd (exclusief 'niet van toepassing')	Medewerkers (n=1.162)	ICT-verantwoordelijk (n=330)
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	91%	96%
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 anderen wat ik heb gedaan	83% -	92%
Als ik een openbare computer heb gebruikt dan log ik na gebruik al mijn accounts uit (bank, social media en e-mail)	83%	85%
Mijn werkgever maakt automatisch back-ups van alle bestanden (volledige back-ups)	66% -	77% -
Ik heb de privacy instellingen van mijn social media accounts aangepast ten opzichte van de standaardinstellingen	62% -	69%
Ik let op of er een slotje en/of https bij het webadres staat	62% -	80% +
Als ik op een link in een phishing e-mail zou klikken dan zou ik mij daarvoor schamen	56% -	54%
Ik maak thuis regelmatig back-ups van mijn bestanden	48%	65%
Ik maak op mijn werk regelmatig back-ups van de bestanden op mijn werklaptop	39%	68%
Ik maak thuis gebruik van een extern opslagapparaat dat continu online is	16%	28%
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 uit schaamte niet aan anderen wat ik heb gedaan	12%	7% -
Ik verstuur werkbestanden van mijn werk e-mailadres naar mijn privé e-mail	7% -	9%
Als ik getroffen zou worden door ransomware en gevraagd wordt om te betalen om weer toegang tot mijn persoonlijke bestanden te krijgen, dan zou ik daarvoor betalen	4%	6% +

Significantie verschillen (p<.05) tussen medewerkers (Totaal) en ICT-medewerkers zijn aangegeven met groen (hoger). Verschillen tussen de andere groepen zijn ook op deze wijze gemarkeerd. Verschillen met 2022 zijn met '+' en '-' aangegeven.

Meerderheid gebruikt bij thuiswerken wifinetwerk met wachtwoord

- De meeste medewerkers maken bij het thuiswerken gebruik van Wifi met een wachtwoord (85%).
- 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.
- Kleine letters, hoofdletters en cijfers worden in vier op de vijf van de zelfverzonnen wachtwoorden gebruikt. Ongeveer de helft gebruikt leestekens en speciale tekens. Een derde (35%) heeft een wachtwoord van 12 tekens of langer.

Van wat voor netwerkverbinding maakt u thuis gebruik? Voorgelegd aan medewerkers die weleens thuis werken	**Totaal**		**Medewerkers grootteklasse**			**Vitale infrastructuur**	
	Medewerkers (n=544)	ICT (n=254)	Minder dan 10 medewerkers (n=78)	10 t/m 199 medewerkers (n=139)	200 of meer medewerkers (n=327)	Ja (n=92)	Nee (n=452)
Een wifi-netwerkverbinding met wachtwoord	85%	89%	86%	85%	83%	71%	86%
Een VPN verbinding	32%	38%	22%	33%	49%	61%	29%
Via een internetkabel (niet draadloos; LAN)	22%	37%	22%	21%	26%	13%	23%
Een hotspot verbinding (3G/4G/5G) via mijn smartphone of tablet	10%	13%	12%	10%	9%	8%	11%
Een wifi-netwerkverbinding zonder wachtwoord (bv openbaar (wifi-)netwerk)	0%	2%	1%	0%	1%	0%	1%

Significantie verschillen (p<.05) tussen medewerkers (Totaal) en ICT-medewerkers zijn aangegeven met groen(hoger). Verschillen tussen de andere groepen en het totaal zijn ook op deze wijze gemarkeerd.

5. Slachtofferschap en aangiftebereidheid

Phishing komt vaakst voor in de werksituatie

- Een vijfde (21%) van de medewerkers heeft de afgelopen 12 maanden een phishingmail op het werk ontvangen.
- Onder ICT-verantwoordelijken is dit aandeel hoger (50%).
- ICT-verantwoordelijken hebben vaker te maken met cybercrime dan andere medewerkers.
- Driekwart van de medewerkers zegt met geen van de voorgelegde voorvallen te maken gehad te hebben in de afgelopen 12 maanden.

Vergelijking met 2022

- Een aantal zaken maakten meer mensen mee dan een jaar eerder. Zo hadden meer ICT-verantwoordelijken te maken met phishing.

Heeft u in de afgelopen 12 maanden zelf weleens te maken gehad met een van de onderstaande voorvallen in uw werksituatie?	ICT	Medewerkers			
	Totaal (n=330)	Totaal (n=1.162)	Minder dan 10 medewerkers (n=142)	10 t/m 199 medewerkers (n=346)	200 of meer medewerkers (n=674)	Vitaal (n=167)
Mails ontvangen met poging tot phishing	50% +	21%	28%	17%	24%	24%
Acquisitiefraude	10%	4%	8%	2%	0,9%	4%
Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik die bijna niet van echt te onderscheiden is	10%	3%	7% +	1%	3% +	4%
Gebeld door iemand die zich voordeed als bedrijf of officiële instantie om geld of gegevens te bemachtigen	9%	3% -	5%	2%	2%	2%
Benaderd op social media met een vraag om een onbekende link aan te klikken	7%	3%	7%	2%	2%	3%
Dat iemand dreigde mijn bestanden te openbaren of dit ook echt deed	3%	1% -	2%	1%	0,6%	0,0%
Benaderd via WhatsApp door iemand die zich voordeed als een bekende die probeerde geld te ontvangen	3%	3%	3%	3%	2%	0,4%
Dat iemand in een apparaat heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	2%	0,2%	0,0%	0,3%	0,0%	0,0%
Ransomware	2%	0,4%	0,7%	0,3%	0,3%	0,0%
Dat iemand in een account heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	2%	0,7%	2%	0,3%	0,1%	0,0%
Identiteitsdiefstal	1,1%	0,2%	0,7%	0,0%	0,1%	0,0%
Een foute link ook daadwerkelijk hebben aangeklikt in de zin dat deze een virus, spam, phishing of andere ongewenste poging tot cybercrime bevatte	1,0%	0,9%	0,0%	1%	1%	0,2%
Dat een computer tijdelijk niet werkte door malware zoals bijvoorbeeld een virus	0,8%	1,0%	1%	0,9%	1% +	0,0%
Dat door het downloaden van geïnfecteerde software/bestanden malware verspreid werd (o.a. via een e-mail)	0,3%	0,8%	1%	0,9%	0,6% +	0,0%
Geen van deze voorvallen	44%	74%	66%	78%	72%	71%

Meest melding bij ICT-afdeling en Fraudehelpdesk

- ICT-verantwoordelijken doen wanneer zij een voorval van cybercrime meemaken vaker dan medewerkers aangifte of melding bij de politie. Medewerkers doen hun melding van cybercrime juist vaker bij de ICT-afdeling van hun bedrijf (34%). Bij grotere bedrijven met meer dan 200 medewerkers doen zes op de tien medewerkers dit.
- De meerderheid van zowel ICT-verantwoordelijken (56%) als medewerkers (59%) onderneemt geen actie nadat men te maken kreeg met cybercrime in de werksituatie.
- Medewerkers van kleine bedrijven ondernemen het minst vaak actie (35%), dit percentage is vanwege het lage aantal waarnemingen indicatief.
- ICT-verantwoordelijken doen vaker dan medewerkers aangifte bij de politie.

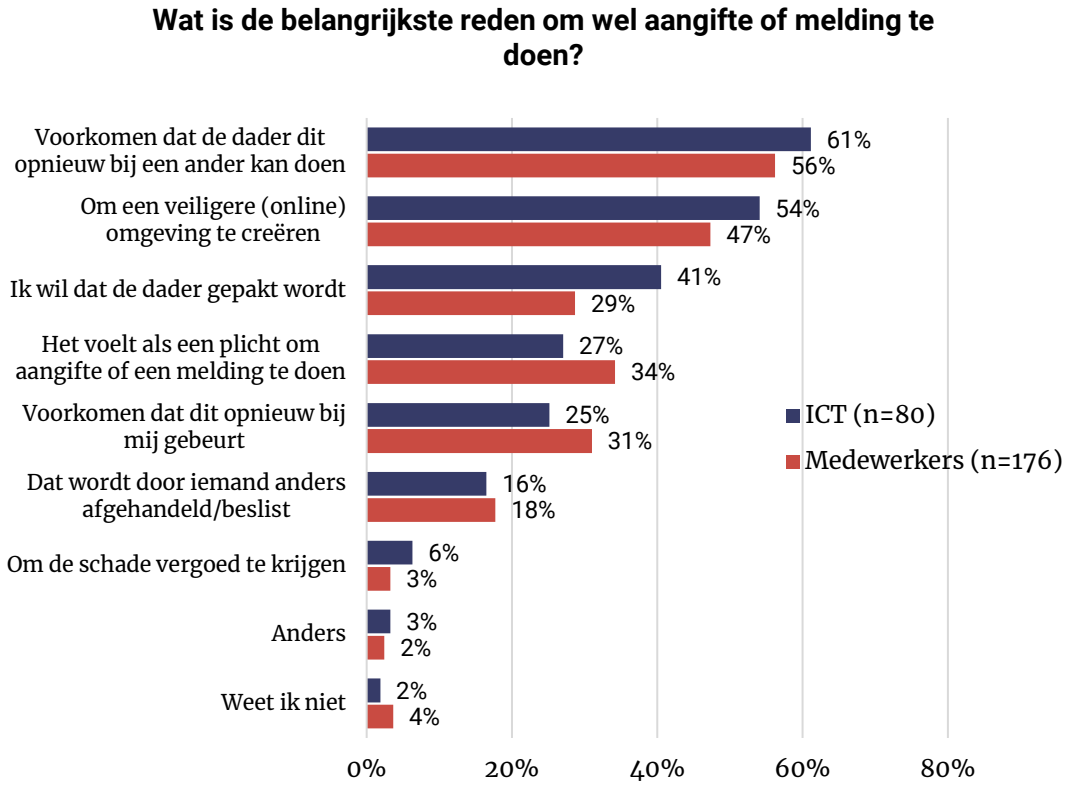
Vergelijking met 2022
Medewerkers doen in 2023 vaker aangifte bij de politie als ze cybercrime meemaken.

U geeft aan dat u zelf in uw werksituatie te maken heeft gehad met een of meerdere voorvallen van cybercrime. Heeft u toen een aangifte of melding gedaan? (gesteld aan iedereen die in de werksituatie een geval van cybercrime meemaakte)	**ICT**	**Medewerkers**				
	Totaal n=191	Totaal n=312	Minder dan 10 medewerkers (n=48)*	10 t/m 199 medewerkers (n=77)	200 of meer medewerkers (n=187)	Vitaal (n=53)
Aangifte bij de politie	6% +	3% +	4%	3%	4%	1%
Melding bij de politie	6%	2%	4%	0%	3%	0%
Melding bij Fraudehelpdesk	11%	8%	15%	5% -	5%	4%
Melding bij de gemeente	2%	0%	0%	0%	1%	0%
Melding bij SeniorWeb	1%	1%	2%	0%	0%	0%
Melding bij de ICT-afdeling van mijn bedrijf	26%	34%	21% +	34%	61%	53% +
Melding bij het Nationaal Cyber Security Centrum (NCSC)	0%	2%	2%	1%	2%	2%
Bij een andere organisatie	7%	2% -	4%	0%	2%	0%
Nee, ik heb hier niks mee gedaan	56%	59%	65% -	64%	30%	46%

Significante verschillen tussen medewerkers en ICT-verantwoordelijken zijn aangegeven met groen (hoger) en rood (lager).
Significante verschillen tussen 2022 en 2021 zijn aangegeven met '+' (toename) en '-' (afname).
*Laag aantal waarnemingen. Indicatieve uitkomsten.

Veiliger omgeving en voorkomen herhaling belangrijkste redenen voor melding of aangifte

- Zes op de tien medewerkers willen met de melding of aangifte voorkomen dat de dader andere slachtoffers kan maken. Ook wil meer dan de helft een veiligere online omgeving creëren.
- De minst belangrijke reden om melding of aangifte te doen is om de schade vergoed te krijgen.



Kwart 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.
- Ook vindt men het te veel moeite of denkt men dat het geen zin heeft.
- Een op de tien heeft weinig vertrouwen in instanties waar men aangifte of melding kan doen.

Wat zijn de belangrijkste redenen om geen aangifte of melding te doen? (maximaal 3)	Medewerkers (n=136)	ICT-verantwoordelijken (n=111)
Ik ondervond geen of weinig schade	41%	47%
Het kost te veel moeite	17%	15%
Het heeft geen zin, er wordt niets gedaan met de aangifte of melding	13%	25%
Ik los het zelf op	12%	13%
Het is niet zo belangrijk	12%	13%
Dat wordt door iemand anders afgehandeld/beslist	12%	10%
Ik heb weinig vertrouwen in de instanties om aangifte of een melding te doen	11%	10%
Ik weet niet bij welke instantie ik moet zijn voor het oplossen van dit type delict	7%	5%
Er is niet de kennis om dit type delict aan te pakken	2%	3%
Ik vind dat het eigenlijk mijn eigen schuld is	1%	0%
Ik wilde aangifte doen maar dit werd mij afgeraden	1%	0%
Ik ben bang dat de dader wraak zal nemen	0%	0%
Ik ondervond geen of weinig schade	0%	0%
Ik schaam me dat ik slachtoffer ben geworden van het delict	0%	0%
Anders	13%	11%
Weet ik niet	7%	9%

Significante verschillen tussen medewerkers en ICT-verantwoordelijken zijn aangegeven met groen.

Contactgegevens

I&O Research Enschede
Zuiderval 70
Postbus 563
7500 AN Enschede
053 - 200 52 00
KVK-nummer 08198802
info@ioresearch.nl
www.ioresearch.nl

I&O Research Amsterdam
Piet Heinkade 55
1019 GM Amsterdam
020 – 308 48 00
info@ioresearch.nl
www.ioresearch.nl