Rapportage

Cybersecurity onderzoek Veilig Online 2021

Deelrapport bedrijfsleven
medewerkers en ICT-verantwoordelijken

i&o research

Ministerie van Economische Zaken en Klimaat

www.ioresearch.nl

Inhoudsopgave

Managementsamenvatting

Samenvatting 1/3

Kennisniveau van medewerkers en ICT-verantwoordelijken is vergelijkbaar met 2020

- Net als in 2020 schatten circa drie op de tien medewerkers hun kennis over online veiligheid als (zeer) goed (30%). Medewerkers in grootbedrijven (36%) en medewerkers in de vitale infrastructuur (40%) schatten hun kennis hoger in dan andere werknemers.
- ICT-verantwoordelijken schatten hun kennis over online veiligheid (zoals verwacht) hoger in dan medewerkers, maar toch schat nog bijna een op de vijf ICT-verantwoordelijken deze als matig tot (zeer) slecht (17%). Ruim vier op de tien ICT-verantwoordelijken beoordelen hun kennis als (zeer) goed (44%).

Medewerkers schatten het risico dat zij te maken krijgen met cybercrime laag in

- Bijna de helft denkt te maken te kunnen krijgen met phishing, malware, hacking, ransomware of een DDoS-aanval. Andere specifieke vormen van cybercrime worden minder vaak genoemd, tot circa een derde denkt hiermee te maken te kunnen krijgen. Er zijn hierbij slechts enkele verschillen tussen medewerkers van verschillende bedrijfsgrootte; medewerkers van grootbedrijven en medewerkers in de vitale infrastructuur denken vaker dan andere medewerkers dat ze te maken kunnen krijgen met een DDoS-aanval. Medewerkers van klein-MKB denken relatief vaak te maken te kunnen krijgen met bankhelpdeskfraude (34%, tegenover 21% gemiddeld onder alle werknemers).
- ICT-verantwoordelijken schatten het risico dat zij te maken kunnen krijgen met verschillende vormen van cybercrime hoger in dan medewerkers. Dit kan te maken hebben met de kennis die zij hebben vanwege hun functie en met het feit dat zij in hun werk vaker te maken krijgen met cybercrime. De helft van de ICT-verantwoordelijken kreeg in de afgelopen 12 maanden te maken met een poging tot phishing (medewerkers 26%). Daarnaast kregen veel ICT-verantwoordelijken (ook) te maken met acquisitiefraude (28%), met een onechte uitnodiging op sociale media voor zakelijk gebruik (22%), of werden zij op social media benaderd met een vraag om een onbekende link aan te klikken (21%).

Samenvatting 2/3

Sinds de coronacrisis maken meer ICT-verantwoordelijken zich zorgen over de online veiligheid op het werk

- Een op de tien ICT-verantwoordelijken maakt zich (zeer) veel zorgen over de online veiligheid op het werk en bij 15 procent zijn hun zorgen toegenomen sinds de coronacrisis. Medewerkers maken zich minder vaak zorgen. Net als in 2020 maken zeven op de tien werknemers zich (zeer) weinig zorgen, tegenover 47 procent van de ICT-verantwoordelijken. Ruim een op de drie werknemers van kleine bedrijven zegt zich minimaal enige zorgen te maken (37%). Dat is boven gemiddeld vaak.

Veel medewerkers weten niet of er afspraken zijn over veilig online gedrag op het werk

- Een kwart van de medewerkers weet niet of er afspraken zijn in hun bedrijf (27%) over veilig online gedrag. Van de ICT-verantwoordelijken weet 8 procent het niet. Bijna een op de tien werknemers en ICT-verantwoordelijken zegt dat er in hun bedrijf *geen* afspraken zijn (8%). Bijna een kwart van de medewerkers van klein-MKB zegt dat er bij hen geen afspraken zijn (23%). In grootbedrijven en bedrijven in de vitale infrastructuur worden gemiddeld de meeste acties ondernomen.

Er is veel draagvlak voor afspraken, maar medewerkers kennen ze vaak niet

- Waar afspraken zijn gemaakt over veilig online gedrag, is daar ook veel draagvlak voor. Zes op de zeven medewerkers en ICT-verantwoordelijken (die in een organisatie werken waar afspraken zijn gemaakt), hebben begrip voor de maatregelen. Medewerkers van grootbedrijven (93%) hebben vaker begrip voor de maatregelen dan andere medewerkers.
- Bijna iedereen voelt zich verantwoordelijk voor het eigen online gedrag op het werk. Toch valt er ook in bedrijven waar wel afspraken zijn gemaakt, nog wel wat te winnen wat betreft bekendheid en duidelijkheid van de regels. Ongeveer zes tot zeven op de tien medewerkers en ICT-verantwoordelijken vinden de gemaakte afspraken duidelijk, denken ze allemaal te kennen en vinden dat ze voldoende worden toegepast.
- Hoewel ongeveer zes op de zeven medewerkers en ICT-verantwoordelijken het goed zouden vinden als hun collega's hen aanspreken als ze zich niet aan de afspraken zouden houden, doen zij dit omgekeerd veel minder vaak. Zeven op de tien ICT-verantwoordelijk zou zelf iemand aanspreken (70%) en slechts 46 procent van de medewerkers zou dit naar eigen zeggen doen. Medewerkers van groot-MKB spreken elkaar minder vaak aan op onveilig gedrag dan in 2020.

Samenvatting 3/3

Medewerkers en ICT-verantwoordelijken vinden dat ze minder goed omgaan met online risico's dan in 2020

- Het rapportcijfer dat medewerkers en ICT-verantwoordelijken zichzelf geven voor hoe zij omgaan met online risico's is nog altijd een ruime voldoende (medewerkers 6,7 en ICT-verantwoordelijk 7,0), maar is lager dan in 2020.

De helft van de medewerkers maakt melding van (een poging tot) cybercrime

- Dit betekent ook dat de helft van de medewerkers geen melding maakte toen zij te maken hadden met cybercriminaliteit (52%). Hetzelfde geldt voor ICT-verantwoordelijken die hiermee te maken kregen (50%). Wie wel melding deed, deed dit in veel van de gevallen bij de ICT-afdeling van hun bedrijf (circa 30% van beide groepen). Medewerkers van grootbedrijven deden vaker dan andere medewerkers melding in geval van cybercrime, van deze groep zegt 41 procent dat zij *geen* melding deden. Dit kan ermee te maken hebben dat grotere bedrijven vaker een ICT-afdeling hebben dan kleinere bedrijven.

Back-ups worden vaker door de werkgever gemaakt dan door de werknemer zelf

- Back-ups worden niet door iedereen regelmatig gemaakt en het is vaker de werkgever die dit doet, dan werknemers zelf. In grootbedrijven is het aandeel dat zelf back-ups maakt met 34 procent het laagst. Een deel van de medewerkers ervaart belemmeringen om zelf back-ups te maken. Zo zegt 15 procent niet te weten hoe je een back-up maakt en 19 procent vindt dat dit teveel tijd kost. Bij ICT-verantwoordelijken is dit 7 procent (weet niet hoe) en 15 procent (kost teveel tijd).

Medewerkers gebruiken vaak het standaard wachtwoord voor hun (Wifi)netwerkverbinding

- Zes op de tien medewerkers werkten de afgelopen 12 maanden thuis. De meest gebruikte netwerkverbinding thuis is een (wifi)netwerkverbinding met wachtwoord (83% bij medewerkers). Ruim een op de drie medewerkers gebruikt hiervoor het standaard (bijgeleverde) wachtwoord (37%). Dit komt neer op 31 procent van alle medewerkers die thuis een router gebruiken met een standaard wachtwoord.

Inleiding

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 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 in Nederland.

Onderzoeksdoel

Het doel van dit onderzoek is het monitoren van de cyber awareness en cyber skills van Nederlanders door de jaren heen. Tot 1 januari 2020 werd dit jaarlijkse 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. Aanvullend beoogt dit onderzoek om inzichten te vergaren van kennis, houding en gedrag van Nederlanders met betrekking tot online veiligheid en het bieden van inzichten voor beleidsvorming met betrekking tot dit thema.

Inleiding

De hoofdvraag van het onderzoek luidt: **Wat is de kennis, houding en gedrag van het algemeen publiek, jongeren, medewerkers en ICT-verantwoordelijken in het bedrijfsleven en ambtenaren op het gebied van (verbeteren van) online veiligheid?**

Deze hoofdvraag bestaat uit drie deelvragen:

1. Wat weten de doelgroepen over online veiligheid en het verbeteren van de online veiligheid?

2. Wat vinden de doelgroepen van hun eigen online gedrag als het gaat om veiligheid en vaardigheden?

3. Wat doen de doelgroepen op het gebied van hun online veiligheid en het verbeteren daarvan?

Leeswijzer

Dit deelrapport geeft de resultaten van medewerkers en ICT-verantwoordelijken in het bedrijfsleven. Medewerkers worden in het rapport uitgesplitst naar verschillende grootteklassen en of men werkzaam is in de vitale infrastructuur. Ten behoeve van leesbaarheid worden ICT-verantwoordelijken in sommige figuren afgekort tot 'ICT'.

Hoofdstuk 1 t/m 3 van dit rapport behandelt de onderzoeksresultaten voor respectievelijk elk van de drie onderzoeksvragen.

Verantwoording

In totaal deden 1.066 medewerkers mee aan het onderzoek en 525 ICT-verantwoordelijken. Zij zijn deels afkomstig uit de steekproef Algemeen publiek en deels uit een aparte steekproef. De aparte steekproef bestond uit 2.625 medewerkers en 902 ICT-verantwoordelijken. Respondenten zijn afkomstig uit het I&O Research (consumenten) Panel en uit het I&O Bedrijven Panel. Het online veldwerk vond plaats van 7 t/m 19 juli 2021. Er zijn maximaal 2 reminders gestuurd tijdens het veldwerk.

Resultaten: kennis over online risico’s

Acht op de tien ICT-verantwoordelijken schatten eigen kennis over online veiligheid als redelijk tot zeer goed

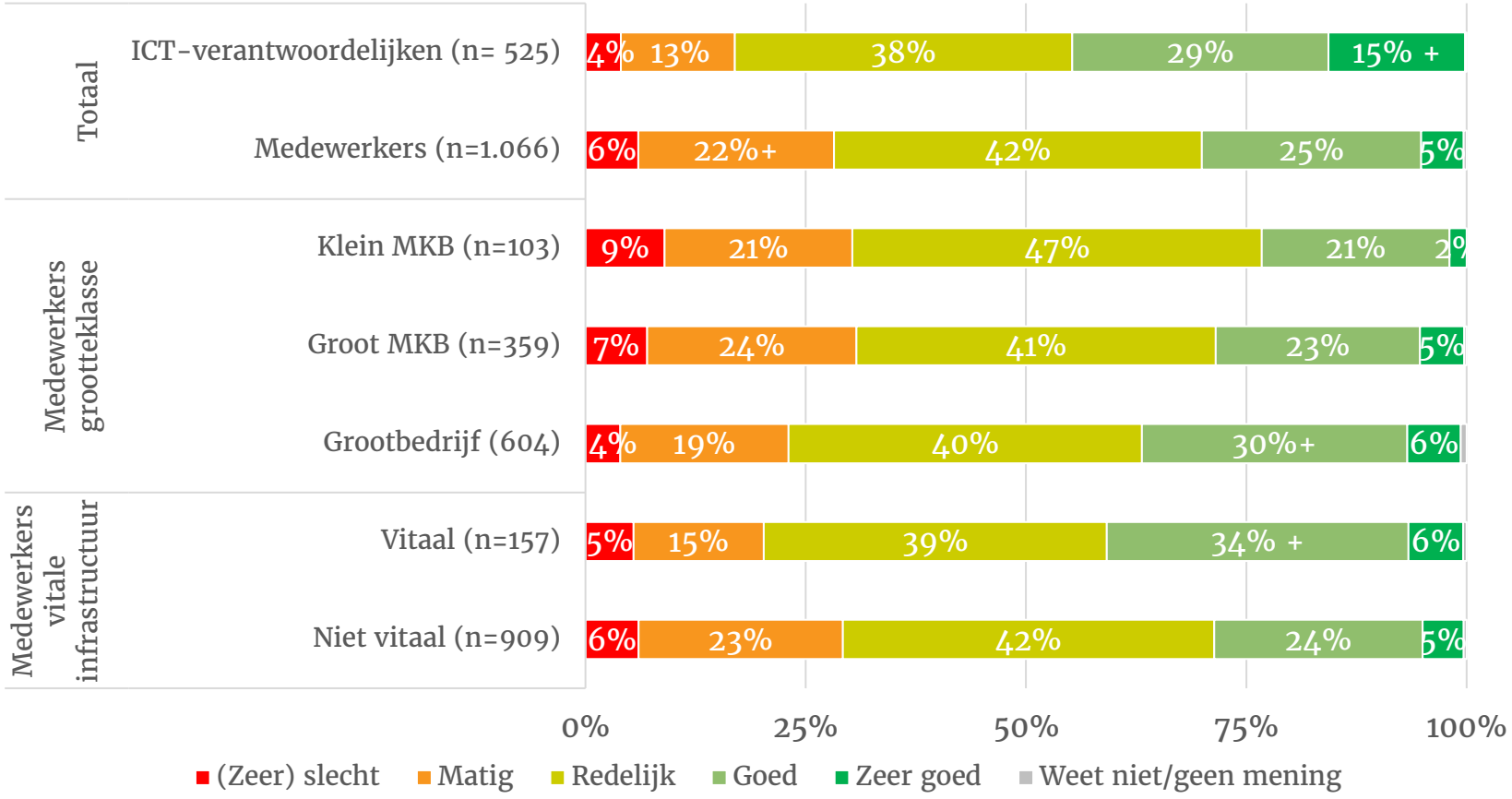
Net als in 2020 schatten medewerkers hun eigen kennis over online veiligheid gemiddeld lager dan ICT-verantwoordelijken. Toch schatten nog bijna twee op de tien ICT-verantwoordelijken hun kennis als matig tot (zeer) slecht (17%).

Ruim vier op de tien ICT-verantwoordelijken schatten hun kennis als (zeer) goed.

Drie op de tien medewerkers schatten hun kennis over online veiligheid als (zeer) goed (30%). Een vergelijkbaar aandeel (29%) schat hun eigen kennis als matig tot zeer slecht.

Deze resultaten zijn vergelijkbaar met 2020.

Hoe schat u uw eigen kennis over digitale en online veiligheid in?



ICT-verantwoordelijken denken vaker dan medewerkers te maken te krijgen met verschillende vormen van cybercrime

In het algemeen zijn ICT-verantwoordelijken iets vaker bekend met verschillende vormen van cybercrime dan medewerkers. Ook schatten ICT-verantwoordelijken de kans dat zij er in hun werksituatie mee te maken kunnen krijgen, hoger in dan medewerkers.

De kans om te maken te krijgen met verschillende vormen van cybercrime, wordt over het algemeen niet heel hoog ingeschat. Van phishing, malware, hacking, ransomware en DDoS-aanval wordt het vaakst gedacht dat men er in de werksituatie mee te maken kan krijgen.

Op deze en de volgende pagina staan 14 voorgelegde vormen van cybercriminaliteit, op volgorde van bekendheid	Kent de betekenis (naar eigen zeggen)		Herkent de omschrijving als correct*				Denkt er in werksituatie mee te maken te kunnen krijgen**			
	(n=525) ICT	(n=1.066) Medewerkers		ICT	Medewerkers			ICT	Medewerkers	
Phishing	98%	96%	n=92	94%	92%	n=237	n=513	69%	47%	n=1026
Hacking	98%	95%	n=88	98%	96%	n=243	n=510	60%	46%	n=1007
Identiteitsfraude	97%	95%	n=101	97%	98%	n=241	n=505	46%	29%	n=1012
Vriend-in-nood (whatsapp)-fraude	96%	92%	n=105	96%	93%	n=233	n=503	26%	18%	n=985
Bankhelpdeskfraude	88%	81%	n=78	85%	91%	n=176	n=462	38%	21%	n=872
Malware	91%	78%	n=88	89%	89%	n=172	n=473	67%	48%	n=846
DDoS-aanval	89%	73%	n=82	95%	98%	n=151	n=454	57%	45%	n=792

*Een juiste omschrijving voorgelegd van (willekeurig) 2 begrippen waarvan men de betekenis zegt te kennen. | percentage ik weet zeker dat het klopt + ik denk dat het klopt
**Alle begrippen voorgelegd waarvan men de betekenis zegt te kennen | percentage zeker + waarschijnlijk wel
Significantie verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met groen (hoger) of rood (lager).
Zie bijlage 1 en bijlage 2 voor een overzicht van medewerkers naar grootteklasse en vitale infrastructuur

ICT-verantwoordelijken zijn vaker bekend met specifieke vormen van cybercriminaliteit dan medewerkers

Crypojacking, social engineering en botnet zijn relatief onbekende vormen van cybercrime bij zowel medewerkers als ICT-verantwoordelijken. ICT'ers denken vaker dan medewerkers dat ze op het werk met deze specifieke vormen van cybercriminaliteit te maken krijgen. Ook met andere voorgelegde vormen van cybercrime denken ICT-verantwoordelijken vaker te maken te krijgen op het werk dan medewerkers dat denken.

Op deze en de vorige pagina staan 14 voorgelegde vormen van cybercriminaliteit, op volgorde van bekendheid	Kent de betekenis (naar eigen zeggen)		Herkent de omschrijving als correct*				Denkt er op het werk mee te maken te kunnen krijgen**			
	(n=525) ICT	(n=1.066) Medewerkers		ICT	Medewerkers			ICT		Medewerkers	
Helpdeskfraude	85%	73%	n=75	99%	87%	n=157	n=437	48%	28%	n=785
Ransomware	91%	70%	n=102	88%	88%	n=159	n=469	65%	47%	n=769
QR-codefraude	71%	63%	n=63	94%	96%	n=120	n=360	38%	23%	n=661
Spoofing	60%	43%	n=58	82%	80%	n=81	n=296	51%	35%	n=466
Cryptojacking	58%	35%	n=46	80%	78%	n=61	n=267	26%	16%	n=383
Social engineering	50%	25%	n=33	77%	64%	n=51	n=223	54%	36%	n=285
Botnet	53%	24%	n=33	90%	88%	n=33	n=245	46%	35%	n=264

*Een juiste omschrijving voorgelegd van (willekeurig) 2 begrippen waarvan men de betekenis zegt te kennen. | percentage ik weet zeker dat het klopt + ik denk dat het klopt
**Alle begrippen voorgelegd waarvan men de betekenis zegt te kennen | percentage zeker + waarschijnlijk wel
Significantie verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met groen (hoger) of rood (lager).
Zie bijlage 1 en bijlage 2 voor een overzicht van medewerkers naar grootteklasse en vitale infrastructuur

Resultaten: zorgen om online veiligheid

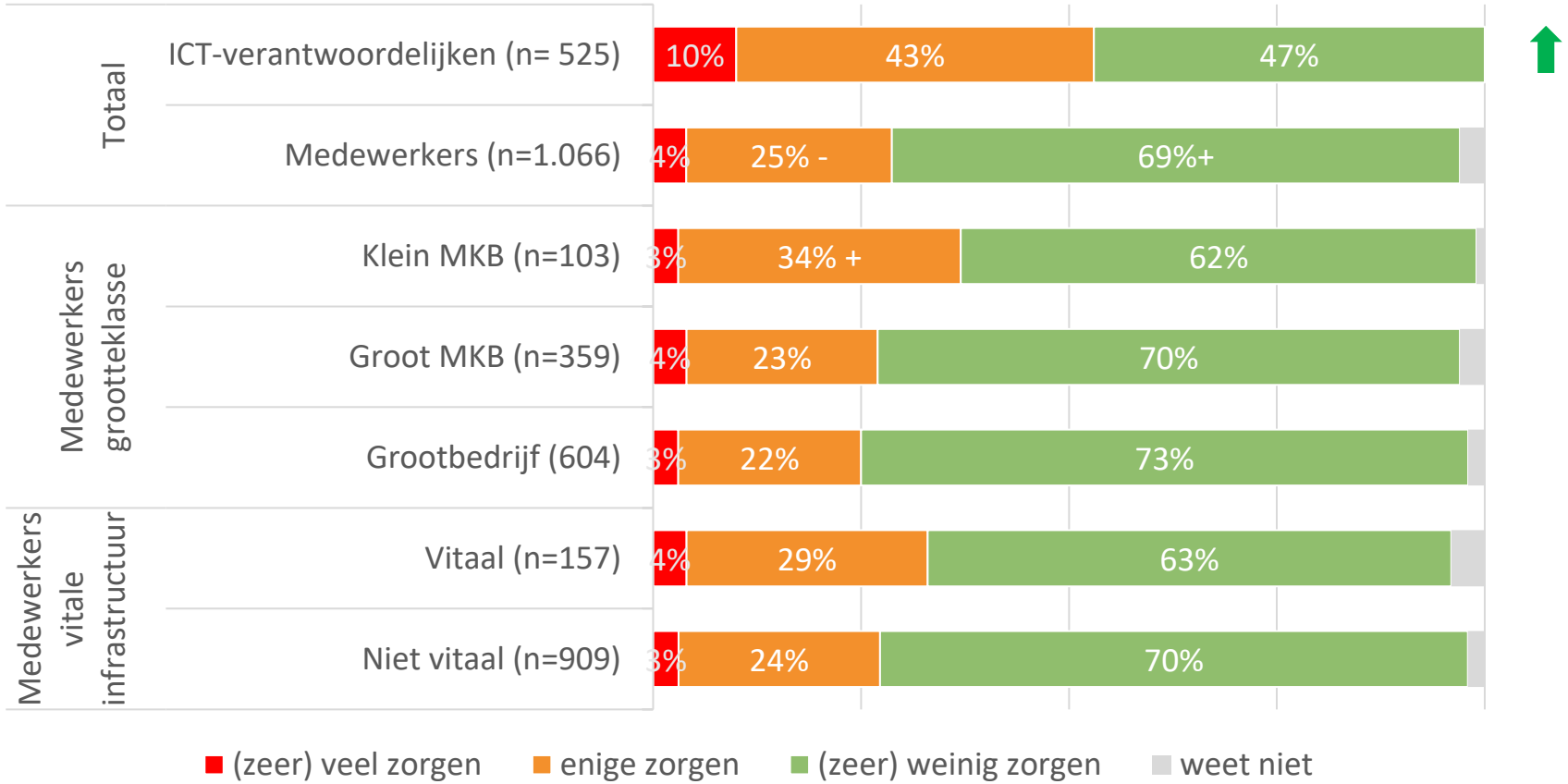
ICT-verantwoordelijken maken zich meer zorgen dan medewerkers over online veiligheid en deze zorgen zijn toegenomen ten opzichte van vorig jaar

Gemiddeld maken ICT-verantwoordelijken zich meer zorgen om digitale veiligheid op het werk dan medewerkers.

Een op de tien ICT-verantwoordelijken maakt zich (zeer) veel zorgen. Zorgen zijn toegenomen ten opzichte van 2020.

Zeven op de tien werknemers zeggen zich (zeer) weinig zorgen te maken. Dat is vergelijkbaar met 2020.

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



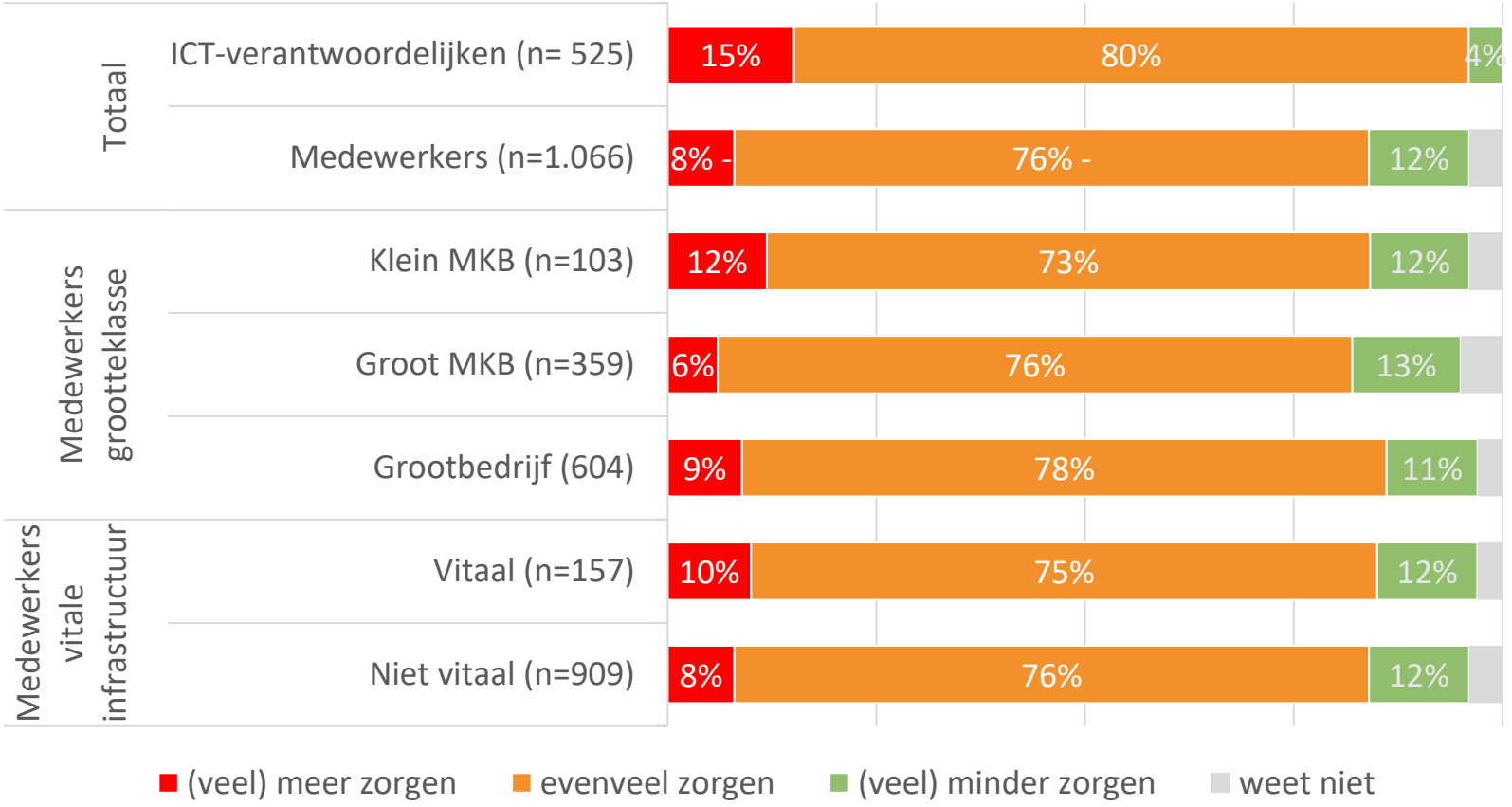
Significantie verschillen ten opzichte van 2020 zijn aangegeven met een ⬆ (meer zorgen).
Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en – (lager).
Verschillen naar grootteklasse en vitale infrastructuur zijn niet significant.

Bij ICT-verantwoordelijken zijn zorgen vaker toegenomen sinds de coronacrisis dan bij medewerkers

Een op de zeven ICT-verantwoordelijken zegt dat hun zorgen over hun online veiligheid zijn toegenomen sinds de coronacrisis (15%). Bij medewerkers is dit lager (8%).

Circa driekwart van beide groepen zegt dat zij evenveel zorgen hebben over hun online veiligheid als voor de coronacrisis.

Maakt u zich sinds de coronacrisis meer of minder zorgen over uw eigen online veiligheid in uw werksituatie?



Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en – (lager).
Verschillen naar grootteklasse en vitale infrastructuur zijn niet significant.

Een kwart van de medewerkers weet niet of er op hun werk acties zijn ondernomen voor veilig online gedrag

Van de medewerkers weet 27 procent niet of er acties zijn genomen en 8 procent zegt dat er geen enkele actie is ondernomen in hun bedrijf. Als er wel acties zijn genomen, dan lopen die sterk uiteen.

Welke acties zijn er binnen uw bedrijf/organisatie ondernomen ten behoeve van online veilig gedrag?	ICT	Medewerkers				
	Totaal n=525	Totaal n=1.066	Klein MKB n=103	Groot MKB n=359	Grootbedrijf n=604	Vitaal n=159
Alleen systeembeheerders kunnen software installeren	46%	41%	22%	40%	54%	50%
Afspraken over het gebruik van websites en/of e-mail	50%	37%	16%	35%	53%	52%
Afspraken gemaakt over het versturen/uitwisselen van bestanden	43%	32%	16%	29%	47%	47%
Afspraken gemaakt over hoe je veilig online thuiswerkt	41%	31%	13%	28%	48%	47%
Afspraken gemaakt over het versturen/uitwisselen van persoonsgegevens	49%	30%	19%	26%	46%	48%
Afspraken over gebruik zakelijke smartphones, laptops en/of tablets	42%	29%	8%	26%	49%	27%
Afspraken over gebruikmaken opslagmedia als usb-sticks of externe harde schijven	35%	27%	9%	25%	41%	45%
Afspraken over gebruik van sociale media	34%	23%	10%	19%	39%	41%
Toegang geblokkeerd tot bepaalde websites of sociale media	25%	22%	8%	18%	42%	38%
toegang geblokkeerd tot bepaalde verzendplatforms (zoals WeTransfer)	13%	11%	5%	8%	24%	22%
Het gebruik van USB-sticks in onze organisatie is onmogelijk gemaakt	9%	10%	5%	9%	18%	17%
geen enkele actie ten behoeve van veilig online gedrag	8%	8%	23%	7%	2%	4%
Weet ik niet	8%	27%	33%	30%	20%	22%

Significantie verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met groen (hoger) of rood (lager).
Hetzelfde geldt voor significante verschillen ten opzichte van het gemiddelde van medewerkers.

Wanneer men bekend is met de afspraken over online veiligheid, heeft men meestal ook begrip voor die afspraken

Van de medewerkers en ICT-verantwoordelijken die weten dat er in hun organisatie afspraken zijn over veilig online gedrag, heeft het merendeel ook begrip voor de maatregelen. Ook voelt bijna iedereen zich verantwoordelijk voor hun eigen online gedrag op het werk.

Zes tot zeven op de tien medewerkers en ICT-verantwoordelijken vinden de gemaakte afspraken duidelijk en denken ze allemaal te kennen. ICT-medewerkers denken vaker alle afspraken te kennen dan medewerkers.

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=428	Totaal n=747	Klein MKB n=45	Groot MKB n=229	Groot-bedrijf n=473	Vitaal n=125
Voelt zich **verantwoordelijk** voor eigen online gedrag op hun werk	96%	92%	91%	92% +	93% +	92% +
Heeft **begrip** voor de gemaakte afspraken	85%	87%	76%	85% +	93%	87%
Vindt de afspraken over online veilig moet gedrag **duidelijk**	71%	74%	67%	72%	80%	77%
Is bekend met **alle** afspraken over online veilig gedrag	71%	63%	60%	61%	66%	68%

Significantie verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met groen (hoger) of rood (lager).
Hetzelfde geldt voor significante verschillen ten opzichte van het gemiddelde van medewerkers.
Significante verschillen ten opzichte van 2020 zijn aangeven met + (hoger) of –(lager).

Aanspreken op online veilig gedrag gebeurt niet overal

Ongeveer zes op de zeven medewerkers en ICT-verantwoordelijken (werkend in een bedrijf waar afspraken zijn gemaakt), vinden het goed als hun collega's hen zouden aanspreken als ze zich niet aan de afspraken zouden houden. Dit percentage is hoger dan in 2020. Met name medewerkers doen dit omgekeerd zelf veel minder graag (46%).

Ruim de helft van beide groepen wordt weleens aangesproken op hun gedrag. Ruim vier op de tien ICT-verantwoordelijk en medewerkers vinden dat hun leidinggevende het goede voorbeeld geeft.

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=428	Totaal n=747	Klein MKB n=45	Groot MKB n=229	Groot-bedrijf n=473	Vitaal n=125
Vindt het goed als collega's hen aanspreken als ze zich niet aan de afspraken houden	87% +	84% +	78%	83%	86%	84%
Wordt op hun werk aangesproken als ze zich niet aan de afspraken houden	58%	53%	49%	51% -	57%	66%
Spreekt collega's er op aan als zij zich niet aan de afspraken houden	70%	46%	58%	43% -	48%	52%
Vindt dat hun leidinggevende het goede voorbeeld geeft m.b.t. veilig online gedrag	47%	43%	47%	41% -	45%	52%

Significantie verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met groen (hoger) of rood (lager).
Hetzelfde geldt voor significante verschillen ten opzichte van het gemiddelde van medewerkers.
Significante verschillen t.o.v. 2020 (op totaalniveau) zijn aangegeven met + hoger en – (lager)

Afspraken om online veilig gedrag te bevorderen kunnen nog vaker worden toegepast

Circa vier op de vijf medewerkers en ICT-verantwoordelijk vinden het makkelijk om zich aan de gemaakte afspraken te houden.

Er is ruimte voor verbetering als het gaat om goede tools ten behoeve van veilig online gedrag en het toepassen van de gemaakte afspraken. Circa twee derde vindt dat zij toegang krijgen tot goede tools voor veilig online gedrag op het werk en vindt dat de gemaakte afspraken voldoende worden toegepast.

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=428	Totaal n=747	Klein MKB n=45	Groot MKB n=229	Groot-bedrijf n=473	Vitaal n=125
Vindt het gemakkelijk om zich aan de afspraken te houden	80%	83%	84%	82%	83%	81%
Krijgt toegang tot goede tools en instrumenten om online veilig gedrag te bevorderen	71%	65%	62%	60%	74%	68%
Vindt dat de gemaakte afspraken voldoende worden toegepast	63%	65%	62%	62%	70%	74%

Significantie verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met groen (hoger) of rood (lager).
Hetzelfde geldt voor significante verschillen ten opzichte van het gemiddelde van medewerkers.
Significante verschillen t.o.v. 2020 (op totaalniveau) zijn aangegeven met + hoger en – (lager)

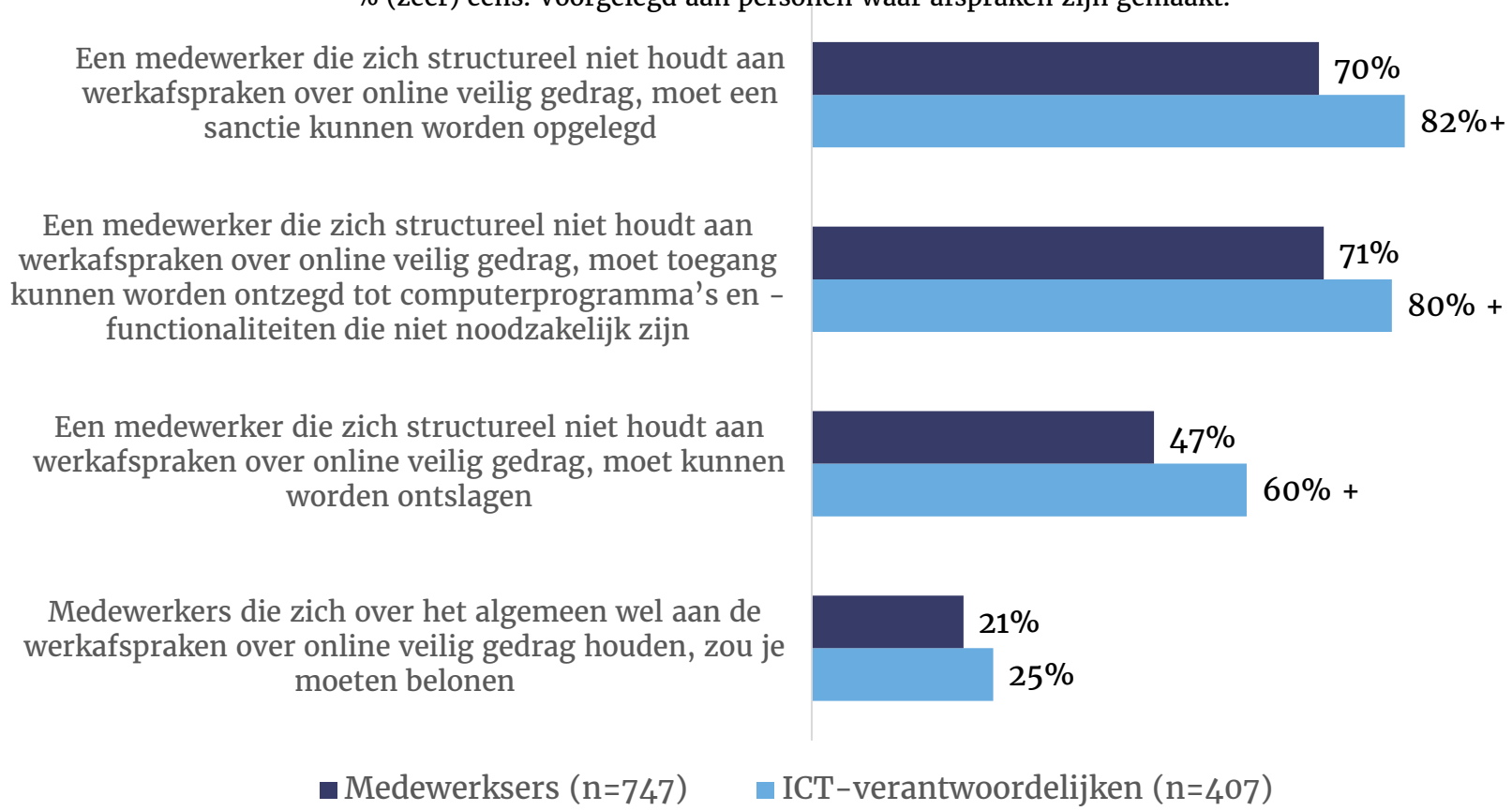
Meerderheid van medewerkers en ICT-verantwoordelijken vindt dat sancties mogen worden opgelegd als afspraken niet worden nageleefd

Circa 70 procent van de werknemers vindt dat sancties mogen worden opgelegd als een medewerkers zich niet aan de afspraken houdt en dat diegene toegang mag worden ontzegd. ICT-verantwoordelijken vinden nog wat vaker dat dat mag.

Als iemand afspraken structureel schendt, is ontslag geoorloofd volgens bijna de helft van de medewerkers en zes op de tien ICT-verantwoordelijken.

Slechts een klein percentage vindt een beloning terecht voor medewerkers die zich juist wel aan de afspraken houden.

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



Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en – (lager).
Zie bijlage 3 voor een uitsplitsing van medewerkers naar bedrijfsgrootte en vitale infrastructuur

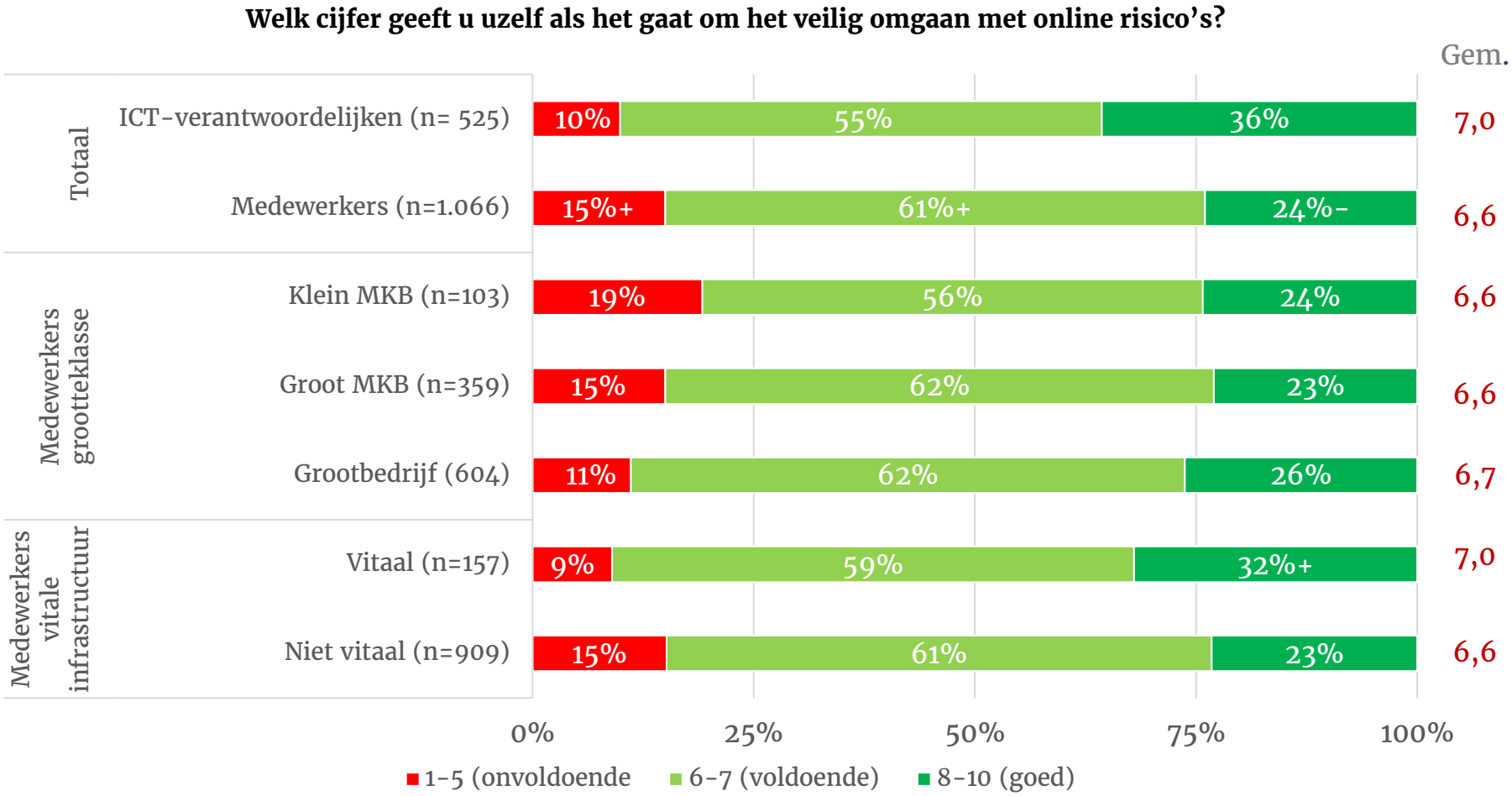
Resultaten: online gedrag

Zowel medewerkers en ICT-verantwoordelijken geven zichzelf een lager rapportcijfer dan in 2020

In vergelijking met medewerkers (24%) geven ICT-verantwoordelijk zichzelf gemiddeld vaker een hoog rapportcijfer voor hoe zij omgaan met online risico's (36%).

Toch geeft ook een op de tien ICT-ers zichzelf een onvoldoende op dit vlak.

Onder werknemers is het zelfs 15 procent die zichzelf een onvoldoende geeft.



Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met + (hoger) en – (lager).
Achter de grafiek staat het gemiddeld gegeven antwoord. Verschillen ten opzichte van 2020 zijn aangegeven met rood (lager) of groen (hoger).

Net als in 2020 zijn phishing en acquisitiefraude de meest voorkomende vormen van cybercriminaliteit in de werksituatie

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=525	Totaal n=1.066	Klein MKB n=103	Groot MKB n=359	Groot-bedrijf n=604	Vitaal n=159
Phishingmail ontvangen	51%	26%	26%	25%	29%	27%
Acquisitiefraude	28%	10%	13%	10%	7%	7%
Benaderd op social media met een vraag om een onbekende link aan te klikken	21%	8%	6%	8%	9%	14%
Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik	22%	7%	5%	7%	8%	7%
Een foute link ook daadwerkelijk aangeklikt	6%	3%	3%	4%	3%	2%
Website werkte tijdelijk niet (bijv. door DDoS-aanval)	6%	3%	1%	3%	4%	4%
Computer werkte tijdelijk niet door malware	3%	3%	1%	3%	3%	5%
Ransomware	3%	3%	2%	3%	4%	5%
Malware verspreid door downloaden geïnfecteerde software/ bestanden	5%	2%	2%	2%	3%	3%
Bestanden geopend/gegevens ingevuld n.a.v. een phishingbericht	4%	2%	0%	2%	1%	0%
Benaderd voor WhatsAppfraude	4%	2%	2%	2%	3%	6%
Identiteitsdiefstal	3%	2%	1%	3%	1%	4%
Iemand logde zonder toestemming bij een apparaat in	1%	2%	2%	3%	2%	3%
Iemand logde zonder toestemming bij een account in	3%	1%	0%	2%	1%	2%

Significantie verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met groen (hoger) of rood (lager).
Hetzelfde geldt voor significante verschillen ten opzichte van het gemiddelde van medewerkers.

De helft van de medewerkers en ICT-verantwoordelijken maakt geen melding van cybercrime

De helft van de medewerkers en ICT-verantwoordelijken doet geen aangifte bij een (poging) tot cybercrime in hun werksituatie. Als men wel melding maakt dan doet men dat in de meeste gevallen bij de ICT-afdeling van hun bedrijf. Op gepaste afstand volgt een melding bij de fraudehelpdesk.

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=347	Totaal n=407	Klein MKB n=42	Groot MKB n=128	Groot-bedrijf n=237	Vitaal n=65
Melding bij de ICT-afdeling van hun bedrijf	28%	32%	10%	30%	49%	34%
Melding bij fraudehelpdesk	16%	9%	12%	9%	6%	10%
Aangifte bij de politie	4%	4%	0%	5%	4%	4%
Melding bij de politie	2%	3%	5%	4%	2%	1%
Melding bij de gemeente	2%	1%	0%	2%	0%	0%
Melding bij SeniorWeb	0%	1%	0%	2%	0%	0%
Ergens anders	8%	3%	2%	3%	4%	5%
Heeft niets gedaan	**50%**	**52%**	**71%**	**52%**	**41%**	**49%**

Significantie verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met groen (hoger) of rood (lager).
Hetzelfde geldt voor significante verschillen ten opzichte van het gemiddelde van medewerkers.

Back-ups worden vaker door werkgever gemaakt dan door werknemer zelf

Back-ups worden niet door iedereen regelmatig gemaakt en het is vaker de werkgever die dit doet dan werknemers zelf. Een deel van de werknemers ervaart belemmeringen om een back-up te maken. Van de medewerkers zegt 15 procent niet te weten hoe zij een back-up moeten maken en 19 procent vindt dat dit teveel tijd kost. Bij ICT-ers is dit 7 procent (weet niet hoe) en 15 procent (kost teveel tijd).

Negen op de tien medewerkers en ICT-verantwoordelijken zouden direct melding doen als ze een virus hebben gedownload.

Iets minder dan een op de tien werknemers verstuurt wel eens werkbestanden naar hun privémail.

Een klein aandeel van de werknemers met een werktelefoon of laptop, laat die gebruiken door hun kinderen.

In hoeverre zijn de volgende uitspraken van toepassing op uw gedrag? % meestal wel + altijd (percentages exclusief categorie 'niet van toepassing')	ICT n=525	Medewerkers n=1.066
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	93%	89%
Mijn werkgever maakt automatisch back-ups van alle bestanden (volledige back-ups)	81%	64%
Ik maak op mijn werk regelmatig back-ups van de bestanden op mijn werklaptop	63%	41%
Ik verstuur werkbestanden van mijn werk e-mailadres naar mijn privé e-mail.	9%	8%
Ik laat mijn kind(eren) gebruikmaken van mijn werktelefoon	4%	7%
Ik laat mijn kind(eren) gebruikmaken van mijn werklaptop	3%	5%

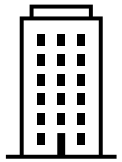
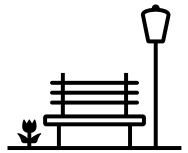
Zie bijlage 4 voor een uitsplitsing van de resultaten van medewerkers naar bedrijfsgrootte en vitale infrastructuur
Significantie verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met groen (hoger) of rood (lager).

Medewerkers van grootbedrijven werkten de afgelopen 12 maanden minder vaak op kantoor dan in 2020

Vanwege het coronavirus werkten veel mensen het afgelopen jaar vaker thuis dan daarvoor. Zes op de tien medewerkers werkten de afgelopen 12 maanden thuis.

Van de ICT'ers zelfs 80 procent. Een behoorlijk aandeel werkte daarnaast (ook) weleens vanuit kantoor en sommigen op een openbare locatie.

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

	ICT	Medewerkers				
	Totaal n=525	Totaal n=1.066	Klein MKB n=103	Groot MKB n=359	Groot-bedrijf n=604	Vitaal n=157
	68%	61%	51%	66%	56% ↓	63%
	80%	57%	61%	53%	62%	67%
	13%	18%	24%	17%	17%	19%

Significantie verschillen ten opzichte van 2020 zijn aangegeven met een ↓ (lager).
Verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met groen (hoger) of rood (lager).
Hetzelfde geldt voor verschillen binnen medewerkers naar verschillende grootteklassen of de vitale infrastructuur.

Drie op de tien medewerkers gebruiken thuis een router met het standaard wachtwoord

De meest gebruikte netwerkverbinding thuis is een (wifi)netwerkverbinding (router) met wachtwoord. Bij ICT-verantwoordelijken is dit in 79 procent van de gevallen een zelf gekozen wachtwoord. Medewerkers hebben minder vaak zelf een wachtwoord gekozen (60%) en gebruiken in 37 procent van de gevallen het standaard (bijgeleverde) wachtwoord. Dit komt neer op 31 procent van alle medewerkers.

Zelfverzonnen wachtwoorden bestaan in de meeste gevallen uit een combinatie van bijvoorbeeld verschillende lettergroottes, cijfers, leestekens, of bijzondere karakters. Niet iedereen met een zelfverzonnen wachtwoord, gebruikt een heel lang wachtwoord. Bij 47 procent van de ICT-verantwoordelijken en 44% van de medewerkers is het wachtwoord minimaal 12 tekens lang.

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	86%	83%	92%	83%	78%	83%
Een VPN verbinding en/of cloud verbinding (‘in de cloud werken’)	53%	41%	25%	41%	49%	50%
Via een internetkabel (niet draadloos; LAN)	39%	23%	16%	24%	24%	25%
Een hotspot verbinding (3G/4G/5G) via mijn smartphone of tablet	10%	8%	14%	6%	7%	6%
Een (wifi-)netwerkverbinding zonder wachtwoord (bv openbaar)	0%	1%	0%	2%	1%	1%

Significantie verschillen tussen ICT-verantwoordelijken en medewerkers zijn aangegeven met groen (hoger) of rood (lager).
Hetzelfde geldt voor significante verschillen ten opzichte van het gemiddelde van medewerkers.

Bijlagen

Bijlage 1 | Bekendheid met vormen van cybercrime

In welke mate bent u bekend met de onderstaande zaken? % Daar heb ik zelf weleens mee te maken gehad +Ik ken iemand die er wel eens mee te maken heeft gehad + Nooit mee te maken gehad, maar ik weet wel wat dit is	Medewerkers							
	Klein MKB		Groot MKB		Grootbedrijf		Vitaal	
Phishing	n=103	96%	n=359	96%	n=604	97%	n=157	100%
Hacking	n=103	94%	n=359	95%	n=604	94%	n=157	96%
Identiteitsfraude	n=103	96%	n=359	95%	n=604	95%	n=157	97%
Vriend-in-nood (whatsapp)-fraude	n=103	91%	n=359	92%	n=604	93%	n=157	89%
Bankhelpdeskfraude	n=103	77%	n=359	82%	n=604	83%	n=157	89%
Malware	n=103	75%	n=359	77%	n=604	81%	n=157	91%
DDoS-aanval	n=103	66%	n=359	74%	n=604	75%	n=157	80%
Helpdeskfraude	n=103	69%	n=359	74%	n=604	74%	n=157	82%
Ransomware	n=103	64%	n=359	69%	n=604	75%	n=157	79%
QR-codefraude	n=103	60%	n=359	65%	n=604	61%	n=157	66%
Spoofing	n=103	49%	n=359	40%	n=604	45%	n=157	49%
Cryptojacking	n=103	30%	n=359	36%	n=604	36%	n=157	47%
Social engineering	n=103	20%	n=359	24%	n=604	29%	n=157	38%
Botnet	n=103	18%	n=359	25%	n=604	26%	n=157	30%

Significantie verschillen ten opzichte van andere medewerkers zijn aangegeven met groen (hoger) of rood (lager).

Bijlage 2 | Waarmee denkt men in de werksituatie te maken te kunnen krijgen

In hoeverre denkt u in uw werksituatie te maken kunt krijgen met deze vormen van cybercriminaliteit?** % zeker wel + waarschijnlijk wel	Medewerkers							
	Klein MKB		Groot MKB		Grootbedrijf		Vitaal	
Phishing	n=99	53%	n=345	44%	n=582	50%	n=157	49%
Hacking	n=97	47%	n=342	45%	n=568	46%	n=152	51%
Identiteitsfraude	n=99	34%	n=338	26%	n=575	31%	n=151	29%
Vriend-in-nood (whatsapp)-fraude	n=94	21%	n=331	17%	n=560	17%	n=144	18%
Bankhelpdeskfraude	n=80	34%	n=293	19%	n=499	20%	n=139	20%
Malware	n=78	53%	n=277	46%	n=491	50%	n=142	49%
DDoS-aanval	n=68	38%	n=268	43%	n=456	52%	n=127	56%
Helpdeskfraude	n=72	34%	n=264	25%	n=449	31%	n=129	32%
Ransomware	n=66	47%	n=251	46%	n=452	49%	n=127	50%
QR-codefraude	n=61	33%	n=232	20%	n=368	26%	n=106	16%
Spoofing	n=51	32%	n=143	36%	n=272	35%	n=85	35%
Cryptojacking	n=31*	22%	n=131	13%	n=221	19%	n=76	15%
Social engineering	n= te laag		n=85	20%	n=179	25%	n=62	33%
Botnet	n= te laag		n=86	30%	n=159	37%	n=53	31%

Significantie verschillen ten opzichte van andere medewerkers zijn aangegeven met groen (hoger) of rood (lager).
* Indicatief: lage n
**Alleen begrippen voorgelegd waarvan men de betekenis zegt te kennen

Bijlage 3 | Welke maatregelen mag een organisatie volgens werknemers nemen om naleving regels te bevorderen (1/2)

In hoeverre bent u het eens of oneens met de volgende stellingen? % (zeer) eens. Voorgelegd aan personen waar afspraken zijn gemaakt.	Medewerkers			
	Klein MKB n=45	Groot MKB n=229	Groot-bedrijf n=473	Vitaal n=125
Een medewerker die zich structureel niet houdt aan werkafspraken over online veilig gedrag, moet een sanctie kunnen worden opgelegd	71%	69%	73%	77%
Een medewerker die zich structureel niet houdt aan werkafspraken over online veilig gedrag, moet toegang kunnen worden ontzegd tot computerprogramma's en -functionaliteiten die niet noodzakelijk zijn	67%	71%	73%	69%
Een medewerker die zich structureel niet houdt aan werkafspraken over online veilig gedrag, moet kunnen worden ontslagen	56%	45%	48%	48%
Medewerkers die zich over het algemeen wel aan de werkafspraken over online veilig gedrag houden, zou je moeten belonen	24%	19%	23%	23%

Significantie verschillen ten opzichte van andere medewerkers zijn aangegeven met groen (hoger) of rood (lager).

Bijlage 4 | Welke maatregelen mag een organisatie volgens werknemers nemen om naleving regels te bevorderen (2/2)

In hoeverre zijn de volgende uitspraken van toepassing op uw gedrag? % meestal wel + altijd (percentages exclusief categorie 'niet van toepassing')	Medewerkers			
	Klein MKB n=103	Groot MKB n=359	Groot-bedrijf n=604	Vitaal n=157
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	94%	89%	86%	91%
Mijn werkgever maakt automatisch back-ups van alle bestanden (volledige back-ups)	53%	66%	66%	68%
Ik maak op mijn werk regelmatig back-ups van de bestanden op mijn werklaptop	46%	44%	34%	49%
Ik verstuur werkbestanden van mijn werk e-mailadres naar mijn privé e-mail	9%	8%	8%	8%
Ik laat mijn kind(eren) gebruikmaken van mijn werktelefoon	7%	7%	2%	5%
Ik laat mijn kind(eren) gebruikmaken van mijn werklaptop	2%	5%	4%	4%

Verschillen tussen de deelgroepen op deze pagina zijn indicatief en moeten met voorzichtigheid worden geïnterpreteerd.
De basis van de percentages verschilt, omdat deze is berekend exclusief het percentage dat 'niet van toepassing' zegt.
Het hoogste geval is 58% van de medewerkers kleinbedrijf die 'niet van toepassing' zeggen op de stelling of hun kind gebruikmaakt van hun werktelefoon.

I&O Research Enschede

Zuiderval 70
Postbus 563
7500 AN Enschede
T (053) 200 52 00
E info@ioresearch.nl
KvK-nummer 08198802

I&O Research Amsterdam

Piet Heinkade 55
1019 GM Amsterdam
T (020) 308 48 00
E info@ioresearch.nl