# Nationaal Cybersecurity Bewustzijnsonderzoek 2019

## Cyberbewustzijn en vaardigheden onder de Nederlandse (beroeps)bevolking

Willemijn Bot
Kevin Hengstz

19 september 2019

Omnicom Public Relations Group

ALERT online

motivaction research and strategy

# Achtergrond

In opdracht van Omnicom Public Relations Group heeft Motivaction International B.V. voor het derde jaar op rij onderzoek uitgevoerd voor de Alert Online-campagne naar het bewustzijn van cybergevaren en het online gedrag van de Nederlandse (beroeps-)bevolking.

## Aanleiding

In 2012 is de NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid) de campagne Alert Online gestart om de bewustwording op het gebied van cybersecurity te verhogen en online bewust gedrag te laten integreren in de levensstijl van mensen en organisaties. In de campagneperiode is landelijk aandacht voor het belang van cybersecurity, zowel thuis als onderweg en op het werk.

## Doelstelling

Voorafgaand aan de campagne die jaarlijks in oktober of november plaatsvindt wordt een grootschalig onderzoek onder de Nederlandse bevolking uitgevoerd. Het doel van dit onderzoek is om de *cyber awareness* en de *cyber skills* van Nederlanders te monitoren door de jaren heen. Een belangrijke pijler voor de Alert Online campagne is om de bewustwording van cybergevaren bij burgers en werkgevers te vergroten en handelingsperspectieven te bieden voor veilig gebruik van cybermiddelen. Het doel van dit onderzoek dient beide doelstellingen: enerzijds het vergaren van kennis over gedrag van Nederlanders met betrekking tot cyberveiligheid en anderzijds het bieden van inzichten voor een succesvolle Alert Online-campagne.

# Samenvattende conclusies (1/4)

**Twee derde van de Nederlanders schat in dat de eigen kennis over digitale en online veiligheid goed is**

Over het algemeen schat een meerderheid van de Nederlanders in dat hun kennis over digitale en online veiligheid goed is. Bijna zeven op de tien Nederlanders zeggen dat die kennis op z'n minst redelijk is, volgens een kwart is die zelfs goed tot zeer goed.

De kennis over cyberrisico's groeit gestaag. Ook minder voorkomende gevaren, zoals portscans en keyloggers, zijn dit jaar bekender bij het brede publiek. Tegelijkertijd neemt ook de bekendheid van phishing mails en cyberaanvallen nog toe. Desondanks blijft de bekendheid van risico's onder het Nederlands publiek nog wel achter bij die van de werkende doelgroepen.

**MKB'er schatten de schade van digitale risico's relatief laag in**

De schade van digitale risico's schatten Nederlanders relatief beperkt in. Onder professionele doelgroepen zijn daar veel verschillen te zien: medewerkers die in vitale sectoren werken schatten de gevolgen een stuk ernstiger in dan MKB'ers, met name bij kleine MKB-bedrijven.

Het merendeel van de Nederlanders is bekend met maatregelen die ze kunnen treffen om zich te beschermen tegen online criminaliteit. Het grote publiek wordt bovendien steeds bekender met opties als een digitale wachtwoordkluis of wachtwoordmanager, VPN-verbindingen, open source hard- en software en web tracking blockers.

**Minder vaak sprake van cybercriminaliteit op privé sociale media dan vorig jaar**

Hoewel de bekendheid en het bewustzijn groeit, hebben Nederlanders naar hun eigen idee niet vaker te maken met online of digitale criminaliteit. Zowel privé als op het werk is het aandeel Nederlanders dat weleens te maken heeft gehad met een cybervoorval min of meer gelijk aan vorig jaar. Dat geldt niet voor cybercriminaliteit via sociale media in een privésituatie: vrijwel alle doelgroepen geven aan dat dit tegenwoordig minder vaak voorkomt.

Hoewel het aantal ervaringen met cybercriminaliteit gelijk blijft, nemen Nederlanders vaker maatregelen. Het type maatregelen verandert wel: zowel werkende als niet-werkende Nederlanders installeren bijvoorbeeld minder vaak een firewall. Dat wil uiteraard niet zeggen dat ze minder goed beschermd zijn; wellicht hadden ze die firewall al eerder geïnstalleerd.

# Samenvattende conclusies (2/4)

**55% van de Nederlanders checkt het mailadres om phishingmails te ontmaskeren**

Dit jaar is in het onderzoek meer nadruk gelegd op phishing: hoe vaak gebeurt het, wat zijn de gevolgen en hoe proberen Nederlanders te voorkomen dat ze erin trappen? Het aantal ervaringen met phishing ligt op een vergelijkbaar niveau als vorig jaar, en circa één op de acht (werkende) Nederlanders zegt weleens op het werk daadwerkelijk op een foute link te hebben geklikt. In de meeste gevallen was het toen zo dat internetcriminelen onterecht toegang kregen tot bepaalde systemen en gegevens. In mindere mate zijn ook bestanden kwijtgeraakt of gegevens in verkeerde handen geraakt.

De meeste Nederlanders kijken vooral naar het mailadres van de afzender om een phishing mail te ontmaskeren. Circa een derde van de Nederlanders kijkt naar taalgebruik en schrijfstijl. Slechts een klein deel van de Nederlanders geeft aan mails nooit te controleren op echtheid, of geeft aan phishing mails echt niet te kunnen herkennen.

**Zorgen over diefstal van online identiteit gegroeid**

De mate waarin Nederlanders zich zorgen maken om hun online veiligheid thuis is vergelijkbaar met vorig jaar. Op het werk maken Nederlanders zich juist meer zorgen, met name MKB'ers en ambtenaren. Wellicht komen die grotere zorgen voort uit meer bewustzijn van en meer (publieke en media-)aandacht voor cybergevaren; het aantal ervaringen met cybervoorvallen op het werk is immers gelijk gebleven.

Als we inzoomen op twee specifieke voorvallen – diefstal van een online identiteit en cyberaanvallen – is te zien dat met name de zorgen over dat eerste gegroeid zijn. Niet alleen onder het Nederlands publiek, maar ook onder de werkende doelgroepen. De zorgen om een cyberaanval zijn gelijk gebleven, of zelfs gedaald.

Nederlanders verwachten nog altijd het meeste risico te lopen als ze een link in een e-mail openen. Vergeleken met vorig jaar zien ze echter ook openbare computers vaker als een belangrijk risico.

# Samenvattende conclusies (3/4)

**Veilig online gedrag: niet op onbekende links klikken, verschillende wachtwoorden gebruiken en geen persoonlijke gegevens delen online**

De associatie die veel Nederlanders hebben bij veilig online gedrag op het werk en privé verschillen niet: meestal denken ze aan niet op onbekende links klikken, verschillende wachtwoorden gebruiken en geen persoonlijke gegevens delen online. Het merendeel van de Nederlanders geeft aan dat ze naar hun idee veilig omgaan met verschillende online zaken. Nederlanders geven zich zelf dit jaar een hoger rapportcijfer voor 'veilig omgaan met online gevaren'.

De antwoorden die respondenten geven over stellingen over gedrag laten het beeld zien dat ongeveer de helft van de Nederlanders inderdaad (meestal) veilig bezig is online. Zij loggen accounts uit op openbare computers, passen privacy-instellingen aan, bezoeken alleen websites met een groen slotje of maken thuis regelmatig back-ups van bestanden. Tegelijkertijd is er dus nog een aanzienlijk deel van de bevolking dat dat meestal nog niet doet.

**Een derde van de Nederlanders vindt de instructies voor online en digitale bescherming ingewikkeld**

Of veiligheidsmaatregelen een belemmering vormen, verdeelt het Nederlands publiek. Circa een vijfde ziet zulke zaken – zoals tweestapsverificatie of het niet automatisch kunnen opslaan van wachtwoorden – als een te grote belemmering. Anderzijds ziet circa de helft van de Nederlanders dat niet zo. Ruim een derde vindt de instructies om je online en digitaal te beschermen vaak ingewikkeld.

# Samenvattende conclusies (4/4)

Dit jaar is voor het eerst uitgebreid aandacht besteed aan cybersecurity op de werkvloer: worden daar afspraken over gemaakt, hoe gaan medewerkers en leidinggevenden daarmee om en lukt het bedrijven en organisaties om die afspraken te borgen?

**Medewerkers naar eigen zeggen meer compliant dan leidinggevenden**

De meeste werknemers geven aan dat bij hun organisatie of bedrijf inderdaad sprake is van afspraken over hoe zij zich veilig kunnen gedragen online. Meestal zijn dat afspraken over het gebruik van websites en e-mail en het veilig versturen van bestanden. Leidinggevenden hebben daarnaast relatief vaak afspraken over het gebruik van sociale media op het werk. Een kwart van de medewerkers geeft aan niet op de hoogte te zijn of er bij hun werkgever sprake is van dergelijke afspraken.

Als die afspraken er zijn, dan houdt een meerderheid zich er ook aan. Die compliance ligt hoger onder medewerkers dan onder leidinggevenden. Medewerkers hebben eveneens vaker begrip voor de maatregelen en vinden het vaker gemakkelijk om zich er aan te houden dan leidinggevenden. Ook voelen zij zich meer verantwoordelijk voor hun eigen online gedrag. Ze zien leidinggevenden relatief minder als een goed voorbeeld op dit vlak. Vergeleken met leidinggevenden zijn medewerkers wel minder geneigd collega's er op aan te spreken als ze zien dat die de afspraken overtreden. Ondanks de verschillen tussen medewerkers en leidinggevenden, heeft ook een meerderheid van de leidinggevenden wel een positieve, begripvolle houding over de werkafspraken over online veilig gedrag.

**Eén op de vijf werkgevers monitort (vrijwel) nooit of medewerkers zich houden aan de afspraken over online veilig gedrag**

Of er ook gemonitord wordt in hoeverre werknemers zich aan de gemaakte afspraken houden, verschilt sterk. Bij drie op de tien werkgevers meten ze dat structureel, bij ruim een kwart incidenteel en bij een vijfde (vrijwel) nooit. Zes op de tien leidinggevenden ervaren belemmeringen bij het borgen van de afspraken. Meestal gaat het dan om een gebrek aan prioriteit ervoor, en communicatie erover.

Een aanzienlijk deel van de leidinggevenden vindt dat de gevolgen bij overtreding van afspraken over online veilig gedrag verregaand mogen zijn. Driekwart is van mening dat sancties gerechtvaardigd zijn, en 44% vindt dat je werknemers moet kunnen ontslaan als een medewerker zich niet aan de afspraken houdt.

# Campagnekansen en -mogelijkheden

De resultaten uit dit onderzoek worden ook gebruikt om de doelgroepen bewust te maken van cybersecurity en om hen concrete handelingsperspectieven te bieden. Campagnerichtingen die wij o.b.v. de resultaten zien, zijn de volgende:

**GAMIFICATION: secure gedrag naar 100%**
- Hoe cybersecure ben je nu (bijv. o.b.v. p40)? En hoe kun je naar 100% cybersecure gaan? Of hoe scoor je t.o.v. anderen (SOCIAL PROOF)

**GOED OP WEG: awareness groeit elk jaar (Geen FEAR campagne, FEEDBACK & CONSISTENCY)**
- Veel awareness indicatoren zien positieve groei. Goed op weg, maar hoe blijf je op de hoogte van nieuwe dreigingen?

**ZORGEN WEGNEMEN: maak je geen zorgen, wij helpen je**
- Wij zijn op de hoogte van de belangrijkste zorgen, en wij ondernemen actie zoals:…..

**LEAD BY EXAMPLE: B2B-campagne**
- Medewerkers vinden dat ze het beter doen dan leidinggevenden wanneer het gaat om cybersecurity

**VEILIGER ONLINE IS NIET MAKKELIJK. Wij helpen jou de volgende stap te zetten (ACKNOWLEDGE RESISTENCE)**
- Je kunt niet leren zonder (tijd) te investeren  Internetcriminelen worden steeds slimmer, neem de moeite om je ertegen te wapenen

**EMOTIONELE WAARDE: ook privé is er wel degelijk iets te halen**
- Privé is men minder veilig dan op het werk, terwijl je privé misschien wel meer te verliezen hebt

# Methode en opzet (1/2)

## Veldwerkperiode en respons

Het onderzoek is kwantitatief online uitgevoerd onder het ISO-26362-gecertificeerde webpanel van Motivaction, StemPunt. Het veldwerk is tussen 26 juni en 10 juli online uitgevoerd. Via een link in de uitnodigingsmail kwamen respondenten direct in de online vragenlijst terecht.

## Steekproef en doelgroepen

De onderzoekspopulatie van dit onderzoek bestaat uit een representatieve steekproef van n = 1.004 Nederlanders in de leeftijd van 16 tot 80 jaar.* Naast de representatieve steekproef voor Nederlanders worden de resultaten van vijf specifieke groepen werkenden weergegeven (zie volgende pagina voor de beschrijving van de groepen). Om uitspraken te kunnen doen over de verschillende groepen zijn voor de subgroepen aanvullend respondenten geworven om de benodigde minimale steekproefomvang van n = 250 te behalen. In een aantal gevallen is gebruik gemaakt van een partnerbureau om respondenten te benaderen. De totale onderzoeksgroep van Nederlanders en beroepsbevolking bestond uit n = 1.818 personen.

## Weging

De netto steekproef van n = 1.004 Nederlanders (16 tot 80 jaar) is gewogen om verschillen ten opzichte van de Nederlandse bevolking te corrigeren. Op basis van de CBS Gouden Standaard is de data gewogen op leeftijd, geslacht, opleidingsniveau en regio. De aanvullende steekproeven binnen de werkzame bevolking zijn niet gewogen omdat hier geen referentiecijfers van beschikbaar zijn.

* In eerdere metingen (2017 en 2018) zijn Nederlanders in de leeftijd van 13 – 80 jaar ondervraagd. Vanwege wettelijke beperkingen is het niet langer mogelijk Nederlanders jonger dan 16 jaar te betrekken bij onderzoek zonder expliciete toestemming van hun ouders/verzorgers. Om die reden is de ondergrens per 2019 verhoogd naar 16 jaar. De resultaten van de eerdere metingen uit 2017 en 2018 in deze rapportage zijn wel gebaseerd op 13- t/m 80-jarigen.

# Methode en opzet (2/2)

## Doelgroepen

In de rapportage geven we de resultaten weer voor de Nederlandse bevolking van 16 tot en met 80 jaar. Waar het vragen over de werksituatie betreft worden alleen percentages weergegeven van de werkzame bevolking. Naast de representatieve steekproef onder het Nederlandse publiek worden de resultaten van vijf specifieke groepen werkenden weergegeven:

- 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)
- Ambtenaren
- Medewerkers in de vitale infrastructuur
    - Deze doelgroep is gedefinieerd als werknemers die van hun werkgever een pc, laptop, smartphone en/of tablet ter beschikking hebben gekregen en 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

# Leeswijzer

## Significante verschillen

In de rapportage gaan we in op significante verschillen. Enerzijds bespreken we verschillen tussen de vijf subdoelgroepen, daarnaast gaan we – waar relevant en mogelijk – in op verschillen met de vorige meting uit 2018. Voor de doelgroep Nederlands publiek bespreken we – in tekstkaders – eveneens verschillen naar leeftijd, opleidingsniveau of geslacht, mits die van toegevoegde waarde zijn. Alle resultaten, inclusief verschillen tussen doelgroepen en metingen, zijn terug te vinden in het separaat geleverde tabellenboek.

Door het hele rapport worden de significante verschillen aangegeven met een kleur, in de vorm van pijlen, kaders en gekleurde cijfers.

**Groen** = significante **over**vertegenwoordiging

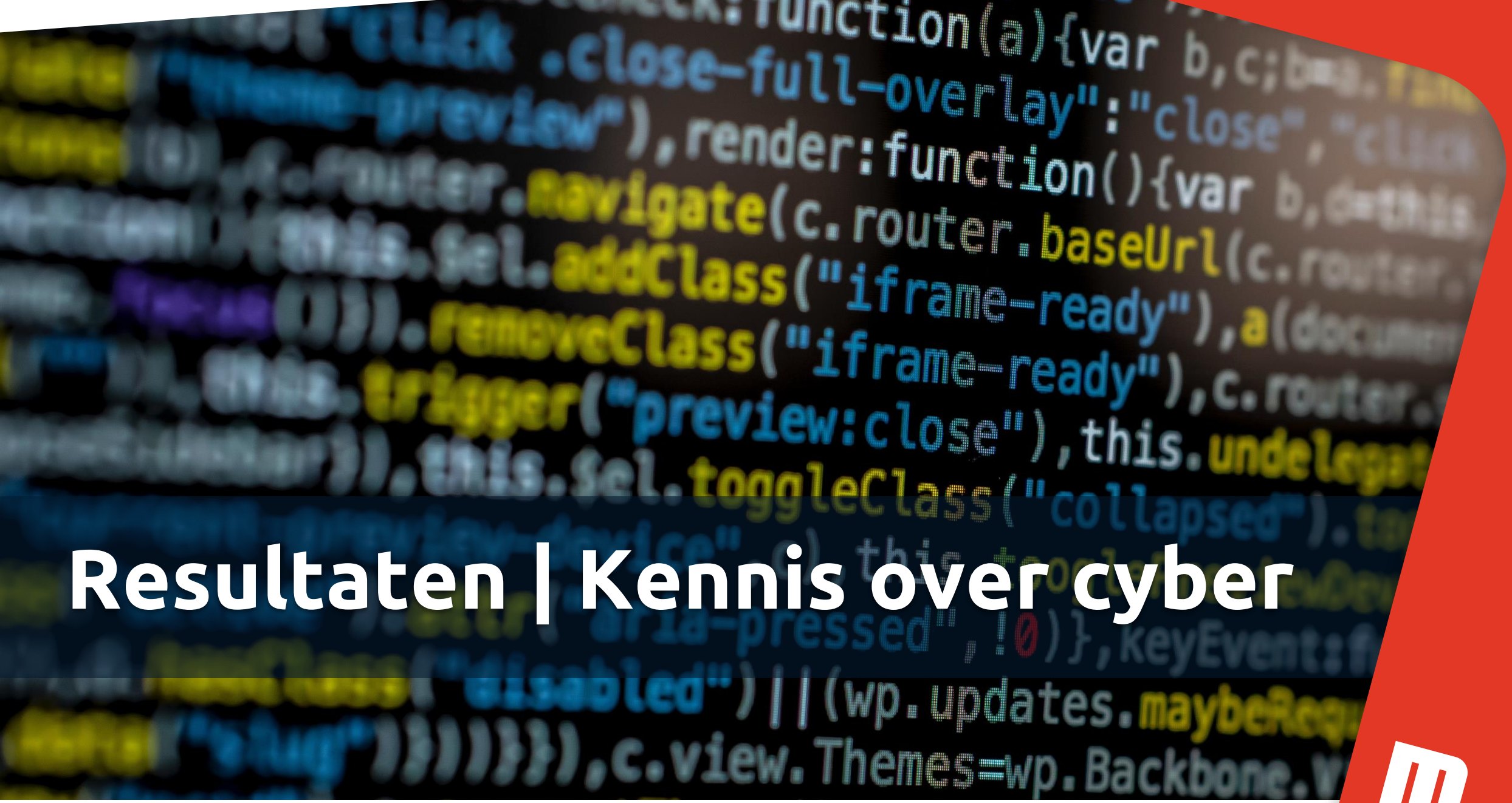
**Rood** = significante **onder**vertegenwoordiging

- Verschillen *tussen doelgroepen* worden aangeduid met rood of groen gemarkeerde percentages of met rode en groene kaders (in/om staafdiagrammen).
- Verschuivingen *ten opzichte van 2018* worden aangeduid met groene pijltjes omhoog (bij een toename) of rode pijltjes omlaag (bij een afname).
- Verschillen *binnen de Nederlandse bevolking* (naar geslacht, leeftijd en opleiding) benoemen we alleen tekstueel, waar significant en relevant.

Significanties van de verschillen tussen doelgroepen zijn gebaseerd op de gemiddeldes van antwoordschalen, terwijl in tabellen en grafieken veelal percentages getoond worden. Om die reden kan het bijvoorbeeld voorkomen dat een percentage van een groep dat lager is, toch groen gekleurd is (waarmee een significante oververtegenwoordiging wordt aangeduid). Dat resultaat is dan op gemiddeldeniveau wel significant hoger.*

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.

*Zie bijvoorbeeld het veilig gebruik van een wifi-verbinding onderweg door MKB'ers, op pagina 34.



# Resultaten | Kennis over cyber

# Nederlands publiek en medewerkers uit klein MKB schatten de eigen kennis over digitale veiligheid gemiddeld lager in

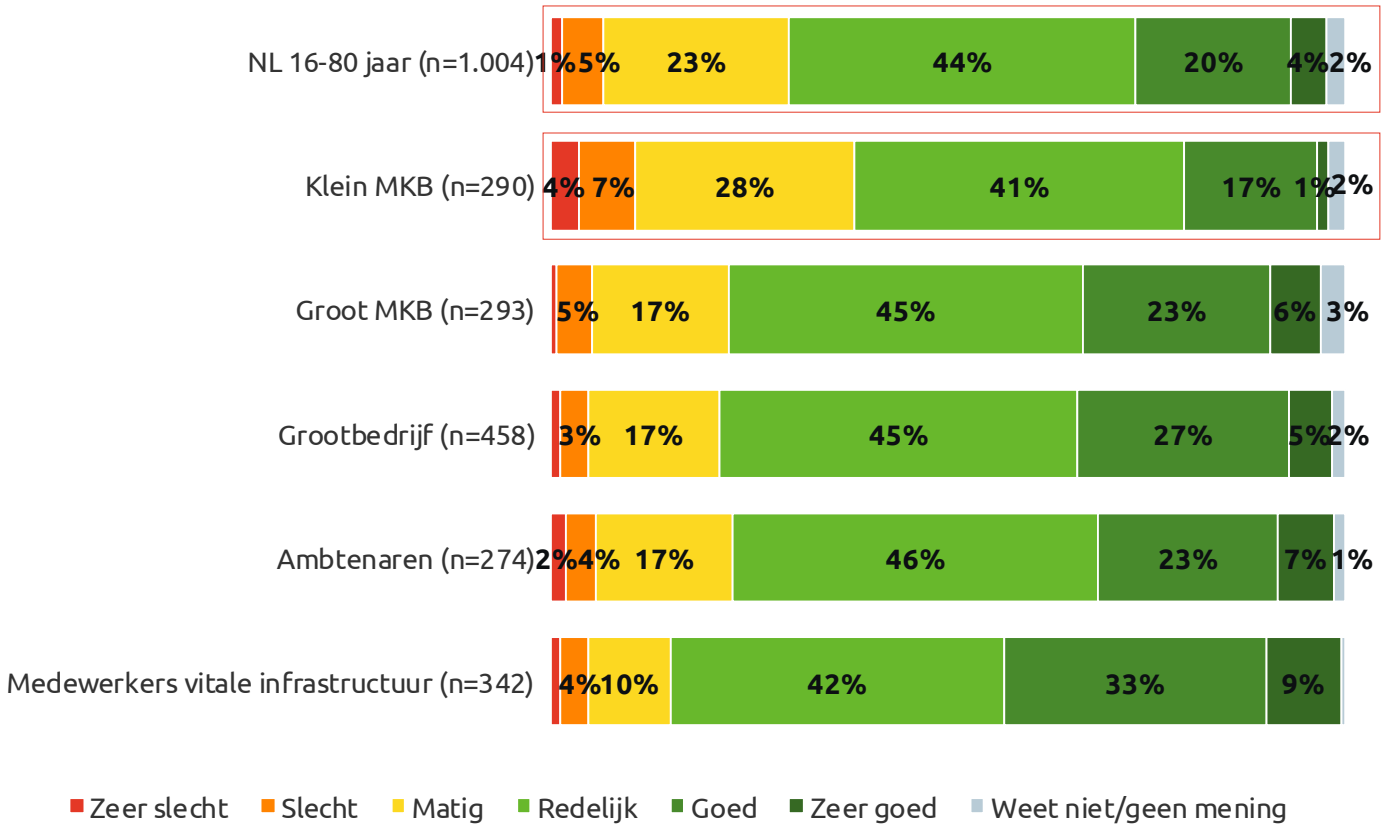
## Verschillen tussen doelgroepen

- Het Nederlands publiek en werknemers bij kleine MKB-bedrijven schatten hun eigen kennis over digitale en online veiligheid lager in dan de andere doelgroepen.

## Verschillen binnen Nederland

- Mannen schatten hun eigen kennis over digitale en online veiligheid hoger in dan vrouwen (32% (zeer) goed onder mannen vs. 16% onder vrouwen).
- Jongere Nederlanders (tot 34 jaar) schatten hun eigen kennis hoger in (34% goed tot zeer goed). Oudere Nederlanders (55 jaar en ouder) schatten hun kennis lager in (17% goed tot zeer goed).
- Hoogopgeleiden schatten hun eigen kennis hoger in (29% goed tot zeer goed), laagopgeleiden lager (15%).

**Allereerst willen we graag van je weten: hoe schat jij je eigen kennis over digitale en online veiligheid in?**




*Deze vraag is nieuw toegevoegd in 2019.*

# Nederlanders met meerdere digitale risico's beter bekend dan vorig jaar

## Vergelijking met 2018

- Nederlanders (16 – 80 jaar) zijn dit jaar beter bekend met phishing mails, cyberaanvallen, datalekken, spyware, keyloggers en portscans.
- Ook medewerkers van grootbedrijven, ambtenaren en werknemers binnen de vitale infrastructuur zijn beter bekend met keyloggers.
- Er is één daling t.o.v. 2018: ambtenaren zijn minder bekend met ransomware (47% vs. 58%).

## Verschillen tussen doelgroepen

- Over het algemeen zijn werknemers binnen de vitale infrastructuur beter bekend met verschillende digitale risico's. Ook ambtenaren zijn met relatief veel digitale gevaren beter bekend, zoals met phishing mails, identiteitsfraude, cyberaanvallen en datalekken.
- Het Nederlands publiek is met veel digitale risico's juist minder bekend.

*Dat de verschillen bij het Nederlands publiek significant zijn heeft met name te make met de grootte van die steekproef. Qua percentages ligt de bekendheid op min of meer hetzelfde niveau als onder MKB'ers.*

| **Kun je aangeven in welke mate je bekend bent met de onderstaande zaken?** % ik weet wat het is* | **NL 16-80 jaar** (n=1.004) | **Klein MKB** (n=290) | **Groot MKB** (n=293) | **Grootbedrijf** (n=458) | **Ambtenaren** (n=274) | **Vitale infra-structuur** (n=342) |
|---|---|---|---|---|---|---|
| Phishing mails | 79% ↑ | 80% | 79% | 83% | 89% | 83% |
| Identiteitsfraude | 75% | 78% | 77% | 82% | 84% | 83% ↑ |
| Cyberaanval | 71% ↑ | 71% | 73% | 78% | 80% | 81% |
| Datalek | 58% ↑ | 66% | 60% | 70% | 83% ↑ | 72% |
| Spyware | 58% ↑ | 61% | 59% | 66% | 67% | 71% |
| DDoS-aanval | 48% | 52% | 48% | 57% | 62% | 60% |
| Malware | 52% | 60% | 53% | 60% | 61% | 67% |
| Ransomware | 37% | 46% | 40% | 44% | 47% ↓ | 50% |
| Keylogger | 21% ↑ | 21% | 21% | 28% ↑ | 33% ↑ | 38% ↑ |
| Botnet | 16% | 20% | 16% | 18% | 22% | 25% |
| Social engineering | 13% | 20% | 19% | 21% | 22% | 34% |
| Spoofing | 12% | 16% | 15% | 16% | 12% | 24% ↑ |
| Portscan | 10% ↑ | 14% | 13% | 16% | 14% | 22% |
| Juice jacking | 5% | 5% | 9% | 6% | 10% | 14% |

* In de bijlage is een tabel opgenomen met de % nooit van gehoord per doelgroep

# Medewerkers uit klein MKB schatten schade bij veel digitale risico's kleiner in

## Vergelijking met 2018

- Bij twee doelgroepen zijn verschillen met vorig jaar zichtbaar: het Nederlands publiek en medewerkers uit vitale sectoren.
- Nederlanders achten de kans op schade tijdens werksituaties dit jaar groter bij phishing, spyware en juice jacking.
- Medewerkers uit de vitale infrastructuur achten de kans op schade in werksituaties juist kleiner dit jaar voor phishing, DDoS-aanvallen en ransomware.

## Verschillen tussen doelgroepen

- Over het algemeen achten MKB'ers de schade van veel gevaren kleiner, met name privé. Medewerkers die werkzaam zijn in de vitale infrastructuur schatten de schade van veel risico's juist groter in, zowel privé als op hun werk.

| **Hoe groot acht je de kans op (computer)-schade** % (Zeer) groot | **NL 16-80 jaar** | | **Klein MKB** | | **Groot MKB** | | **Grootbedrijf** | | **Ambtenaren** | | **Vitale infrastructuur** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Werk | Privé | Werk | Privé | Werk | Privé | Werk | Privé | Werk | Privé | Werk | Privé |
| Phishing mails | 16% ↑ | 13% | 10% | 9% | 17% | 13% | 14% | 18% | 15% | 16% | 19% ↓ | 19% ↓ |
| Identiteitsfraude | 9% | 8% | 3% | 3% | 8% | 9% | 8% | 11% | 10% | 9% | 14% | 14% ↓ |
| Cyberaanval | 10% | 6% | 4% | 4% | 10% | 8% | 10% | 8% | 12% | 7% | 16% | 13% |
| Datalek | 14% | 7% | 3% | 3% | 13% | 7% | 12% | 8% | 17% | 7% | 17% | 13% |
| Spyware | 9% ↑ | 9% | 4% | 5% | 10% | 13% | 9% | 10% | 10% | 9% | 14% | 15% ↓ |
| DDoS-aanval | 12% | 5% | 5% | 4% | 13% | 6% | 8% | 6% | 13% | 7% | 13% ↓ | 11% |
| Malware | 10% | 7% | 4% | 6% | 9% | 10% | 7% | 11% | 10% | 12% | 12% | 18% |
| Ransomware | 9% | 9% | 6% | 4% | 9% | 11% | 5% | 11% | 6% | 8% | 10% ↓ | 16% |
| Keylogger | 10% | 5% | 4% | 1% | 9% | 8% | 4% | 7% | 10% | 10% | 11% | 12% |
| Botnet | 11% | 8% | 4% | 3% | 12% | 15% | 9% | 9% | 3% | 7% | 9% | 15% |
| Social engineering | 14% | 6% | 5% | 3% | 13% | 9% | 8% | 7% | 13% | 7% | 15% | 9% |
| Spoofing | 12% | 6% | 5% | 5% | 12% | 12% | 9% | 9% | 8% | 3% | 16% | 14% |
| Portscan | 12% | 10% | 10% | 7% | 9% | 16% | 5% | 10% | 15% | 11% | 12% | 16% |
| Juice jacking | 18% ↑ | 13% | 9% | 10% | 16% | 17% | 13% ↑ | 14% | 11% | 7% | 17% | 15% |

# Meerderheid Nederlanders bekend met verschillende digitale beveiligingsopties

## Vergelijking met 2018

- Vergeleken met vorig jaar zijn Nederlanders beter bekend geraakt met minder bekende beveiligingsmaatregelen, zoals een digitale wachtwoordenmanager, VPN-verbindingen, open source hard- en software en web tracking blockers.
- Ook medewerkers van grootbedrijven en van vitale sectoren zijn met verschillende opties beter bekend geraakt, zoals de spyware scanner en de digitale wachtwoordenmanager.

## Verschillen tussen doelgroepen

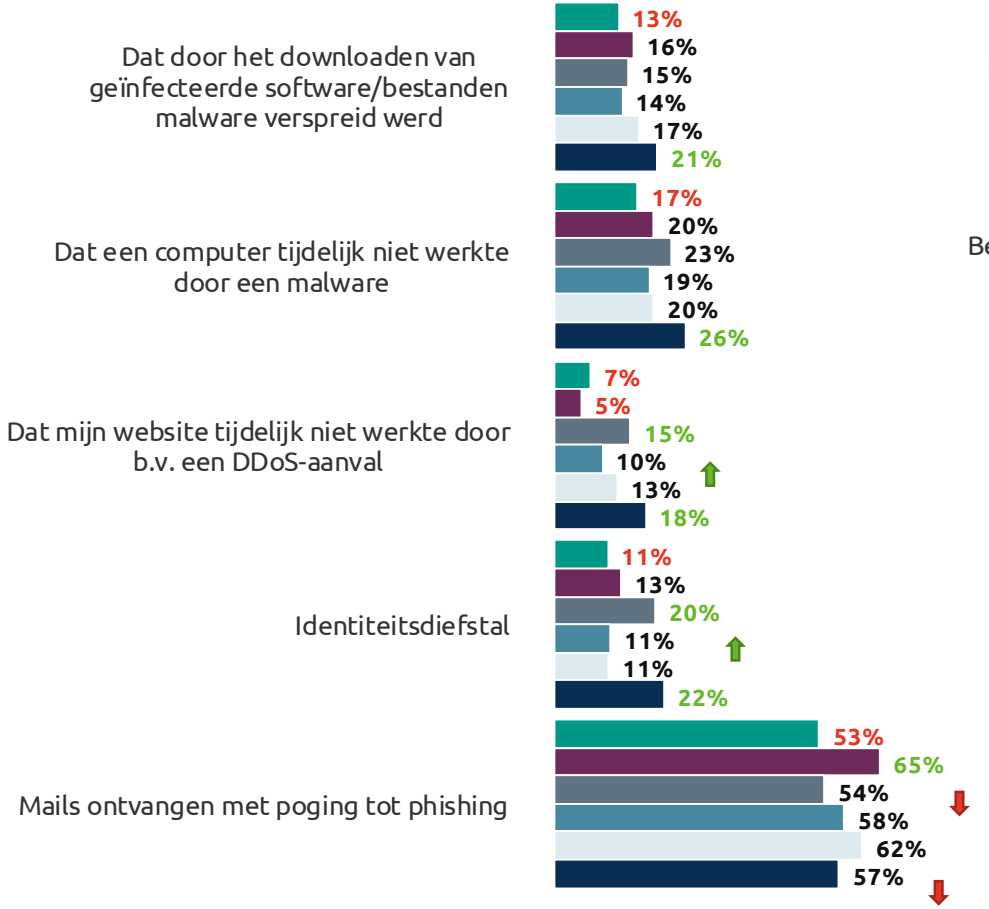
- Ondanks de stijging in bekendheid van een aantal maatregelen blijft het Nederlands publiek relatief het minst bekend met de verschillende beveiligingsopties. Met name medewerkers uit vitale sectoren, ambtenaren en medewerkers van grootbedrijven zijn met een aantal opties beter bekend, zoals cloud diensten en tweestapsverificatie.

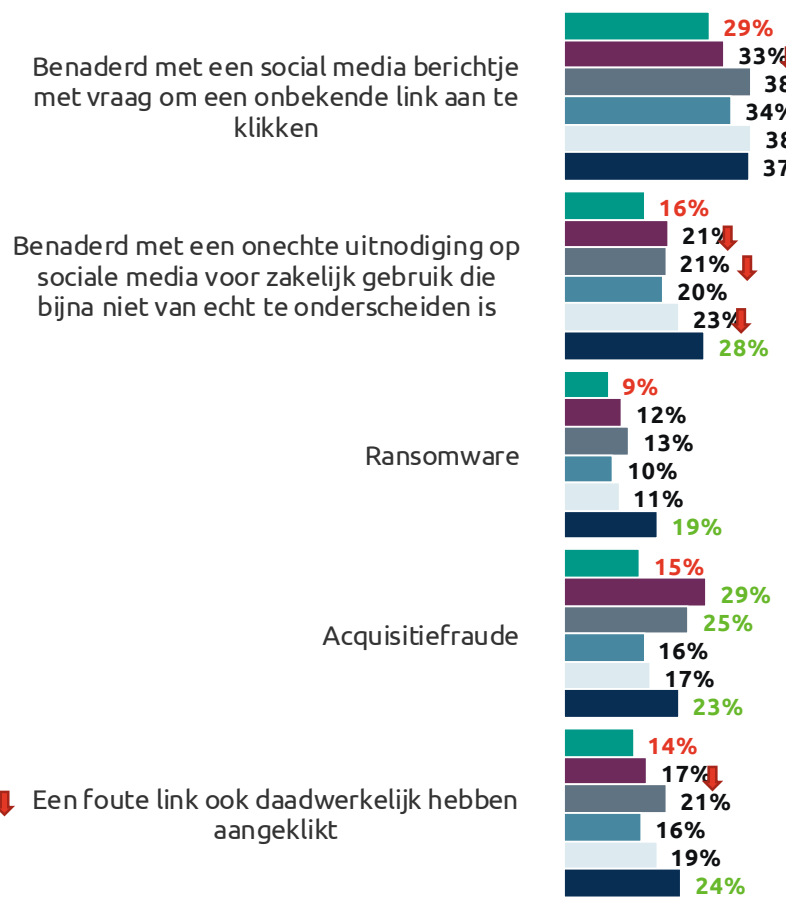
| **Kun je aangeven in welke mate je bekend bent met de onderstaande zaken?** % Weleens van gehoord /weet wat het is/gebruik ik | **NL 16-80 jaar** (n=1.004) | **Klein MKB** (n=290) | **Groot MKB** (n=293) | **Grootbedrijf** (n=458) | **Ambtenaren** (n=274) | **Vitale infrastructuur** (n=342) |
|---|---|---|---|---|---|---|
| Virusscanner | 96% | 94% | 97% | 98% | 98% | 98% |
| Automatische updates | 95% | 93% | 96% | 96% | 99% | 97% ↑ |
| Instellingen om cookies te blokkeren/uit te zetten | 92% | 91% | 94% | 97% ↑ | 96% | 96% |
| Cloud diensten | 88% | 91% | 92% | 94% | 96% | 95% |
| Biometrische online bescherming | 80% | 85% | 85% | 85% | 89% | 87% |
| Tweestapsverificatie | 80% | 85% | 87% | 89% | 90% | 92% ↑ |
| Spyware scanner | 76% | 82% | 83% | 85% ↑ | 84% | 90% ↑ |
| Digitaal wachtwoordenkluisje/ wachtwoordmanager | 82% ↑ | 84% | 87% ↑ | 88% ↑ | 90% | 94% ↑ |
| Ad-blocker | 73% | 74% | 82% | 81% | 79% | 85% |
| VPN-verbindingen | 72% ↑ | 75% | 80% | 86% ↑ | 81% | 90% |
| Open source hardware- en software | 63% ↑ | 71% ↑ | 71% | 71% | 72% | 83% |
| Web tracking blocker | 58% ↑ | 61% | 67% | 67% | 65% | 79% |


# Resultaten | Ervaringen met digitale risico's

# Minder vaak sprake van cybercriminaliteit via sociale media dan in 2018

**Heb je in een privésituatie ooit weleens te maken gehad met één van de onderstaande voorvallen?** *% Ja, ikzelf (en iemand anders)*




*Groen gemarkeerd percentage: voorval is significant vaker voorgekomen in deze groep ten opzichte van de andere groepen*

*Rood gemarkeerd percentage: voorval is significant minder vaak voorgekomen in deze groep ten opzichte van de andere groepen*

*Ten opzichte van 2018 geven significant meer personen aan het voorval te hebben meegemaakt*

*Ten opzichte van 2018 geven significant minder personen aan het voorval te hebben meegemaakt*

- NL 16 – 80 jaar (n=1.004)
- Klein MKB (n=290)
- Groot MKB (n=293)
- Grootbedrijf (n=458)
- Ambtenaren (n=274)
- Vitale infrastructuur (n=342)

*In totaal heeft 71% van de Nederlanders weleens een cybervoorval meegemaakt*

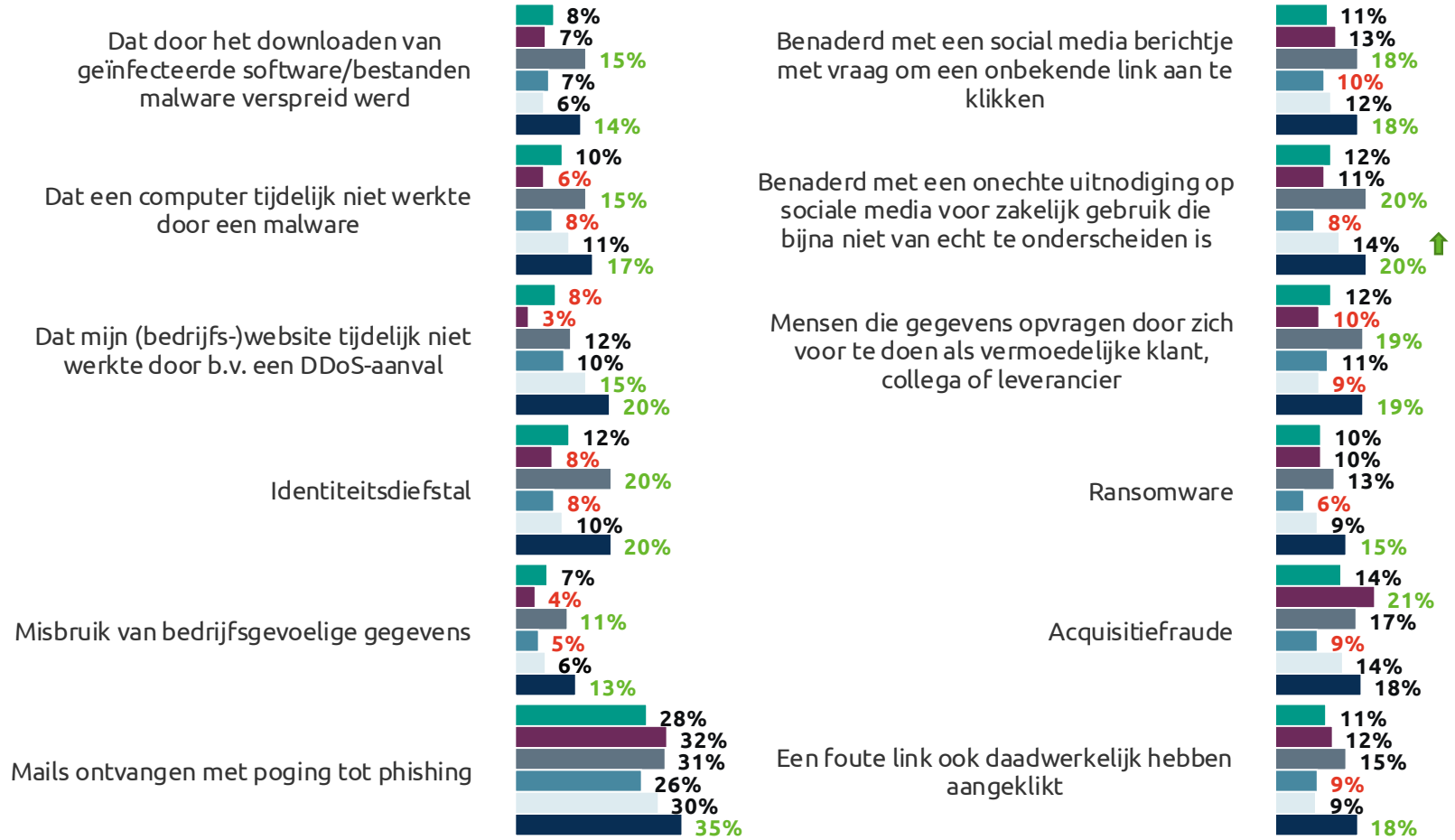
# Vier op de tien Nederlanders scherpen beveiliging niet aan na cyberincidenten

| **Heb je maatregelen getroffen nadat je dit [voorval van cybercriminaliteit in de privésituatie] hebt meegemaakt?** *Basis: Heeft één of meer voorvallen meegemaakt* *Top 10 maatregelen + geen maatregel* | **NL 16-80 jaar** (n=715) | **Klein MKB** (n=237) | **Groot MKB** (n=227) | **Groot-bedrijf** (n=345) | **Ambtenaren** (n=220) | **Vitale infra-structuur** (n=271) | **Hoe vaak doe je deze maatregel?** *Basis: onderneemt maatregel* *% Vaak + bijna altijd* | |
|---|---|---|---|---|---|---|---|---|
| Ik heb antivirussoftware geïnstalleerd | 35% ↓ | 36% | 26% ↓ | 30% ↓ | 30% ↓ | 27% ↓ | 66% ↑ | n = 441 |
| Ik heb het gerapporteerd/ aangifte gedaan | 26% | 25% | 22% | 25% | 27% | 22% | 35% | n = 340 |
| Ik heb een firewall geïnstalleerd of geüpdatet | 26% | 30% | 21% ↓ | 22% | 21% ↓ | 27% | 46% | n = 332 |
| Ik maak mijn wachtwoorden complexer | 24% ↓ | 26% | 24% | 28% | 24% | 31% | 55% ↑ | n = 353 |
| Ik controleer of websites HTTPS gebruiken | 24% ↓ | 24% | 21% | 21% ↓ | 22% ↓ | 26% | 72% | n = 317 |
| Ik heb een software update uitgevoerd | 22% ↓ | 25% | 19% ↓ | 24% | 21% ↓ | 27% | 62% | n = 309 |
| Ik maak nu back-ups van de bestanden op mijn laptop | 14% ↓ | 16% | 12% | 11% ↓ | 12% ↓ | 15% ↓ | 45% | n = 178 |
| Ik heb toestemmingen van apps op mijn telefoon beperkt | 13% | 14% | 15% | 14% | 17% | 19% | 57% | n = 185 |
| Ik maak nu back-ups van mijn smartphone | 10% | 10% | 10% | 10% | 7% ↓ | 16% | 60% | n = 131 |
| Ik verstuur geen werkgerelateerde bestanden van mijn werk meer naar huis* | 7% | 10% | 12% | 9% | 10% | 13% | 46% | n = 114 |
| Geen van bovenstaande, ik heb niets gedaan (+ inverse: % wel iets gedaan) | 44% ↓ (56%) | 40% ↓ (60%) | 42% (58%) | 47% (53%) | 41% ↓ (59%) | 32% (68%) | | |

* Deze maatregel stond vorig jaar niet in de top 10.

# Medewerkers uit groot MKB hebben maken relatief vaak een digitaal voorval mee

**Heb je in een werksituatie ooit weleens te maken gehad met één van de onderstaande voorvallen?** *% Ja, ikzelf (en iemand anders)*




*Groen gemarkeerd percentage: voorval is significant vaker voorgekomen in deze groep ten opzichte van de andere groepen*

*Rood gemarkeerd percentage: voorval is significant minder vaak voorgekomen in deze groep ten opzichte van de andere groepen*

*Ten opzichte van 2018 geven significant meer personen aan het voorval te hebben meegemaakt*

*Ten opzichte van 2018 geven significant minder personen aan het voorval te hebben meegemaakt*

- Werkend Nederland (n=501)
- Klein MKB (n=290)
- Groot MKB (n=293)
- Grootbedrijf (n=458)
- Ambtenaren (n=274)
- Vitale infrastructuur (n=342)

*In totaal heeft 48% van de werkende Nederlanders weleens een cybervoorval meegemaakt in een werksituatie*

# Ongeveer één op de vijf Nederlanders meldt cyberincidenten op het werk

| **Heb je maatregelen getroffen nadat je dit [voorval van cybercriminaliteit in de werksituatie) hebt meegemaakt?** *Basis: Heeft één of meer voorvallen meegemaakt* *Top 10 maatregelen + geen maatregel* | **NL 16-80 jaar** (n=241) | **Klein MKB** (n=151) | **Groot MKB** (n=171) | **Groot-bedrijf** (n=221) | **Ambtenaren** (n=135) | **Vitale infra-structuur** (n=229) |
|---|---|---|---|---|---|---|
| Ik heb het gerapporteerd/aangifte gedaan | 20% | 26% | 13% | 18% | 26% | 19% |
| Ik heb het gemeld bij onze systeembeheerder(s)/IT-afdeling* | 19% | 16% | 20% | 22% | 34% | 21% |
| Ik maak mijn wachtwoorden complexer | 15% ↑ | 16% | 18% | 15% | 15% | 17% |
| Ik heb een software update uitgevoerd | 15% | 12% ↓ | 12% | 15% | 13% | 16% ↓ |
| Ik heb een firewall geïnstalleerd of geüpdatet | 15% | 16% ↓ | 15% ↓ | 15% ↓ | 12% ↓ | 20% ↓ |
| Ik ben een wachtwoordmanager gaan gebruiken | 11% | 9% | 9% | 9% | 9% | 13% |
| Ik controleer of websites HTTPS gebruiken | 11% | 11% | 18% ↑ | 16% | 11% | 21% |
| Ik heb antivirussoftware geïnstalleerd | 11% | 13% ↓ | 13% | 15% | 9% | 16% ↓ |
| Ik heb toestemmingen van apps op mijn telefoon beperkt** | 10% | 8% | 12% | 8% | 9% | 11% |
| Ik maak nu back-ups van de bestanden op mijn laptop | 10% | 11% | 11% | 8% | 10% | 14% ↓ |
| Geen van bovenstaande, ik heb niets gedaan (+ inverse: % wel iets gedaan) | 41% ↓ (59%) | 43% ↓ (57%) | 39% (61%) | 44% (56%) | 36% ↓ (64%) | 33% (67%) |

| **Hoe vaak doe je deze maatregel?** *Basis: onderneemt maatregel* *% Vaak + bijna altijd* | |
|---|---|
| 40% | n = 137 |
| 46% | n = 152 |
| 53% | n = 108 |
| 62% | n = 89 |
| 56% | n = 99 |
| 59%* | n = 62 |
| 69% | n = 98 |
| 60% | n = 88 |
| 50%* | n = 63 |
| 55%* | n = 67 |

* Deze categorie is toegevoegd in 2019. Ongeveer 30% van de mensen die het intern gemeld heeft, heeft ook aangifte gedaan/het gerapporteerd.
** Deze maatregel stond vorig jaar niet in de top 10

*Resultaat indicatief vanwege laag aantal waarnemingen

# Klikken op phishing mail leidt meestal tot toegang tot systemen voor internetcriminelen

**Je geeft aan dat je op je werk weleens een foute link hebt aangeklikt. Wat waren de gevolgen daarvan?** *Top 3 meest voorkomende gevolgen*
(Basis: heeft op werk weleens een foute link aangeklikt)

| **Werkend Nederland** (n=55) | **Klein MKB** (n=35) | **Groot MKB** (n=45) | **Grootbedrijf** (n=41) | **Ambtenaren** (n=24) | **Vitale infrastructuur** (n=60) |
|---|---|---|---|---|---|
| **Internetcriminelen** hebben **toegang** gekregen tot ons bedrijfssysteem en gegevens | **Internetcriminelen** hebben **toegang** gekregen tot ons bedrijfssysteem en gegevens | **Internetcriminelen** hebben **toegang** gekregen tot ons bedrijfssysteem en gegevens | **Internetcriminelen** hebben **toegang** gekregen tot ons bedrijfssysteem en gegevens | Ik kreeg te maken met **extra online beveiligingssoftware-maatregelen** | **Internetcriminelen** hebben **toegang** gekregen tot ons bedrijfssysteem en gegevens |
| Ik ben mijn **bestanden kwijtgeraakt**/mijn bestanden zijn onbruikbaar geworden | Ik moest **geld betalen** om weer toegang te krijgen tot mijn bestanden | Ik ben mijn **bestanden kwijtgeraakt**/mijn bestanden zijn onbruikbaar geworden | Mijn bestanden zijn (online) gedeeld/**in verkeerde handen** geraakt | **Internetcriminelen** hebben **toegang** gekregen tot ons bedrijfssysteem en gegevens | Mijn persoonlijke gegevens zijn gebruikt om **identiteitsfraude** te plegen |
| Mijn bestanden zijn (online) gedeeld/**in verkeerde handen** geraakt | Ik ben mijn **bestanden kwijtgeraakt**/mijn bestanden zijn onbruikbaar geworden | Mijn persoonlijke gegevens zijn gebruikt om **identiteitsfraude** te plegen | Mijn persoonlijke gegevens zijn gebruikt om **identiteitsfraude** te plegen | Mijn bestanden zijn (online) gedeeld/**in verkeerde handen** geraakt | Mijn bestanden zijn (online) gedeeld/**in verkeerde handen** geraakt |
| Eén op de vijf ondervond **geen gevolgen** | Een kwart ondervond **geen gevolgen** | Eén op de tien ondervond **geen gevolgen** | Vier op de tien ondervonden **geen gevolgen** | Eén op de drie ondervond **geen gevolgen** | Eén op de vijf ondervond **geen gevolgen** |

*Deze vraag is nieuw toegevoegd in 2019.*

*Gezien de lage aantallen per doelgroep, zijn voor deze vraag geen percentages getoond. De resultaten zijn indicatief.*

# Nederlanders kijken meestal naar het mailadres om een phishing mail te ontmaskeren

## Verschillen binnen Nederland

- Mannen kijken vaker naar de links die in de mail zijn opgenomen om een phishing mail te herkennen dan vrouwen (34% vs. 19%).
- Jongeren (16 – 24 jaar) kijken vaker naar de links die in de mail zijn opgenomen (36%) en letten er vaker niet op of iets een phishing mail is (4%).
- 25 - 34-jarigen kijken vaker naar het mailadres (64%), de logo's (12%) en het lettertype (6%).
- 35 – 44-jarigen kijken vaker naar het lettertype in de mail (6%). 45 - 54-jarigen kijken vaker naar het mailadres van de afzender (62%) en de schrijfstijl (37%).
- Oudere Nederlanders (65 - 80 jaar) kijken vaker of de website waarnaar verwezen wordt beveiligd is (36%) en of zij persoonlijk worden aangesproken in de mail (21%).
- Hoogopgeleiden kijken vaker naar het mailadres (66%), taalgebruik (41%) en de links die in de mail zijn opgenomen (32%). Middelbaar opgeleiden kijken vaker naar de opmaak van het bericht (24%).
- Laagopgeleiden geven vaker aan phishingsmails niet te herkennen, omdat ze er te echt uit zien (5%).

**Naar welke onderdelen van een mail kijk jij vooral om een phishingmail te herkennen?**
(Basis - NL 16 - 80 jaar, bekend met phishing mails, n=944)


*Deze vraag is nieuw toegevoegd in 2019.*

# Resultaten | Zorgen om digitale veiligheid

# Medewerkers uit het MKB maken zich relatief weinig zorgen om hun digitale veiligheid thuis

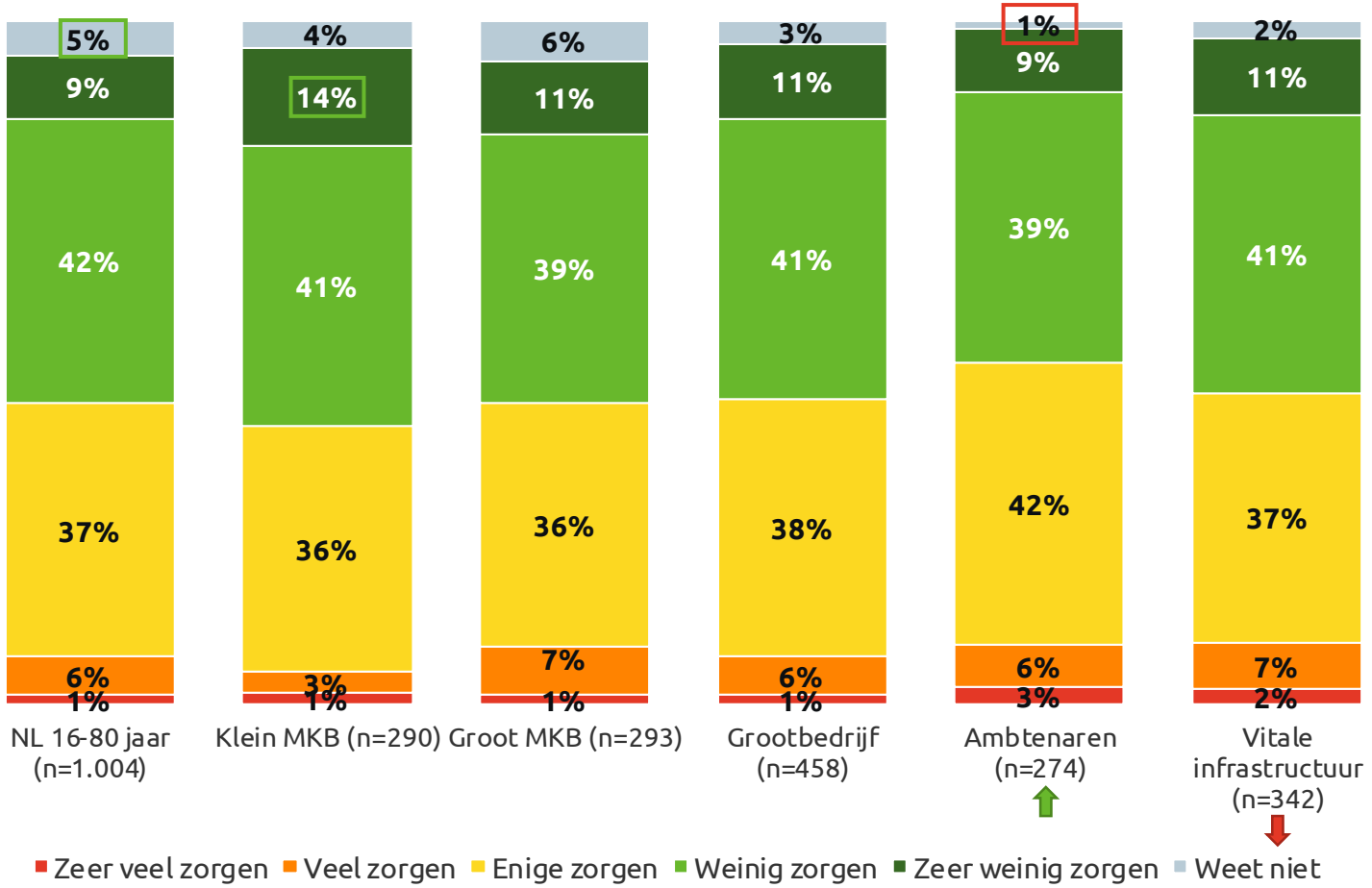
### Vergelijking met 2018

- Ambtenaren maken zich dit jaar meer zorgen over hun online en digitale veiligheid in privésituaties.
- Medewerkers uit de vitale sector maken zich dit jaar minder zorgen over hun online veiligheid in privésituaties.

### Verschillen tussen doelgroepen

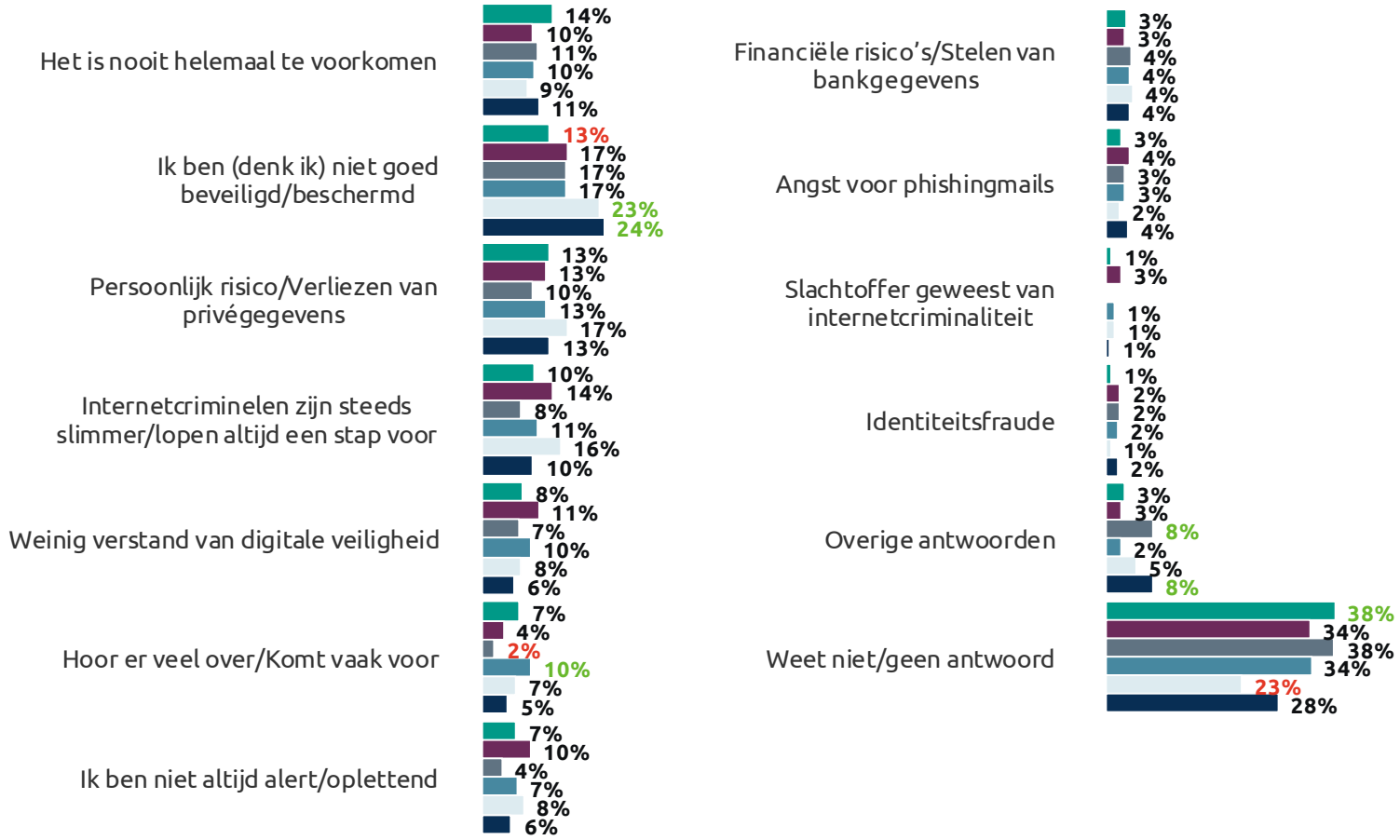
- Medewerkers uit het klein MKB maken zich minder zorgen om hun online/digitale veiligheid in privésituaties dan de andere doelgroepen.

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



# Ambtenaren en werknemers in vitale sectoren vrezen vaker niet goed beveiligd te zijn

**Waarom maak je je zorgen als het gaat om jouw online/digitale veiligheid in je privésituatie?** Basis: maakt zich tenminste enige zorgen




*Groen gemarkeerd percentage: reden is significant vaker genoemd door deze groep ten opzichte van de andere groepen*

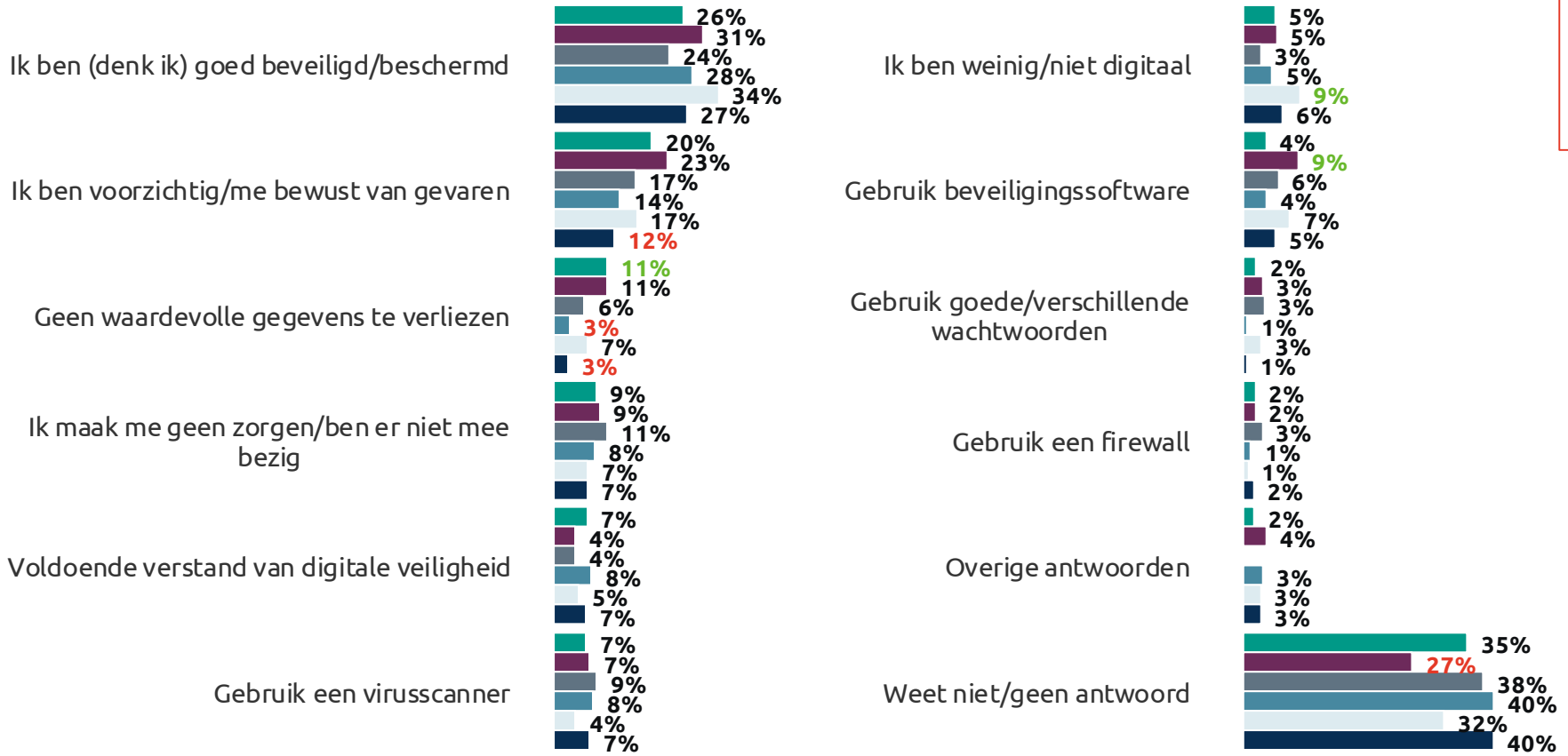
*Rood gemarkeerd percentage: reden is significant minder vaak genoemd door deze groep ten opzichte van de andere groepen*

- NL 16 – 80 jaar (n=511)
- Klein MKB (n=160)
- Groot MKB (n=147)
- Grootbedrijf (n=238)
- Ambtenaren (n=134)
- Vitale infrastructuur (n=178)

*Deze vraag is nieuw toegevoegd in 2019.*

# Nederlanders denken relatief vaak privé geen waardevolle gegevens te verliezen te hebben

**Waarom maak je je (zeer) weinig zorgen als het gaat om jouw online/digitale veiligheid in je privésituatie?**
Basis: maakt zich (zeer) weinig zorgen




*Groen gemarkeerd percentage: reden is significant vaker genoemd door deze groep ten opzichte van de andere groepen*

*Rood gemarkeerd percentage: reden is significant minder vaak genoemd door deze groep ten opzichte van de andere groepen*

*Deze vraag is nieuw toegevoegd in 2019.*

# Medewerkers in groot MKB maken zich het vaakst zorgen over digitale veiligheid op het werk

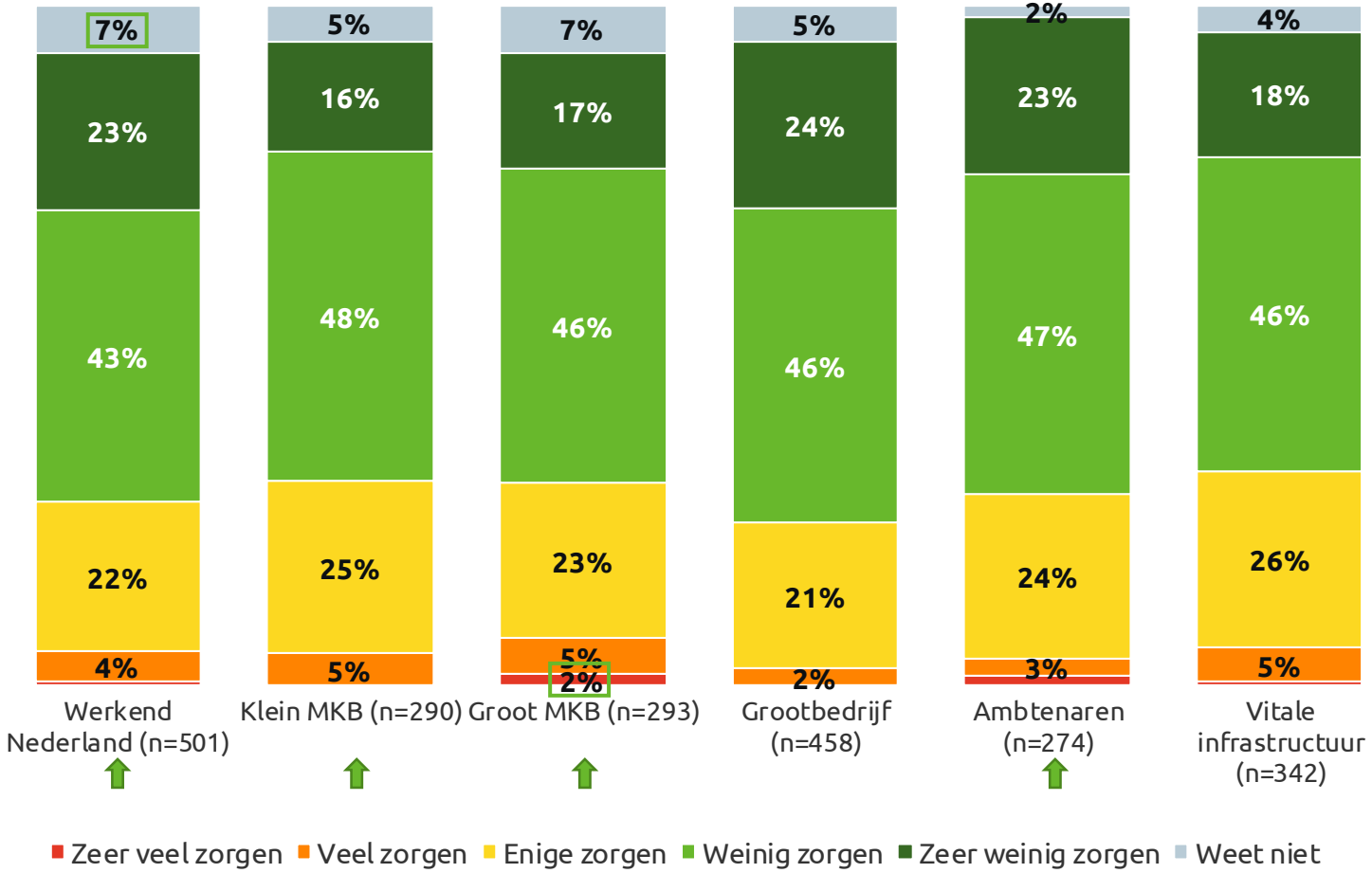
## Vergelijking met 2018

- Werkende Nederlanders maken zich meer zorgen over hun online/digitale veiligheid op het werk dan vorig jaar.
- Binnen werkende Nederlanders maken werknemers uit het klein MKB en groot MKB en ambtenaren zich meer zorgen dan vorig jaar over hun online veiligheid in werksituaties.

## Verschillen tussen doelgroepen

- Medewerkers uit het groot MKB en die werkzaam zijn in vitale sectoren maken zich meer zorgen om de digitale veiligheid op werk dan de andere doelgroepen.
- Medewerkers uit grootbedrijven maken zich juist minder zorgen.

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



# Zorgen om diefstal van online identiteit gestegen

## Vergelijking met 2018

- Ten opzichte van vorig jaar zijn bij alle doelgroepen de zorgen over dat iemand de online identiteit steelt, toegenomen.

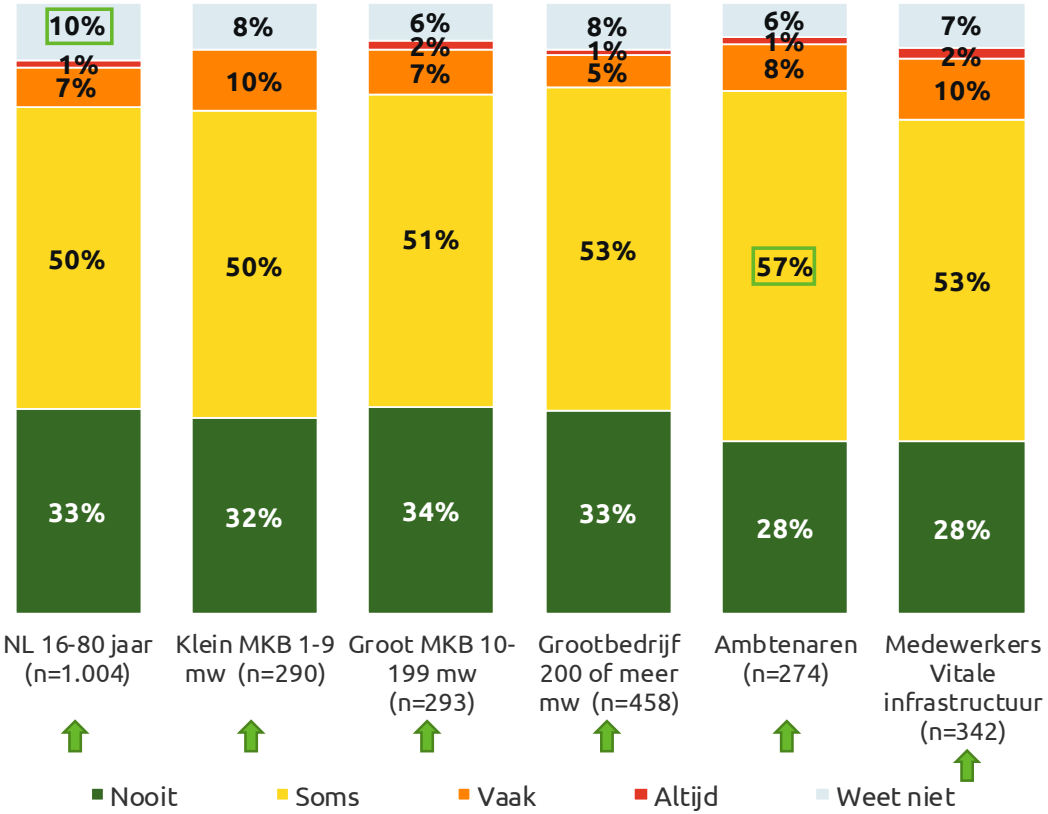
## Verschillen tussen doelgroepen

- Tussen de verschillende doelgroepen zitten op totaalniveau geen verschillen qua zorgen om online diefstal. Wel maken ambtenaren zich iets vaker soms zorgen over de diefstal van hun online identiteit.

## Verschillen binnen Nederland

- Jongeren (16 tot 24 jaar) maken zich er minder vaak zorgen over dat hun online identiteit gestolen wordt (42% nooit).
- Hoogopgeleiden maken zich vaker soms zorgen dat iemand hun online identiteit steelt (56% soms).

**Maak je je er weleens zorgen over dat iemand jouw online identiteit steelt?**



# Circa helft Nederlanders maakt zich weleens zorgen om een cyberaanval

## Vergelijking met 2018

- De zorgen over dat men zelf te maken krijgt met een cyberaanval zijn gedaald bij drie doelgroepen: medewerkers uit groot MKB en grootbedrijf, en medewerkers die werkzaam zijn in de vitale infrastructuur.

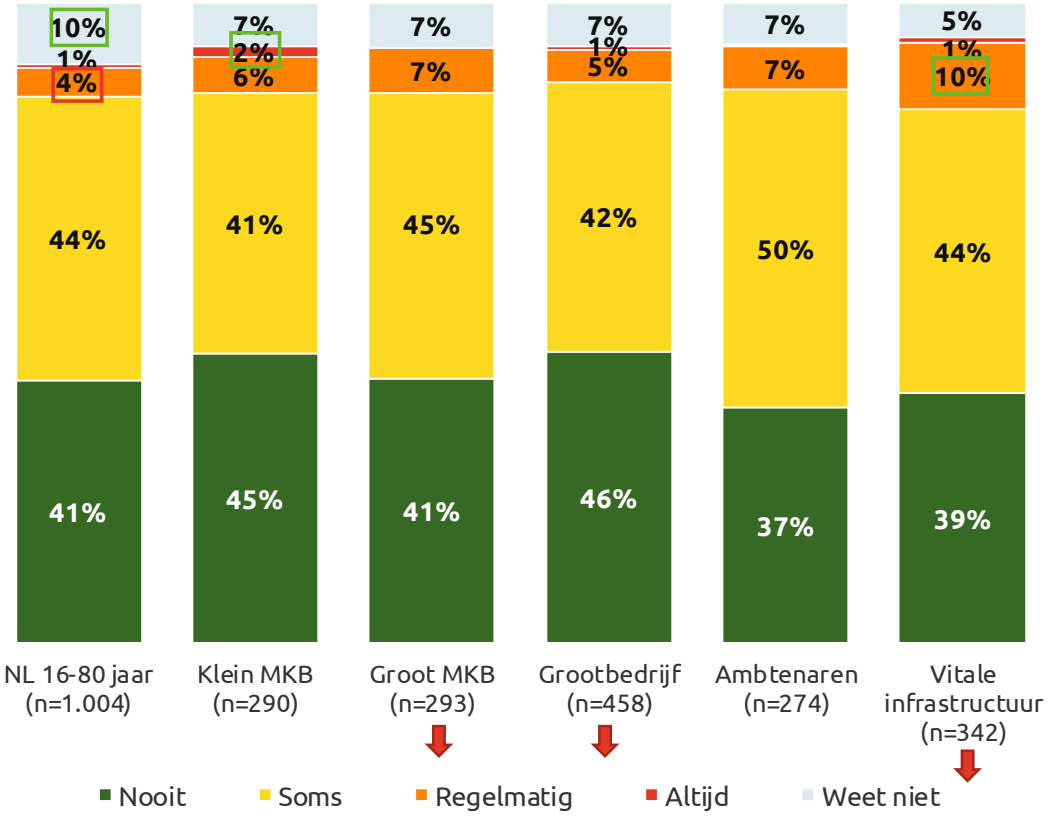
## Verschillen tussen doelgroepen

- Over cyberaanvallen maken medewerkers uit vitale sectoren zich vaker regelmatig zorgen. Werknemers van kleine MKB-bedrijven maken zich iets vaker altijd zorgen, en Nederlanders maken zich juist minder vaak regelmatig zorgen over een cyberaanval (vergeleken met de overige doelgroepen).

## Verschillen binnen Nederland

- Laagopgeleiden vinden het risico op een cyberaanval lastiger in te schatten dan hoger opgeleiden (20% weet niet). Hoogopgeleiden maken zich vaker zorgen over een cyberaanval (8% regelmatig/altijd)

**Ben je er weleens bezorgd over dat je zelf te maken krijgt met een cyberaanval?**



# Risico slachtoffer te worden van cybercriminaliteit

## Vergelijking met 2018

- Vergeleken met vorig jaar zien veel doelgroepen (alle behalve klein MKB) werken op een openbare computer als een groter risico om slachtoffer te worden van cybercriminaliteit.
- Medewerkers uit het grootbedrijf en uit de vitale infrastructuur zien het tot stand brengen van een wifi-verbinding minder vaak als een cyberrisico.

## Verschillen tussen doelgroepen

- Privé-gebruikers denken vaker slachtoffer te worden van cybercriminaliteit als ze bestanden downloaden van internet, vergeleken met de andere (werkende en professionele) doelgroepen.
- Ambtenaren verwachten juist vaker slachtoffer te worden door het openen van een link in een e-mail, door op een openbare computer actief te zijn of door een wifi-verbinding tot stand te brengen.
- MKB'ers uit grote MKB-bedrijven verwachten juist minder vaak slachtoffer te worden als zij een link vanuit een e-mail openen of als ze bestanden van het internet downloaden.

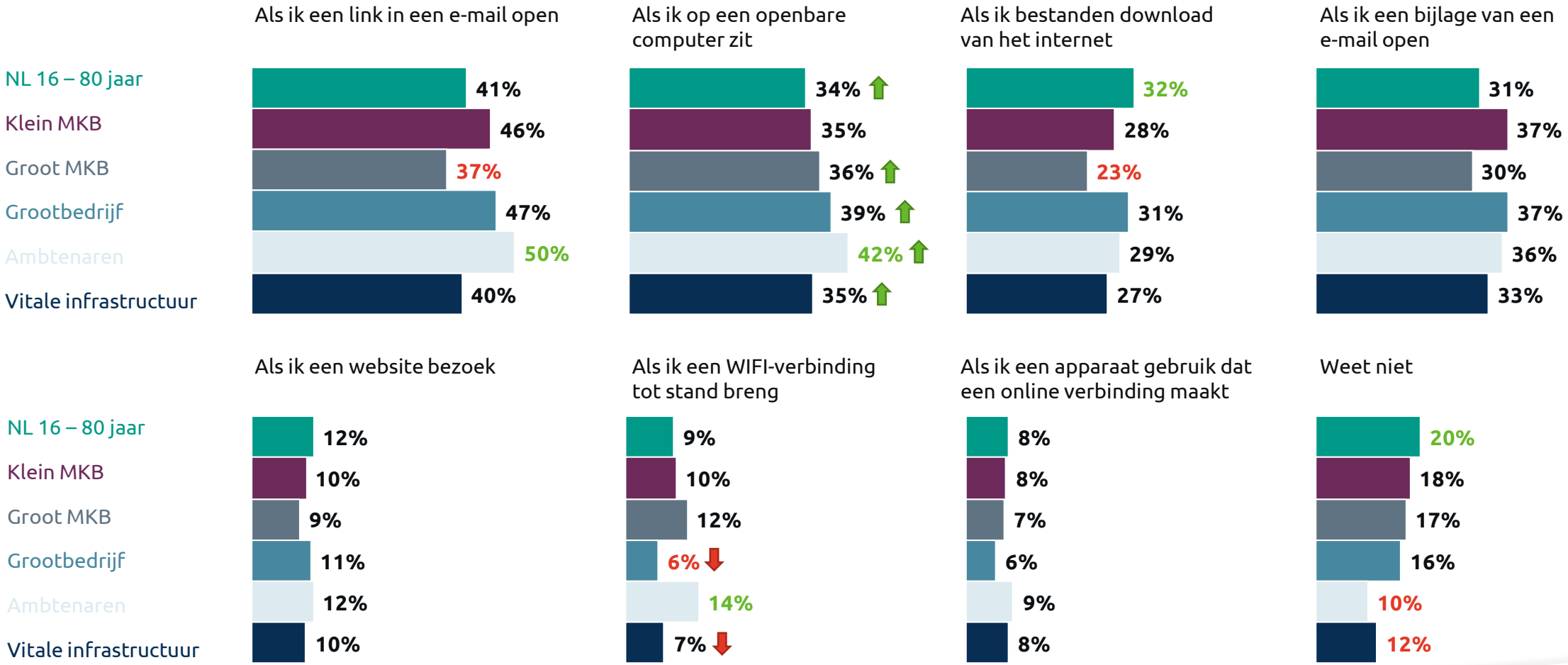
## Verschillen binnen Nederland

- Mannen verwachten vaker slachtoffer te worden door de bijlage van een e-mail te openen (34% vs. 28% onder vrouwen) of door een website te bezoeken (15% vs. 9%). Vrouwen schatten het risico groter in bij onder andere openbare computers (38% vs. 30% onder mannen) en het doen van online betalingen (op pc) (10% vs. 5%).
- Jongeren (16 – 24 jaar) denken vaker slachtoffer te worden als ze bestanden downloaden (40%) of als ze iets op social media zetten (12%). 25 – 34-jarigen denken vaker risico te lopen als ze op een openbare computer zitten (42%). 45 – 54-jarigen als ze een mailbijlage openen (37%), en 55 – 64-jarigen als ze een website bezoeken.
- Hoogopgeleiden verwachten vaker risico te lopen als ze een e-maillink openen (49%), bestanden downloaden (38%) of op een openbare computer zitten (39%). Laagopgeleiden als ze betalingen doen via hun laptop/desktop (12%).

➢ *De grafiek staat op de volgende pagina.*

# (Werkende) Nederlanders zien een openbare computer vaker als een groot risico bij cybercriminaliteit

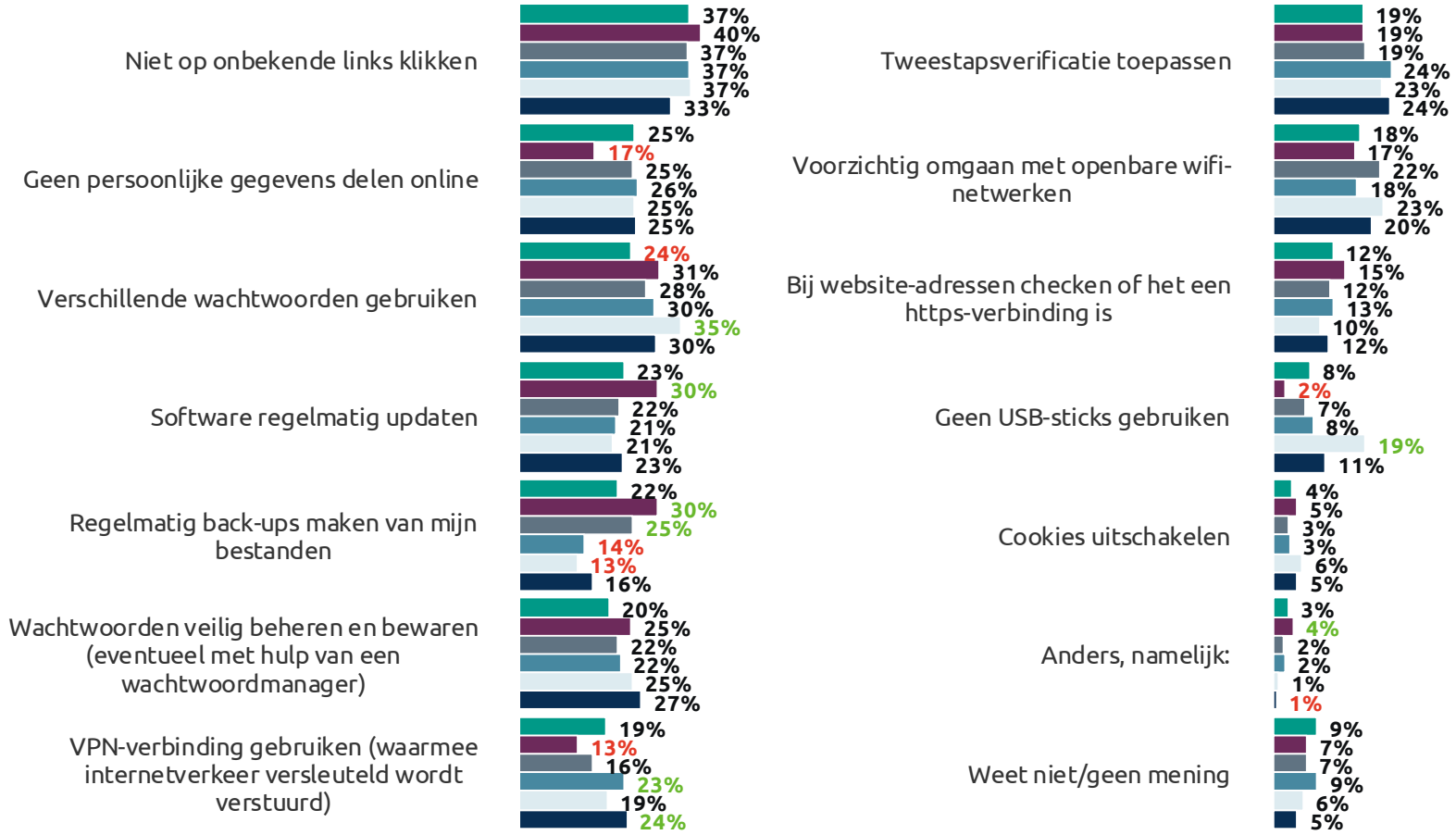
**Wanneer denk je dat je de grootste risico's loopt om slachtoffer te worden van cybercriminaliteit?** *Top 7 + weet niet*



# Resultaten | Digitaal gedrag

# MKB’ers denken relatief vaker aan back-ups van bestanden en updates van software als het om veilig online gedrag gaat

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




*Groen gemarkeerd percentage: antwoord is significant vaker gegeven door deze groep ten opzichte van de andere groepen*

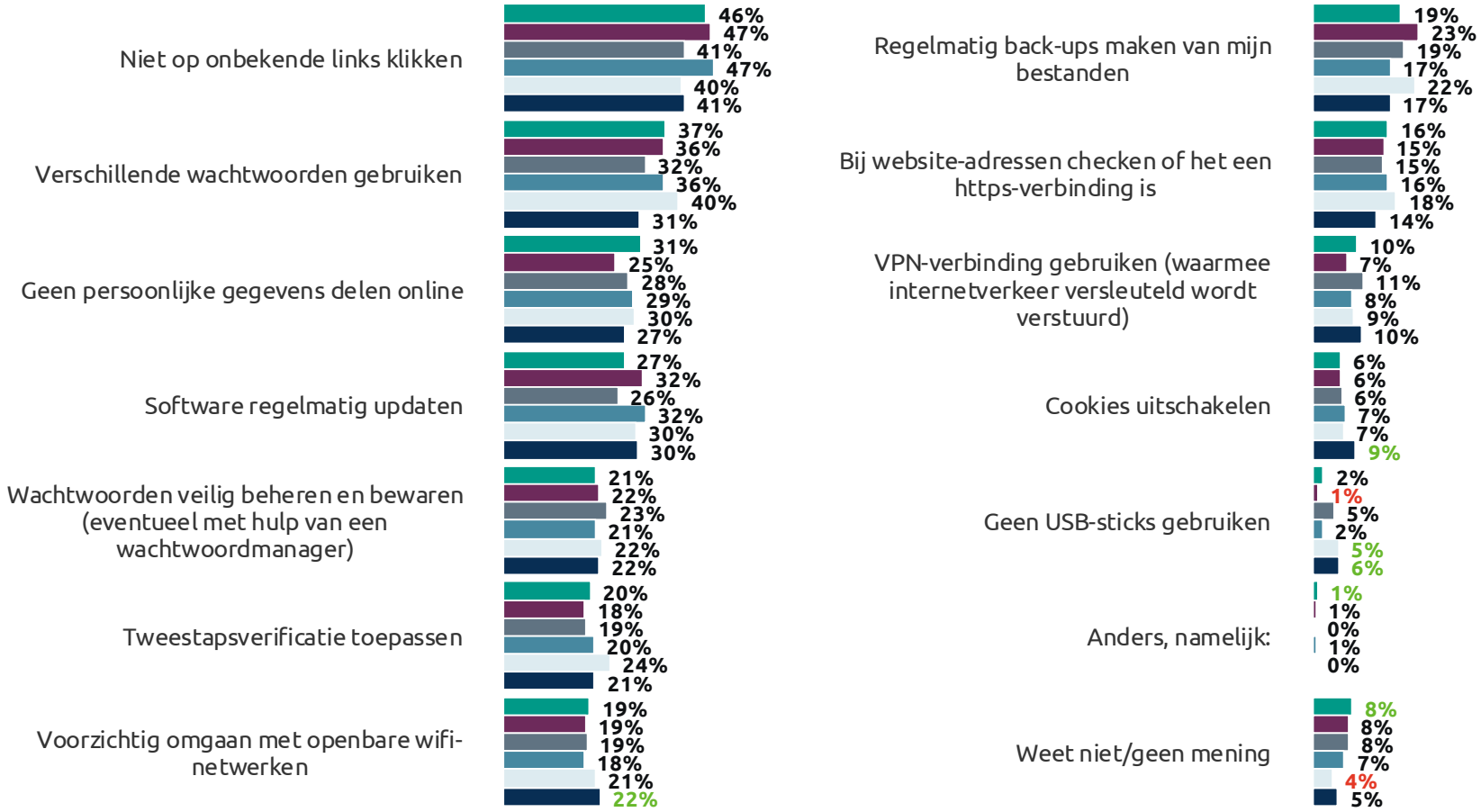
*Rood gemarkeerd percentage: antwoord is significant minder vaak gegeven door deze groep ten opzichte van de andere groepen*

- Werkend Nederland (n=501)
- Klein MKB (n=290)
- Groot MKB (n=293)
- Grootbedrijf (n=458)
- Ambtenaren (n=274)
- Vitale infrastructuur (n=342)

*Deze vraag is nieuw toegevoegd in 2019.*

# Veilig online gedrag thuis: vooral verschillende wachtwoorden gebruiken en niet op onbekende links klikken

**Waar denk jij in eerste instantie aan bij 'veilig online gedrag' <u>in een privésituatie</u>?**




*Groen gemarkeerd percentage: antwoord is significant vaker gegeven door deze groep ten opzichte van de andere groepen*

*Rood gemarkeerd percentage: antwoord is significant minder vaak gegeven door deze groep ten opzichte van de andere groepen*

- Werkend Nederland (n=501)
- Klein MKB (n=290)
- Groot MKB (n=293)
- Grootbedrijf (n=458)
- Ambtenaren (n=274)
- Vitale infrastructuur (n=342)

*Deze vraag is nieuw toegevoegd in 2019.*

# Nederlanders gaan veiliger om met gebruik van verschillende wachtwoorden, back-ups en online apparaten

## Verschillen binnen Nederland

- Mannen gaan naar eigen zeggen vaker veilig om met het gebruik van verschillende wachtwoorden (70% vs. 61% onder vrouwen), het gebruik maken van een wifi-verbinding onderweg (58% vs. 48%), het beschermen van hun gegevens door back-ups (64% vs. 53%), het updaten van hun software (80% vs. 72%) en het afgeven van toestemmingen op webshops (61% vs. 56%).
- Jongere Nederlanders (tot 24 jaar) gaan vaker veilig om met meerdere zaken, waaronder het bewaren van hun wachtwoorden (76%) en het gebruik van USB-sticks (67%). 25- t/m 34-jarigen gaan vaker veilig om met het gebruik van verschillende wachtwoorden (66%), het gebruik van wifi onderweg (64%), het omgaan met nepmails (79%), het beschermen van hun gegevens via back-ups (59%), het beheren en gebruik maken van persoons- en klantgegevens (68%), het updaten van software (78%) en het gebruik van USB-sticks (69%).
- Middelbaar opgeleiden gaan vaker veilig om met het gebruik van verschillende wachtwoorden (69%) en met het afgeven van toestemmingen op webshops (61%). Laagopgeleiden gaan minder vaak veilig om met het gebruik van USB-sticks (48%) en met het gebruik maken van hun devices door anderen (54%).

➢ *De grafiek staat op de volgende pagina.*

# Nederlanders gaan veiliger om met gebruik van verschillende wachtwoorden, back-ups en online apparaten

| In welke mate ga je veilig om met de volgende zaken? % goed/zeer goed/uitstekend | NL 16-80 jaar (n=1.004) | Klein MKB (n=290) | Groot MKB (n=293) | Groot-bedrijf (n=458) | Ambtenaren (n=274) | Vitale infra-structuur (n=342) |
|---|---|---|---|---|---|---|
| Bewaren van wachtwoorden | 72% | 70% | **74%** | 75% | 69% ↓ | **79%** |
| Gebruik van verschillende wachtwoorden | 65% ↑ | 62% | 68% | 67% | 64% | 70% |
| Gebruik van wifi-verbinding onderweg | 53% | 58% | **60%** | 66% ↑ | 57% | **70%** |
| Werken in een cloud | 47% | 49% | 55% | 51% | 54% | 61% |
| Opgaan met nepmails (poging tot phishing) | 77% | 80% | 79% | 82% | 79% | 83% |
| Beschermen van gegevens tegen diefstal via back-ups | 59% ↑ | 60% | **64%** | 58% | 58% | **66%** |
| Beheer en gebruik van persoons- en klantgegevens | 65% | 69% | **68%** | 71% | 64% ↓ | **76%** |
| Updaten van software | 76% | 77% | 78% | 81% | 81% | **82%** |
| Gebruik van USB-sticks | 60% | 64% | **64%** | 66% | 67% | 67% |
| Afgeven van toestemmingen op websites | 54% | 52% ↓ | 59% | 62% | 56% | 66% |
| Afgeven van toestemmingen op webshops | **58%** | 64% | 59% ↓ | 65% | 57% ↓ | 67% |
| Gebruik van jouw devices door anderen | 65% | 70% | 75% | 76% ↑ | 76% | 80% |
| Gebruik maken van apparaten die online verbinding kunnen maken | 41% ↑ | 38% | 48% | 49% | 48% | 56% ↑ |

# Eén op de zes Nederlanders maakt altijd gebruik van beschikbare open wifi-netwerken

## Vergelijking tussen doelgroepen

- Nederlanders maken minder vaak gebruik van een VPN-verbinding waarmee internetverkeer versleuteld verstuurd wordt. Medewerkers uit vitale sectoren maken daar vaker gebruik van.
- Dat verschil met Nederlanders en medewerkers uit de vitale infrastructuur is ook van toepassing op het gebruik maken van een verbinding via smartphone of tablet (hotspot).

## Verschillen binnen Nederland

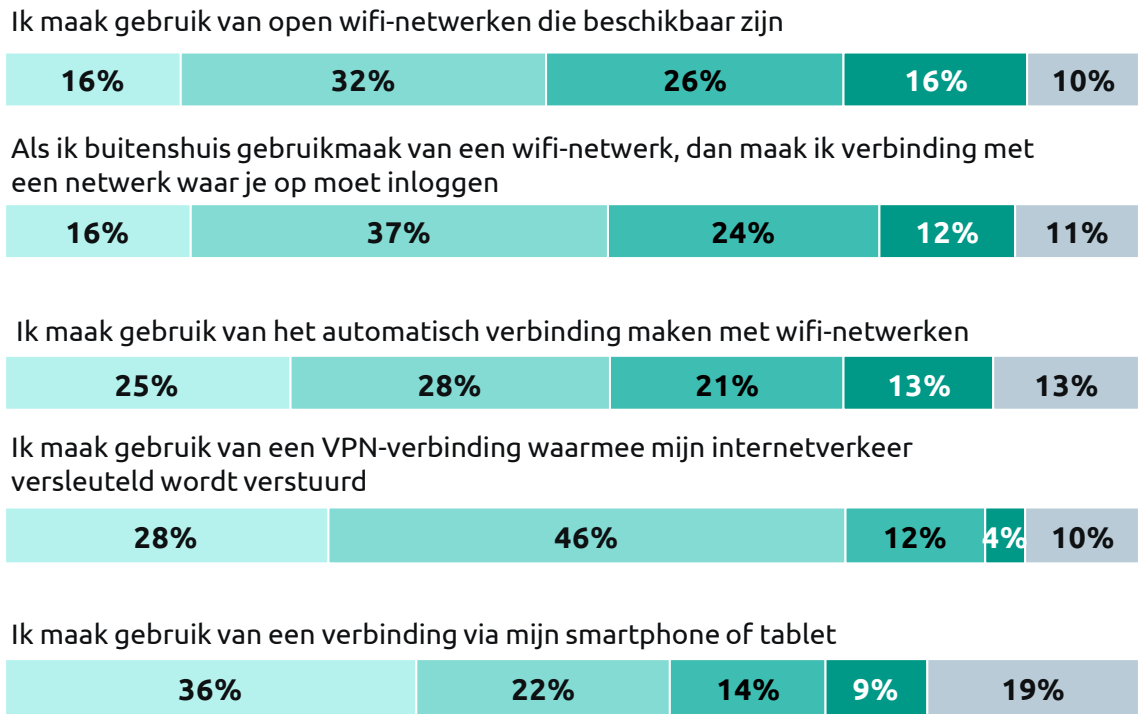
- Er zijn geen verschillen naar geslacht.
- Jongeren (16 – 24 jaar) maken vaker gebruik van open wifi-netwerken (80% weleens). Nederlanders in de leeftijd van 45 – 64 doen dat minder vaak (ca. 54% weleens).
- Nederlanders tussen 35 en 44 jaar maken vaker verbinding met een openbaar wifi-netwerk waarop ze moeten inloggen (82% weleens). 55 – 64-jarigen doen dat minder vaak (66%).
- Nederlanders in de leeftijd van 25 tot 34 jaar maken vaker gebruik van 'netwerk onthouden' (80% weleens), in tegenstelling tot 65-plussers (64%).
- Daarnaast maken ze vaker gebruik van een VPN-verbinding (57% weleens). Jongeren (tot 24 jaar) doen dat juist minder (45%).
- Jongere Nederlanders (tot 34 jaar) maken vaker gebruik van een verbinding via hun smartphone of tablet (ca. 76% weleens), 55- tot 64-jarigen doen dat juist minder vaak (50%).
- Hoogopgeleiden maken vaker verbinding met een netwerk waar ze op moeten inloggen (84% weleens), maken vaker gebruik van een VPN-verbinding (59% weleens) en maken vaker gebruik van een verbinding via hun smartphone of tablet (71% weleens). Middelbaar opgeleiden doen dat eerste (inloggen op een netwerk) minder vaak (71% weleens).

*Deze vraag is nieuw toegevoegd in 2019.*

➢ *De grafiek staat op de volgende pagina.*

# Eén op de zes Nederlanders maakt altijd gebruik van beschikbare open wifi-netwerken

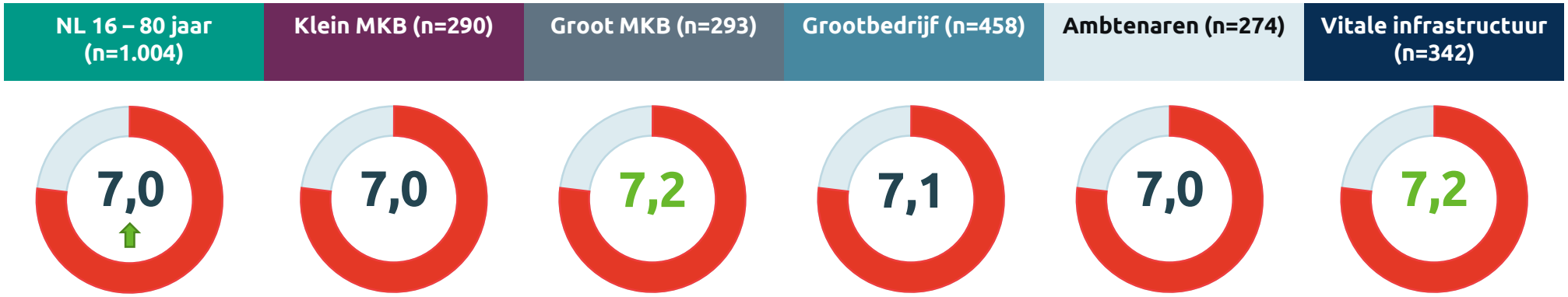
**Hieronder staat een aantal stellingen die gaan over het gebruikmaken van een wifi-verbinding terwijl je onderweg of op een externe locatie bent. In hoeverre zijn deze stellingen van toepassing op jouw gedrag?**
(Basis – NL 16 – 80 jaar, n=1.004)




*Deze vraag is nieuw toegevoegd in 2019. Voor resultaten uitgesplitst naar doelgroep: zie bijlage*

# Nederlanders gaan naar hun eigen idee dit jaar veiliger om met online gevaren dan vorig jaar

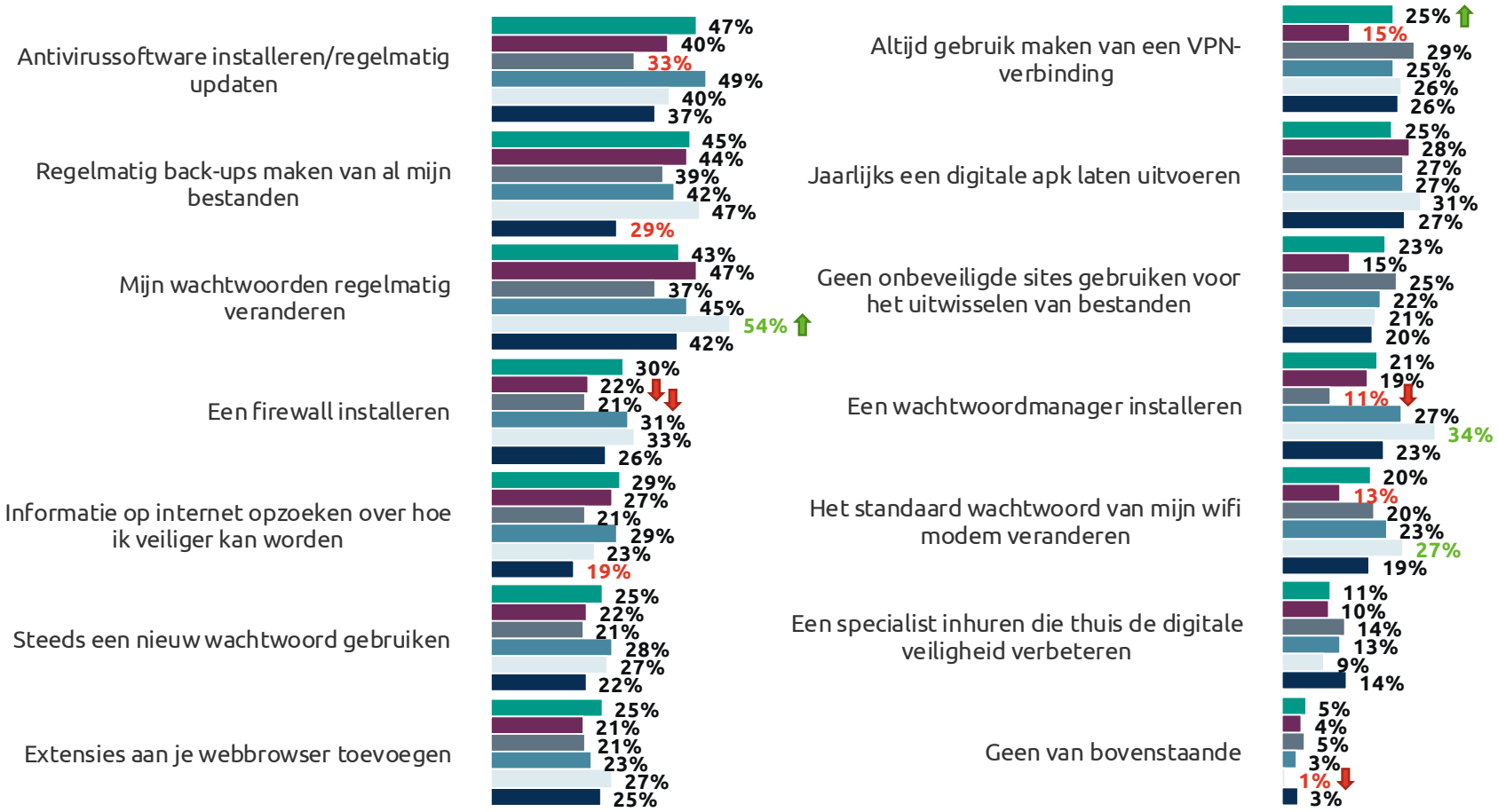
**Welk cijfer geef jij jezelf als het gaat om het veilig omgaan met online gevaren?**




| **Heb je er behoefte aan dat je persoonlijke veiligheid beter wordt?** | NL 16 – 80 jaar (n=1.004) | Klein MKB (n=290) | Groot MKB (n=293) | Grootbedrijf (n=458) | Ambtenaren (n=274) | Vitale infrastructuur (n=342) |
|---|---|---|---|---|---|---|
| • Vind ik niet nodig | 40% | 41% | 42% | 44% | 38% | 44% |
| • Ja, zou ik wel willen | 38% | 39% | 41% | 38% | **48%** | 44% |
| • Weet niet/geen mening | 23% | 21% | 17% | 18% | **13%** | **12%** |

# Ambtenaren vaker bereid tot verschillende opties om online veiligheid te verbeteren

**Welke van de onderstaande acties zou je bereid zijn om te doen om jouw online veiligheid te verbeteren?**
(Basis - Heeft behoefte aan verbetering online veiligheid)




*Groen gemarkeerd percentage: antwoord is significant vaker gegeven door deze groep ten opzichte van de andere groepen*

*Rood gemarkeerd percentage: antwoord is significant minder vaak gegeven door deze groep ten opzichte van de andere groepen*

*Ten opzichte van 2018 geven significant meer personen aan hiertoe bereid te zijn*

*Ten opzichte van 2018 geven significant minder personen aan hiertoe bereid te zijn*

# Vier op de tien loggen accounts uit na gebruik van een openbare computer

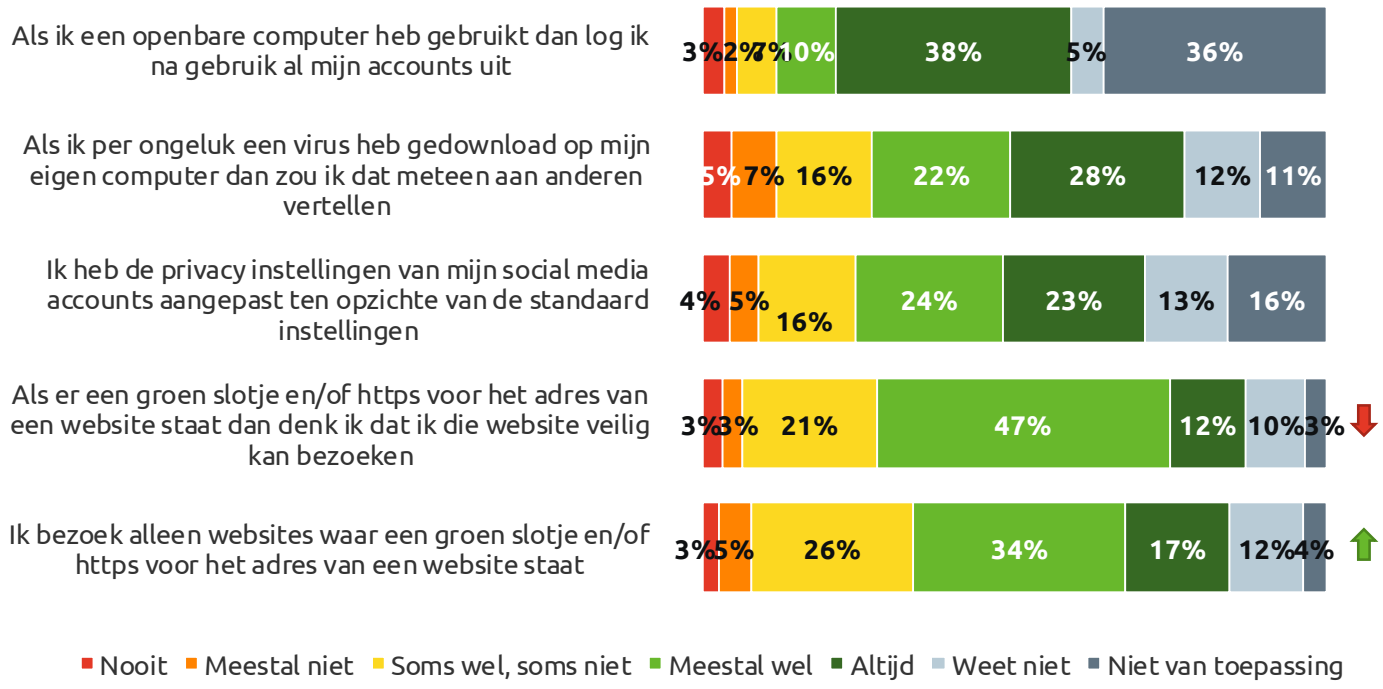
## Vergelijking met 2018

- Nederlanders denken minder vaak dat een website veilig is om een te bezoeken als er een groen slotje (of https) voor een website-adres staat.
- Ze bezoeken wel vaker alleen websites waar zo'n slotje (of code) voor staat dan vorig jaar.

## Verschillen binnen Nederland

- Vrouwen zouden het vaker meteen aan anderen vertellen als ze per ongeluk een virus hebben gedownload op hun computer (32% altijd, vs. 24% onder mannen). Dat geldt ook voor oudere Nederlanders (65 jaar en ouder) (38% altijd).
- Vrouwen bezoeken vaker alleen websites waar een groen slotje (en/of https) voor het adres staat (19% altijd vs. 14% onder mannen). Ook oudere Nederlanders (55 jaar en ouder) (24%) en laagopgeleiden scoren hierop relatief hoger (21%).
- Hoogopgeleiden denken vaker zij een website veilig kunnen bezoeken als er een groen slotje voor staat (17% altijd).

**In hoeverre zijn de volgende uitspraken van toepassing?**
(Basis - NL 16-80 jaar, n=1.004)



# Jongere Nederlanders (tot 44 jaar) vaker bereid te betalen na hack door ransomware

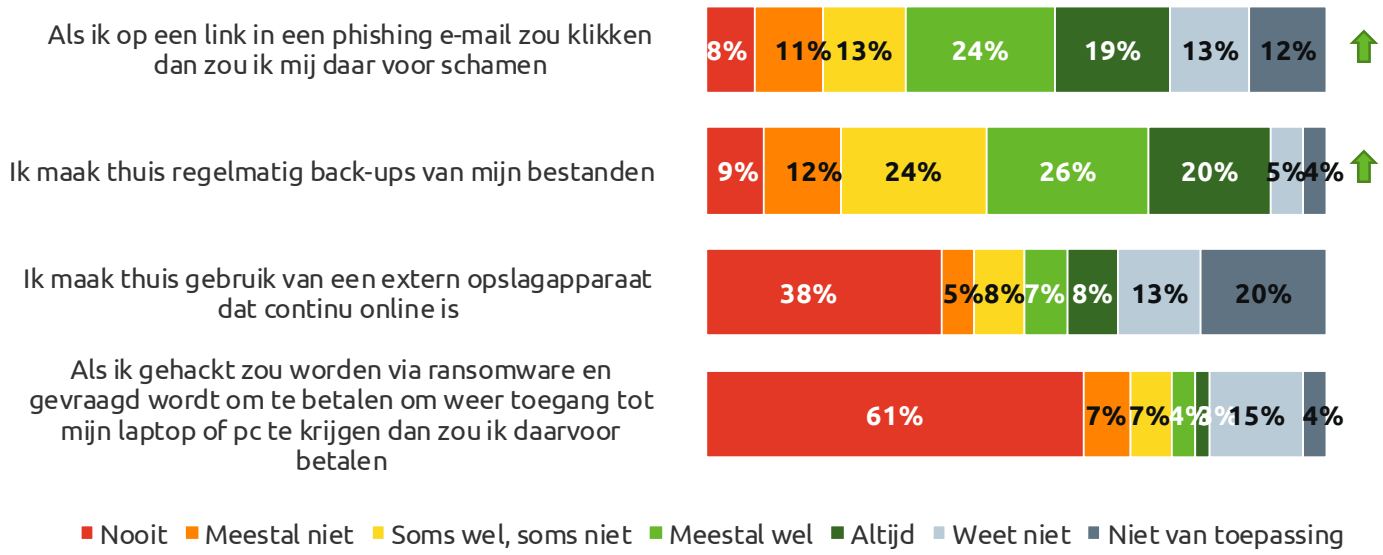
## Vergelijking met 2018

- Nederlanders schamen zich dit jaar vaker als ze op een phishing link zouden klikken
- Daarnaast maken ze vaker regelmatig back-ups van hun bestanden vergeleken met afgelopen jaar.

## Verschillen binnen Nederland

- Oudere Nederlanders (65 jaar en ouder) (27% altijd) en hoogopgeleiden (25%) zouden zich er vaker voor schamen als zij op een link in een phishing e-mail zouden klikken.
- Mannen (24% altijd vs. 16% onder vrouwen) en hoogopgeleiden (25%) maken vaker thuis regelmatig back-ups van hun bestanden.
- Mannen (10% altijd vs. 7%) en jongeren (25 – 34 jaar) (14% altijd) maken vaker thuis gebruik van een extern opslagapparaat dat continu online is.
- Jongere Nederlanders (16 tot 44 jaar) zouden vaker betalen om weer toegang te krijgen tot hun bestanden als ze gehackt worden via ransomware (ca. 5% altijd).

**In hoeverre zijn de volgende uitspraken van toepassing?**
(Basis - NL 16-80 jaar, n=1.004)



# Eén op de drie ouders laat kinderen nooit gebruik maken van hun werklaptop of -telefoon

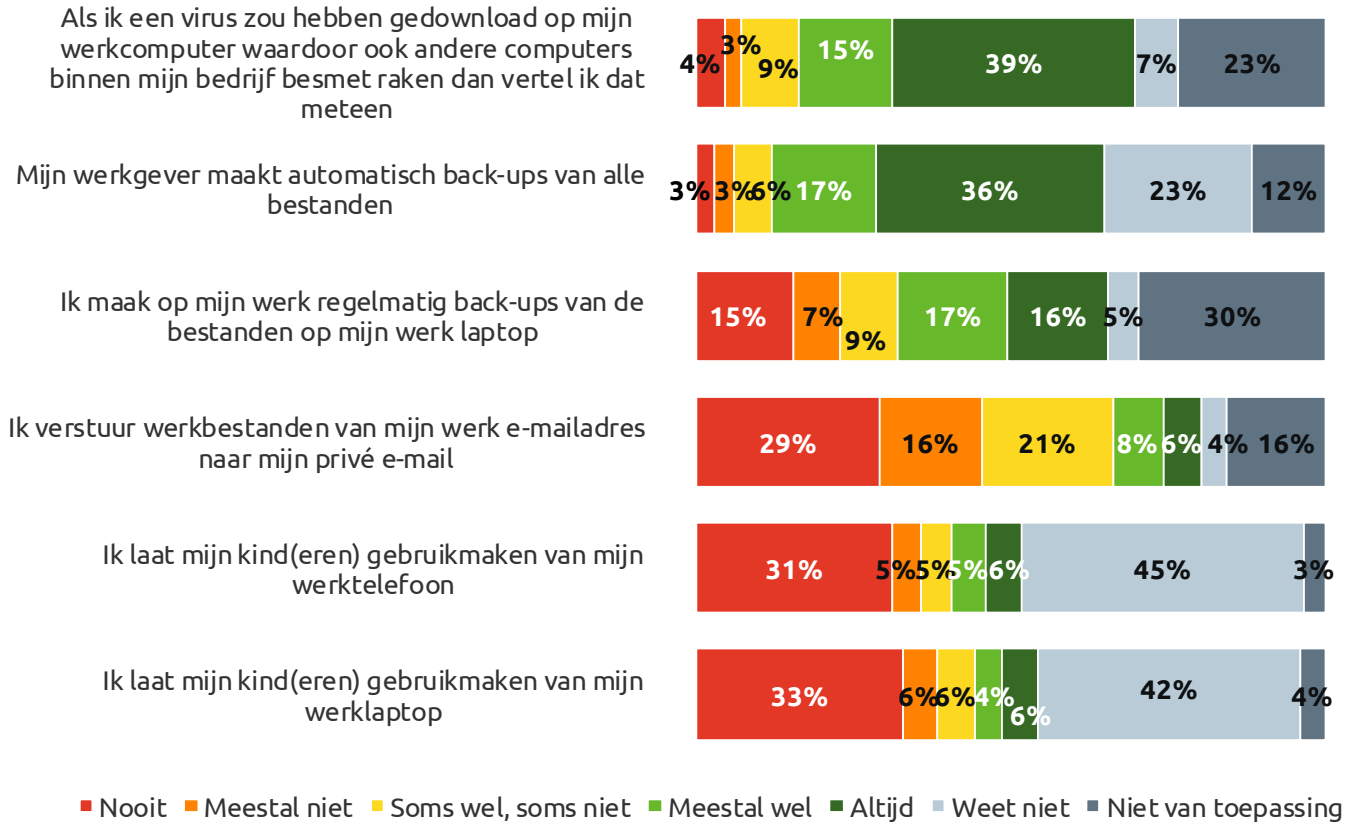
## Vergelijking met 2018

- Er zijn geen verschillen met 2018 op de stellingen hiernaast.

## Verschillen binnen Nederland

- Vrouwen (40% altijd, vs. 38% onder mannen), oudere Nederlanders (45 jaar en ouder) (ca. 52% altijd) en hoogopgeleiden (42% altijd) zouden het vaker meteen vertellen als hij een virus hebben gedownload op hun werkcomputer waardoor ook andere computers besmet raken.
- Nederlanders in de leeftijd van 45 jaar en ouder geven vaker aan dat hun werkgever automatisch back-ups maakt van alle bestanden (49% altijd).
- Jonge Nederlanders (16 – 24 jaar) maken zelf regelmatig back-ups van hun werkbestanden op hun werklaptop (28% altijd).
- Jongere Nederlanders (16 – 34 jaar) versturen vaker werkbestanden van hun werkmail naar hun privé mail (ca.13% altijd).

**In hoeverre zijn de volgende uitspraken van toepassing?**
(Basis - Werkenden, n=501)



# Een op de vijf Nederlanders ziet beveiligingsmaatregelen als een te grote belemmering

## Vergelijking met 2017*

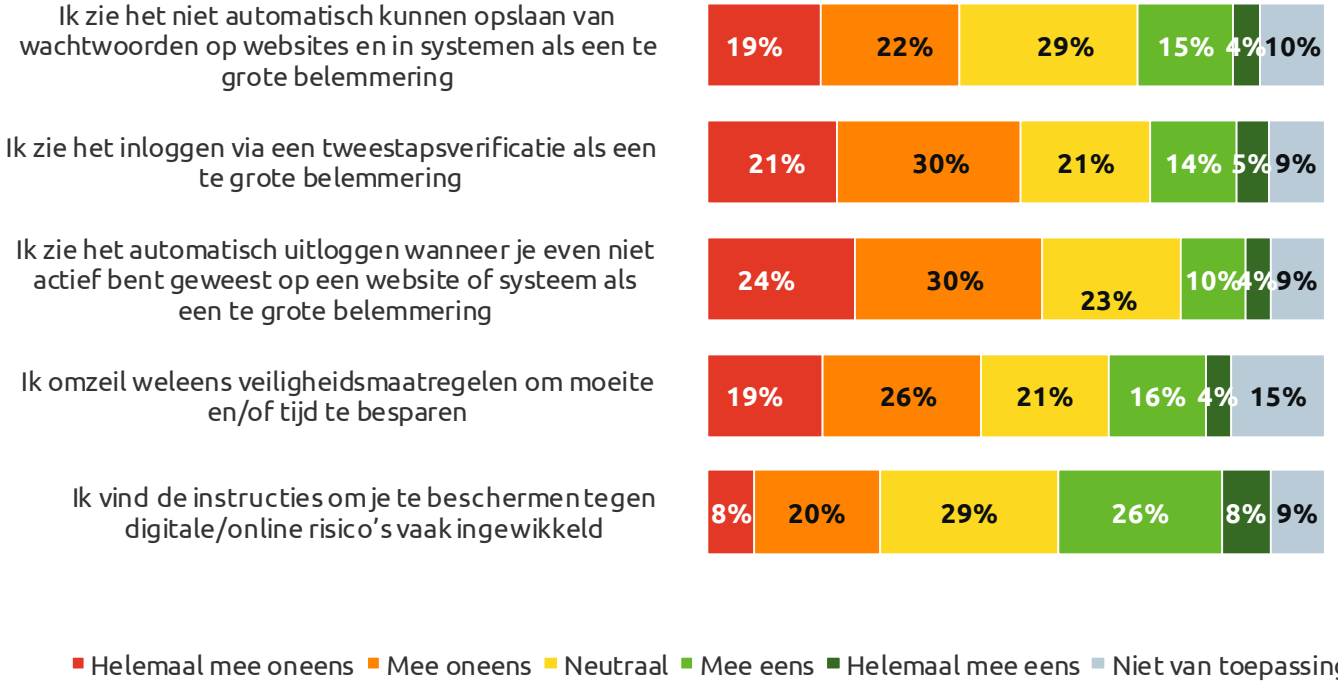
- Vergeleken met twee jaar terug zien Nederlanders tweestapsverificatie en automatisch uitloggen gemiddeld genomen minder vaak als een te grote belemmering. Wel vinden ze vaker dat de instructies om je te beschermen tegen digitale en online gevaren ingewikkeld zijn (31% in 2017).

## Verschillen binnen Nederland

- Nederlanders tussen 25 en 34 jaar (30%) zien het niet automatisch kunnen opslaan van wachtwoorden vaker als een te grote belemmering
- Jonge Nederlanders (16 – 24 jaar) zien het automatisch uitloggen als je even niet actief bent vaker als een te grote belemmering (16%).
- Jongere Nederlanders (16 – 44 jaar) omzeilen vaker weleens veiligheidsmaatregelen om moeite of tijd te besparen (ca. 32%).
- Vrouwen (39% vs. 30% onder mannen) en oudere Nederlanders (65 jaar en ouder) (44%) vinden de instructies om je te beschermen tegen online risico's vaker ingewikkeld.

* Deze vraag is niet gesteld in 2018. De resultaten zijn daarom vergeleken met 2017. Significante verschillen zijn alleen in tekst vermeld.

**Kun je aangeven in hoeverre je het eens bent met de volgende stellingen?**
(Basis - NL 16-80 jaar, n=1.004)




*Voor resultaten uitgesplitst naar doelgroep: zie bijlage*

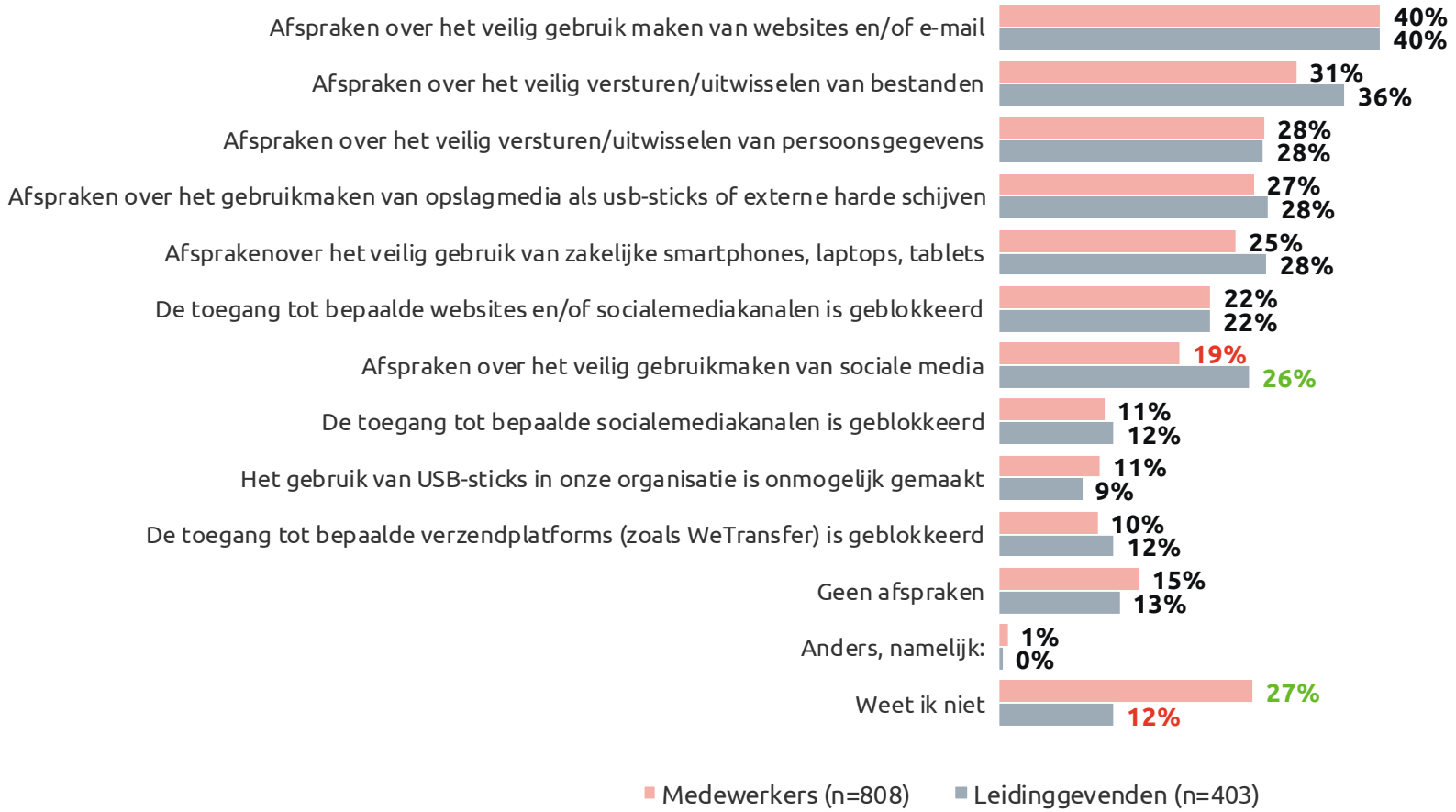
# Resultaten | Cybersecurity op de werkvloer

# Vier op de tien bedrijven hebben afspraken over het veilig gebruik maken van websites en e-mail

## Verschillen tussen doelgroepen

- Leidinggevenden hebben vaker afspraken binnen hun bedrijf/organisatie over veilig online gedrag dan medewerkers (75% onder leidinggevenden vs. 60% medewerkers).*
- Leidinggevenden hebben vaker afspraken over het veilig gebruik van sociale media dan medewerkers.

**Welke afspraken zijn er binnen jouw bedrijf/organisatie gemaakt over hoe je je online veilig gedraagt?**




*Deze vraag is nieuw toegevoegd in 2019.*

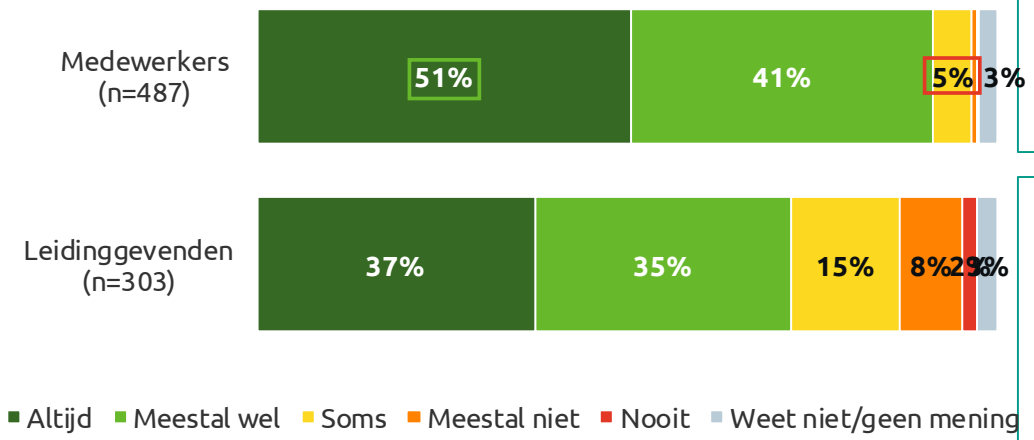
* Deze percentages zijn gebaseerd op een combinatie van de percentages 'geen afspraken' en 'weet ik niet'.

# De helft van de medewerkers houdt zich altijd aan de afspraken over online veilig gedrag

### Verschillen tussen doelgroepen

- Medewerkers houden zich naar eigen zeggen vaker aan de afspraken die binnen hun bedrijf of organisatie zijn gemaakt over hoe zij zich online veilig (moeten) gedragen.

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




**Waarom houden medewerkers zich niet aan de afspraken over online veilig gedrag?**
(Basis – medewerkers die zich (soms) niet aan de afspraken houden, n = 30)*

- Ze worden niet aangemoedigd om zich er aan te houden
- De afspraken zijn niet duidelijk
- De afspraken zijn niet zinvol

* Vanwege het lage aantal respondenten, worden geen percentages getoond. De uitkomsten zijn indicatief.

**Waarom houden leidinggevenden zich niet aan de afspraken over online veilig gedrag?**
(Basis – leidinggevenden die zich (soms) niet aan de afspraken houden, n = 76)*

- Andere collega's houden zich er ook niet aan
- Er wordt niet genoeg gecommuniceerd over de afspraken
- Ze worden niet aangemoedigd om zich er aan te houden

* Vanwege het lage aantal respondenten, worden geen percentages getoond. De uitkomsten zijn indicatief.

*Deze vraag is nieuw toegevoegd in 2019.*

# Medewerkers voelen zich meer verantwoordelijk voor hun online gedrag dan leidinggevenden

**Verschillen tussen doelgroepen**

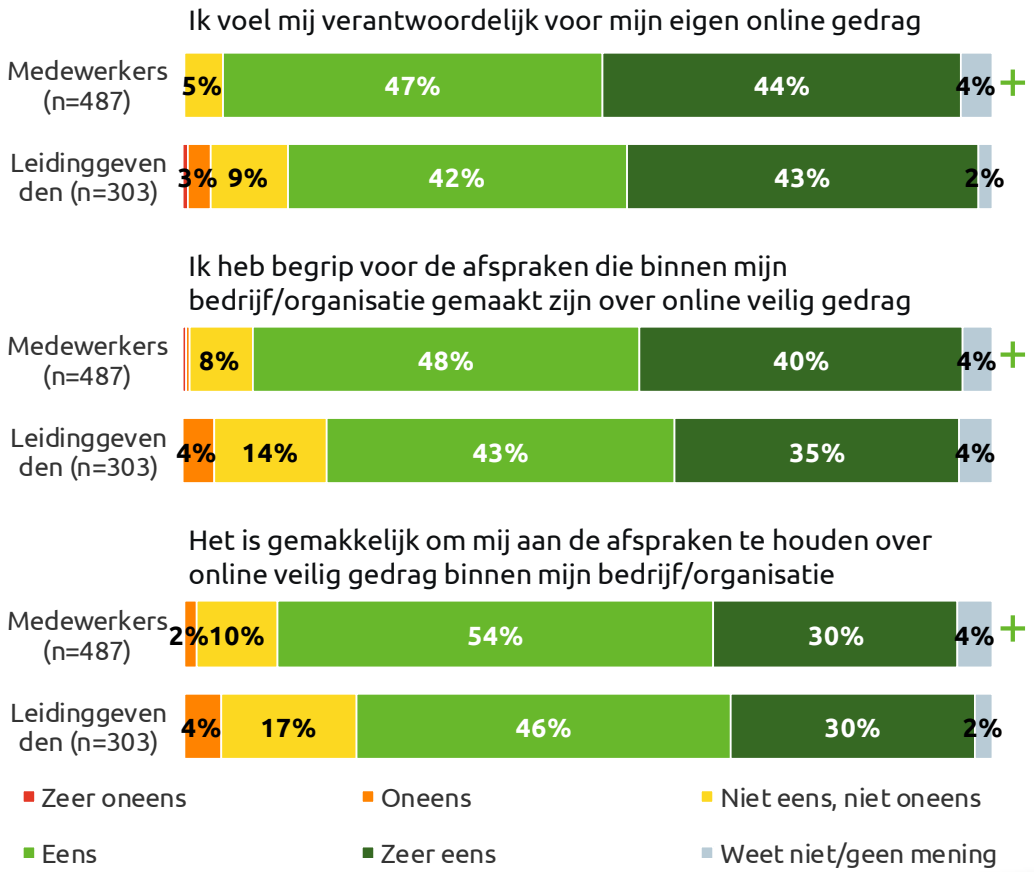
- *Deze pagina:*

  In vergelijking met leidinggevenden voelen medewerkers zich vaker verantwoordelijk voor hun eigen online gedrag, hebben ze vaker begrip voor begrip voor de afspraken over online veilig gedrag en vinden ze het vaker gemakkelijk om zich aan die afspraken te houden.

- *Volgende pagina:*

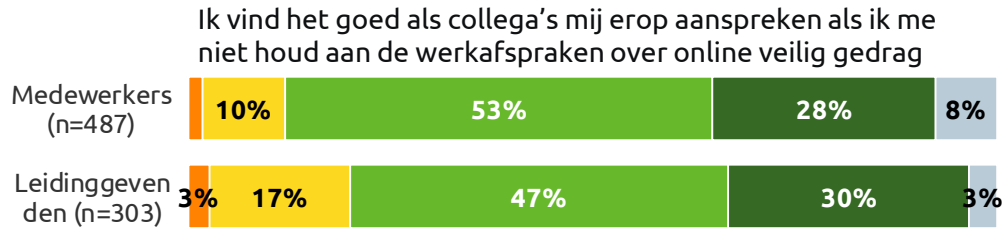
  In vergelijking met leidinggevenden zijn medewerkers minder geneigd om collega's er op aan te spreken als zij merken dat zij zich niet houden aan de werkafspraken over veilig online gedrag. Ook vinden medewerkers minder vaak dan leidinggevenden dat leidinggevenden het goede voorbeeld geven wat betreft online veilig gedrag.

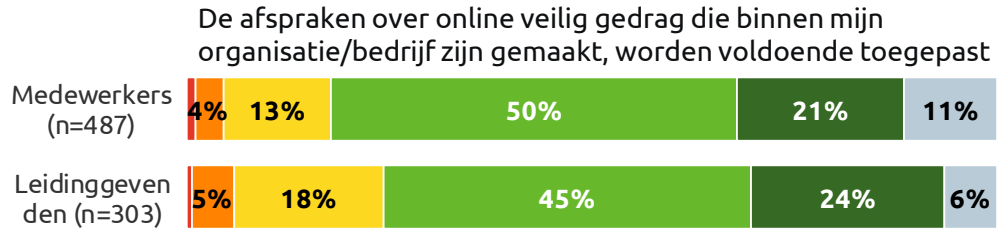
**In hoeverre ben je het eens met de volgende stellingen?**
(Basis – Er zijn afspraken over online veilig gedrag)

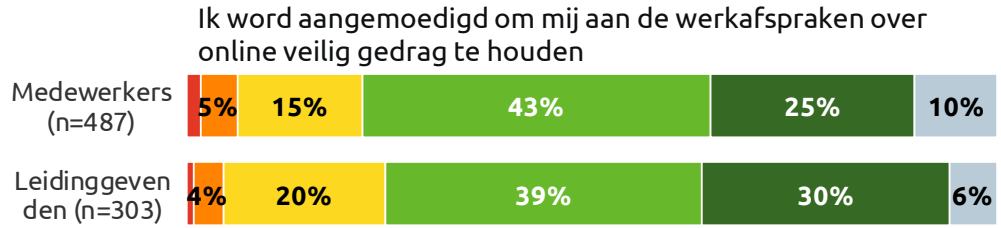


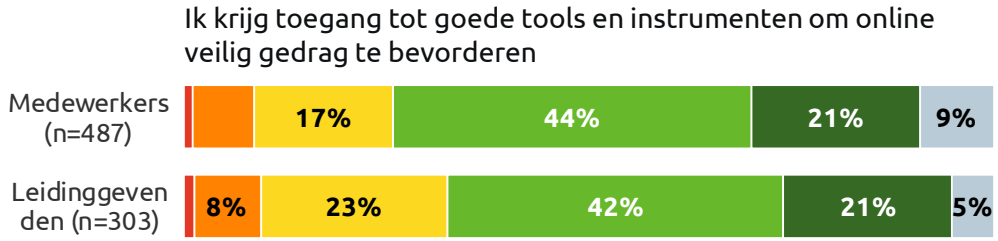

*Deze vraag is nieuw toegevoegd in 2019.*

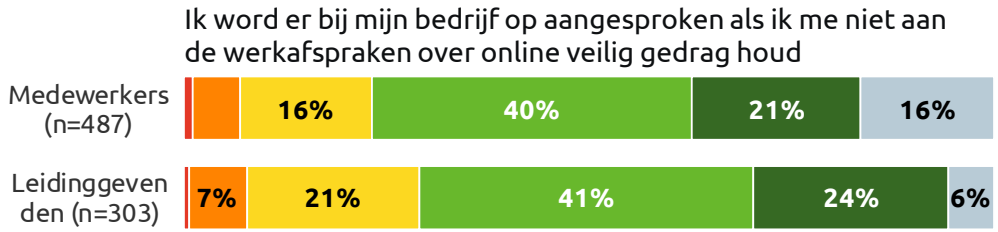
# Helft van de medewerkers vindt dat de leidinggevende het goede voorbeeld gaat qua online gedrag

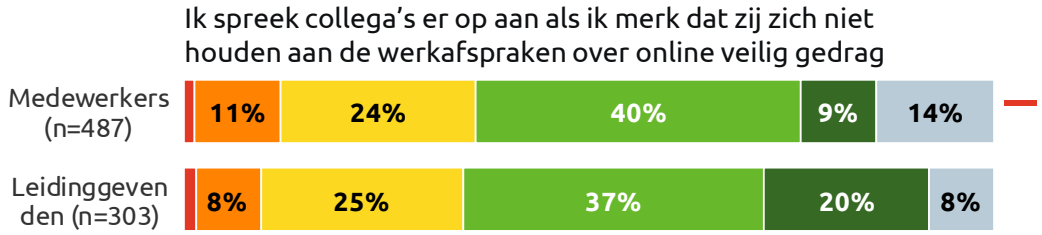



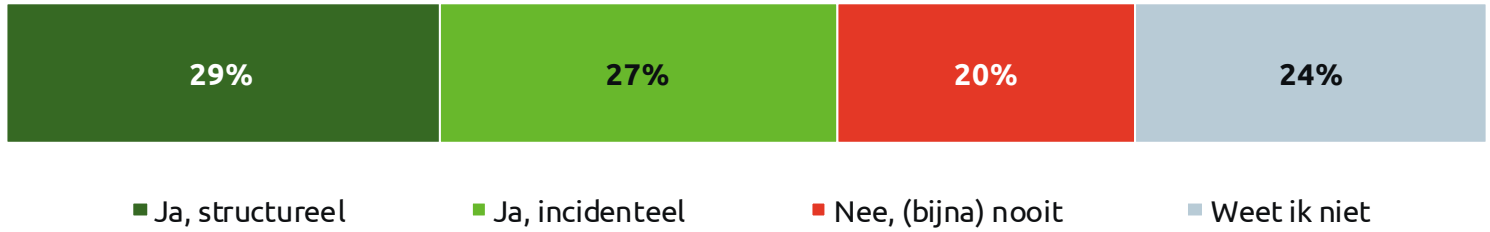




# Eén op de vijf bedrijven meet nooit of medewerkers zich houden aan de afspraken over online veilig gedrag

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




*Deze vraag is nieuw toegevoegd in 2019.*

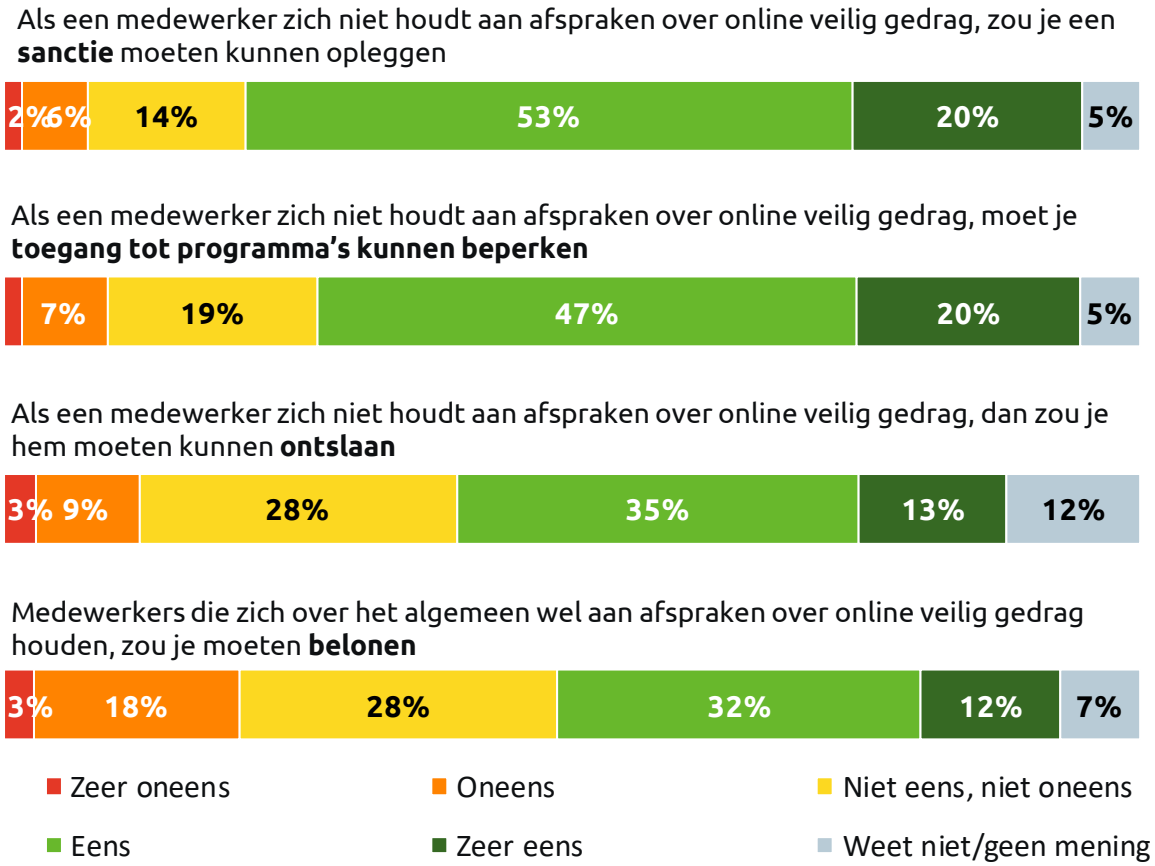
# Zes op de tien leidinggevenden ervaren belemmeringen bij het borgen van de afspraken over veilig online gedrag

**Welke belemmeringen ervaar je binnen jouw bedrijf bij het borgen van de afspraken voor online veilig gedrag?**
(Basis - Leidinggevend met afspraken over online veilig gedrag, n=303)


*Deze vraag is nieuw toegevoegd in 2019.*

# Ruim vier op de tien leidinggevenden vinden dat ontslag mogelijk moet zijn als medewerkers zich niet veilig gedragen online

**In hoeverre ben je het eens met de volgende stellingen?**
(Basis – Leidinggevend met afspraken over online veilig gedrag, n=303)




*Deze vraag is nieuw toegevoegd in 2019.*

# Bijlagen

# Bijlage | (On)bekendheid digitale risico's

| **Kun je aangeven in welke mate je bekend bent met de onderstaande zaken?** % Nog nooit van gehoord | **NL 16-80 jaar** (n=1.004) | **Klein MKB** (n=290) | **Groot MKB** (n=293) | **Grootbedrijf** (n=458) | **Ambtenaren** (n=274) | **Vitale infra-structuur** (n=342) |
|---|---|---|---|---|---|---|
| Phishing mails | 6% | 7% | 4% | 4% | 3% | 5% |
| Identiteitsfraude | 6% | 8% | 4% | 3% | 2% | 3% |
| Cyberaanval | 4% | 6% | 2% | 3% | 1% | 2% |
| Datalek | 10% | 9% | 8% | 9% | 4% | 5% |
| Spyware | 13% | 11% | 8% | 6% | 10% | 8% |
| DDoS-aanval | 20% | 16% | 16% | 15% | 13% | 14% |
| Malware | 15% | 14% | 14% | 9% | 9% | 8% |
| Ransomware | 25% | 22% | 20% | 19% | 18% | 13% |
| Keylogger | 54% | 51% | 45% | 42% | 39% | 27% |
| Botnet | 62% | 54% | 57% | 51% | 53% | 39% |
| Social engineering | 51% | 45% | 47% | 42% | 43% | 28% |
| Spoofing | 66% | 60% | 57% | 56% | 59% | 43% |
| Portscan | 69% | 68% | 59% | 59% | 60% | 43% |
| Juice jacking | 79% | 80% | 68% | 72% | 68% | 54% |

# Bijlage | Gebruik van wifi onderweg

| Hieronder staat een aantal stellingen die gaan over het gebruikmaken van een wifi-verbinding terwijl je onderweg of op een externe locatie bent. In hoeverre zijn deze stellingen van toepassing op jouw gedrag? | NL 16-80 jaar | | Klein MKB | | Groot MKB | | Grootbedrijf | | Ambtenaren | | Vitale infrastructuur | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | % nooit | % soms/ regelmatig /altijd | % nooit | % soms/ regelmatig /altijd | % nooit | % soms/ regelmatig /altijd | % nooit | % soms/ regelmatig /altijd | % nooit | % soms/ regelmatig /altijd | % nooit | % soms/ regelmatig /altijd |
| Ik maak gebruik van open wifi-netwerken die beschikbaar zijn (waarbij ik niet hoef in te loggen) | 28% | 62% | 32% | 65% | 28% | 66% | 30% | 66% | 31% | 65% | 31% | 65% |
| Als ik buitenshuis gebruikmaak van een wifi-netwerk, dan maak ik verbinding met een netwerk waar je op moet inloggen | 16% | 73% | **8%** | **85%** | 17% | 76% | 14% | 81% | 16% | 79% | 14% | 82% |
| Ik maak gebruik van het automatisch verbinding maken met wifi-netwerken (netwerk onthouden) | 16% | 75% | 17% | 79% | 16% | 78% | 16% | 80% | 12% | 85% | 13% | 82% |
| Ik maak gebruik van een VPN-verbinding waarmee mijn internetverkeer versleuteld wordt verstuurd | **36%** | **45%** | 33% | 56% | 30% | 55% | 27% | 65% | 32% | 59% | **19%** | **75%** |
| Ik maak gebruik van een verbinding via mijn smartphone of tablet (bijv. 3G/4G netwerk en telefoon als hotspot of een tablet met een data-abonnement) | **25%** | **62%** | 26% | 68% | 22% | 70% | 20% | 75% | 23% | 72% | **14%** | **83%** |

# Bijlage | Belemmering door veiligheidsmaatregelen

| Kun je aangeven in hoeverre je het eens bent met de volgende stellingen? % (helemaal) mee eens | NL 16 – 80 jaar | Klein MKB | Groot MKB | Grootbedrijf | Ambtenaren | Vitale infrastructuur |
|---|---|---|---|---|---|---|
| Ik zie het niet automatisch kunnen opslaan van wachtwoorden op websites en in systemen als een te grote belemmering | 20% | 20% | 23% | 18% | 22% | 24% |
| Ik zie het inloggen via een tweestapsverificatie als een te grote belemmering | 19% | 17% | 19% | 20% | 18% | 21% |
| Ik zie het automatisch uitloggen wanneer je even niet actief bent geweest op een website of systeem als een te grote belemmering | 14% | 15% | 17% | 13% | 18% | 18% |
| Ik omzeil weleens veiligheidsmaatregelen om moeite en/of tijd te besparen | 20% | 21% | 23% | 18% | 22% | **25%** |
| Ik vind de instructies om je te beschermen tegen digitale/online risico's vaak ingewikkeld | 34% | 36% | 34% | **30%** | 38% | 35% |

# Bijlage | Onderzoekstechnische informatie

- **Veldwerkperiode**
  - Het veldwerk is uitgevoerd in de periode van 26 juni 2019 tot 10 juli 2019
- **Methode respondentenselectie**
  - Uit het StemPunt-panel van Motivaction en via een partnerpanelbureau
- **Incentives**
  - De respondenten hebben als dank voor deelname aan het onderzoek punten voor het StemPunt-spaarprogramma ontvangen
- **Weging**
  - De onderzoeksdata voor de Nederlandse bevolking (16 – 80 jaar) zijn gewogen. Daarbij fungeerde de Gouden Standaard van het CBS als herwegingskader.
- **Inschakelen externe leveranciers**
  - Voor de volgende werkzaamheden heeft Motivaction bij dit onderzoek gebruik gemaakt van de diensten van gespecialiseerde bedrijven: uitvoeren veldwerk voor de doelgroep medewerkers in de vitale infrastructuur.
- **Responsverantwoording online onderzoek**
  - Op de slotdatum van het veldwerk (zie bij Veldwerkperiode) was het gewenste aantal vragenlijsten ingevuld en is de toegang tot de vragenlijst op internet afgesloten.
- **Bewaartermijn primaire onderzoeksbestanden**
  - Digitaal beschikbare primaire onderzoeksbestanden worden tenminste 12 maanden na afronden van het onderzoek bewaard.
- **Overige onderzoekstechnische informatie**
  - Overige onderzoekstechnische informatie en een exemplaar van de bij dit onderzoek gehanteerde vragenlijst is op aanvraag beschikbaar voor de opdrachtgever

# Auteursrecht

Het auteursrecht op dit rapport ligt bij de opdrachtgever. Voor het vermelden van de naam Motivaction in publicaties op basis van deze rapportage - anders dan integrale publicatie - is echter schriftelijke toestemming vereist van Motivaction International B.V.

### 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.

# 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