Veilig online 2020

Medewerkers bedrijfsleven (vitaal en niet-vitaal)

Kevin Hengstz
Rebecca van der Grient

B6456
25 september 2020

Ministerie van Economische Zaken en Klimaat

motivaction
insights and strategy

Inhoudsopgave

Achtergrond

Op verzoek van het ministerie van Economische Zaken en Klimaat (hierna: ministerie van EZK), directie Digitale Economie, brengt Motivaction International B.V. een onderzoeksvoorstel uit naar de beleving van de digitale veiligheid in Nederland.

In 2019 stelde de Nationaal Coördinator Terrorismebestrijding Nederland (hierna: NCTV) in het Cybersecuritybeeld Nederland rapport dat Nederland kwetsbaar is voor digitale aanvallen, doordat ze achterblijft in haar weerbaarheid*. Dit geldt niet alleen voor bedrijven, maar ook voor overheidsinstellingen en burgers. Tegelijkertijd is digitalisering één van de prioriteiten van het ministerie van EZK. Digitalisering biedt volop kansen voor welvaart en welzijn in Nederland, maar komt ook met uitdagingen. Want kunnen wel alle burgers en bedrijven meekomen in de digitale wereld of blijven hun digitale vaardigheden achter. En weten burgers en bedrijven wat ze kunnen doen om hun eigen digitale weerbaarheid te verhogen? Met het huidige onderzoek wil het ministerie van EZK achterhalen hoe Nederlanders hun digitale veiligheid inrichten en welke belemmeringen zij ervaren bij het inrichten van hun digitale veiligheid.

Het doel van dit onderzoek is het monitoren van de cyber awareness en cyberskills van Nederlanders door de jaren heen. Tot 1 januari 2020 werd dit bewustzijnsonderzoek in opdracht van de NCTV van het ministerie van Justitie en Veiligheid uitgevoerd. Per deze datum heeft het ministerie van Economische Zaken en Klimaat (EZK) dit overgenomen. Verder heeft dit onderzoek tot doel om inzichten te vergaren van kennis, houding en gedrag van Nederlanders met betrekking tot online veiligheid en anderzijds het bieden van inzichten voor beleidsvorming met betrekking tot dit thema.

Het rapport dat voor u ligt gaat in op houding en gedrag naar online veiligheid onder medewerkers en ICT-verantwoordelijken.

*Bron: https://www.ncsc.nl/onderwerpen/cyber-security-beeld-nederland/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019

Doelstelling

Het doel (monitoring) van dit onderzoek is enerzijds het vergaren van kennis, houding en gedrag van medewerkers en ICT-verantwoordelijken met betrekking tot online veiligheid en anderzijds het bieden van inzichten voor beleidsvorming met betrekking tot dit thema. Bij de drie deelonderwerpen zijn de volgende onderzoeksvragen geformuleerd:

Kennis

- Met welke digitale risico's zijn medewerkers en ICT-verantwoordelijken bekend?
- Hoe groot schat men de kans dat zij thuis en op werk te maken krijgen met deze digitale risico's?
- Waaraan kan men digitale risico's herkennen?
- Is men weleens slachtoffer geweest van een cybercrime?
- Welke afspraken zijn er op het werk wat betreft cybersecurity?

Houding

- Hoe schatten medewerkers en ICT-verantwoordelijken hun eigen digitale vaardigheden in?
- In hoeverre heeft men behoefte en ambitie om de eigen digitale vaardigheden te verbeteren?
- In hoeverre maakt men zich zorgen om digitale risico's thuis en op het werk?
- In hoeverre ervaart men belemmeringen bij veilig online gedrag?
- In hoeverre vindt men de afspraken op het werk wat betreft cybersecurity duidelijk?

Gedrag

- Wat verstaat men onder veilig online gedrag thuis en op het werk?
- In hoeverre vertoont men veilig online gedrag (bijv. met het gebruik van wachtwoorden, netwerkverbindingen, bestanden, het beheren van gegevens en gebruik van verschillende apparaten)?
- In hoeverre maakt men gebruik van beveiligde/openbare wifi-netwerken?
- Welke acties heeft men ondernomen om de eigen online veiligheid te verbeteren?
- In hoeverre houdt men zich aan de op het werk gemaakte afspraken voor veilig online gedrag?

Samenvatting

> Medewerkers

> ICT-verantwoordelijken

Samenvatting Medewerkers (1/3)

Kennis

Medewerkers van grote bedrijven en groot-MKB zijn het meest positief over hun kennisniveau over digitale gevaren

Bij de grotere bedrijven (vanaf 10 medewerkers) beoordeelt circa vier op de tien zichzelf als goed. Medewerkers in het klein-MKB zijn het minst positief over hun hun kennisniveau (27%). In dit onderzoek zijn een aantal digitale gevaren voorgelegd. Identiteitsfraude, phishing en hacking zijn bij alle vier medewerkersgroepen het meest bekend (minstens 84%). Medewerkers in de vitale infrastructuur zijn vaker bekend met de minder bekende digitale risico's (cryptojacking: 48%; spoofing: 50%; botnets: 40%).

Relatief lage kans op schade volgens medewerkers

De kans dat medewerkers schade ondervinden als gevolg van een risico wordt relatief laag ingeschat. Met name medewerkers in het klein-MKB schatten de kans vaak onder de 10%. Medewerkers in de vitale infrastructuur geven in vergelijking vaak een hogere kans op (rond de 15%). Met name DDos-aanvallen krijgen onder deze groep een ‘hoge’ kans inschatting (17%). Waarschijnlijk heeft dit ook te maken met de toename in het aantal DDos-aanvallen waar onder andere overheidsinstellingen en internetproviders door zijn getroffen*. Als het gaat om de digitale veiligheid van de werksituatie in het algemeen, dan zijn het de medewerkers in het grootbedrijf die zich hier het minst zorgen over maken en medewerkers in het klein-MKB het meest.

Medewerkers binnen de vier type bedrijven weten goed hoe ze phishingmails kunnen herkennen

Om phishing te herkennen checken medewerkers meestal het e-mailadres van de afzender. Medewerkers binnen de vitale infrastructuur checken het e-mailadres wel minder vaak (55%) dan medewerkers die niet in een vitale infrastructuur werken (klein-MKB: 66%, groot-MBK: 59% en grootbedrijf: 61%). Met name medewerkers uit het klein-MKB zijn alert op vragen naar specifieke gegevens en wachtwoorden.

* https://nos.nl/artikel/2346721-steeds-meer-ddos-aanvallen-op-bedrijven-en-organisaties.html

Samenvatting Medewerkers (2/3)
Houding

Beveiligingsopties bekend, maar lang niet altijd ingezet om de veiligheid te verbeteren

Medewerkers in het klein-MKB geven vaker aan verschillende acties te hebben ondernomen om hun online veiligheid te verbeteren, zoals het gebruiken en updaten van antivirussoftware (65%), het maken van back-ups (58%), beveiligingsupdates uitvoeren (58%) en links controleren voor er op te klikken (56%). In vergelijking voeren medewerkers in het groot-MKB en in vitale infrastructuur deze opties minder vaak uit. Deze groepen lijken ook minder vaak bereid om acties te ondernemen om hun veiligheid te verbeteren. Medewerkers in het klein-MKB en in grootbedrijven juist vaker. Het lijkt er ook op dat medewerkers in het klein-MKB minder vaak belemmeringen in tijd, gemak en kosten ervaren om hun veiligheid te verhogen dan medewerkers van andere type bedrijven.

Medewerkers ervaren weinig zorgen rondom hun digitale veiligheid

Medewerkers maken zich relatief weinig zorgen om hun digitale veiligheid. Vooral medewerkers in grootbedrijven ervaren weinig zorgen (76%). De mate waarin medewerkers zich zorgen maken verschilt ook. Medewerkers in het klein-MKB maken zich in verhouding vaker enige zorgen (36%). Medewerkers in de vitale infrastructuur ervaren naar verhouding vaker veel tot zeer veel zorgen (10%). Wanneer specifiek gevraagd wordt naar cyberaanvallen zijn de zorgen beperkt. Medewerkers in vitale organisaties maken zich relatief het meeste zorgen (11%). Uit onderzoek van het CBS blijkt dat kleine bedrijven minder vaak in aanraking komen met cyberaanvallen. Medewerkers in het klein-MKB maken zich dan ook het minst zorgen (3%)*.

Vooral medewerkers in de vitale infrastructuur komen in aanraking met digitale risico's

Phishing komt bij alle medewerkersgroepen het vaakst voor, met name in het klein-MKB. Deze groep komt ook vaker in aanraking met acquisitiefraude. Medewerkers in de vitale infrastructuur zijn in de afgelopen 12 maanden vaker in aanraking geweest met de meeste andere digitale risico's. De meesten ondernemen actie nadat ze in aanraking zijn gekomen met een digitaal risico. In verhouding zijn medewerkers bij grootbedrijven minder vaak in actie gekomen (63% vs. 71% onder de andere medewerkers). Medewerkers in vitale organisaties komen het vaakst in actie (77%) en treffen vaker verschillende maatregelen.

* https://www.cbs.nl/nl-nl/nieuws/2018/42/kleine-bedrijven-minder-vaak-slachtoffer-cyberaanval

Samenvatting Medewerkers (3/3)
Gedrag

In het klein-MKB zijn minder vaak werkafspraken over veilig online gedrag gemaakt

In het groot-MKB , bij grootbedrijven en in de vitale infrastructuur zijn vaak afspraken gemaakt hoe men zich online dient te gedragen (77%). Bij medewerkers in het klein-MKB gebeurt dit minder vaak (45%). Met name in grootbedrijven en bedrijven in de vitale infrastructuur zijn meer verschillende afspraken gemaakt. Het draagvlak voor de afspraken is ook relatief groot onder medewerkers in grootbedrijven. Hoewel medewerkers in het klein-MKB vaak sneller zelf stappen ondernemen op het gebied van online veiligheid vinden ze minder vaak dat afspraken over veilig online gedrag binnen de organisatie duidelijk zijn (68%) en dat de afspraken voldoende worden toegepast in hun bedrijf/organisatie (65%). Ook beschikken ze minder vaak over de juiste tools en instrumenten om zich veilig online te gedragen of te bevorderen. Dit komt waarschijnlijk doordat het klein-MKB minder budget heeft om alle tools en instrumenten aan te schaffen dan grotere bedrijven en omdat afspraken in grotere bedrijven vaker centraal geregeld zijn.

Onder medewerkers in de vitale infrastructuur wordt online gedrag meer gemonitord; zij geven iets vaker aan zich niet altijd aan afspraken te houden

Medewerkers in het groot-MKB geven wat vaker aan dat zij zich niet altijd aan gemaakte werkafspraken omtrent veilig online gedrag houden (soms tot altijd: 19%). Dit zien we ook terug bij medewerkers in de vitale infrastructuur (soms tot altijd: 21%). Veilig online gedrag wordt structureel en incidenteel gemonitord onder medewerkers in de vitale infrastructuur (60%). Onder medewerkers in het klein-MKB juist minder vaak (36%). Medewerkers in het klein-MKB ervaren minder vaak belemmeringen om afspraken rondom veilig online gedrag te borgen (64%) in vergelijking met de andere type bedrijven (52%).

Minder steun voor belonen dan straffen bij het niet naleven van werkafspraken over online gedrag

Medewerkers van de verschillende type bedrijven staan er hetzelfde in als het gaat om consequenties bij het niet naleven van veilig online gedrag, ongeveer twee derde van de medewerkers vindt dat er sancties opgelegd moeten kunnen worden. Ze verschillen echter wel sterk van mening als het gaat om het belonen van goed gedrag. Medewerkers in het groot-MKB en van de vitale infrastructuur zijn daar vaker voorstander van dan medewerkers in het klein-MKB en van grootbedrijven.

Samenvatting

> Medewerkers

> ICT-verantwoordelijken

Samenvatting ICT-verantwoordelijken (1/2)

Kennis & houding

Goed op de hoogte van digitale en online veiligheid

ICT-verantwoordelijken schatten hun kennis over digitale en online veiligheid (zoals te verwachten valt) vaak in als goed tot zeer goed. Met name verantwoordelijken van grootbedrijven schatten hun kennisniveau als zeer hoog. ICT-verantwoordelijken van grootbedrijven geven aan goed op de hoogte te zijn van de digitale risico's.

Weinig zorgen om de digitale veiligheid

ICT-verantwoordelijken van grootbedrijven gebruiken meer soorten digitale beveiligingsopties en maken zich, waarschijnlijk mede hierdoor, minder vaak zorgen over hun digitale veiligheid dan ICT-verantwoordelijken van andere type bedrijven. ICT-verantwoordelijken in het klein-MKB maken zich juist meer zorgen over de algemene digitale veiligheid in hun werksituatie. Wanneer het gaat om cyberaanvallen maken ICT-verantwoordelijken in het groot-MKB en bij grootbedrijven zich meer zorgen. Zij zijn dan ook vaker slachtoffer van cyberaanvallen dan kleinere bedrijven*.

Over het algemeen is de inschatting dat men schade ondervindt van digitale risico's laag. In vergelijking met de andere type bedrijven geven ICT-verantwoordelijken van het klein-MKB een opvallend lagere kans op schade door phishing (8% vs. 15%).

ICT-verantwoordelijken in groot-MKB vaakst in aanraking gekomen met digitale risico's

ICT-verantwoordelijken van groot-MKB zijn in de afgelopen 12 maanden vaker in aanraking gekomen met een digitaal risico. Ze hebben dan ook vaker maatregelen getroffen om risico's in de toekomst te verkleinen (76%).

* https://www.cbs.nl/nl-nl/nieuws/2018/42/kleine-bedrijven-minder-vaak-slachtoffer-cyberaanval

Samenvatting ICT-verantwoordelijken (2/2)

Houding & gedrag

ICT-verantwoordelijken in het MKB ervaren de meeste belemmeringen en onduidelijkheid als het gaat om digitale bescherming

Relatief veel ICT-verantwoordelijken in het MKB vinden de instructies om jezelf te beschermen tegen digitale risico's ingewikkeld. ICT'ers van grootbedrijven hebben hier minder moeite mee (21%). In het groot-MKB ervaren ICT-verantwoordelijken het maken van back-ups en het automatisch uitloggen vaker als belemmering dan de andere type bedrijven.

Meesten vinden werkafspraken rondom veilig online gedrag duidelijk

In grootbedrijven is volgens ICT-verantwoordelijken het pakket aan werkafspraken rondom veilig online gedrag het meest uitgebreid. In het klein-MKB zijn vaker geen bedrijfsafspraken. Vrijwel alle ICT-verantwoordelijken ervaren een hoge mate van eigen verantwoordelijkheid voor eigen online gedrag. Daarnaast is er hoge mate van begrip voor de afspraken en staat men er voor open om aangesproken te worden op het eigen gedrag. De meesten vinden de afspraken duidelijk en dat het makkelijk is om zich aan de gemaakte afspraken te houden. Een meerderheid vindt ook dat de gemaakte afspraken voldoende worden toegepast in de organisatie. ICT-verantwoordelijken in het groot-MKB geven wat vaker aan dat ze moeite hebben om zich altijd aan de werkafspraken te houden.

Eigen gedrag wordt beoordeelt als goed; minder steun voor belonen dan straffen bij het niet naleven van werkafspraken over online gedrag

ICT-verantwoordelijken van grootbedrijven vinden vaker dat ze goed omgaan met digitale zaken. ICT-verantwoordelijken in het groot-MKB en grootbedrijven geven zichzelf gemiddeld een hoger cijfer voor hun eigen gedrag (7.6) dan hun collega's in het klein-MKB (7.2). Als toelichting op hun cijfer geven ICT-verantwoordelijken aan dat zij goed op de hoogte zijn of hun beveiliging goed op orde hebben.

ICT-verantwoordelijken van grootbedrijven geven vaker aan dat bij hun het online gedrag (incidenteel) wordt gemonitord. Ook hier zien we dat er meer steun is voor de consequenties wanneer men afspraken niet naleeft dan voor het belonen van goed gedrag.

Leeswijzer

Leeswijzer (1/2)

In de rapportage tonen we de resultaten voor de verschillende groepen werkende Nederlanders. Het rapport is onderverdeeld in twee hoofdstukken: medewerkers en eind- of medeverantwoordelijken voor de ICT/automatisering binnen het bedrijf of organisatie. We beginnen met de resultaten van medewerkers. Binnen de groep medewerkers vier doelgroepen, namelijk:

- Medewerkers in het klein-MKB (1-9 medewerkers, inclusief ZZP'ers)
- Medewerkers in het groot-MKB (10-199 medewerkers)
- Medewerkers in het grootbedrijf (200 of meer medewerkers)
- Medewerkers in de vitale infrastructuur. Deze doelgroep is gedefinieerd als medewerkers die werkzaam zijn in een bedrijf of organisatie die zich bezighoudt met één van de onderstaande processen:
    - Transport en distributie elektriciteit
    - Gasproductie en distributie gas
    - Internettoegang (Internetproviders)
    - Drinkwatervoorziening
    - Keren en beheren waterkwantiteit
    - Vlucht- en vliegtuigafhandeling (bijvoorbeeld op Schiphol)
    - Scheepvaartafwikkeling (bijvoorbeeld 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

Dit hoofdstuk is onderverdeeld in verschillende thema's: het kennisniveau van medewerkers, hun zorgen over digitale veiligheid, hun digitale gedrag, ervaringen met digitale risico's en afspraken op de werkvloer omtrent veilig online gedrag.

Leeswijzer (2/2)

In het tweede hoofdstuk gaan we in op de resultaten van de ICT-verantwoordelijken. Ook in dit hoofdstuk wordt onderscheid gemaakt tussen doelgroepen:

- ICT/automatisering verantwoordelijken binnen het klein-MKB (1 t/m 9 medewerkers, incl. ZZP'ers).
- ICT/automatisering verantwoordelijken binnen het groot-MKB (10 t/m 199 medewerkers).
- ICT/automatisering verantwoordelijken binnen het grootbedrijf (200 of meer medewerkers).

Ook in dit hoofdstuk worden de volgende thema's behandeld: het kennisniveau van medewerkers, hun zorgen over digitale veiligheid, hun digitale gedrag, ervaringen met digitale risico's en afspraken op de werkvloer omtrent veilig online gedrag.

De focus van dit rapport ligt op de verschillen tussen groepen medewerkers of ICT-verantwoordelijken. In beide hoofdstukken zijn echter ook de referentiecijfers van het Nederlands publiek vermeld om te laten zien hoe medewerkers en ICT-verantwoordelijken scoren.

De resultaten staan steeds in grafiek vorm of in tabel vorm. In tekst bespreken we de belangrijkste inzichten. Alle resultaten zijn terug te vinden in het separaat geleverde tabellenboek. Significante verschillen worden in het rapport aangegeven met een kleur, in de vorm van gekleurde cijfers.

Groen = significant hoger

Rood = significant lager

Geaggregeerde percentages die we in de tekst noemen, kunnen soms iets (1 procentpunt) afwijken van de som van de onderliggende percentages in de grafiek. Dat komt door afrondingsverschillen. Percentages lager dan 2% zijn niet opgenomen in de grafiek. Dit is vanwege de leesbaarheid van de grafiek.

Resultaten

> Medewerkers

> ICT-verantwoordelijken

Resultaten medewerkers
Kennis over digitale risico's

Medewerkers | Kennis digitale risico's

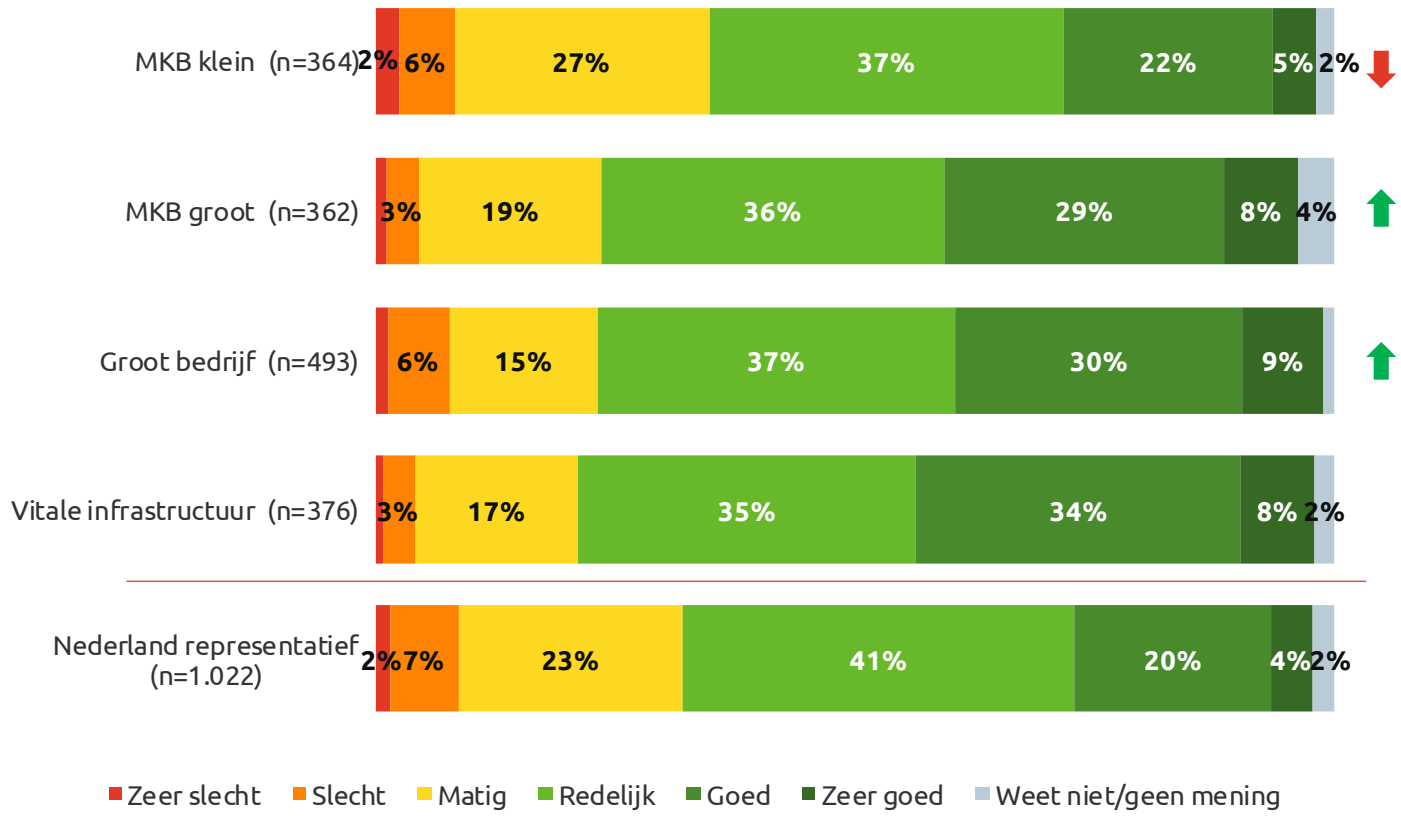
Inschatting eigen kennisniveau lager bij medewerkers in het klein-MKB

De kennis over online veiligheid is het hoogst onder medewerkers in de vitale infrastructuur: van hen geeft 42% aan dat hun kennis (zeer) goed is.

De kennis van medewerkers in het groot-MKB en grote bedrijven is gelijk (% goed tot zeer goed is respectievelijk 37% en 39%).

Medewerkers van een klein-MKB schatten hun eigen kennis over online veiligheid minder goed in (27% (zeer) goed). Dit is vergelijkbaar met het Nederlands publiek.

Hoe schat jij je eigen kennis over digitale en online veiligheid in?



*Percentages < 2% worden t.b.v. de leesbaarheid niet getoond in de grafiek

Significant verschil t.o.v. de andere medewerkersgroepen

Medewerkers | Kennis digitale risico's

Medewerkers vitale infrastructuur zijn vaker bekend met de onbekendere digitale risico's

Kun je aangeven in welke mate je bekend bent met de onderstaande zaken? % weleens mee te maken gehad + ik weet wat dit is	Medewerkers klein-MKB (n=364)	Medewerkers groot-MKB (n=362)	Medewerkers Grootbedrijf (n=493)	Medewerkers vitale infrastructuur (n=376)	Nederland representatief (n=1.022)
Identiteitsfraude	94%	87%	92%	87%	89%
Hacking	92%	85%	94%	87%	88%
Phishing	92%	84%	90%	87%	83%
Malware	79%	73%	75%	77%	65%
Vriend-in-nood-fraude	76%	61%	68%	62%	62%
DDos-aanval	74%	63%	73%	72%	59%
Helpdeskfraude	70%	63%	65%	67%	57%
Ransomware	70%	62%	66%	67%	52%
Cryptojacking	34%	41%	40%	48%	26%
Spoofing	33%	43%	38%	50%	24%
Botnet	28%	34%	32%	40%	19%

Medewerkers | Kennis digitale risico's

Medewerkers klein-MKB schatten kans op schade het laagst in; medewerkers vitale infrastructuur juist hoger

Hoe groot acht je de kans dat je in jouw werksituatie computer/financiële schade oploopt, geen gebruik kunt maken van je computer als gevolg hiervan? *% groot + zeer groot* Basis – is bekend met digitaal risico	**Medewerkers klein-MKB (n=364)**	**Medewerkers groot-MKB (n=362)**	**Medewerkers Grootbedrijf (n=493)**	**Medewerkers vitale infrastructuur (n=376)**	**Nederland representatief (n=1.022)**
Phishing	10%	10%	13%	16%	8%
Malware	8%	13%	11%	14%	9%
Hacking	9%	11%	13%	15%	13%
Ransomware	5%	15%	10%	14%	12%
Helpdeskfraude	4%	9%	8%	12%	12%
Vriend-in-nood-fraude	6%	6%	8%	9%	7%
Identiteitsfraude	9%	10%	10%	12%	11%
DDos-aanval	6%	14%	13%	17%	13%
Spoofing	3%	13%	7%	14%	5%
Botnet	3%	11%	11%	16%	8%
Cryptojacking	2%	10%	11%	14%	6%

Medewerkers | Kennis digitale risico's

Medewerkers vitale infrastructuur letten minder op het mailadres om een phishing mail te ontmaskeren

Naar welke onderdelen van een mail kijk jij vooral om een phishingmail te herkennen? Basis - Bekend of heeft ervaring met phishing	Medewerkers klein-MKB (n=364)	Medewerkers groot-MKB (n=362)	Medewerkers Grootbedrijf (n=493)	Medewerkers vitale infrastructuur (n=376)	Nederland representatief (n=1.022)
Het mailadres van de afzender	66%	59%	61%	55%	59%
Vraag om persoonlijke gegevens	50%	39%	52%	46%	52%
Het taalgebruik in het onderwerp of in de mail zelf (de toon)/De schrijfstijl in de mail	56%	47%	53%	46%	50%
Of er om geld wordt gevraagd	40%	29%	38%	31%	40%
Het doeladres waar de link naar verwijst, voordat je er op klikt	38%	33%	36%	32%	34%
De opmaak van het bericht	31%	36%	34%	33%	33%
De urgentie die uit de inhoud van de mail spreekt (moet er snel actie ondernomen worden)	32%	24%	27%	24%	30%
De link(s) die in de mail zijn opgenomen /de link die achter de knop 'klik hier' staat	32%	33%	36%	33%	29%
De naam van de afzender	24%	26%	29%	27%	28%
De aanhef/of ik persoonlijk aangesproken word in de mail	22%	18%	27%	18%	24%
De logo's in de mail	13%	8%	13%	12%	12%
Het lettertype van de mail	3%	7%	5%	6%	5%
Ik let hier nooit op als ik een mail bekijk	0%	1%	1%	1%	1%
Ik kan dit niet herkennen, de mails zien er te echt uit	0%	0%	0%	1%	1%
Anders, namelijk:	2%	1%	2%	2%	2%
Weet niet/geen mening	2%	3%	2%	2%	3%

Medewerkers | Kennis digitale risico's

Medewerkers groot-MKB kijken minder vaak bij berichten of om bepaalde gegevens of inloggegevens wordt gevraagd om phishing te ontdekken

Naar welke onderdelen van een mail kijk jij vooral om een phishingmail te herkennen? Basis - Bekend of heeft ervaring met phishing	Medewerkers klein-MKB (n=364)	Medewerkers groot-MKB (n=362)	Medewerkers Grootbedrijf (n=493)	Medewerkers vitale infrastructuur (n=376)	Nederland representatief (n=1.022)
Of om bepaalde gegevens wordt gevraagd	60%	43%	55%	46%	55%
Of gevraagd wordt of ik mijn inloggegevens en wachtwoord wil invoeren	56%	37%	48%	41%	51%
Of er om geld wordt gevraagd	48%	45%	53%	51%	49%
Vraag om persoonlijke gegevens	44%	38%	44%	40%	44%
De link/betaalverzoek	36%	36%	39%	37%	37%
Het taalgebruik in het bericht/de schrijfstijl	32%	33%	34%	28%	34%
De urgentie die uit de inhoud spreekt (moet er snel actie ondernomen worden)	33%	24%	33%	26%	30%
De naam van de afzender	25%	30%	32%	27%	28%
De opmaak van het bericht	14%	22%	13%	18%	15%
De profiel foto	4%	8%	7%	10%	7%
Het lettertype van het bericht	1%	5%	2%	7%	2%
Ik let hier nooit op als ik een bericht bekijk	2%	1%	1%	1%	1%
Ik kan dit niet herkennen, de berichten zien er te echt uit	1%	0%	0%	1%	1%
Anders, namelijk:	5%	3%	3%	1%	4%
Weet niet/geen mening	6%	5%	7%	5%	7%

Medewerkers | Kennis digitale risico's

Medewerkers in het groot-MKB en vitale infrastructuur geven minder vaak aan van de meer gebruikte beveiligingsopties gebruik te maken

Kun je aangeven in welke mate je bekend bent met onderstaande zaken? *% ja, gebruik ik*	Medewerkers klein-MKB (n=364)	Medewerkers groot-MKB (n=362)	Medewerkers Grootbedrijf (n=493)	Medewerkers vitale infrastructuur (n=376)	Nederland representatief (n=1.022)
Virusscanner	85%	74%	82%	72%	81%
Het maken van back-ups van je gegevens	81%	67%	75%	65%	68%
Automatische updates	82%	71%	79%	72%	78%
Tweestapsverificatie	70%	64%	78%	64%	64%
Cloud diensten	57%	52%	57%	49%	43%
Voor elk account en apparaat ander ww gebruiken	64%	49%	56%	50%	52%
Instellingen om te cookies blokkeren/ uit te zetten	55%	50%	57%	49%	47%
Gebruik van lange wachtwoorden (wachtzinnen)	55%	55%	57%	56%	52%
Ad-blocker	42%	45%	44%	38%	37%
Spyware scanner	43%	35%	39%	38%	32%
Biometrische online bescherming	34%	37%	45%	38%	34%
Digitaal wachtwoordenkluisje/ wachtwoordmanager	32%	35%	32%	32%	26%
VPN-verbindingen	26%	36%	42%	39%	25%
Web tracking blocker	24%	25%	22%	23%	16%
Open source hardware- en software	18%	21%	22%	26%	15%

Resultaten medewerkers
Zorgen om digitale veiligheid

Medewerkers | Zorgen om digitale veiligheid

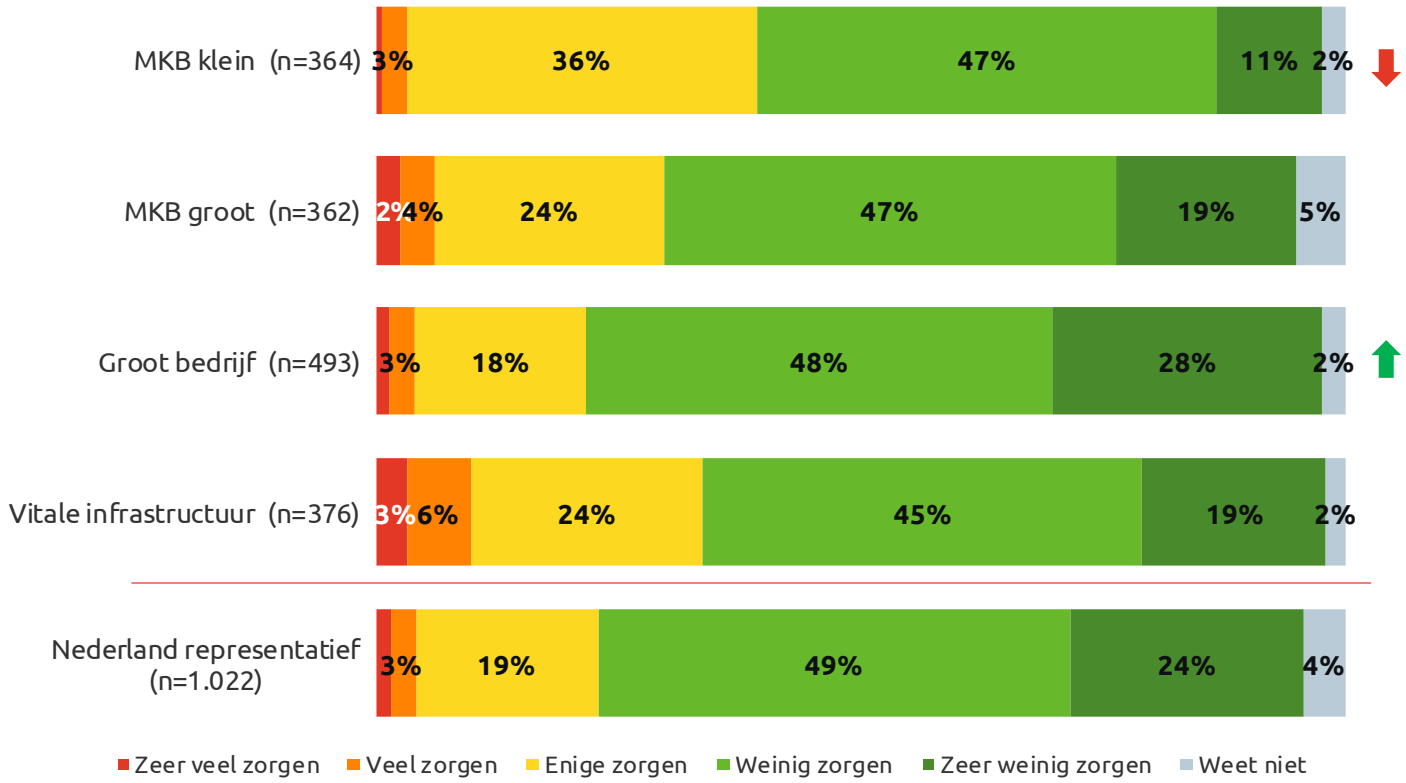
Medewerkers grootbedrijf minst bezorgd om digitale veiligheid

Driekwart van de medewerkers van grootbedrijven (76%) maken zich weinig zorgen om hun online/digitale veiligheid in de werksituatie.

Medewerkers in de vitale infrastructuur maken zich naar verhouding het meest zorgen (10% (zeer) veel). Al is de groep die zich geen zorgen maakt (64%) ongeveer even groot als onder medewerkers in het MKB groot (66%).

Medewerkers in het klein-MKB hebben vaker enige zorgen (36%).

In hoeverre maak je je zorgen over jouw online/digitale veiligheid in je werksituatie?



**Percentages < 2% worden t.b.v. de leesbaarheid niet getoond in de grafiek*

Significant verschil t.o.v. de andere medewerkersgroepen

Medewerkers | Zorgen om digitale veiligheid

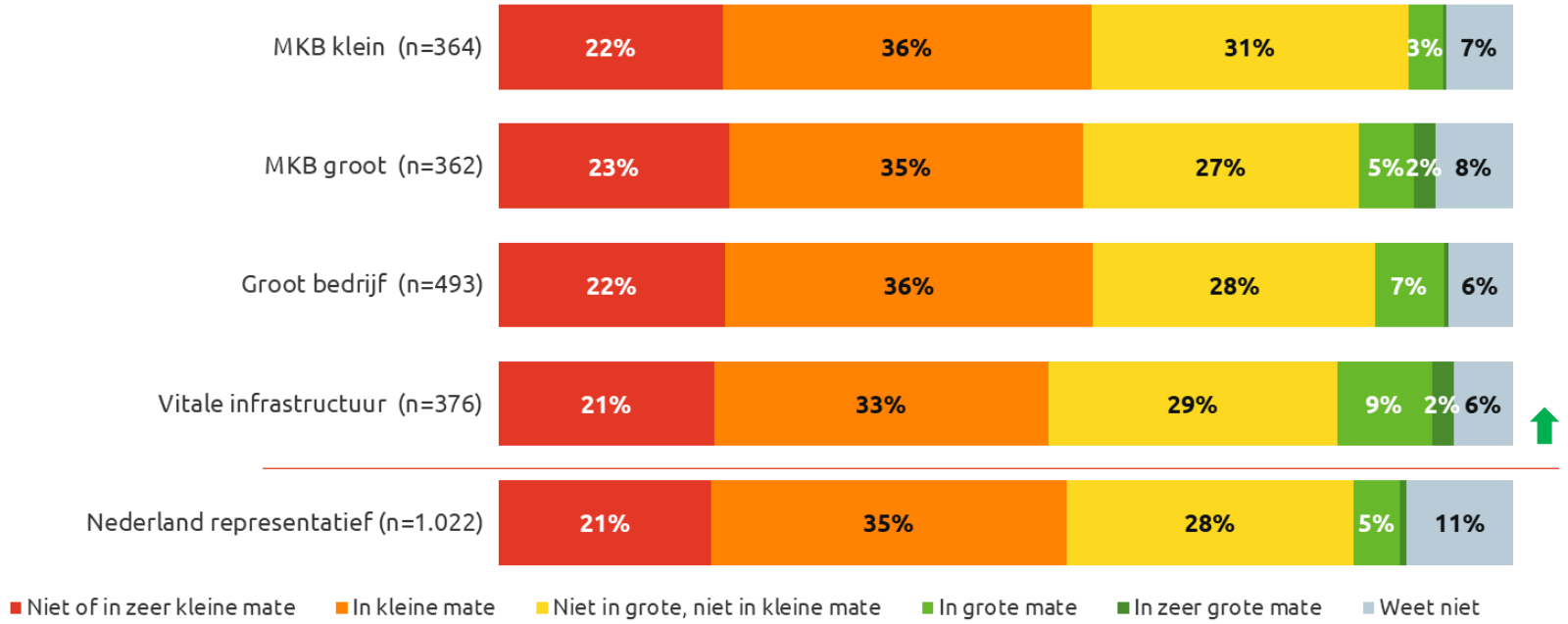
Medewerkers in de vitale infrastructuur maken zich vaker grotere zorgen om een cyberaanval

Medewerkers in de vitale infrastructuur maken zich naar verhouding meer zorgen om cyberaanval (11%). Medewerkers in het klein-MKB juist minder vaak (4%), maar dit verschil is indicatief.

De mate waarin medewerkers zicht niet of in kleine mate zorgen maken om een cyberaanval is gelijk tussen type bedrijven.

Cyberaanval
Onder een cyberaanval verstaan we een digitale aanval die tot gevolg heeft dat:
- een ICT-systeem niet meer betrouwbaar werkt
- een ICT-systeem tijdelijk niet beschikbaar is
- de informatie die opgeslagen is op het ICT-systeem gestolen wordt of aangetast wordt zodat het niet meer bruikbaar is

In welke mate maak je je zorgen dat je zelf te maken krijgt met een cyberaanval?



**Percentages < 2% worden t.b.v. de leesbaarheid niet getoond in de grafiek*

Significant verschil t.o.v. de andere medewerkersgroepen

Resultaten medewerkers
Digitaal gedrag

Medewerkers | Digitaal gedrag

MKB Klein werkt vooral thuis; de rest wel meer op kantoor

Op welk van onderstaande locaties heb je in de afgelopen 12 maanden gewerkt (denk hierbij ook aan 'nieuwe' werkplekken door het coronavirus)?

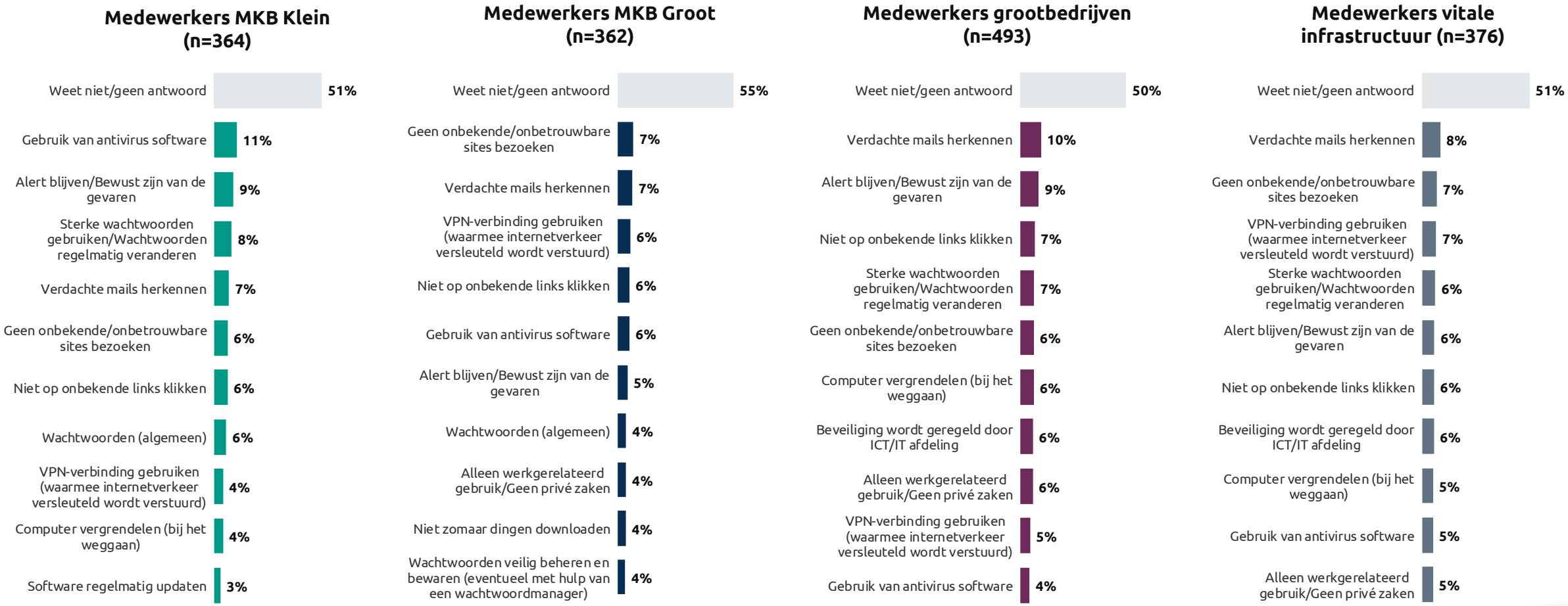
	Thuis	Kantoor	Openbare plek
Medewerkers MKB Klein (n=364)	73%	41%	22%
Medewerkers MKB Groot (n=362)	53%	70%	18%
Medewerkers grootbedrijven (n=493)	57%	66%	26%
Medewerkers vitale infrastructuur (n=376)	61%	69%	22%

Van wat voor netwerkverbinding maak je <u>thuis</u> gebruik?

	klein-MKB n=151	groot-MKB n=254	grootbedrijf n=325	Vitale infrastructuur (n=259)
Een (wifi-)netwerkverbinding met wachtwoord	81%	66%	70%	65%
Een (wifi-)netwerkverbinding zonder wachtwoord	4%	6%	5%	8%
Een VPN verbinding en/of cloud verbinding ('in de cloud werken')	8%	22%	16%	19%
Een hotspot verbinding (3G/4G) via mijn smartphone of tablet	1%	1%	1%	3%
Anders	1%	2%	2%	2%
Weet ik niet	4%	4%	6%	4%

Medewerkers | Digitaal gedrag
Associaties met veilig online gedrag wisselend per sector

Waar denk jij in eerste instantie aan bij veilig online gedrag op je werk?



**Voor de leesbaarheid wordt in de grafiek alleen de top-10 weergegeven*

Medewerkers | Digitaal gedrag

Medewerkers klein-MKB zijn kritischer op hun gedrag als het gaat om wifi onderweg en werken in de cloud

In welke mate ga je veilig om met de volgende zaken? *% Zeer goed + uitstekend*	Medewerkers klein-MKB (n=364)	Medewerkers groot-MKB (n=362)	Medewerkers Grootbedrijf (n=493)	Medewerkers Vitale nfrastructuur (n=376)	Nederland representatief (n=1.022)
Het updaten van mijn software updates	46%	46%	47%	47%	**39%**
Het laten gebruiken van jouw devices door anderen	44%	42%	41%	46%	**35%**
Omgaan met nepmails/met poging tot phishing mails	42%	39%	44%	44%	**38%**
Het bewaren van mijn wachtwoorden	34%	38%	31%	36%	**29%**
Het gebruik van verschillende wachtwoorden	34%	37%	34%	36%	**28%**
Het beperken van schade door diefstal, beschadiging of verwijdering door het maken van back-ups	32%	35%	**28%**	33%	**23%**
Het beheren en gebruik maken van persoons- en klantgegevens	**26%**	33%	30%	**36%**	**26%**
Het gebruik van USB-sticks	**23%**	29%	28%	31%	**23%**
Het afgeven van toestemmingen op websites	23%	27%	25%	**31%**	**19%**
Het afgeven van toestemmingen op webshops	21%	31%	**20%**	27%	**18%**
Het gebruik maken van wifi verbinding terwijl je onderweg bent	**18%**	26%	24%	**30%**	**18%**
Het werken in een cloud	**16%**	26%	23%	**29%**	**16%**

Medewerkers | Digitaal gedrag
MKB Groot schat eigen online gedrag het hoogst in

Welk cijfer geef jij jezelf als het gaat om het veilig omgaan met online gevaren?
(gemiddelde)

Medewerkers MKB klein (n=364)	Medewerkers MKB groot (n=362)	Medewerkers grootbedrijven (n=493)	Medewerkers vitale infrastructuur (n=376)	Nederland representatief (n=1.022)
7,1	7,4	7,1	7,3	7,0

Kun je toelichten waarom je jezelf dit cijfer geeft? (Top 5*)

Medewerkers MKB klein (n=364)		Medewerkers MKB groot (n=362)		Medewerkers grootbedrijven (n=493)		Medewerkers vitale infrastructuur (n=376)	
28%	Ik ben goed op de hoogte/Ik heb alles op orde	30%	Ik ben goed op de hoogte/Ik heb alles op orde	28%	Ik ben goed op de hoogte/Ik heb alles op orde	33%	Ik ben goed op de hoogte/Ik heb alles op orde
22%	**Er is (altijd) ruimte voor verbetering**	19%	Ik ben alert/bewust van de gevaren/voorzichtig	19%	Ik ben alert/bewust van de gevaren/voorzichtig	20%	Ik ben alert/bewust van de gevaren/voorzichtig
20%	Ik ben alert/bewust van de gevaren/voorzichtig	8%	**Er is (altijd) ruimte voor verbetering**	15%	Er is (altijd) ruimte voor verbetering	14%	Er is (altijd) ruimte voor verbetering
8%	Ik ben hier niet bewust mee bezig/Ik ben (soms) te laks	5%	Ik ben hier niet bewust mee bezig/Ik ben (soms) te laks	8%	Ik ben hier niet bewust mee bezig/Ik ben (soms) te laks	6%	Ik ben hier niet bewust mee bezig/Ik ben (soms) te laks
8%	Ik heb hier geen/weinig verstand van	4%	Ik heb hier geen/weinig verstand van	7%	Ik heb hier geen/weinig verstand van	4%	Ik heb hier geen/weinig verstand van

*Deze vraag is open gesteld en achteraf gecodeerd.

Medewerkers | Digitaal gedrag

MKB Groot en vitale infrastructuur minder ondernomen t.b.v. online veiligheid

Welke van de onderstaande acties heb je ondernomen of doe je om jouw online veiligheid te verbeteren?	Medewerkers klein-MKB (n=364)	Medewerkers groot-MKB (n=362)	Medewerkers Grootbedrijf (n=493)	Medewerkers Vitale infrastructuur (n=376)	Nederland representatief (n=1.022)
Antivirussoftware gebruiken en regelmatig updaten	65%	47%	54%	43%	58%
Regelmatig back-ups maken van al mijn bestanden	58%	43%	50%	40%	42%
Regelmatig (beveiligings)updates doen	58%	43%	55%	45%	51%
Controleren op welke links ik klik	56%	45%	53%	42%	50%
Direct software updates uitvoeren	51%	40%	47%	38%	44%
Een firewall installeren	48%	32%	36%	34%	32%
Geen gebruik meer maken van onbeveiligde sites om bestanden uit te wisselen	40%	29%	35%	30%	33%
Mijn wachtwoorden regelmatig veranderen	38%	38%	37%	34%	33%
Lange wachtwoorden of wachtzinnen gebruiken van minimaal 12 tekens.	38%	30%	39%	36%	32%
Geen gebruik maken van openbare wifi-netwerken	37%	28%	31%	30%	30%
Het standaard wachtwoord van mijn wifi modem veranderen (in een sterk en uniek ww)	31%	25%	30%	23%	24%
Steeds een nieuw wachtwoord gebruiken dat ik nog niet eerder gebruikt heb	28%	23%	28%	20%	23%
Een wachtwoordmanager gebruiken	24%	17%	20%	15%	15%
Extensies aan je webbrowser toevoegen om cookies, advertenties en automatisch toegang tot Javascripts te blokkeren	18%	15%	22%	14%	16%
Altijd gebruik maken van een VPN-verbinding	12%	16%	19%	18%	12%
Informatie op internet opzoeken over hoe ik veiliger kan worden	11%	10%	10%	13%	10%
Specialist inhuren die thuis langskomt om de digitale veiligheid te verbeteren installeren	9%	5%	3%	3%	5%
Jaarlijks een digitale apk laten uitvoeren	6%	6%	4%	5%	4%
Geen van bovenstaande	4%	5%	4%	3%	7%

Medewerkers | Digitaal gedrag

MKB Groot en vitale infrastructuur ook minder bereid acties te ondernemen

Welke van de onderstaande acties heb je ondernomen of doe je om jouw online veiligheid te verbeteren?	Medewerkers klein-MKB (n=364)	Medewerkers Groot-MKB (n=362)	Medewerkers Grootbedrijf (n=493)	Medewerkers Vitale Infrastructuur (n=376)	Nederland representatief (n=1.022)
Regelmatig back-ups maken van al mijn bestanden	48%	31%	42%	30%	40%
Regelmatig (beveiligings)updates doen	47%	34%	47%	35%	43%
Antivirussoftware gebruiken en regelmatig updaten	46%	33%	46%	32%	48%
Controleren op welke links ik klik	41%	32%	41%	31%	40%
Direct software updates uitvoeren	41%	33%	41%	32%	39%
Mijn wachtwoorden regelmatig veranderen	40%	32%	37%	31%	33%
Het standaard wachtwoord van mijn wifi modem veranderen (in een sterk en uniek wachtwoord)	38%	23%	35%	25%	30%
Een firewall installeren	37%	30%	37%	32%	35%
Geen gebruik maken van openbare wifi-netwerken	37%	28%	31%	26%	31%
Lange wachtwoorden of wachtzinnen gebruiken van meer dan 12 tekens	36%	31%	38%	30%	31%
Geen gebruik meer maken van onbeveiligde sites om bestanden uit te wisselen	36%	27%	36%	26%	35%
Steeds een nieuw wachtwoord gebruiken dat ik nog niet eerder gebruikt heb	28%	23%	30%	26%	26%
Extensies aan je webbrowser toevoegen om cookies, advertenties en automatisch toegang tot Javascripts te blokkeren	28%	22%	28%	22%	25%
Een wachtwoordmanager gebruiken	26%	16%	24%	17%	19%
Informatie op internet opzoeken over hoe ik veiliger kan worden	25%	17%	26%	18%	23%
Jaarlijks een digitale apk laten uitvoeren	20%	13%	16%	14%	15%
Altijd gebruik maken van een VPN-verbinding	19%	20%	26%	24%	19%
Een specialist inhuren die bij mij thuis langskomt om de digitale veiligheid te verbeteren installeren	11%	8%	8%	7%	9%
Geen van bovenstaande	13%	11%	9%	8%	10%

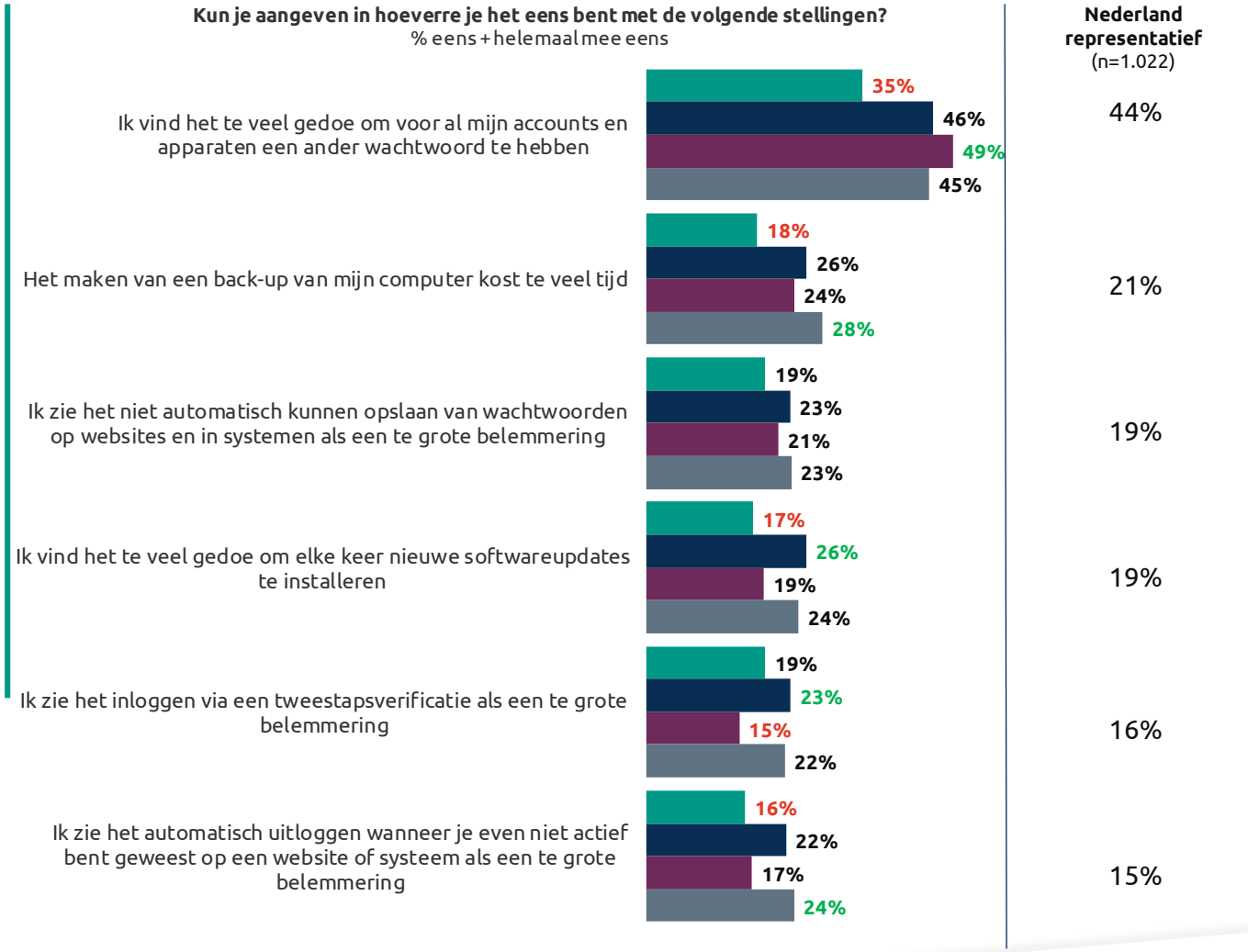
Medewerkers | Digitaal gedrag

Medewerkers klein-MKB ervaren minder vaak belemmeringen in tijd en gemak

Medewerkers in het klein-MKB vinden minder vaak:

- dat het te veel gedoe is om overal een ander wachtwoord voor te hebben (35%) (medewerkers grootbedrijven juist vaker: 49%);
- dat het maken van back-ups te veel tijd kost (18%) (medewerkers vitale infrastructuur juist vaker (28%);
- dat het te veel gedoe is om nieuwe software updates te installeren (17%) (medewerkers in het groot-MKB juist vaker (26%);
- dat het automatisch uitloggen een belemmering is (16%) (medewerkers vitale infrastructuur juist vaker (24%).

Medewerkers in het groot-MKB ervaren het inloggen via een tweestapsverificatie vaker als een te grote belemmering (23%). Medewerkers van grootbedrijven juist minder vaak (15%).

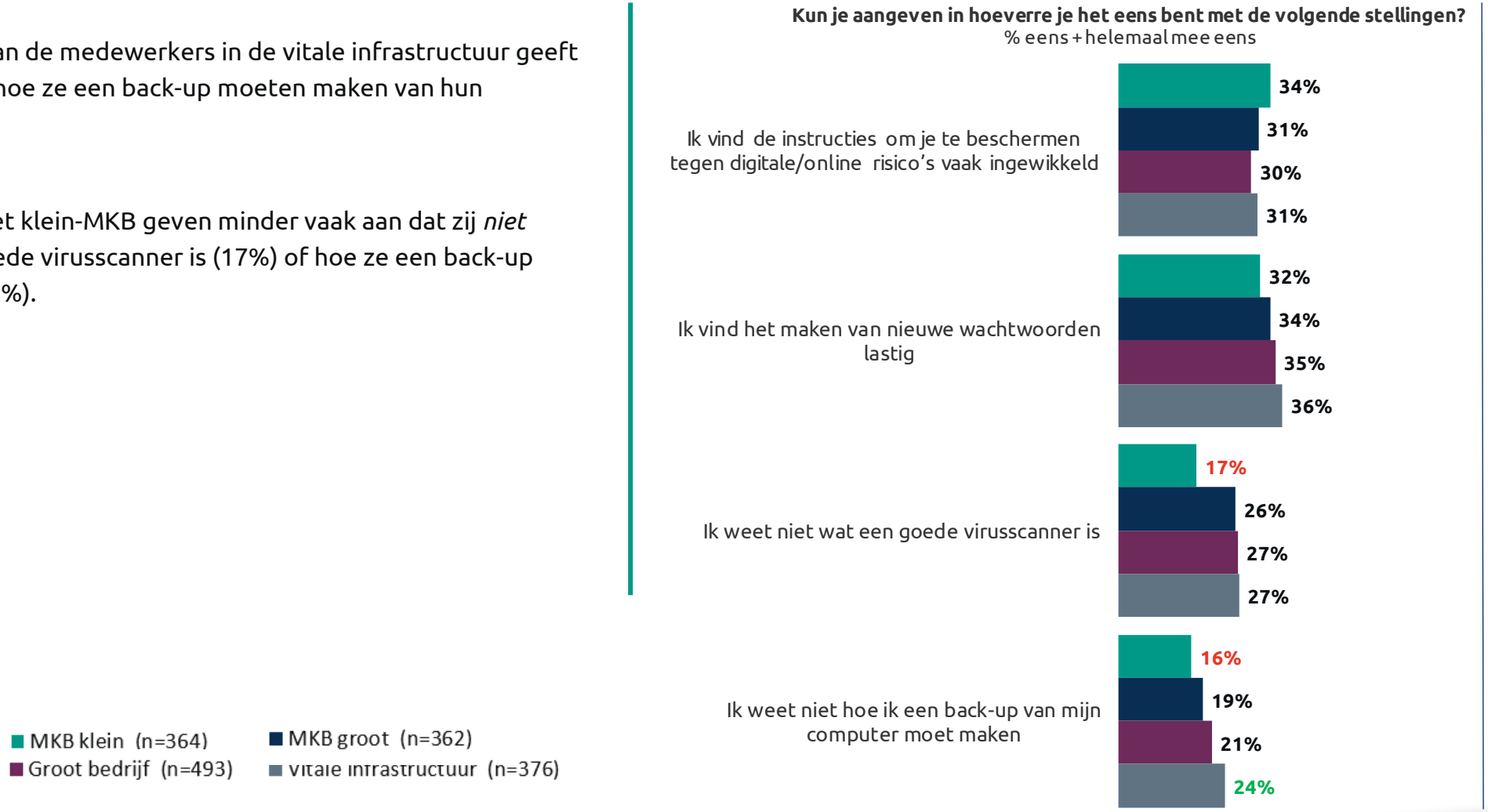


Medewerkers | Digitaal gedrag

Medewerkers vitale infrastructuur geven vaker aan niet te weten hoe ze een back-up van hun computer moeten maken

Een kwart (24%) van de medewerkers in de vitale infrastructuur geeft aan niet te weten hoe ze een back-up moeten maken van hun computer.

Medewerkers in het klein-MKB geven minder vaak aan dat zij *niet* weten wat een goede virusscanner is (17%) of hoe ze een back-up moeten maken (16%).

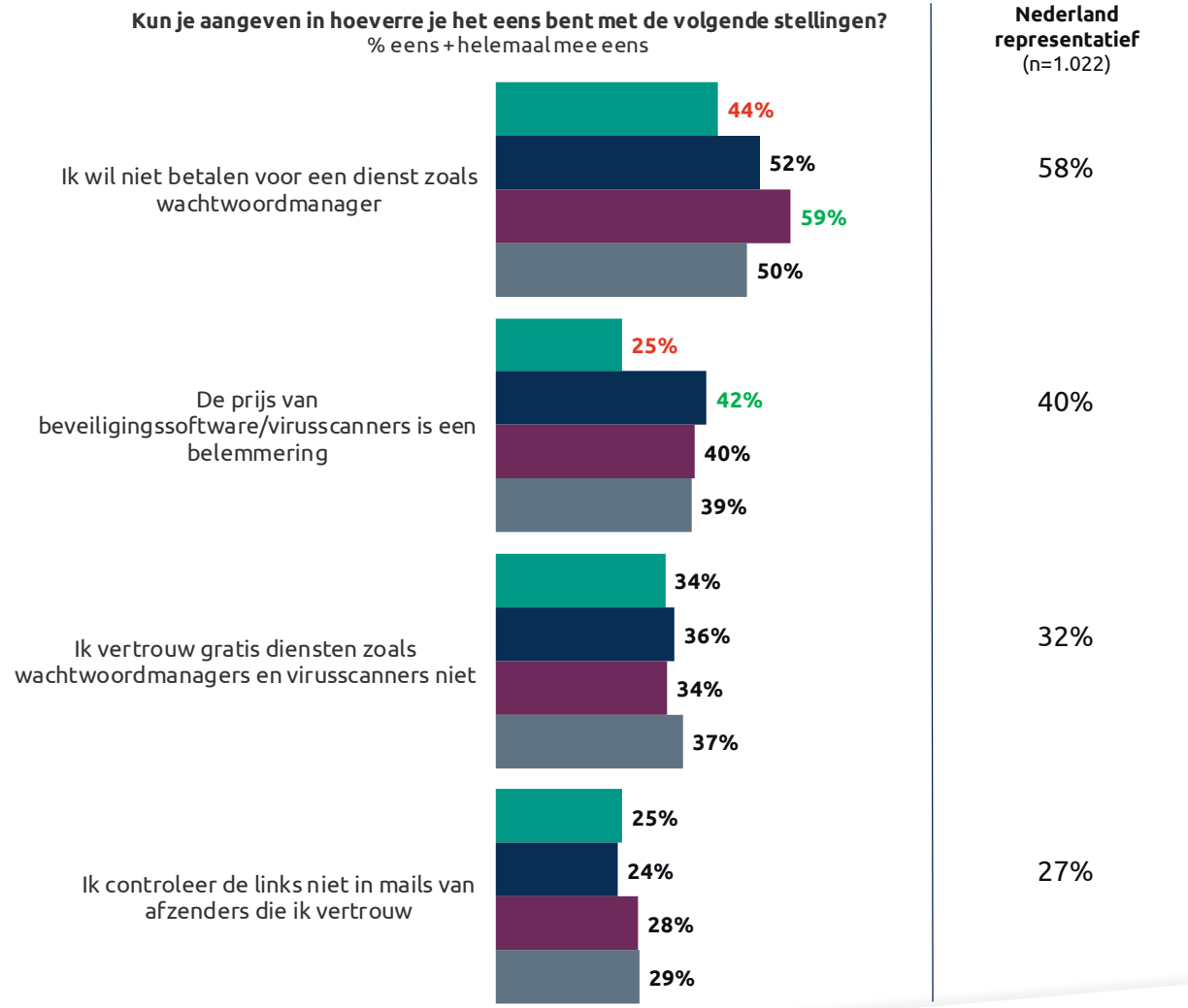


Medewerkers | Digitaal gedrag

Medewerkers klein-MKB ervaren minder financiële belemmeringen

Medewerkers in het klein-MKB geven minder vaak aan dat het voor hen belemmering is om te betalen voor een dienst (44%), medewerkers in het grootbedrijf zien dit het vaakst als belemmering (59%).

De prijs van beveiligingssoftware wordt door medewerkers in het groot-MKB het vaakst als belemmering gezien (42%). In het klein-MKB is de prijs minder vaak een drempel (25%).



Medewerkers | Digitaal gedrag

Medewerkers in het groot-MKB hebben een hogere betaalbereidheid bij een hack via ransomware

In hoeverre zijn de volgende uitspraken van toepassing? % ik doe dit nooit	MKB Klein (n=364)	MKB Groot (n=362)	Grootbedrijf (n=493)	Vitale infrastructuur (n=376)	Nederland representatief (n=1.022)
Als ik gehackt zou worden via ransomware en gevraagd wordt om te betalen om weer toegang tot mijn laptop of pc te krijgen dan zou ik daarvoor betalen	53%	45%	55%	46%	57%
Ik laat mijn kind(eren) gebruikmaken van mijn werklaptop	38%	32%	44%	38%	37%
Ik maak thuis gebruik van een extern opslagapparaat dat continu online is	30%	26%	37%	29%	35%
Ik laat mijn kind(eren) gebruikmaken van mijn werktelefoon	36%	32%	42%	37%	33%
Ik verstuur werkbestanden van mijn werk e-mailadres naar mijn privé e-mail	24%	24%	34%	23%	30%
Ik maak op mijn werk regelmatig back-ups van de bestanden op mijn werk laptop	7%	8%	15%	9%	14%
Ik maak thuis regelmatig back-ups van mijn bestanden	4%	4%	7%	5%	7%
Als ik op een link in een phishing e-mail zou klikken dan zou ik mij daar voor schamen	6%	6%	7%	8%	7%
Ik heb de privacy instellingen van mijn social media accounts aangepast ten opzichte van de standaard instellingen	2%	3%	5%	3%	3%
Ik bezoek alleen websites waar een slotje en/of https voor het adres van een website staat	2%	2%	3%	1%	3%
Als ik een openbare computer heb gebruikt dan log ik na gebruik al mijn accounts uit	3%	3%	2%	4%	2%
Mijn werkgever maakt automatisch back-ups van alle bestanden	2%	1%	1%	0%	2%
Als ik door heb dat ik een virus heb gedownload op mijn werkcomputer waardoor andere computers binnen mijn bedrijf besmet raken vertel ik meteen aan anderen wat ik heb gedaan	1%	1%	2%	1%	2%
Als er een slotje en/of https voor het adres van een website staat dan denk ik dat ik die website veilig kan bezoeken	1%	4%	2%	2%	2%

Resultaten medewerkers
Ervaringen met digitale risico’s

Medewerkers | Ervaringen met digitale risico's

Medewerkers vitale infrastructuur komen vaker in aanraking met digitale risico's

Heb je in een werksituatie in de afgelopen 12 maanden weleens te maken gehad met één van de onderstaande voorvallen? % Ikzelf	**MKB Klein (n=364)**	**MKB Groot (n=362)**	**Grootbedrijf (n=493)**	**Vitale infrastructuur (n=376)**	**Nederland representatief (werkend, n=477)**
Mails ontvangen met poging tot phishing	33%	25%	20%	27%	16%
Acquisitiefraude	16%	14%	6%	15%	6%
Benaderd met een social media berichtje met vraag om een onbekende link aan te klikken	12%	10%	10%	15%	7%
Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik die bijna niet van echt te onderscheiden is	8%	10%	6%	13%	5%
Mensen die gegevens opvragen door zich voor te doen als vermoedelijke klant, collega of leverancier	8%	12%	7%	15%	6%
Dat een computer tijdelijk niet werkte door een malware zoals bijvoorbeeld een virus	3%	11%	4%	13%	5%
Dat mijn (bedrijfs-) website tijdelijk niet werkte door b.v. een DDoS-aanval	2%	10%	6%	15%	5%
Ransomware	2%	7%	3%	10%	2%
Iemand in een account heeft ingelogd zonder dat de eigenaar/gebruiker daar toestemming voor gegeven heeft	2%	8%	4%	10%	4%
Iemand in een apparaat heeft ingelogd zonder dat de eigenaar/gebruiker daar toestemming voor gegeven heeft	4%	8%	5%	13%	5%
Een foute link ook daadwerkelijk aangeklikt die een virus, spam, phishing of andere ongewenste poging bevatten	3%	8%	5%	10%	6%
Dat door het downloaden van geïnfecteerde software/bestanden malware verspreid werd	3%	8%	4%	14%	3%
Identiteitsdiefstal	3%	7%	4%	11%	3%
Misbruik van bedrijfsgevoelige gegevens	2%	7%	4%	12%	6%
Geen van bovenstaande	57%	62%	68%	56%	74%

Medewerkers | Ervaringen met digitale risico's

Medewerkers vitale infrastructuur treffen vaker maatregelen na ervaring met een digitaal voorval

Heb je maatregelen getroffen nadat je dit hebt meegemaakt?	MKB Klein (n=171)	MKB Groot (n=158)	Grootbedrijf (n=185)	Vitale infrastructuur (n=187)	Nederland representatief (werkend, n=151)
Ik ben voorzichtiger met het klikken op links	28%	18%	17%	19%	14%
Ik heb het gerapporteerd/ aangifte gedaan	16%	21%	18%	20%	14%
Ik controleer of iemand is die hij/zij zegt te zijn als ik een vreemd verzoek van hem/haar krijg	22%	15%	14%	20%	13%
Ik heb het gemeld bij onze systeembeheerder(s)/IT-afdeling	6%	21%	17%	19%	15%
Ik heb antivirussoftware geïnstalleerd	15%	15%	11%	16%	13%
Ik heb toestemmingen van apps op mijn telefoon beperkt	14%	13%	14%	14%	14%
Ik maak mijn wachtwoorden complexer	15%	16%	11%	11%	12%
Ik controleer of websites HTTPS gebruiken	15%	13%	8%	14%	7%
Ik heb een software update uitgevoerd	15%	11%	11%	14%	6%
Ik deel mijn wachtwoorden niet (meer) met anderen	14%	12%	11%	13%	8%
Ik heb een firewall geïnstalleerd of geüpdatet	11%	15%	11%	12%	12%
Ik heb tweefactorauthenticatie ingesteld op mijn apparaten / accounts	13%	12%	9%	15%	8%
Ik verstuur geen werkgerelateerde bestanden van mijn werk meer naar huis	4%	12%	11%	16%	11%
Ik maak nu back-ups van de bestanden op mijn laptop	10%	12%	8%	12%	7%
Ik maak nu back-ups van mijn tablet	11%	10%	8%	10%	7%
Ik maak nu back-ups van mijn smartphone	5%	10%	8%	14%	2%
Ik ben een wachtwoordmanager gaan gebruiken	6%	12%	6%	13%	7%
Ik ben nu een VPN-verbinding gaan gebruiken via mijn laptop	4%	8%	11%	14%	8%
Ik ben nu een VPN-verbinding gaan gebruiken via mijn smartphone	4%	11%	5%	12%	5%
Ik versleutel mijn harde schijf	2%	9%	5%	15%	3%
Ik ben nu een VPN-verbinding gaan gebruiken via mijn tablet	5%	11%	4%	9%	7%
Ik gebruik apps om meer controle te krijgen over het besturingssysteem dan de fabrikant toestaat	4%	6%	8%	8%	7%
Anders, namelijk:	6%	5%	4%	2%	3%
Geen van bovenstaande, ik heb niets gedaan	35%	27%	37%	23%	40%

Resultaten medewerkers
Digitale veiligheid op de werkvloer

Medewerkers | Afspraken op de werkvloer

Medewerkers in het klein-MKB hebben minder vaak werkafspraken over online veilig gedrag

Welke afspraken zijn er binnen jouw bedrijf/ organisatie gemaakt over hoe je je online veilig gedraagt?	MKB Klein (n=364)	MKB Groot (n=362)	Grootbedrijf (n=493)	Vitale infrastructuur (n=376)	Werkend Nederland (n=477)
Er zijn afspraken gemaakt over het gebruikmaken van websites en/of e-mail	20%	29%	47%	42%	33%
Er zijn afspraken gemaakt over het veilig versturen/uitwisselen van bestanden	21%	28%	47%	41%	35%
Er zijn afspraken gemaakt over het versturen/uitwisselen van persoonsgegevens	17%	25%	43%	37%	31%
Er zijn afspraken gemaakt over het gebruikmaken van opslagmedia als usb-sticks of externe harde schijven	17%	25%	39%	38%	26%
Er zijn afspraken gemaakt over het gebruik van zakelijke smartphones, laptops, tablets	14%	24%	39%	34%	25%
Alleen de systeembeheerders kunnen software installeren	14%	23%	40%	31%	31%
Er zijn afspraken gemaakt over het gebruikmaken van sociale media	14%	22%	35%	31%	27%
De toegang tot bepaalde websites en/of socialemediakanalen is geblokkeerd	9%	17%	38%	34%	17%
De toegang tot bepaalde socialemediakanalen is geblokkeerd	5%	9%	23%	18%	27%
De toegang tot bepaalde verzendplatforms is geblokkeerd	5%	7%	23%	18%	16%
Het gebruik van USB-sticks in onze organisatie is onmogelijk gemaakt	4%	8%	20%	16%	14%
Anders, namelijk:	9%	2%	3%	1%	3%
Weet ik niet	11%	14%	14%	10%	18%
In mijn bedrijf/organisatie zijn geheel geen afspraken gemaakt over hoe je je online veilig gedraagt	44%	19%	6%	7%	13%

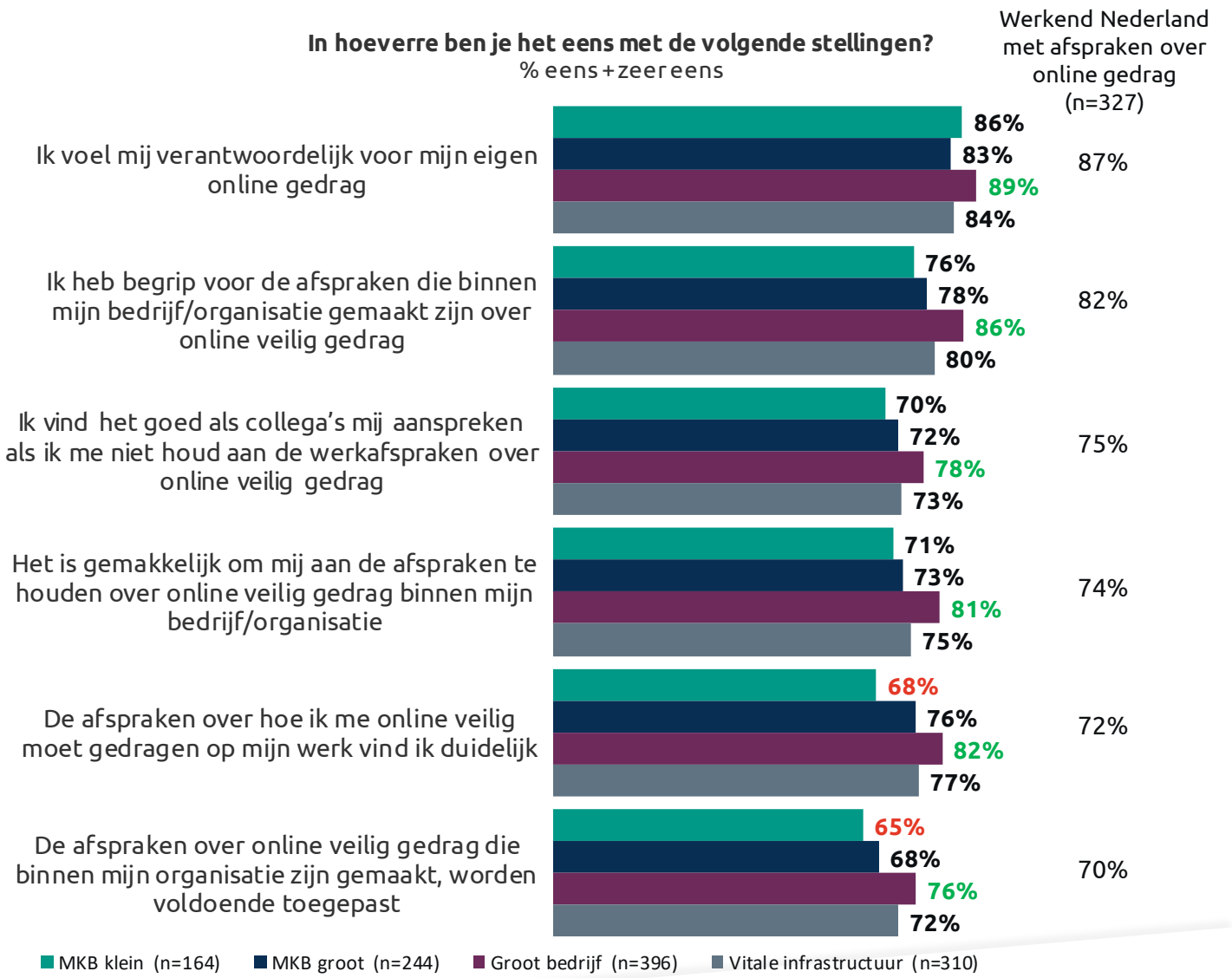
Medewerkers | Digitale veiligheid op de werkvloer

Breder draagvlak onder medewerkers grootbedrijven als het gaat om afspraken over veilig online gedrag

Medewerkers bij grootbedrijven geven vaker aan:

- dat ze zich verantwoordelijk te voelen voor hun online gedrag (89%);
- dat ze begrip hebben voor de gemaakte afspraken (86%);
- dat ze vinden dat anderen hen mogen aanspreken om hun online gedrag (78%);
- dat het makkelijk is om je aan afspraken te houden (81%);
- dat afspraken duidelijk zijn (82%);
- dat de afspraken voldoende worden toegepast (76%).

Medewerkers in het klein-MKB vinden minder vaak dat afspraken over veilig online gedrag duidelijk zijn (68%) en vinden minder vaak dat de afspraken voldoende worden toegepast in hun bedrijf/organisatie (65%).



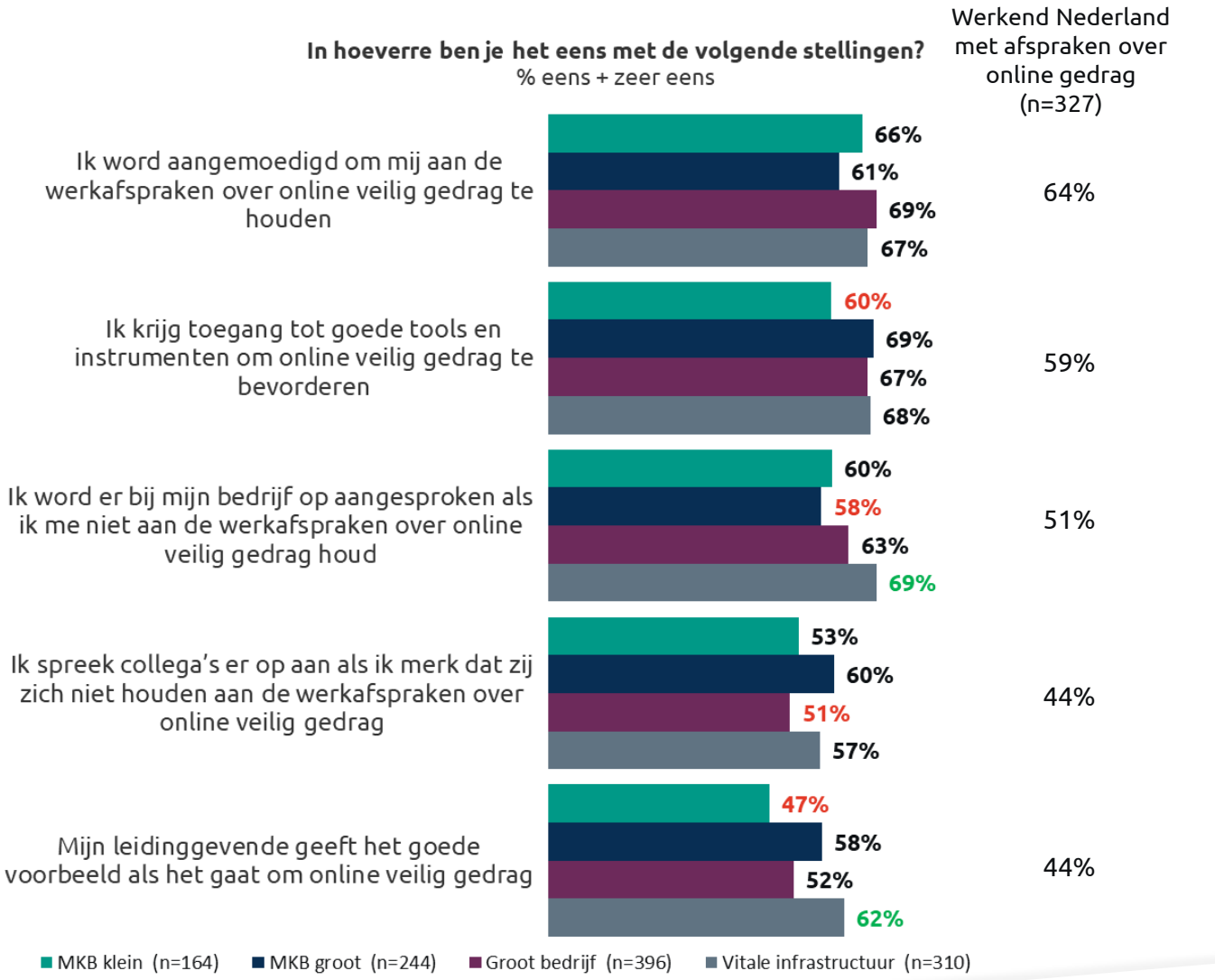
Medewerkers | Digitale veiligheid op de werkvloer

Medewerkers klein-MKB missen vaker de goede tools en instrumenten om veilig online gedrag te bevorderen

Medewerkers in het klein-MKB geven minder vaak aan toegang te hebben tot goede tools en instrumenten om online veilig gedrag te bevorderen (60%). Ook geven zij minder vaak aan dat hun leidinggevende het goede voorbeeld geeft (47%).

Medewerkers in de vitale infrastructuur geven juist vaker aan dat hun leidinggevende het goede voorbeeld geeft (62%). Ze ervaren ook vaker dat ze aangesproken worden als ze zich niet houden aan de gemaakte werkafspraken (69%). Medewerkers in het groot-MKB ervaren dit juist minder vaak (58%).

Medewerkers in grootbedrijven geven minder vaak aan dat zij collega's aanspreken op hun gedrag (51%).



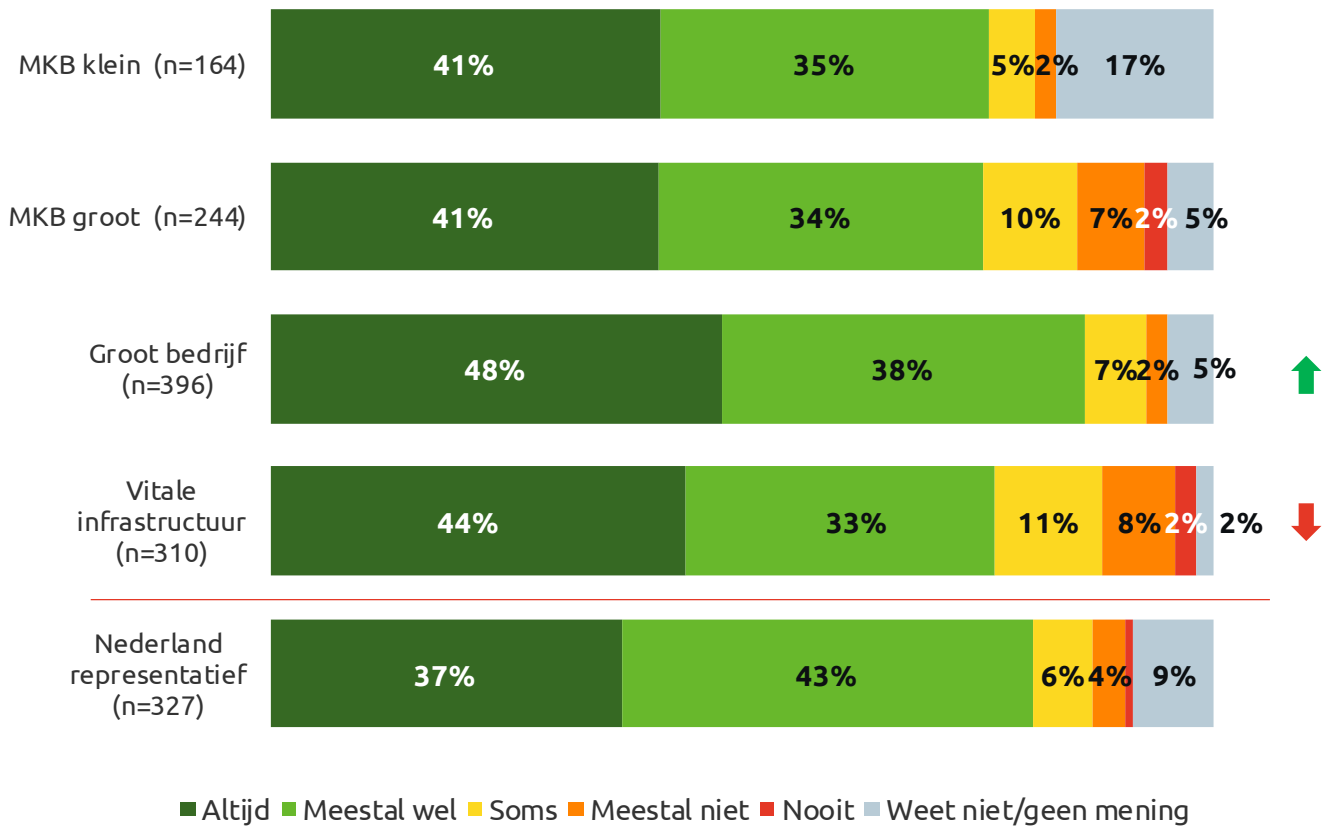
Medewerkers | Digitale veiligheid op de werkvloer

Medewerkers groot-MKB en vitale infrastructuur hebben wat vaker moeite om zich aan de afspraken

Medewerkers in het groot-MKB geven wat vaker aan dat zij zich meestal niet of nooit aan gemaakte werkafspraken omtrent veilig online gedrag houden (9%). Dit zien we ook terug bij medewerkers in de vitale infrastructuur (10%).

Medewerkers in grootbedrijven geven vaker aan dat zij zich altijd of meestal wel houden aan de gemaakte afspraken (86%).

In hoeverre houd jij je aan de afspraken die binnen jouw bedrijf/organisatie gemaakt zijn over hoe je je online veilig gedraagt?
(Basis - Werkend met afspraken over online veilig gedrag)



Significant verschil t.o.v. de andere medewerkersgroepen

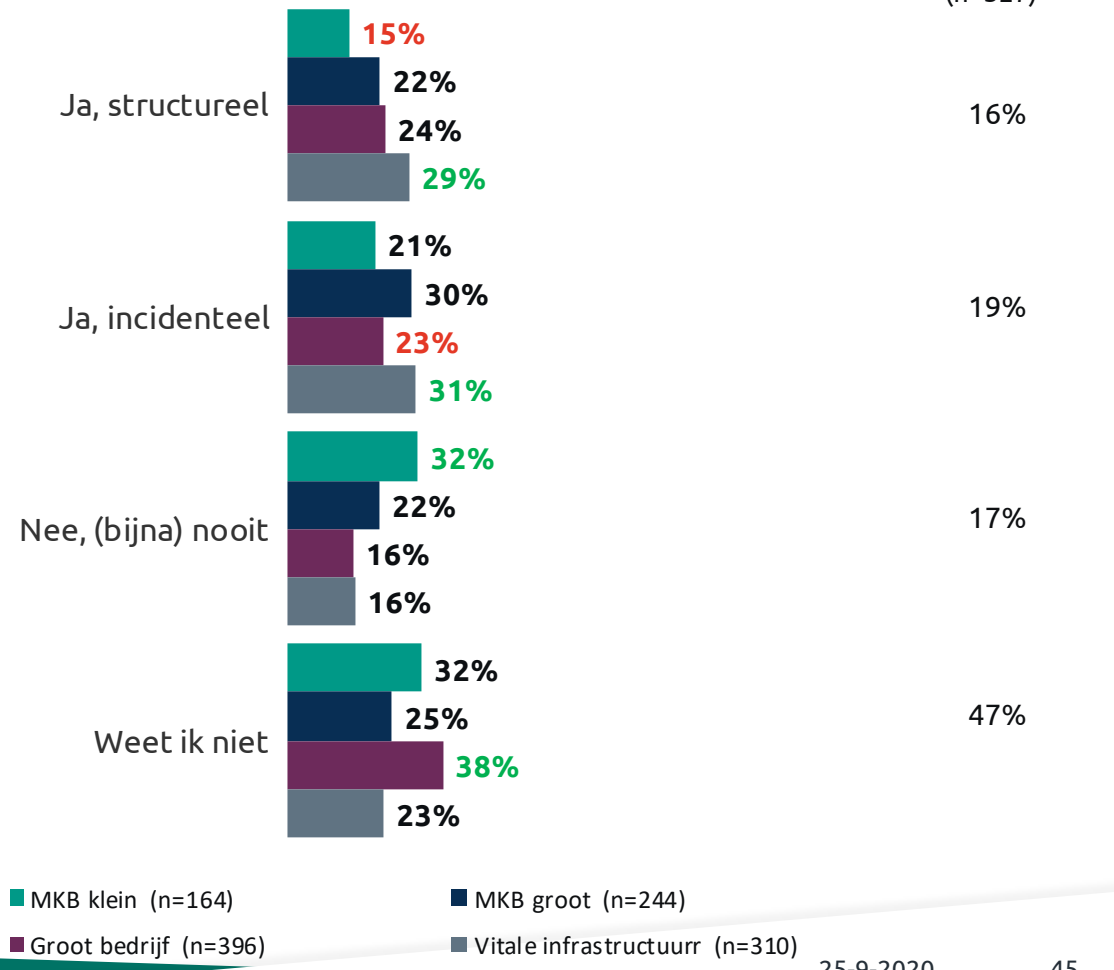
Medewerkers | Digitale veiligheid op de werkvloer

Veilig online gedrag wordt minder gemonitord onder medewerkers in het klein-MKB

Medewerkers in het klein-MKB geven minder vaak aan dat er binnen hun bedrijf/organisatie structureel wordt gemeten of medewerkers zich aan de gemaakte afspraken houden. Zij geven juist vaker aan dat er (bijna) nooit wordt gemeten.

Onder medewerkers in de vitale infrastructuur wordt vaker structureel (29%) of incidenteel (31%) het compliance gedrag gemeten.

Wordt binnen jouw bedrijf of organisatie gemeten in hoeverre medewerkers zich aan de afspraken voor online veilig gedrag houden? (Basis - Werkend met afspraken over online veilig gedrag)



Medewerkers | Digitale veiligheid op de werkvloer

Medewerkers in het klein-MKB ervaren minder vaak belemmeringen om afspraken rondom veilig online gedrag te borgen

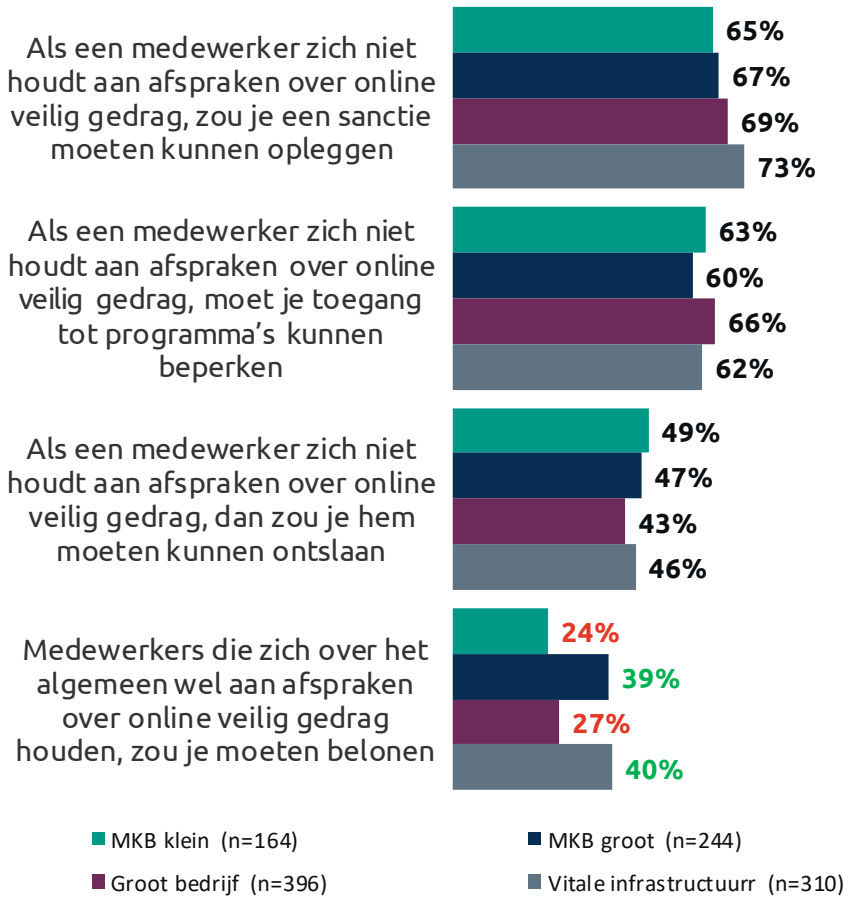
Welke belemmeringen ervaar je binnen jouw bedrijf bij het borgen van de afspraken voor online veilig gedrag? Basis – Werkend met afspraken over online veilig gedrag	**MKB Klein (n=164)**	**MKB Groot (n=244)**	**Grootbedrijf (n=396)**	**Vitale infrastructuur (n=310)**	**Werkend Nederland (n=327)**
Er wordt niet duidelijk over gecommuniceerd	7%	14%	13%	12%	13%
Te weinig tijd	10%	13%	9%	13%	9%
Er wordt geen prioriteit aan gegeven	9%	9%	13%	11%	12%
Er wordt niet voldoende over gecommuniceerd	9%	9%	14%	9%	13%
Er wordt niet aansprekend over gecommuniceerd	5%	9%	12%	12%	9%
Er wordt niet eenduidig over gecommuniceerd	4%	10%	12%	11%	12%
Het is onduidelijk bij wie de borging hiervan ligt	7%	9%	11%	10%	10%
Te weinig mankracht	8%	11%	7%	9%	7%
Gebrek aan draagvlak vanuit het management	7%	7%	8%	10%	6%
Te weinig kennis binnen de organisatie	11%	8%	6%	5%	7%
Te weinig budget	10%	7%	6%	7%	7%
Geen van deze/geen belemmeringen	64%	46%	53%	46%	54%

Medewerkers | Digitale veiligheid op de werkvloer

Met name verschillen in houding naar belonen van goed gedrag

Medewerkers in het klein-MKB en bij grootbedrijven vinden minder vaak dat medewerkers beloond zouden moeten worden als ze zich aan gemaakte afspraken houden omtrent veilig online gedrag. Medewerkers in het groot-MKB en van vitale infrastructuur juist vaker.

In hoeverre ben je het hiermee eens? % eens + zeer eens
(Basis - Werkend met afspraken over online veilig gedrag)



Werkend Nederland met afspraken over online gedrag (n=327)

65%

61%

40%

28%

Resultaten ICT-verantwoordelijken

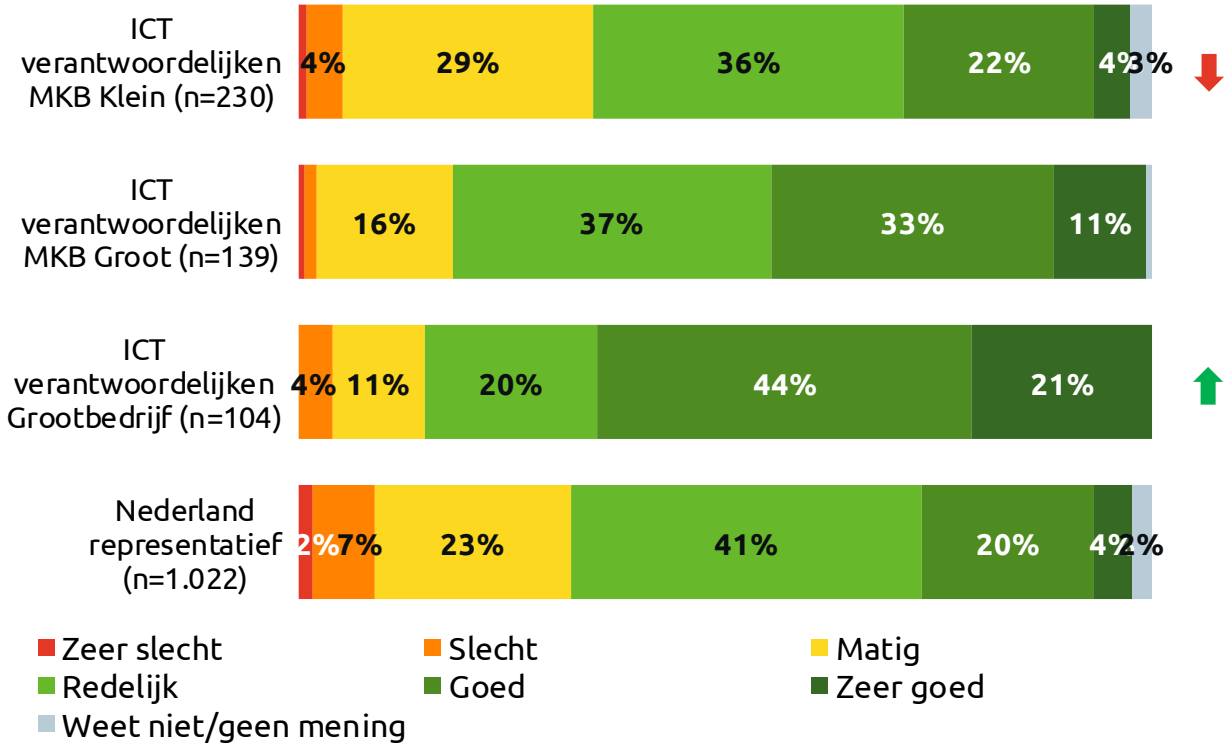
Resultaten ICT-verantwoordelijken
Kennis over Digitale risico's

ICT-verantwoordelijken | Kennis over digitale risico's

ICT verantwoorden schatten hun kennisniveau vaker in als 'goed'

ICT-verantwoordelijken schatten hun kennis over digitale en online veiligheid (zoals te verwachten valt) vaker in als goed tot zeer goed. Met name verantwoordelijken van grootbedrijven schatten hun kennis als hoog in.

Hoe schat jij je eigen kennis over digitale en online veiligheid in?



*Percentages < 2% worden t.b.v. de leesbaarheid niet getoond in de grafiek

Significant verschil t.o.v. de andere medewerkersgroepen

ICT-verantwoordelijken | Kennis over digitale risico's

Hoge bekendheid met de verschillende digitale risico's

ICT-verantwoordelijken zijn beter bekend met de digitale risico's in vergelijking met het Nederlands publiek. Met name ICT-verantwoordelijken van grootbedrijven kennen veel digitale risico's.

De ICT'ers van klein-MKB zijn in verhouding met wat minder digitale risico's bekend.

Kun je aangeven in welke mate je bekend bent met de onderstaande zaken? % weleens mee te maken gehad + ik weet wat dit is	ICT-verantwoordelijken klein-MKB (n=230)	ICT-verantwoordelijken groot-MKB (n=139)	ICT-verantwoordelijken Grootbedrijf (n=104)	Nederland representatief (n=1.022)
Phishing	93%	88%	91%	83%
Malware	81%	81%	93%	65%
Hacking	93%	86%	92%	88%
Ransomware	72%	77%	90%	52%
Helpdeskfraude	70%	77%	83%	57%
Vriend-in-nood-fraude	77%	67%	78%	62%
Identiteitsfraude	94%	84%	94%	89%
DDos-aanval	78%	75%	86%	59%
Spoofing	34%	56%	61%	24%
Botnet	32%	49%	61%	19%
Cryptojacking	35%	55%	63%	26%

ICT-verantwoordelijken | Kennis over digitale risico's

Klein-MKB schat de kans op schade als gevolg van phishing lager in

Over het algemeen lijkt het dat ICT-verantwoordelijken ongeveer een even hoge kans-inschatting maken op computerschade of financiële schade in de werksituatie.

Wel geven ICT-verantwoordelijken in het klein-MKB een lagere kans-inschatting voor phishing, DDos-aanval, spoofing en cryptojacking. Grootbedrijven geven juist voor DDos-aanval een hogere risico-inschatting.

Hoe groot acht je de kans dat je in jouw werksituatie computer/financiële schade oploopt, geen gebruik kunt maken van je computer als gevolg hiervan? *% groot + zeer groot* Basis – is bekend met digitaal risico	**ICT-verantwoordelijken klein-MKB**	**ICT-verantwoordelijken groot-MKB**	**ICT-verantwoordelijken Grootbedrijf**	**Nederland representatief**
Phishing	**8%**	14%	17%	**8%**
Malware	7%	13%	9%	**10%**
Hacking	8%	10%	7%	**13%**
Ransomware	7%	11%	9%	**12%**
Helpdeskfraude	4%	10%	7%	**11%**
Vriend-in-nood-fraude	4%	9%	5%	**7%**
Identiteitsfraude	9%	11%	8%	**10%**
DDos-aanval	**4%**	12%	**13%**	**13%**
Spoofing	**3%**	14%	11%	**5%**
Botnet	4%	12%	11%	**8%**
Cryptojacking	**4%**	14%	11%	**6%**

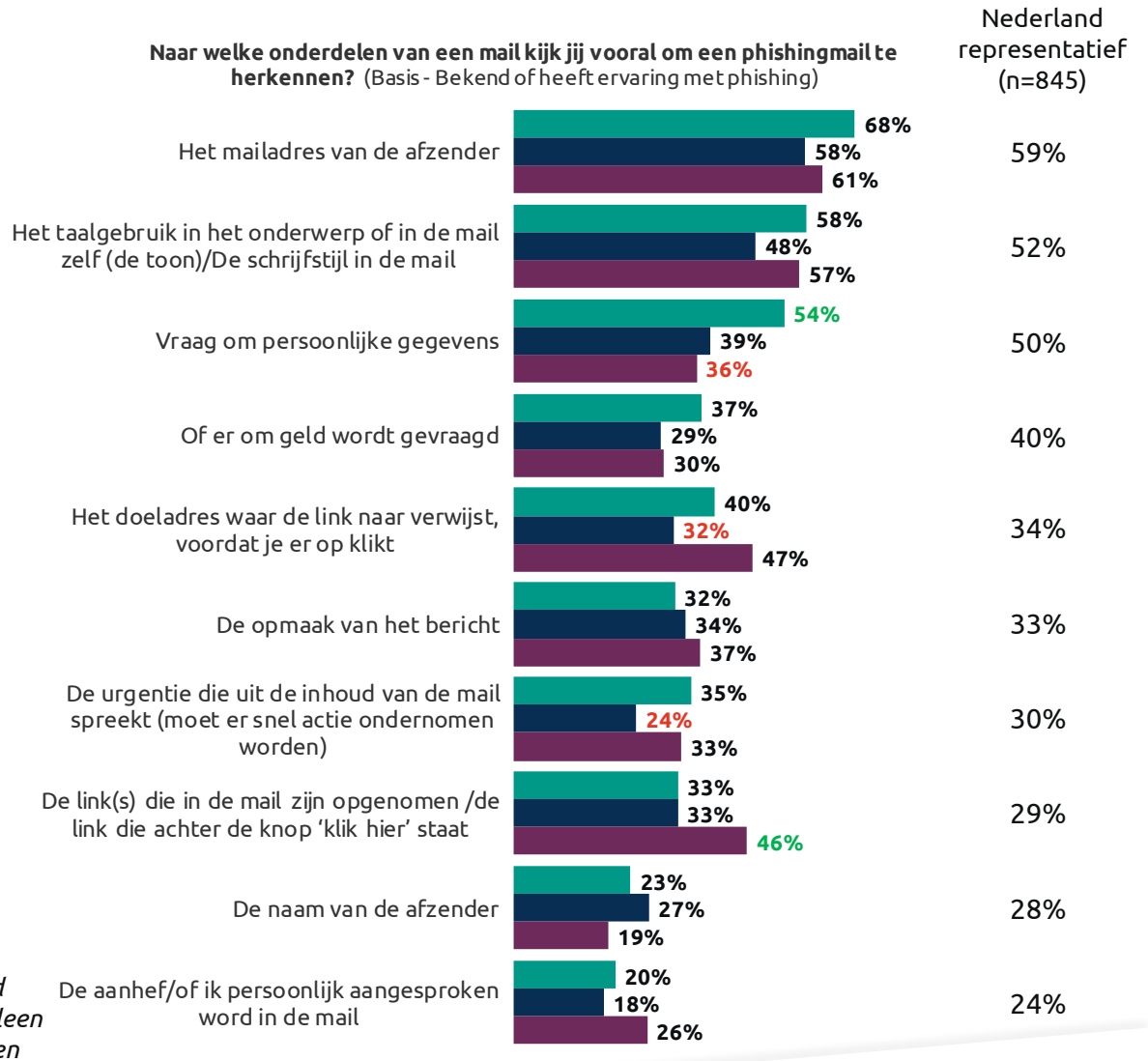
ICT-verantwoordelijken | Kennis over digitale risico's

Grootbedrijven controleren minder vragen om persoonlijke gegevens om phishing mails te herkennen

Om phishingmails te ontmaskeren letten ICT-verantwoordelijken met name op het afzendadres en het taalgebruik/schrijfstijl van de mail.

Verder let klein-MKB vaker op de vraag om persoonlijke gegevens te delen (54%). Grootbedrijven doen dit opvallend minder vaak (36%). Grootbedrijven letten daarentegen wel vaker op links in mails (46%).

ICT-verantwoordelijken in groot-MKB bedrijven geven minder vaak aan dat zij letten op het doeladres waar de link naar verwijst (32%) en de urgentie van mails (24%) dan klein-MKB en grootbedrijven.

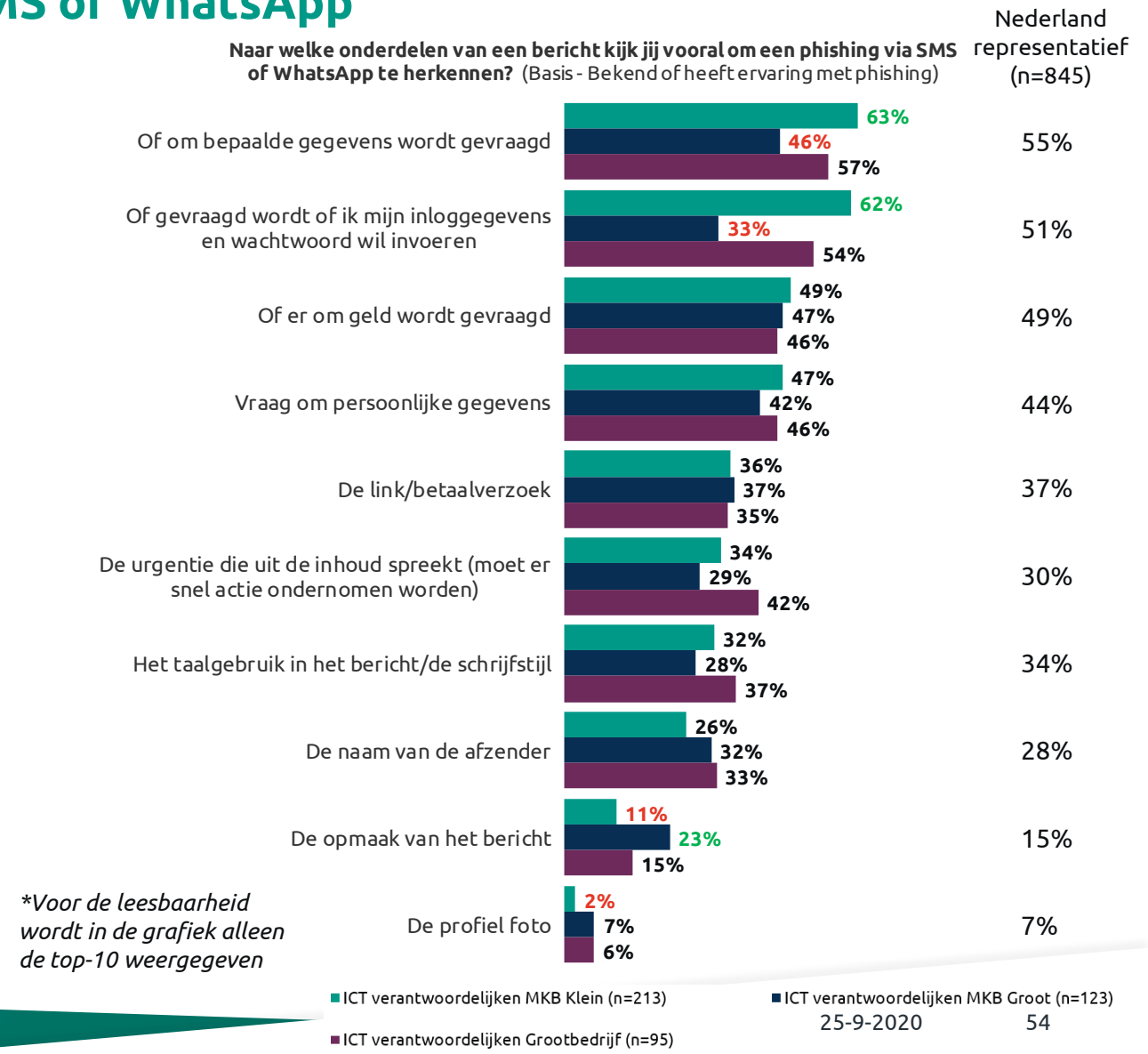


**Voor de leesbaarheid wordt in de grafiek alleen de top-10 weergegeven*

ICT-verantwoordelijken | Kennis over digitale risico's

ICT-verantwoordelijken groot-MKB letten minder op de vraag om bepaalde gegevens en inloggegevens bij phishing via SMS of WhatsApp

Om phishingberichten te ontmaskeren letten ICT-verantwoordelijken met name op of er om bepaalde gegevens wordt gevraagd of om inloggegevens. Met name ICT'ers van klein-MKB letten hier op (respectievelijk 63% en 62%). groot-MKB let juist minder op deze vraag (46% en 33%).



**Voor de leesbaarheid wordt in de grafiek alleen de top-10 weergegeven*

ICT-verantwoordelijken | Kennis over digitale risico's

ICT-verantwoordelijken grootbedrijven gebruiken meer soorten digitale beveiligingsopties

Met name ICT-verantwoordelijken van grootbedrijven maken vaker van verschillende opties gebruik. In het klein-MKB gebruiken ICT-verantwoordelijken het minst vaak tenminste één van de opties.

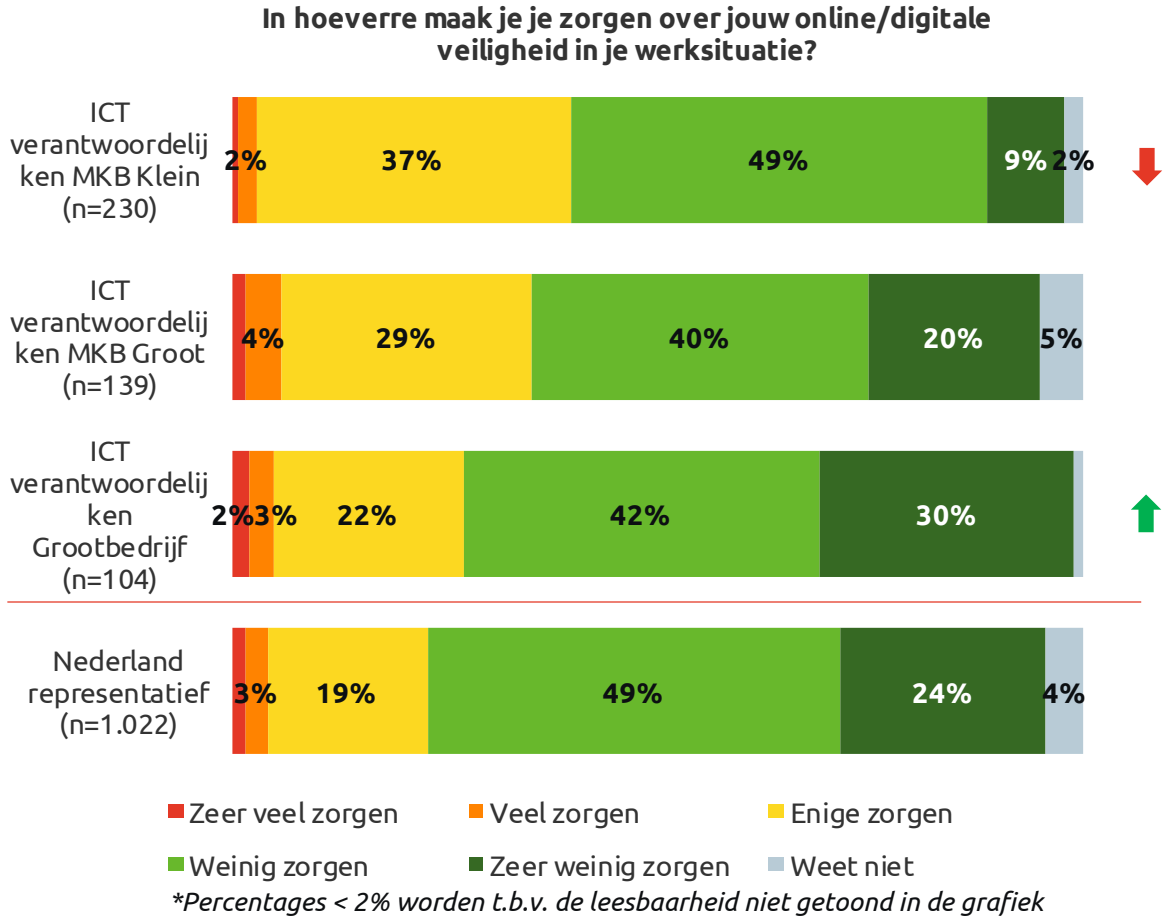
Kun je aangeven in welke mate je bekend bent met onderstaande zaken? *% ja, gebruik ik*	ICT-verantwoordelijken klein-MKB (n=230)	ICT-verantwoordelijken groot-MKB (n=139)	ICT-verantwoordelijken Grootbedrijf (n=104)	Nederland representatief (n=1.022)
Virusscanner	86%	72%	85%	81%
Het maken van back-ups van je gegevens	83%	68%	81%	68%
Automatische updates	83%	71%	76%	78%
Tweestapsverificatie	72%	68%	81%	64%
Cloud diensten	57%	60%	69%	43%
Voor elk account en apparaat een ander wachtwoord gebruiken	63%	52%	60%	52%
Instellingen om cookies te blokkeren/ uit te zetten	58%	55%	69%	47%
Gebruik van lange wachtwoorden (wachtzinnen)	53%	58%	58%	52%
Ad-blocker	46%	49%	59%	37%
Spyware scanner	46%	43%	56%	32%
Biometrische online bescherming	33%	42%	55%	34%
Digitaal wachtwoordenkluisje/ wachtwoordmanager	32%	42%	45%	26%
VPN-verbindingen	29%	47%	62%	25%
Web tracking blocker	28%	30%	45%	16%
Open source hardware- en software	21%	26%	33%	15%

Resultaten ICT-verantwoordelijken
Zorgen om Digitale veiligheid

ICT-verantwoordelijken | Zorgen digitale veiligheid

Gemiddeld meer zorgen om digitale veiligheid bij klein-MKB

ICT-verantwoordelijken in het klein-MKB maken zich vaker zorgen over hun online/digitale veiligheid in de werksituatie (40%). ICT-verantwoordelijken van grootbedrijven ervaren juist minder zorgen (27%).



*Percentages < 2% worden t.b.v. de leesbaarheid niet getoond in de grafiek

Significant verschil t.o.v. de andere medewerkersgroepen

ICT-verantwoordelijken | Zorgen digitale veiligheid

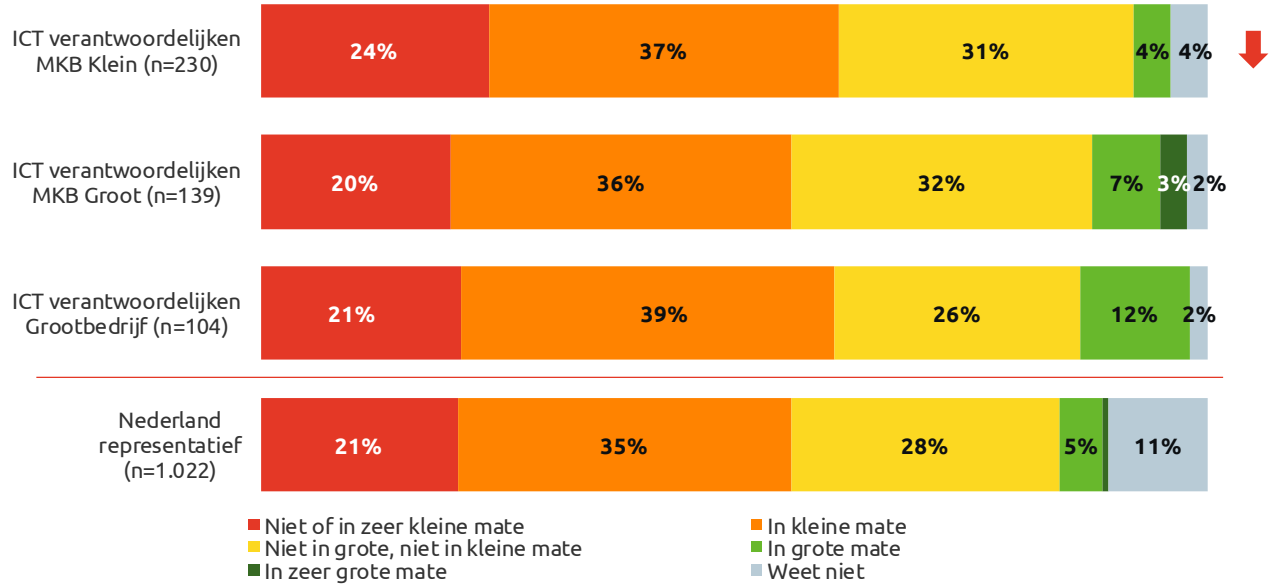
MKB groot en grootbedrijven maken zich in iets grotere mate zorgen om cyberaanvallen

ICT-verantwoordelijken in het MKB groot en grootbedrijven geven vaker aan zich in grotere mate zorgen te maken (10% en 12%). ICT-verantwoordelijken in het MKB klein maken zich beduidend minder in grote mate zorgen (4%). Zij evenaren daarmee het niveau van het Nederlandse publiek (5%).

Cyberaanval
Onder een cyberaanval verstaan we een digitale aanval die tot gevolg heeft dat:

- een ICT-systeem niet meer betrouwbaar werkt
- een ICT-systeem tijdelijk niet beschikbaar is
- de informatie die opgeslagen is op het ICT-systeem gestolen wordt of aangetast wordt zodat het niet meer bruikbaar is

In welke mate maak je je zorgen dat je zelf te maken krijgt met een cyberaanval?



Percentages < 2% worden t.b.v. de leesbaarheid niet getoond in de grafiek

Significant verschil t.o.v. de andere medewerkersgroepen

Resultaten ICT-verantwoordelijken
Digitaal gedrag

ICT-verantwoordelijken | Digitaal gedrag

Grotere bedrijven maken vaker gebruik van VPN- en/of cloudverbinding

Op welk van onderstaande locaties heb je in de afgelopen 12 maanden gewerkt (denk hierbij ook aan 'nieuwe' werkplekken door het coronavirus)?

	Thuis	Kantoor	Openbare plek
ICT-verantwoordelijken MKB Klein (n=230)	79%	**42%**	20%
ICT-verantwoordelijken MKB Groot (n=139)	**72%**	**84%**	**11%**
ICT-verantwoordelijken Grootbedrijven (n=104)	**86%**	**86%**	19%

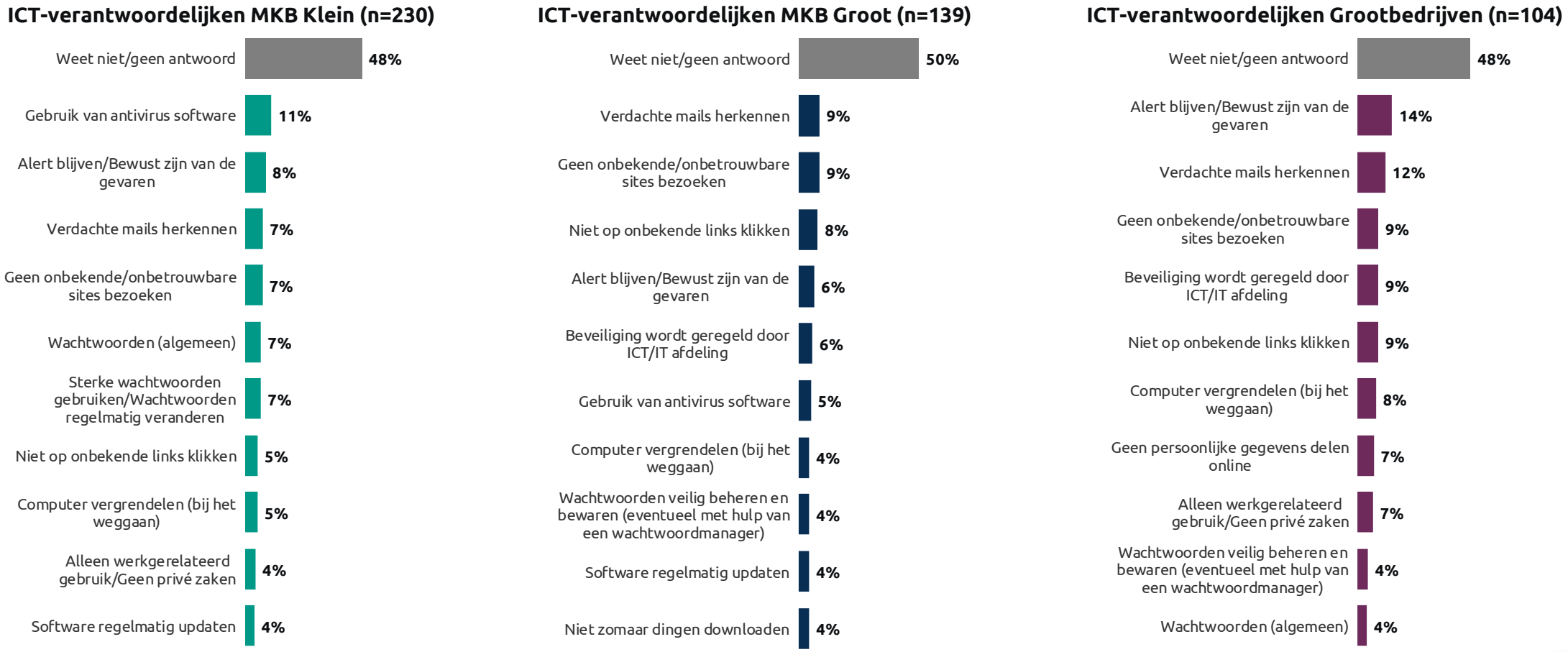
Van wat voor netwerkverbinding maak je <u>thuis</u> gebruik?

	klein-MKB n=181	groot-MKB n=100	Grootbedrijf n=89
Een (wifi-)netwerkverbinding met wachtwoord	**85%**	**65%**	**65%**
Een (wifi-)netwerkverbinding zonder wachtwoord	6%	5%	2%
Een VPN verbinding en/of cloud verbinding ('in de cloud werken')	**8%**	**25%**	**29%**
Een hotspot verbinding (3G/4G) via mijn smartphone of tablet	0%	2%	0%
Anders	1%	2%	2%
Weet ik niet	1%	1%	1%

ICT-verantwoordelijken | Digitaal gedrag

Meesten kunnen spontaan niet benoemen wat veilig online gedrag is

Waar denk jij in eerste instantie aan bij veilig online gedrag op je werk?



**Deze vraag is open gesteld en achteraf gecodeerd. Voor de leesbaarheid wordt in de grafiek alleen de top-10 weergegeven*

ICT-verantwoordelijken | Digitaal gedrag

ICT-verantwoordelijken van klein-MKB vinden vaker dat ze (nog) niet goed omgaan met digitale zaken

ICT verantwoordelijken van grootbedrijven geven vaker aan dat ze zeer goed omgaan met digitale zaken. In vergelijking met hen geven ICT-verantwoordelijken van het klein-MKB aan dat ze het wat minder goed doen.

In welke mate ga je veilig om met de volgende zaken? *% zeer goed + uitstekend*	**ICT-verantwoordelijken klein-MKB (n=230)**	**ICT-verantwoordelijken groot-MKB (n=139)**	**ICT-verantwoordelijken Grootbedrijf (n=104)**	**Nederland representatief (n=1.022)**
Het updaten van mijn software updates	49%	54%	66%	39%
Het laten gebruiken van jouw devices door anderen	48%	48%	59%	35%
Omgaan met nepmails met poging tot phishing mails	43%	45%	62%	38%
Het bewaren van mijn wachtwoorden	34%	42%	53%	29%
Het gebruik van verschillende wachtwoorden	34%	40%	55%	28%
Het beperken van schade door diefstal, beschadiging of verwijdering door het maken van back-ups	33%	40%	47%	23%
Het beheren en gebruik maken van persoons- en klantgegevens	26%	42%	46%	26%
Het gebruik van USB-sticks	25%	34%	43%	23%
Het afgeven van toestemmingen op websites	24%	30%	42%	19%
Het afgeven van toestemmingen op webshops	21%	40%	38%	18%
Het gebruik maken van een wifi verbinding terwijl je onderweg bent	19%	29%	40%	18%
Het werken in een cloud	17%	34%	42%	16%

ICT-verantwoordelijken | Digitaal gedrag

ICT-verantwoordelijken van grotere bedrijven geven zichzelf een gemiddeld hoger cijfer voor hun eigen gedrag

ICT-verantwoordelijken vinden dat ze zelf goed omgaan met online gevaren. Dat blijkt uit de goede voldoendes die ze zichzelf geven. Met name ICT-verantwoordelijken in het groot-MKB en van grootbedrijven beoordelen zichzelf als goed.

Als toelichting op hun cijfer geven ICT-verantwoordelijken aan dat zij goed op de hoogte zijn of hun beveiliging goed op orde hebben.

Welk cijfer geef jij jezelf als het gaat om het veilig omgaan met online gevaren?
(gemiddelde)

Kun je toelichten waarom je jezelf dit cijfer geeft? (Top 5*)

28%	Ik ben goed op de hoogte/Ik heb alles op orde	31%	Ik ben goed op de hoogte/Ik heb alles op orde	34%	Ik ben goed op de hoogte/Ik heb alles op orde
22%	**Er is (altijd) ruimte voor verbetering**	24%	Weet niet/geen antwoord	21%	Ik ben alert/bewust van de gevaren/voorzichtig
20%	Ik ben alert/bewust van de gevaren/voorzichtig	15%	Ik ben alert/bewust van de gevaren/voorzichtig	13%	**Ik heb ervaring in de ict/it security**
8%	Ik heb hier geen/weinig verstand van	9%	**Er is (altijd) ruimte voor verbetering**	11%	Er is (altijd) ruimte voor verbetering
7%	Ik ben hier niet bewust mee bezig/Ik ben (soms) te laks	7%	Ik ben hier niet bewust mee bezig/Ik ben (soms) te laks	8%	**De online wereld/criminaliteit verandert constant**

*Deze vraag is open gesteld en achteraf gecodeerd.

ICT-verantwoordelijken | Digitaal gedrag

ICT-verantwoordelijken van groot-MKB maken het minst gebruik van de verschillende beveiligingsopties

Welke van de onderstaande acties heb je ondernomen of doe je om jouw online veiligheid te verbeteren?	ICT-verantwoordelijken klein-MKB (n=230)	ICT-verantwoordelijken groot-MKB (n=139)	ICT-verantwoordelijken Grootbedrijf (n=104)	Nederland representatief (n=1.022)
Antivirussoftware gebruiken en regelmatig updaten	73%	50%	67%	58%
Regelmatig (beveiligings)updates doen	63%	46%	68%	51%
Regelmatig back-ups maken van al mijn bestanden	62%	45%	66%	42%
Controleren op welke links ik klik	60%	45%	66%	50%
Direct software updates uitvoeren	54%	42%	64%	44%
Een firewall installeren	52%	41%	51%	32%
Mijn wachtwoorden regelmatig veranderen	39%	40%	57%	33%
Geen gebruik meer maken van onbeveiligde sites om bestanden uit te wisselen	41%	27%	51%	33%
Lange wachtwoorden of wachtzinnen gebruiken van minimaal 12 tekens.	40%	32%	47%	32%
Geen gebruik maken van openbare wifi-netwerken	38%	31%	41%	30%
Het standaard wachtwoord van mijn wifi modem veranderen (in een sterk en uniek wachtwoord)	32%	31%	46%	24%
Steeds een nieuw wachtwoord gebruiken dat ik nog niet eerder gebruikt heb	29%	31%	40%	23%
Een wachtwoordmanager gebruiken	27%	21%	41%	15%
Extensies aan je webbrowser toevoegen om cookies, advertenties en automatisch toegang tot Javascripts te blokkeren	21%	18%	38%	16%
Altijd gebruik maken van een VPN-verbinding	15%	19%	36%	12%
Informatie op internet opzoeken over hoe ik veiliger kan worden	13%	12%	19%	10%
Jaarlijks een digitale apk laten uitvoeren	8%	9%	5%	4%
Een specialist inhuren die bij mij thuis langskomt om de digitale veiligheid te verbeteren installeren	9%	6%	3%	5%
Geen van bovenstaande	4%	4%	1%	7%

ICT-verantwoordelijken | Digitaal gedrag

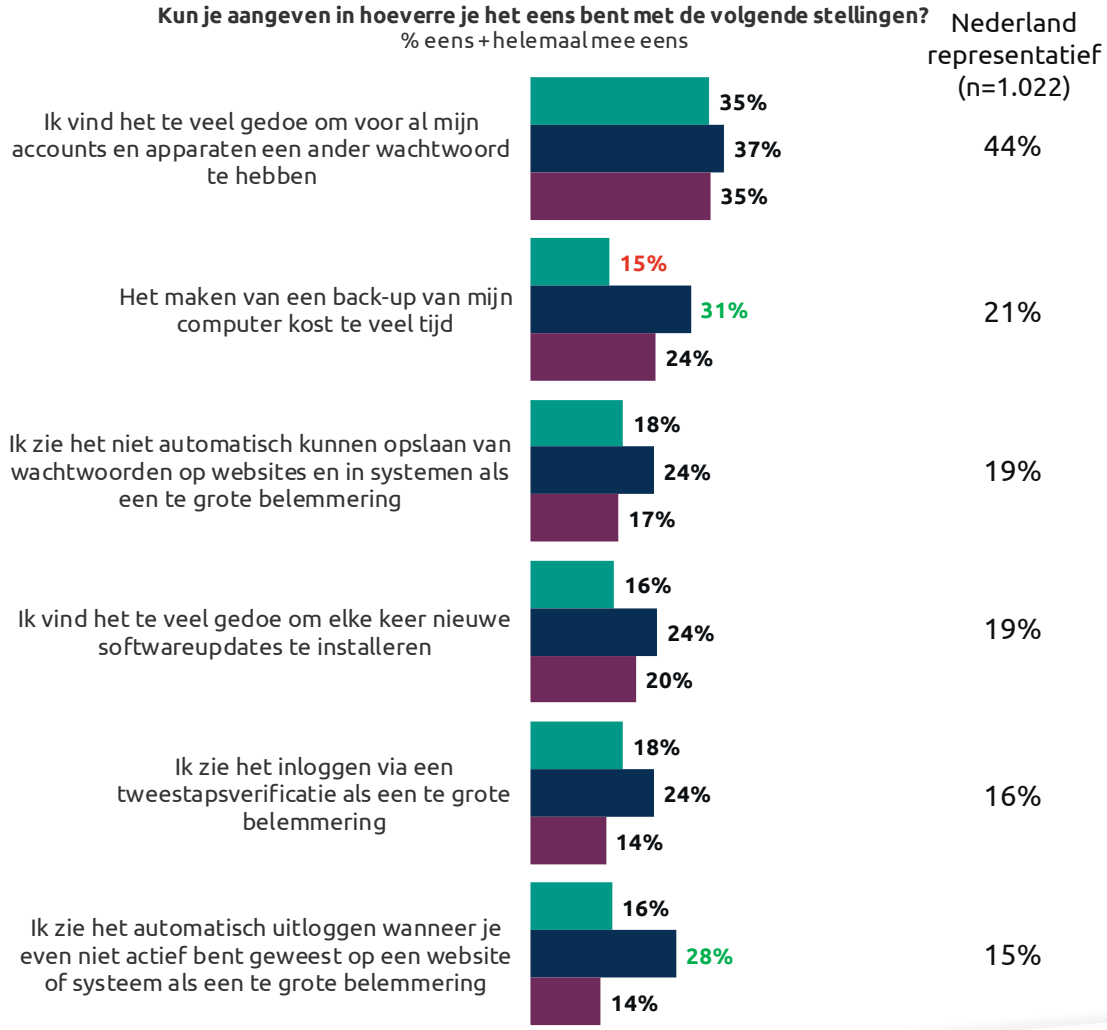
ICT-verantwoordelijken van groot-MKB zijn in mindere mate bereid om verschillende acties te ondernemen om online veiligheid te vergroten

Welke van de onderstaande acties zou je bereid zijn om te doen om jouw online veiligheid te verbeteren?	ICT-verantwoordelijken klein-MKB (n=230)	ICT-verantwoordelijken groot-MKB (n=139)	ICT-verantwoordelijken Grootbedrijf (n=104)	Nederland representatief (n=1.022)
Regelmatig (beveiligings)updates doen	50%	35%	49%	43%
Antivirussoftware gebruiken en regelmatig updaten	47%	35%	49%	48%
Regelmatig back-ups maken van al mijn bestanden	48%	32%	47%	40%
Controleren op welke links ik klik	43%	32%	46%	40%
Direct software updates uitvoeren	42%	35%	46%	39%
Een firewall installeren	40%	33%	47%	35%
Mijn wachtwoorden regelmatig veranderen	40%	34%	49%	33%
Geen gebruik meer maken van onbeveiligde sites om bestanden uit te wisselen	36%	29%	40%	35%
Lange wachtwoorden of wachtzinnen gebruiken van minimaal 12 tekens.	36%	35%	52%	31%
Geen gebruik maken van openbare wifi-netwerken	37%	29%	42%	31%
Het standaard wachtwoord van mijn wifi modem veranderen (in een sterk en uniek wachtwoord)	35%	27%	41%	30%
Steeds een nieuw wachtwoord gebruiken dat ik nog niet eerder gebruikt heb	30%	27%	37%	26%
Een wachtwoordmanager gebruiken	28%	21%	34%	19%
Extensies aan je webbrowser toevoegen om cookies, advertenties en automatisch toegang tot Javascripts te blokkeren	28%	24%	37%	25%
Altijd gebruik maken van een VPN-verbinding	20%	22%	37%	19%
Informatie op internet opzoeken over hoe ik veiliger kan worden	26%	16%	30%	23%
Jaarlijks een digitale apk laten uitvoeren	23%	13%	17%	15%
Een specialist inhuren die bij mij thuis langskomt om de digitale veiligheid te verbeteren installeren	14%	11%	8%	9%
Geen van bovenstaande	15%	11%	14%	10%

ICT-verantwoordelijken | Digitaal gedrag

Groot-MKB ervaart het maken van back-ups en het automatisch uitloggen vaker als belemmering dan de andere type bedrijven

ICT-verantwoordelijken binnen groot-MKB ervaren vaker belemmeringen bij het maken van back-ups (31%) en het automatisch uitloggen wanneer je even niet actief bent geweest (28%).

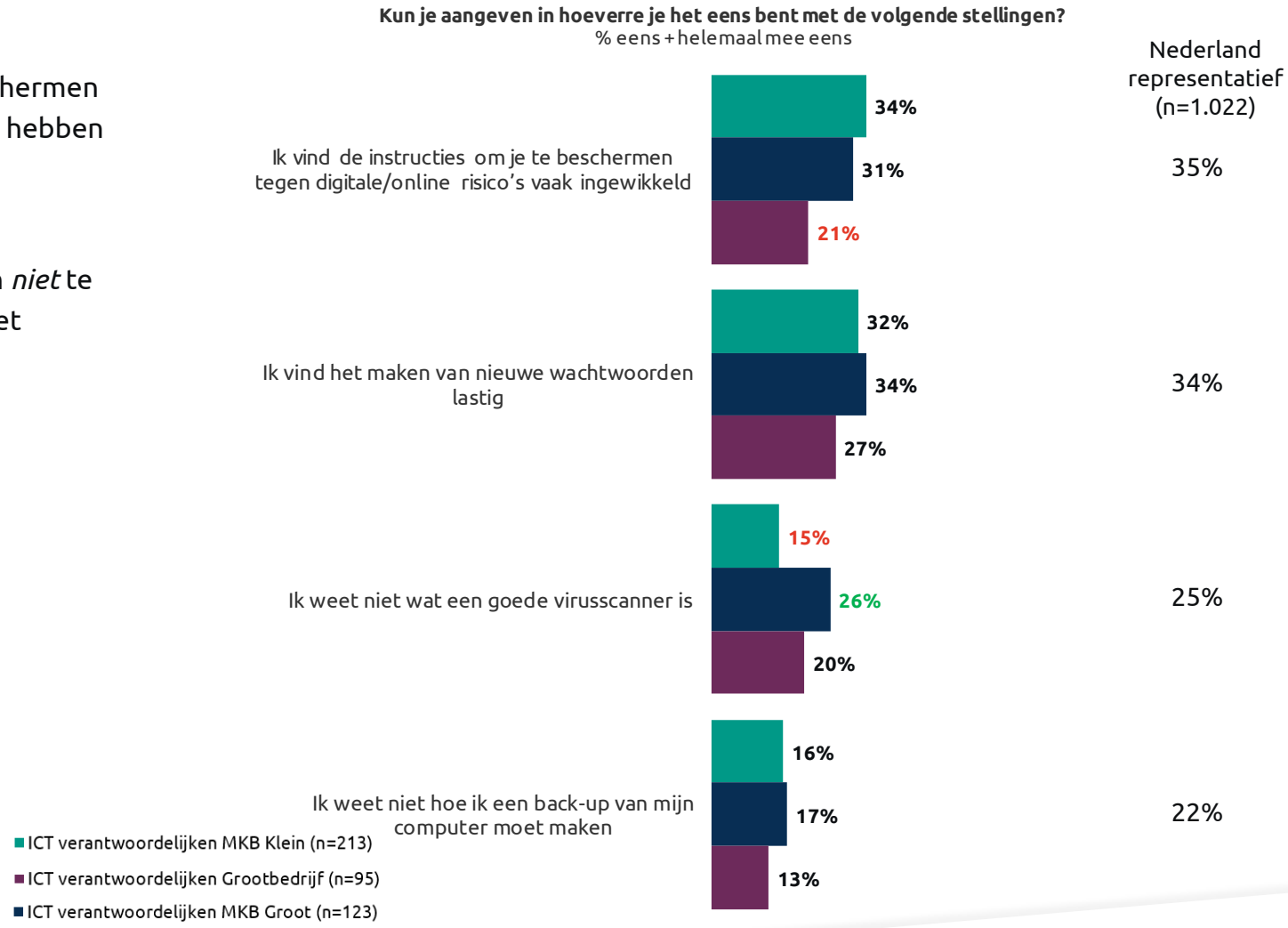


ICT-verantwoordelijken | Digitaal gedrag

Relatief veel ICT-verantwoordelijken in klein- en groot-MKB vinden instructies om jezelf te beschermen tegen digitale risico's ingewikkeld

In dezelfde mate als het Nederlands publiek vinden ICT-verantwoordelijken van het MKB dat instructies om jezelf te beschermen tegen digitale risico's ingewikkeld zijn. ICT'ers van grootbedrijven hebben hier minder moeite mee (21%).

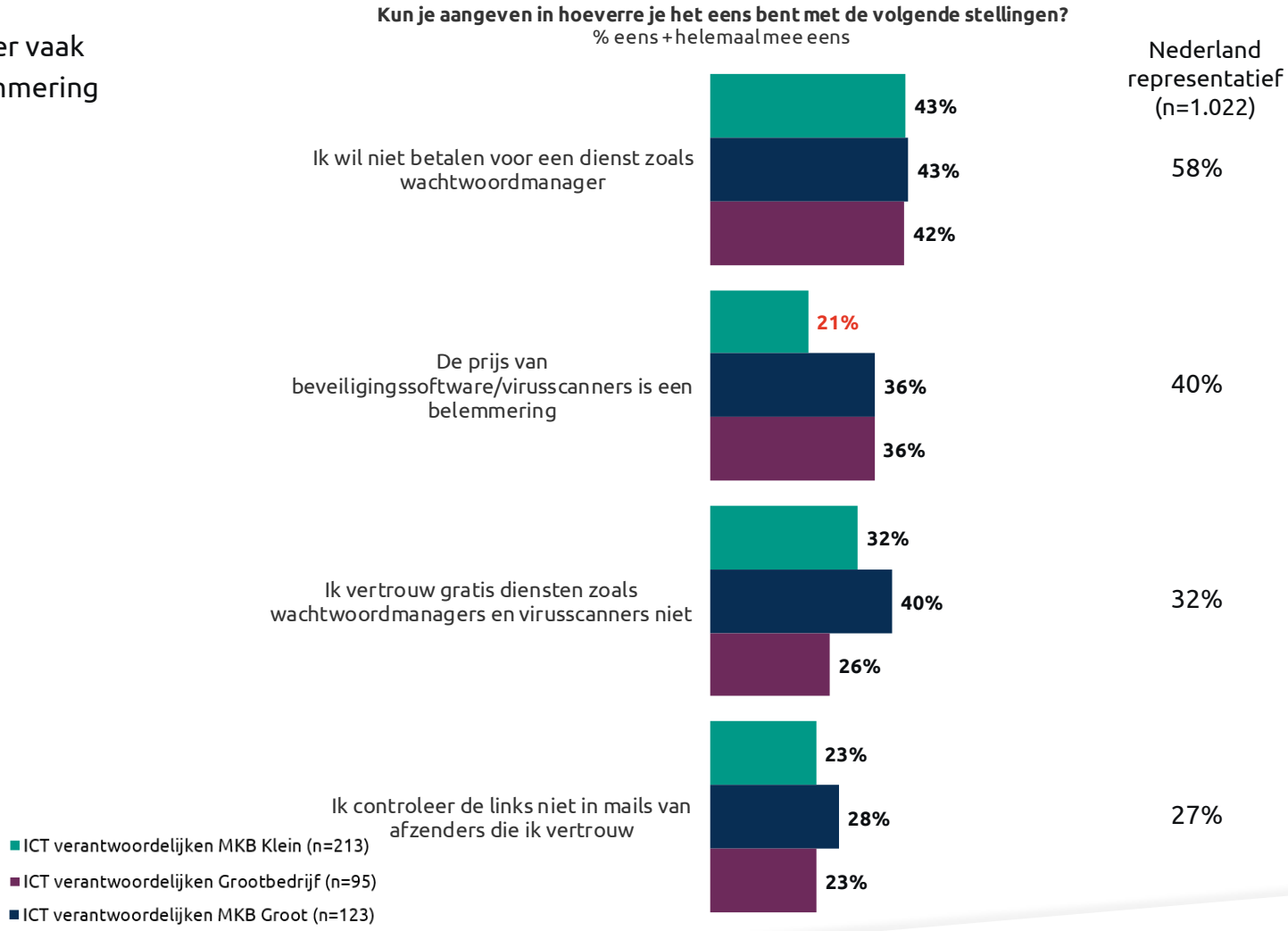
ICT-verantwoordelijken van het klein-MKB geven minder vaak aan *niet* te weten wat een goede virusscanner is (15%). In dit geval wil dat niet zeggen dat ze vaker weten wat *wel* goede virusscanners zijn.



ICT-verantwoordelijken | Digitaal gedrag

Met name voor ICT-verantwoordelijken in klein-MKB is prijs minder vaak een belemmering

Met name ICT-verantwoordelijken van het klein-MKB geven minder vaak aan dat de prijs van beveiligingssoftware/virusscanners een belemmering is (21%).



ICT-verantwoordelijken | Digitaal gedrag

Circa de helft van de ICT-verantwoordelijken zou niet betalen bij een hack

In hoeverre zijn de volgende uitspraken van toepassing? % Ik doe dit nooit	ICT-verantwoordelijken klein-MKB (n=230)	ICT-verantwoordelijken groot-MKB (n=139)	ICT-verantwoordelijken Grootbedrijf (n=104)	Nederland representatief (n=1.022)
Als ik gehackt zou worden via ransomware en gevraagd wordt om te betalen om weer toegang tot mijn laptop of pc te krijgen dan zou ik daarvoor betalen	55%	47%	50%	57%
Ik laat mijn kind(eren) gebruikmaken van mijn werklaptop	43%	39%	56%	37%
Ik laat mijn kind(eren) gebruikmaken van mijn werktelefoon	39%	39%	54%	33%
Ik maak thuis gebruik van een extern opslagapparaat dat continu online is	32%	26%	39%	35%
Ik verstuur werkbestanden van mijn werk e-mailadres naar mijn privé e-mail	23%	26%	43%	30%
Als ik op een link in een phishing e-mail zou klikken dan zou ik mij daar voor schamen	7%	5%	4%	7%
Ik maak op mijn werk regelmatig back-ups van de bestanden op mijn werk laptop	5%	7%	15%	14%
Ik heb de privacy instellingen van mijn social media accounts aangepast ten opzichte van de standaard instellingen	3%	3%	6%	3%
Ik maak thuis regelmatig back-ups van mijn bestanden	3%	2%	5%	7%
Als er een slotje en/of https voor het adres van een website staat dan denk ik dat ik die website veilig kan bezoeken	2%	4%	2%	2%
Ik bezoek alleen websites waar een slotje en/of https voor het adres van een website staat	2%	3%	1%	3%
Als ik een openbare computer heb gebruikt dan log ik na gebruik al mijn accounts uit	3%	1%	1%	2%
Mijn werkgever maakt automatisch back-ups	3%	1%	1%	2%
Als ik door heb dat ik een virus heb gedownload op mijn werkcomputer waardoor andere computers binnen mijn bedrijf besmet raken vertel ik meteen aan anderen wat ik heb gedaan	0%	2%	2%	2%

ICT-verantwoordelijken
Ervaringen met digitale risico's

ICT-verantwoordelijken | Ervaringen

ICT-verantwoordelijken hebben het meest te maken met phising mails

Heb je in een werksituatie in de afgelopen 12 maanden weleens te maken gehad met één van de onderstaande voorvallen? % Ikzelf	ICT-verantwoordelijken klein-MKB (n=230)	ICT-verantwoordelijken groot-MKB (n=139)	ICT-verantwoordelijken Grootbedrijf (n=104)	Nederland representatief (n=1.022)
Mails ontvangen met poging tot phishing	37%	34%	28%	16%
Acquisitiefraude	16%	21%	5%	6%
Benaderd met een social media berichtje met vraag om een onbekende link aan te klikken	11%	14%	13%	7%
Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik die bijna niet van echt te onderscheiden is	8%	14%	10%	5%
Mensen die gegevens opvragen door zich voor te doen als vermoedelijke klant, collega of leverancier	7%	14%	11%	6%
Dat een computer tijdelijk niet werkte door een malware zoals bijvoorbeeld een virus	2%	18%	5%	5%
Dat mijn (bedrijfs-) website tijdelijk niet werkte door b.v. een DDoS-aanval	1%	14%	9%	5%
Ransomware	2%	12%	4%	2%
Iemand in een account heeft ingelogd zonder dat de eigenaar/gebruiker daar toestemming voor gegeven heeft	1%	12%	3%	4%
Iemand in een apparaat heeft ingelogd zonder dat de eigenaar/gebruiker daar toestemming voor gegeven heeft	1%	11%	6%	5%
Een foute link ook daadwerkelijk aangeklikt die een virus, spam, phishing of andere ongewenste poging bevatten	3%	9%	5%	6%
Dat door het downloaden van geïnfecteerde software/bestanden malware verspreid werd	2%	10%	5%	3%
Identiteitsdiefstal	2%	8%	7%	3%
Misbruik van bedrijfsgevoelige gegevens	0%	9%	7%	6%
Geen van bovenstaande voorvallen	57%	53%	55%	74%

ICT-verantwoordelijken | Ervaringen

ICT-verantwoordelijken in klein-MKB treffen het minst vaak maatregelen

Heb je maatregelen getroffen nadat je dit hebt meegemaakt?	ICT-verantwoordelijken klein-MKB (n=107)	ICT-verantwoordelijken groot-MKB (n=74)	ICT-verantwoordelijken Grootbedrijf (n=57)	Nederland representatief (n=151)
Ik ben voorzichtiger met het klikken op links	29%	18%	13%	14%
Ik heb het gerapporteerd/ aangifte gedaan	19%	20%	14%	14%
Ik controleer of iemand is die hij/zij zegt te zijn als ik een vreemd verzoek van hem/haar krijg	22%	14%	15%	13%
Ik maak mijn wachtwoorden complexer	13%	16%	12%	12%
Ik controleer of websites HTTPS gebruiken	16%	14%	10%	7%
Ik heb het gemeld bij onze systeembeheerder(s)/IT-afdeling	7%	20%	18%	15%
Ik heb een software update uitgevoerd	17%	12%	7%	6%
Ik heb een firewall geïnstalleerd of geüpdatet	12%	12%	12%	12%
Ik heb antivirussoftware geïnstalleerd	15%	15%	4%	13%
Ik deel mijn wachtwoorden niet (meer) met anderen	14%	11%	9%	8%
Ik maak nu back-ups van de bestanden op mijn laptop	9%	16%	9%	7%
Ik heb toestemmingen van apps op mijn telefoon beperkt	11%	15%	7%	14%
Ik heb tweefactorauthenticatie ingesteld op mijn apparaten / accounts	10%	11%	9%	8%
Ik maak nu back-ups van mijn tablet	8%	11%	5%	7%
Ik ben nu een VPN-verbinding gaan gebruiken via mijn laptop	3%	11%	12%	8%
Ik verstuur geen werkgerelateerde bestanden van mijn werk meer naar huis	2%	11%	12%	11%
Ik ben een wachtwoordmanager gaan gebruiken	5%	11%	4%	7%
Ik maak nu back-ups van mijn smartphone	4%	8%	9%	2%
Ik versleutel mijn harde schijf	2%	9%	9%	3%
Ik ben nu een VPN-verbinding gaan gebruiken via mijn tablet	3%	8%	7%	7%
Ik gebruik apps om meer controle te krijgen over het besturingssysteem dan de fabrikant toestaat	3%	9%	4%	7%
Ik ben nu een VPN-verbinding gaan gebruiken via mijn smartphone	3%	5%	5%	5%
Anders, namelijk:	7%	5%	4%	3%
Geen van bovenstaande, ik heb niets gedaan	37%	26%	42%	40%

ICT-verantwoordelijken
Digitale veiligheid op de werkvloer

ICT-verantwoordelijken | Digitale veiligheid werkvloer

ICT verantwoordelijk in klein-MKB hebben vaker geen bedrijfsafspraken; bij grootbedrijven is het afsprakenpakket het meest uitgebreid

Welke afspraken zijn er binnen jouw bedrijf/ organisatie gemaakt over hoe je je online veilig gedraagt?	ICT-verantwoordelijken klein-MKB (n=230)	ICT-verantwoordelijken groot-MKB (n=139)	ICT-verantwoordelijken Grootbedrijf (n=104)	Werkend Nederland (n=477)
Er zijn afspraken gemaakt over het veilig versturen/uitwisselen van bestanden	19%	41%	63%	35%
Er zijn afspraken gemaakt over het gebruikmaken van websites en/of e-mail	21%	39%	59%	33%
Er zijn afspraken gemaakt over het gebruikmaken van opslagmedia als usb-sticks	17%	39%	61%	26%
Er zijn afspraken gemaakt over het versturen/uitwisselen van persoonsgegevens	16%	36%	59%	31%
Er zijn afspraken gemaakt over het gebruik van zakelijke smartphones, laptops, tablets	15%	35%	56%	25%
Alleen de systeembeheerders kunnen software installeren	17%	31%	46%	31%
Er zijn afspraken gemaakt over het gebruikmaken van sociale media	15%	26%	54%	27%
De toegang tot bepaalde websites en/of socialemediakanalen is geblokkeerd	10%	17%	43%	17%
De toegang tot bepaalde socialemediakanalen is geblokkeerd	7%	9%	29%	27%
De toegang tot bepaalde verzendplatforms is geblokkeerd	6%	10%	31%	16%
Het gebruik van USB-sticks in onze organisatie is onmogelijk gemaakt	5%	6%	24%	14%
Anders, namelijk:	10%	1%	2%	3%
Weet ik niet	10%	6%	7%	18%
In mijn bedrijf/organisatie zijn geheel geen afspraken gemaakt over hoe je je online veilig gedraagt	46%	11%	6%	13%

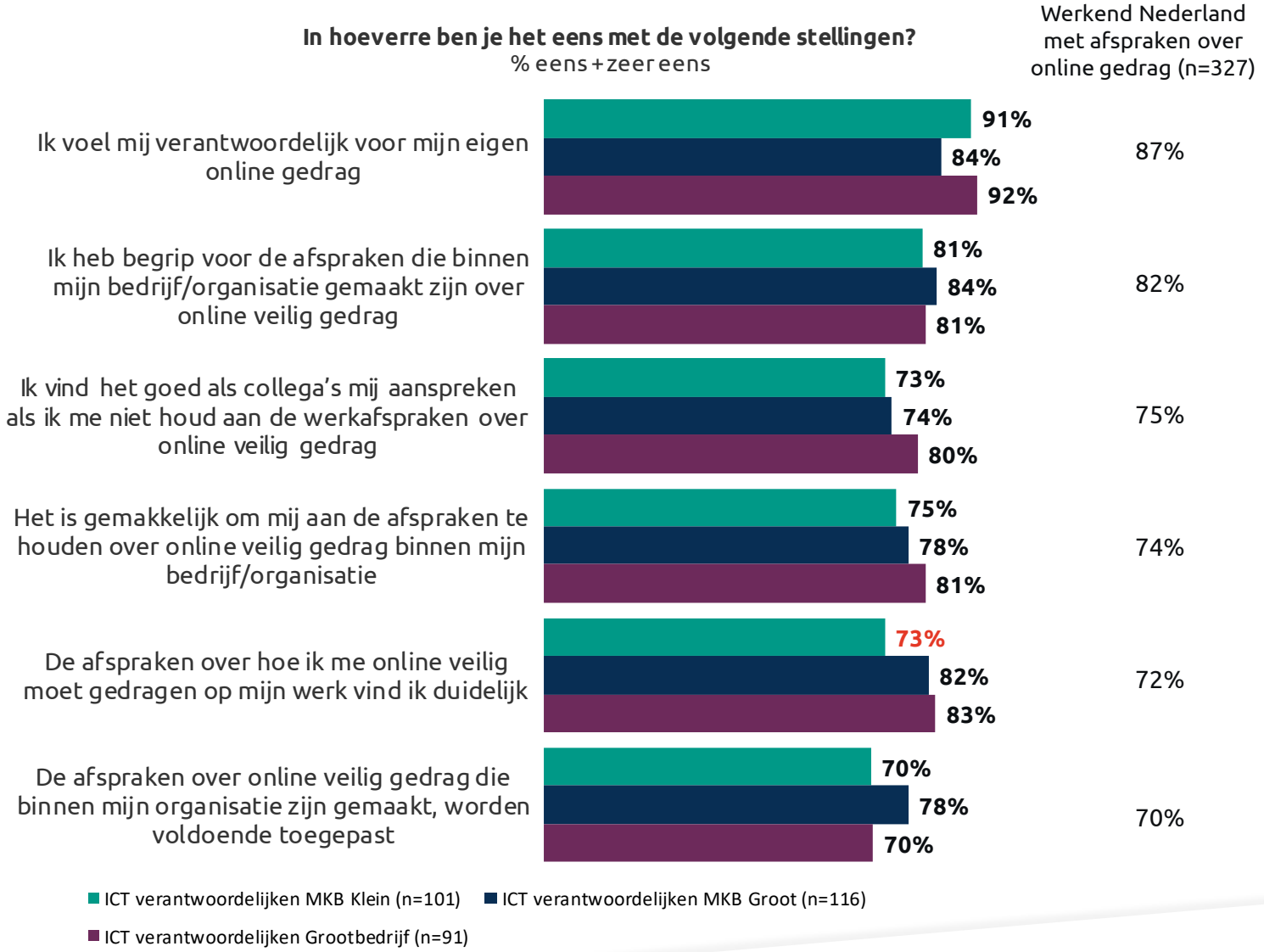
ICT-verantwoordelijken | Digitale veiligheid werkvloer

Hoge mate van eigen verantwoordelijkheid voor eigen online gedrag

Vrijwel alle ICT-verantwoordelijken die werkafspraken over online gedrag hebben bij hun bedrijf/organisatie, voelen zich verantwoordelijk voor hun eigen online gedrag.

Daarnaast is er hoge mate van begrip voor de afspraken en staat men er voor open om aangesproken te worden op het eigen gedrag. De meesten vindende afspraken duidelijk en at het makkelijk is om zich aan de gemaakte afspraken te houden.

Een meerderheid vindt dat de gemaakte afspraken voldoende worden toegepast in de organisatie.



ICT-verantwoordelijken | Digitale veiligheid werkvloer

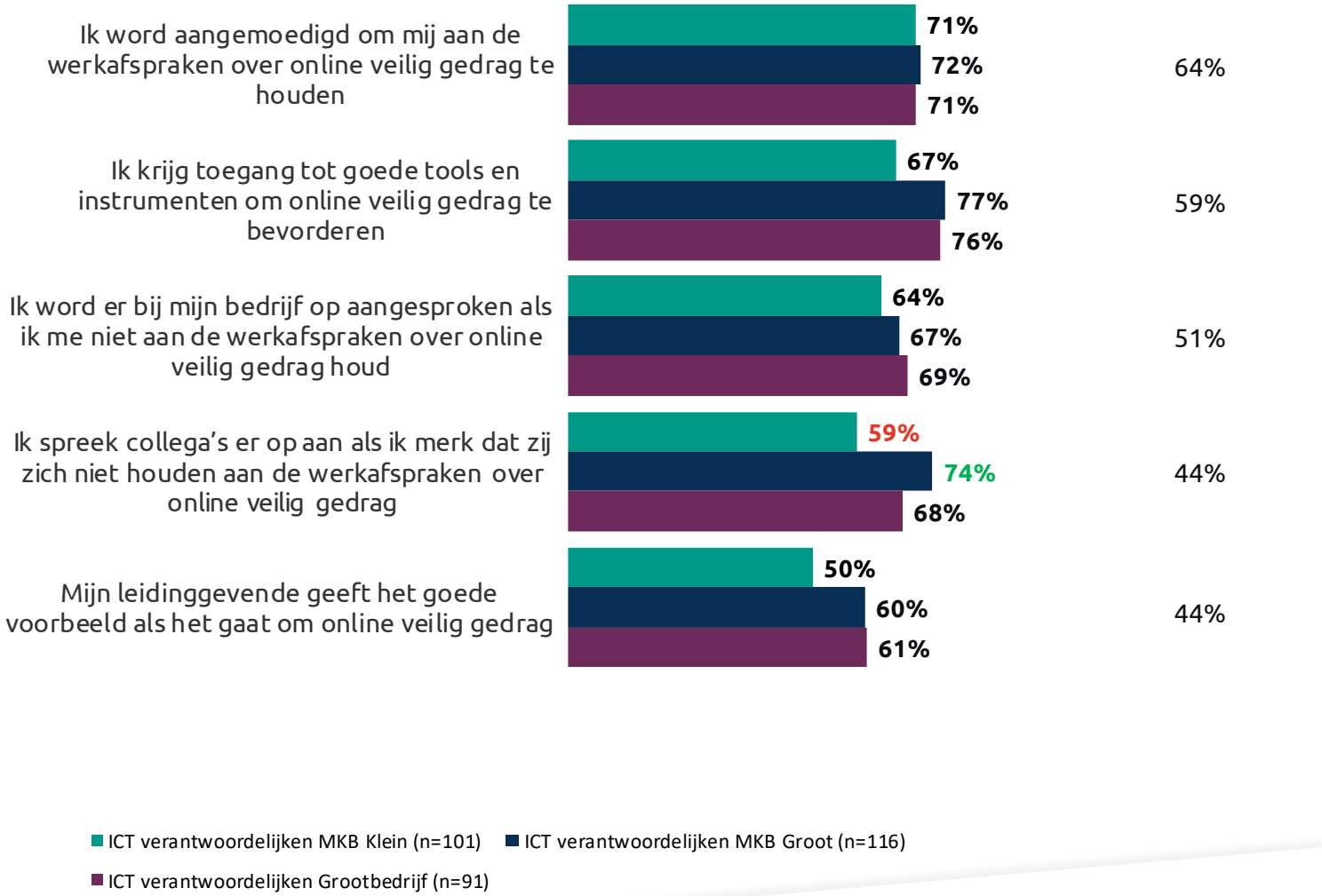
Meeste ICT-ers voelen zich aangemoedigd om zich aan de werkafspraken te houden

Een meerderheid van de ICT-verantwoordelijken in zowel grote als kleine bedrijven hebben het gevoel dat ze aangemoedigd worden om zich aan de werkafspraken te houden, ze krijgen de goede tools en instrumenten aangereikt om veilig online gedrag te bevorderen en worden aangesproken op hun gedrag als dit niet binnen de afspraken is.

ICT-verantwoordelijken in groot-MKB geven vaker aan dat zij hun collega's er op aan zouden spreken wanneer zij zich niet houden aan de werkafspraken dan ICT-verantwoordelijken in het klein-MKB.

Verder vindt een meerderheid van de ICT-ers dat hun leidinggevende het goede voorbeeld geeft.

In hoeverre ben je het eens met de volgende stellingen?
% eens + zeer eens

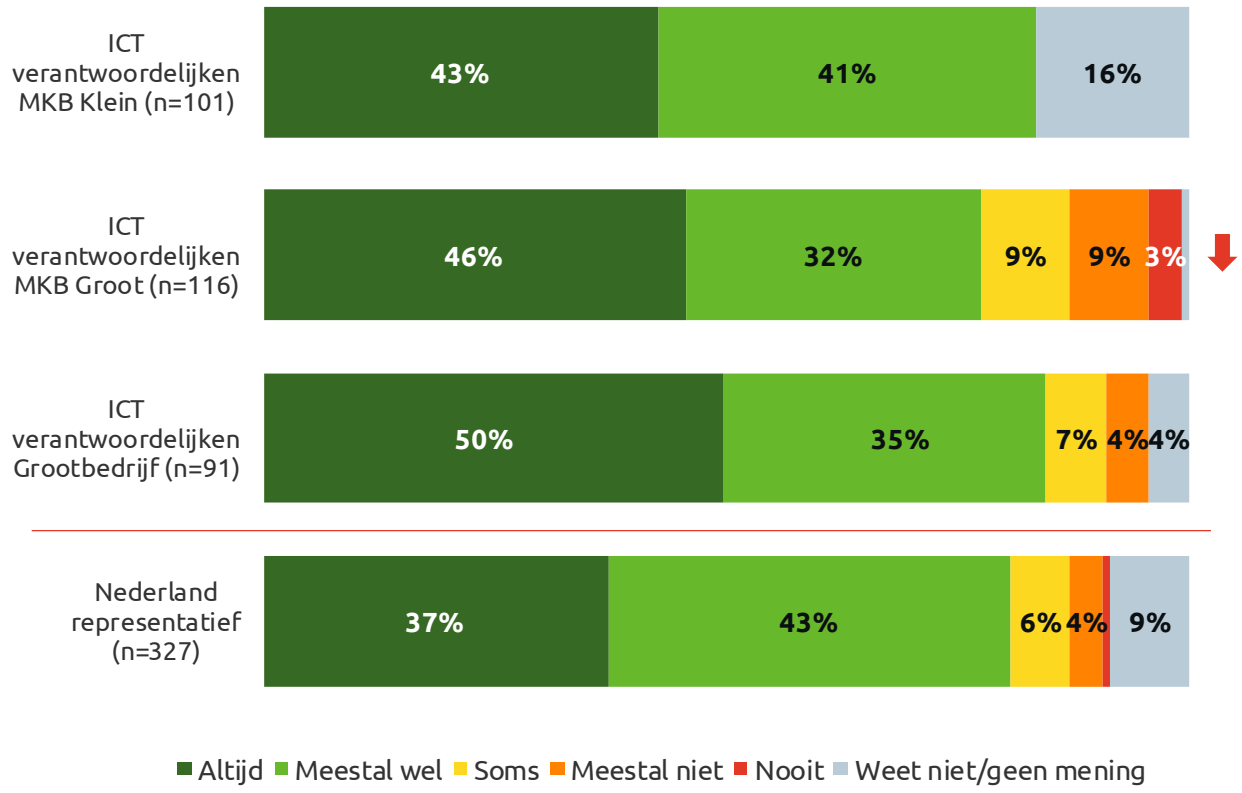


ICT-verantwoordelijken | Digitale veiligheid werkvloer

ICT verantwoordelijk in groot-MKB hebben wat vaker moeite om zich aan de afspraken

De meesten ICT-verantwoordelijken houden zich meestal wel of altijd aan de gemaakte afspraken omtrent online gedrag. ICT-verantwoordelijken uit het groot-MKB geven in vergelijking wat vaker aan zich niet altijd aan de afspraken te houden.

In hoeverre houd jij je aan de afspraken die binnen jouw bedrijf/organisatie gemaakt zijn over hoe je je online veilig gedraagt?
(Basis - Werkend met afspraken over online veilig gedrag)



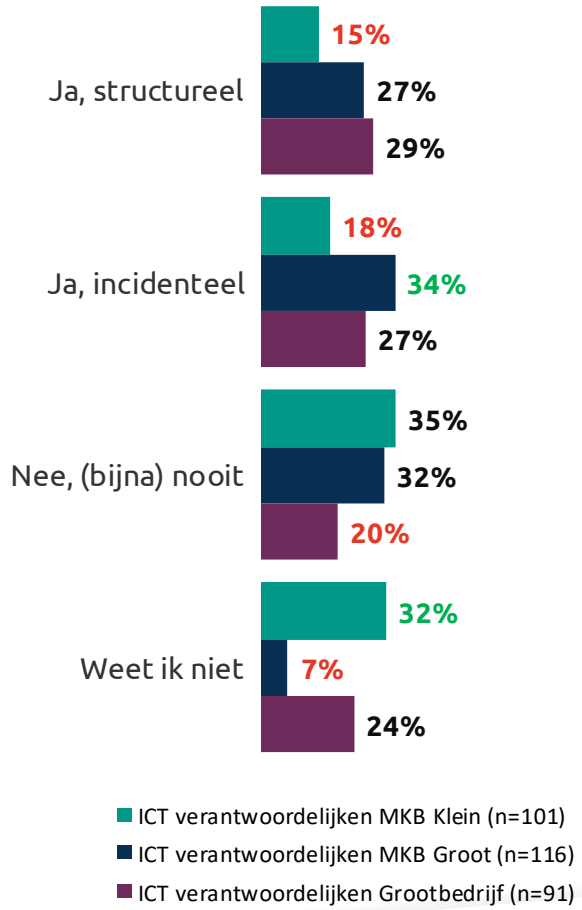
Significant verschil t.o.v. de andere medewerkersgroepen

ICT-verantwoordelijken | Digitale veiligheid werkvloer

Grotere bedrijven monitoren (incidenteel) vaker het online gedrag dan klein-MBK

ICT-verantwoordelijken in het klein-MKB geven minder vaak aan dat er in hun organisatie structureel of incidenteel gemeten wordt in hoeverre medewerkers zich aan afspraken omtrent veilig online gedrag houden. Zij geven vaker aan niet te weten of dit gebeurt.

Wordt binnen jouw bedrijf of organisatie gemeten in hoeverre medewerkers zich aan de afspraken voor online veilig gedrag houden? (Basis - Werkend met afspraken over online veilig gedrag)



Werkend Nederland met afspraken over online gedrag (n=327)
16%
19%
17%
47%

ICT-verantwoordelijken | Digitale veiligheid werkvloer

ICT-verantwoordelijken van klein-MKB ervaren minder belemmeringen in het borgen van werkafspraken over veilig online gedrag

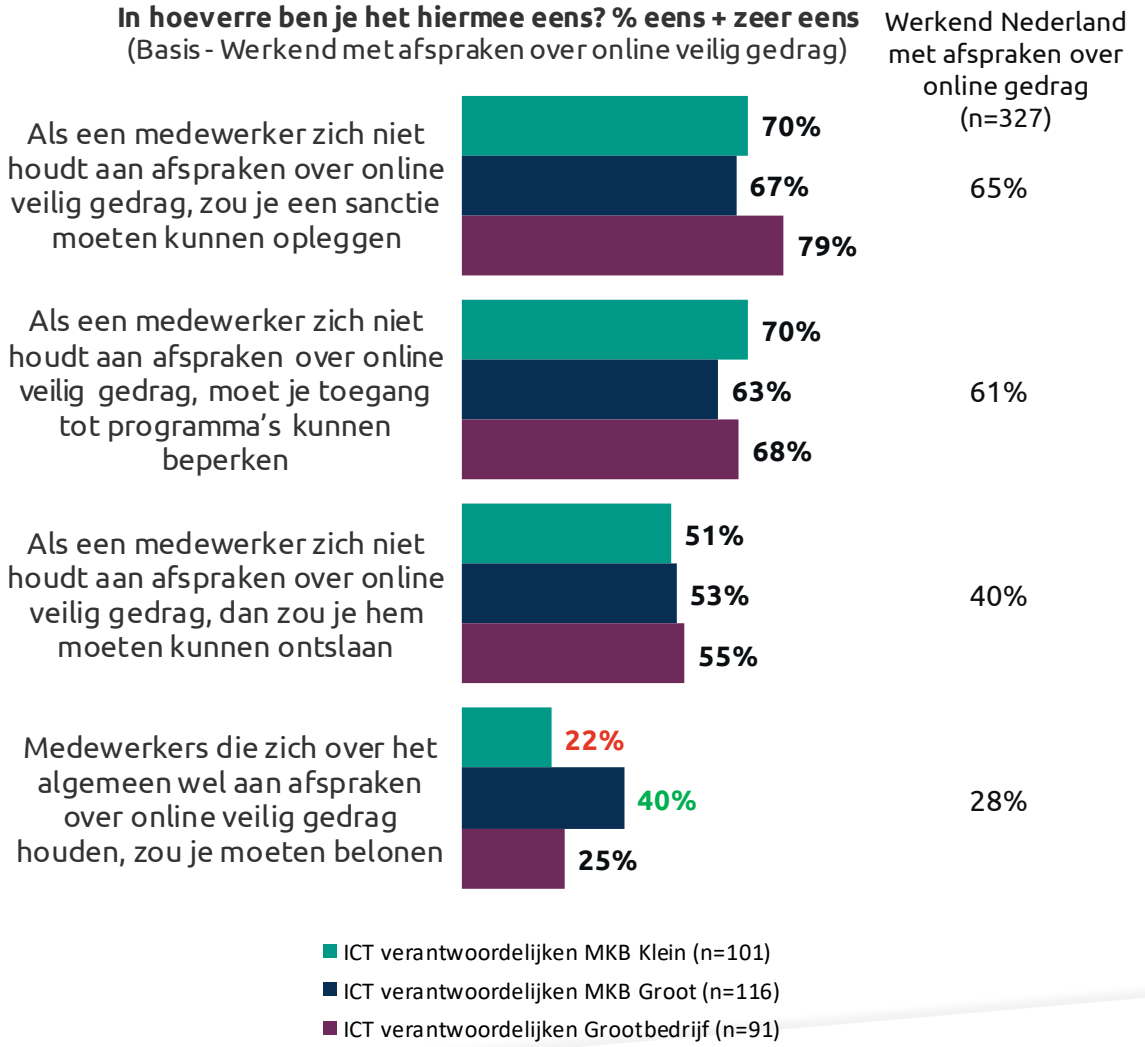
Welke belemmeringen ervaar je binnen jouw bedrijf bij het borgen van de afspraken voor online veilig gedrag? Basis – Werkend met afspraken over online veilig gedrag	**ICT-verantwoordelijken klein-MKB (n=101)**	**ICT-verantwoordelijken groot-MKB (n=116)**	**ICT-verantwoordelijken Grootbedrijf (n=91)**	**Werkend Nederland (n=327)**
Te weinig tijd	10%	15%	15%	**9%**
Er wordt niet voldoende over gecommuniceerd	10%	10%	18%	**13%**
Er wordt niet duidelijk over gecommuniceerd	**3%**	15%	17%	**13%**
Het is onduidelijk bij wie de borging hiervan ligt	8%	12%	13%	**10%**
Er wordt geen prioriteit aan gegeven	7%	11%	13%	**12%**
Te weinig mankracht	8%	12%	9%	**7%**
Te weinig kennis binnen de organisatie	11%	8%	11%	**7%**
Er wordt niet eenduidig over gecommuniceerd	**3%**	9%	**16%**	**12%**
Er wordt niet aansprekend over gecommuniceerd	**4%**	6%	**19%**	**9%**
Gebrek aan draagvlak vanuit het management	**3%**	9%	**13%**	**6%**
Te weinig budget	9%	**3%**	7%	**7%**
Geen van deze/geen belemmeringen	**69%**	**43%**	**41%**	**54%**

ICT-verantwoordelijken | Digitale veiligheid werkvloer

Grote mate van rechtvaardiging sancties; minder voor belonen

Onder ICT-verantwoordelijken is een relatief groot draagvlak voor het opleggen van sancties. Daarnaast vinden de meeste dat medewerkers toegang ontzegd moet kunnen worden als zij zich niet houden aan afspraken. Circa de helft staat positief over de mogelijkheid om een medewerker te ontslaan als deze zich niet houdt aan afspraken over online veilig gedrag.

Er is minder steun voor het belonen van goed gedrag. ICT-verantwoordelijken in het groot-MKB staan positiever tegenover het belonen van goed gedrag (40%) dan medewerkers in het klein-MKB (22%).



Bijlagen

Bijlage: herkennen phishingmails ICT-verantwoordelijken

Naar welke onderdelen van een mail kijk jij vooral om een phishingmail te herkennen? Basis – bekend met phishing	**ICT-verantwoordelijken klein-MKB (n=213)**	**ICT-verantwoordelijken groot-MKB (n=123)**	**ICT-verantwoordelijken Grootbedrijf (n=95)**	**Nederland representatief (n=845)**
Het mailadres van de afzender	68%	58%	61%	59%
Het taalgebruik in het onderwerp of in de mail zelf (de toon)/De schrijfstijl in de mail	58%	48%	57%	50%
Vraag om persoonlijke gegevens	**54%**	39%	**36%**	52%
Het doeladres waar de link naar verwijst, voordat je er op klikt	40%	**32%**	47%	34%
Of er om geld wordt gevraagd	37%	29%	30%	40%
De urgentie die uit de inhoud van de mail spreekt (moet er snel actie ondernomen worden)	35%	**24%**	33%	30%
De link(s) die in de mail zijn opgenomen /de link die achter de knop 'klik hier' staat	33%	33%	**46%**	29%
De opmaak van het bericht	32%	34%	37%	33%
De naam van de afzender	23%	27%	19%	28%
De aanhef/of ik persoonlijk aangesproken word in de mail	20%	18%	26%	24%
De logo's in de mail	12%	11%	16%	12%
Het lettertype van de mail	**3%**	7%	**11%**	5%
Ik let hier nooit op als ik een mail bekijk	0%	1%	0%	1%
Ik kan dit niet herkennen, de mails zien er te echt uit	0%	0%	0%	1%
Anders, namelijk:	3%	2%	5%	2%
Weet niet/geen mening	3%	2%	0%	3%

Bijlage: herkennen phishingberichten ICT-verantwoordelijken

Naar welke onderdelen van een bericht kijk jij vooral om een phishing via SMS of WhatsApp te herkennen? Basis – bekend met phishing	ICT-verantwoordelijken klein-MKB (n=213)	ICT-verantwoordelijken groot-MKB (n=123)	ICT-verantwoordelijken Grootbedrijf (n=95)	Nederland representatief (n=845)
Of om bepaalde gegevens wordt gevraagd	63%	46%	57%	55%
Of gevraagd wordt of ik mijn inloggegevens en wachtwoord wil invoeren	62%	33%	54%	51%
Of er om geld wordt gevraagd	49%	47%	46%	49%
Vraag om persoonlijke gegevens	47%	42%	46%	44%
De link/betaalverzoek	36%	37%	35%	37%
De urgentie die uit de inhoud spreekt (moet er snel actie ondernomen worden)	34%	29%	42%	30%
Het taalgebruik in het bericht/de schrijfstijl	32%	28%	37%	34%
De naam van de afzender	26%	32%	33%	28%
De opmaak van het bericht	11%	23%	15%	15%
De profiel foto	2%	7%	6%	7%
Het lettertype van het bericht	0%	7%	3%	2%
Ik let hier nooit op als ik een bericht bekijk	1%	1%	1%	1%
Ik kan dit niet herkennen, de berichten zien er te echt uit	0%	0%	0%	1%
Anders, namelijk:	7%	3%	7%	4%
Weet niet/geen mening	7%	4%	4%	7%

Methode en opzet

Methode

Het onderzoek is kwantitatief online uitgevoerd onder het ISO-26362-gecertificeerde webpanel van Motivaction, StemPunt.

Doelgroep

De doelgroep bestaat uit werkende Nederlanders in het klein-MKB, groot-MKB, in het grootbedrijf en in de vitale infrastructuur. In de leeswijzer is opgenomen welke processen onder vitale infrastructuur vallen. Binnen de doelgroepen is onderscheid gemaakt tussen medewerkers en verantwoordelijken voor de ICT/automatisering binnen het bedrijf/de organisatie.

Steekproef

Om uitspraken te kunnen doen over de verschillende groepen is gekozen om voor de groepen medewerkers een minimaal steekproef omvang van n = 250 te behalen. Voor de ICT-verantwoordelijken is gekozen om een minimale steekproef omvang van n = 100 te behalen. In een aantal gevallen is gebruik gemaakt van een partnerbureau om respondenten te benaderen. De steekproeven binnen de werkzame bevolking zijn niet gewogen omdat hier geen referentiecijfers van beschikbaar zijn. De netto steekproef bestaat uit n = 470 ICT-verantwoordelijken.

Vragenlijst en veldwerk

Respondenten kregen per e-mail een uitnodiging met daarin een link naar de online vragenlijst. De vragenlijst is in samenwerking met betrokkenen vanuit ministerie van EZK opgesteld. Het veldwerk is tussen 11 augustus en 23 augustus 2020 online uitgevoerd.

Wij verminderen onze footprint

Motivaction is ISO 14001-gecertificeerd

Motivaction gebruikt energiezuinige auto’s

Motivaction gebruikt groene stroom

Motivaction gebruikt uitsluitend papier met een FSC-label

Auteursrecht

Beeldmateriaal

Motivaction heeft datgene gedaan wat redelijkerwijs van ons verwacht kan worden om de rechthebbenden op beeldmateriaal te achterhalen. Mocht u desondanks menen recht te kunnen doen gelden op gebruikt beeldmateriaal, neem dan contact op met Motivaction.

Pers- en publicatiebeleid

Het vermelden van de naam van Motivaction in persberichten en/of andere publicaties over door Motivaction uitgevoerd onderzoek is gebonden aan een aantal voorwaarden, zoals vastgelegd in ons Pers- en publicatiebeleid.

Motivaction International B.V.

Marnixkade 109F
1015ZL Amsterdam

Postbus 15262
1001MG Amsterdam

020 589 83 83

info@motivaction.nl

www.motivaction.nl

Weet wat mensen drijft.

motivaction
insights and strategy