Cybersecurity onderzoek Alert Online 2022

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
2022/207

Datum
september 2022

Opdrachtgever
Ministerie van Economische Zaken en Klimaat

Auteurs
Melle Conradie
Bram Doms

Inhoudsopgave

1. Managementsamenvatting

Samenvatting | 1/2

Kennisniveau van medewerkers en ICT-verantwoordelijken is vergelijkbaar met 2021
Net als in 2021 schatten ongeveer drie op de tien medewerkers hun kennis over online veiligheid in als (zeer) goed (27%). ICT-verantwoordelijken (43%) en medewerkers in de vitale infrastructuur (40%) schatten hun kennis hoger in dan andere werknemers. Toch schat een vijfde van de ICT-verantwoordelijken zijn kennis als matig (15%) tot (zeer) slecht (5%) in. ICT-verantwoordelijken bij kleine bedrijven schatten hun kennis gemiddeld lager in dan ICT-verantwoordelijken die bij grotere bedrijven werken.

Medewerkers schatten het risico dat zij te maken krijgen met cybercrime lager in dan ICT-verantwoordelijken
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 significant groter. Ook alle andere voorgelegde vormen van cybercrime worden door ICT-verantwoordelijken aannemelijker geacht dan door andere medewerkers.

Meerderheid ICT-verantwoordelijken heeft zorgen over online veiligheid
Ruim de helft van de ICT-verantwoordelijken (54%) maakt zich zorgen over de eigen online veiligheid. Voor medewerkers is dit percentage significant lager. Wel geven ICT-verantwoordelijken zichzelf een hoger cijfer als het gaat om het omgaan met online risico's (7,1; medewerkers totaal 6,9).

Kwart van kleine bedrijven onderneemt geen actie om veilig online te zijn
Adviezen/richtlijnen over het gebruikmaken van websites of e-mail zijn de meest genomen acties bij bedrijven. Grote bedrijven en bedrijven in vitale sectoren ondernemen significant vaker dan gemiddeld acties ten behoeve van online veilig gedrag. Kleine bedrijven ondernemen minder acties, bovendien onderneemt een kwart van deze bedrijven (24%) geen enkele actie ten behoeve van veilig online gedrag (totaal 8%).

In bedrijven waar afspraken zijn gemaakt over veilig online gedrag, vinden vier op de vijf medewerkers het gemakkelijk om zich aan die afspraken te houden. Beloningen voor het vertonen van het juiste online gedrag worden door een vijfde ondersteund, voor het opleggen van sancties is meer steun: twee derde is hiervoor.

Samenvatting | 2/2

Medewerkers werken in 2022 weer vaker op kantoor

Er werd door medewerkers afgelopen jaar vaker op kantoor gewerkt. In het onderzoek van 2021 werkte 61 procent op kantoor, in 2022 is dit percentage 86 procent. Het aandeel medewerkers en ICT'ers dat thuiswerkt is gelijk gebleven. Onder medewerkers die thuiswerken gebruikt 85 procent een wifiverbinding met wachtwoord.

Phishing komt het vaakst voor in de werksituatie

Een op de vijf medewerkers ontving in de afgelopen 12 maanden op het werk een phishingmail. Gebeld worden om geld of gegevens te bemachtigen staat op de tweede plaats. ICT'ers hebben vaker te maken met alle voorgelegde vormen van cybercrime dan andere medewerkers.

Meerderheid onderneemt geen actie op cybercrime

Ruim de helft van de medewerkers die te maken kregen met cybercrime (56%) deed 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 (29%). De belangrijkste redenen om aangifte of melding te doen zijn een veiliger online omgeving creëren (59%) en voorkomen dat de dader opnieuw slachtoffers maakt (57%). ICT-verantwoordelijken willen naar verhouding vaak dat de dader gepakt wordt.
Een kwart van degenen die geen aangifte doet, geeft aan dat ze denken dat dit geen zin heeft. Een vijfde vindt het (daarnaast) te veel moeite en ook een vijfde vindt het niet zo belangrijk. ICT-verantwoordelijken noemen relatief vaak dat ze weinig vertrouwen hebben in de instanties die de melding of aangifte op moeten pakken.

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 cyber secure 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 een 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 de cyber awareness en cyberskills 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 met betrekking tot dit thema.

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?**

Deze hoofdvraag bestaat uit 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?

Dit deelrapport richt zich specifiek op de doelgroep werknemers in het bedrijfsleven.

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=123);
2 10 t/m 199 medewerkers (n=374);
3 200 of meer medewerkers (n=669).

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.

Verantwoording

In totaal deden 1.166 medewerkers mee aan dit onderzoek en 382 ICT-verantwoordelijken. De respondenten zijn afkomstig uit het I&O Research Panel. Het online veldwerk vondplaats van 11 t/m 25 juli 2022. De resultaten zijn gewogen naar bedrijfsgrootte. Daarmee zijn de resultaten representatief voor dit kenmerk.

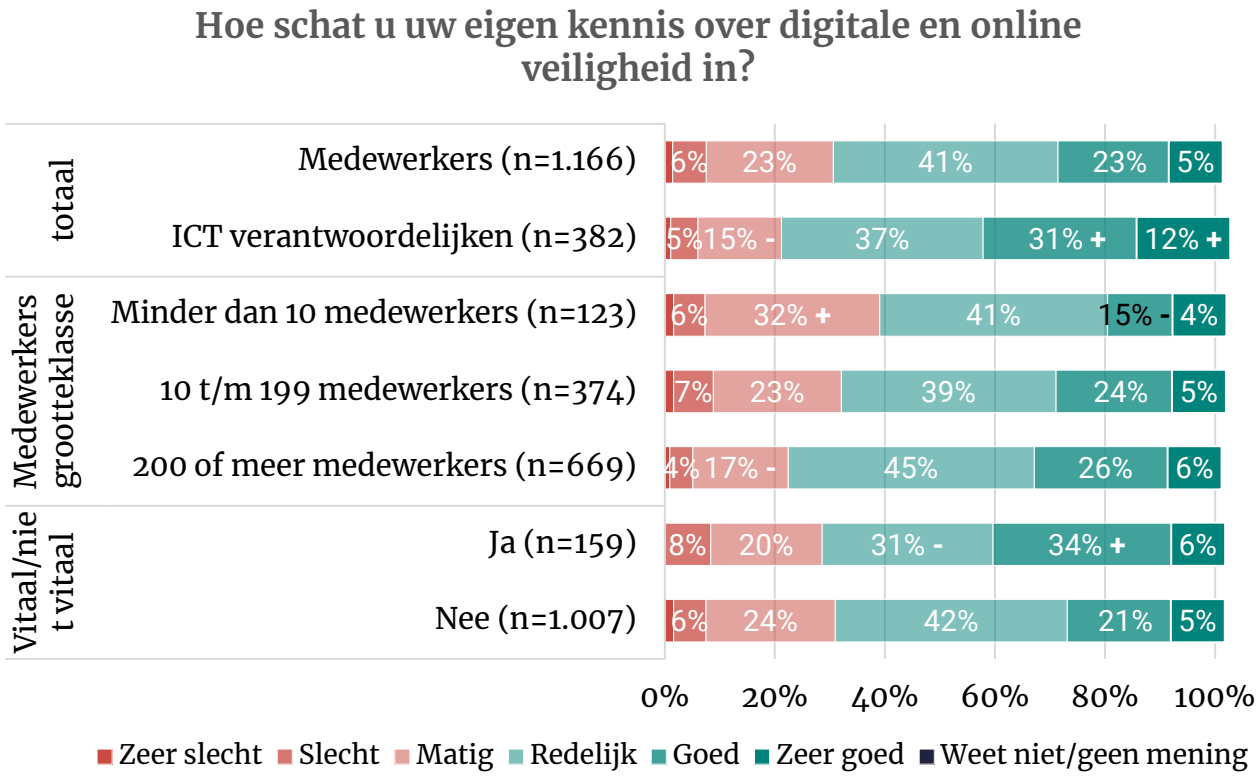
---

[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

Zeven op de tien medewerkers vinden eigen kennis over online veiligheid redelijk tot zeer goed

- Medewerkers schatten hun eigen kennis over online veiligheid lager in dan ICT-verantwoordelijken. Een derde van de medewerkers schat de eigen kennis in als (zeer) slecht tot matig. Voor ICT-verantwoordelijken geldt dit voor een vijfde.
- Naarmate de bedrijven waar zij werken meer werknemers hebben, vinden werknemers dat ze beter op de hoogte zijn.
- Personeel werkzaam in vitale sectoren beoordeelt zijn kennis beter dan andere medewerkers.
- Zzp'ers beoordelen hun kennis vaker als matig dan ICT-verantwoordelijken bij grote bedrijven.



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

ICT-medewerkers denken vaker te maken te krijgen met cybercrime

- ICT-verantwoordelijken kennen de verschillende vormen van cybercrime beter dan medewerkers. Ook schatten ze de kans om ermee te maken te krijgen meestal hoger in.
- Van de meeste vormen denken minder werkenden last te kunnen hebben dan in 2021. Alleen van hacking denken nu meer medewerkers ermee te maken te kunnen krijgen.
- ICT-verantwoordelijken bij kleinere bedrijven en zzp'ers verwachten minder vaak dan andere ICT'ers te maken te krijgen met helpdeskfraude.

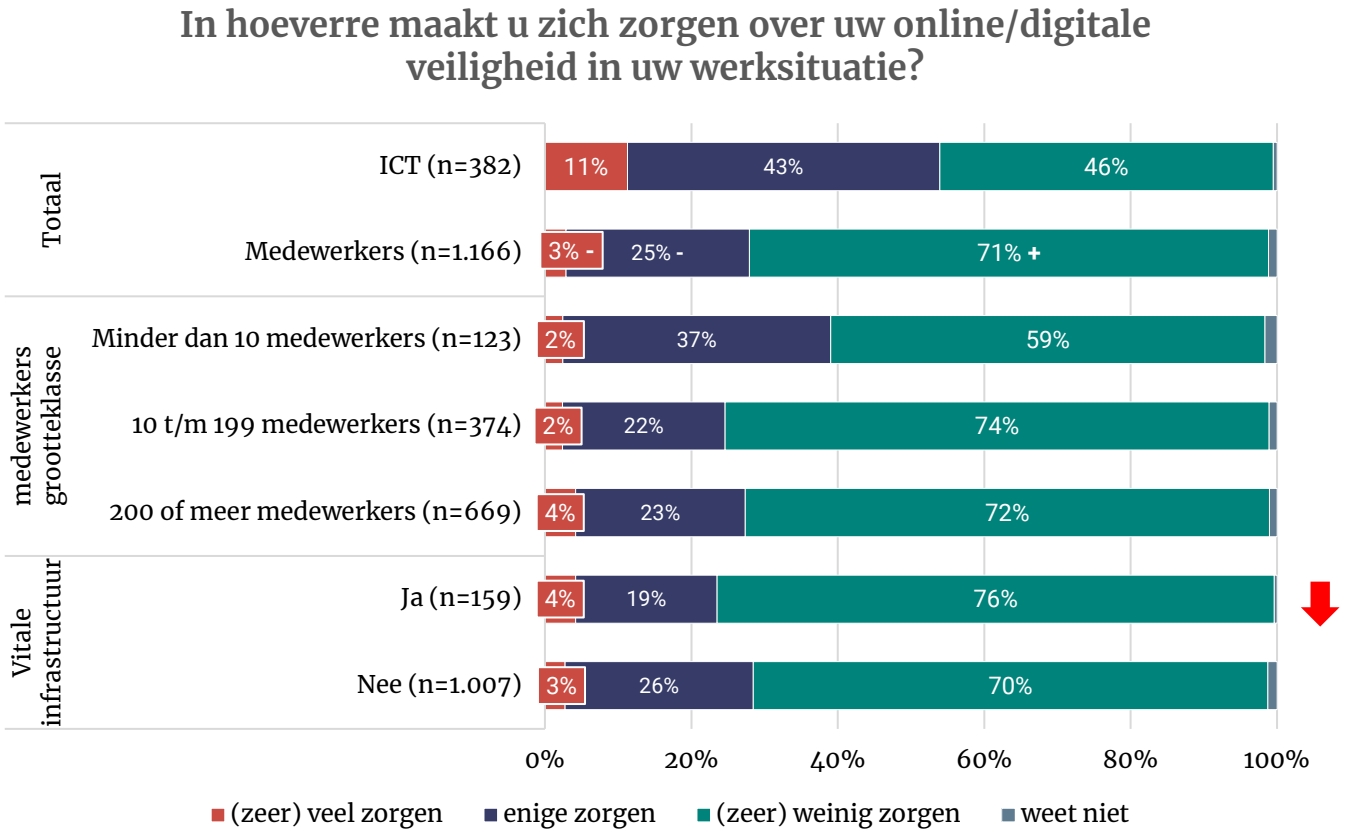
In deze tabel staan 11 voorgelegde vormen van cybercriminaliteit, op volgorde van bekendheid	Kent de betekenis (naar eigen zeggen)		Denkt er in werksituatie mee te maken te kunnen krijgen*			
	Medewerkers (n=1.158)	ICT-verantwoordelijk (n=381)	Medewerkers		ICT-verantwoordelijk	
Hacking	96%	97%	52% +	n=1.123	62%	n=371
Phishing	95%	98%	51%	n=1.113	67%	n=373
Identiteitsfraude	95%	97%	19% -	n=1.116	36% -	n=370
Vriend-in-nood-fraude (ook wel WhatsApp fraude)	92%	96%	9% -	n=1.081	18%	n=365
Bankhelpdeskfraude	87% +	95% +	13%	n=1.017	23% -	n=362
Helpdeskfraude	78% +	90% +	18% -	n=921	30% -	n=344
Malware	76%	90%	41%	n=912	56% -	n=344
DDoS-aanval	73%	89%	37% -	n=885	43% -	n=339
Ransomware	69%	88%	38% -	n=837	55% -	n=336
QR-code fraude	60%	74%	10% -	n=710	20% -	n=283
Social engineering	30% +	48%	8% -	n=365	18% -	n=182

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).
*Alle begrippen voorgelegd waarvan men de betekenis zegt te kennen | percentage zeker + waarschijnlijk wel.

4. Zorgen en online gedrag op het werk

Meerderheid ICT-verantwoordelijken heeft zorgen over online veiligheid

- Ruim de helft van de ICT-verantwoordelijken (54%) maakt zich zorgen over de eigen online veiligheid. Voor medewerkers is dit percentage significant lager: onder deze groep zegt 28 procent zich (zeer) veel of enige zorgen te maken.
- Bij kleinere bedrijven (minder dan 10 werknemers) maakt men zich vaker zorgen dan in grotere bedrijven. Dit geldt ook voor zzp'ers. De groep die eerder aangaf minder kennis te hebben, voelt zich dus vaker onveilig.
- Medewerkers in de vitale sectoren maken zich significant minder vaak zorgen ten opzichte van 2021 (76%, 2021: 63%).

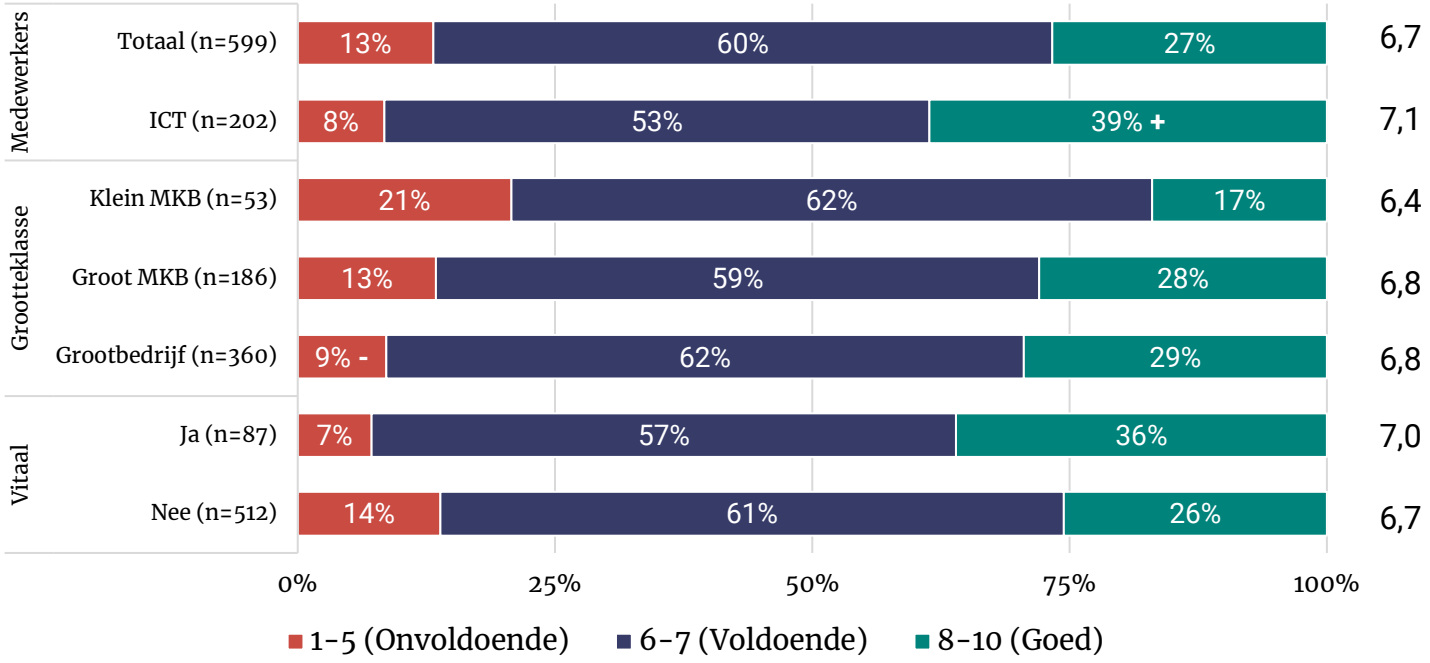


Significantie verschillen ten opzichte van 2021 zijn aangegeven met een ↓ (minder zorgen).
Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en –(lager).

ICT-verantwoordelijken geven hogere cijfers voor eigen omgang met online risico's

- Gemiddeld geven medewerkers zichzelf een 6,7 als het gaat om het omgaan met online risico's. Dat is lager dan de 7,1 die ICT-verantwoordelijken zichzelf geven. Zij kiezen vaker voor een 8 of hoger.
- Medewerkers van het grootbedrijf geven zich naar verhouding minder vaak een onvoldoende.
- Zzp'ers geven zichzelf in vergelijking met andere ICT-verantwoordelijken vaker een 6 of een 7 in plaats van een 8 of hoger.
- De uitkomsten verschillen niet met de cijfers van 2021.

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



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

Bij kwart kleine bedrijven geen acties om veilig online te zijn

- Acht procent van alle bedrijven neemt geen enkele actie ten behoeve van online veilig gedrag. Bij kleine bedrijven is dat zelfs 24 procent.
- Adviezen/richtlijnen over het gebruikmaken van websites of e-mail zijn de meest genomen acties.
- Grote bedrijven en bedrijven in vitale sectoren ondernemen significant vaker dan gemiddeld acties ten behoeve van online veilig gedrag. Kleine bedrijven ondernemen minder acties.

Welke acties zijn er binnen uw bedrijf/organisatie ondernomen ten behoeve van online veilig gedrag?	ICT	Medewerkers				
	Totaal n=382	Totaal n=1.166	Klein MKB n=123	Groot MKB n=374	Grootbedrijf n=669	Vitaal n=159
Adviezen/richtlijnen over het gebruikmaken van websites/of e-mail	37%	39%	21%	37%	55%	50%
Afspraken over het versturen/uitwisselen van bestanden en/of persoonsgegevens	36%	30%	15%	25%	48%	50%
Regels over het gebruikmaken van websites/of e-mail	34%	36%	19%	32%	54%	55%
Twee-factorauthenticatie verplicht voor toegang	32%	31%	16%	28%	46%	37%
Alleen systeembeheerders kunnen software installeren	30%	40%	20%	41%	53%	49%
Regels over hoe je veilig online thuiswerkt	28%	28%	11%	25%	47%	41%
Afspraken over het gebruik van zakelijke smartphones, laptops en/of tablets voor privé en/of zakelijk gebruik	28%	28%	14%	25%	45%	45%
Afspraken over het gebruikmaken van opslagmedia als usb-sticks of externe harde schijven	25%	21%	12%	16%	37%	40%
Adviezen/richtlijnen over hoe je veilig online thuiswerkt	24%	26%	11%	25%	39%	39%
Regels over het gebruikmaken van sociale media	22%	18%	12%	14%	30%	31%
Adviezen/richtlijnen over het gebruikmaken van sociale media	21%	18%	11%	14%	30%	23%
Toegang tot bepaalde websites en/of sociale media kanalen is geblokkeerd	18%	21%	9%	16%	42%	41%
Toegang tot bepaalde verzendplatforms (zoals WeTransfer) is geblokkeerd	12%	9%	4%	5%	21%	20%
Het gebruik van USB-sticks in onze organisatie is onmogelijk gemaakt	8%	10%	4%	7%	19%	16%
Er is een verzekering afgesloten tegen de financiële gevolgen van cybercrime	7%	6%	3%	7%	6%	13%
Anders	13%	3%	6%	2%	3%	4%
Weet ik niet	10%	22%	28%	23%	16%	14%
Geen enkele actie ondernomen ten behoeve van veilig online gedrag	15%	8%	24%	6%	1%	3%

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

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 met betrekking tot online veilig gedrag te houden. Eenzelfde percentage vindt het goed wanneer men op het niet naleven hiervan aangesproken wordt door collega's.
- De helft zegt ook daadwerkelijk aangesproken te worden als ze zich niet aan de afspraken houden. ICT-verantwoordelijken spreken collega's vaker aan op werkafspraken over online veilig gedrag dan andere medewerkers. Tegelijkertijd willen minder ICT-verantwoordelijken daar zelf op aangesproken worden.

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=287	Totaal n=886	Klein MKB n=60	Groot MKB n=267	Groot-bedrijf n=559	Vitaal n=138
Het is gemakkelijk om mij aan de afspraken te houden over online veilig gedrag binnen mijn bedrijf/organisatie	75%	80%	78%	77%	86%	81%
Ik vind het goed als collega's mij erop aanspreken als ik me niet houd aan de werkafspraken over online veilig gedrag	72%	80%	67%	81%	84%	84%
Ik word er op mijn werk op aangesproken als ik me niet aan de werkafspraken houd over online veilig gedrag	49%	47%	40%	46%	52%	50%
Ik spreek collega's er op aan als zij zich niet houden aan de werkafspraken over online veilig gedrag	58%	44%	33%	46%	43%	48%
Mijn leidinggevende geeft het goede voorbeeld als het gaat om online veilig gedrag	43%	43%	35%	45%	45%	46%

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

Driekwart medewerkers vindt afspraken over veilig online gedrag duidelijk

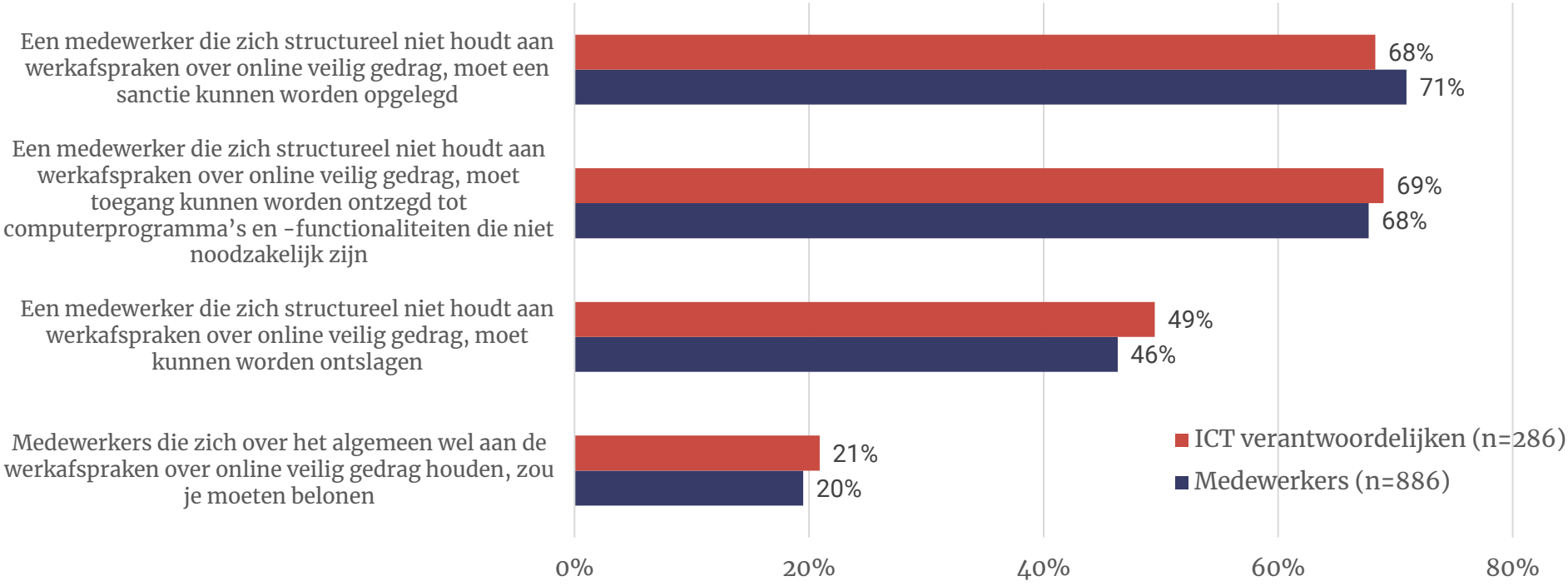
- Driekwart (73%) van de medewerkers vindt de afspraken over veilig online gedrag duidelijk. Twee derde zegt toegang te hebben tot de juiste tools om veilig online te kunnen werken en vindt dat afspraken voldoende worden toegepast. De resultaten voor ICT-verantwoordelijken en medewerkers zijn vergelijkbaar.
- Medewerkers van het grootbedrijf zijn het vaker eens met alle stellingen. 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=287	Totaal n=886	Klein MKB n=60	Groot MKB n=267	Groot-bedrijf n=559	Vitaal n=138
De afspraken over hoe ik me online veilig moet gedragen op mijn werk vind ik duidelijk	69%	73%	62%	71%	81%	76%
Ik krijg toegang tot goede tools en instrumenten (bijvoorbeeld twee-stapsverificatie of een wachtwoordmanager) om online veilig gedrag te bevorderen	65%	67%	48%	65%	77%	68%
De afspraken over online veilig gedrag die binnen mijn organisatie/bedrijf zijn gemaakt, worden voldoende toegepast	63%	61%	58%	57%	69%	68%

Ruime meerderheid voor sancties bij niet naleven werkafspraken

- Zeven op de tien medewerkers vinden dat sancties opgelegd moeten kunnen worden als men zich structureel niet aan werkafspraken houdt.
- Werkenden zijn minder vaak voor een beloning voor medewerkers die zich juist goed aan deze afspraken houden.
- Er zijn geen significante verschillen tussen wat medewerkers en ICT-verantwoordelijken vinden.

In hoeverre bent u het eens of oneens met de volgende stellingen?
% (zeer) eens. Voorgelegd aan personen waar afspraken zijn gemaakt



Zes op de tien zouden zich schamen na klikken op phishinglink, maar meerderheid vertelt wel als ze virus downloaden

- Werkgevers maken vaak automatische back-ups van alle bestanden, driekwart van de medewerkers zegt dat hun werkgever dit doet. Voor ICT-verantwoordelijken ligt dit percentage op 90 procent.
- Negen op de tien zouden het meteen aan anderen vertellen wanneer men een virus heeft gedownload.
- Zes op de tien zouden zich schamen wanneer men op een phishinglink heeft geklikt.
- ICT-verantwoordelijken maken vaker back-ups op hun werklaptop of thuis dan andere medewerkers.

In hoeverre zijn de volgende uitspraken van toepassing op uw gedrag? % meestal wel + altijd (exclusief 'niet van toepassing')	Medewerkers (n=1.166)	ICT-verantwoordelijk (n=382)
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	91%	89%
Als ik een openbare computer heb gebruikt dan log ik na gebruik al mijn accounts uit (bank, social media en e-mail)	84%	81%
Mijn werkgever maakt automatisch back-ups van alle bestanden (volledige back-ups)	74%	90%
Ik bezoek alleen websites waar een slotje en/of https voor het adres van een website staat	68%	72%
Ik heb de privacy instellingen van mijn social media accounts aangepast ten opzichte van de standaard instellingen	67%	70%
Als ik op een link in een phishing e-mail zou klikken dan zou ik mij daarvoor schamen.	62%	57%
Ik maak thuis regelmatig back-ups van mijn bestanden	52%	69%
Ik maak op mijn werk regelmatig back-ups van de bestanden op mijn werklaptop	42%	69%
Ik maak thuis gebruik van een extern opslagapparaat dat continu online is	18%	34%
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%	12%
Ik verstuur werkbestanden van mijn werk e-mailadres naar mijn privé e-mail	9%	11%
Als ik getroffen zou worden door ransomware (gijzelsoftware) en gevraagd wordt om te betalen om weer toegang tot mijn persoonlijke bestanden te krijgen dan zou ik daarvoor betalen	4%	3%

Significantie verschillen (p<.05) tussen medewerkers (Totaal) en ICT-medewerkers zijn aangegeven met groen(hoger) of rood (lager).

Medewerkers werken in 2022 weer vaker op kantoor

- Vanwege het coronavirus werkten mensen in 2021 vaker thuis dan daarvoor. Dit jaar stijgt het aantal medewerkers dat naar kantoor gaat weer.
- In de afgelopen 12 maanden werkten negen op de tien medewerkers (86%) op kantoor. Niettemin wordt door ruim de helft (57%) van de medewerkers (ook) thuis gewerkt. ICT'ers doen dit significant vaker (84%).

Door het coronavirus, werken veel mensen op andere plekken dan zij voorheen deden.
Op welk van onderstaande locaties heeft u in de afgelopen 12 maanden gewerkt?
Meer antwoorden mogelijk

	Medewerkers n=1.106	ICT-verantwoordelijk n=382
	86% +	74% +
	57% -	84%
	14%	17%

Significantie verschillen (p<.05) tussen medewerkers (Totaal) en ICT-medewerkers zijn aangegeven met groen(hoger) of rood (lager).

Meerderheid gebruikt wifi verbinding met wachtwoord

- Negen op de tien medewerkers maken thuis gebruik van Wifi met een wachtwoord. Meer dan de helft (56%) heeft een zelfverzonnen wachtwoord op de router. Vier op de tien (39%) gebruiken het standaard met de router meegeleverde wachtwoord.
- Kleine letters, hoofdletters en cijfers worden in meer dan 80 procent van de zelfverzonnen wachtwoorden gebruikt. Leestekens en speciale tekens worden door ongeveer de helft gebruikt. Vier op de tien hebben een wachtwoord van 12 tekens of langer.

Van wat voor netwerkverbinding maakt u thuis gebruik? Voorgelegd aan medewerkers die weleens thuis werken	ICT	Medewerkers				
	Totaal n=525	Totaal n=1.066	Klein MKB n=103	Groot MKB n=359	Groot-bedrijf n=604	Vitaal n=157
Een wifi-netwerkverbinding met wachtwoord	88%	85%	91%	87%	80%	81%
Een VPN verbinding	32%	37%	21%	35%	51%	50%
Via een internetkabel (niet draadloos; LAN)	30%	22%	23%	21%	22%	19%
Een cloud verbinding ('in de cloud werken' / werken op afstand)	29%	21%	12%	23%	23%	30%
Een hotspot verbinding (3G/4G/5G) via mijn smartphone of tablet	11%	11%	13%	12%	8%	9%
Een wifi-netwerkverbinding zonder wachtwoord (bv openbaar (wifi-) netwerk)	2%	1%	0%	2%	0%	0%

5. Slachtofferschap en aangiftebereidheid

Phishing en spoofing komen vaakst voor in de werksituatie

- Een op de vijf medewerkers heeft de afgelopen 12 maanden een phishingmail op het werk ontvangen.
- Vijf procent kreeg te maken met spoofing. Andere vormen van cybercrime kwamen duidelijk minder voor.
- Ook in 2021 kwam phishing het meeste voor.
- ICT-verantwoordelijken hebben vaker te maken met cybercrime dan andere medewerkers.

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=382	Totaal n=1.166	Klein MKB n=123	Groot MKB n=375	Groot-bedrijf n=669	Vitaal n=159
Mails ontvangen met poging tot phishing	37%	21%	18%	21%	25%	25%
Gebeld door iemand die zich voordeed als bedrijf of officiële instantie om geld of gegevens te bemachtigen	10%	5%	4%	5%	3%	3%
Acquisitiefraude	12%	4%	5%	4%	1%	1%
Benaderd op social media met een vraag om een onbekende link aan te klikken	10%	4%	4%	4%	1%	1%
Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik die bijna niet van echt te onderscheiden is	8%	3%	1%	3%	1%	1%
Een foute link ook daadwerkelijk hebben aangeklikt in de zin dat deze een virus, spam, phishing of andere ongewenste poging tot cybercrime bevatten	1,8%	1,5%	1,6%	1,8%	2,2%	2,2%
Benaderd via WhatsApp door iemand die zich voordeed als een bekende die probeerde geld te ontvangen	1,7%	1,4%	3,2%	1,0%	1,4%	1,4%
Ransomware	1,7%	0,8%	2,4%	0,5%	0,4%	0,4%
Dat door het downloaden van geïnfecteerde software/bestanden malware verspreid werd (oa via een e-mail)	0,9%	0,4%	0,0%	0,5%	0,0%	0,0%
Dat een computer tijdelijk niet werkte door malware zoals bijvoorbeeld een virus	1,2%	0,4%	0,8%	0,3%	0,0%	0,0%
Iemand in een apparaat (computer, telefoon) heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	1,1%	0,3%	0,8%	0,0%	0,4%	0,4%
Iemand in een account (social media, webwinkel, e-mail, bank) heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	0,7%	0,2%	0,8%	0,0%	0,4%	0,4%
Identiteitsdiefstal	0,5%	0,1%	0,0%	0,0%	0,4%	0,4%

Meldingen cybercrime meest bij fraudehelpdesk en ICT-afdeling

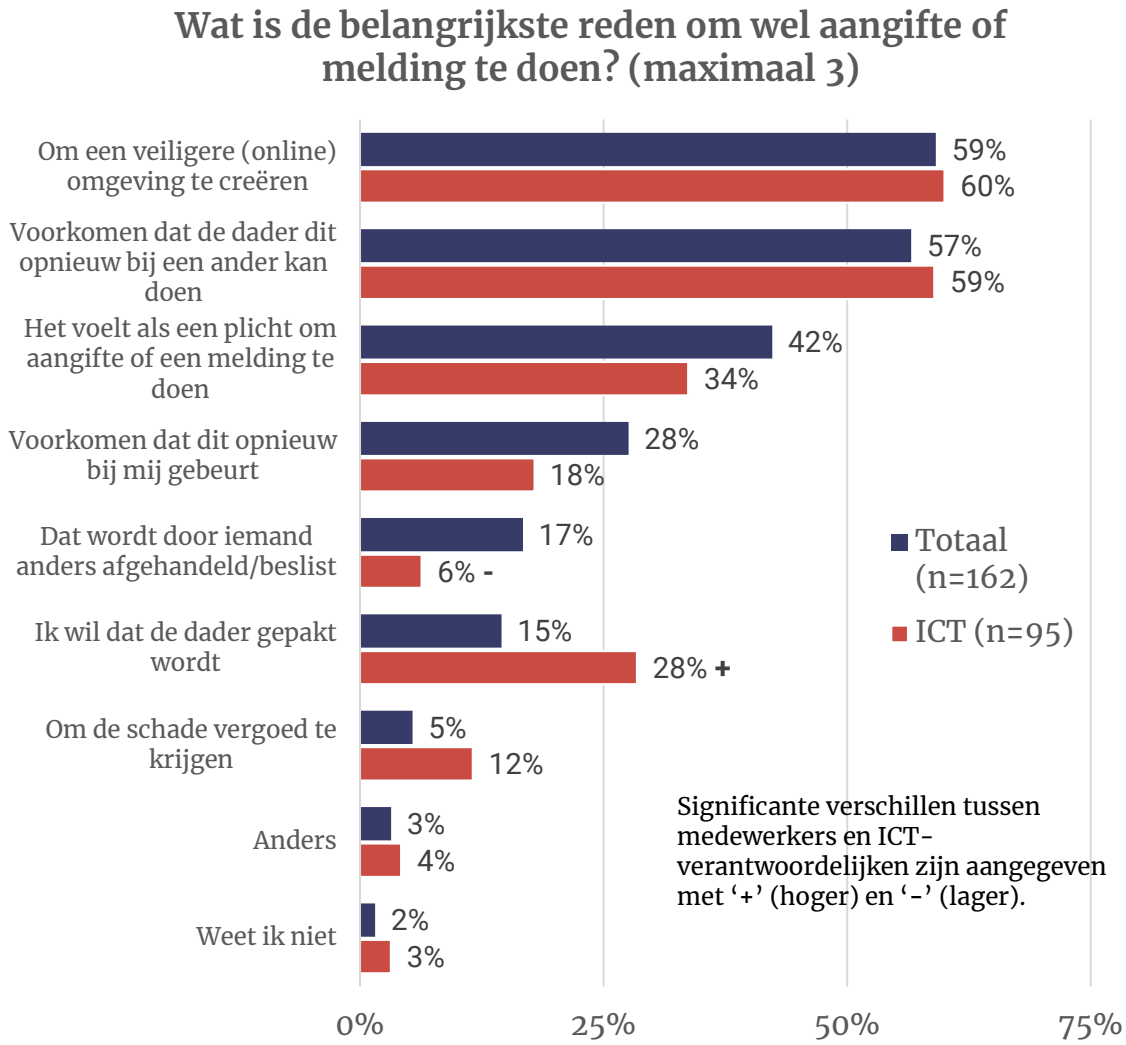
- ICT-verantwoordelijken doen vaker (19%) dan medewerkers (11%) een melding bij de fraudehelpdesk. Medewerkers doen hun melding van cybercrime juist vaker bij de ICT-afdeling van hun bedrijf (29%). Bij grotere bedrijven met meer dan 200 medewerkers doet bijna de helft dit.
- Meldingen of aangiften bij politie, gemeente, NCSC of SeniorWeb komen nauwelijks voor. Het grootste deel (56%) kiest ervoor om geen actie te ondernemen nadat men te maken kreeg met cybercrime in de werksituatie.
- Medewerkers van kleine bedrijven ondernemen het minst vaak actie (19%), dit percentage is vanwege het lage aantal waarnemingen slechts indicatief.
- In vergelijking met 2021 doen medewerkers minder vaak 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=193	Totaal n=325	Klein MKB n=31*	Groot MKB n=107	Groot-bedrijf n=187	Vitaal n=45*
Aangifte bij de politie	2%	1% -	0%	0% -	3%	4%
Melding bij de politie	4%	1%	0%	1%	0%	0%
Melding bij fraudehelpdesk	19%	11%	10%	12%	8%	4%
Melding bij de gemeente	2%	1%	3%	1%	0%	0%
Melding bij SeniorWeb	1%	1%	3%	0%	0%	0%
Melding bij de ICT-afdeling van mijn bedrijf	22%	29%	6%	27%	48%	25%
Melding bij het Nationaal Cyber Security Centrum (NCSC)	3%	1%	0%	1%	1%	0%
Bij een andere organisatie	6%	5%	6%	5%	3%	1%
Nee, ik heb hier niks mee gedaan	51%	56%	81%	56%	42%	69% +

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 een veiliger omgeving creëren. Net zo vaak noemt men dat men wil dat de dader geen andere slachtoffers kan maken.
- Medewerkers geven vaker dan ICT-verantwoordelijken aan dat ze niet zelf kunnen beslissen wat er gebeurt met de aangifte of melding. Ook is het pakken van de dader vaker een reden voor hen.



Kwart medewerkers denkt dat melding/aangifte geen zin heeft

- De voornaamste reden om geen melding of aangifte te doen, is omdat men denkt dat het geen zin heeft.
- Een vijfde vindt het te veel moeite of vindt het niet zo belangrijk.
- ICT-verantwoordelijken hebben gemiddelde genomen minder vertrouwen in de instanties die de melding of aangifte op moeten pakken.

Wat zijn de belangrijkste redenen om geen aangifte of melding te doen? (maximaal 3)	Medewerkers (n=162)	ICT-verantwoordelijke (n=95)
Het heeft geen zin, er wordt niets gedaan met de aangifte of melding	27%	38%
Het kost te veel moeite	19%	22%
Het is niet zo belangrijk	19%	18%
Ik los het zelf op	15%	23%
Dat wordt door iemand anders afgehandeld/beslist	12%	4%
Ik weet niet bij welke instantie ik moet zijn voor het oplossen van dit type delict	10%	13%
Ik heb weinig vertrouwen in de instanties om aangifte of een melding te doen	10%	22%
Er is niet de kennis op dit type delict aan te pakken	5%	7%
Ik schaam me dat ik slachtoffer ben geworden van het delict	1%	0%
Ik vind dat het eigenlijk mijn eigen schuld is	1%	1%
Ik ben bang dat de dader wraak zal nemen	0%	1%
Ik wilde aangifte doen maar dit werd mij afgeraden	0%	2%

Significante verschillen tussen medewerkers en ICT-verantwoordelijken zijn aangegeven met groen (hoger) en rood (lager).

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