motivaction
research and strategy

Nationaal Cybersecurity Bewustzijnsonderzoek

Rapportage 2017

Auteurs:
Anne Blanksma Çeta
Femke Konings

28-9-2017

ALERT online

OmnicomPublicRelationsGroup

Balancing Security and Mobility
De bewustwordingscampagne Alert Online wordt mede gefinancierd door het Fonds voor Interne Veiligheid van de Europese Unie

Inhoudsopgave

Achtergrond

In opdracht van Omnicom Public Relations Group (OPRG) heeft Motivaction International B.V. een onderzoek uitgevoerd voor de Alert Online-campagne naar het bewustzijn van cybergevaren en het online gedrag van de Nederlandse (beroeps-)bevolking. Deze campagne wordt in opdracht van het ministerie van Veiligheid en Justitie uitgevoerd en wordt gesubsidieerd door het Fonds voor interne veiligheid van de Europese Unie.

Aanleiding

In 2012 is de NCTV 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.

Conclusies 1/4

Nederlanders maken zich nauwelijks zorgen over digitale veiligheid op het werk, in privésfeer zijn er meer zorgen

Drie kwart van werkend Nederland maakt zich weinig tot zéér weinig zorgen over de digitale veiligheid in zijn of haar werksituatie. In de privésituatie zijn er meer zorgen over digitale veiligheid: 46% maakt zich hierover (enige tot grote) zorgen. De toegenomen aandacht voor cybergevaren in de media en in publiekscampagnes heeft er mogelijk toe geleid dat men zich meer zorgen is gaan maken over de digitale veiligheid thuis. Een derde van de mensen voelt zich thuis niet beschermd tegen een cyberaanval. Dit komt vooral omdat men vaak niet weet hoe zich hier tegen te wapenen, anderzijds wordt de kans hierop over het algemeen laag ingeschat. Na een daling van de zorgen in 2016 ten opzichte van 2015, is er in 2017 weer een stijging te zien in het aandeel van de Nederlanders dat zich thuis zorgen maakt. De mate van zorg voor de online veiligheid op het werk is in dezelfde periode licht gedaald van 27% in 2015 naar 21% in 2017. Onder de belangrijke beroepsgroep *medewerkers in de vitale infrastructuur* (medewerkers met een computer die zich bezighouden met vitale processen zoals drinkwatervoorziening, elektriciteit, betalingsverkeer tussen banken, etcetera) zijn er wel meer zorgen over digitale veiligheid: 16% maakt zich (zeer) veel zorgen, 39% enigszins zorgen. Maar ook onder deze groep maakt een substantiële groep van 45% zich (zeer) weinig zorgen.

Cyberonveiligheid tot zekere mate geaccepteerd: lage inschatting impact, wel regelmatig slachtoffer

De reden dat mensen zich relatief weinig zorgen maken over hun digitale veiligheid lijkt vooral te liggen in hun lage inschatting van de impact van diverse vormen van cybercrime. De kans op (computer)schade wordt op alle vormen lager dan 15% ingeschat terwijl per voorval 10% tot 55% hier wel persoonlijk een ervaring mee heeft. Een mogelijke verklaring hiervoor is dat de schade beperkt bleef of van korte duur was. Nederlanders schatten hun eigen online skills over het algemeen hoog in. Een ruime meerderheid van de Nederlanders denkt goed, zeer goed of zelfs uitstekend om te gaan met potentieel gevaarlijke situaties. Wanneer iemand daadwerkelijk slachtoffer is geworden van een vorm van cybercrime dan zorgt dit vaak wel degelijk tot een aanpassing van het gedrag. Veel slachtoffers geven aan voorzichtiger te zijn geworden na het voorval of voorzorgsmaatregelen te hebben getroffen.

Conclusies 2/4

Cyberzorgen vooral gericht op conventionele cybergevaren: e-mails met hyperlinks of bijlagen

Nederlanders denken vooral risico te lopen door e-mails met hyperlinks of met een besmette bijlage. Uit de cijfers blijkt dat mensen vaker thuis benaderd zijn met phishing mails op een privé-e-mailadres dan op een werk-e-mailadres (55% van alle Nederlanders i.p.v. 39% van alle werkenden). Hierdoor is waarschijnlijk het idee ontstaan dat er thuis meer is om je zorgen over te maken en minder in werksituaties, waar phishing mails vaak niet door spamfilters heenkomen. Nederlanders denken dat zij op een veilige manier met dreigingen omgaan door enkel alert te zijn op links in e-mails en bijlagen bij e-mails.

Blinde vlek voor nieuwe gevaren: openbare wifi-netwerken, juice jacking, keyloggers, etcetera.

Cybercriminaliteit vindt steeds vaker plaats buiten de meer traditionele vorm van een e-mail met een hyperlink of een besmette bijlage. Deze vormen staan echter nog niet op de radar van de gemiddelde Nederlander. De termen om deze gevaren aan te duiden zijn nog nauwelijks bekend en ook de situaties waarin deze zich voordoen worden niet als risicovol herkend. Zo zijn er buitenshuis en onderweg diverse situaties denkbaar waarin men slachtoffer kan worden van cybercriminelen. Bijvoorbeeld in het geval dat een telefoon of laptop automatisch met een openbaar netwerk verbinding maakt zonder dat de gebruiker hier erg in heeft. Wanneer men eenmaal heeft ingelogd op een verkeerd netwerk zal altijd verbinding worden gemaakt met dit netwerk zodra men in het bereik van dit netwerk komt, zonder dat de gebruiker het doorheeft en zonder dat om goedkeuring gevraagd wordt. Of in het geval dat er gebruik wordt gemaakt van internetbankieren over een onbeveiligde wifi-verbinding. Bij een USB-oplaadpunt op een vliegveld kan men slachtoffer worden van *juice jacking* doordat de USB-poort gegevens uitleest of malware installeert. Banners op websites of in apps kunnen geïnfecteerde advertentiesoftware bevatten die het apparaat bij bezoek besmetten. Allemaal voorbeelden van gevaren die niet via een e-mail verspreidt worden.

Conclusies 3/4

Medewerkers in de vitale infrastructuur zijn als groep binnen de Nederlandse beroepsbevolking beter op de hoogte van digitale gevaren. Zij hebben meer kennis van online gevaren en schatten de kans dat situaties zich voordoen ook hoger in. De mate van zorg in deze groep is hoger voor zowel werk- als privésituaties. Deze groep beschermt zichzelf minder vaak met de traditionele virusscanner, zoals de meeste Nederlanders dat doen, maar maken al gebruik van meer geavanceerde technieken zoals *spyware scanners* en *web tracking blockers*.

Media exposure over cybergevaren zorgt voor meer bekendheid en meer voorzichtigheid

In het eerst half jaar van 2017 was er veel media-aandacht voor incidenten met ransomware en dat is terug te zien in de cijfers. De bekendheid van dit fenomeen is fors toegenomen bij alle groepen in de samenleving. Personen die iets gehoord, gezien of gelezen hebben over een cyberaanval in de afgelopen zes maanden geven in meerderheid aan voorzichtiger te zijn geworden als reactie op de berichtgeving.

Gebrek aan kennis en lage prioriteit belangrijkste redenen om geen preventiemaatregelen te treffen

De belangrijkste redenen om niet voorbereid te zijn op een cyberaanval thuis zijn: *Ik weet niet hoe ik dat moet doen*, *de kans is klein dat mij dit overkomt* en *daar heb ik nog nooit over nagedacht*. Een gebrek aan kennis van preventiemaatregelen wordt het meest genoemd als motivatie om niet voorbereid te zijn. Maar het lijkt ook geen hoge prioriteit te hebben bij het Nederlands publiek: men is van mening dat de kans klein is persoonlijk getroffen te worden en denkt er vaak helemaal niet over na.

Medewerkers hebben weinig kennis van databeveiliging binnen het bedrijf

De helft van alle werkenden geeft aan informatie te krijgen van zijn of haar werkgever over veilig online werken, de andere helft van de werkende Nederlanders geeft aan hier nooit informatie over te hebben gekregen. De veiligheidsprocedures binnen het bedrijf of de organisatie waar men werkt is voor veel medewerkers *een black box*. Of de servers waar data op staan beveiligd zijn en op welke manier, is voor veel werknemers niet bekend. Ook de manier waarop persoons- of klantgegevens verstuurd worden is bij velen niet bekend.

Conclusies 4/4

Cyberrisico's voor jonge kinderen: veel online, er kijkt vaak geen volwassene mee, veel risicovol gedrag

Kinderen in groep 7 en 8 zijn vaak online actief. Negen van de tien kinderen in deze leeftijdsgroep beschikken over een smartphone en 7 van de 10 kinderen heeft een eigen account op een van de drie grote social media platformen: Facebook, Instagram en Snapchat. De helft van deze jonge gebruikers geeft aan niet zonder social media te kunnen. 81% van de kinderen geeft aan dat hun ouders op de hoogte zijn van wat zij doen op internet en op social media, veel ouders kennen ook de wachtwoorden van de socialmedia-accounts van hun kinderen. Toch lijkt er niet altijd direct toezicht te zijn wanneer kinderen online zijn. Kinderen zijn vaak online zonder dat er een volwassene naast hen zit en meekijkt op het scherm.

Kinderen hebben veel vrijheid online en worden regelmatig geconfronteerd met risicovolle situaties. Kinderen ontvangen vriendschapsverzoeken van vreemden en worden gevraagd om op onbekende links te klikken. Een op de drie kinderen van 11 of 12 jaar vertoont wel eens risicovol gedrag zoals het klikken op banners op een website of op links in socialmedia-berichten. Ook de links op Facebook die verwijzen naar online persoonlijkheidstesten worden regelmatig door kinderen aangeklikt.

Kinderen maken met hun smartphone regelmatig gebruik van openbare wifi-netwerken, maar de meeste kinderen weten niet hoe je kunt herkennen of een netwerk veilig is. Ook gebruikt een kwart van alle kinderen altijd hetzelfde wachtwoord voor alle websites wat er bij een hack toe leidt dat kwaadwillenden in één keer toegang hebben tot alle accounts van het kind. Kinderen in groep 7 en 8 krijgen veel voorlichting over veilig online gedrag op school en van hun ouders. Maar doordat kinderen veel vrijheid krijgen online en gedrag plaatsvindt buiten het zicht van de ouders vormt deze groep een belangrijke risicogroep voor cybergevaren.

Methode en opzet

Veldwerkperiode en respons

Het veldwerk is uitgevoerd in de maanden juli en augustus van 2017. In totaal is aan 10.810 Nederlanders in de leeftijdscategorie 13-80 jaar een uitnodiging gestuurd voor deelname. 2.106 personen hebben de enquête volledig en correct ingevuld, een respons van 19%. Aan 1.617 panelleden is een uitnodiging verstuurd met het verzoek de vragenlijst door hun kind van 11 of 12 jaar te laten invullen. Op de sluitingsdatum hadden 108 kinderen de enquête correct en volledig ingevuld, een response van 7%.

De onderzoekspopulatie van dit onderzoek bestaat uit een representatieve steekproef van 1.123 Nederlanders in de leeftijd 13-80 jaar. Om uitspraken te kunnen doen over verschillende subgroepen in de beroepsbevolking zijn voor 6 subgroepen aanvullende respondenten geworven om de benodigde minimale steekproef omvang van n=250 te behalen. In een aantal gevallen is gebruikgemaakt van een partnerbureau om respondenten te benaderen.

Weging

De netto steekproef van 1.123 Nederlanders in de leeftijd 13-80 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 en de aanvullende steekproef van kinderen in groep 7 en 8 zijn niet gewogen omdat hier geen referentiecijfers van beschikbaar zijn.

Leeswijzer

Doelgroepen

In dit onderzoek worden alle resultaten weergegeven voor de Nederlandse bevolking 13 tot en met 80 jaar. Waar het vragen over de werksituatie betreft worden alleen percentages weergegeven van de werkzame bevolking.

Naast de representatieve steekproef worden overal de resultaten van 6 specifieke groepen werkenden weergegeven:

- Medewerkers in het klein MKB (1-9 medewerkers, inclusief ZZP'ers)
- Medewerkers in het groot MKB (10-200 medewerkers)
- Medewerkers in het Grootbedrijf (meer dan 200 medewerkers)
- Rijksambtenaren
- Ambtenaren buiten de Rijksoverheid
- Medewerkers in de vitale infrastructuur (zie pagina 9 voor definitie van deze doelgroep)

Kinderen in groep 7 en 8

In het laatste hoofdstuk van dit rapport zijn de resultaten weergegeven van het aanvullende onderzoek naar cyber awareness en cyber skills dat uitgevoerd is onder kinderen van 11 of 12 jaar.

Significante verschillen

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

GROEN = significante **over**vertegenwoordiging

ORANJE = significante **onder**vertegenwoordiging

Leeswijzer

Medewerkers vitale infrastructuur

De vitale infrastructuur is in dit onderzoek gedefinieerd als personen die van hun werkgever een pc, laptop, smartphone of tablet ter beschikking hebben gekregen en die werken in een bedrijf/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

Verschillen naar achtergrondkenmerken

Indien er verschillen zijn aangetroffen op leeftijd, opleidingsniveau of geslacht is dit vermeld in de tekst mits van toegevoegde waarde. Alle verschillen per doelgroep zijn terug te vinden in het bijgevoegde tabellenboek.

Risicoperceptie en slachtofferschap

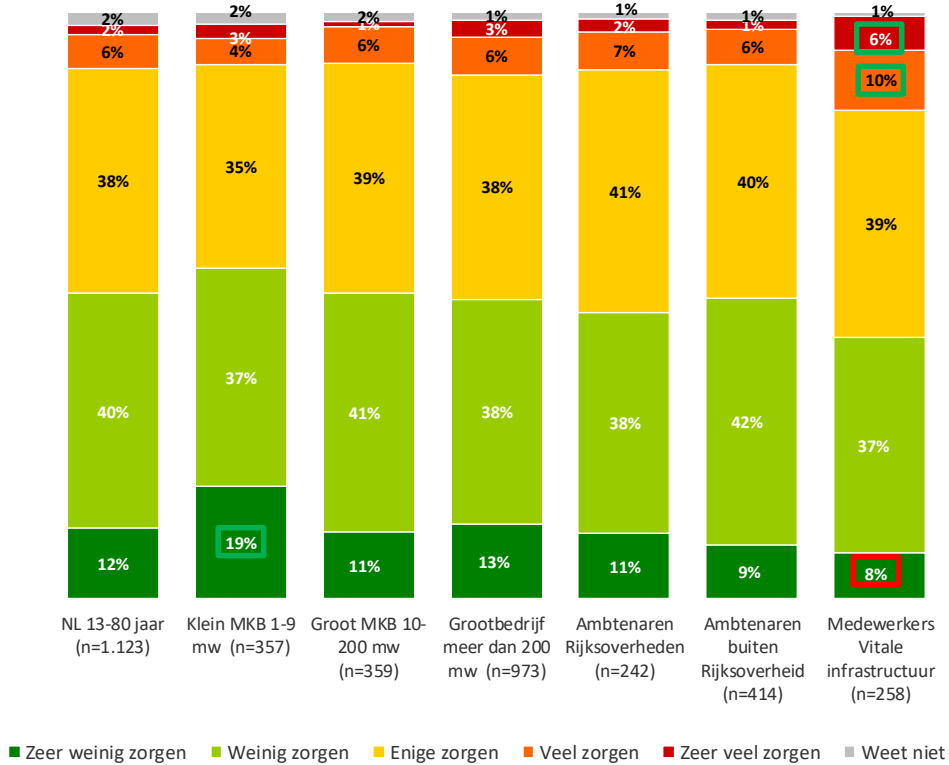
Helft van Nederlanders maakt zich weinig zorgen over digitale veiligheid thuis

- Ongeveer de helft van de Nederlanders (52%) maakt zich weinig zorgen over zijn of haar online veiligheid thuis. 38% maakt zich enige zorgen en 8% van de Nederlanders maakt zich veel of zeer veel zorgen.
- Medewerkers in de vitale infrastructuur maken zich meer zorgen om hun digitale veiligheid in de privésituatie dan andere groepen in de beroepsbevolking. 16% maakt zich (zeer) veel zorgen om hun digitale veiligheid in de privésituatie.

Verschillen binnen Nederlandse bevolking 13-80:

- Laagopgeleiden maken zich minder zorgen om hun digitale veiligheid thuis.
- Jongeren tussen de 13 en de 18 jaar maken zich minder zorgen om hun digitale veiligheid thuis. Ouderen van 65 en ouder maken zich juist meer zorgen om hun digitale veiligheid.

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

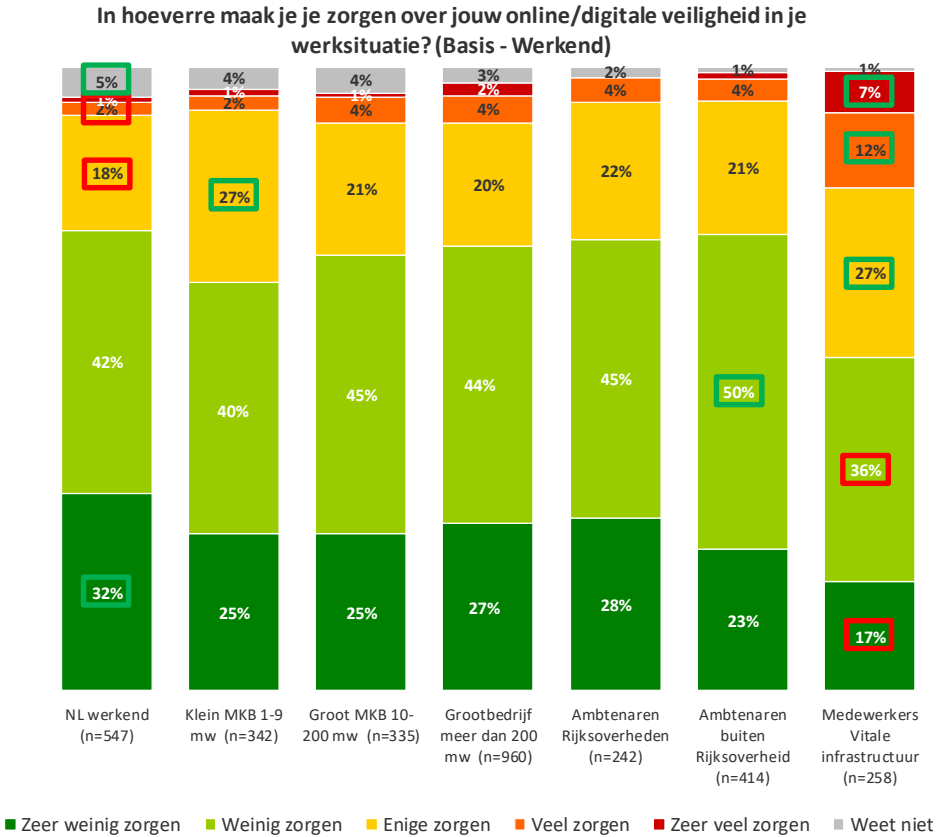


Weinig zorgen over digitale veiligheid in werksituatie

- Nederlanders maken zich minder zorgen over hun digitale veiligheid op het werk dan thuis. 21% van de werkende Nederlanders maakt zich zorgen over zijn of haar online veiligheid op het werk. 52% van alle Nederlanders maakt zich thuis zorgen. (zie vorige pagina).
- Medewerkers in de vitale infrastructuur maken zich meer zorgen over hun digitale veiligheid dan andere groepen in de beroepsbevolking. 19% maakt zich (zeer) veel zorgen en 27% enige zorgen versus 6% of minder bij de andere groepen.
- Ambtenaren (buiten de overheid) maken zich minder zorgen over cyberdreigingen op het werk.

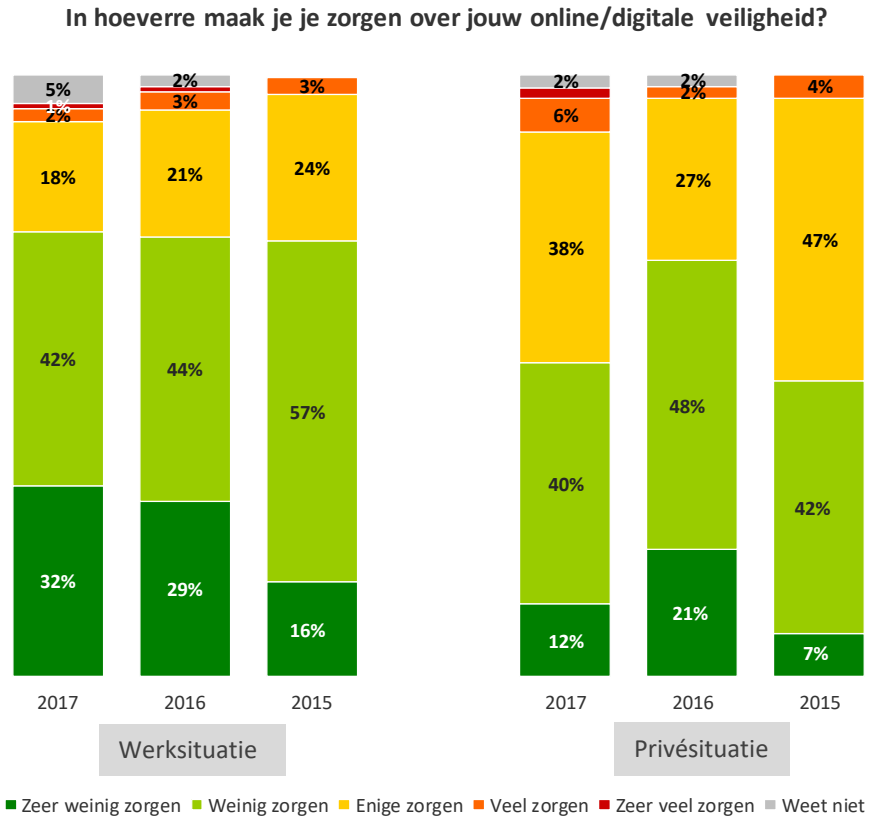
Verschillen binnen werkzame bevolking (13-80):

- Laagopgeleiden maken zich op het werk minder zorgen om hun digitale veiligheid dan midden- en hoogopgeleiden.



Mate van zorgen over veiligheid thuis weer terug op niveau van 2015

- In 2015 maakte 51% van alle Nederlanders zich zorgen over de online veiligheid thuis, in 2016 was dit gedaald tot 29%. In 2017 is dit weer gestegen naar 46% van de bevolking.
- De mate van zorgen over de veiligheid in de werksituatie laat een lichte dalende trend zien van 27% in 2015 naar 24% in 2026 en 21% in 2017. Hierbij moet worden opgemerkt dat het in 2015 nog niet mogelijk was om de vraag te beantwoorden met ‘weet niet’.



Phishing mails, identiteitsfraude en cyberaanval zijn bekendste cybergevaren

Wat *phishing mails* en *identiteitsfraude* inhouden is bekend bij 8 op de 10 Nederlanders. Het minst bekende gevaar is juice jacking (het verspreiden van malware of het stelen van data via een USB-oplaadpunt).

Werkende Nederlanders zijn vaker bekend met de verschillende online gevaren dan niet werkende Nederlanders.

Binnen de werkende bevolking zijn medewerkers in de vitale infrastructuur, rijksambtenaren en medewerkers van grote bedrijven vaker bekend met de verschillende online gevaren.

Kun je aangeven in welke mate je bekend bent met de onderstaande zaken? *% Ik weet wat dit is*	NL 13-80 jaar (n=1.123)	Klein MKB 1-9 mw (n=357)	Groot MKB 10-200 mw (n=359)	Grootbedrijf meer dan 200 mw (n=973)	Ambtenaren Rijksoverheden (n=242)	Ambtenaren buiten Rijksoverheid (n=414)	Medewerkers vitale infrastructuur (n=258)
Phishing mails	79%	86%	83%	86%	94%	89%	81%
Identiteitsfraude	79%	83%	81%	85%	90%	88%	83%
Cyberaanval	72%	77%	79%	80%	87%	80%	84%
Spyware	62%	69%	65%	71%	81%	71%	74%
Malware	57%	67%	59%	66%	75%	67%	70%
Datalek	50%	57%	59%	66%	74%	70%	69%
Ransomware	49%	58%	51%	60%	67%	60%	67%
DDoS-aanval	41%	47%	42%	53%	60%	47%	60%
Een keylogger	19%	21%	23%	29%	29%	27%	36%
Social engineering	13%	16%	14%	19%	17%	14%	33%
Spoofing	12%	13%	13%	16%	16%	11%	26%
Portscan	11%	13%	14%	18%	16%	12%	28%
Honeypot	6%	8%	11%	11%	12%	6%	22%
Juice jacking	4%	6%	8%	8%	3%	5%	19%

Bekendheid ransomware sterk toegenomen

Ten opzichte van de meting in 2016 is de bekendheid van ransomware sterk toegenomen. In 2016 had 53% van de bevolking hier nog nooit van gehoord. In 2017 heeft 18% er nog nooit van gehoord: 82% van de bevolking weet nu (ongeveer) wat dit inhoudt.

	% Nooit van gehoord (Nederlandse bevolking 13-80)	
	2017	2016
Phishing mails	6%	7%
Identiteitsfraude	3%	6%
Cyberaanval	3%	0%
Spyware	9%	-
Malware	14%	20%
Datalek	16%	20%
Ransomware	↓ 18%	53%
DDoS-aanval	28%	-
Een keylogger	56%	-
Social engineering	56%	60%
Spoofing	70%	-
Portscan	70%	-
Honeypot	80%	-
Juice jacking	82%	-
Botnets	-	63%

"-" optie is niet voorgelegd in het betreffende jaar

Kans op slachtofferschap wordt niet hoog ingeschat

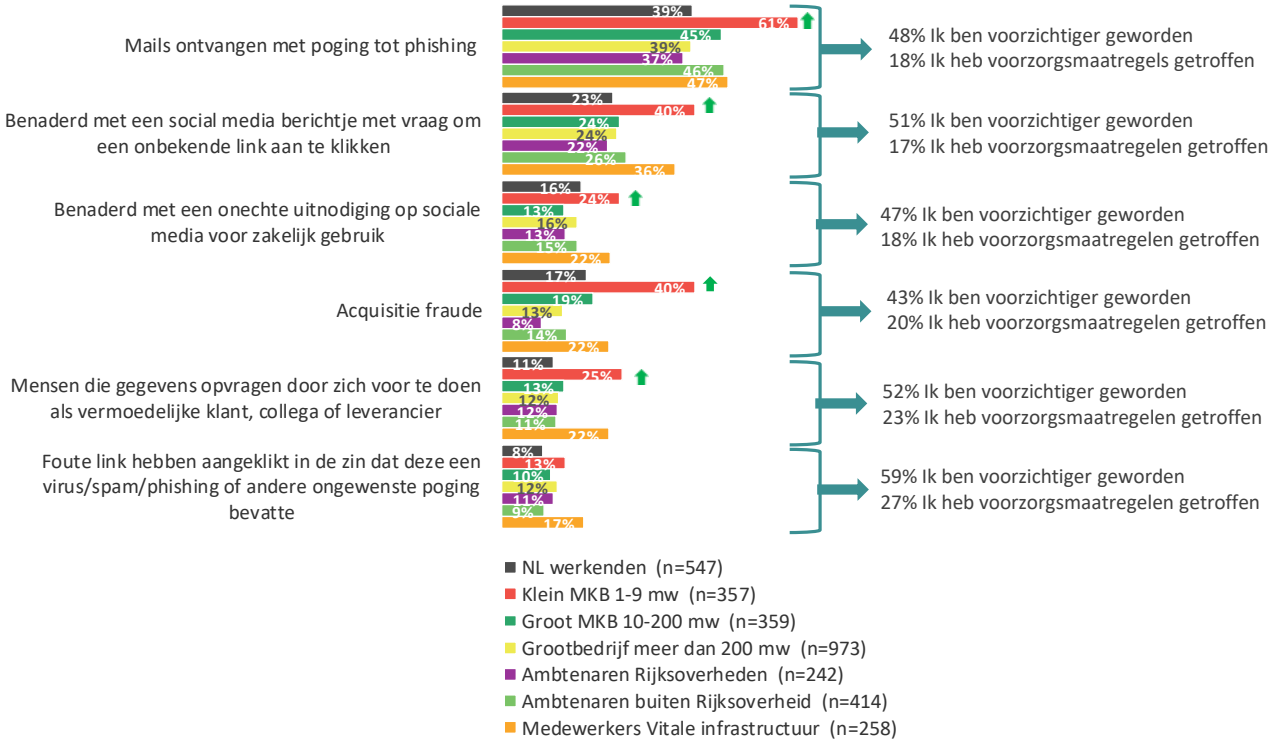
Hoe groot schat je de kans op (computer)schade *% (Zeer) groot*	NL 13-80 jaar		Klein MKB 1-9 mw		Groot MKB 10-200 mw		Grootbedrijf meer dan 200 mw		Ambtenaren Rijksoverheden		Ambtenaren buiten Rijksoverheid		Medewerkers vitale infrastructuur	
	Werk	Privé	Werk	Privé	Werk	Privé	Werk	Privé	Werk	Privé	Werk	Privé	Werk	Privé
Phishing mails	7%	12%	7%	6%	11%	15%	10%	13%	7%	11%	9%	14%	17%	22%
Identiteitsfraude	4%	5%	3%	4%	5%	7%	5%	6%	3%	5%	4%	5%	14%	15%
Cyberaanval	6%	5%	3%	3%	6%	7%	9%	6%	8%	4%	10%	6%	17%	14%
Spyware	6%	7%	3%	3%	8%	8%	6%	9%	4%	9%	5%	8%	16%	18%
Malware	5%	7%	2%	3%	6%	8%	6%	11%	5%	8%	4%	8%	4%	19%
Datalek	6%	5%	3%	4%	8%	7%	10%	6%	6%	3%	12%	4%	18%	15%
Ransomware	5%	6%	3%	3%	6%	8%	5%	8%	2%	5%	4%	6%	12%	17%
DDoS-aanval	5%	x	3%	x	6%	x	8%	x	9%	x	6%	x	17%	x
Een keylogger	3%	2%	3%	3%	5%	4%	5%	5%	0%	1%	1%	2%	15%	16%
Social engineering	4%	3%	2%	2%	5%	6%	7%	6%	3%	3%	2%	2%	14%	14%
Spoofing	2%	3%	2%	2%	3%	6%	6%	7%	1%	1%	1%	2%	16%	15%
Portscan	5%	x	2%	x	8%	x	7%	x	4%	x	2%	x	20%	x
Honeypot	1%	x	3%	x	4%	x	9%	x	6%	x	1%	x	16%	x
Juice jacking	6%	4%	4%	4%	6%	10%	10%	11%	0%	0%	1%	6%	18%	23%

De kans om slachtoffer te worden van cybercriminaliteit wordt over het algemeen niet hoog ingeschat: over geen enkel gevaar maakt meer dan 20% van de Nederlanders zich thuis of op het werk zorgen. De kans om thuis slachtoffer te worden wordt wel hoger ingeschat dan de kans om op het werk slachtoffer te worden. Medewerkers in de vitale infrastructuur schatten vrijwel alle risico's hoger in.

Veel ervaring als cyberslachtoffer, 1 op 5 neemt dan maatregelen

- 39% van de werkende Nederlanders heeft zelf wel eens een phishing mail ontvangen. De helft van deze personen is hierna voorzichtiger geworden en 18% trof voorzorgsmaatregelen.
- Medewerkers in het klein MKB (<9 medewerkers) hebben vaker te maken met phishing mails, mensen die zich voordoen als klant of leverancier en met acquisitiefraude.

Heb je <u>in een werksituatie</u> ooit weleens te maken gehad met één van de onderstaande voorvallen? (Werkend - % Ja, ikzelf)

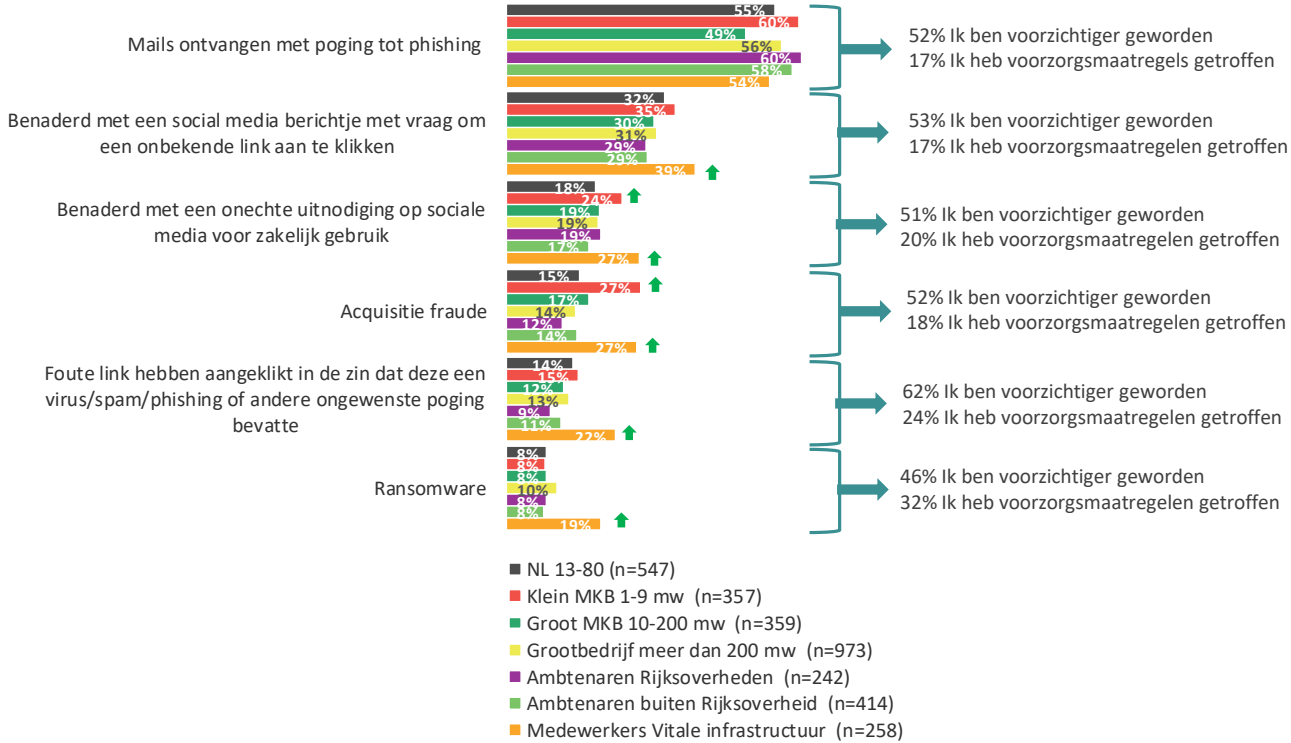


8% van de Nederlanders heeft privé te maken gehad met ransomware, helft is voorzichtiger geworden

- 55% van alle Nederlanders heeft thuis wel eens een phishing e-mail ontvangen. De helft van de personen die dit heeft meegemaakt is hierdoor voorzichtiger geworden, 17% heeft voorzorgsmaatregelen getroffen naar aanleiding van de ontvangen phishing mail.

- Medewerkers in de vitale infrastructuur schatten het risico om slachtoffer te worden van cybercrime hoger in dan andere beroepsgroepen (zie p. 12). Deze groep geeft ook vaker aan zelf slachtoffer te zijn geworden van verschillende cyberdreigingen of iemand te kennen die dit heeft meegemaakt.

Heb je <u>in een privésituatie</u> ooit weleens te maken gehad met één van de onderstaande voorvallen? (Allen - % Ja, ikzelf)



Hyperlinks en bijlage in e-mail ingeschat als grootste risico om slachtoffer te worden van cybercriminaliteit

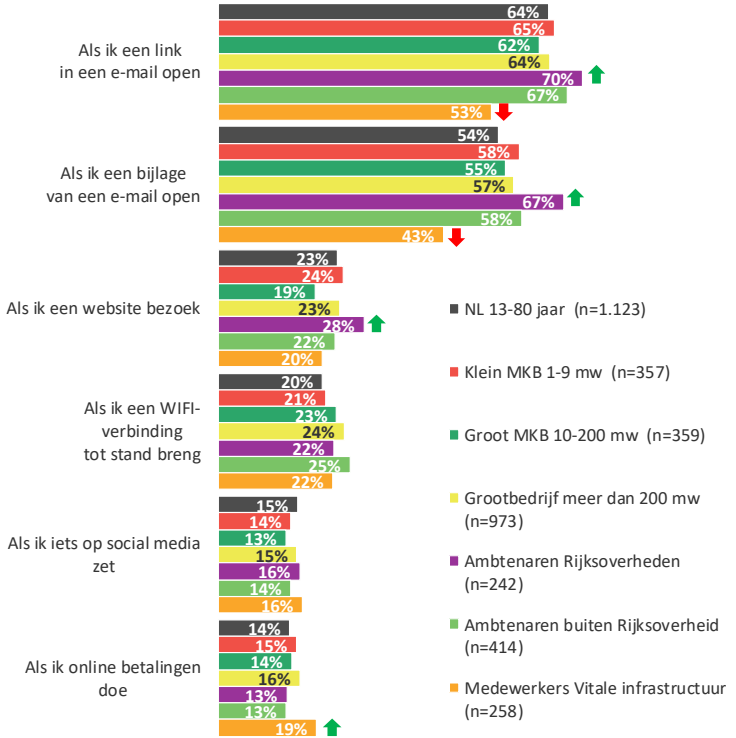
- Nederlanders denken dat je het grootste risico loopt om slachtoffer te worden van cybercriminaliteit als je een link in een e-mail aanklikt, of een bijlage van een e-mail opent.
- Rijksambtenaren schatten de risico's van een link of bijlage hoger in. Medewerkers in de vitale infrastructuur zijn juist minder bezorgd over e-mails en schatten bijvoorbeeld het gevaar bij online betalingen hoger in dan de andere groepen.

Verschillen binnen Nederlandse bevolking 13-80:

- Mannen denken vaker dan vrouwen je een risico loopt bij het openen van een bijlage bij een e-mail (55% vs. 48%). Vrouwen juist bij een link in e-mail (65% vs. 58%) of als ze iets op social media zetten (18% vs. 11%).
- Ouderen (65+) denken vaker dat het risico het grootst is bij het openen van een bijlage in de mail in vergelijking met de andere leeftijdsgroepen. Jongeren (13 t/m 18) als ze een website bezoeken. En jongvolwassenen (19 t/m 24) als ze een wifi-verbinding tot stand brengen.
- Laagopgeleiden denken minder vaak dat het risico groot is bij een link of een bijlage in de mail dan midden of hoogopgeleiden. Hoogopgeleiden denken vaker dat het grootste risico zich voordoet bij het tot stand brengen van een wifi-verbinding.

Grafiek gaat door op volgende pagina.

Wanneer denk je dat je de grootste risico's loopt om slachtoffer te worden van cybercriminaliteit? (Maximaal 3 antwoorden mogelijk)

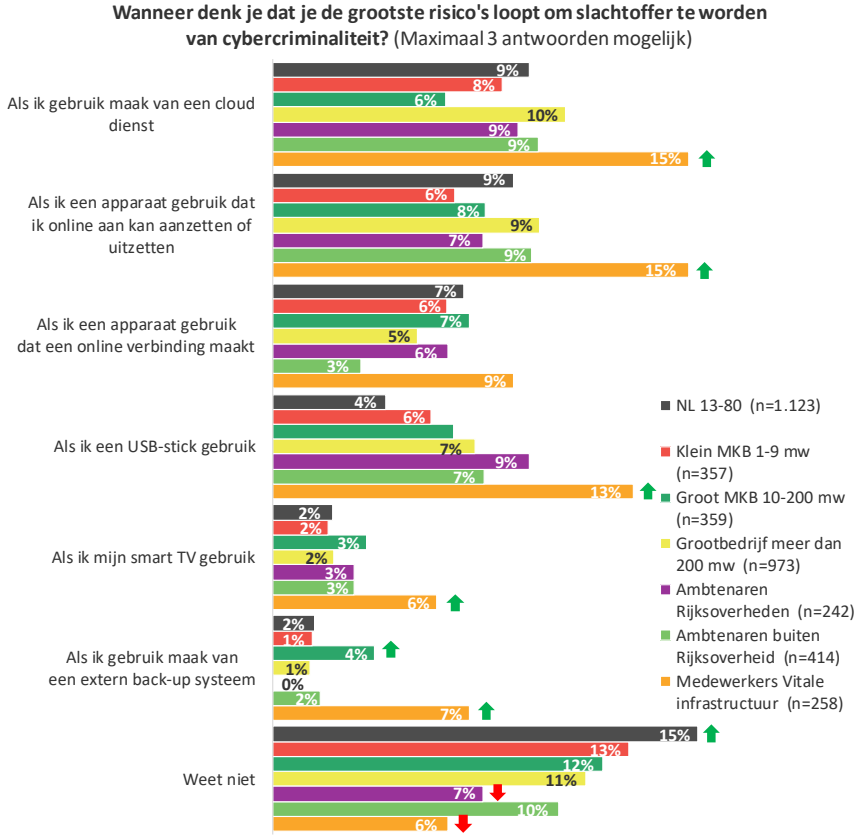


Medewerkers vitale infrastructuur schatten risico's hoger in dan andere doelgroepen

- Medewerkers in de vitale infrastructuur denken vaker dat er een risico is om slachtoffer te worden van cybercrime bij het gebruikmaken van een clouddienst (15%), een apparaat dat online aangezet of uitgezet kan worden (15%), bij gebruik van een USB-stick (13%), bij gebruik van Smart TV (6%) en als gebruikgemaakt wordt van een extern back-up-systeem (7%) dan de andere doelgroepen.
- Ambtenaren buiten de Rijksoverheid denken vaker dat je risico loopt op cybercriminaliteit bij het gebruikmaken van een extern back-up-systeem (4%) dan andere doelgroepen.
- Het Nederlandse publiek geeft vaker aan niet te weten (15%) wanneer men het grootste risico loopt om slachtoffer te worden van cybercriminaliteit.

Verschillen binnen Nederlandse bevolking 13-80:

- Vrouwen denken vaker dan mannen dat je risico loopt als je gebruik maakt van clouddiensten.
- Laagopgeleiden geven vaker aan niet te weten wanneer je het grootste risico loopt om slachtoffer te worden van cybercriminaliteit.



Nederlander denkt goede cybersecurity-vaardigheden te hebben

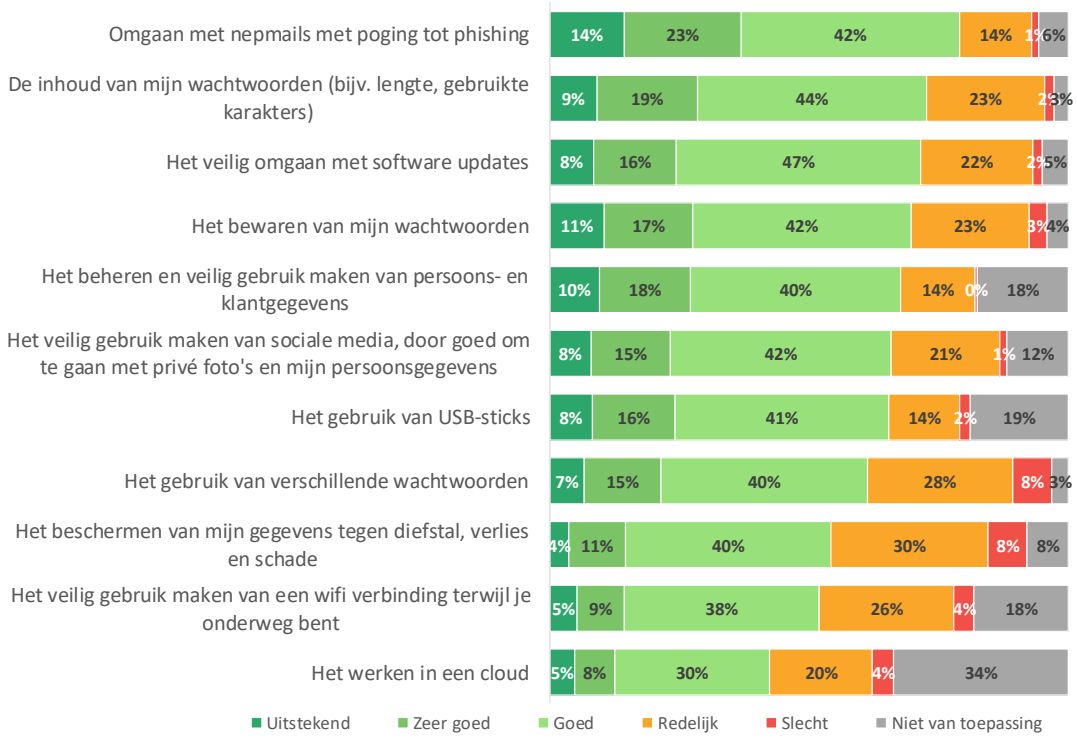
Bij ieder van de voorgelegde onderwerpen geeft meer dan de helft van de Nederlanders aan goed, zeer goed of uitstekend te handelen.

- Medewerkers in de vitale infrastructuur denken vaker goed om te gaan met het bewaren van wachtwoorden, voldoende verschillende wachtwoorden te gebruiken en dat hun wachtwoorden inhoudelijk goed zijn.
- Medewerkers in de vitale infrastructuur schatten ook vaker dan andere groepen in dat zij op een goede manier omgaan met wifi-netwerken onderweg, het beschermen van gegevens tegen diefstal, het werken in een cloud, het veilig omgaan met software updates en op een veilige manier omgaan met USB-sticks.

Verschillen binnen Nederlandse bevolking 13-80:

- Mannen schatten op alle onderwerpen hun gedrag beter in dan vrouwen, met uitzondering van het veilig gebruikmaken van social media.
- Er zijn geen verschillen naar opleidingsniveau. Laagopgeleiden schatten hun gedrag even veilig in als middenopgeleiden en hoogopgeleiden.

In hoeverre denk je dat je op een veilige wijze omgaat met de volgende zaken?
(NL 13-18, n=1123)



Maatregelen ter preventie

Werkzame bevolking (behalve MKB) is vaker bekend met preventiemaatregelen dan totale bevolking

- De meeste groepen werkende Nederlanders zijn meer op de hoogte van de preventiemaatregelen die zijn voorgelegd dan de gemiddelde Nederlander. Uitzondering hierop zijn medewerkers in het klein MKB. Vooral medewerkers van bedrijven met minder dan 10 medewerkers hebben minder kennis van preventiemogelijkheden. Zo heeft 36% van de medewerkers in het klein MKB nog nooit van een VPN-verbinding gehoord.

Kun je aangeven in welke mate je bekend bent met de onderstaande zaken? *% Wel eens van gehoord /weet wat het is/ gebruik ik*	NL 13-80 (n=1.123)	Klein MKB 1-9 mw (n=357)	Groot MKB 10-200 mw (n=359)	Grootbedrijf meer dan 200 mw (n=973)	Ambtenaren Rijksoverheden (n=242)	Ambtenaren buiten Rijksoverheid (n=414)	Medewerkers vitale infrastructuur (n=258)
Virusscanner	98%	98%	99%	98%	100%	99%	98%
Automatische updates	96%	96%	97%	98%	98%	98%	99%
Instellingen om cookies te blokkeren/uit te zetten	93%	93%	92%	95%	97%	96%	97%
Cloud diensten	87%	93%	93%	95%	97%	97%	98%
Biometrische online bescherming	81%	86%	87%	87%	92%	89%	91%
Spyware scanner	80%	83%	87%	85%	88%	86%	93%
Digitaal wachtwoordenkluisje/ wachtwoordmanager	76%	78%	84%	82%	86%	88%	88%
Tweestapsverificatie	73%	79%	84%	84%	87%	87%	92%
Ad-blocker	72%	75%	81%	80%	83%	82%	91%
Vpn-verbindingen	60%	64%	77%	76%	79%	79%	90%
Web tracking blocker	52%	55%	60%	62%	64%	61%	76%

Bekendheid tweestapsverificatie is toegenomen

- In vergelijking met 2016 is de bekendheid van tweestapsverificatie toegenomen. Vorig jaar had 41% van de Nederlanders hier nog nooit van gehoord, dit jaar is dat nog 27%. De bekendheid van de andere maatregelen is grotendeels ongewijzigd.

NB: De optie *Ad-blocker* was in 2016 omschreven als: “instellingen om online advertenties te blokkeren/uit te zetten”. Dit verklaart mogelijk de afname van de bekendheid hiervan.

	% Nooit van gehoord (Nederlandse bevolking 13-80)	
	2017	2016
Virusscanner	2%	2%
Automatische updates	4%	3%
Instellingen om cookies te blokkeren/uit te zetten	7%	8%
Cloud diensten	13%	-
Biometrische online bescherming *	19%	16%
Spyware scanner	20%	-
Digitaal wachtwoordenkluisje/ wachtwoordmanager *	24%	27%
Tweestapsverificatie	↓ 27%	41%
Ad-blocker *	↑ 28%	12%
Vpn-verbindingen	40%	39%
Web tracking blocker	48%	-

* Optie is vorig jaar in andere bewoording/ met een andere toelichting voorgelegd

- is niet voorgelegd

Virusscanner en automatische updates meest gebruikte preventie-maatregelen

- 86% van alle Nederlanders gebruikt een virusscanner en 76% maakt gebruik van automatische updates.
- Medewerkers in de vitale infrastructuur maken minder vaak gebruik van virusscanners maar gebruiken daarentegen wel vaker: spywarescanners, clouddiensten, ad-blockers, VPN-verbindingen, wachtwoordmanagers, biometische bescherming en web tracking blockers.

Kun je aangeven in welke mate je bekend bent met de onderstaande zaken? *% gebruik ik*	NL 13-80 (n=1.123)	Klein MKB 1-9 mw (n=357)	Groot MKB 10-200 mw (n=359)	Grootbedrijf meer dan 200 mw (n=973)	Ambtenaren Rijksoverheden (n=242)	Ambtenaren buiten Rijksoverheid (n=414)	Medewerkers vitale infrastructuur (n=258)
Virusscanner	86%	89%	86%	87%	93%	87%	81%
Automatische updates	76%	78%	74%	82%	85%	84%	75%
Instellingen om cookies te blokkeren/uit te zetten	44%	51%	43%	52%	52%	51%	52%
Tweestapsverificatie	41%	42%	47%	53%	52%	55%	52%
Spyware scanner	40%	46%	43%	46%	48%	45%	53%
Cloud diensten	40%	46%	44%	46%	43%	52%	51%
Ad-blocker	34%	38%	30%	37%	36%	33%	41%
VPN-verbindingen	17%	19%	31%	31%	30%	31%	44%
Digitaal wachtwoordenkluisje/ wachtwoordmanager	17%	21%	22%	21%	20%	22%	34%
Biometrische online bescherming	13%	12%	15%	21%	23%	21%	29%
Web tracking blocker	13%	11%	14%	15%	11%	13%	26%

Bijna de helft van de werkenden maakt nooit gebruik van een VPN-verbinding voor internetverkeer

- Bijna de helft (45%) van de werkenden maakt nooit gebruik van een VPN-verbinding waarmee ze hun internetverkeer versleuteld versturen. 26% doet dit soms en 29% doet dit regelmatig of altijd.
- Een op de vijf werkenden maakt altijd gebruik van automatisch verbinding maken met wifi-netwerken.
- 70% van alle werkenden gebuikt zijn smartphone wel eens als hotspot.

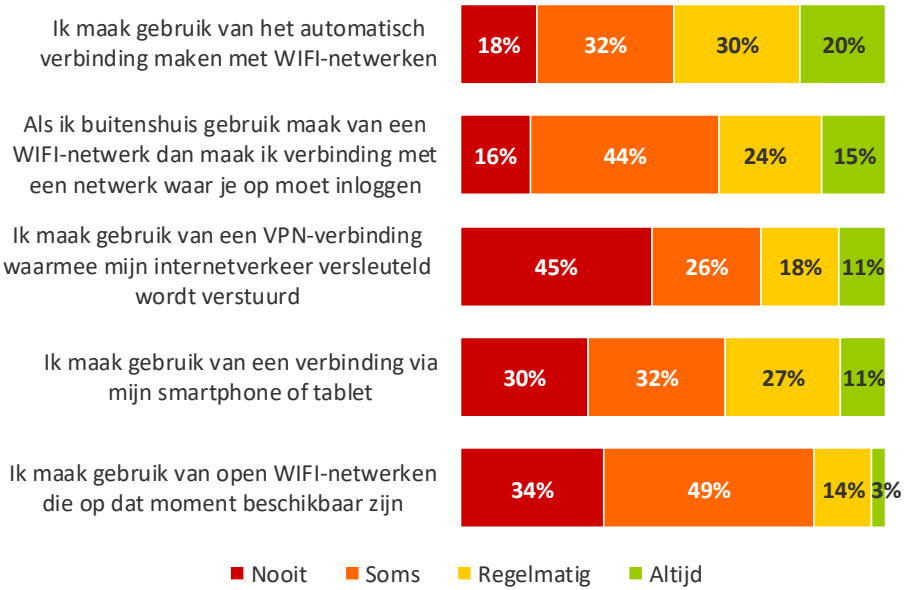
- Medewerkers in de vitale infrastructuur maken vaker gebruik van een VPN-verbinding dan de andere doelgroepen.
- Medewerkers in de vitale infrastructuur maken vaker gebruik van open wifi-netwerken dan de andere doelgroepen.

Verschillen binnen Nederlandse bevolking 13-80:

- Vrouwen maken minder vaak gebruik van een VPN-verbinding dan mannen.

Hieronder staat een aantal stellingen die gaan over het gebruik maken van een wifi-verbinding terwijl je onderweg of op locatie aan het werk bent.

In hoeverre is iedere stelling van toepassing is op jouw gedrag? (Basis - Werkenden)



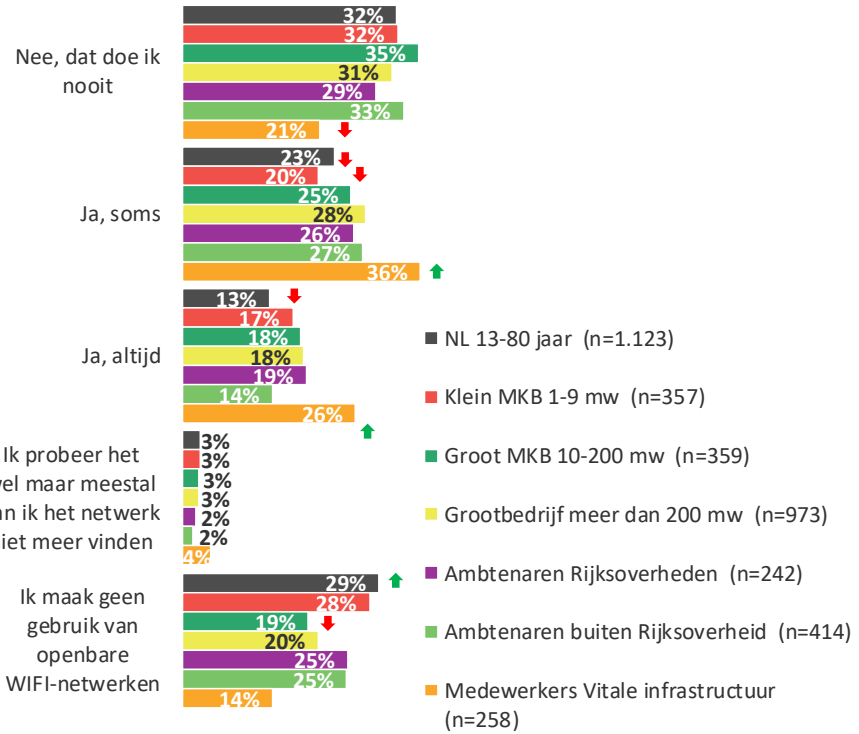
Een derde verwijdert nooit een openbaar wifi-netwerk na gebruik

- Ongeveer een derde van alle Nederlanders maakt geen gebruik van openbare wifi-netwerken (29%).
- 32% van alle Nederlanders gebruikt openbare wifi-netwerken en verwijdert deze netwerken na gebruik nooit.
- Medewerkers in de vitale infrastructuren verwijderen openbare wifi-netwerken vaker uit hun lijst van netwerken dan de andere groepen werkenden.

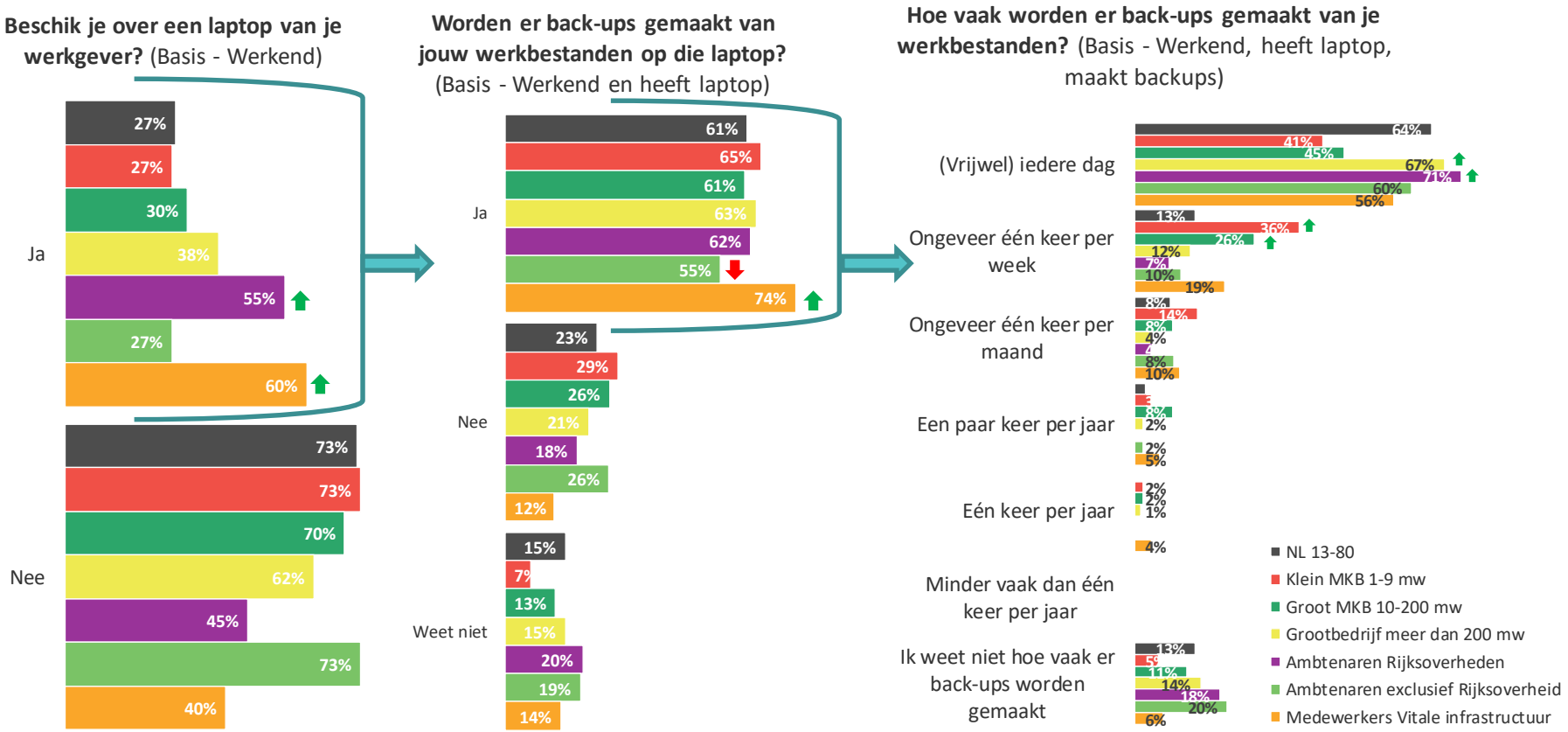
Verschillen binnen Nederlandse bevolking 13-80:

- Vrouwen geven vaker aan nooit openbare wifi-netwerken te verwijderen na gebruik.
- 55- t/m 80-jarigen geven *vaker* aan geen gebruik te maken van openbare wifi-netwerken. 13- t/m 24-jarigen geven vaker aan nooit openbare wifi-netwerken te verwijderen na gebruik

Als je gebruik hebt gemaakt van een openbaar WIFI-netwerk (zonder een wachtwoord en zonder in te loggen) verwijder je dan dat netwerk direct na gebruik uit de lijst met WIFI-netwerken?



Meeste werklaptops maken back-ups (meestal dagelijks)



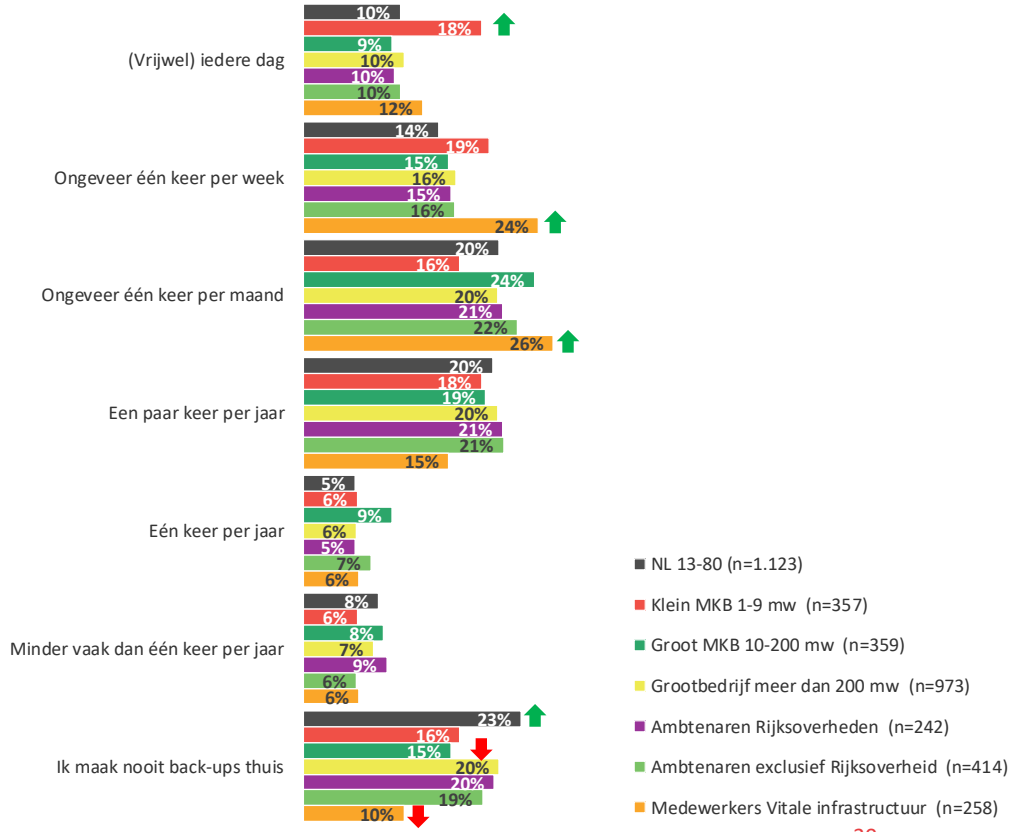
Driekwart van alle Nederlanders maakt wel eens back-ups thuis

- 77% van alle Nederlanders maakt wel eens back-ups van computerbestanden thuis. Meestal gebeurt dit één keer per maand (20%) of een paar keer per jaar (20%). 23% van alle Nederlanders maakt nooit back-ups.
- Medewerkers in de vitale infrastructuur maken thuis vaker back-ups dan andere groepen werkenden.
- Medewerkers in het klein MKB (inclusief ZZP'ers) maken vaker dan andere groepen in de beroepsbevolking dagelijks back-ups van hun privébestanden.

Verschillen binnen Nederlandse bevolking 13-80:

- 36% van de laagopgeleiden maakt thuis nooit back-ups (landelijk 23%).
- Mannen maken vaker back-ups dan vrouwen en jongeren tot 25 jaar maken vaker back-ups dan oudere doelgroepen.

Hoe vaak maak je thuis back-ups van computerbestanden?



Motieven achter gedrag

Zes op de tien Nederlanders zou nooit betalen bij ransomware

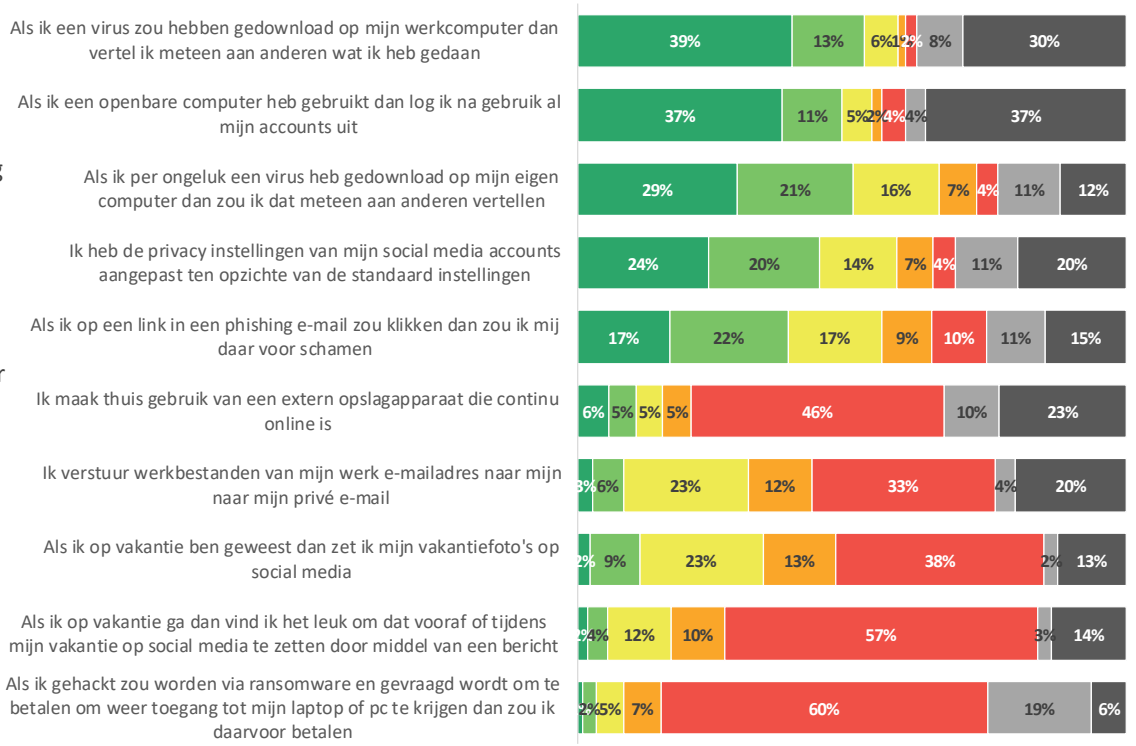
- De meeste Nederlanders zouden er met anderen over praten als zij een virus hebben gedownload op hun eigen computer of op hun werkcomputer.
- 39% van de Nederlanders zou zich vrijwel zeker schamen (altijd/meestal) indien zij een link in een phishing mail aan zouden klikken.
- 60% van de Nederlanders zou nooit betalen indien zij gehackt zou worden met ransomware, 8% overweegt wel een betaling (soms/meestal/altijd) en 20% weet het niet.

- Medewerkers in de vitale infrastructuur overwegen vaker om te betalen in het geval van ransomware (31% i.p.v. 8% onder alle Nederlanders), loggen vaker uit op openbare computers (70% i.p.v. 54%), versturen vaker e-mails vanaf een werk- naar een privéadres en hebben thuis vaker een externe opslag die continu online is.
- Ambtenaren sturen minder vaak e-mails van hun werkadres naar hun privéadres.

Verschillen binnen Nederlandse bevolking 13-80:

- Vrouwen zouden het vaker tegen iemand zeggen als zij een virus hebben gedownload.
- Laagopgeleiden sturen minder vaak e-mails van een werkadres naar een privéadres.

In hoeverre zijn de volgende uitspraken van toepassing op jouw gedrag?
(NL 13-18, n=1123)



Ingewikkelde instructies belangrijkste reden voor ontbreken bescherming

- Een op de drie Nederlanders vindt de instructies om je te beschermen tegen online gevaren vaak ingewikkeld.
- Medewerkers in de vitale infrastructuur ervaren veiligheidsmaatregelen vaker als een belemmering. 29% van de medewerkers in de vitale infrastructuur geeft aan weleens veiligheidsmaatregelen te omzeilen om moeite of tijd te besparen.

Kun je aangeven in hoeverre je het eens bent met de volgende stellingen? *% (Helemaal) mee eens*	NL Rep (n=1.123)	Klein MKB 1-9 mw (n=357)	Groot MKB 10-200 mw (n=359)	Grootbedrijf meer dan 200 mw (n=973)	Ambtenaren Rijksoverheden (n=242)	Ambtenaren buiten Rijksoverheid (n=414)	Medewerkers vitale infrastructuur (n=258)
Ik vind de instructies om je te beschermen tegen digitale/online gevaren vaak ingewikkeld	33%	27%	26%	28%	25%	26%	34%
Ik zie het inloggen via een tweestapsverificatie als een te grote belemmering	21%	21%	19%	19%	15%	19%	**26%**
Ik zie het niet automatisch kunnen opslaan van wachtwoorden op websites en in systemen als een te grote belemmering	17%	15%	18%	16%	17%	14%	**24%**
Ik zie het automatisch uitloggen wanneer je even niet actief bent geweest op een website of systeem als een te grote belemmering	**15%**	17%	19%	18%	20%	16%	**25%**
Ik omzeil weleens veiligheidsmaatregelen om moeite en/of tijd te besparen	13%	13%	18%	16%	11%	14%	**29%**

Helft Nederlanders herkent zichzelf in de omschrijving van een digi-regular

- Ongeveer de helft van de Nederlanders herkent zichzelf het meest in de omschrijving van de digi-regular, 16% ziet zichzelf als digibeet.
- Ambtenaren buiten de Rijksoverheid herkennen zich vaker in het type digi-regular dan de andere doelgroepen.
- Medewerkers vitale infrastructuur noemen zichzelf vaker een cyberpro dan de andere doelgroepen.

Verschillen binnen Nederlandse bevolking 13-80:

- Mannen herkennen zichzelf vaker in het type cyberpro en digi-regular dan vrouwen. Vrouwen herkennen zichzelf vaker in het type digi-flextarier en digibeet.
- 13- t/m 18-jarigen zien zichzelf vaker als cyberpro dan andere leeftijdsgroepen. 55- t/m 80-jarigen zien zichzelf vaker als digibeet.
- Hoogopgeleiden herkennen zichzelf vaker in het type digi-flextarier en digi-regular. Laagopgeleiden herkennen zichzelf vaker in het type digibeet of geen van de vier typen.

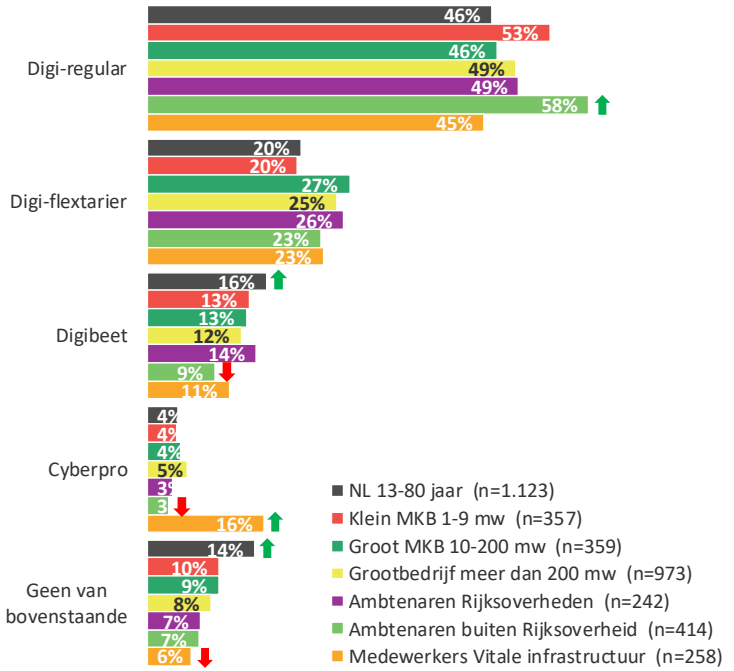
"Ik heb vaste routines. Ik maak af en toe back-ups van mijn bestanden en ik heb anti-virus software op mijn computer. Als er een software update voor mijn computer is dan installeer ik die."

"ik doe in elke situatie iets anders. Ik let meestal goed op welke persoonsgegevens ik deel op internet, maar ik gebruik ook weleens een open wifi-verbinding in een café. Ik luister graag naar de adviezen van anderen op cybergebied."

"Ik weet eigenlijk heel weinig van computers en het internet. Ik weet ook niet wat ik zou moeten doen om mijn computers en bestanden beter te beveiligen."

"Ik weet alles van cybersecurity en ik heb mijzelf optimaal beschermt. Ik geef anderen graag advies over online veiligheid en help hen hier actief mee."

In welk type online gedrag herken jij jezelf het meest?



Digitale veiligheid op het werk

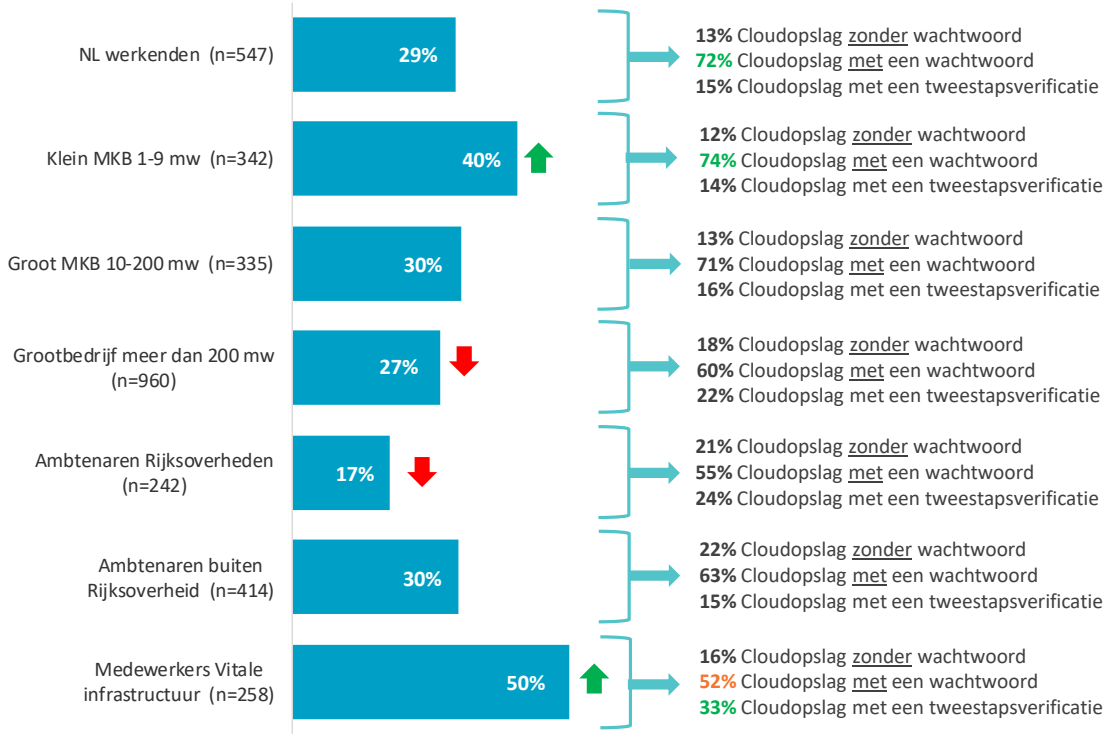
Minderheid van werkende Nederlanders gebruikt een cloud

- 29% van alle werkende Nederlanders gebruikt een cloud.
- Bij de medewerkers in de vitale infrastructuur en in het klein MKB wordt vaker gewerkt met een cloud. Rijksambtenaren gebruiken het minst vaak een cloud voor werkdoeleinden.

Verschillen binnen Nederlandse bevolking 13-80:

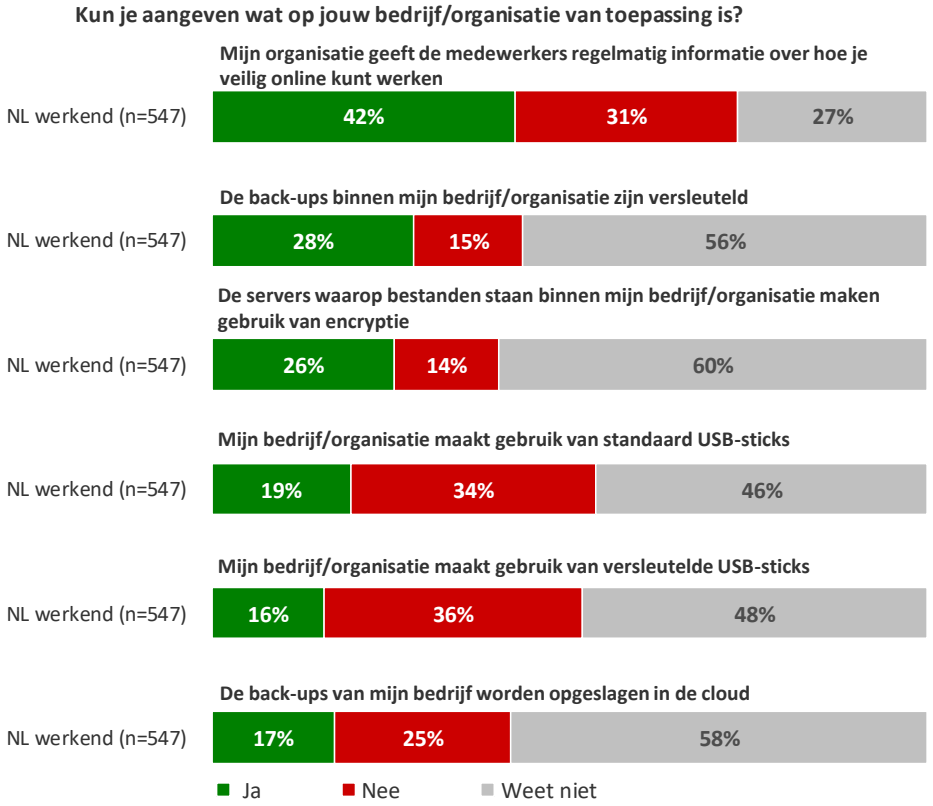
- Mannen maken vaker gebruik van cloudopslag dan vrouwen.
- Hoogopgeleiden maken vaker gebruik van cloudopslag dan midden- en laagopgeleiden.
- Laagopgeleiden die een cloudopslag gebruiken, maken minder vaak gebruik van cloudopslag met een wachtwoord.

Maak je voor jouw werk gebruik van een cloudopslag? % Ja



Ongeveer de helft van de werkenden krijgt van werkgever informatie over hoe veilig online te werken

- 42% van de werkzame bevolking geeft aan dat zij regelmatig informatie krijgen van hun organisatie over hoe je veilig online kunt werken.
- Veel medewerkers weten niet wat er gebeurt binnen hun organisatie met back-ups en hoe bestanden opgeslagen zijn. 60% van de werkende Nederlanders weet niet of servers waar bestanden op staan gebruikmaken van encryptie of niet.



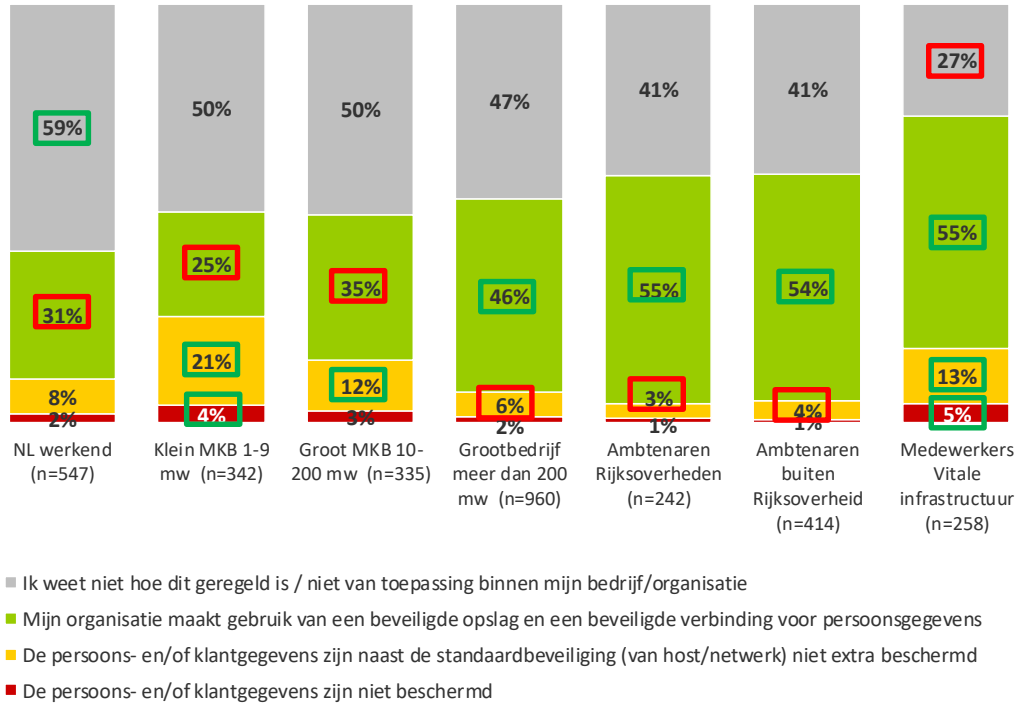
Meeste werkenden weten niet hoe persoons- en/of klantgegevens beschermd zijn binnen bedrijf/organisatie

- 59% van alle werkenden weet niet hoe de persoons- en/of klantgegevens beschermd zijn bij de werkgever. Van de personen die wel weten hoe er wordt omgegaan met persoonsgegevens en klantgegevens weten de meesten dat er gebruik wordt gemaakt van beveiligde verbindingen en van een beveiligde opslag.
- Medewerkers in de vitale infrastructuur zijn het vaakst op de hoogte van de beveiliging van gegevens bij hun werkgever.

Verschillen binnen Nederlandse bevolking 13-80:

- Vrouwen geven vaker aan dat ze niet weten of persoonsgegevens beschermd worden binnen hun organisatie/bedrijf dan mannen.
- Laagopgeleiden geven vaker aan dat ze dit niet weten of dat het niet van toepassing is op hun bedrijf.

Kun je aangeven welke stelling het meest op jouw bedrijf/organisatie van toepassing is? (Basis - Werkend)



Cyberaanvallen

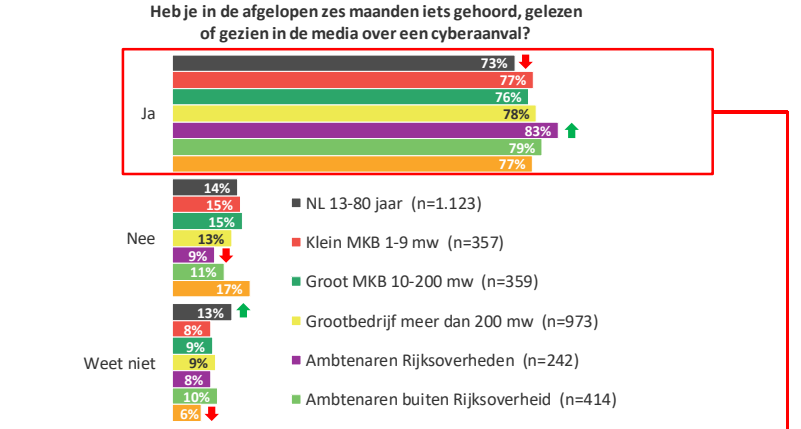
Als reactie op het nieuws over cyberaanvallen zijn mensen vooral voorzichtiger geworden

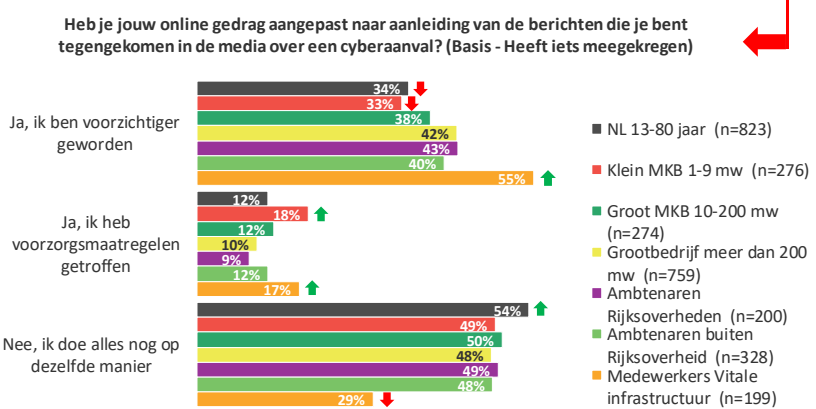
- 73% van alle Nederlanders heeft in de afgelopen zes maanden iets gehoord, gezien of gelezen over een cyberaanval.
- Ambtenaren van de Rijksoverheid hebben vaker iets gezien, gelezen of gehoord in de media over een cyberaanval (83%) dan de andere doelgroepen.

- Medewerkers in de vitale infrastructuur geven vaker aan dat ze voorzichter zijn geworden als reactie op nieuws in de media (55%) en dat ze vaker voorzorgsmaatregelen hebben getroffen (17%). Ook medewerkers in het klein MKB (1-9 medewerkers) geven vaker aan dat ze voorzorgmaatregelen hebben genomen (18%).

Verschillen binnen Nederlandse bevolking 13-80:

- Mannen geven vaker aan nieuws over cyberaanvallen te hebben vernomen dan vrouwen.
- Hoogopgeleiden geven vaker aan iets gezien te hebben over cyberaanvallen in de media dan midden- en laagopgeleiden. Laagopgeleiden die iets gezien hebben over cyberaanvallen geven wel vaker aan voorzorgsmaatregelen te hebben getroffen.





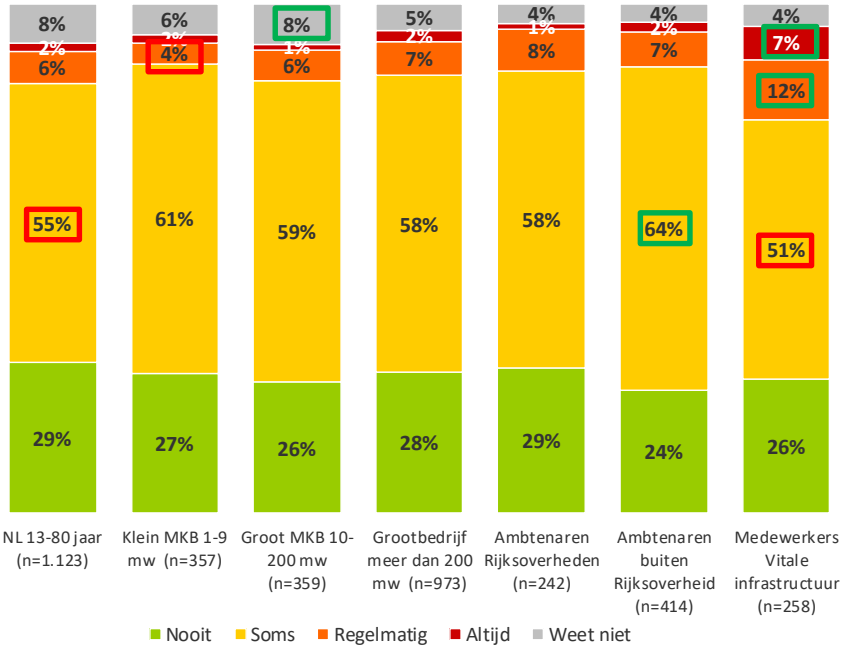
Kwart van de Nederlanders maakt zich nooit zorgen dat ze zelf te maken krijgen met een cyberaanval

- Twee van de drie Nederlanders (63%) maakt zich wel eens zorgen dat hij/zij zelf te maken krijgt met een cyberaanval.
- Medewerkers in de vitale infrastructuur geven vaker aan dat ze regelmatig (12%) of altijd (7%) bezorgd zijn voor een cyberaanval.

Verschillen binnen Nederlandse bevolking 13-80:

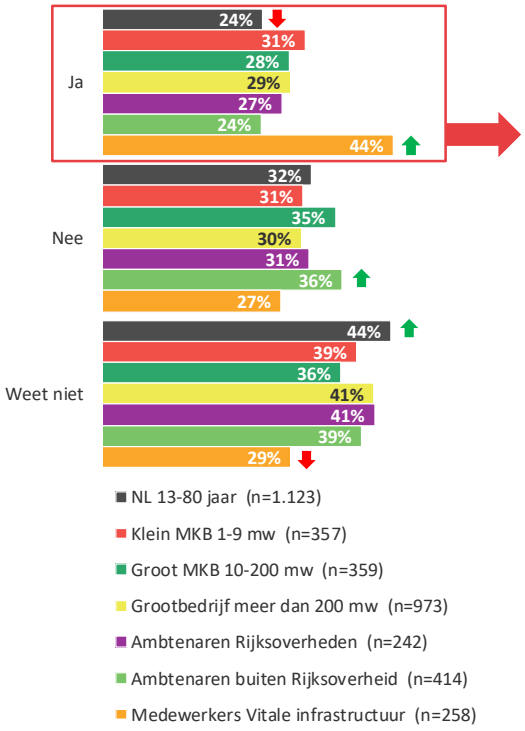
- Mannen geven vaker aan zich nooit zorgen te maken dat ze zelf te maken krijgen met een cyberaanval.
- 19- t/m 34-jarigen geven vaker aan zich nooit zorgen te maken dat ze zelf te maken krijgen met een cyberaanval.

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



Een derde van de Nederlanders is thuis niet voorbereid op een cyberaanval

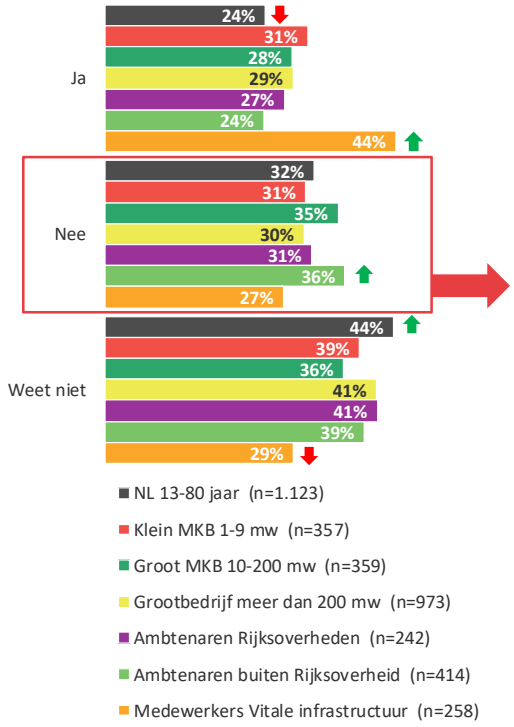
Ben je thuis voorbereid op een cyberaanval?



Op welke manier ben je thuis voorbereid op een cyberaanval? *% genoemd*	NL 13-80 jaar	Klein MKB 1-9 mw	Groot MKB 10-200 mw	Grootbedrijf meer dan 200 mw	Ambtenaren Rijks-overheden	Ambtenaren buiten Rijksoverheid	Medewerkers vitale infrastructuur
Ik heb thuis antivirussoftware geïnstalleerd	94%	72%	83%	69%	75%	83%	90%
Ik klik nooit op een link in een e-mail die ik niet vertrouw	85%	76%	73%	71%	75%	81%	78%
Ik voer automatische software beveiligingsupdates direct uit zonder ze uit te stellen	79%	68%	79%	55%	72%	71%	63%
Ik heb een firewall thuis	59%	55%	61%	63%	61%	73%	68%
Ik maak back-ups van mijn bestanden op mijn laptop	85%	75%	73%	45%	49%	48%	45%
Ik maak back-ups van mijn smartphone	61%	59%	46%	42%	39%	34%	21%
Ik verstuur nooit werk gerelateerde bestanden van mijn werk naar huis	27%	29%	35%	28%	25%	53%	33%
Ik maak back-ups van mijn tablet	43%	56%	28%	19%	31%	20%	24%
Anders, namelijk:	0%	6%	3%	4%	10%	8%	9%
Geen van bovenstaande	0%	0%	0%	5%	4%	2%	0%

Nederlanders weten vaak niet hoe ze zich moeten voorbereiden op een cyberaanval en schatten de kans op een aanval laag in

Ben je thuis voorbereid op een cyberaanval?

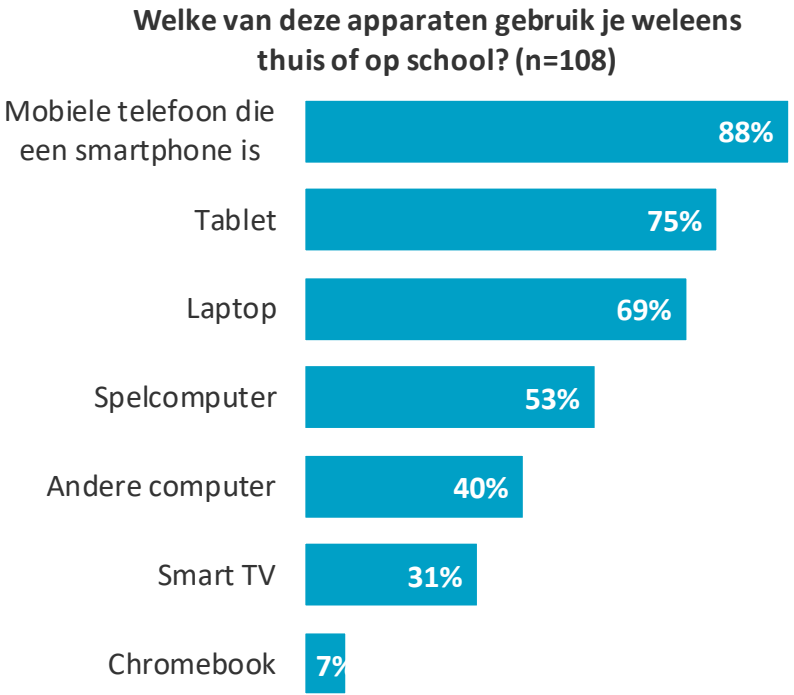


Wat is de belangrijkste reden dat je niet bent voorbereid op een cyberaanval? *% genoemd*	NL 13-80 jaar	Klein MKB 1-9 mw	Groot MKB 10-200 mw	Grootbedrijf meer dan 200 mw	Ambtenaren Rijksoverheden	Ambtenaren buiten Rijksoverheid	Medewerkers vitale infrastructuur
Ik weet niet hoe ik dat moet doen	38%	38%	39%	38%	38%	38%	23%
De kans is klein dat mij dit overkomt	32%	34%	31%	33%	34%	27%	30%
Daar heb ik nog nooit over nagedacht	26%	17%	27%	27%	21%	28%	17%
Je kan het toch niet voorkomen, hackers vinden altijd wel een manier	25%	27%	25%	24%	30%	22%	23%
Ik vind computerzaken ingewikkeld	21%	25%	11%	21%	18%	18%	19%
Ik heb geen zin om me hier in te verdiepen	17%	15%	18%	18%	21%	15%	16%
Ik heb geen tijd om mij hier mee bezig te houden	10%	8%	12%	9%	7%	7%	14%
Op mijn leeftijd is het lastig om de nieuwste ontwikkelingen op computergebied bij te houden	16%	14%	8%	6%	8%	7%	7%
Ik vind dit niet interessant	5%	10%	8%	6%	1%	4%	4%
Veiligheidsmaatregelen maken mijn computer/laptop/ tablet/telefoon traag	4%	1%	2%	7%	4%	5%	9%
Weet niet	4%	2%	6%	6%	8%	7%	3%
Geen van bovenstaande	4%	3%	2%	2%	1%	3%	0%

Kinderen

Smartphone meest gebruikte apparaat thuis of op school

- Kinderen gebruiken thuis of op school vaak een smartphones. 88% van de kinderen tussen de 11 en 12 jaar gebruikt weleens een smartphone.
- Tablets en laptops zijn ook populaire apparaten in groep 7 en 8. Driekwart van de kinderen geeft aan thuis of op school gebruik te maken van een tablet en ongeveer zeven op de tien gebruiken een laptop (69%).
- De helft van de kinderen (53%) gebruikt thuis of op school een spelcomputer. In mindere mate worden andere computers gebruikt (40%) en smart Tv's (31%). Een Chromebook (7%) wordt het minst gebruikt door de kinderen in groep 7 en 8.



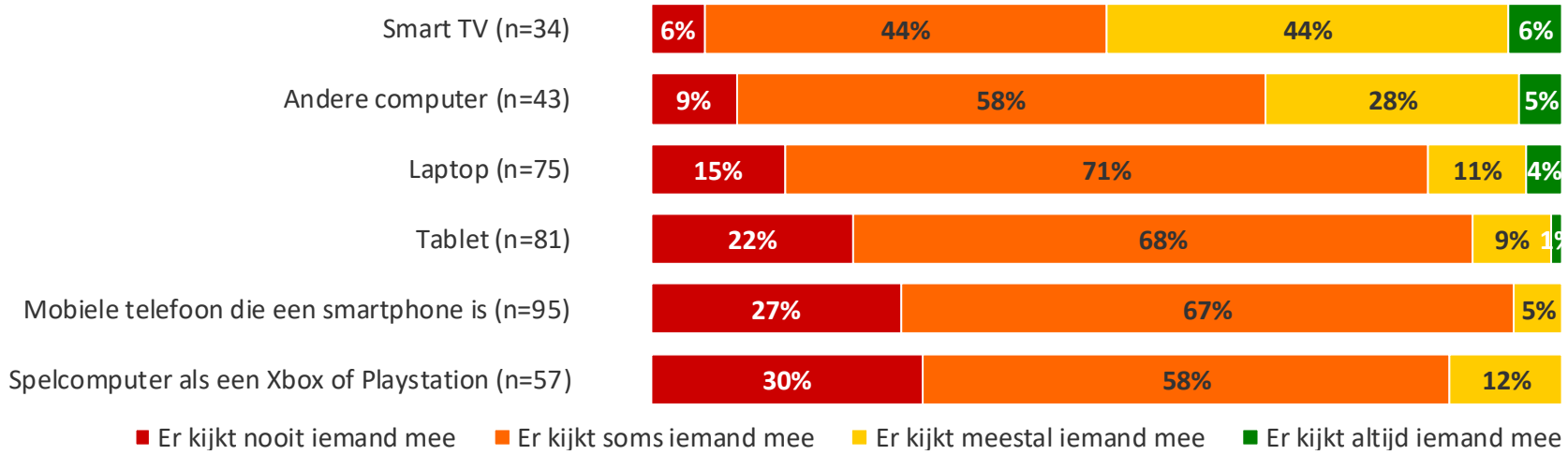
Apparaten vooral gebruikt voor spelletjes en social media

Welke van de volgende dingen doe je weleens:	% doe ik weleens op een laptop (n=80)	% doe ik weleens op een smartphone (n=95)	% doe ik weleens op een tablet (n=81)
Online spelletjes spelen	85%	81%	86%
Op social media gaan	81%	89%	81%
Chatten met vrienden/vriendinnen	69%	93%	62%
Klikken op algemene updates als het wordt gevraagd op het scherm	66%	60%	49%
Klikken op updates van antivirusprogramma's als het gevraagd wordt op het scherm	49%	x	x
Een test invullen op social media	36%	32%	28%
Klikken op reclame bovenaan/aan de zijkant van een website	33%	20%	28%
Klikken op een link naar een onbekende website	30%	25%	23%

Een op de drie kinderen vertoont wel eens risicovol gedrag. Potentieel gevaarlijk gedrag vindt iets vaker plaats op een laptop dan op een smartphone of tablet. 30% van de kinderen die gebruikmaakt van een laptop klikt wel eens op links naar onbekende websites en 33% klikt wel eens op banners.

Ouders kijken *soms* mee; veel vrijheid met smartphone

Kijkt er dan weleens iemand mee met wat jij aan het doen bent om ervoor te zorgen dat jij geen rare of verkeerde dingen doet? (Basis - Gebruikt apparaat)



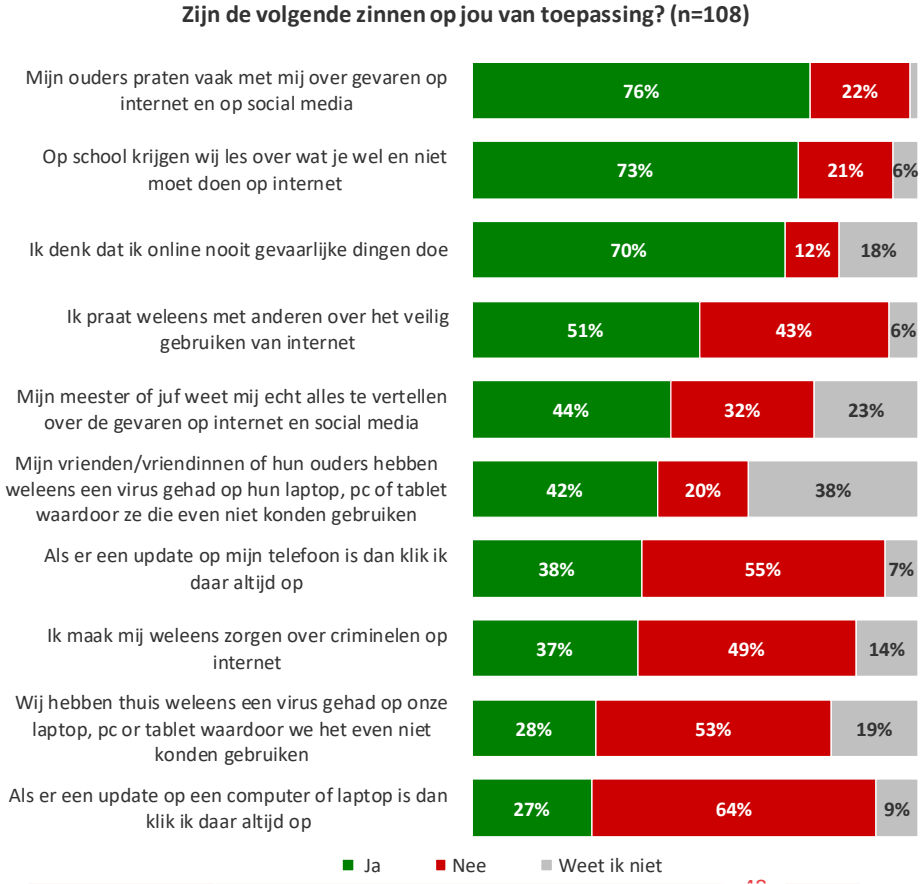
Kinderen geven vaak aan dat er *soms* iemand meekijkt*

Controle op wat kinderen doen op apparaten is laag. Slechts een klein aantal kinderen geeft aan dat er *meestal* of *altijd* iemand meekijkt om te zien of ze geen rare of verkeerde dingen doen op een van de apparaten. Het deel van de kinderen dat aangeeft dat er *nooit* iemand meekijkt is het hoogst op een tablet (22%), smartphone (27%) of spelcomputer (30%).

*Voor een aantal apparaten is de n te klein waardoor alleen speculatieve uitspraken kunnen worden gedaan.

Driekwart van de kinderen praat met ouders over gevaren op internet en social media

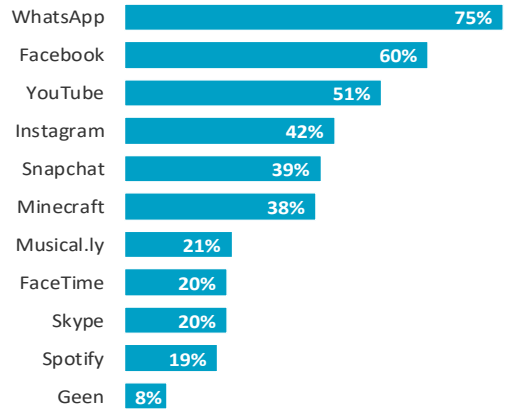
- Driekwart van de kinderen van 11 of 12 jaar praat met zijn ouders over de gevaren op internet en op social media (76%). 73% van de kinderen krijgt op school les over wat ze wel en niet moeten doen op internet. 44% vindt dat de meester of juf ze alles kan vertellen over de gevaren op internet en social media. De helft van de kinderen (51%) praat weleens met anderen over het veilig gebruiken van internet.
- Zeven op de tien kinderen (70%) denkt dat ze online nooit gevaarlijke dingen doen.
- 37% van de kinderen van 11 of 12 jaar maakt zich wel eens zorgen over criminelen op internet.
- Kinderen geven vaker aan dat vrienden/vriendinnen weleens een virus hebben gehad (42%) dan dat zij zelf thuis hebben gehad (28%).
- Kinderen klikken vaker op een update op een smartphone (38%) dan op een update op de computer of laptop (27%).



WhatsApp meest gebruikte app onder kinderen

- WhatsApp is het meest populair onder de ondervraagde kinderen. Driekwart van de ondervraagden kinderen (75%) heeft een account bij WhatsApp. Op afstand volgen Facebook (60%) en YouTube (51%).
- Bijna één op de tien kinderen (8%) geeft aan geen account te hebben bij de voorgelegde websites of apps.
- 24% van de kinderen geeft aan dat zij altijd zelf de privacy-instellingen op social media regelen. 51% doet dit soms zelf en soms met zijn/haar ouders (net hoe het uitkomt). 23% geeft aan dat de ouders dit altijd voor hen doen. 1% geeft aan dat zij nooit bezig zijn geweest met de privacy-instellingen op social media.

Heb je een eigen account op één of meer van deze websites of apps? (n=108)

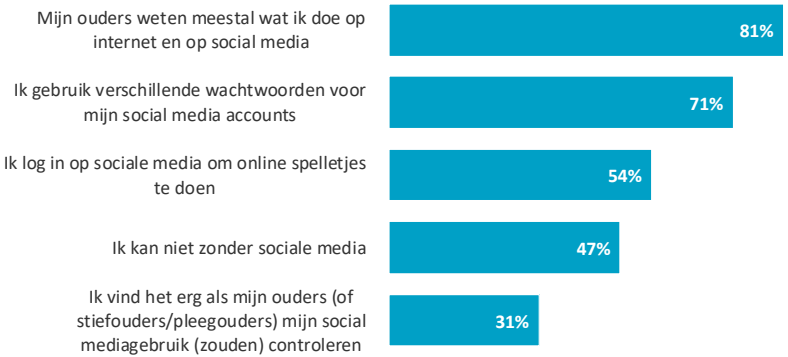


In hoeverre regel jij zelf de privacy instellingen op social media?	% (Basis - Is lid van social media; n=78)
Ik doe dit soms zelf of met mijn ouders samen	51%
Ik doe dit altijd zelf	24%
Dat doen mijn ouders (stiefouders/pleegouders) altijd	23%
Ik heb dit nog nooit gedaan	1%

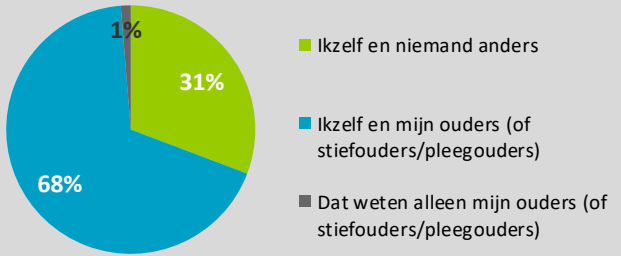
Kinderen geven aan dat ouders op de hoogte zijn van wat zij doen op internet en social media

- Ongeveer acht op de tien (81%) van de ondervraagde kinderen geeft aan dat hun ouders weten wat zij doen op internet en social media.
- Social media wordt door ongeveer de helft (54%) van de kinderen gebruikt om spelletjes te spelen.
- 47% van de kinderen die social media gebruikt is het eens met de stelling “Ik kan niet zonder social media”.
- Bijna één derde (31%) van de kinderen vindt het erg als hun ouders hun socialmedia-gebruik (zouden) controleren.
- Een kwart van de ondervraagde kinderen (26%) geeft aan dat zij geen andere wachtwoorden voor hun socialmedia-accounts gebruiken, en dus overal hetzelfde wachtwoord gebruiken.
- 68% van de kinderen geeft aan dat hun verzorgers de wachtwoorden van hun socialmedia-accounts weten.

Zijn de volgende zinnen op jou van toepassing?
(% ja, Basis - Is lid van social media; n=78)

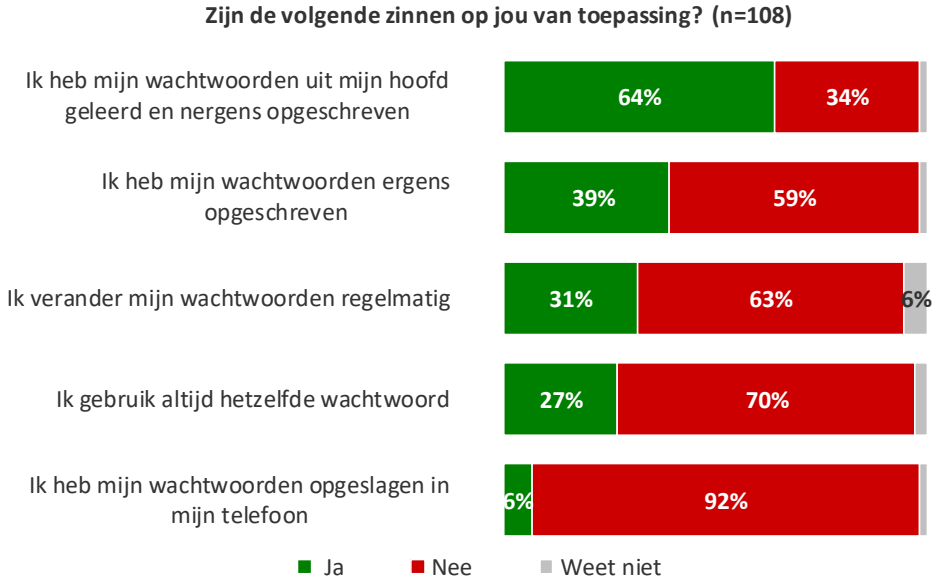


Wie weten jouw wachtwoorden om in te loggen op social media? (Basis - Is lid van social media, n=78)



Wachtwoorden worden meestal uit het hoofd geleerd

- Twee derde van de kinderen (64%) heeft zijn of haar wachtwoorden uit het hoofd geleerd. Ongeveer vier op de tien geven aan dat zij hun wachtwoorden ergens hebben opgeschreven en 6% slaat zijn of haar wachtwoorden op in zijn telefoon.
- Een kwart van de kinderen (27%) geeft aan dat zij altijd hetzelfde wachtwoord gebruiken. Ongeveer een derde (31%) verandert zijn of haar wachtwoord regelmatig.



Helft van de kinderen maakt gebruik van openbare wifi

- 48% van de kinderen van 11 en 12 jaar maakt gebruik van openbare wifi-netwerken waarbij geen wachtwoord wordt gevraagd.
- Een deel van de kinderen denkt te kunnen zien of een website onveilig is (34%),of een website nep is (27%) en of een wifi-netwerk onveilig is (27%).

Zijn de volgende zinnen op jou van toepassing?	% Ja op mij van toepassing (n=108)
Ik maak gebruik van wifi-netwerken waar je geen wachtwoord hoeft in te voeren	48%
Als ik niet thuis ben dan maak ik altijd verbinding met een gratis, openbaar wifi-netwerk	43%
Ik let erop dat een wifi-netwerk veilig is	41%
Ik kijk goed naar het adres van een website in de adresbalk om te kijken of een website veilig is	41%
Ik weet hoe je kunt zien of een website onveilig is	34%
Ik weet hoe je kunt zien dat een website nep is	27%
Ik weet hoe je kan zien dat een wifi-netwerk niet veilig is	27%

Zes op tien kinderen in groep 7 en 8 heeft weleens een vriendschapsverzoek van een onbekende gehad

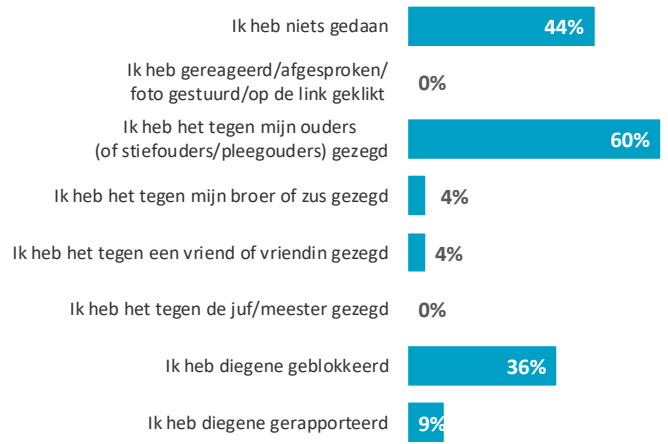
- 59% van de kinderen in groep 7 en 8 heeft wel eens een vriendschapsverzoek gekregen van een onbekende.
- Geen van de ondervraagde kinderen heeft afgesproken met iemand die ze alleen via het internet hebben leren kennen.

Heb je zelf weleens....	% Weleens gedaan/gehad (Basis – Is lid van social media, n=78)
Een vriendschapsverzoek gehad van iemand die je niet persoonlijk kent?	59%
Een berichtje gehad van iemand die je niet persoonlijk kent?	38%
Op een onbekende link geklikt?	28%
Een berichtje gestuurd naar iemand die je niet persoonlijk kent?	13%
Een vriendschapsverzoek gestuurd naar iemand die je niet kent?	10%
Meegemaakt dat iemand online zegt wie hij/zij is maar in werkelijkheid een heel andere persoon is?	6%
Je adres aan iemand gegeven die je alleen via internet kent?	1%
Een foto van jezelf gestuurd naar iemand die je nog niet in het echt hebt ontmoet?	0%
Afgesproken met iemand die je op internet hebt leren kennen?	0%

4 op 10 kinderen heeft risicovolle ervaringen online

Heb jij weleens meegemaakt (n=108):	Heb ik *zelf* weleens meegemaakt	Heb ik niet zelf meegemaakt maar wel *iemand die ik ken*	Heb ik *zelf* weleens meegemaakt en ook *iemand die ik ken*
Ontdekt dat iemand een andere naam of foto gebruikt op het internet dan in het echt	5%	8%	5%
Dat iemand mij vroeg of ik mijn adres wilde opsturen	5%	8%	4%
Dat iemand vroeg of ik een foto van mijzelf wilde opsturen	2%	11%	3%
Dat iemand vroeg of ik een naaktfoto van mijzelf wilde opsturen	1%	6%	2%
Dat iemand zomaar naar mij een naaktfoto stuurde	1%	4%	0%
Dat iemand vroeg om mijn bankrekeningnummer/creditcardnummer of die van mijn ouders te geven	2%	4%	1%
Dat iemand die ik niet kende met mij wilde videobellen (zoals skypen of facetimen)	5%	6%	2%
Dat iemand die ik niet kende mij via WhatsApp een bericht stuurde	16%	6%	5%
Dat iemand die ik heb leren kennen op internet vroeg om af te spreken zonder andere mensen erbij	3%	5%	4%
Een e-mail gekregen waarin iemand om geld vroeg	2%	5%	1%
Een e-mail met een link er in gekregen waar misschien een virus in zat	6%	13%	6%

Wat heb je gedaan na die gebeurtenis?
(Basis - Heeft één of meerdere gebeurtenis zelf meegemaakt, n=45)*

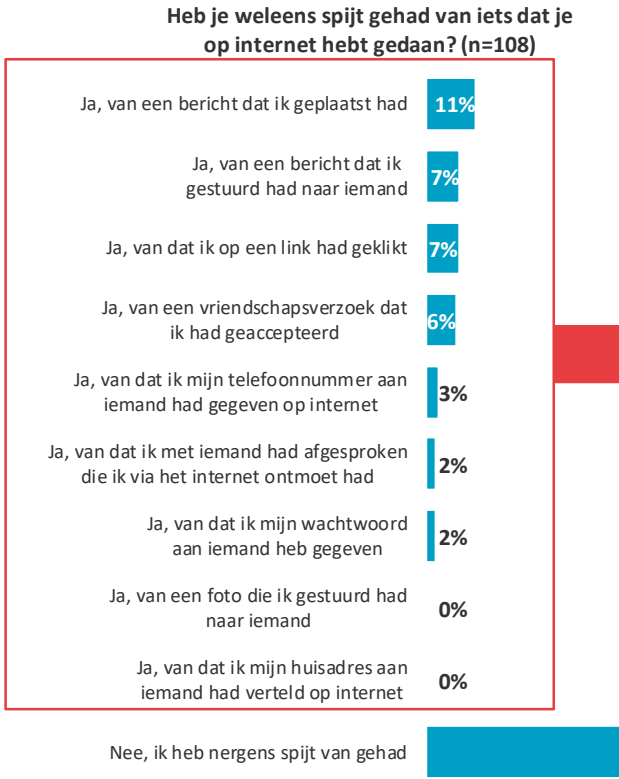


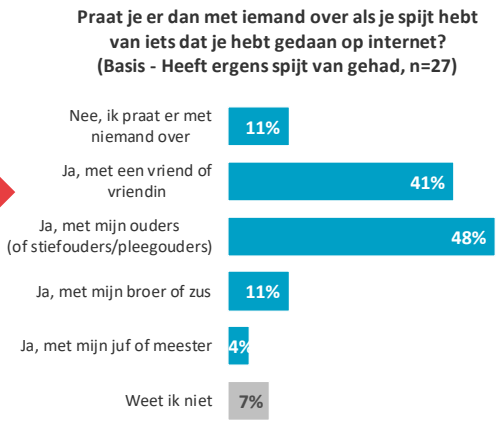
42% van de ondervraagde kinderen heeft zelf weleens een of meerdere voorgelegde gebeurtenissen meegemaakt
Ongeveer twee op de tien (21%) kinderen heeft zelf weleens meegemaakt dat iemand die ze niet kenden hen berichten stuurden via WhatsApp. 12% heeft weleens een link gekregen waar misschien een virus in zat en 10% heeft ontdekt dat iemand een andere naam of foto gebruikt op internet dan in het echt. Vaak lichten kinderen ouders of verzorgers in over de gebeurtenis.

* Uitsplitsing naar specifieke gebeurtenis niet mogelijk vanwege lage n per gebeurtenis

Meeste kinderen geen spijt over gedrag op internet

- 75% van de kinderen van 11 en 12 jaar geeft aan nog nooit spijt te hebben gehad van eigen gedrag op het internet.
- Een geplaatst bericht is de voornaamste reden dat kinderen spijt hebben, gevolgd door een bericht dat ze gestuurd hebben naar iemand (7%), een link waarop ze geklikt hebben (7%) en een vriendschapsverzoek dat ze geaccepteerd hebben (6%).
- In de meeste gevallen van spijt praten kinderen met iemand hierover (82%).
- Kinderen praten vooral met hun ouders/verzorgers (48%) of vrienden/vriendinnen (41%) als ze spijt hebben over hun gedrag op internet.





BIJLAGE

Bijlage | Onderzoekstechnische informatie - kwantitatief

- **Veldwerkperiode**
  - Het veldwerk is uitgevoerd in de periode 18-07-2017 tot 04-08-2017
- **Methode respondentenselectie**
  - Uit het StemPunt-panel van Motivaction
  - Uit een door Motivaction aangeschaft adressenbestand
- **Incentives**
  - De respondenten hebben als dank voor deelname aan het onderzoek punten voor het StemPunt spaarprogramma ontvangen
- **Weging**
  - De onderzoeksdata voor de doelgroep NL 13-80 zijn gewogen , daarbij fungeerde het Mentality-ijkbestand als herwegingskader. Dit ijkbestand is wat betreft sociodemografische gegevens gewogen naar de Gouden Standaard van het CBS
- **Inschakelen externe leveranciers**
  - Voor de volgende werkzaamheden heeft Motivaction bij dit onderzoek gebruik gemaakt van de diensten van gespecialiseerde bedrijven: uitvoeren veldwerk voor de doelgroepen ambtenaren en medewerkers in de vitale infrastructuur.
- **Responsverantwoording online onderzoek**
  - In de veldwerkperiode is aan 10.810 personen een uitnodigingsmail verstuurd. 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

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.

motivaction
research and strategy

Motivaction International B.V.
Marnixkade 109
1015 ZL Amsterdam

Postbus 15262
1001 MG Amsterdam

T +31 (0)20 589 83 83
M info@motivaction.nl

www.motivaction.nl