Veilig Online 2020

Rebecca van der Grient
Natascha Schippers
Kevin Hengstz

Ministerie van Economische Zaken
en Klimaat

B6456 Ministerie EZK

25 september 2020

motivaction
insights and strategy

Inhoudsopgave

Achtergrond

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

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

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

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

Doelstelling en onderzoeksvragen

Het doel (monitoring) van dit onderzoek is enerzijds het vergaren van kennis, houding en gedrag van Nederlanders met betrekking tot online veiligheid en anderzijds het bieden van inzichten voor beleidsvorming met betrekking tot dit thema.

Bij de drie deelonderwerpen zijn de volgende onderzoeksvragen geformuleerd:

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

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

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

Methode en opzet

Methode en opzet

Methode

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

Opzet

Voor de opzet van het onderzoek is grotendeels de opzet van het Alert Online-onderzoek van voorgaande jaren aangehouden, zodat, waar mogelijk, een vergelijking kan worden gemaakt met resultaten uit voorgaande jaren. Het meetinstrument (digitale vragenlijst) is aangepast naar nieuwe inzichten vanuit het gedragsanalysemodel van Motivaction (kennis-houding-gedrag-opzet), waarop in de verdieping ook is gerapporteerd.

Doelgroep

De doelgroep bestaat uit Nederlanders van 16 tot en met 80 jaar.

Steekproef en representativiteit

De netto steekproef van n = 1.022 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.

Vragenlijst en veldwerk

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

Daarnaast zijn er twee doelgroepenrapportages: Ambtenaren en Bedrijfsleven.

Management summary

Hoofdpunten van het onderzoek

Veilig Online 2020; voortzetting van de stabiele trend uit 2018 en 2019
De mate waarin Nederlanders 'veilig online' zijn, is op hoofdlijnen onveranderd in vergelijking met de voorgaande jaren. Op de volgende pagina's zullen we dieper ingaan op de kennis van online risico's, de houding en zorgen ten aanzien van het online domein en hoe het met het online gedrag is gesteld anno 2020.

De belangrijkste Veilig Online trends:

- **Nederlanders geven hun eigen online gedrag een voldoende**
  - De meesten (87%) geven zichzelf een (goede) voldoende. 32% geeft zichzelf zelfs een 8 of hoger.
  - Het gemiddelde cijfer is gelijk aan vorig jaar (7,0). (p43)
- **Nederlanders vinden dat zij goed op de hoogte zijn van online veiligheid**
  - Twee derde (65%) van de Nederlanders schat de eigen kennis over online veiligheid als redelijk tot (zeer) goed
  - Inschatting van de eigen kennis over online veiligheid als goed of slecht inschatten is gelijk aan vorig jaar (p18).
- **Nederlanders schatten de kans dat ze schade ondervinden van online risico's laag in**
  - Voor de meeste online gevaren schat één op de tien Nederlanders de kans (zeer) groot in dat zij er persoonlijk schade van zullen ondervinden (p23)
- **Nederlanders maken zich beperkt zorgen om hun online veiligheid**
  - Van de Nederlanders maakt 50% zich (zeer) weinig zorgen, maakt 40% zich enige zorgen en maakt 9% zich (zeer) veel zorgen
  - De mate dat Nederlanders zich zorgen maken om hun online veiligheid in de privésituatie is in de afgelopen drie jaar stabiel gebleven (p29)

Samenvatting: Kennis

Nederlanders vinden dat zij goed op de hoogte zijn van digitale en online veiligheid

De meeste Nederlanders vinden dat zij (redelijk) goed op de hoogte zijn van online veiligheid (65%). Slechts een klein aantal vindt dat hij/zij onder de maat op de hoogte is (9%). In dit onderzoek zijn een aantal digitale gevaren voorgelegd. Van de meeste van deze gevaren geven Nederlanders aan te weten wat het is, met name identiteitsfraude (89%). De hoge bekendheid ligt er mogelijk aan dat deze vorm van fraude ook offline kan voorkomen. Verder geeft circa een kwart (23%) aan weleens te maken te hebben gehad met phishing en is 60% bekend met phishing.

In de basis weten Nederlanders hoe ze phishing berichten kunnen herkennen

Om phishing te herkennen kijken Nederlanders met name naar het mailadres van de afzender (59%), of er om persoonlijke gegevens (52%) of geld (40%) wordt gevraagd en wat het taalgebruik of de schrijfstijl is van de mail (50%). Links in mails wordt door 29% bekeken en 34% kijkt naar het doeladres achter de link. Phishing gebeurt ook steeds vaker via SMS en WhatsApp. Om die phishing berichten te ontmaskeren bekijken Nederlanders of in de berichten gevraagd wordt om bepaalde gegevens (55%), of er gevraagd wordt om inloggegevens en wachtwoorden in te voeren (51%), of er om geld wordt gevraagd (49%) en of er om persoonlijke gegevens wordt gevraagd (44%).

Nederlanders schatten de kans dat ze schade ondervinden van digitale risico's laag in

De risico-inschatting van verschillende digitale risico's is laag. Risico's zijn vaak abstract, dus moeilijk voor te stellen voor mensen. Een probleem hierbij is dat mensen geneigd zijn om risico's te negeren. Zij nemen daardoor vaak geen voorbereidende maatregelen of doen geen aanpassingen aan hun gedrag om hun persoonlijke risico kleiner te maken. Mensen zijn daarnaast vaak geneigd om risico's lager in te schatten of denken dat vooral andere mensen risico lopen. De lage risico-inschatting uit zich in de lage mate van zorgen die we al eerder beschreven.

Samenvatting: Houding

Nederlanders maken zich beperkt zorgen om hun digitale veiligheid

46% van de Nederlanders geeft aan dat zij zich weinig zorgen maken om hun online veiligheid in hun privésituatie. 6% maakt zich wel veel zorgen. Nederlanders die zich veel zorgen of enige zorgen maken om hun online veiligheid geven aan dat ze zich zorgen maken omdat ze bang zijn de aanpak van internetcriminelen niet door te hebben (48%), omdat ze bang zijn dat mensen hun gegevens kunnen inzien (47%) en omdat ze bang zijn dat financiële gegevens worden gestolen (44%). Nederlanders die zich geen zorgen maken om hun online veiligheid, geven aan dat ze zich geen zorgen maken omdat ze altijd controleren of websites en links vals zijn (43%), omdat ze hun apparaten updaten (43%) en omdat ze regelmatig virusscans maken (42%). De mate waarin Nederlanders zich zorgen maken om hun online veiligheid in de privésituatie is in de afgelopen drie jaar stabiel gebleven (44-46% maakt zich (zeer) veel tot enige zorgen).

De behoefte bij Nederlanders die achterlopen op online veiligheid om zichzelf te verbeteren in online veiligheid is laag

De meeste Nederlanders die bereid zijn om acties te ondernemen, zijn ook degenen die al reeds acties hebben ondernomen (61%). Behoefte om de eigen online veiligheid te verbeteren bij de groep die vooralsnog minder acties heeft genomen is relatief laag. Acties die deze Nederlanders eventueel bereid zijn om te ondernemen zijn het gebruiken van antivirussoftware (48%), het regelmatig uitvoeren van (beveiligings)updates (43%), het controleren van links (40%), het regelmatig maken van back-ups (40%) en het direct uitvoeren van software updates (39%).

Nederlanders willen niet betalen voor betere diensten om veiligheid te verhogen en hebben moeite met beveiligingsinstructies

Nederlanders ervaren nog het meest belemmeringen die financieel van aard zijn. 58% wil niet betalen voor een dienst (zoals een wachtwoord manager) en vindt 40% de prijs van beveiligingssoftware/virusscanner een belemmering. Gratis diensten voor wachtwoordmanagers en virusscanner worden door een derde van de Nederlanders (33%) niet vertrouwt. De meeste Nederlanders geven aan geen moeite te hebben met het maken van back-ups (57%) en weten wat een goede virusscanner is (45%). Meer moeite hebben Nederlanders met beveiligingsinstructies (35%) en het maken van steeds nieuwe wachtwoorden (34%). Ze vinden het ook veel gedoe om voor elk apparaat en account een ander wachtwoord te hebben (44%). Overigens oordelen ze dat ze zelf goed omgaan met het hun wachtwoorden (69%) en het gebruiken van verschillende wachtwoorden (66%).

Samenvatting: Gedrag

Nederlanders vinden hun online gedrag vaak veilig

Een meerderheid van de Nederlanders oordeelt dat zij redelijk tot zeer veilig omgaan met de verschillende voorgelegde zaken ten aanzien van veilig online gedrag; zo oordeelt een meerderheid dat zij goed omgaan met het updaten van hun software (79%), met pogingen tot phishingmails (73%), het gebruik van hun devices door anderen (61%), het maken van back-ups (58%), het geven van toestemmingen op webshops (56%) en het gebruik van USB-sticks (55%).

Verder geven Nederlanders aan dat zij vaak wel de privacy-instellingen van hun social media accounts hebben aangepast (48%). Daarnaast letten Nederlanders op slotjes bij websites (55%). 60% denkt dat een website veilig is als er een slotje op staat.

Nederlanders geven hun eigen online gedrag een voldoende

Nederlanders geven zichzelf gemiddeld een 7,0 als het gaat om veilig omgaan met online gevaren. Nederlanders die zichzelf een onvoldoende geven, vinden dat ze weinig verstand hebben van online gevaren (37%) en geven aan dat ze er niet altijd bewust mee bezig zijn (27%). Nederlanders die zichzelf een voldoende geven, vinden dat ze juist wel goed op de hoogte zijn (30%) en geven aan alert te zijn op online gevaren (20%).

Twee derde van de Nederlanders het afgelopen jaar in aanraking is gekomen met een digitaal risico

Bijna de helft van de Nederlanders (45%) heeft in de afgelopen 12 maanden mails ontvangen met poging tot phishing in de privésituatie en 16% ontving dergelijke mails in de werksituatie. Phishing is daarmee het meest voorkomende digitaal gevaar. Het is dus belangrijk dat Nederlanders bekend zijn met phishing en phishing kunnen herkennen om zichzelf te beschermen. Ruim vier op de vijf Nederlanders (83%) is bekend met phishing en van deze groep weet bijna iedereen phishing te herkennen (98%). Er wordt met name gelet op het mailadres (59%), de vraag om persoonlijke gegevens (52%) en het taalgebruik (50%).

Samenvatting: werk en corona (1/2)

Weinig zorgen om de digitale veiligheid in een werksituatie

73% geeft aan zich zeer weinig zorgen te maken over hun online veiligheid in een werksituatie. Dat zijn meer Nederlanders dan vorig jaar (66%).

Drie op de tien thuiswerkers heeft nog steeds het standaard wachtwoord op de router

De meeste Nederlanders hebben ook geen duidelijk beeld wat veilig online gedrag op werk inhoud (57%) of in een privésituatie (52%). Door de coronacrisis hebben meer mensen thuis moeten werken. 48% van de werkende Nederlanders geeft aan in de afgelopen 12 maanden thuis te hebben gewerkt. Zij maken thuis vaak gebruik van een netwerkverbinding met wachtwoord (78%). Dit wachtwoord blijkt nog relatief vaak het standaardwachtwoord te zijn van de router (29%). Werknemers kun vaak niet benoemen wat hun werkgever heeft gedaan aan speciale maatregelingen om thuiswerken sinds de coronacrisis mogelijk te maken (57%). 16% geeft aan dat zijn/haar werkgever bedrijfsapparatuur tot de beschikking heeft gesteld.

Bij de meeste bedrijven zijn afspraken over hoe men zich veilig online dient te gedragen

Zeven op de tien (69%) werkende Nederlanders geven aan dat bij hun bedrijf/organisatie afspraken zijn gemaakt omtrent online veilig gedrag. 13% geeft aan dat er bij hun bedrijf/organisatie geen afspraken zijn gemaakt. Afspraken die gemaakt zijn hebben vaak betrekking op het veilig versturen/uitwisselen van bestanden (35%), het gebruik maken van websites en/of e-mail (33%), dat alleen systeembeheerders software kunnen installeren (31%) en het versturen/uitwisselen van persoonsgegevens (31%).

Samenvatting: werk en corona (2/2)

Het is niet moeilijk om je aan werkafspraken te houden, maar deze afspraken mogen duidelijker gecommuniceerd worden

Degenen die werkafspraken hebben (69%), vinden het niet moeilijk om zich (altijd) aan die afspraken te houden (81%). Circa de helft (46%) ervaart wel belemmeringen bij het borgen van afspraken omtrent veilig onlinegedrag. Dit heeft met name te maken met de manier waarop gecommuniceerd wordt. Dit is niet altijd duidelijk (13%), niet voldoende (13%) of eenduidig (12%).

Het thuisnetwerk de zwakke plek voor bedrijven

Door het hele onderzoek heen zien we dat het voorkomen van online risico's scherper wordt gemonitord en nageleefd in de werksituatie dan in de privé-situatie. Bedrijven doen er veel aan om de online veiligheid op orde te hebben. Maar nu met het massale thuiswerken zou het thuisnetwerk en de thuissituatie wel eens de achilleshiel van het bedrijfsnetwerk kunnen worden; routerpaswoorden worden niet aangepast en kinderen maken gebruik van bedrijfshardware.

Samenvatting: Digitality doelgroepen

Technoprogressiviteit en 'The Social Dilemma'
In de verdieping wordt het Digitality doelgroepenmodel toegelicht. Voor deze samenvatting hebben zijn de 2 belangrijkste insights uitgelicht die mede op basis van de onderliggende dimensies 'technoprogressiviteit' en 'digital social engagement' kunnen worden verklaard.

Technoprogressiviteit: Jongeren vs. ouderen
Hoe komt het dat ouderen vaker online risico lopen dan jongeren, ondanks dat zij een meer alerte houding hebben?

- In het onderzoek is aantoonbaar dat ouderen:
  - Een meer alerte houding hebben dan jongeren
  - Maar minder up-to-date kennis hebben dan jongeren
- Dit maakt dat ouderen realistisch zijn over de eigen kennis en door het gebrek aan up-to-date kennis van de gevaren, nog steeds het grootste gevaar lopen
- Dit maakt ook dat jongeren wellicht voldoende kennis hebben, maar soms ook de eigen kennis overschatten en laksere houding aannemen, waardoor zij ook gevaar lopen.

Techno-progressieve mannen vs. digitaal-sociale vrouwen
Hoe komt het dat vrouwen vaker last hebben van 'the social dilemma'?

Zowel uit dit onderzoek als eerder Digitality-onderzoek blijkt dat vrouwen het internet vaker 'sociaal' gebruiken en mannen vaker 'functioneel':

- Vrouwelijke Digital Interactors zijn relatief het meest kwetsbaar vanwege beperkte affiniteit met digitale technologie en relatief hoog digitaal sociaal gedrag.
- Mannelijke Digital Functionalists zijn relatief het minst kwetsbaar vanwege de hoge affiniteit met digitale technologie en relatief laag digitaal sociaal gedrag; gebruikt digitaal meer functioneel

Resultaten

Leeswijzer resultaten

Significante verschillen

In de rapportage tonen we de resultaten voor de doelgroep Nederlands publiek in grafiek vorm of in tabel vorm. In tekst bespreken we de belangrijkste inzichten van het Nederlands publiek. Waar relevant – en mogelijk – gaan we in op verschillen met de vorige meting uit 2019. We bespreken – 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 = significant hoger
Rood = significante lager

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 gemiddelde niveau 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. Percentages lager dan 2% zijn soms niet opgenomen in de grafiek. Dit is vanwege de leesbaarheid van de grafiek.

Verdiepingen

In dit onderzoek is gekeken naar digitale kennis, houding en gedrag. Hiervoor is enerzijds het gedragsanalysemodel van Motivaction gebruikt. De beschrijving van dit model en de inzichten staan in de verdieping. Daarnaast is er gebruik gemaakt van het segmentatiemodel Digitality. De segmentatie is gebaseerd op de digitale overtuigingen en houdingen van Nederlanders. De beschrijving van dit model en de inzichten staan in de verdieping.
Omdat de focus van dit onderzoek op het Nederlands publiek ligt, zijn die cijfers gerapporteerd in het rapport. We zien in het onderzoek dat de Digitality-groepen (sterk) verschillen op verschillende onderdelen van dit onderzoek. Deze onderdelen zijn te herkennen aan het Digitality- icoontje
> Klik op het icoontje om naar uitgesplitste resultaten naar Digitality doelgroepen te gaan.

Kennis over online risico's

Kennis

Twee derde schat de eigen kennis over online veiligheid als redelijk tot (zeer) goed

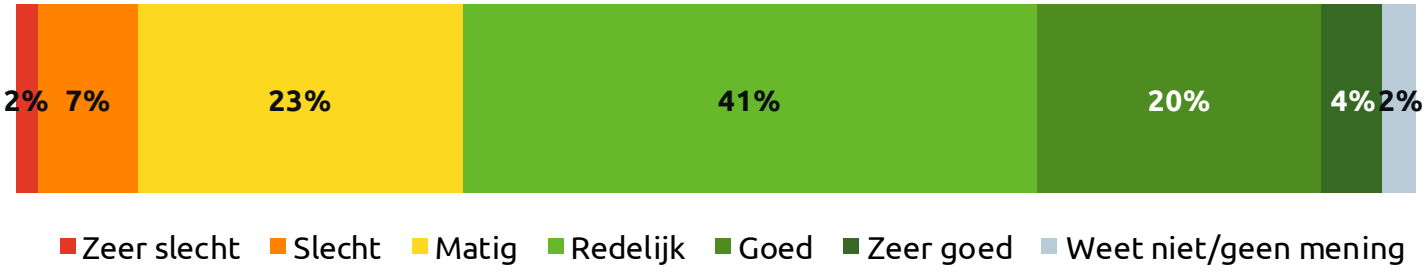
Een kwart (24%) van de Nederlanders schat de eigen kennis over online veiligheid goed tot zeer goed in. 41% vindt de eigen kennis redelijk (samen 65%). Circa een kwart (23%) schat zichzelf matig in en 9% noemt zijn eigen kennis (zeer) slecht.

De mate waarin Nederlanders hun eigen kennis over online veiligheid als goed of slecht inschatten is gelijk aan vorig jaar.

Verschillen binnen Nederland

- Mannen schatten hun eigen kennis over online veiligheid hoger in dan vrouwen (31% (zeer) goed onder mannen vs. 18% onder vrouwen).
- Nederlanders van 55 jaar en ouder schatten hun kennis over online veiligheid lager in dan jongere Nederlanders (19% vs. 28%). Met name jongere Nederlands tussen de 18 en 24 jaar (34%) en tussen de 35 en 44 jaar (34%) schatten hun kennis over online veiligheid als (zeer) goed.
- Hoogopgeleiden schatten hun kennis over online veiligheid hoger in (30% goed tot zeer goed). Tegenover 20% onder laagopgeleiden.

Hoe schat jij je eigen kennis over digitale en online veiligheid in?
(Basis - Nederland representatief, n=1.022)



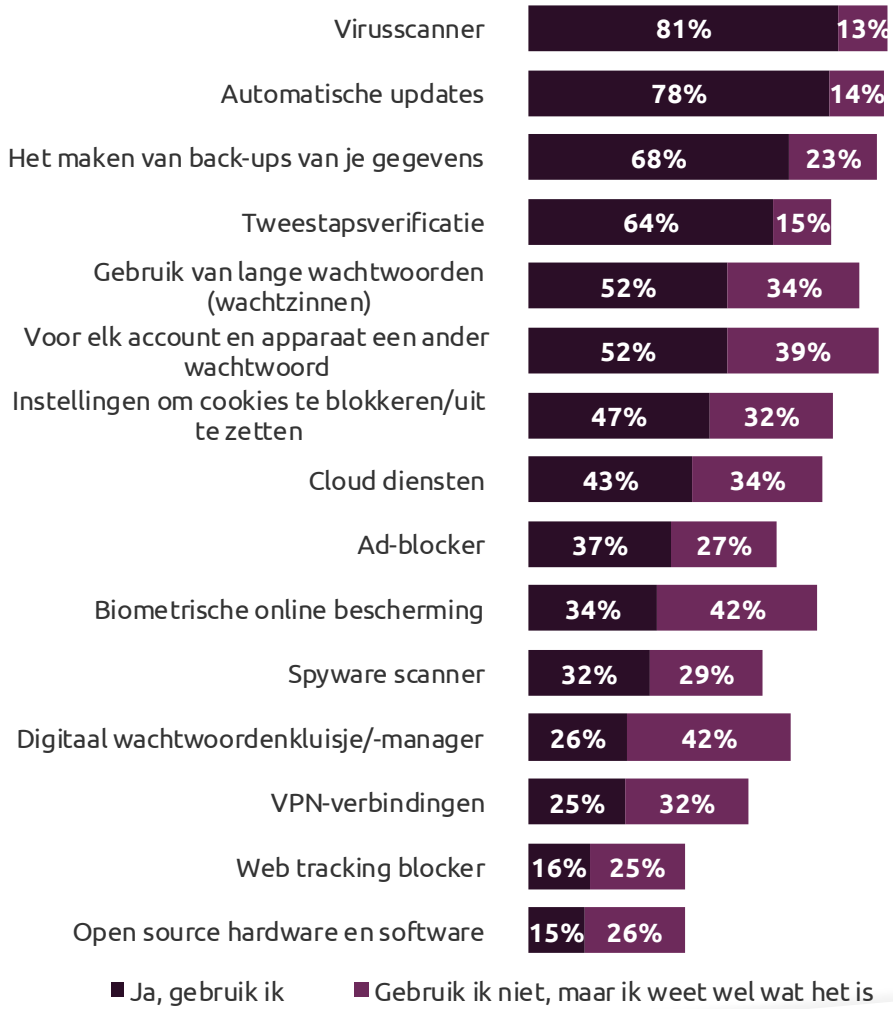
Kennis

Meerderheid Nederlanders bekend met verschillende online beveiligingsopties

De meeste Nederlanders zijn bekend met de verschillende online beveiligings-opties. Web tracking blocker (41%) en open source hardware- en software (41%) zijn het minst bekend en gebruikt.

In vergelijking met vorig jaar geven meer Nederlanders aan bekend te zijn met spyware scanner (29% vs. 2019: 21%), met cloud diensten (34% vs. 29%), met webtracking blockers (25% vs. 20%), met VPN-verbindingen (32% vs. 26%) en met open source hardware- en software (26% vs,. 22%). Meer Nederlanders maken gebruik van automatische updates (78% vs. 74%), tweestapsverificatie (64% vs. 55%) en biometrische online bescherming (34% vs. 25%).

Kun je aangeven in welke mate je bekend bent met onderstaande zaken? (Basis - Nederland representatief, n=1.022)



	2019 Gebruik ik	2019 Ken ik
Virusscanner	78%	11%
Automatische updates	**74%**	13%
Het maken van back-ups van je gegevens	Nieuw t.o.v. 2019	
Tweestapsverificatie	**55%**	15%
Gebruik van lange wachtwoorden (wachtzinnen)	Nieuw t.o.v. 2019	
Voor elk account en apparaat een ander wachtwoord	Nieuw t.o.v. 2019	
Instellingen om cookies te blokkeren/uit te zetten	47%	29%
Cloud diensten	43%	**29%**
Ad-blocker	33%	25%
Biometrische online bescherming	**25%**	41%
Spyware scanner	34%	**21%**
Digitaal wachtwoordenkluisje/-manager	23%	39%
VPN-verbindingen	24%	**26%**
Web tracking blocker	13%	**20%**
Open source hardware en software	15%	**22%**

Rood = significant **lager** dan in 2020

*Zie de bijlage voor het volledige overzicht

Kennis
Nederlanders zijn het meest bekend met identiteitsfraude

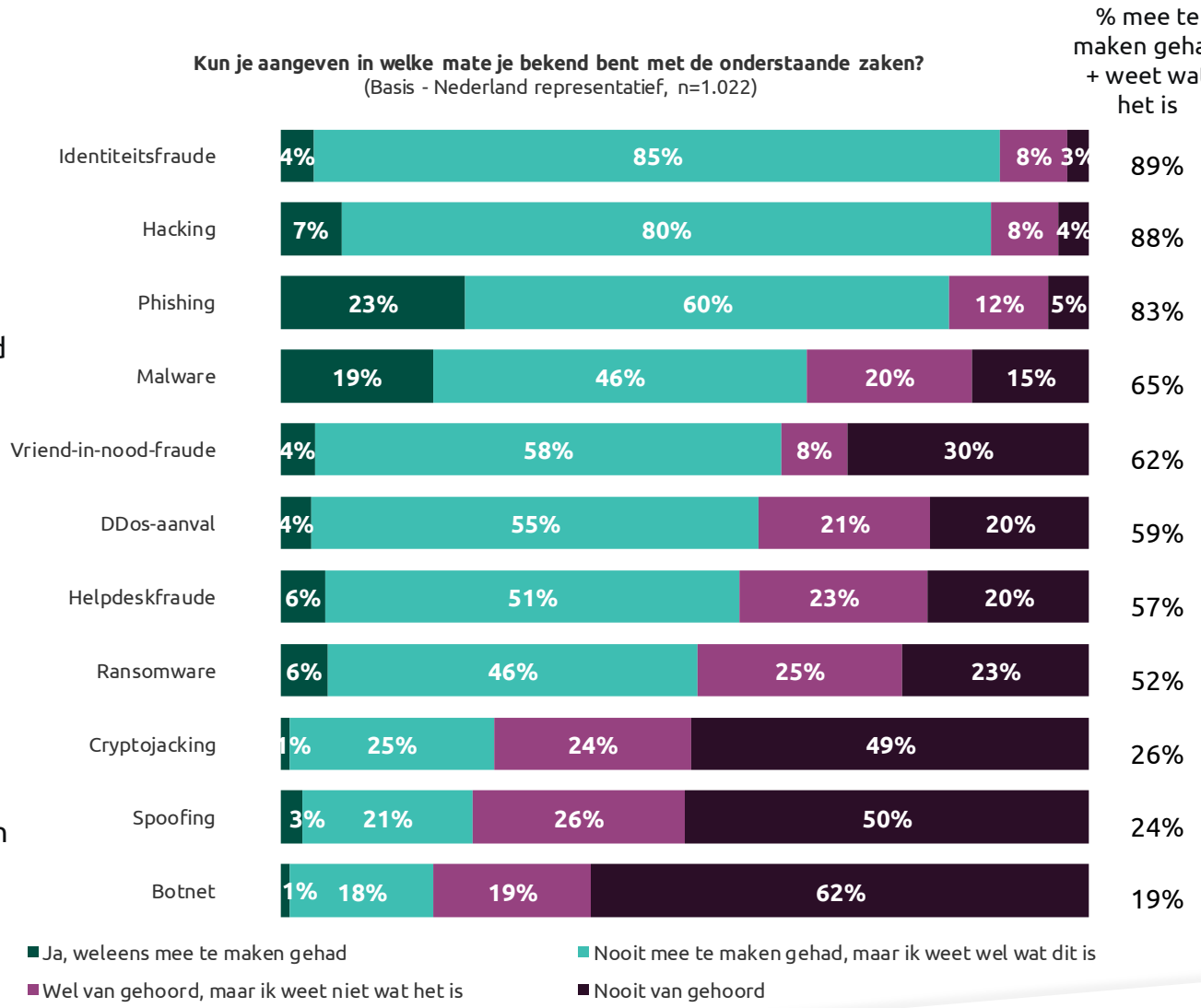
- Identiteitsfraude is het meest bekend (89%). Nederlanders geven met name aan te weten wat dit is (85%), maar komen hier niet vaak mee in aanraking (4%).
- Identiteitsfraude wordt qua bekendheid op de voet gevolgd door hacking (88%). De meesten geven aan deze cybercrime te kennen (80%).
- Circa een kwart (23%) van de Nederlanders heeft weleens te maken gehad met phishing. Van de voorgelegde vormen is phishing de meest voorkomende vorm van online risico's waar Nederlanders mee in aanraking zijn gekomen. 60% van de Nederlanders heeft er niet mee te maken gehad, maar kent het wel.
- Het minst bekend zijn Nederlanders met Botnets (19%).

Verschillen binnen Nederland

Mannen zijn vaker bekend met de verschillende online risico's.

Jongeren t/m 24 jaar geven vaker aan nooit gehoord te hebben van de verschillende risico's of niet te weten wat deze zijn. 65-plussers hebben vaker nog nooit gehoord van de drie minst bekende online risico's.

Laagopgeleiden geven vaker aan niet bekend te zijn de voorgelegde online risico's.



Kennis

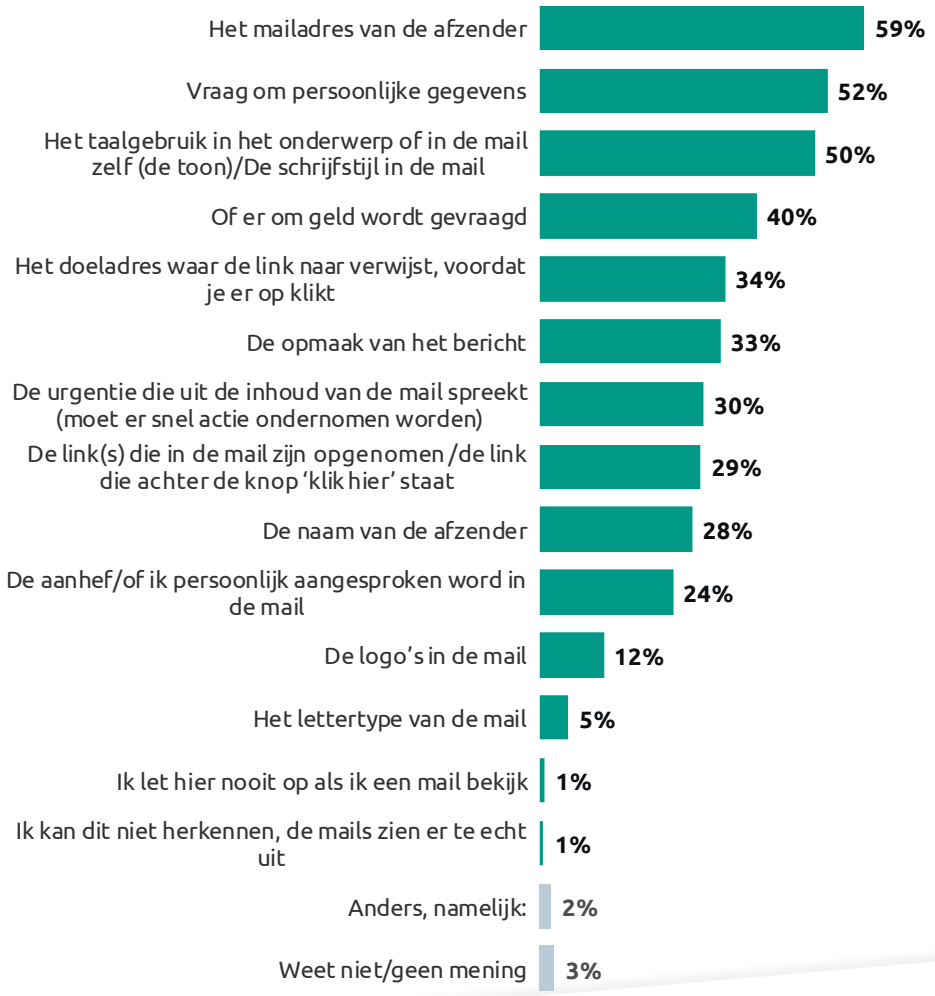
Om phishingsmails te ontmaskeren kijken Nederlanders naar het mailadres, de vraag om persoonlijke gegevens en het taalgebruik

Phishing is een veel voorkomend online risico. In april 2020 berichtte de Nederlandse Vereniging van Banken (NVB) dat zij in 2019 vaker slachtoffers hebben van phishing*. De schade door phishing verdubbelde ten opzichte van 2018. Het is dus belangrijk dat Nederlanders phishing herkennen om zichzelf te beschermen. Aan Nederlanders die aangaven bekend te zijn met phishing (83%) is gevraagd waar zij op letten om een phishingmail te herkennen. Zij geven aan dat ze met name letten op het mailadres (59%), de vraag om persoonlijke gegevens (52%) en het taalgebruik (50%). Vrijwel niemand geeft aan dat ze deze berichten niet kunnen herkennen (1%) of niet op letten (1%).

Verschillen binnen Nederland

- Mannen letten vaker op het afzendadres (63% vs. 55%), het doeladres van de link (39% vs. 29%), de naam van de afzender (31% vs. 25%) en de opgenomen links in de mail (34% vs. 25%). Vrouwen of er om geld wordt gevraagd (45% vs. 35%).
- Jongeren (16 t/m 34 jaar) kijken vaker naar het afzendadres (74%). 65-plussers juist minder vaak (45%). 25 t/m 34 jarigen geven vaker aan dat zij letten op de opmaak van het bericht (42%) en op de naam van de afzender (37%). 55 t/m 80 jarigen letten meer op de urgentie van de mail (37%).
- Hoogopgeleiden kijken vaker naar het mailadres (65%), het taalgebruik (57%) en de links in de mail (38%). Laagopgeleiden doen dit juist minder vaak (mailadres: 43%, taalgebruik: 40% en links: 17%). Zij kijken wel vaker naar de aanhef van de mail (31%).

Naar welke onderdelen van een mail kijk jij vooral om een phishingmail te herkennen? (Basis - Bekend of heeft ervaring met phishing, n=845)



*) https://www.nvb.nl/nieuws/veel-meer-phishing-en-bankpasfraude-in-2019/

Kennis

Men herkent phishingberichten via SMS of WhatsApp aan de vraag om (inlog)gegevens en geld

Tegenwoordig komt phishing ook vaak voor via SMS of WhatsApp. Om dit soort phishingberichten te herkennen, kijken Nederlanders of er om bepaalde gegevens worden gevraagd (55%), of er om inloggegevens worden gevraagd (51%) of er om geld wordt gevraagd (49%). Vrijwel niemand geeft aan dat ze deze berichten niet kunnen herkennen (1%) of niet op letten (1%).

Verschillen binnen Nederland

- Vrouwen letten vaker op of er om inloggegevens wordt gevraagd (55% vs. 47%) of om geld (53% vs. 45%). Mannen letten vaker dan vrouwen op de naam van de afzender (32% vs. 24%).
- 65-plussers letten vaker op of er om inloggegevens worden gevraagd (61%) en op de urgentie van het bericht (37%). Jongeren van 16 t/m 34 jaar letten vaker op de naam van de afzender (37%). Jongeren tussen de 25 en 34 jaar letten ook vaker op taalgebruik en schrijfstijl (48%). Dit is iets wat ouderen veel minder doen (55 en ouder: 25%).
- Hoogopgeleiden kijken vaker naar het taalgebruik/de schrijfstijl (43%) en de urgentie van het bericht (35%). Laagopgeleiden kijken juist minder vaak naar het taalgebruik/de schrijfstijl (23%).

Naar welke onderdelen van een bericht kijk jij vooral om een phishing via SMS of WhatsApp te herkennen? (Basis - Bekend of heeft ervaring met phishing, n=845)

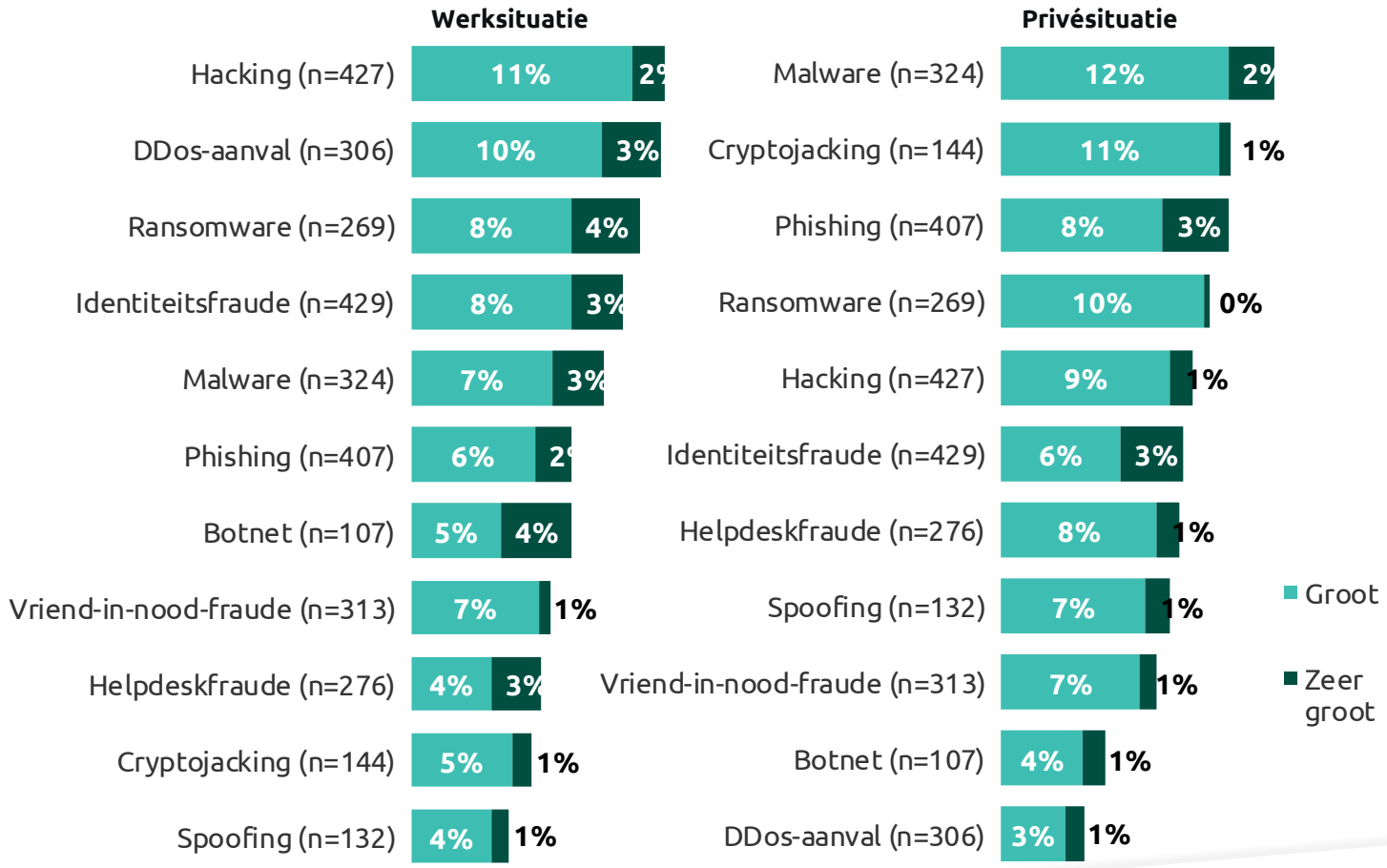
Kennis

Werkende Nederlanders verwachten dat ze meer risico lopen op ander soort digitale risico's in de privésituatie dan op werk

Werkende Nederlanders verwachten dat ze meer risico lopen van ander soort digitale risico's in de privésituatie dan op werk. Op werk staan hacking (13%), een DDos-aanval (13%) en ransomware (12%) bovenaan, terwijl men verwacht thuis meer risico te lopen op malware (13%), cryptojacking (12%) en phishing (11%). Echter de verschillen tussen locaties zijn klein (vaak vier procentpunten verschil of minder).

Met name voor een DDos-aanval en cryptojacking zijn de verschillen tussen thuis en werk nog relatief groot (respectievelijk 9 procentpunten verschil en 6 procentpunten verschil).

Hoe groot acht je de kans dat je <u>in jouw […]</u> (computer)schade of financiële schade oploopt, tijdelijk geen gebruik kunt maken van je computer of gegevens kwijtraakt als gevolg van de volgende zaken? (Basis – Is bekend met de digitale risico's)



Kennis

Hoewel Nederlanders aangeven bepaalde online risico's te kennen, verwarren ze nog relatief vaak beschrijvingen van online risico's

Respondenten hebben aangegeven in welke mate ze bekend zijn met een aantal online risico's (zie pagina 19). Over maximaal twee online risico's waarvan de respondent had aangegeven hier ervaring mee te hebben (weleens mee te maken gehad) of te kennen (nooit mee te maken gehad, maar ik weet wel wat dit is), is een verdiepende vraag gesteld. Respondenten kregen een beschrijving van de specifieke online risico te lezen. Deze kon een juiste beschrijving van de online risico zijn of een onjuiste beschrijving. De vraag aan de respondent was om aan te geven in welke mate hij/zij dacht dat de weergegeven beschrijving klopte bij het online risico.

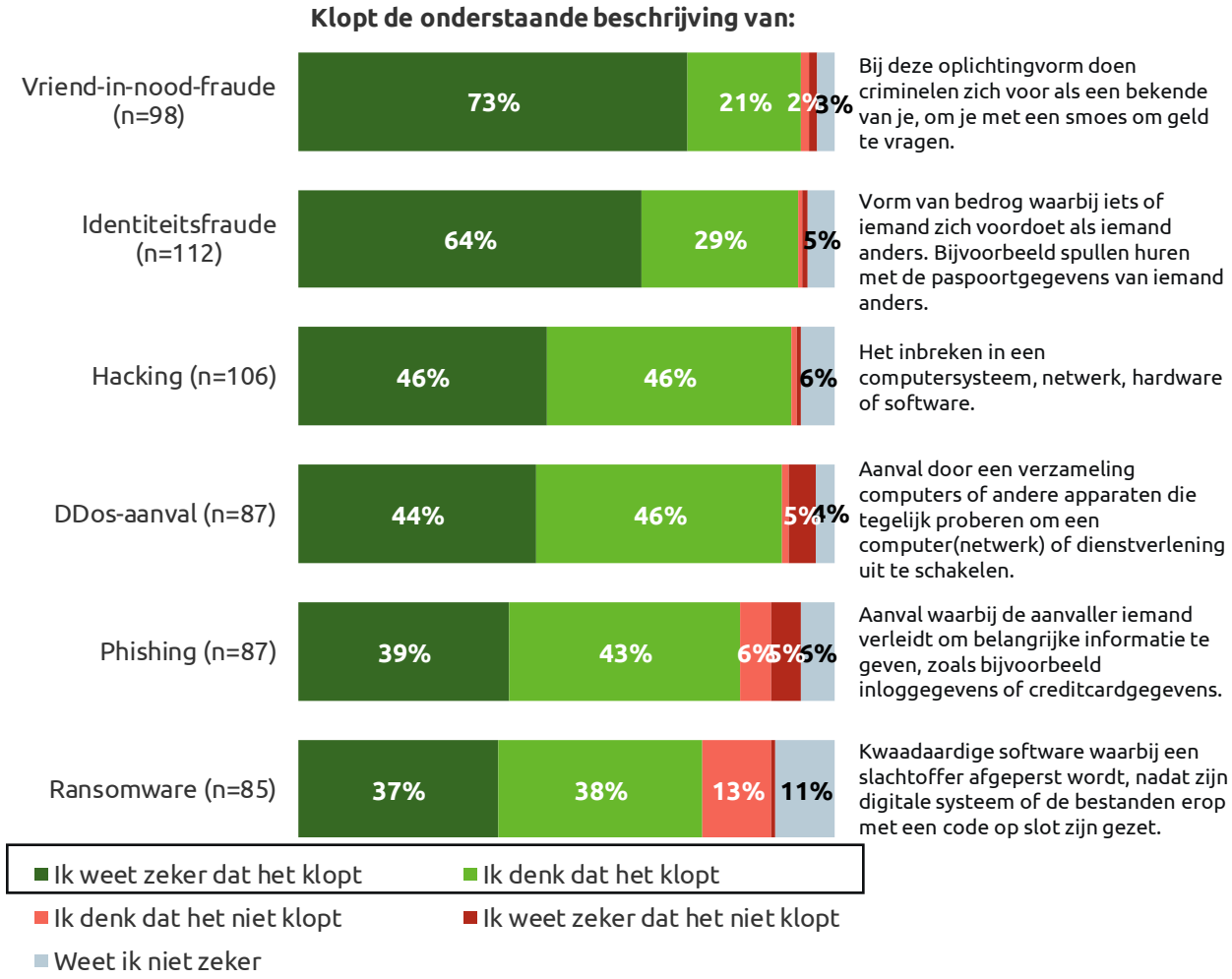
Op de volgende twee pagina's tonen we eerst de resultaten van de juiste beschrijving en daarna de resultaten van de foute beschrijving. Wat op valt is:

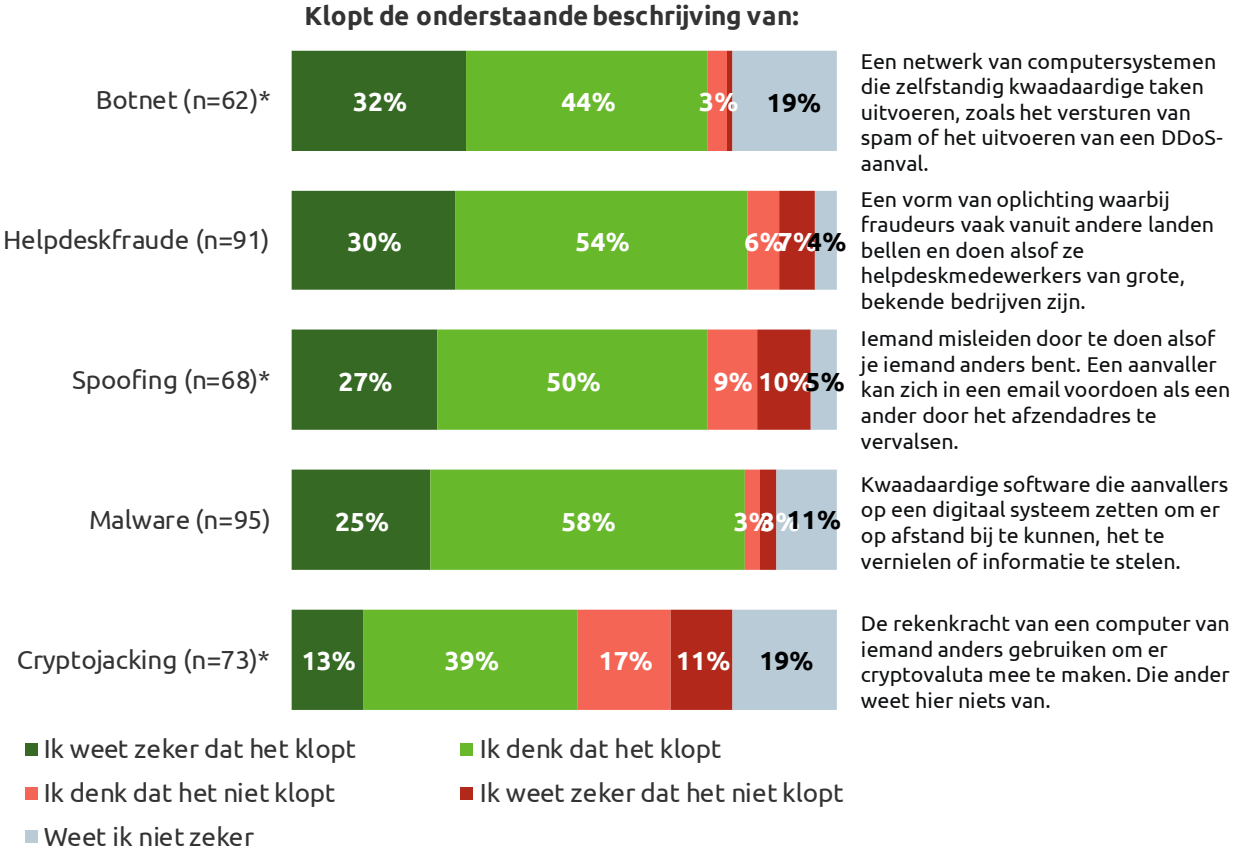
- Bij de correcte beschrijvingen
  - zijn ondervraagden relatief vaak zeker dat de beschrijving juist in. En de meeste anderen gevallen denken ze dat de beschrijvingen juist zijn. Het komt weinig voor dat men bij de correcte beschrijvingen aangeeft dat deze niet kloppen.
  - hoewel men aangaf bekend te zijn met botnets en cryptojacking, geeft een op de vijf aan dat ze niet weten of de gegeven beschrijving klopt*.
  - bij de juiste beschrijving van cryptojacking en spoofing geven nog relatief vaak ondervraagden aan dat de beschrijving niet klopt*.
- Bij de foutieve beschrijvingen
  - geven ondervraagden nog relatief vaak aan dat de foute beschrijving klopt. Men verwart online risico's die ongeveer op elkaar lijken of met elkaar te maken hebben, zoals spoofing, phishing en identiteitsfraude.
  - ook de meer onbekende online risico's (zoals cryptojacking en spoofing) worden relatief vaak ten onrechte als correct aangeduid.

*) Resultaat is indicatief wegens het lage aantal waarnemingen (n<80)

Kennis

Juiste beschrijvingen worden vaak als goede beschrijvingen aangemerkt. Men is minder zeker over beschrijvingen van spoofing en cryptojacking.

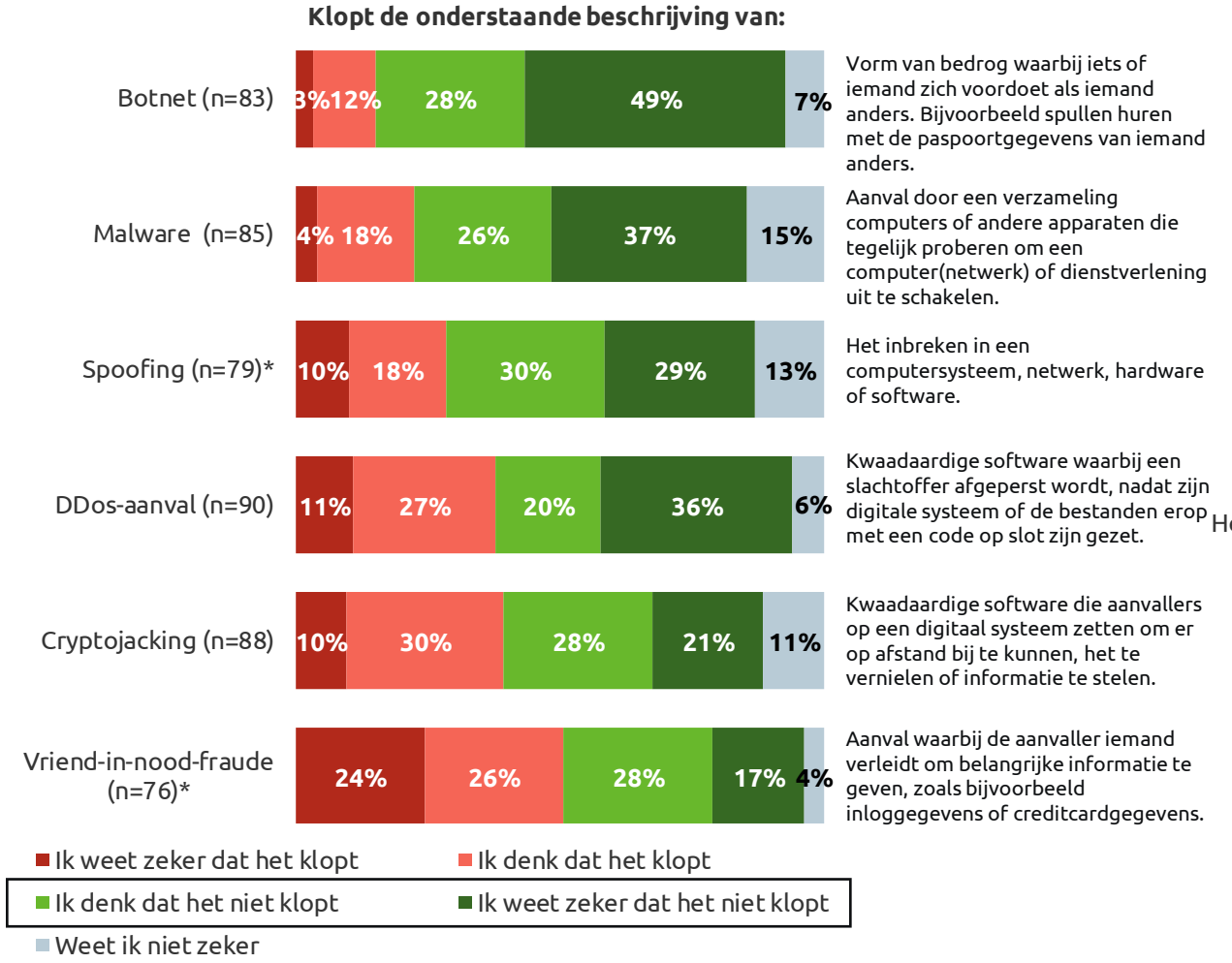


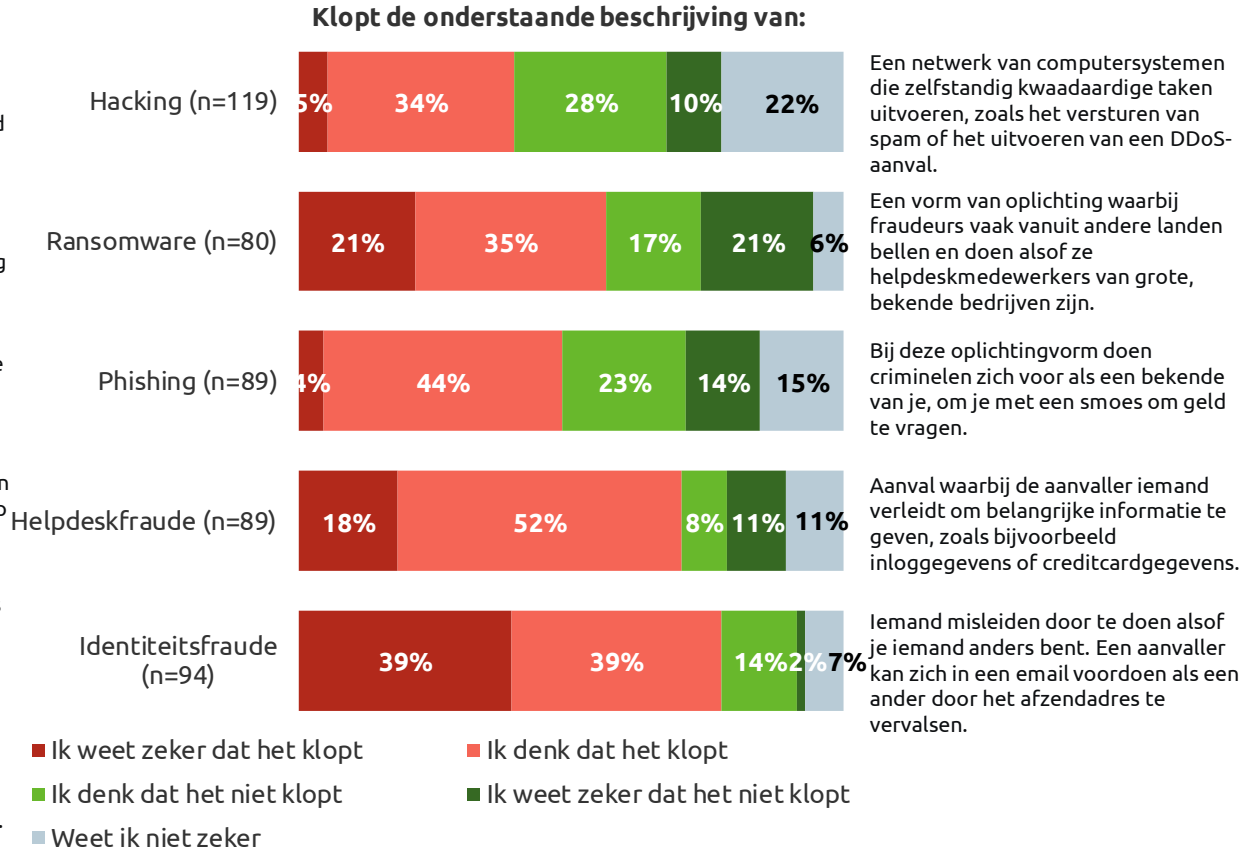


*Resultaat is indicatief wegens het lage aantal waarnemingen (n<80)

Kennis

Foute beschrijvingen worden relatief vaak ten onrechte als juist aangemerkt





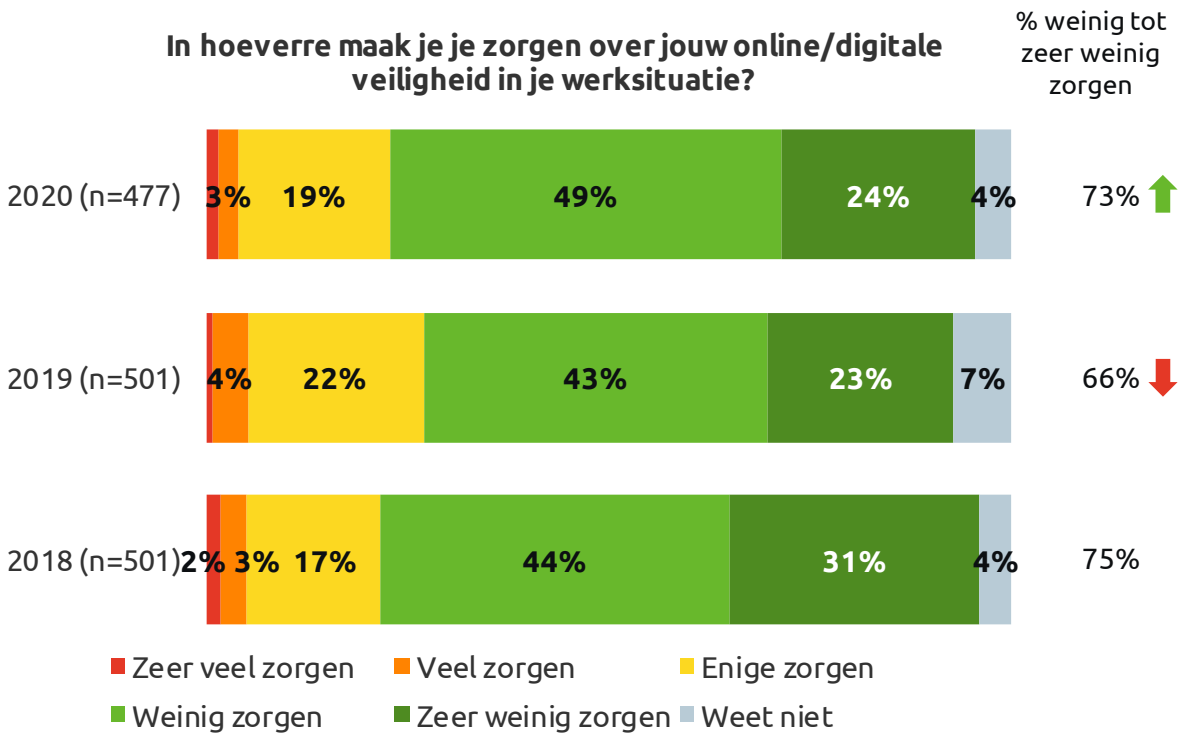
*Resultaat is indicatief wegens het lage aantal waarnemingen (n<80)

Zorgen om online veiligheid

Zorgen
Mate van zorgen over online veiligheid op werk afgenomen

Vorig jaar zagen we dat het aandeel werkende Nederlanders dat zich weinig tot zeer weinig zorgen maakte om online veiligheid was afgenomen (van 75% naar 66%). Dit jaar geven weer meer Nederlanders aan zich geen zorgen te maken (73%).

Dit jaar maakt 4% zich veel tot zeer veel zorgen en 19% maakt zich enige zorgen (samen 23%) over de online veiligheid in de werksituatie.

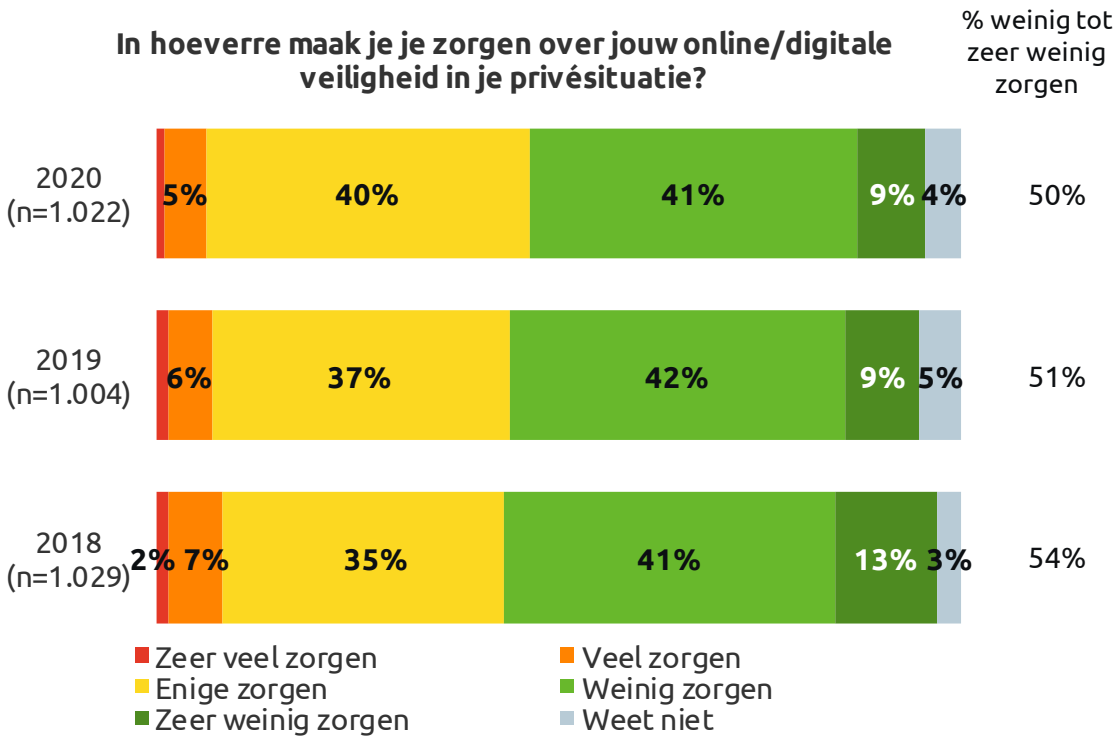


Zorgen
Mate van zorgen om online veiligheid in de privésituatie stabiel

De mate dat Nederlanders zich zorgen maken om hun online veiligheid in de privésituatie is in de afgelopen drie jaar stabiel gebleven. 6% maakt zich veel tot zeer veel zorgen en 40% maakt zich enige zorgen (samen 46%). Dat is dubbel zoveel dan in de werksituatie (23%; zie ook vorige pagina). In de privésituatie zijn Nederlanders natuurlijk zelf verantwoordelijk voor hun veiligheid, wat de hogere mate van zorgen kan verklaren.

Verschillen binnen Nederland

Met name jongeren (16 t/m 34 jaar) maken zich minder zorgen om hun online veiligheid in de privésituatie (64%). Nederlanders in de leeftijd 65 t/m 80 maken zich vaker enige zorgen (52%).



Zorgen

Meeste zorgen om de steeds slimmere aanpak van internetcriminelen en dat de eigen gegevens door anderen misbruikt worden

Nederlanders die zich zorgen maken om hun online veiligheid in de privésituatie (46%) maken zich met name zorgen om de aanpak van internetcriminelen (48%). De aanpak van criminelen wordt steeds vernuftiger en Nederlanders zijn bang dat ze de trucjes niet door (kunnen) hebben. Daarnaast maken ze zich zorgen dat mensen in hun gegevens kunnen kijken en daar misbruik van kunnen maken (47%), dat financiële gegevens gestolen worden (44%), dat hun computer niet meer naar behoren werkt (37%) en dat persoonlijke gegevens worden gestolen (32%). Circa een kwart vindt dat cybercrime veel voorkomt (27%). Een op de vijf erkent dat de beveiliging niet op orde is (20%).

Verschillen binnen Nederland

- Met name vrouwen maken zich zorgen om de steeds slimmere aanpak van internetcriminelen (53% vs. 43%). Ze worden ook banger gemaakt door anderen (17% vs. 7%).
- Hoogopgeleiden maken zich vaker zorgen dat hun computer niet meer werkt (46%) en dat hun beveiliging niet op orde is (26%). Zij geven vaker aan al eens slachtoffer te zijn geweest (10%). Laagopgeleiden maken zich vaker zorgen omdat ze van zichzelf vinden dat ze te weinig verstand hebben van online veiligheid (25%).

Waarom maak je je zorgen als het gaat om jouw online/digitale veiligheid in je privésituatie?	Maakt zich zorgen (n=475)
Internetcriminelen zijn steeds slimmer met hun aanpak/je hebt het niet door	48%
Dat mensen in mijn gegevens kunnen kijken/misbruik van maken	47%
Dat mijn financiële gegevens worden gestolen	44%
Dat mijn computer niet meer werkt en ik nergens meer bij kan	37%
Dat mijn persoonlijke gegevens worden gestolen	32%
Omdat het vaak voorkomt dat mensen slachtoffer zijn van cybercrime	27%
Dat mijn geld wordt gestolen	23%
Dat mensen zich online voordoen als mij	21%
Dat mijn beveiliging niet op orde is	20%
Ik heb weinig verstand van digitale veiligheid	16%
Omdat ik voor mijn beveiliging afhankelijk ben van anderen	15%
Omdat ik anderen hier vaak over hoor	12%
Ik let niet altijd goed op	8%
Ik ben al eens slachtoffer geweest van internetcriminaliteit	5%
Anders	1%
Weet niet	2%

Zorgen

Nederlanders die zich (zeer) weinig zorgen maken gaan actief om met het beveiligen van hun online veiligheid

Nederlanders die zich weinig zorgen maken om online veiligheid (50%) maken zich weinig zorgen omdat ze controleren op valse websites en links (43%), hun apparaten updaten (43%), regelmatig virusscans uitvoeren (42%), zichzelf geen aantrekkelijk doelwit voor criminelen vinden (38%), menen dat hun beveiliging goed op orde is (37%) en omdat ze voor verschillende apparaten en accounts verschillende wachtwoorden hebben (34%).

Verschillen binnen Nederland

Mannen die zich geen zorgen maken om hun online veiligheid geven vaker aan dan vrouwen die zich geen zorgen maken om hun online veiligheid, dat zij websites en links te controleren (50% vs. 35%), hun apparaten te updaten (49% vs. 36%), dat hun beveiliging goed op orde is (44% vs. 30%), veel verschillende wachtwoorden hebben (38% vs. 29%) en regelmatig back-ups maken (33% vs. 22%).

Laagopgeleiden die zich geen zorgen maken om hun online veiligheid geven minder vaak dan anderen die zich geen zorgen maken om hun online veiligheid aan dat zij back-ups te maken (18%). Middelbaar opgeleiden geven minder vaak aan dat zij websites en links controleren (37%).

Waarom maak je je (zeer) weinig zorgen als het gaat om jouw online/digitale veiligheid in je privésituatie?	Maakt zich geen zorgen (n=504)
Ik controleer altijd op valse websites en valse links	43%
Ik update altijd mijn apparaten	43%
Ik doe regelmatig een virusscan	42%
Ik ben geen aantrekkelijk doelwit voor criminelen	38%
Ik heb mijn beveiliging goed op orde	37%
Ik heb voor veel van mijn apparaten en accounts een ander wachtwoord	34%
Ik maak regelmatig back-ups van mijn gegevens	27%
Ik heb lange wachtwoorden	27%
Ik heb niks te verbergen	22%
Ik verwissel vaak van wachtwoord	18%
Ik heb niks te verbeteren	2%
Anders	6%
Weet niet	4%

Zorgen
Weinig zorgen om cyberaanvallen

6% van de Nederlanders maakt zich (zeer) grote zorgen dat ze te maken krijgen met een cyberaanval. Meerderheid 56% maakt zich in beperkte mate zorgen en 28% niet of in beperkte mate.

Wanneer mensen het gevoel hebben dat ze zelf weinig risico lopen, zullen ze zich weinig geroepen voelen om zich meer te beschermen tegen cyberaanvallen.

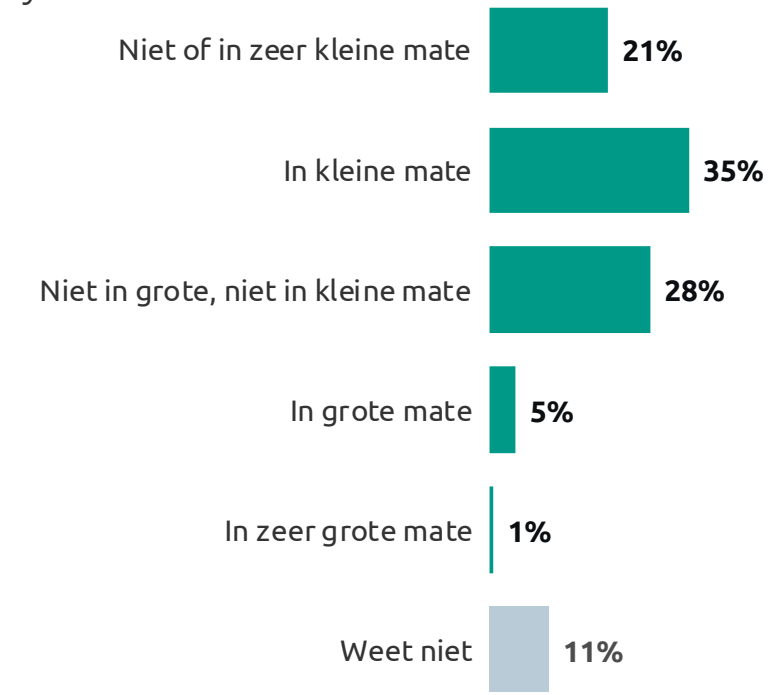
Voor deze resultaten is er geen vergelijking met voorgaande jaren beschikbaar, omdat er toen andere schalen zijn gebruikt (nooit, soms, regelmatig en altijd).

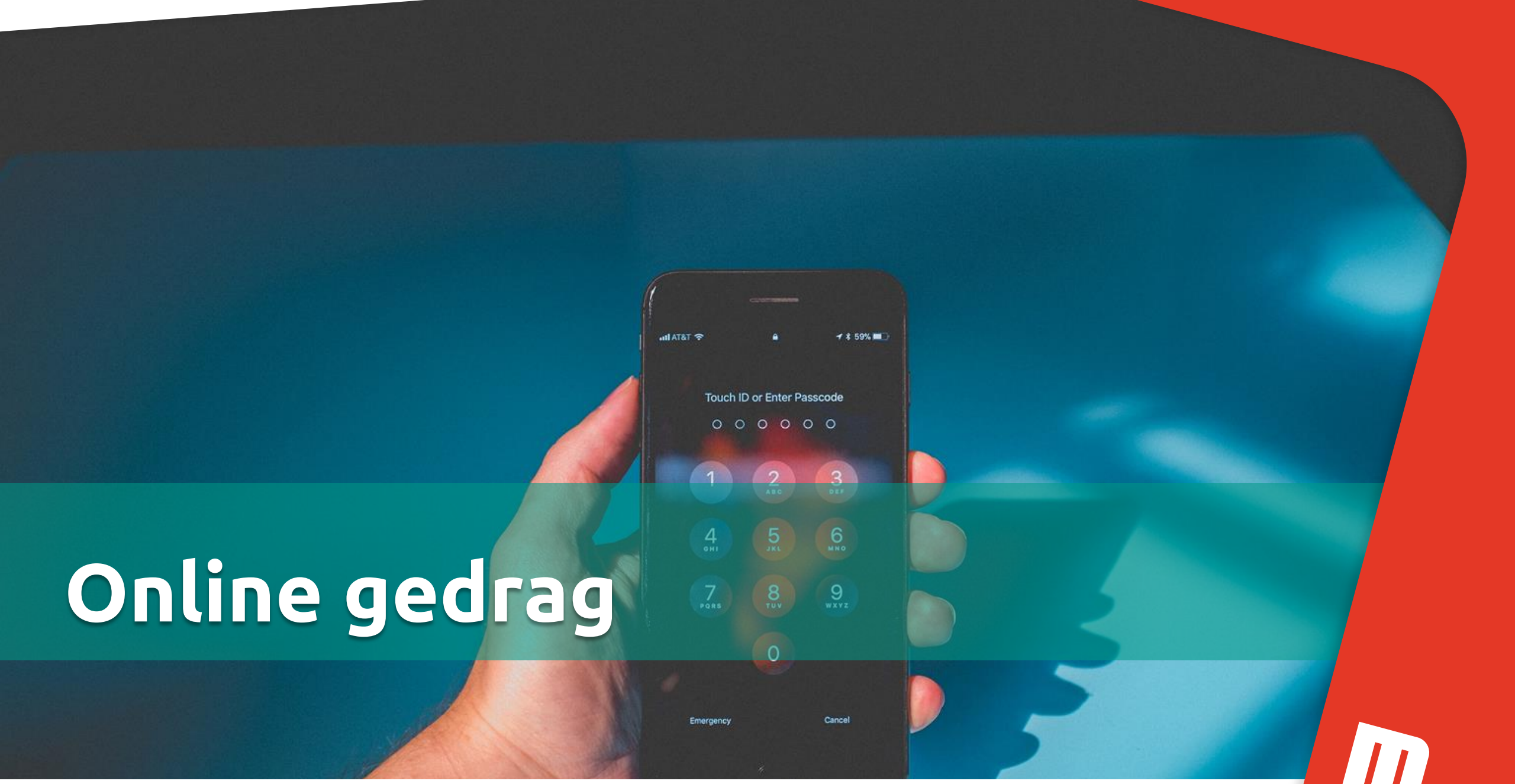
Verschillen binnen Nederland

- Mannen geven vaker aan zich niet of in (zeer) kleine mate zorgen te maken om een cyberaanval dan vrouwen (60% vs. 52%).
- Jongeren maken zich vaker minder zorgen om cyberaanvallen (16 t/m 24 jaar: 61%; 25 t/m 34 jaar: 67%).
- Hoogopgeleiden maken zich vaker minder zorgen om cyberaanvallen (64% vs. 46% onder laagopgeleiden).

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

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





Online gedrag

Online gedrag

Meesten maken thuis gebruik van een netwerkverbinding met wachtwoord

In de afgelopen 12 maanden heeft 48% van werkend Nederland (ook) thuisgewerkt, 57% heeft (ook) op kantoor gewerkt en 26% heeft (ook) op een openbare plek gewerkt. Dit onderzoek is uitgevoerd tijdens de coronacrisis. Veel Nederlanders moesten vanwege de coronamaatregelen vanuit huis werken.

18% heeft (ook) op een andere plek dan thuis, het kantoor of een openbare plek gewerkt (dit wordt niet in het figuur hiernaast getoond).

De meeste maken, ongeacht hun werklocatie, verbinding via een (wifi)netwerkverbinding met een wachtwoord. Nederlanders die thuis of kantoor werken maken daarnaast ook weleens gebruik van een VPN verbinding en/of cloud verbinding (18%). Nederlanders die op een openbare plek werken, maken ook weleens gebruik van een netwerkverbinding zonder wachtwoord (18%) of van een hotspotverbinding (15%).

Op welk van onderstaande locaties heb je in de afgelopen 12 maanden gewerkt (denk hierbij ook aan 'nieuwe' werkplekken door het coronavirus)? (Basis - Werkend, n=477

Thuis	Kantoor	Openbare plek
48%	57%	26%

Van wat voor netwerkverbinding maak je dan gebruik

	n=230	n=272	n=124
Een (wifi-)netwerkverbinding met wachtwoord	78%	67%	44%
Een (wifi-)netwerkverbinding zonder wachtwoord	2%	4%	18%
Een VPN verbinding en/of cloud verbinding ('in de cloud werken')	18%	18%	5%
Een hotspot verbinding (3G/4G) via mijn smartphone of tablet	1%	1%	15%
Anders	-	1%	10%
Weet ik niet	1%	8%	7%

Online gedrag

Helft heeft geen beeld bij veilig online gedrag op werk of in een privésituatie

Het beeld dat Nederlanders spontaan hebben van veilig online gedrag op werk of in de privé situatie is erg divers. Zie de volgende pagina voor de resultaten.

Het meest top of mind veilig online gedrag op het werk is bij Nederlanders; verdachte mails herkennen (8%), een VPN-verbinding gebruiken (6%) en niet op onbekende links klikken (6%).

Voor de privésituatie noemen Nederlanders het meest antivirus software gebruiken (15%), alert blijven/Bewust zijn van de gevaren (10%) en verdachte mails herkennen (9%).

De meesten kunnen zelf niet beschrijven wat veilig online gedrag is (op werk: 57%; privé: 52%).

Werk

Privé

Online gedrag

Geen consensus over wat veilig online gedrag is

Waar denk jij in eerste instantie aan bij veilig online gedrag…*	…op je werk	…in een privésituatie
Verdachte mails herkennen	8%	9%
VPN-verbinding gebruiken (waarmee internetverkeer versleuteld wordt verstuurd)	6%	2%
Niet op onbekende links klikken	6%	9%
Sterke wachtwoorden gebruiken/Wachtwoorden regelmatig veranderen	6%	10%
Alert blijven/Bewust zijn van de gevaren	6%	10%
Geen onbekende/onbetrouwbare sites bezoeken	5%	5%
Gebruik van antivirus software	5%	15%
Alleen werkgerelateerd gebruik/Geen privé zaken	4%	0%
Wachtwoorden (algemeen)	4%	2%
Beveiliging wordt geregeld door ICT/IT afdeling	4%	0%
Computer vergrendelen (bij het weggaan)	4%	1%
Wachtwoorden veilig beheren en bewaren (eventueel met hulp van een wachtwoordmanager)	3%	3%
Niet zomaar dingen downloaden	3%	1%
Firewall installeren	3%	2%

Waar denk jij in eerste instantie aan bij veilig online gedrag…*	…op je werk	…in een privésituatie
Tweestapsverificatie toepassen	2%	1%
Regelmatig back-ups maken van mijn bestanden	2%	2%
Bij website-adressen checken of het een https-verbinding is	1%	4%
Geen persoonlijke gegevens delen online	1%	8%
Verschillende wachtwoorden gebruiken	1%	6%
Software regelmatig updaten	1%	4%
Veilig online bankieren	1%	3%
Voorzichtig omgaan met openbare wifi-netwerken	1%	1%
Cookies uitschakelen	0%	1%
Een adblocker gebruiken	0%	1%
Anders	7%	6%
Weet niet/geen antwoord	57%	52%

*Deze vraag is open gesteld en achteraf gecodeerd

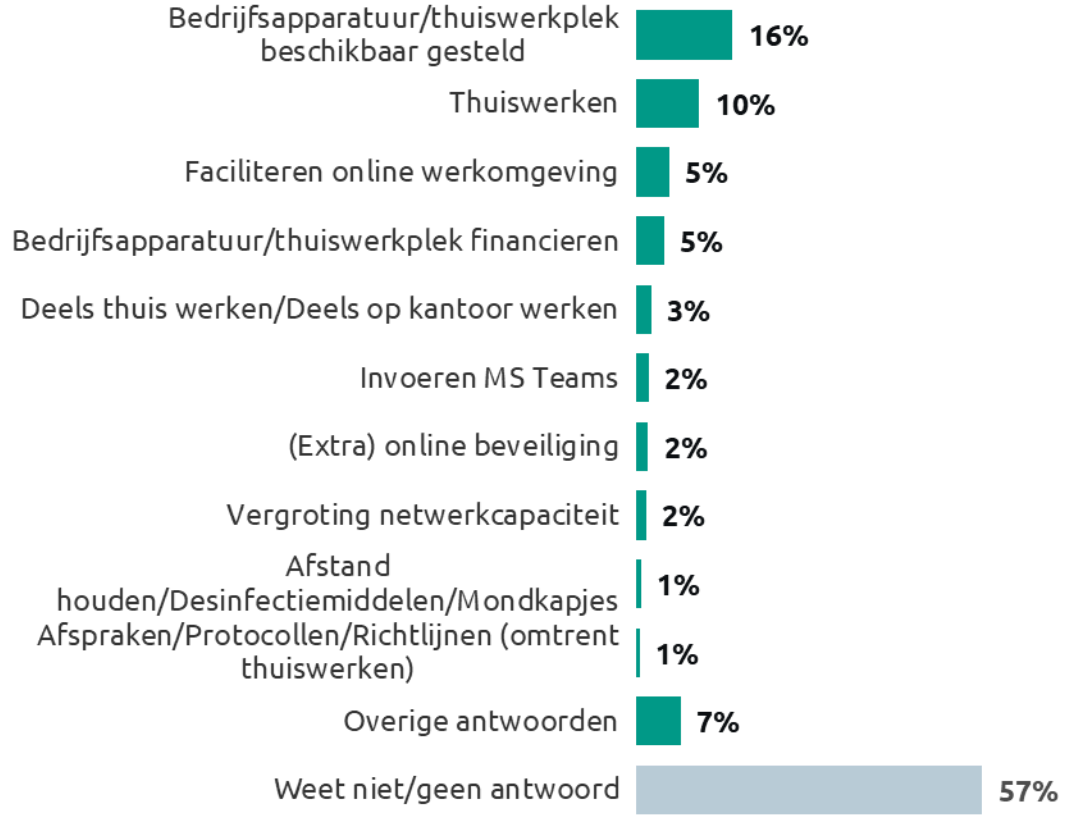
Online gedrag

Meer dan de helft kan geen maatregelen noemen die de werkgever heeft getroffen sinds het begin van de coronacrisis om thuis te werken

Bijna zes op de tien (57%) Nederlanders die in de afgelopen 12 maanden weleens hebben thuis gewerkt kunnen geen speciale maatregelen noemen die hun werkgever heeft getroffen sinds het begin van de coronacrisis.

Degenen die wel maatregelingen kunnen noemen, hebben het vaak over het beschikbaar stellen van bedrijfsapparatuur (om de thuiswerkplek in te richten, 16%). Verder wordt thuiswerken zelf als speciale maatregel van de werkgever genoemd.

Heeft jouw werkgever speciale maatregelen getroffen sinds het begin van de coronacrisis wat betreft thuiswerken en wat voor maatregelen?*
(Basis - Werkt thuis, n=230)



*Deze vraag is open gesteld en achteraf gecodeerd

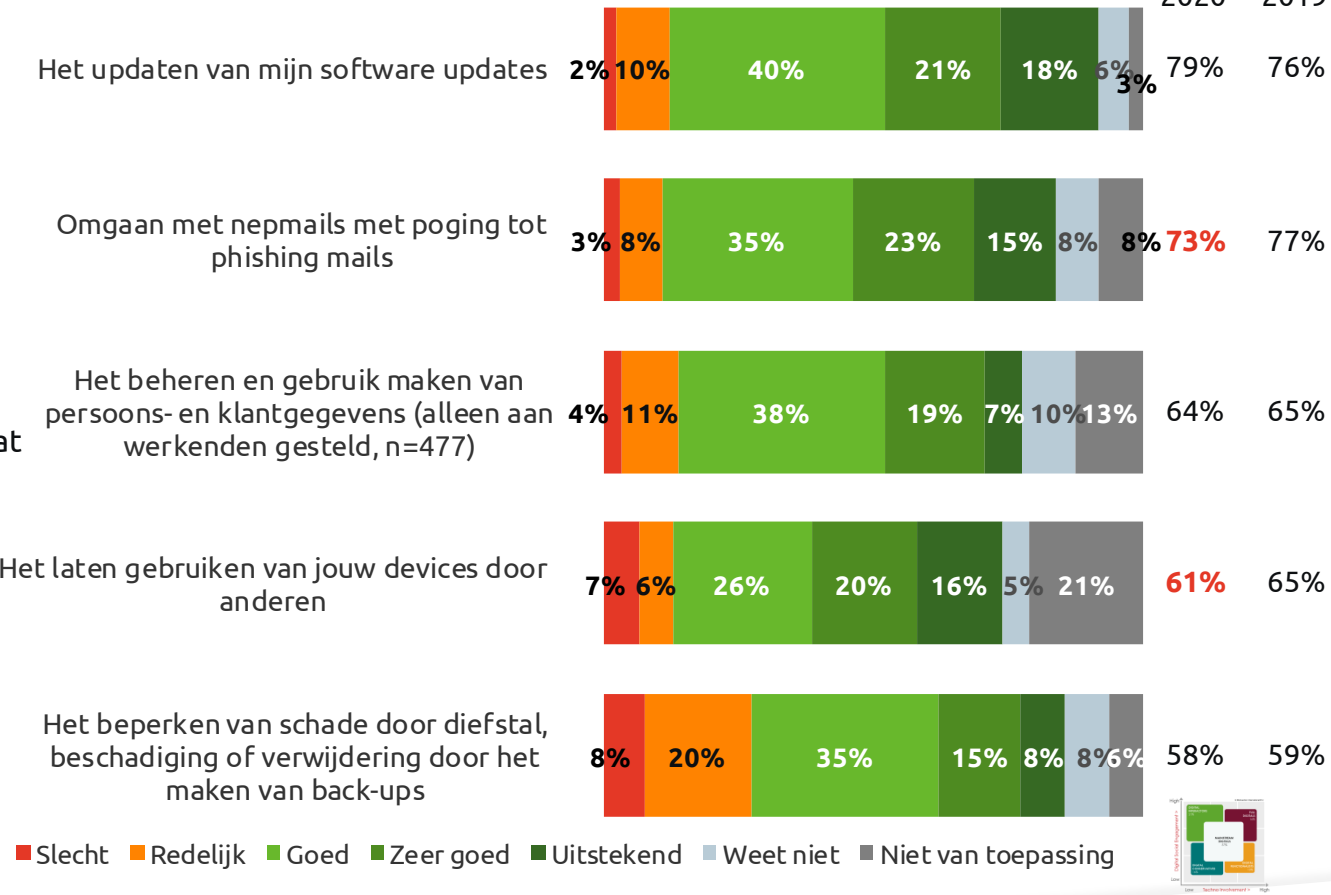
Online gedrag
Nederlanders gaan minder goed om met phishingmails dan vorig jaar

De meeste Nederlanders oordelen dat zij (zeer) veilig omgaan met verschillende digitale zaken. In vergelijking met vorig jaar vinden minder Nederlanders dat ze goed met phishing mails (73% vs. 77%) en hun devices (61% vs. 64%) omgaan.

Verschillen binnen Nederland

- Mannen vinden vaker dan vrouwen dat ze zeer goed tot uitstekend omgaan met software updates (50% vs. 29%), phishingmails (41% vs. 35%), beheren en gebruiken van gegevens (30% vs. 19%), gebruik van eigen devices door anderen (43% vs. 28%) en het maken van back-ups (28% vs. 19%).
- Jongeren (t/m 24 jaar) vinden vaker dan de rest van de Nederlanders dat ze zeer goed tot uitstekend omgaan met phishingmails (46%), met software updates (49%) en het laten gebruiken van hun devices door anderen (55%). Jongeren van 16 t/m 34 vinden vaker dat ze zeer goed tot uitstekend omgaan met het maken van back-ups (31%).
- Hoogopgeleiden vinden dat ze vaker zeer goed tot uitstekend omgaan met phishing mails (43% vs. 31% onder laagopgeleiden) en het laten gebruiken van de eigen devices door anderen (46% vs. 20% onder laagopgeleiden). Hoogopgeleiden vinden vaker dat ze het redelijk tot slecht doen met het maken van back-ups (33%).

Er zijn een aantal zaken die je kunt doen om veilig online te gaan. Hoe ga je om met de volgende zaken?
(Basis – Nederland representatief, n=1.022)



Rood = significant lager dan in 2019

Online gedrag

Minder zeker als het gaat om het geven van toestemmingen online, gebruik van een USB-stick, wifiverbindingen onderweg en het werken in de cloud

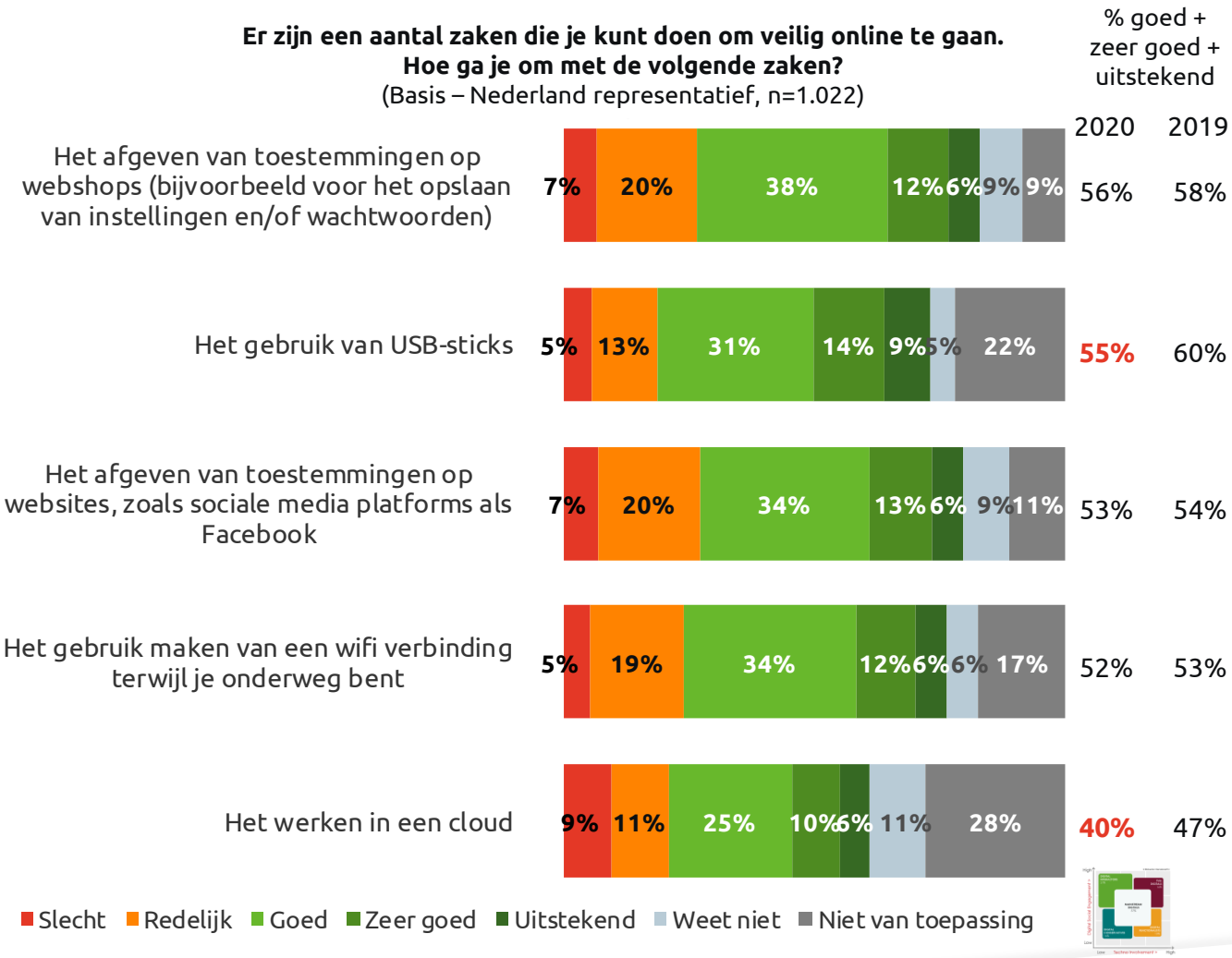
Nederlanders zijn wat minder zeker over hun gedrag als het gaat om het afgeven van toestemmingen op webshops of websites, het gebruik van USB-sticks, het gebruik van wifiverbindingen en werken in de cloud.

In vergelijking met vorig jaar vinden Nederlanders dit jaar dat ze minder goed omgaan met USB-sticks (55% vs. 60%) en met het werken in de cloud (40% vs. 47%).

Verschillen binnen Nederland

- Mannen beoordelen zichzelf hoger op het gebruik van wifiverbindingen (24% vs. 13%), gebruik van een USB-stick (29% vs. 18%), afgeven van toestemmingen (website: 22% vs. 16% en webshop: 23% vs. 14%) en werken in de cloud (21% vs. 11%).
- Jongeren (t/m 24 jaar) vinden vaker dat ze goed omgaan wifi-verbindingen (32%), gebruik van een USB-stick (31%), afgeven van toestemmingen (website: 25%; webshop: 29%) en werken in een cloud (26%).
- Hoogopgeleiden vinden dat ze vaker zeer goed omgaan met wifiverbindingen (24%) en afgeven van toestemmingen bij websites (24%), maar juist slechter bij webshops (slecht tot redelijk: 31%). Laagopgeleiden weten vaker niet hun gedrag te beoordelen.

Er zijn een aantal zaken die je kunt doen om veilig online te gaan. Hoe ga je om met de volgende zaken?
(Basis – Nederland representatief, n=1.022)



Rood = significant **lager** dan in 2019

Online gedrag

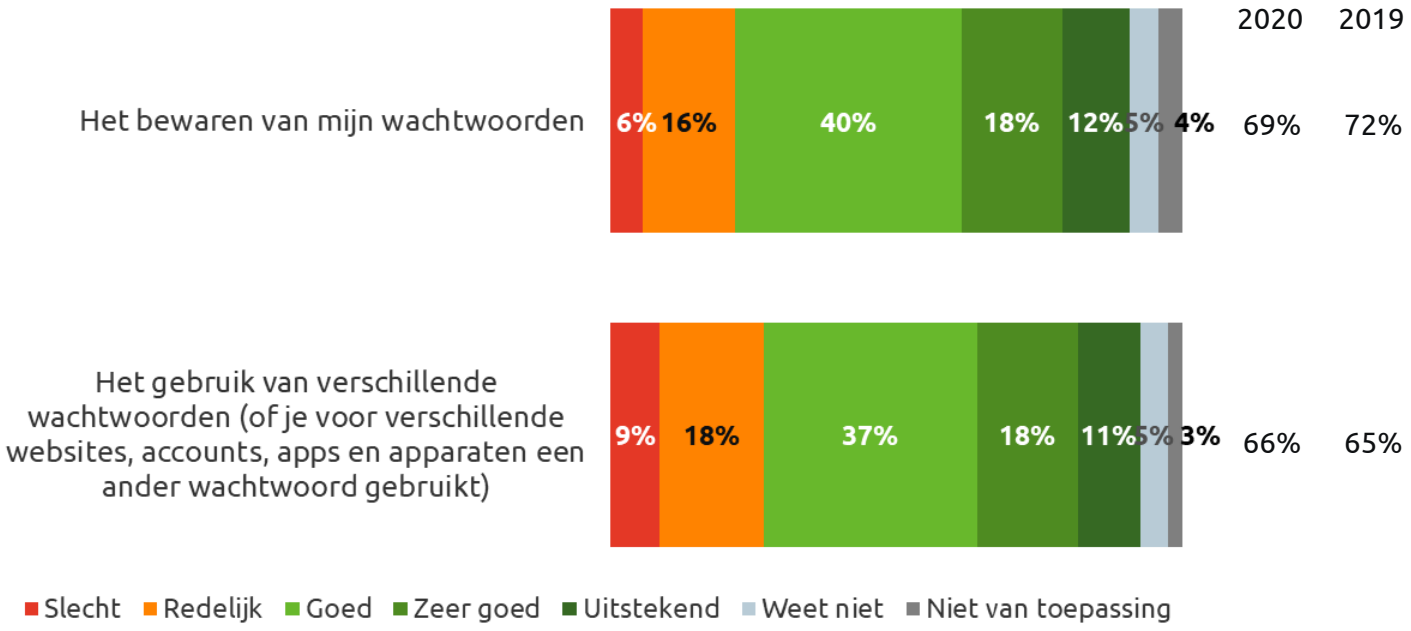
Meerderheid van de Nederlanders vindt dat ze goed omgaan met het gebruik van verschillende wachtwoorden

Zeven op de tien Nederlanders (69%) vinden dat ze goed omgaan met het bewaren van hun wachtwoorden. Een op de vijf (22%) schatten in dat ze het onvoldoende doen. Verder vindt een merendeel dat ze goed tot uitstekend om gaan met het gebruik van verschillende wachtwoorden (66%). 27% schat in dat ze dat niet zo goed doen.

Verschillen binnen Nederland

- Mannen vinden vaker dat ze zeer goed tot uitstekend omgaan met het bewaren van hun wachtwoorden (34% vs. 25%) en het gebruik van verschillende wachtwoorden (34% vs. 23%).
- Jongeren (t/m 24 jaar) vinden vaker dat ze zeer goed tot uitstekend omgaan met het bewaren van hun wachtwoorden (44%).
- Hoogopgeleiden vinden dat ze vaker zeer goed tot uitstekend omgaan met het bewaren van hun wachtwoorden (46%), maar geven vaker aan dat ze het redelijk tot slecht doen als het gaat om het gebruik van verschillende wachtwoorden (32%).

Er zijn een aantal zaken die je kunt doen om veilig online te gaan. Hoe ga je om met de volgende zaken?
(Basis – Nederland representatief, n=1.022)



Rood = significant lager dan in 2019

Online gedrag
Drie op de tien gebruikt standaard routerwachtwoord

Aan de Nederlanders die thuiswerken en met een wachtwoord verbinding maken met hun netwerk is een aantal verdiepende vragen gesteld over het wachtwoord. Drie op de tien thuiswerkers gebruiken het standaard routerwachtwoord (29%) en 67% heeft zelf een wachtwoord verzonnen.

Is dit wachtwoord een zelfverzonnen wachtwoord door jou of een huisgenoot of is dit het standaardwachtwoord van de router?
(Basis - Gebruikt thuis een netwerkverbinding met wachtwoord, n=179)

Zelfverzonnen wachtwoorden bestaan vooral uit kleine letters (79%), hoofdletters (72%) en cijfers (71%). Circa de helft maakt ook gebruik van bijzondere karakters (zoals #) (54%) en leestekens (49%). 40% geeft aan dat hun zelfverzonnen wachtwoord minimaal 12 tekens bevat.

Op de volgende pagina is te zien in welke mate Nederlanders gebruik maken van de combinaties van de 6 opties voor het wachtwoord van de router.

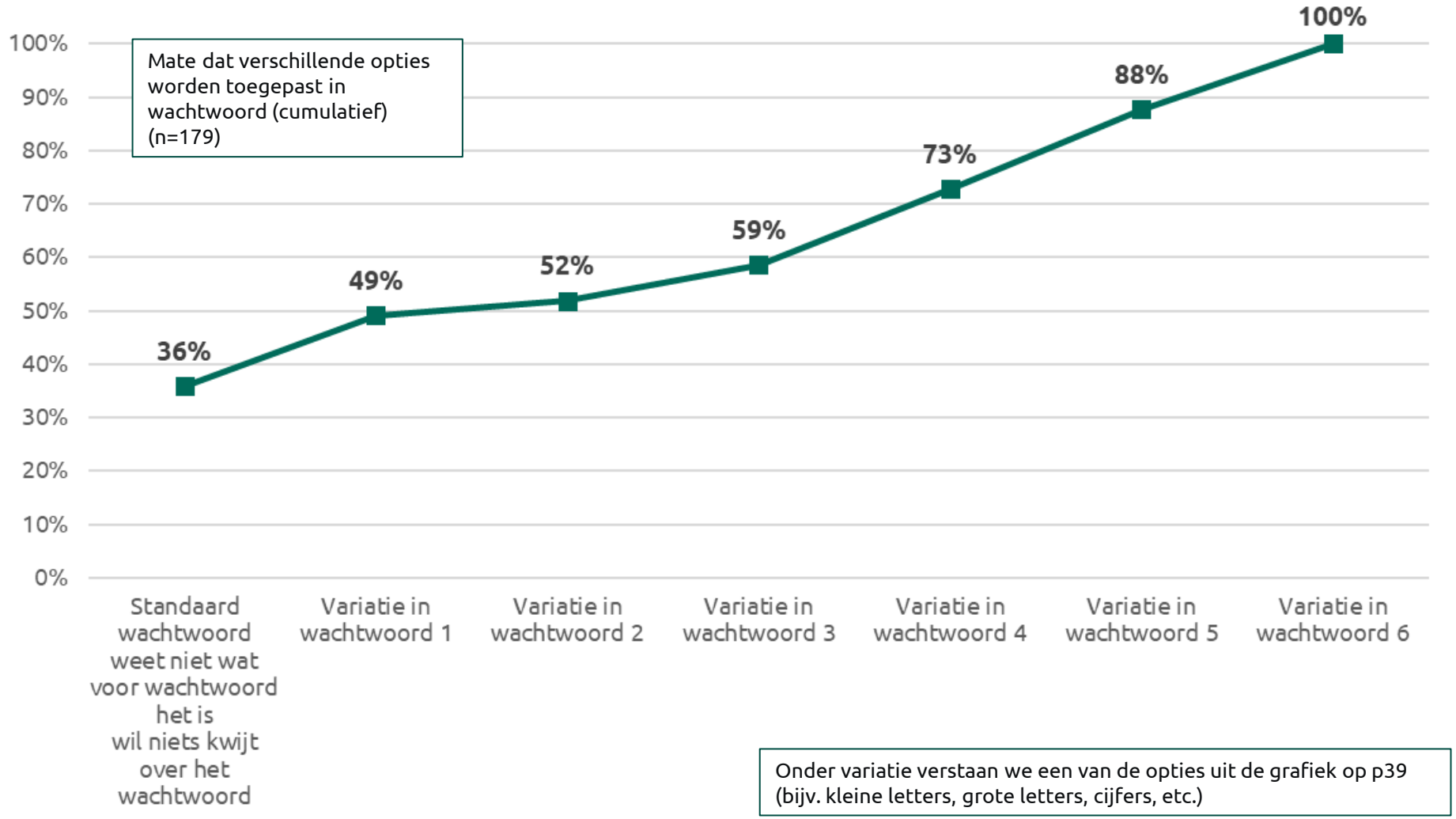
Welke van onderstaande opties is van toepassing op jouw wachtwoord voor de router? (Basis - Wachtwoord is zelfverzonnen, n=119)

Online gedrag

Aantal opties dat gebruikt wordt bij het routerwachtwoord

Op de vorige pagina worden 6 mogelijke opties gegeven om de routerwachtwoord veiliger te maken.

In de grafiek rechts is cumulatief te zien in hoeverre men het aantal wachtwoordopties gebruikt maakt.



Onder variatie verstaan we een van de opties uit de grafiek op p39 (bijv. kleine letters, grote letters, cijfers, etc.)

Online gedrag

Meeste Nederlanders vinden dat ze goed op de hoogte zijn van online gevaren en alles goed op orde hebben

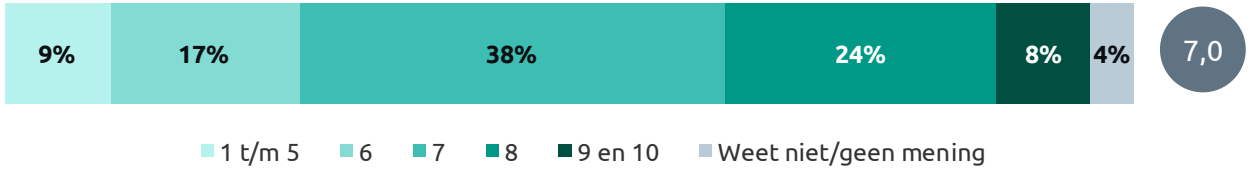
Een op de tien (9%) geeft zichzelf een *on*voldoende als het gaat om het veilig omgaan met online gevaren. De meesten (87%) geven zichzelf een (goede) voldoende. 32% geeft zichzelf zelfs een 8 of hoger. Het gemiddelde cijfer is gelijk aan vorig jaar (7,0).

Redenen waarom men zichzelf een *on*voldoende geeft is omdat ze vinden dat ze te weinig verstand hebben van online gevaren (37%), om dat ze er niet bewust mee bezig zijn (27%) en omdat er altijd ruimte voor verbetering is (14%). Redenen waarom men zichzelf een voldoende geeft is omdat ze vinden dat ze goed op de hoogte zijn (30%), alert zijn op gevaren (20%) en er (altijd) ruimte is voor verbetering (13%).

Verschillen binnen Nederland

- Mannen geven zichzelf gemiddeld een hoger cijfer (7,2).
- Nederlanders tussen de 25 en 34 jaar geven zichzelf gemiddeld een lager cijfer (6,8).

Welk cijfer geef jij jezelf als het gaat om het veilig omgaan met online gevaren? (Basis - Nederland representatief, n=1.022)



Kun je toelichten waarom je jezelf een onvoldoende geeft? (n=96) (Top 5*)

37%	Ik heb er weinig verstand van
27%	Ik ben hier niet bewust mee bezig/Ik ben (soms) te laks
14%	Er is (altijd) ruimte voor verbetering
3%	Volledige veiligheid is onhaalbaar/kost te veel moeite
3%	De online wereld/criminaliteit verandert constant

Kun je toelichten waarom je jezelf een voldoende geeft? (n=887) (Top 5*)

30%	Ik ben goed op de hoogte/ Ik heb alles op orde
20%	Ik ben alert/bewust van de gevaren/voorzichtig
13%	Er is (altijd) ruimte voor verbetering
8%	Ik ben hier niet bewust mee bezig/Ik ben (soms) te laks
6%	Ik kan verdachte mails herkennen

*Deze vraag is open gesteld en achteraf gecodeerd.
Zie de bijlage voor het volledige overzicht.

Online gedrag

Nederlanders ondernemen veel verschillende acties om de eigen online veiligheid te verbeteren

Met name het gebruiken en regelmatig updaten van antivirussoftware (58%) worden gebruikt, net als het doen van (beveiligings-)updates (51%) en het controleren van links (50%). Met name het gebruiken en regelmatig updaten van antivirussoftware (58%) worden gebruikt, net als het doen van (beveiligings-) updates (51%) en het controleren van links (50%). 44% voert software updates meteen uit en 42% maakt regelmatig back-ups van bestanden. Dit zijn ook de acties waarvan men aangeeft ze te willen doen om de eigen online veiligheid te verbeteren.

61% geeft aan dat de acties die zij reeds hebben ondernomen, ook de acties zijn die zij bereid zijn om te doen om hun online veiligheid te verbeteren.

Een vergelijking met voorgaande jaren is niet mogelijk omdat de basis anders is (‘allen’ vs. ‘heeft behoefte aan verbetering online veiligheid’).

Welke van de onderstaande acties […] om jouw online veiligheid te verbeteren? (Basis – Nederland representatief, n=1.022)	**Heb je ondernomen**	**Zou je bereid zijn om te doen**
Antivirussoftware gebruiken en regelmatig updaten	58%	48%
Regelmatig (beveiligings)updates doen	51%	43%
Controleren op welke links ik klik	50%	40%
Direct software updates uitvoeren	44%	39%
Regelmatig back-ups maken van al mijn bestanden	42%	40%
Mijn wachtwoorden regelmatig veranderen	33%	33%
Geen gebruik maken onbeveiligde sites om bestanden uit te wisselen	33%	35%
Een firewall installeren	32%	35%
Lange wachtwoorden/wachtzinnen gebruiken van minimaal 12 tekens.	32%	31%
Geen gebruik maken van openbare wifi-netwerken	30%	31%
Het standaard wachtwoord van mijn wifi modem veranderen (in een sterk en uniek wachtwoord)	24%	30%
Steeds nieuw wachtwoord gebruiken dat ik nog niet eerder gebruikt heb	23%	26%
Extensies aan je webbrowser toevoegen om cookies, advertenties en automatisch toegang tot Javascripts te blokkeren	16%	25%
Een wachtwoordmanager gebruiken	15%	19%
Altijd gebruik maken van een VPN-verbinding	12%	19%
Informatie op internet opzoeken over hoe ik veiliger kan worden	10%	23%
Een specialist inhuren die bij mij thuis langskomt om de digitale veiligheid te verbeteren installeren (denk b	5%	9%
Jaarlijks een digitale apk laten uitvoeren	4%	15%
Geen van bovenstaande	7%	10%

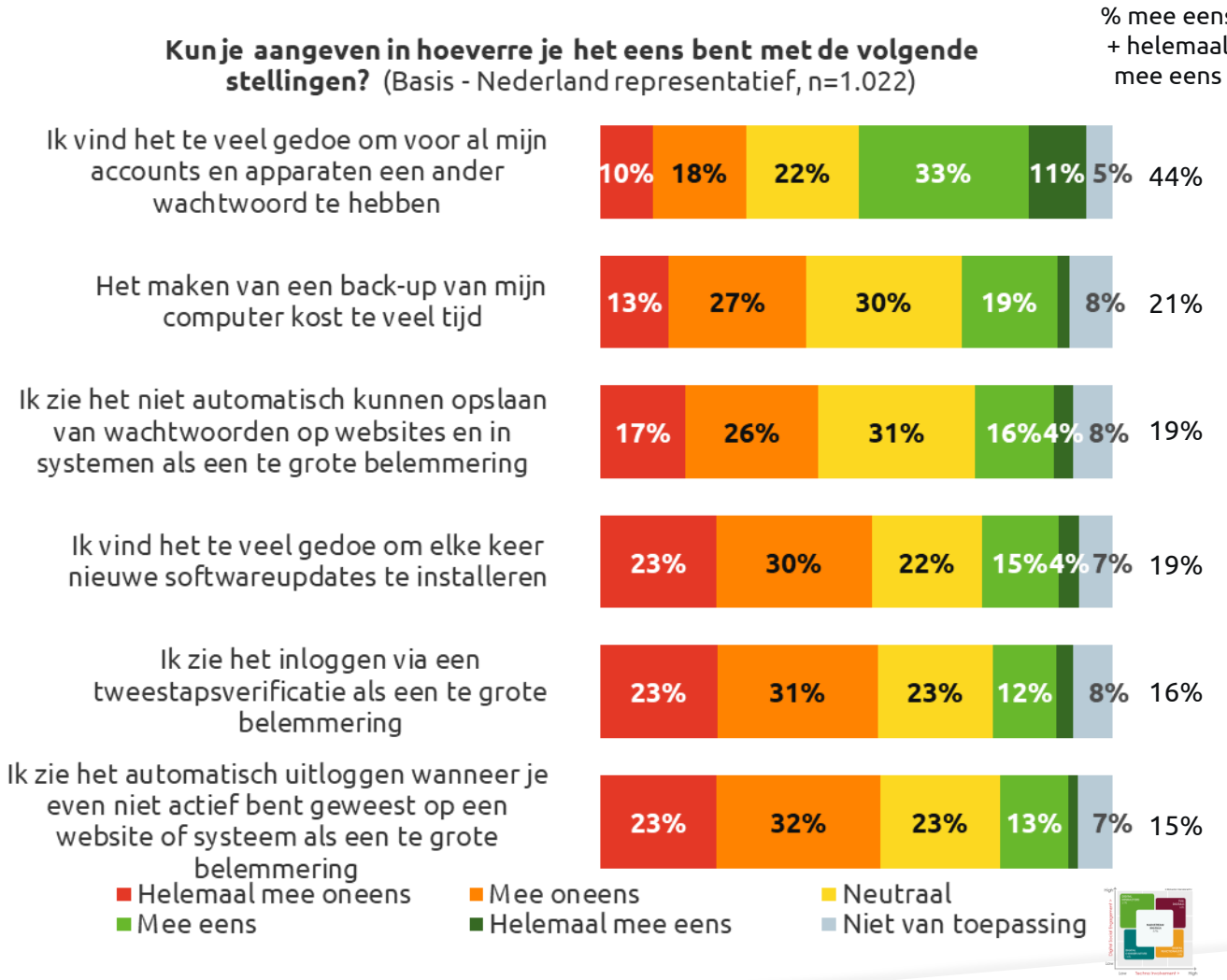
Online gedrag

Vier op de tien vindt het te veel gedoe om overal een ander wachtwoord voor te hebben

Tijd en gemak spelen een relatief kleine rol als het gaat om weerstand. Van de meeste beschreven handelingen die Nederlanders kunnen doen om hun digitale veiligheid te hogen geven Nederlanders aan dat zij hier geen of weinig belemmeringen in ervaren. Nederlanders ervaren echter wel het steeds een ander wachtwoord voor al hun accounts en apparaten als (veel) gedoe (44%).

Verschillen binnen Nederland

- Mannen vinden het maken van een back-up (44% vs. 36%), het installeren van software updates (59% vs. 47%) en het gebruiken van een tweestapsverificatie (59% vs. 50%) minder vaak een belemmering.
- Jongeren (t/m 24 jaar) vinden het automatisch uitloggen vaker een belemmering (22%) en te veel gedoe om nieuwe software updates te installeren (28%). Jongeren (t/m 34 jaar) vinden het vaker te veel gedoe om overal een ander wachtwoord voor te hebben (57%). Nederlanders van 16 t/m 24 en 35 t/m 44 vinden vaker dat het maken van back-ups te veel tijd kost (30% en 32%).
- Hoogopgeleiden ervaren over het algemeen minder belemmeringen en minder gedoe van de beveiligingsmaatregelen. Wel ervaren ze vaker veel gedoe om overal een ander wachtwoord voor te hebben (55%).



Online gedrag

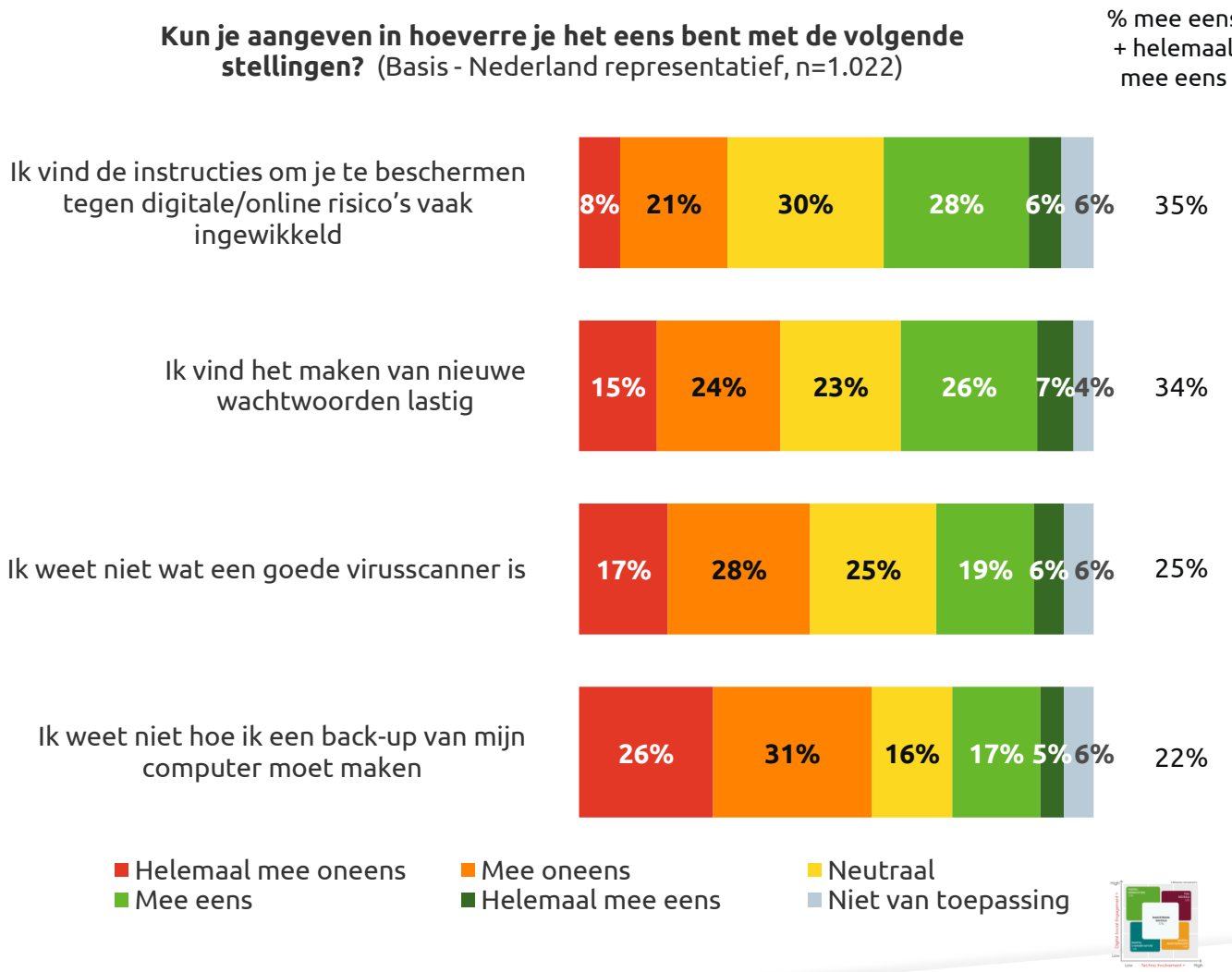
Een kwart tot een derde van de Nederlanders heeft moeite met de complexiteit van online beveiligingsoplossingen

Een derde (35%) van de Nederlanders geeft aan dat zij de instructies om zichzelf te beschermen vaak ingewikkeld vinden. Ook het maken van nieuwe wachtwoorden ervaart men als lastig (34%). Het ontbreekt sommige Nederlanders aan kennis: zij weten niet wat een goede virusscanner is (25%) en niet hoe ze een back-up van de computer moeten maken (22%). Overigens heeft een relatief grote groep Nederlanders hier weinig tot geen moeite mee.

Verschillen binnen Nederland

- Mannen geven vaker aan wel te weten wat een goede virusscanner is en hoe ze een back-up moeten maken. Ook hebben zij minder moeite met veiligheidsinstructies en het maken van nieuwe wachtwoorden.
- Nederlanders tussen de 25 en 34 jaar vinden het lastiger om steeds nieuwe wachtwoorden aan te maken (45%). Jongeren (t/m 34 jaar) weten vaker niet wat een goede virusscanner is (34%) en jongeren (t/m 24) weten vaker niet hoe ze een back-up moeten maken (30%).
- Laagopgeleiden hebben meer moeite met veiligheidsinstructies (44%).

Kun je aangeven in hoeverre je het eens bent met de volgende stellingen? (Basis - Nederland representatief, n=1.022)



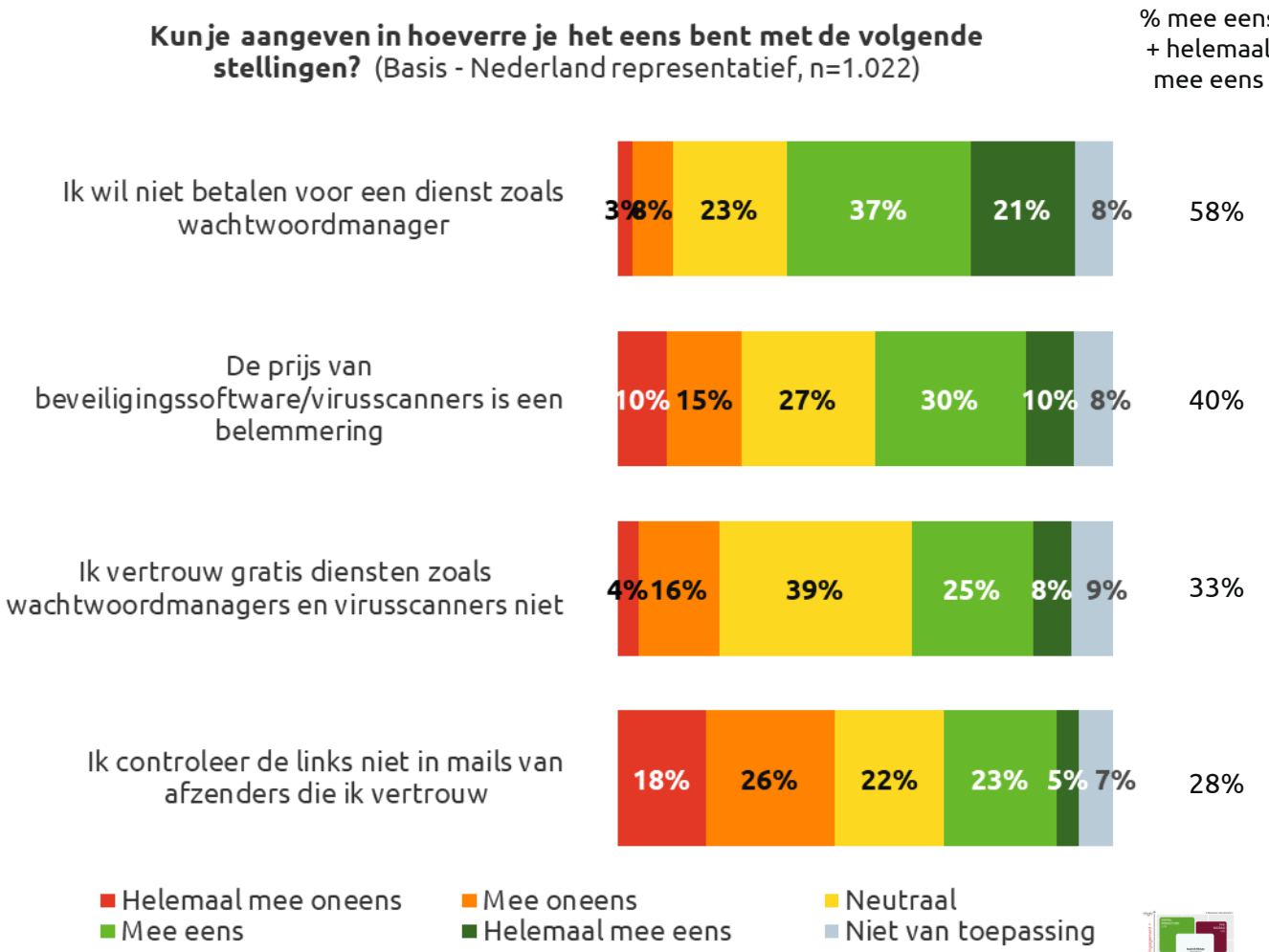
Online gedrag
Voor veel Nederlanders is prijs een belemmering voor online beveiliging

Ruim vier op de tien (44%) Nederlanders geven aan dat ze links in de mails van afzenders die ze vertrouwen controleren. 28% doet dat niet. Een derde van de Nederlanders (33%) vertrouwt gratis diensten zoals wachtwoordmanagers en virusscanners, tegenover 20% die gratis diensten niet vertrouwt. De meeste Nederlanders zouden ook niet betalen voor een dienst als een wachtwoordmanager (58%). Ook vindt 40% de prijs van beveiligingssoftware/virusscanners vaak een belemmering.

Verschillen binnen Nederland

- Mannen geven vaker aan dat ze niet willen betalen voor een dienst (61% vs. 55%) en vaker gratis diensten vertrouwen (25% vs. 16%).
- Prijs voor beveiligingssoftware/virusscanners is voor jongeren vaker een probleem (t/m 24 jaar: 65% en t/m 34 jaar: 55%). Zij staan dan ook wat minder wantrouwend tegenover gratis diensten. Jongeren (t/m 24 jaar) klikken ook vaker op links in mails van afzenders die ze vertrouwen zonder te controleren.

Kun je aangeven in hoeverre je het eens bent met de volgende stellingen? (Basis - Nederland representatief, n=1.022)

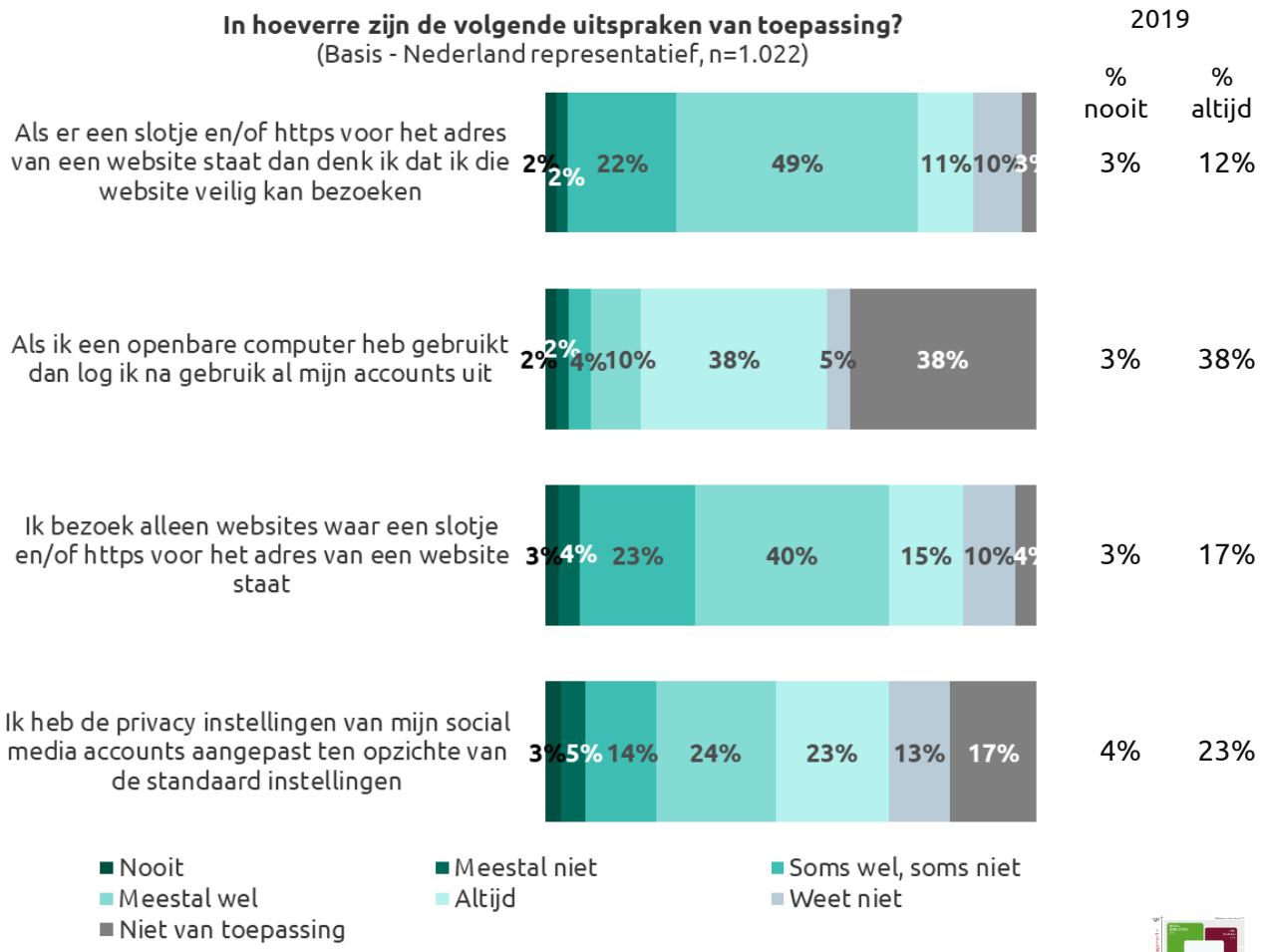


Online gedrag
Helft heeft zijn/haar privacy instellingen van social media accounts aangepast

Circa de helft (48%) van de Nederlanders heeft meestal wel tot altijd zijn/haar privacy instellingen van hun social media accounts aangepast ten opzichte van de standaard instellingen. 8% doet dat meestal niet of nooit. Nederlanders letten verder regelmatig op het slotje voor het webadres. 61% denkt dat een webadres met slotje veilig is en 55% geeft aan vrijwel alleen websites te bezoeken met een slotje.

Bijna drie op de tien (38%) Nederlanders maken geen gebruik van openbare computers. Degenen die dat wel doen (52%) geven aan dat ze vrijwel altijd uitloggen op hun accounts als ze openbare computers hebben gebruikt (48%). Een klein aantal Nederlanders doet dat (bijna) nooit (4%).

We zien geen verschillen in gedragingen ten opzichte van vorig jaar (op basis van % nooit en % altijd).



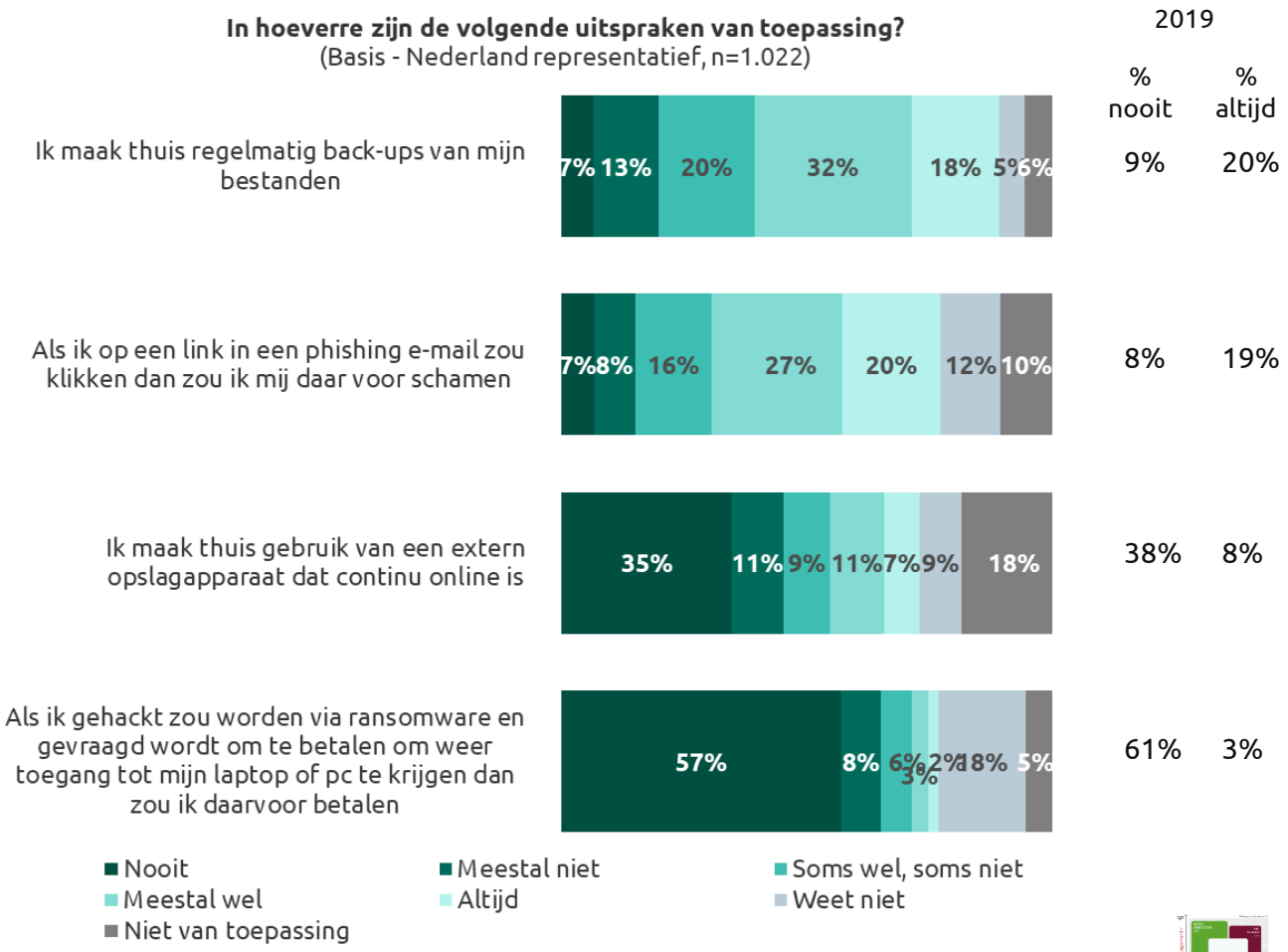
Online gedrag

Meerderheid zou nooit betalen bij via ransomware gehackte computer

Circa zes op de tien (57%) geven aan dat zij *nooit* zouden betalen om hun computer vrij te krijgen als deze gehackt is via ransomware. Een klein aantal Nederlanders (5%) zou meestal wel tot altijd betalen.

50% van de Nederlanders geeft aan dat zij thuis regelmatig back-ups van hun bestanden. 20% doet dat vrijwel niet. Verder geeft 47% aan dat zij zich zouden schamen als zij op een link in een phishing mail zouden klikken. 15% zou dat niet doen.

We zien geen verschillen in gedragingen ten opzichte van vorig jaar (op basis van % nooit of % altijd).

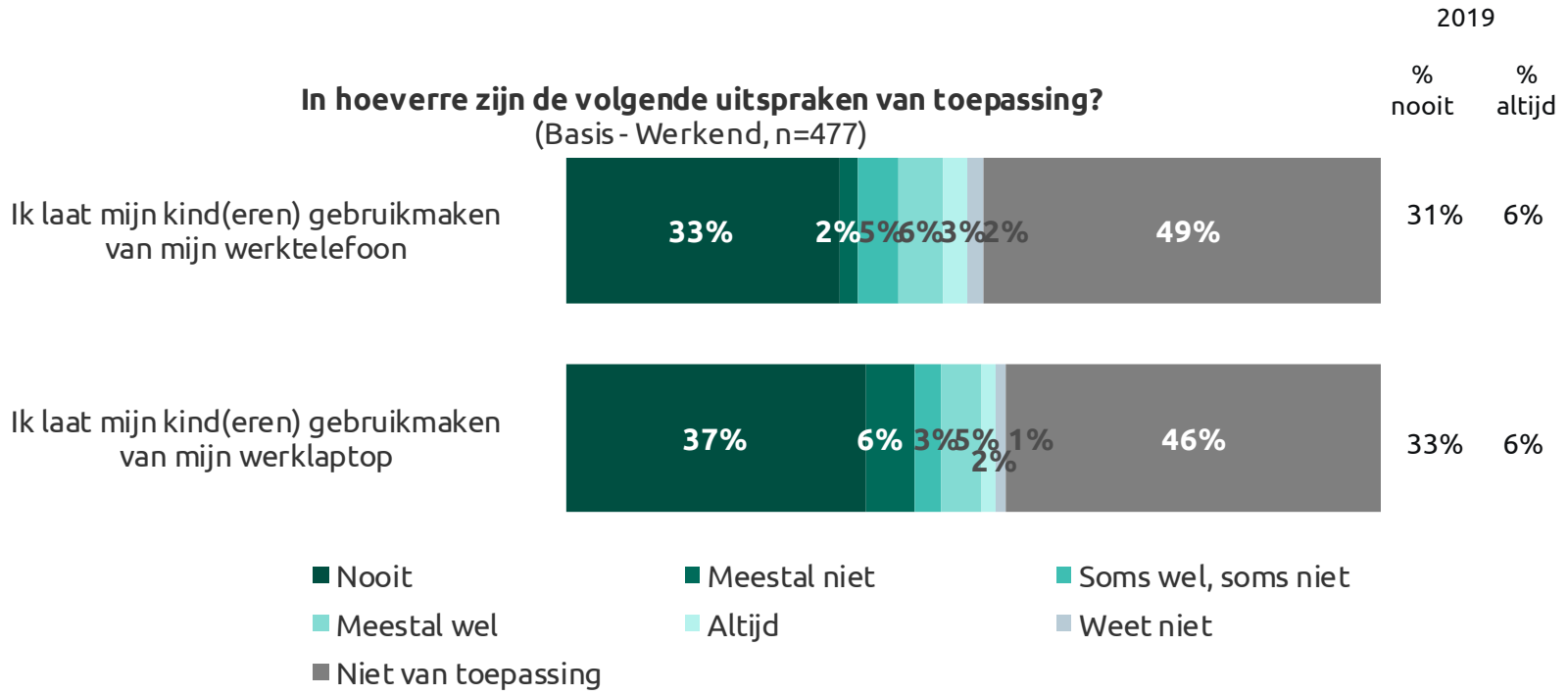


Online gedrag
Ruime meerderheid laat kinderen bedrijfsapparaten nooit gebruiken

Circa de helft geeft aan dat deze stellingen niet van toepassing zijn op hen, aangezien zij óf geen kinderen en/of geen werkapparatuur.

Van degenen die dat wel hebben laat een derde hun kinderen nooit op de apparaten (telefoon: 33%; laptop: 37%).

Dit verschilt niet ten opzichte van vorig jaar (op basis van % nooit en % altijd).



Online gedrag

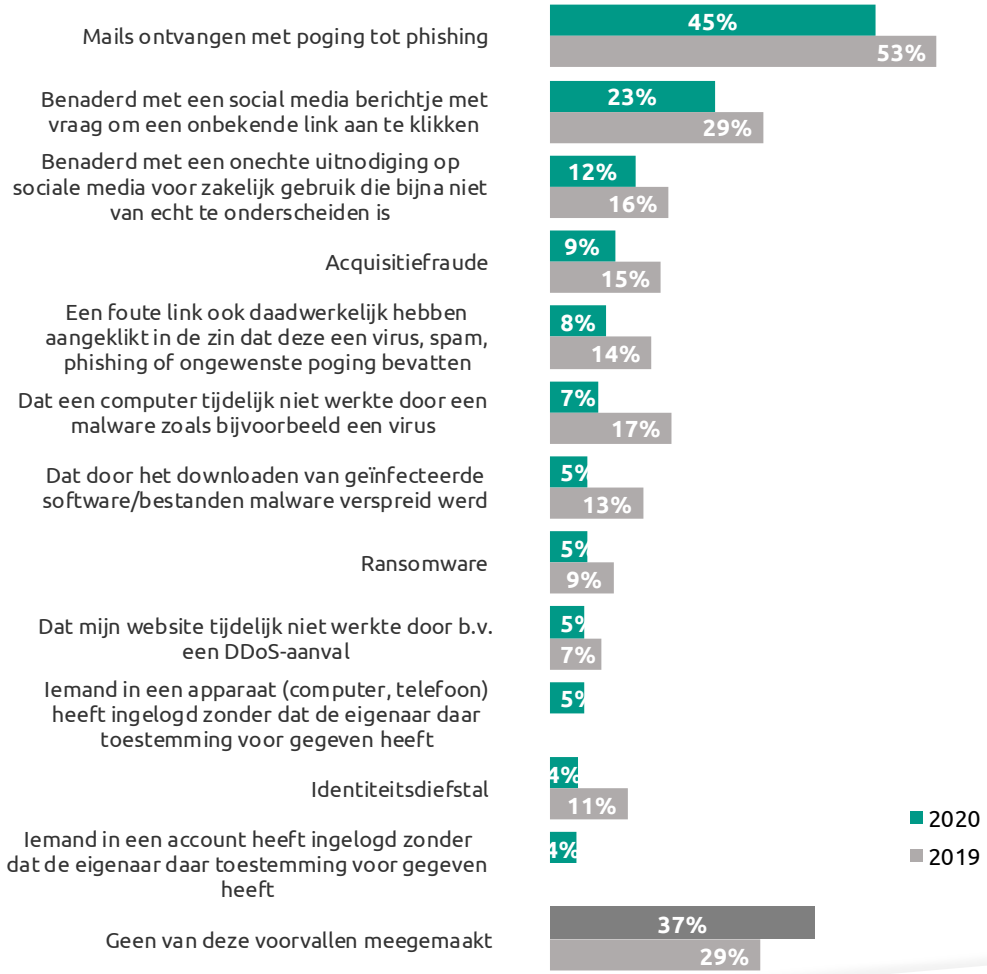
Twee derde is in de afgelopen 12 maanden in aanraking gekomen met een digitaal risico

37% heeft in de afgelopen 12 maanden geen van de voorgelegde voorvallen meegemaakt.

Degenen die wel een voorval hebben gemaakt (63%), komen met name in aanraking met phishing (45%). Een kwart (23%) is op social media benaderd met de vraag om op een onbekende link te klikken.

Er lijkt een dalende trend zichtbaar ten opzichte van 2019, echter zijn dit geen significante verschillen; Nederlanders zijn dit jaar, in vergelijking met 2019, met net zoveel digitale risico's in aanraking gekomen.

Heb je in een privésituatie in de afgelopen 12 maanden weleens te maken gehad met één van de onderstaande voorvallen?
(Basis - Nederland representatief; 2020 n=1.022; 2019 n=1.004)



Online gedrag

Een derde van de Nederlanders die in de afgelopen 12 maanden te maken kreeg met een digitaal risico heeft geen maatregelen getroffen

Men is n.a.v. een voorval beter op verzoeken gaan controleren (26%), heeft aangifte gedaan (24%), antivirussoftware geïnstalleerd (22%) of wachtwoorden niet meer gedeeld (19%). Een derde (32%) heeft geen actie ondernomen.

Heb je maatregelen getroffen nadat je dit hebt meegemaakt?	Heeft één of meer voorvallen meegemaakt (n=648)
Ik controleer of iemand is die hij/zij zegt te zijn als ik een vreemd verzoek van hem/haar krijg	26%
Ik heb het gerapporteerd/ aangifte gedaan	24%
Ik heb antivirussoftware geïnstalleerd	22%
Ik deel mijn wachtwoorden niet (meer) met anderen	19%
Ik heb een software update uitgevoerd	18%
Ik maak mijn wachtwoorden complexer	16%
Ik heb een firewall geïnstalleerd of geüpdatet	15%
Ik heb toestemmingen van apps op mijn telefoon beperkt	11%
Ik maak nu back-ups van de bestanden op mijn laptop	11%
Ik maak nu back-ups van mijn smartphone	8%
Ik ben een wachtwoordmanager gaan gebruiken	7%
Ik maak nu back-ups van mijn tablet	6%
Ik ben nu een VPN-verbinding gaan gebruiken via mijn smartphone	5%
Ik verstuur geen werkgerelateerde bestanden van mijn werk meer naar huis	5%
Ik ben nu een VPN-verbinding gaan gebruiken via mijn tablet	5%
Ik ben nu een VPN-verbinding gaan gebruiken via mijn laptop	4%
Ik gebruik apps om meer controle te krijgen over het besturingssysteem dan de fabrikant toestaat	3%
Ik versleutel mijn harde schijf	2%
Anders, namelijk:	7%
Geen van bovenstaande, ik heb niets gedaan	32%

Veilig online op het werk

Veilig online op het werk

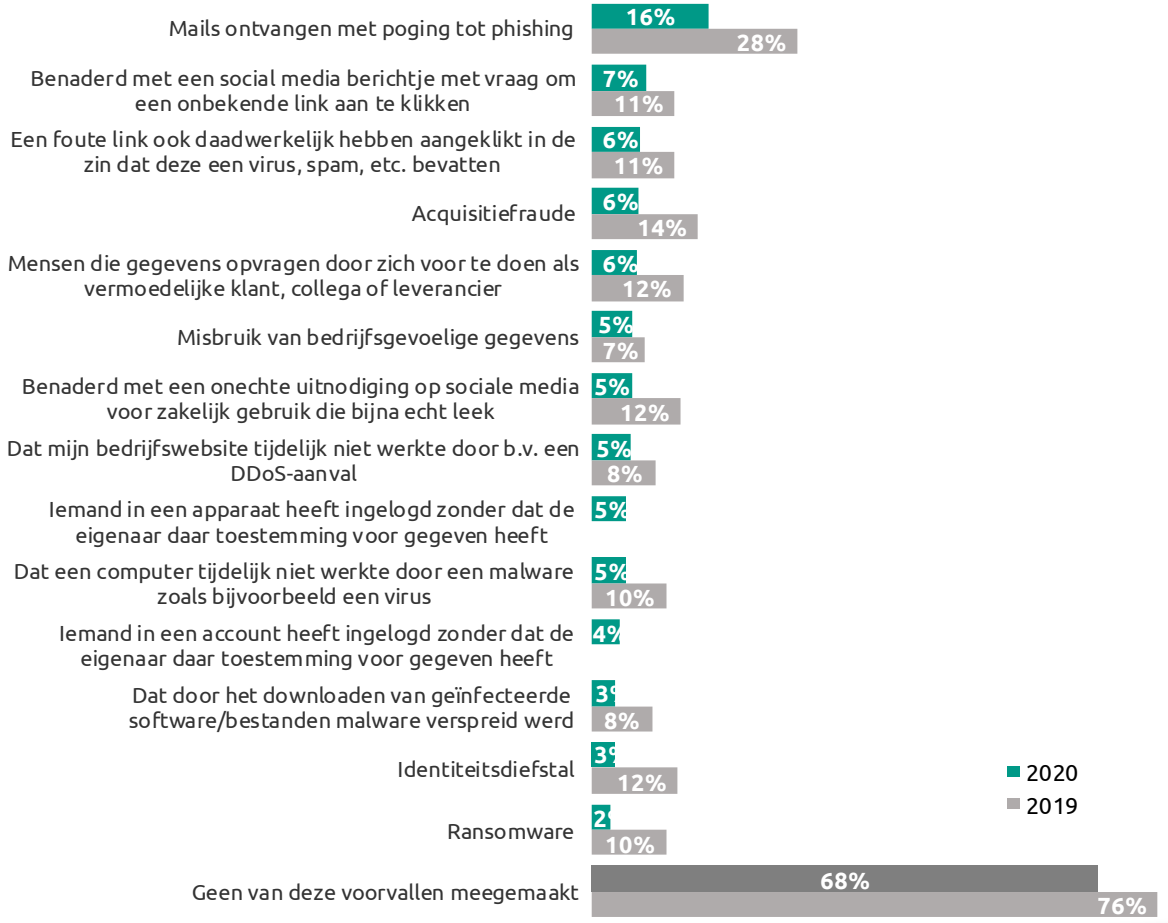
Drie op de tien werknemers heeft in werksituatie te maken met een online risico

68% heeft in de afgelopen 12 maanden geen van de voorgelegde voorvallen meegemaakt.

Ook op werk is phishing de meest voorkomende voorval van online risico (16%).

Er lijkt een dalende trend zichtbaar ten opzichte van 2019, echter zijn dit geen significante verschillen; Nederlanders zijn op het werk dit jaar, in vergelijking met 2019, met net zoveel digitale risico's in aanraking gekomen.

Heb je in een werksituatiein de afgelopen 12 maanden weleens te maken gehad met één van de onderstaande voorvallen?
(Basis - Werkend; 2020 n=477; 2019 n=501)



Veilig online op het werk

Vier op de tien werknemers heeft geen maatregelen getroffen na in aanraking te zijn geweest met een digitaal risico

Stappen die gezet nadat iemand in aanraking is geweest met een online risico is dat ze het melden bij hun systeembeheerder (15%), voorzichtiger zijn geworden (14%), aangifte hebben gedaan (14%) of toestemmingen van apps hebben beperkt (14%). Vier op de tien (40%) hebben geen actie ondernomen.

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

Veilig online op het werk

Meesten bedrijven hebben interne afspraken over veilig online gedrag gemaakt

Bijna zeven op de tien werkende Nederlanders (69%) hebben intern afspraken gemaakt over hoe werknemers zich veilig online gedragen. 13% geeft aan dat er geen afspraken zijn gemaakt en 18% is niet bekend of er afspraken zijn gemaakt.

Er zijn veel verschillende soorten afspraken gemaakt die betrekking hebben op procedures, zoals het uitwisselen van bestanden, als het gebruik van soorten website en apparaten. Bij bepaalde bedrijven zijn actief bepaalde sociale mediakanalen en verzendplatforms geblokkeerd.

In 2020 zijn meer werkenden bekend met de werkafspraken omtrent veilig online gedrag (69% vs. 57%). Hieronder verstaan we medewerkers die ofwel bekend zijn met de werkafspraken of werken voor een bedrijf/organisatie die werkafspraken heeft gemaakt met de werknemers over veilig online gedrag.

Welke afspraken zijn er binnen jouw bedrijf/organisatie gemaakt over hoe je je online veilig gedraagt? (Basis - Werkend, n=477)

Veilig online op het werk

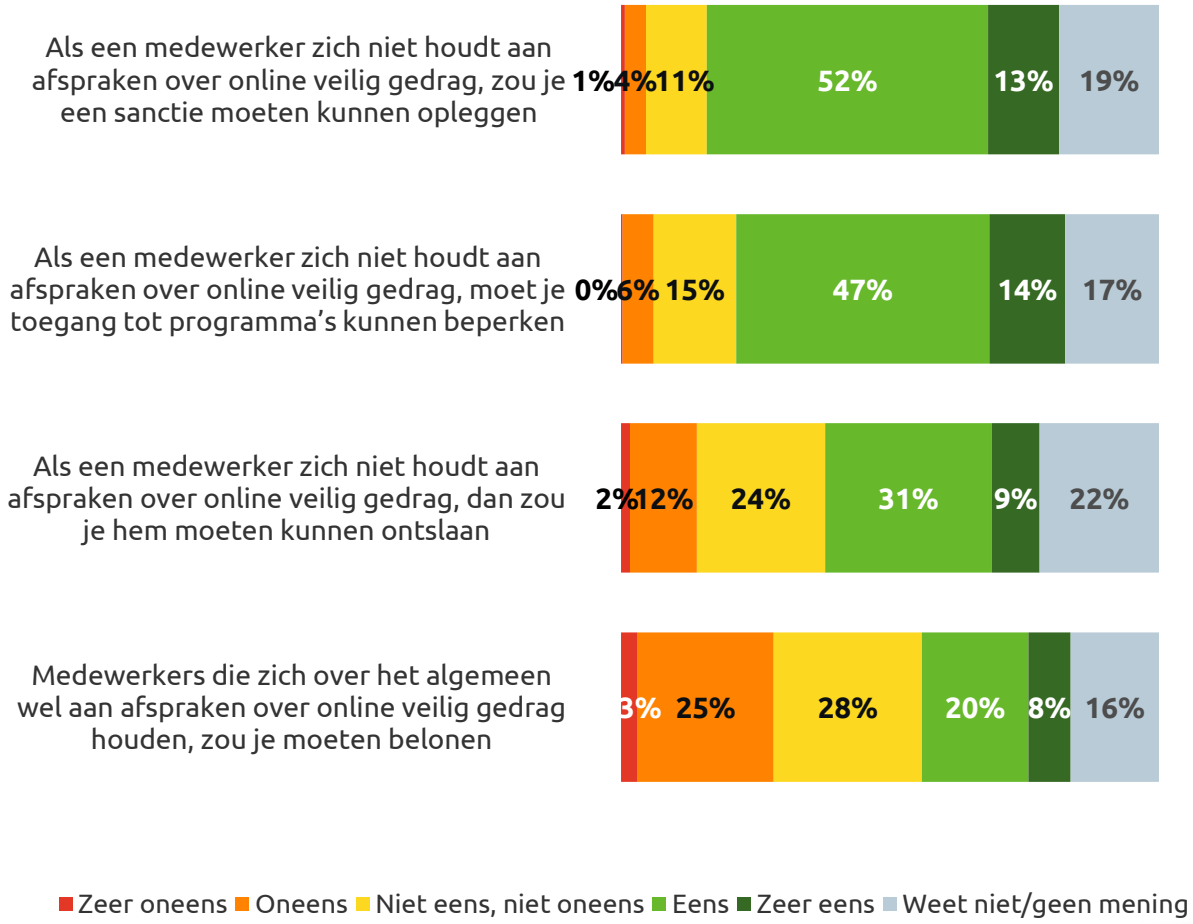
Relatief veel steun voor consequenties wanneer medewerkers zich niet aan gemaakte afspraken houden

Het merendeel van de werkenden staat positief tegenover maatregelen indien medewerkers zich niet aan de afspraken over online veilig gedrag houden, maar 'goed' gedrag belonen vindt een minderheid nodig.

Een ruime meerderheid van de werkenden (65%) vindt dat er sancties opgelegd moeten kunnen worden indien de afspraken over online veiligheid niet nageleefd worden. Ook vinden zes op de tien (61%) werkenden dat in zo een geval toegang tot programma's beperkt moet worden. 40% vindt dat bij het breken van de afspraken, de betreffende persoon ontslagen zou moeten kunnen worden.

Goed gedrag belonen wordt door een minderheid een goed idee gevonden; 28% vindt dat medewerkers die zich in het algemeen wel aan de afspraken houden, beloond zouden moeten worden. Echter vindt een even grote groep (28%) van niet.

In hoeverre ben je het hiermee eens? (n=327)



Veilig online op het werk

Helft ervaart belemmeringen bij borgen afspraken omtrent veilig online gedrag

Circa de helft (46%) geeft aan dat er binnen hun bedrijf belemmeringen zijn om afspraken over veilig online gedrag te borgen. Dit heeft vaak te maken met communicatie, zoals het niet duidelijk over communiceren (13%), niet voldoende over communiceren (13%) of niet eenduidig over communiceren (10%). Verder wordt er volgens 12% van de werkenden geen prioriteit gegeven aan het borgen van de afspraken.

De helft van de werkenden (54%) ervaart geen belemmeringen.

Welke belemmeringen ervaar je binnen jouw bedrijf bij het borgen van de afspraken voor online veilig gedrag?
(Basis - Werkend met afspraken over online veilig gedrag, n=327)

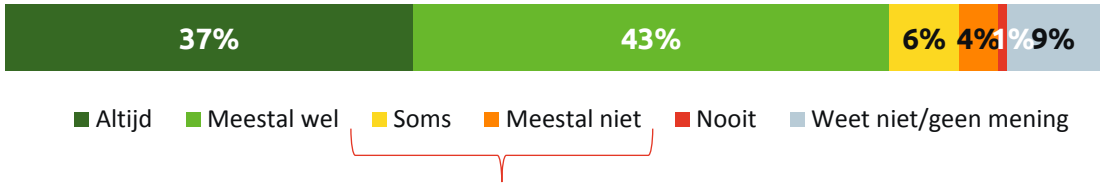
Veilig online op het werk
Merendeel houdt zich aan de gemaakte afspraken

81% van de werkenden geeft aan zich (meestal) aan de afspraken te houden over het veilig online gedrag.

De drie meest genoemde redenen om de afspraken niet na te leven zijn*:

- Gebrek aan aanmoediging om de afspraken na te leven
- Te weinig communicatie over de afspraken
- De afspraken schieten hun doel voorbij.

In hoeverre houd jij je aan de afspraken die binnen jouw bedrijf/organisatie gemaakt zijn over hoe je je online veilig gedraagt?
(Basis – Werkend en heeft afspraken over online veilig gedrag, n=327)



Waarom houd je je (soms/meestal) niet aan de afspraken over online veilig gedrag van jouw bedrijf?*

1. Ik word niet aangemoedigd om me aan afspraken te houden
2. Er wordt niet genoeg gecommuniceerd over de afspraken
3. De afspraken schieten hun doel voorbij
4. De afspraken worden toch niet gehandhaafd
5. Andere collega's houden zich ook niet aan de afspraken
6. De afspraken zijn niet zinvol
7. De afspraken zijn niet duidelijk
8. De afspraken zijn niet op mij van toepassing

**Vanwege de lage n (=35) worden hier geen percentages weergegeven.*

Veilig online op het werk

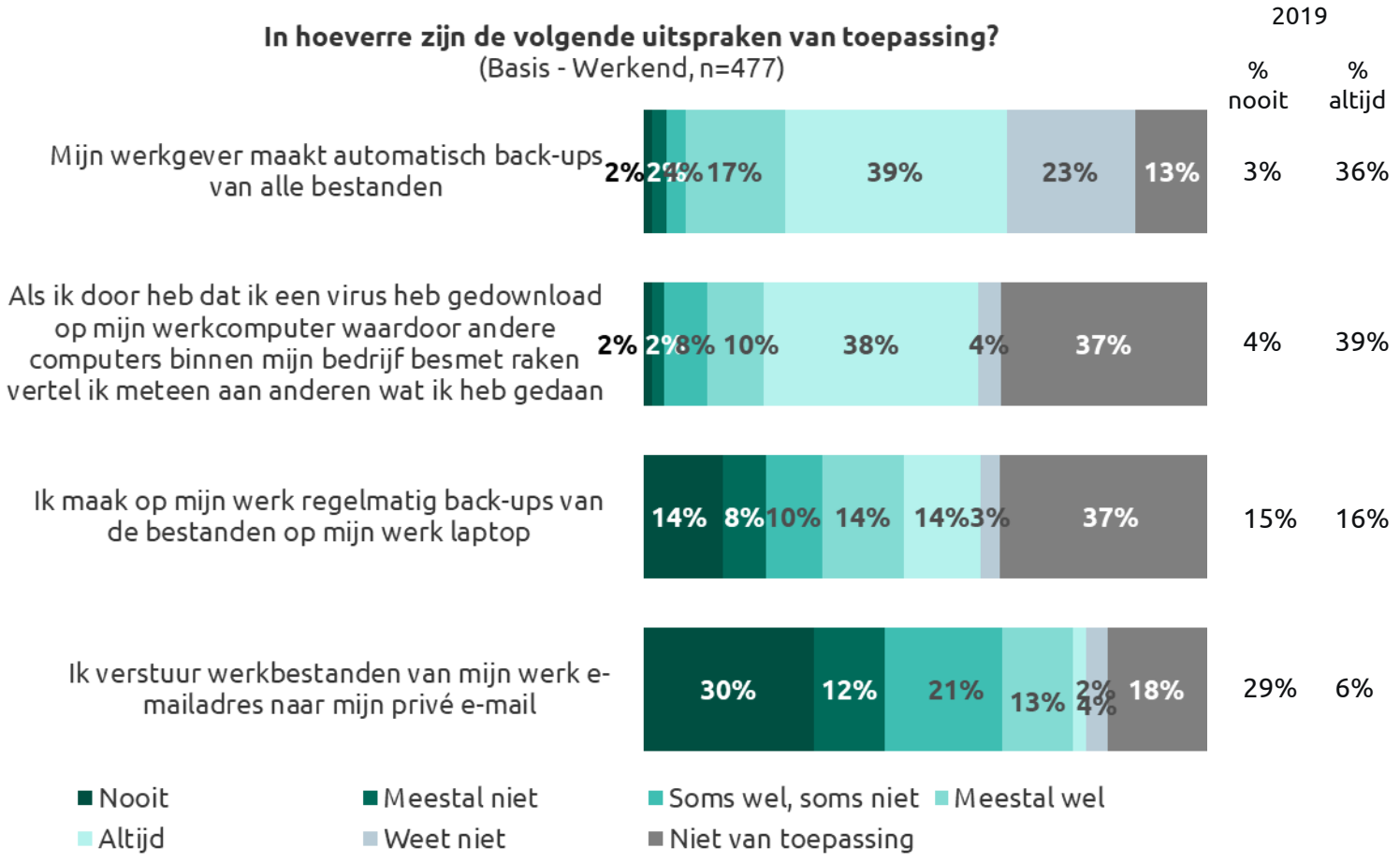
Vier op de tien werknemers zouden het altijd vertellen als ze een virus op hun werkcomputer hebben gedownload

Wanneer Nederlanders door zouden hebben dat ze een virus hebben gedownload op hun werkcomputer waardoor andere computers binnen hun bedrijf besmet zouden raken, zou 38% dat *altijd* vertellen. Slechts een klein aandeel (4%) zou dat (zeer waarschijnlijk) niet vertellen.

57% van de werkenden geeft aan dat hun werkgever vrijwel altijd automatische back-ups maakt van alle bestanden. En 28% maakt zelf zeer regelmatig back-ups van de bestanden op de werk laptop. 22% geeft aan dat vrijwel niet te doen. Verder sturen de meeste werkenden geen werkbestanden via hun werk e-mail naar hun privé e-mail (42%). 21% geeft aan dat dit weleens gebeurt en 15% doet dit vaak.

We zien geen verschillen in gedragingen ten opzichte van vorig jaar (op basis van % nooit en % altijd).

In hoeverre zijn de volgende uitspraken van toepassing?
(Basis - Werkend, n=477)

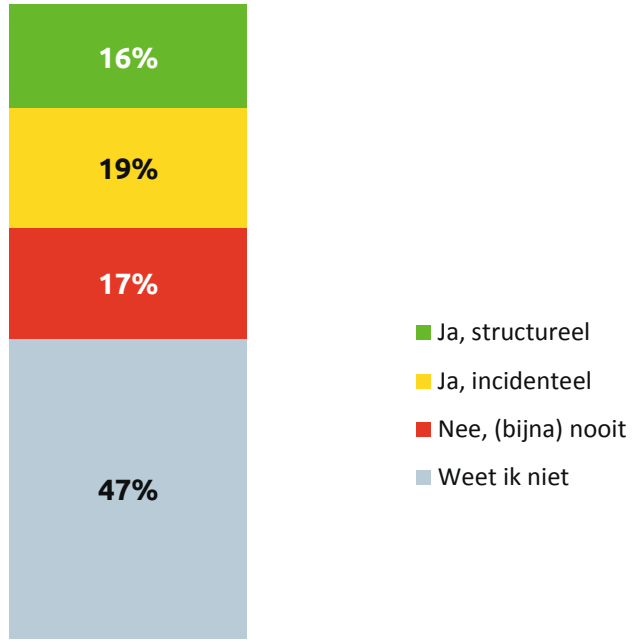


Veilig online op het werk

Bij meeste werknemers is niet bekend of er wordt gemonitord of men zich aan de afspraken voor online veilig gedrag houdt

Circa de helft van de werkenden heeft geen idee of hun bedrijf of organisatie meet in hoeverre medewerkers zich aan de afspraken voor veilig online gedrag houden (47%). Bij ruim een derde (35%) van de werkgevers wordt dit (incidenteel) wel gemeten en bij 17% van de werkenden wordt dit (bijna) nooit gecontroleerd.

Wordt binnen jouw bedrijf of organisatie gemeten in hoeverre medewerkers zich aan de afspraken voor online veilig gedrag houden?
(Basis - Werkend met afspraken over online veilig gedrag, n=327)



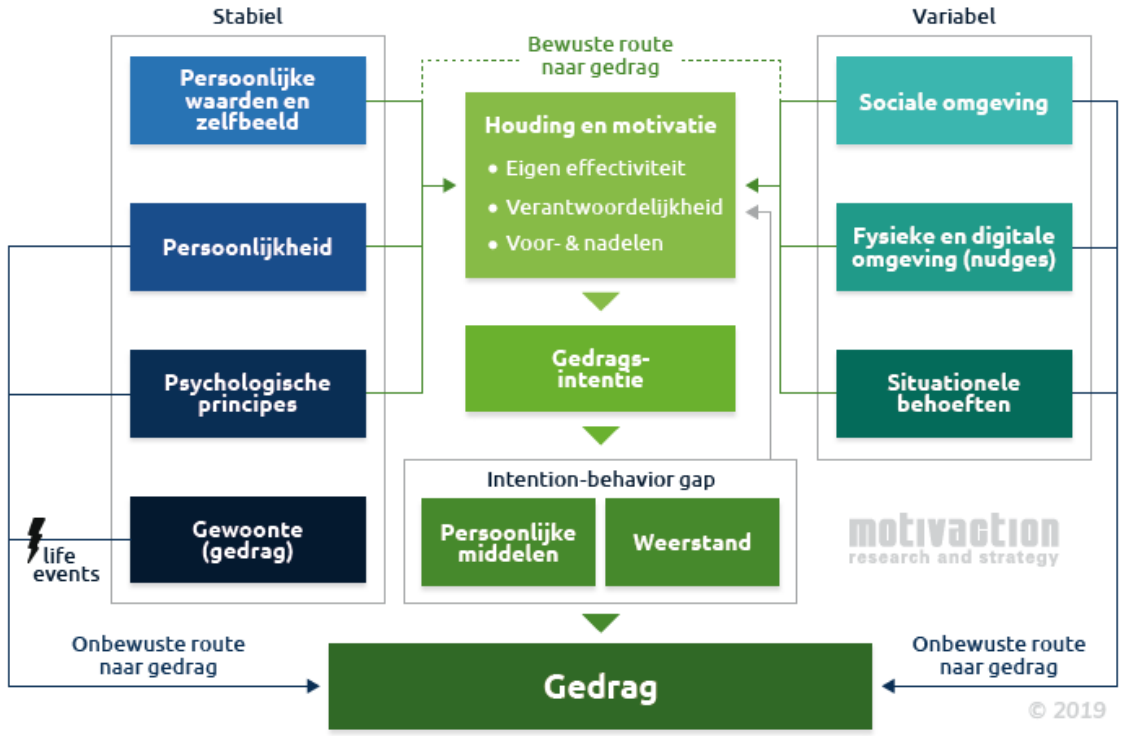
Verdiepingen

Verdieping: Gedragsanalyse

Verdieping | Gedragsanalyse

Ons gedrag bepaalt sterk hoe duurzaam, sociaal, veilig en gezond onze samenleving is, maar ook hoe veilig wij ons voelen. Om burgers en bedrijven bewust te maken van hun gedrag, te overtuigen om gewenst gedrag te vertonen en om gewenst gedrag te faciliteren, is meer nodig dan rationele kennis over hoe men zich online kan beschermen en wat veilig online gedrag is. Emotionele, onbewuste en contextgebonden invloeden hebben namelijk sterke invloed op wat mensen willen en kunnen doen. Of mensen het gewenste gedrag vertonen, hangt onder meer af van de match tussen het (gewenste) zelfbeeld, hun waarden en de (persoonlijke en sociale) normen. Al deze factoren bracht Motivaction samen in haar gedragsmodel.

In dit rapport gebruiken we het model om het gedrag rondom veilig internetten (beter) in kaart te brengen. Op die manier hopen we haakjes te bieden aan het ministerie van EZK om haar bewustzijnscampagne (nog) beter af te stemmen op Nederlanders. We omschrijven het gedrag aan de hand van de volgende pijlers: stabiele factoren, variabele factoren, houding en motivatie, persoonlijke middelen (zoals kennis en ervaringen) en weerstand.



Verdieping | Gedragsanalyse

Stabiele factoren

Omdat men het eigen gedrag online al redelijk goed vindt, is er weinig reden om te veranderen. Het is echter aan te raden om Nederlanders te blijven wijzen op de gevaren en hen aan te moedigen zich online te beschermen. Ze komen namelijk wel in aanraking met online risico's. Uit het onderzoek komt naar voren dat bijna de helft van de Nederlanders (45%) heeft in het afgelopen jaar een phishing mail ontvangen en een kwart (23%) is op social media benaderd om op een onbekende link te klikken.

- De campagne kan zich richten op het vertellen van daadwerkelijke voorvallen. Houdt hiermee rekening dat het niet te abstract moet worden (percentages kunnen abstract en moeilijk voorstelbaar zijn). Combineer numeriek met een verhaal om het toegankelijker te maken voor en makkelijker te communiceren.

Variabele factoren

De coronacrisis heeft ervoor gezorgd dat meer Nederlanders thuis zijn gaan werken. Thuis zijn Nederlanders vaak zelf verantwoordelijk voor hun digitale veiligheid. Een eerste stap is het maken van een veilige verbinding met de router. Het blijkt echter dat 29% van de werkenden met een netwerverbinding nooit het standaard wachtwoord hebben aangepast.

- Zet in op een campagne om mensen bewust te maken van de gevaren van het standaard wachtwoord. Maak inzichtelijk hoe makkelijk het is om dit wachtwoord te achterhalen en dus hoe makkelijk men 'de deur openzet' voor internetcriminelen door niet het standaardwachtwoord aan te passen.
- Geef daarbij handelsperspectief door aan te geven wat een sterk wachtwoord is (tekens, letters, lengte, etc.).

Verdieping | Gedragsanalyse

Houding en motivatie

De risico-inschatting van verschillende digitale risico's is laag. Risico's zijn vaak abstract, dus moeilijk voor te stellen voor mensen. Een probleem hierbij is dat mensen geneigd zijn om risico's te negeren. Zij nemen daardoor vaak geen voorbereidende maatregelen of doen geen aanpassingen aan hun gedrag om hun persoonlijke risico kleiner te maken. Mensen zijn daarnaast vaak geneigd om risico's lager in te schatten of denken dat vooral andere mensen risico lopen. Het blijkt ook dat Nederlanders zich relatief weinig druk maken om hun digitale veiligheid. 40% geeft aan zich enige zorgen te maken en 46% juist heel weinig.

- De campagne kan zich richten op concrete cases om risico meer toegankelijk te maken in het geheugen. Maak het risico voorstelbaar en leg nadruk op de *ernst* van de gevolgen. Men zou meer naar het idee 'het kan ook mij overkomen' moeten om gemotiveerd te worden om zich te beschermen.
- Indien de kans klein is, maar de gevolgen wel groot, kan het helpen om de perceptie van de kans te vergroten door de kans te communiceren over een langere tijdsperiode (bijv. elke 5 jaar). Omdat cybercrime toeneemt is het aan te raden om je juist te concentreren op de stijging van de risicokans.

Persoonlijke middelen

Nederlanders geven aan redelijk op de hoogte te zijn van verschillende digitale risico's. Waarschijnlijk komt dat neer op de naam kennen en ongeveer weten wat de digitale risico inhoudt, want bij het testen van verschillende beschrijvingen hadden sommige Nederlanders moeite om deze goed te beoordelen. De vraag is ook of het nodig is om precies te weten wat een digitaal risico is, als men zich er maar tegen kan beschermen. Phishing is bijvoorbeeld de meest voorkomende digitaal risico waar Nederlanders mee in aanraking komen. Circa een kwart (23%) geeft aan er weleens mee te maken hebben gehad en 16% heeft in de afgelopen 12 maanden een phishing bericht gehad. Om phishing te herkennen kijken Nederlanders met name naar het mailadres van de afzender (59%), of er om persoonlijke gegevens (52%) of geld (40%) wordt gevraagd en wat het taalgebruik of de schrijfstijl is van de mail (50%). Links in mails wordt door 29% bekeken en 34% kijkt naar het doeladres achter de link.

- Het lijkt er op dat Nederlanders weten wat veilig gedrag is en wat ze moeten doen om zichzelf te beschermen. Maar mogelijk is het waarom het belangrijk is om jezelf te beschermen minder sterk aanwezig en dat het belangrijk is om je bescherming te blijven updaten. Awareness zou zich kunnen richten op het belang en motiveren om je online veiligheid up-to-date te houden.

Verdieping | Gedragsanalyse

Weerstand

Wanneer we kijken naar tijd/gemak, complexiteit van informatie en geld, dan lijkt het dat geld een rol speelt als belemmering in veilig online gedrag. Nederlanders willen niet betalen voor diensten die hun veiligheid verhogen (58%) of vinden de prijs te hoog (40%). De prijs wordt afgezet tegen de risico-inschatting dat men slachtoffer kan worden van cybercrime. Omdat de risico-inschatting laag is, zullen mensen minder gemotiveerd zijn om te betalen voor een dienst. Daarnaast heeft een derde (35%) moeite met het begrijpen van instructies om jezelf te beschermen tegen digitale risico's en weet 25% niet wat een goede virusscanner is of hoe je een back-up moet maken van je bestanden (22%). Ook ervaren Nederlanders belemmeringen in gemak en tijd. Ze vinden het te veel gedoe om voor al hun accounts en apparaten een ander wachtwoord te hebben (44%), omdat ze het ook lastig vinden om steeds een nieuw wachtwoord te verzinnen (34%).

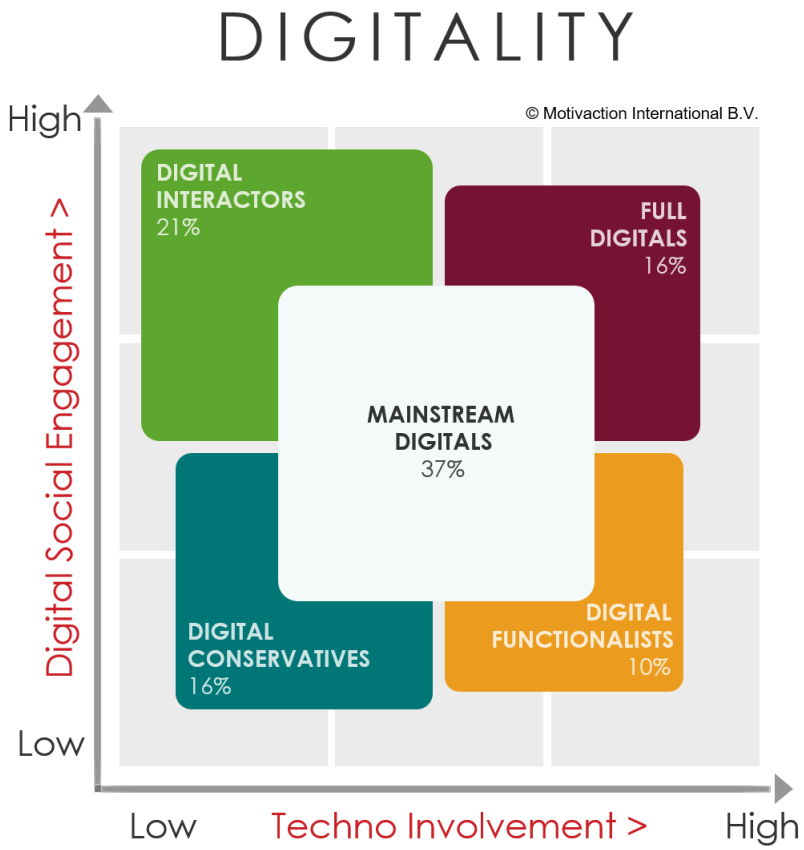
Verdieping: Digitality
Digitale doelgroepensegmentatie

Verdieping | Digitality

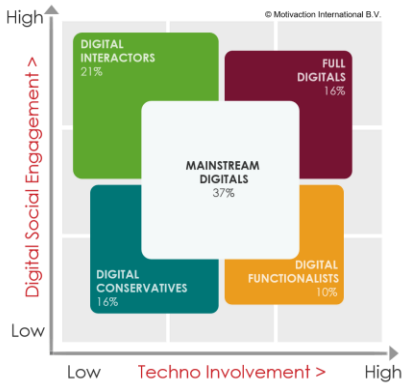
Sinds 2015 voert Motivaction structureel onderzoek uit naar 'het leven in een digitale wereld/cultuur'. Dit 'Digitality' onderzoeksprogramma bestaat uit een jaarlijkse kwantitatieve meting, kwalitatieve verdiepende onderzoeken en het toetsen van toekomstscenario's. Één van de onderdelen van het Digitality-onderzoeksprogramma is het Digitality-doelgroepenmodel. Het Digitality-doelgroepenmodel deelt mensen in op basis van hoe zij omgaan met de overstap naar een 'verbonden wereld', de wijze waarop zij hun digitale leven hebben ingericht en de motieven en attituden die hieraan ten grondslag liggen.

Het model is gebaseerd op twee assen: digital social engagement (mate waarin je bereid bent persoonlijke aspecten van jezelf online te delen) en techno-involvement (mate van tech-savvy-ness en tech-interesse). De vijf typen digitale burgers scoren verschillend op 6 onderliggende digitale waarden. Dit zijn waarden die het gedrag in het digitale domein verklaren.

- **Social**: de mate waarin het sociale leven zich online afspeelt.
- **Tech-savvy**: de mate waarin het gebruik van (online) technologie comfortabel is.
- **Escapism**: de mate waarin het digitale domein een plek is om te ontsnappen aan het dagelijks leven.
- **Distrust en privacy**: de mate waarin privacy binnen het digitale domein wordt gewantrouwd.
- **Interaction**: de mate waarin functionele interacties in het digitale domein plaatsvinden.
- **Online transactions**: de mate waarin men bereid is om digitaal aankopen te doen.



Verdieping | Digitality



In dit Veilig Online 2020 onderzoek hebben we vastgesteld dat de Digitality doelgroepen heel goed differentiëren op het thema 'Veilig Internetten'; zowel op 'gedrag', ''houding' als 'kennis'. (zie ook Digitality tabellenset). In het kort hieronder de afzonderlijke Digitality-doelgroepen getypeerd op het thema Veilig Internetten:

Digital Conservatives

Dit is de groep die **laag** scoort op **Techno-involvement** (tech-savvy-ness) én **laag** op **Digital Social Engagement** (meer functioneel gebruik van Digital). Vind 'privacy' belangrijk omdat zij niet weten wat er mis kan gaan.

Deze groep is de **bewust onbekwame groep** als het gaat om veilig internetten.

- **Kennis**: Zij hebben aantoonbaar de minste kennis over digitale risico's en kennen niet alle verschillende gevaren, al doen zij wel hun best om goed op de hoogte te zijn van de digitale gevaren.
- **Houding:** Zij schatten terecht hun digitale vaardigheden laag in en zijn bewust bezig met het inschatten van digitale risico's.
- **Gedrag:** Zij vertonen zo veilig mogelijk internetgedrag, gezien hun kennis; doen hun best om goed op de hoogte zijn van de gevaren, maar weten zelf niet altijd hoe zij moeten handelen.

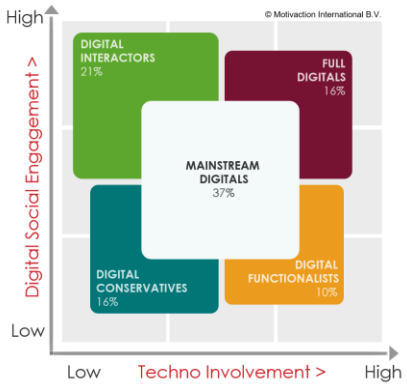
Digital Functionalists

Dit is de groep die **hoog** scoort op **Techno-involvement** (tech-savvy-ness) én **laag** op **Digital Social Engagement** (meer functioneel gebruik van Digital). Vind 'privacy' belangrijk omdat zij weten wat er mis kan gaan.

Deze groep is de **bewust bekwame groep** als het gaat om veilig internetten.

- **Kennis**: Zij hebben aantoonbaar de meeste kennis over digitale risico's en weten de verschillende digitale gevaren ook goed van elkaar te onderscheiden en in te schatten.
- **Houding:** Zij schatten terecht hun digitale vaardigheden hoog in en zijn realistisch in het inschatten van digitale risico's.
- **Gedrag:** Zij vertonen veilig internetgedrag; omdat zij goed op de hoogte zijn van de gevaren en zelf weten hoe zij moeten handelen (en dat kunnen ze doorgaans ook).

Verdieping | Digitality



Mainstream Digitals

De Mainstream Digital groep is letterlijk de middengroep. Zij scoren structureel gemiddeld (vergelijkbaar met Nlrep). In de afgelopen 5 jaar zien we dat de middengroep steeds kleiner wordt; men wordt meer uitgesproken over het digitale leven.

Digital Interactors

Dit is de groep die **laag** scoort op **Techno-involvement** (tech-savvy-ness) én **hoog** op **Digital Social Engagement** (Privacy is ondergeschikt aan de 'user experience') Zij hebben minder moeite privé data te delen (voor incentives).

Deze groep is de **onbewust onbekwame groep** als het gaat om veilig internetten.

- **Kennis**: Zij hebben beperkte kennis over digitale risico's en kennen niet alle verschillende gevaren, en doen ook geen moeite om goed op de hoogte te zijn van de gevaren.
- **Houding:** Zij schatten onterecht hun digitale vaardigheden voldoende-hoog in en zijn niet echt bezig met het inschatten van digitale risico's.
- **Gedrag:** Zij vertonen het meest onveilige internetgedrag, gezien hun beperkte kennis; en hun beperkte motivatie om op de hoogte zijn van de gevaren.

Full Digitals

Dit is de groep die **hoog** scoort op **Techno-involvement** (tech-savvy-ness) én **hoog** op **Digital Social Engagement** (Privacy is ondergeschikt aan de 'user experience') Zij hebben minder moeite privé data te delen (voor incentives).

Deze groep is de **onbewust bekwame groep** als het gaat om veilig internetten.

- **Kennis**: Zij hebben redelijk-goede kennis over digitale risico's; en weten de verschillende gevaren ook goed van elkaar te onderscheiden en in te schatten.
- **Houding:** Zij schatten hun digitale vaardigheden voldoende-hoog in en onderschatten de digitale risico's.
- **Gedrag:** Zij vertonen enigszins onveilig internetgedrag; doordat hun digitale vaardigheden voldoende-hoog zijn, onderschatten zij dat de digitale risico's ook hen kunnen raken.

Verdieping | Digitality
Inzichten bij het onderzoek

Nederlanders die veel online zijn, vinden vaker van zichzelf dat ze goed op de hoogte zijn

Met name Nederlanders die de online wereld omarmen, vinden dat ze goed op de hoogte zijn. Er is echter verschil tussen Nederlanders die echt goed op de hoogte zijn van de technische kanten van het internet (Digital Functionalist) en degenen die de digitale wereld omarmen al onderdeel van het gewone leven (Full Digitals). De eerste groep deelt liever niet (te) veel informatie over zichzelf online, omdat goed op de hoogte zijn van wat er allemaal met persoonlijke data kan worden gedaan. De laatste groep is lang niet altijd op de hoogte van digitale risico's of wil deze niet zien. Zij vinden het geen probleem om informatie over zichzelf te delen online. Ze lopen hierdoor meer gevaar zonder dat ze het door hebben.

Wanneer het te complex wordt, willen sommige Nederlanders de risico's van hun gedrag niet zien

Mainstream Digitals (de grootste groep van Nederland) kijken minder vaak naar links in de mail dan gemiddeld (22%). Ze controleren wel net zo vaak het doeladres achter de link (33%). Dat is juist iets wat Digital Conservatives minder vaak doen (26%). Zij letten vaker op of er om persoonlijke gegevens (60%) of om geld (48%) wordt gevraagd. Met name Nederlanders die vooral gebruikers zijn van internet en weinig (willen) weten van de technische kant van internet (Digital Interactor), hebben weleens te maken gehad met een aantal digitale risico's. Deze groep denkt liever ook niet na over de technische kant omdat ze denken dat ze het niet zullen begrijpen. Ze gaan het liever uit de weg. Ze staan dan ook zo min mogelijk stil bij privacy issues; het is een te complexe discussie waarvan ze de consequenties niet kunnen overzien, en waar ze nu geen last van hebben. Deze groep is echter op sociaal vlak de 'heavy user' en loopt dus relatief veel gevaar.

Angst om niet mee te kunnen komen

Nederlanders die liever offline zijn dan online (Digital Conservatives) zijn vaker onbekend met de verschillende voorgelegde digitale gevaren. Ze staan wantrouwend tegenover digitale privacy omdat ze geen idee hebben wat er allemaal met hun data gebeurt. Bij deze groep heerst echter de angst dat ze niet mee kunnen komen in de digitale wereld.

Bijlagen

Bijlage: overige resultaten

Bijlage | Digitality (1/8)

	Mainstream Digitals (n=326)	Digital Conservatives (n=214)	Digital Interactors (n=187)	Full Digitals (n=161)	Digital Functionalists (n=133)	Nederland representatief (n=1.022)
Hoe schat jij je eigen kennis over digitale en online veiligheid in?						
(Zeer) slecht	7%	17%	10%	5%	3%	9%
Matig	25%	32%	26%	17%	7%	23%
Redelijk tot (zeer) goed	66%	48%	60%	76%	88%	66%
Kun je aangeven in welke mate je bekend bent met de onderstaande zaken? % weleens mee te maken gehad + ik weet wat dit is						
Phishing	88%	80%	68%	83%	94%	83%
Malware	63%	59%	52%	73%	87%	65%
Hacking	90%	85%	77%	94%	96%	88%
Ransomware	51%	47%	40%	56%	69%	52%
Helpdeskfraude	60%	55%	47%	57%	64%	57%
Vriend-in-nood-fraude	65%	52%	52%	65%	80%	62%
Identiteitsfraude	93%	88%	77%	92%	95%	89%
DDos-aanval	58%	53%	46%	70%	76%	59%
Spoofing	22%	18%	22%	22%	42%	24%
Botnet	15%	14%	19%	28%	25%	19%
Cryptojacking	24%	18%	23%	34%	40%	26%

Bijlage | Digitality (2/8)

	Mainstream Digitals (n=326)	Digital Conservatives (n=214)	Digital Interactors (n=187)	Full Digitals (n=161)	Digital Functionalists (n=133)	Nederland representatief (n=1.022)
In hoeverre maak je je zorgen over jouw online/digitale veiligheid in je privésituatie?						
(Zeer) veel zorgen	4%	9%	**11%**	2%	5%	6%
Enige zorgen	43%	46%	39%	36%	33%	40%
(Zeer) weinig zorgen	50%	**40%**	42%	**59%**	**61%**	49%
Welk cijfer geef jij jezelf als het gaat om het veilig omgaan met online gevaren? *Gemidelde*						
	6,9	**6,7**	7,1	7,0	**7,5**	7,0

Bijlage | Digitality (3/8)

	Mainstream Digitals (n=326)	Digital Conservatives (n=214)	Digital Interactors (n=187)	Full Digitals (n=161)	Digital Functionalists (n=133)	Nederland representatief (n=1.022)
Welke van de onderstaande acties heb je ondernomen of doe je om jouw online veiligheid te verbeteren? *5 meest genoemd*						
Antivirussoftware gebruiken en regelmatig updaten	61%	62%	45%	58%	66%	58%
Regelmatig (beveiligings)updates doen	53%	50%	37%	55%	62%	51%
Controleren op welke links ik klik	50%	48%	34%	60%	64%	50%
Direct software updates uitvoeren	45%	43%	26%	55%	52%	44%
Regelmatig back-ups maken van al mijn bestanden	43%	39%	36%	44%	51%	42%
Welke van de onderstaande acties zou je bereid zijn om te doen om jouw online veiligheid te verbeteren? *5 meest genoemd*						
Antivirussoftware installeren/regelmatig updaten	52%	54%	36%	40%	54%	48%
Regelmatig (beveiligings)updates doen	49%	41%	31%	43%	53%	43%
Regelmatig back-ups maken van al mijn bestanden	42%	39%	28%	42%	52%	40%
Controleren op welke links ik klik	39%	38%	32%	43%	53%	40%
Direct software updates uitvoeren	43%	39%	27%	39%	46%	39%

Bijlage | Digitality (4/8)

	Mainstream Digitals (n=326)	Digital Conservatives (n=214)	Digital Interactors (n=187)	Full Digitals (n=161)	Digital Functionalists (n=133)	Nederland representatief (n=1.022)
In welke mate ga je veilig om met de volgende zaken? % goed + zeer goed + uitstekend						
Het updaten van mijn software updates	79%	76%	74%	85%	89%	79%
Omgaan met nepmails met poging tot phishing mails	73%	68%	68%	77%	81%	73%
Het bewaren van mijn wachtwoorden	70%	62%	65%	73%	79%	69%
Het gebruik van verschillende wachtwoorden	61%	64%	63%	71%	78%	66%
Het beheren en gebruik maken van persoons- en klantgegevens	61%	59%	62%	70%	67%	64%
Het laten gebruiken van jouw devices door anderen	61%	48%	61%	76%	63%	61%
Het beperken van schade door diefstal, beschadiging of verwijdering door het maken van back-ups	58%	49%	62%	57%	70%	58%
Het afgeven van toestemmingen op webshops	58%	48%	55%	57%	67%	56%
Het gebruik van USB-sticks	55%	48%	50%	61%	62%	55%
Het afgeven van toestemmingen op websites, zoals sociale media platforms als Facebook	53%	46%	47%	55%	65%	53%
Het gebruik maken van een wifi verbinding terwijl je onderweg bent	50%	42%	51%	63%	63%	52%
Het werken in een cloud	36%	26%	47%	50%	50%	40%

Bijlage | Digitality (5/8)

	Mainstream Digitals (n=326)	Digital Conservatives (n=214)	Digital Interactors (n=187)	Full Digitals (n=161)	Digital Functionalists (n=133)	Nederland representatief (n=1.022)
Kun je aangeven in welke mate je bekend bent met onderstaande zaken? % gebruik ik						
Virusscanner	82%	84%	70%	77%	91%	81%
Automatische updates	83%	77%	61%	81%	88%	78%
Het maken van back-ups van je gegevens	69%	65%	56%	73%	78%	68%
Tweestapsverificatie	67%	54%	43%	80%	80%	64%
Gebruik van lange wachtwoorden (wachtzinnen)	54%	46%	45%	56%	60%	52%
Voor elk account en apparaat een ander wachtwoord gebruiken	54%	56%	38%	42%	70%	52%
Instellingen om cookies te blokkeren/uit te zetten	45%	47%	37%	52%	62%	47%
Cloud diensten	44%	32%	43%	53%	43%	43%
Ad-blocker	33%	30%	34%	46%	53%	37%
Biometrische online bescherming	33%	21%	28%	52%	41%	34%
Spyware scanner	33%	27%	21%	32%	50%	32%
Digitaal wachtwoordenkluisje/wachtwoordmanager	23%	20%	19%	41%	32%	26%
VPN-verbindingen	27%	20%	17%	33%	33%	25%
Web tracking blocker	12%	12%	15%	20%	29%	16%
Open source hardware- en software	11%	10%	11%	22%	26%	15%

Bijlage | Digitality (6/8)

	Mainstream Digitals (n=326)	Digital Conservatives (n=214)	Digital Interactors (n=187)	Full Digitals (n=161)	Digital Functionalists (n=133)	Nederland representatief (n=1.022)
In hoeverre zijn de volgende uitspraken van toepassing? % Nooit						
Als ik gehackt zou worden via ransomware en gevraagd wordt om te betalen om weer toegang tot mijn laptop of pc te krijgen dan zou ik daarvoor betalen	58%	65%	42%	48%	72%	57%
Ik maak thuis gebruik van een extern opslagapparaat dat continu online is	39%	40%	16%	33%	43%	35%
Als ik op een link in een phishing e-mail zou klikken dan zou ik mij daar voor schamen	6%	7%	3%	9%	11%	7%
Ik maak thuis regelmatig back-ups van mijn bestanden	7%	11%	3%	8%	3%	7%
Ik heb de privacy instellingen van mijn social media accounts aangepast ten opzichte van de standaard instellingen	4%	3%	2%	3%	1%	3%
Ik bezoek alleen websites waar een slotje en/of https voor het adres van een website staat	1%	3%	3%	7%	2%	3%
Als ik een openbare computer heb gebruikt dan log ik na gebruik al mijn accounts uit	2%	3%	0%	5%	3%	2%
Als er een groen slotje en/of https voor het adres van een website staat dan denk ik dat ik die website veilig kan bezoeken	1%	4%	2%	2%	3%	2%

Bijlage | Digitality (7/8)

	Mainstream Digitals (n=326)	Digital Conservatives (n=214)	Digital Interactors (n=187)	Full Digitals (n=161)	Digital Functionalists (n=133)	Nederland representatief (n=1.022)
Kun je aangeven in hoeverre je het eens bent met de volgende stellingen?						
Ik wil niet betalen voor een dienst zoals wachtwoordmanager	61%	61%	48%	56%	63%	58%
Ik vind het te veel gedoe om voor al mijn accounts en apparaten een ander wachtwoord te hebben	48%	42%	41%	**52%**	36%	44%
De prijs van beveiligingssoftware/virusscanners is een belemmering	38%	46%	42%	45%	**29%**	40%
Ik vind de instructies om je te beschermen tegen digitale/online risico's vaak ingewikkeld	28%	**53%**	48%	**23%**	**15%**	35%
Ik vind het maken van nieuwe wachtwoorden lastig	32%	35%	**41%**	37%	**21%**	34%
Ik vertrouw gratis diensten zoals wachtwoordmanagers en virusscanners niet	26%	**41%**	35%	29%	33%	32%
Ik controleer de links niet in mails van afzenders die ik vertrouw	22%	28%	**38%**	30%	21%	27%
Ik weet niet wat een goede virusscanner is	24%	27%	28%	26%	**19%**	25%
Ik weet niet hoe ik een back-up van mijn computer moet maken	20%	26%	**30%**	19%	**10%**	22%
Het maken van een back-up van mijn computer kost te veel tijd	15%	19%	**30%**	**31%**	**15%**	21%
Ik vind het te veel gedoe om elke keer nieuwe softwareupdates te installeren	13%	24%	**32%**	18%	**9%**	19%
Ik zie het niet automatisch kunnen opslaan van wachtwoorden op websites en in systemen als een te grote belemmering	15%	22%	**25%**	21%	17%	19%
Ik zie het inloggen via een tweestapsverificatie als een te grote belemmering	16%	14%	**24%**	11%	11%	16%
Ik zie het automatisch uitloggen wanneer je even niet actief bent geweest op een website of systeem als een te grote belemmering	9%	13%	**27%**	21%	12%	15%

Bijlage | Digitality (8/8)

> *Terug naar het rapport*

Heb je in een privésituatie in de afgelopen 12 maanden weleens te maken gehad met één van de onderstaande voorvallen? % ikzelf	Mainstream Digitals (n=326)	Digital Conservatives (n=214)	Digital Interactors (n=187)	Full Digitals (n=161)	Digital Functionalists (n=133)	Nederland representatief (n=1.022)
Mails ontvangen met poging tot phishing	45%	44%	37%	49%	52%	45%
Benaderd met een social media berichtje met vraag om een onbekende link aan te klikken	19%	17%	29%	30%	23%	23%
Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik die bijna niet van echt te onderscheiden is	11%	12%	15%	13%	8%	12%
Acquisitiefraude	3%	9%	12%	7%	8%	9%
Een foute link ook daadwerkelijk hebben aangeklikt in de zin dat deze een virus, spam, phishing of ongewenste poging bevatten	5%	6%	18%	10%	1%	7%
Dat een computer tijdelijk niet werkte door een malware zoals bijvoorbeeld een virus	3%	5%	17%	7%	4%	7%
Ransomware	4%	1%	14%	6%	0%	5%
Dat door het downloaden van geïnfecteerde software/bestanden malware verspreid werd	5%	2%	11%	6%	3%	5%
Dat mijn (bedrijfs-) website tijdelijk niet werkte door b.v. een DDoS-aanval	3%	2%	12%	4%	3%	5%
Iemand in een apparaat (computer, telefoon) heeft ingelogd zonder dat de eigenaar daar toestemming voor gegeven heeft	4%	3%	11%	3%	3%	5%
Identiteitsdiefstal	3%	1%	11%	3%	2%	4%
Iemand in een account (social media, webwinkel, e-mail, bank) heeft ingelogd zonder dat de eigenaar daar toestemming voor gegeven heeft	4%	3%	5%	4%	2%	4%

Bijlage | Kennis
Digitale beveiligingsopties

Kun je aangeven in welke mate je bekend bent met onderstaande zaken? (Basis – Nederland representatief, n=1.022)	Ja gebruik ik	Gebruik ik niet, maar ik weet wel wat het is	Weleens van gehoord, maar weet niet precies wat het is	Nooit van gehoord
Virusscanner	81%	13%	3%	4%
Automatische updates	78%	14%	4%	4%
Het maken van back-ups van je gegevens	68%	23%	6%	4%
Tweestapsverificatie	64%	15%	6%	16%
Voor elk account en apparaat een ander wachtwoord gebruiken	52%	39%	5%	4%
Gebruik van lange wachtwoorden (wachtzinnen)	52%	34%	6%	8%
Instellingen om cookies te blokkeren/uit te zetten	47%	32%	13%	8%
Cloud diensten	43%	34%	13%	11%
Ad-blocker	37%	27%	14%	21%
Biometrische online bescherming	34%	42%	11%	14%
Spyware scanner	32%	29%	20%	19%
Digitaal wachtwoordenkluisje /wachtwoordmanager	26%	42%	15%	17%
VPN-verbindingen	25%	32%	18%	25%
Web tracking blocker	16%	25%	17%	42%
Open source hardware- en software	15%	26%	23%	36%

Terug naar digitale beveiligingsopties

Bijlage | Gedrag

Toelichting op cijfer eigen gedrag

Je geeft jezelf een [cijfer]. Kun je dit toelichten?	Geeft zichzelf een onvoldoende (n=96)	Geeft zichzelf een voldoende (n=887)	Totaal (n=983)
Ik ben goed op de hoogte/Ik heb alles op orde	0%	30%	**27%**
Ik ben alert/bewust van de gevaren/voorzichtig	1%	20%	**18%**
Er is (altijd) ruimte voor verbetering	14%	13%	**13%**
Ik ben hier niet bewust mee bezig/Ik ben (soms) te laks	27%	8%	**10%**
Ik heb hier geen/weinig verstand van	37%	5%	**8%**
Verdachte mails herkennen	1%	6%	**5%**
Ik ga goed met mijn wachtwoorden om	1%	5%	**4%**
Ik ga niet veilig (genoeg) om met mijn wachtwoorden	2%	4%	**4%**
Gebruik van anti-virussoftware	0%	3%	**3%**
Geen persoonlijke gegevens delen online	2%	3%	**3%**
Volledige veiligheid is onhaalbaar/kost te veel moeite	3%	3%	**3%**

Je geeft jezelf een [cijfer]. Kun je dit toelichten?	Geeft zichzelf een onvoldoende (n=96)	Geeft zichzelf een voldoende (n=887)	Totaal (n=983)
Niet op onbekende links klikken	0%	3%	**3%**
Bij mij valt niets te halen/Ik ben maar weinig online	1%	2%	**2%**
De online wereld/criminaliteit verandert constant	3%	2%	**2%**
Geen onbekende/onbetrouwbare sites bezoeken	0%	2%	**1%**
Ik heb ervaring in de ict/it security	0%	2%	**1%**
Regelmatig backups maken van mijn bestanden	0%	1%	**1%**
Software regelmatig updaten	0%	1%	**1%**
Ik accepteer regelmatig cookies	0%	1%	**1%**
Ik besteed mijn online security uit	1%	1%	**1%**
Overige antwoorden	5%	9%	**9%**
Weet niet/geen antwoord	16%	18%	**18%**

Terug naar beoordeling eigen gedrag

Overige bijlagen

Bijlage | Onderzoekstechnische informatie - kwantitatief

Veldwerkperiode

Het veldwerk is uitgevoerd in de periode 11 augustus en 23 augustus 2020.

Methode respondentenselectie

- Uit het StemPunt-panel van Motivaction
- Via een partnerpanelbureau

Incentives

De respondenten hebben als dank voor deelname aan het onderzoek punten voor het StemPunt spaarprogramma ontvangen

Weging

De onderzoeksdata zijn gewogen (zie ook bijlage gewogen en ongewogen data), 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.

Bewaartermijn primaire onderzoeksbestanden

Digitaal beschikbare primaire onderzoeksbestanden worden tenminste 12 maanden na afronden van het onderzoek bewaard. Beeld- en geluidsopnames op cd en niet digitaal beschikbare schriftelijke primaire bestanden zoals ingevulde vragenlijsten, worden tot 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.

Bijlage | Ongewogen en gewogen data

Kenmerken	Ongewogen		Gewogen	
	n	%	n	%
Leeftijd * geslacht				
Man 16 t/m 24 jaar	20	2.0	73	7.1
Vrouw 16 t/m 24 jaar	57	5.6	71	6.9
Man 25 t/m 34 jaar	28	2.7	81	8.0
Vrouw 25 t/m 34 jaar	69	6.8	82	8.0
Man 35 t/m 44 jaar	46	4.5	78	7.6
Vrouw 35 t/m 44 jaar	64	6.3	78	7.6
Man 45 t/m 54 jaar	72	7.0	97	9.5
Vrouw 45 t/m 54 jaar	79	7.7	96	9.4
Man 55 t/m 64 jaar	96	9.4	86	8.5
Vrouw 55 t/m 64 jaar	116	11.4	89	8.7
Man 65 t/m 80 jaar	206	20.2	93	9.1
Vrouw 65 t/m 80 jaar	169	16.5	98	9.6

Kenmerken	Ongewogen		Gewogen	
	n	%	n	%
Opleiding				
Hoog	250	24.5	290	28.4
Middel	498	48.7	507	49.6
Laag	273	26.7	224	21.9
Nielsen-regio				
3 grote gemeenten	91	8.9	121	11.9
West	307	30.0	301	29.5
Noord	109	10.7	101	9.9
Oost	216	21.1	214	20.9
Zuid	264	25.8	243	23.8
Randgemeenten	35	3.4	41	4.0

Wij verminderen onze footprint

Motivaction is ISO 14001-gecertificeerd

Motivaction gebruikt energiezuinige auto’s

Motivaction gebruikt groene stroom

Motivaction gebruikt uitsluitend papier met een FSC-label

Auteursrecht

Beeldmateriaal

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

Pers- en publicatiebeleid

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

Motivaction International B.V.

Marnixkade 109F
1015ZL Amsterdam

Postbus 15262
1001MG Amsterdam

020 589 83 83

info@motivaction.nl

www.motivaction.nl

Weet wat mensen drijft.

motivaction
insights and strategy