Cybersecurity awareness en skills in Nederland

Inhoudsopgave

Achtergrond van het onderzoek

Nederland behoort tot de landen met de meeste internetaansluitingen, nergens in Europa maken zoveel mensen gebruik van internetbankieren als in ons land. We zijn altijd en overal online. Dat geeft Nederland een voorsprong en biedt kansen voor innovatie en economische groei. Maar het betekent ook dat iedereen zich bewust moet zijn van de gevaren en risico's. Ransomware, phishing en malafide advertenties zijn de grootste dreigingen van dit moment. Met een muisklik kun je onbedoeld een heel netwerk besmetten of liggen al je privé- of klantgegevens op straat.

Aanvallen worden geavanceerder en zijn steeds lastiger te herkennen. Een continue aandachtspunt is daarom bewustwording over de online veiligheid. Maar daarmee zijn we er nog niet. Het wordt steeds duidelijker dat Nederlanders ook moeten weten hoe men zich online veilig kan gedragen en hoe en wanneer deze gedragingen moeten worden toegepast. Uit onderzoek van Alert Online 2015 blijkt dat we steeds bewuster zijn van de risico's, maar dat we ons niet perse digitaal bewust gedragen. Het zit blijkbaar nog niet in onze genen.

Omdat de noodzaak blijft groeien wordt ieder najaar de campagne Alert Online gehouden, een initiatief van de overheid, het bedrijfsleven, het onderwijs en de wetenschap. Door gezamenlijk in dezelfde periode activiteiten te ontplooien gericht op het vergroten van de bewustwording en kennis over online veiligheid en het stimuleren van digitaal veilig gedrag, creëert de campagne momentum. Doel is om te investeren in cybersecuritykennis en -kunde. De campagne richt zich op burgers, zelfstandig ondernemers, bedrijven, organisaties, overheden en hun medewerkers. Jong en oud en van werkvloer tot boardroom. Thuis, onderweg en op het werk.

Bewustzijn, kennis, kunde, maar vooral ook talent, vertrouwen, weerbaarheid en innoverend vermogen rondom cybersecurity zijn onmisbaar om de continue stroom kwetsbaarheden en steeds geavanceerdere dreigingen het hoofd te kunnen bieden. Voortbouwend op de focus op 'kennis' in 2014 en 'gedrag' in 2015 wordt in 2016 ingezet op 'skills'. Aangezien het aan deze cybersecurity skills nog vaak ontbreekt bij het veilig handelen, is het ontwikkelen en investeren in deze skills cruciaal.

Inleiding

Doel

Cybersecurity skills zijn het centrale thema van dit onderzoek. Naast het verkrijgen van inzicht in deze skills wordt er net als voorgaande jaren ook ingaan op bewustzijn, kennis en gedrag aangaande cybersecurity.

Doelgroepen

In het onderzoek is er onderscheid gemaakt tussen de onderstaande 7 groepen. Aan de werkzame bevolking in de groepen 3 tot 7 is ook onderscheid gemaakt tussen degenen die wel/niet verantwoordelijk zijn voor het beleid omtrent digitale / online veiligheid binnen het bedrijf.

1. n = 963 Algemeen publiek (inwoners Nederland van 13 jaar en ouder)
2. n = 363 ZZP'ers (zelfstandigen zonder personeel)
3. n = 205 Ambtenaren bij een van de Rijksoverheden (ook inspecties, ZBO's, Belastingdienst, Rijkswaterstaat, DJI, IND, UWV, NZA en de Hoge Colleges van Staat)
4. n = 169 Ambtenaren exclusief Rijksoverheid (werkzaam voor provincies, gemeenten of waterschappen)
5. n = 247 Werknemers klein MKB (2-9 werknemers)
6. n = 289 Werknemers groot MKB (10-249 werknemers)
7. n = 408 Medewerkers grootbedrijf (bij organisaties uit alle sectoren met meer dan 250 medewerkers)

Methode en veldwerk

Er is onderzoek gedaan op basis van twee online vragenlijsten, één voor het algemeen publiek en één voor de werkzame bevolking. Op basis van selectievragen zijn respondenten toegewezen aan de juiste doelgroep of uitgesloten van deelname. Voor een volledig overzicht van de onderzoeksverantwoording, zie pagina 70.

Leeswijzer rapportage

In dit rapport worden drie thema's behandeld, per thema een hoofdstuk:

- H1: Bewustzijn van cybergevaren en de kennis en houding ten opzichte van deze gevaren
- H2: Het niveau van cybersecurity skills in Nederland
- H3: Waar liggen de kansen en bedreigingen voor de ontwikkeling van cybersecurity skills

In de drie hoofdstukken in het hoofdrapport wordt vooral de vergelijking tussen algemeen publiek en werkzame bevolking getrokken. Waar mogelijk is de vergelijking met het voorgaande onderzoek (2015) gemaakt. Ook de significante verschillen op de sociaal-demografische kenmerken geslacht, leeftijd en opleiding zijn weergegeven en zijn als volgt gecategoriseerd:

- Geslacht:
  - man
  - vrouw
- Leeftijd:
  - werkzame bevolking: 20-30jaar / 30-50jaar / 50+
  - algemeen publiek: 13-18jaar / 18-30jaar / 30-50jaar / 50+
- Opleiding:
  - laagopgeleid (geen/LBO/VBO/MAVO)
  - middelbaar opgeleid (MBO/HAVO/VWO)
  - hoogopgeleid (HBO/WO)

Aan het einde volgt per thema een hoofdstuk ter verdieping. Deze hoofdstukken volgen hetzelfde verloop als de hoofdstukken in het hoofdrapport alleen wordt hier ingegaan op de verschillende groepen binnen de werkzame bevolking.

1
Management summary

Management summary in woord

Bewustzijn, kennis en houding

- Mannen zeggen bekender te zijn met cybergevaren en de verschillende vormen van bescherming tegen cybergevaren dan vrouwen. Hoogopgeleiden zijn bekender met cybergevaren en maatregelen ter bescherming van deze gevaren dan laagopgeleiden. Echter maken zowel mannen als hoogopgeleiden van de werkzame bevolking zich wel vaker zorgen over hun digitale veiligheid.
- Hoewel mannen binnen algemeen publiek hun kans om slachtoffer te worden van cybergevaren lager inschatten, worden zij in werkelijkheid vaker slachtoffer. Bij de werkzame bevolking schatten de mannen de situatie 'accurater' in, zij schatten de kans hoger en worden ook daadwerkelijk vaker slachtoffer.
- We vroegen respondenten ook om een inschatting te geven van het kennisniveau om cybergevaren te bestrijden en ook van de mate waarin deze kennis toegepast kan worden. Jongeren geven aan betere cyber skills te hebben dan ouderen, dit geldt voor algemeen publiek en werkzame bevolking. Van de groep die zich bezig houdt met het digitale veiligheidsbeleid binnen een organisatie, schatten 50+ers hun eigen cyber skills voor het gebruik maken van en beleid maken omtrent sociale media lager in dan mensen tot 50 jaar.

Niveau van cybersecurity skills in Nederland

- Over het algemeen lijkt de werkzame bevolking bewuster ofwel veiliger met cybergevaren om te gaan. Dit wil niet zeggen dat het algemeen publiek onveilig gedrag laat zien, zij kiezen vaak ook voor een 'redelijk' veilige optie. Dit is bijvoorbeeld het geval bij het gebruik maken van wifi verbindingen. Op sociale media zijn er weinig verschillen tussen deze groepen te zien, toch denkt ruim 1 op de 10 in beide groepen niet bewust na over de mogelijke gevolgen (voor henzelf of anderen) van sociaal media gebruik. Wat betreft het beheren van wachtwoorden, komt het nog regelmatig voor dat wachtwoorden op een (verstopt) briefje worden geschreven. Bij algemeen publiek is dit bij een kwart het geval, bij werkzame bevolking 17%. Ook geeft 18% van de werkzame bevolking aan dat wanneer zij gebruik maken van een openbare wifi verbinding, zij dit zowel doen met als zonder inlog.
- Een klein gedeelte (ongeveer 1 op de 10) ZZP'ers laat op voor hen belangrijke veiligheidsthema's opvallend gedrag zien, voorbeelden zijn het niet maken van back-ups van werkgerelateerde bestanden en werken in een cloud zonder inloggegevens of wachtwoord.

Management summary in woord (2)

Ontwikkeling van cybersecurity skills

- Zowel voor het zorgen voor digitale veiligheid als het ontwikkelen van cyber skills geven algemeen publiek en ZZP'ers aan dat de gebruiker verantwoordelijk is. Onder werkzame bevolking (exclusief ZZP'ers) wordt de verantwoordelijkheid in eerste instantie bij de ICT-afdeling van de organisatie gelegd.

- Voor het ontwikkelen van kennis en vaardighden om cybergevaren te bestrijden geven vrouwen in vergelijking met mannen aan dit liever via vrienden en familie te doen. Een zelfde verdeling zien we terug bij opleiding: laagopgeleiden geven de voorkeur aan ontwikkeling via mensen in de omgeving.

- Onder de werkzame bevolking geven jongeren (20-30jarigen) aan eerder veiligheidsmaatregelen te omzeilen om moeite en/of tijd te besparen dan 30+ers. Voor zowel algemeen publiek als werkzame bevolking geldt dat hoogopgeleiden minder snel veiligheidsmaatregelen omzeilen dan laagopgeleiden.

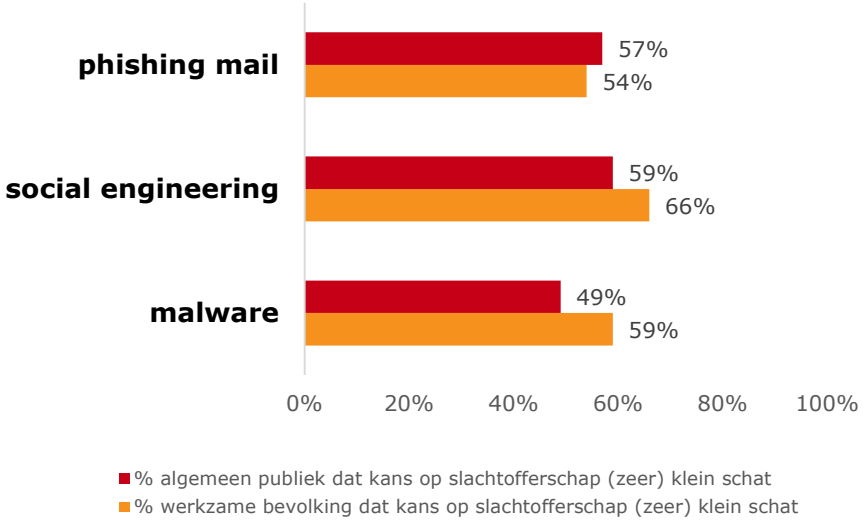
Management summary in woord en beeld

Op de volgende pagina's geven wij u als lezer een overzicht van de meest opvallende resultaten uit het onderzoek. In het vervolg van het rapport zult u een uitwerking vinden van deze resultaten en onderwerpen.

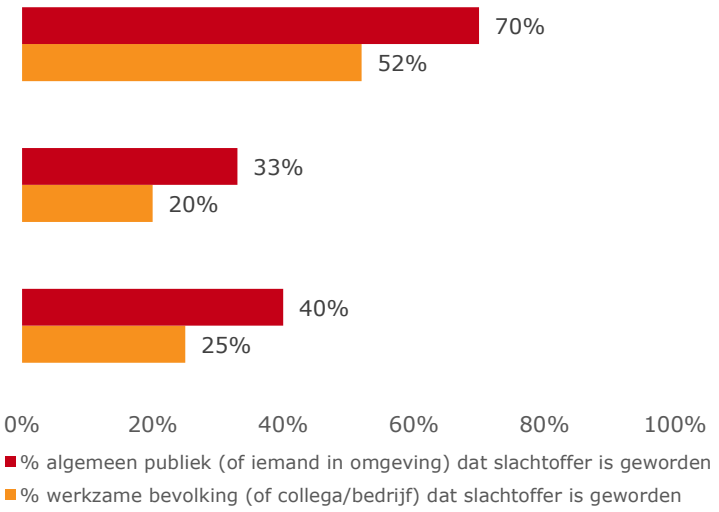
Nederlanders maken zich (deels onterecht) weinig zorgen over hun digitale veiligheid

- De meerderheid van de Nederlanders geeft aan zich (zeer) weinig zorgen te maken over hun digitale veiligheid, zowel algemeen publiek (69%) als de werkzame bevolking (73%). Daarnaast schatten beide groepen de kans op slachtofferschap van digitale gevaren in als (zeer) klein.
- Wat echter opvalt is dat meer dan de helft van het algemeen publiek en werkzame bevolking de kans op slachtofferschap van phishing mails als (zeer) klein schat. Deze schatting is echter niet accuraat want de percentages van daadwerkelijk slachtofferschap liggen boven de 50%. Ook de percentages van daadwerkelijke slachtoffers van social engineering en malware zijn fors te noemen terwijl (meer dan) de helft van de Nederlanders de kans op slachtofferschap als (zeer) klein inschat.

Geschatte kans op slachtofferschap **(zeer) klein**



Daadwerkelijk slachtofferschap



Bekendheid en slachtofferschap van ransomware neemt toe terwijl de inzet van preventiemaatregelen achterblijven

- In 2015 had 7% van het algemeen publiek (zelf of iemand uit de directe omgeving) te maken gehad met ransomware, in 2016 is dit gestegen naar 15%. Onder de werkzame bevolking blijft dit percentage gelijk aan vorig jaar (7%). Ook stijgt de bekendheid met ransomware fors (10%) in beide groepen.

- Ondanks deze groeiende aanwezigheid van ransomware worden de maatregelen ter preventie nog niet optimaal toegepast. Back-ups en automatische updates zouden de dreiging kunnen verlagen maar deze handelingen zitten nog niet in het 'DNA' van alle onderzochte groepen. Hieronder de drie belangrijkste bevindingen:

1. Bijna het gehele algemeen publiek en ZZP'ers zijn bekend met automatische updates. Echter heeft minder dan de helft van algemeen publiek en driekwart van de ZZP'ers automatische updates aanstaan.

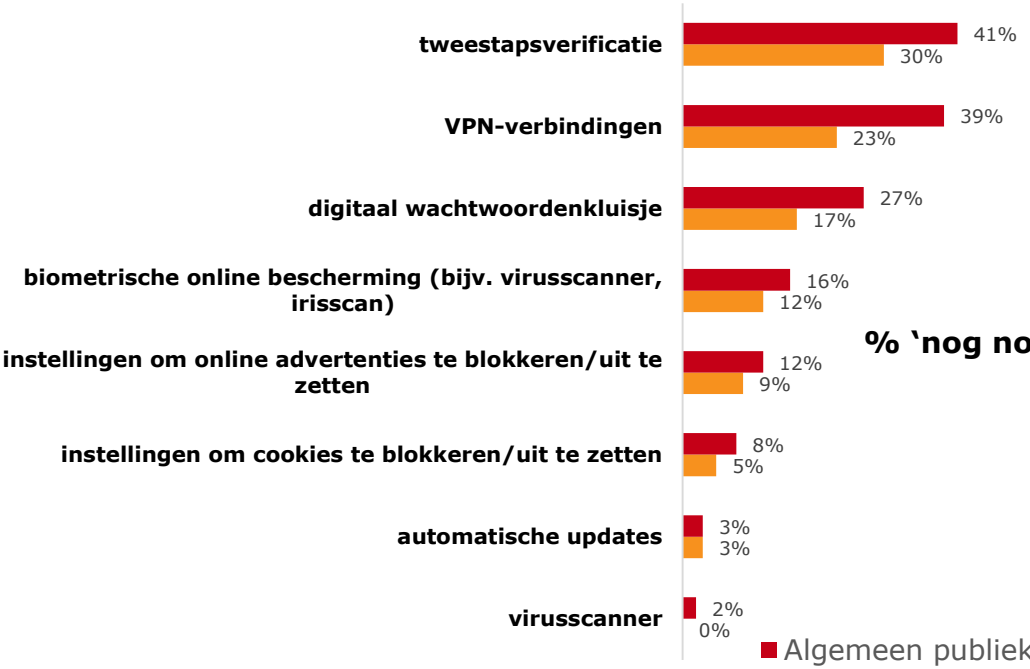
2. Onder ZZP'ers maakt ruim 1 op de 10 nooit een back-up omdat zij hier 'nooit eerder over nagedacht hebben'

3. Een kwart van het algemeen publiek maakt nooit een back-up omdat ze hier 'nooit over nagedacht hebben'

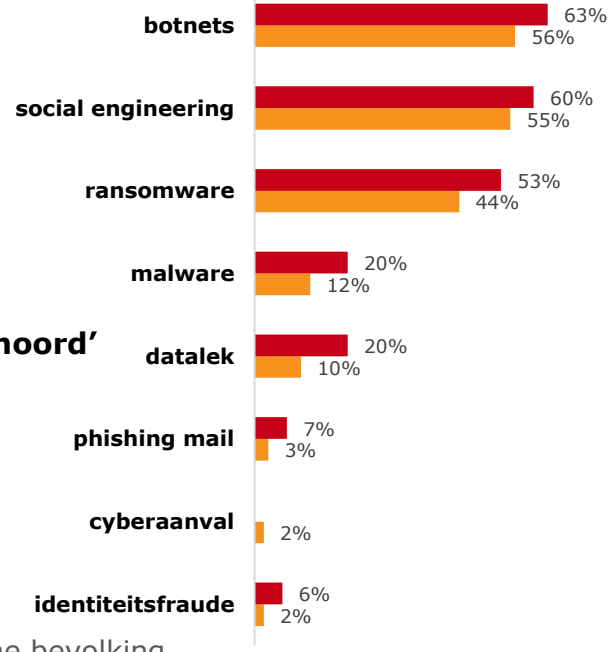
Maatregelen ter preventie van cyber gevaren zijn bekender dan de gevaren zelf, dit is een mogelijke verklaring voor het omzeilen van veiligheidsmaatrelen

- Het aantal Nederlanders dat 'nog nooit gehoord' heeft van veel voorkomende digitale gevaren is over het algemeen groter dan het aantal Nederlanders dat 'nog nooit gehoord' heeft van maatregelen ter preventie van cyber gevaren.
- Ondanks het feit dat deze 'gevaren' en 'maatregelen' niet altijd direct met elkaar in verband staan, is het een aanwijzing dat het bewustzijn en de kennis van het 'waarom' van deze maatregelen gebrekkig is. Dit zou een verklaring kunnen zijn voor de respondenten uit het algemeen publiek (22%) en de werkzame bevolking (13%) die aangeven veiligheidsmaatregelen wel eens te omzeilen.

Bekendheid maatregelen ter preventie cyber gevaren

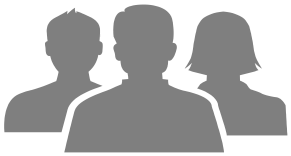


Bekendheid cyber gevaren



Bewustzijn, gebruik en beleid rondom sociaal media laat ruimte tot ontwikkeling zien

- Een fors percentage (16%) van het algemene publiek zegt meestal niet bewust na te denken over de mogelijke gevolgen van het sociale media gebruik. In een samenleving waarin sociale media een steeds prominentere rol inneemt en ook het aantal sociale media kanalen en daarmee de complexiteit toeneemt, is de afwezigheid van het bewustzijn bij deze groep zorgelijk te noemen.
- Onder beleidsmakers (verantwoordelijk voor de digitale en online veiligheid) zegt 4 op de 10 dat het bedrijf geen social media beleid heeft. Het is opvallend dat deze bedrijven wel beleid voeren rondom digitale en online veiligheid, maar dus geen aandacht besteden aan afspraken voor het gebruik van sociale media door medewerkers.



16%

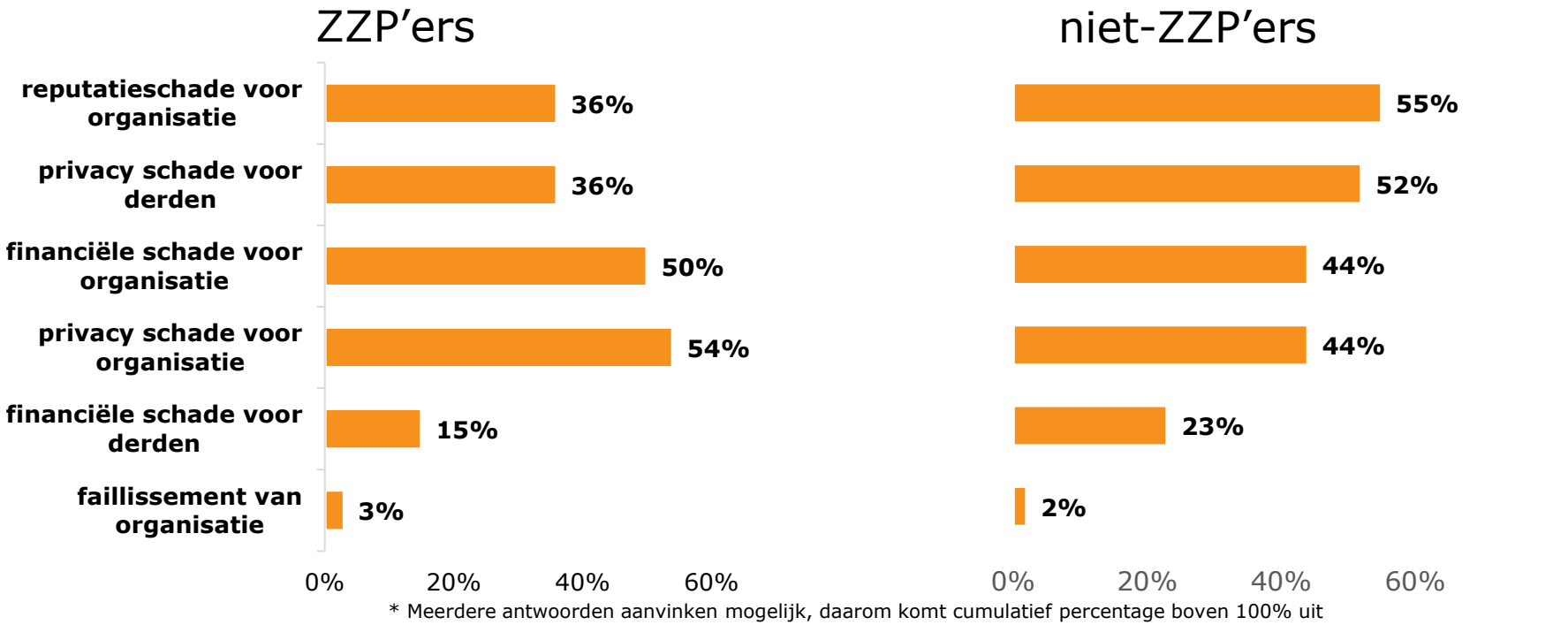
'wanneer ik actief ben op sociale media denk ik meestal **niet bewust** na over de eventuele gevolgen hiervan voor mijzelf en/of mijn vrienden en bekenden'

40%

'mijn bedrijf heeft (zover ik weet) geen social media beleid'

ZZP’ers zien vooral de directe schade voor henzelf en hebben minder oog voor de schade in de keten

- Een grote groep ZZP’ers zegt geen mogelijke gevolgen te zien voor andere organisaties in de keten als gevolg van cyber gevaren. Dit is een opmerkelijke uitkomst aangezien de groep ZZP’ers in Nederland nog steeds groeit en zij daardoor waarschijnlijk steeds vaker deel uit (zullen) maken van een keten.
- Bij de niet-ZZP’ers geeft bijna de helft aan dat de financiële, privacy en reputatieschade het gevolg kunnen zijn van inbreuk op digitale veiligheid in hun werksituatie. Echter hebben maar 6 op de 10 werknemers instructies van hun werkgever gekregen over het veilig gebruik maken van laptop, tablet of smartphone.



* Meerdere antwoorden aanvinken mogelijk, daarom komt cumulatief percentage boven 100% uit

ZZP (n=393) Niet-ZZP (n=1318): Welke mogelijke gevolgen ziet u (vooral) voor u of uw organisatie indien ongewenste inbreuk wordt gemaakt op de digitale veiligheid in uw werksituatie?
Niet-ZZP (n=1318): Heeft u van uw werkgever instructies ontvangen voor het veilig gebruik van uw laptop, tablet of smartphone? Ja 63% Nee 37%

De term datalek is veelal bekend maar maatregelen en het beleid tegen deze dreiging blijven achter

- Slechts 20% van het algemene publiek en 10% van de werkzame bevolking heeft 'nog nooit gehoord' van de term datalek terwijl dit een dreiging is die tot voor kort weinig aandacht kreeg.
- Ondanks de bekendheid van deze dreiging heeft slechts een derde van de organisaties beleid omtrent datalekken. Ook geeft bijna 1 op de 10 aan dat persoons- en/of klantgegevens niet extra beschermd zijn.

34%

'mijn organisatie maakt gebruik van een beveiligde opslag van persoons- en klantgegevens en er is beleid over op welke manier deze gebruikt mogen worden'

8%

'de persoons- en / of klantgegevens binnen mijn organisatie zijn (naast de standaardbeveiliging van host/netwerk) niet extra beschermd'

2

Bewustzijn van cybergevaren en de kennis en houding ten opzichte van deze gevaren

Hacken, virussen, phishing en spam worden spontaan het meest genoemd als cybergevaren

Dit is zo bij zowel het algemeen publiek als de werkzame bevolking het geval.

Algemeen publiek

Werkzame bevolking

Quotes

*"Wifi-wachtwoord te lang onveranderd of **virussen** binnenhalen door downloaden".*

*"**Virussen** binnenhalen, bijvoorbeeld door mail van thuis naar het werk te sturen, als hier een virus inzit heb je het ook in je werkomgeving."*

*"**Virus**, fraude, **phishing** en hierdoor persoonsgegevens of wachtwoorden die onderschept worden."*

*"**Hacken** van privé gegevens."*

*"**Spam** en valse mailtjes."*

*"Wachtwoorden zijn bekend. Verliezen mobiele apparaten. **Phishing**. Usb stick verliezen."*

*"Ik werk voor een opdrachtgever met uitgebreide klantdossiers, **hacken** is een gevaar."*

Algemeen publiek (n=963): Welke gevaren in de digitale / online in uw thuissituatie kunt u spontaan noemen?
Werkzame bevolking (n=1711): Welke gevaren in uw eigen digitale / online omgeving op werk kunt u spontaan noemen?

De bekendheid van het fenomeen ‘datalek’ is fors gestegen

Algemeen publiek is minder bekend met de cybergevaren dan de werkzame bevolking. Voor beide groepen zijn botnets, social engineering en ransomware de meest onbekende cybergevaren. En in mindere mate malware, datalek, phishing mail en identiteitsfraude.

Wat valt op in vergelijking met de vorige meting (2015):

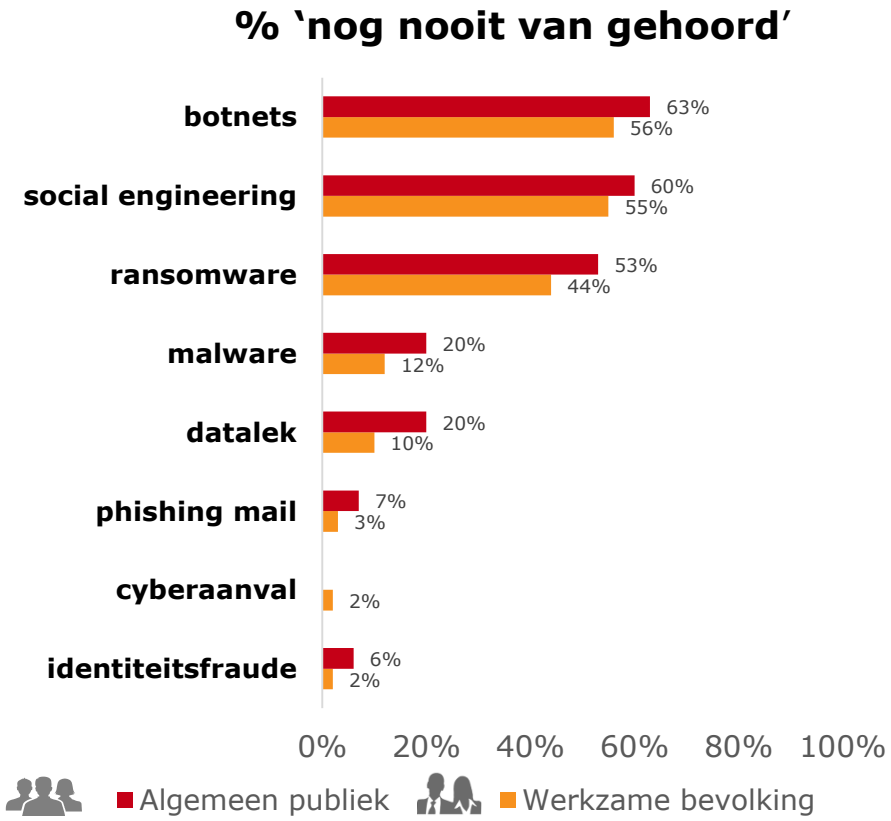
- Wat betreft de onbekendheid met cybergevaren valt vooral het verschil op bij de dreiging ‘ransomware’. In 2015 had 65% van het algemeen publiek en 56% van de werkzame bevolking daar nog nooit van gehoord. In 2016 is de onbekendheid lager, respectievelijk 53% en 44%.

Verschillen op sociaal-demografische kenmerken:

- Bij zowel algemeen publiek als werkzame bevolking zijn malware, botnets, ransomware, social engineering minder bekend onder vrouwen dan mannen. Bij algemeen publiek komt datalek hier nog bij.

- Bij algemeen publiek zijn de alle cybergevaren onder 13-18jarigen het minst bekend met uitzondering van social engineering en datalek. Social engineering is onder 18-30jarigen het minst bekend en datalek onder jongeren (13-18. Onder werkzame bevolking is ransomware onbekender onder 18-30jarigen in vergelijking met de 30+ers.

- In beide groepen geldt: laag en middelbaar opgeleiden zijn minder bekend met de cybergevaren dan hoogopgeleiden. Alleen de bekendheid van identiteitsfraude onder werkzame bevolking verschilt niet significant.

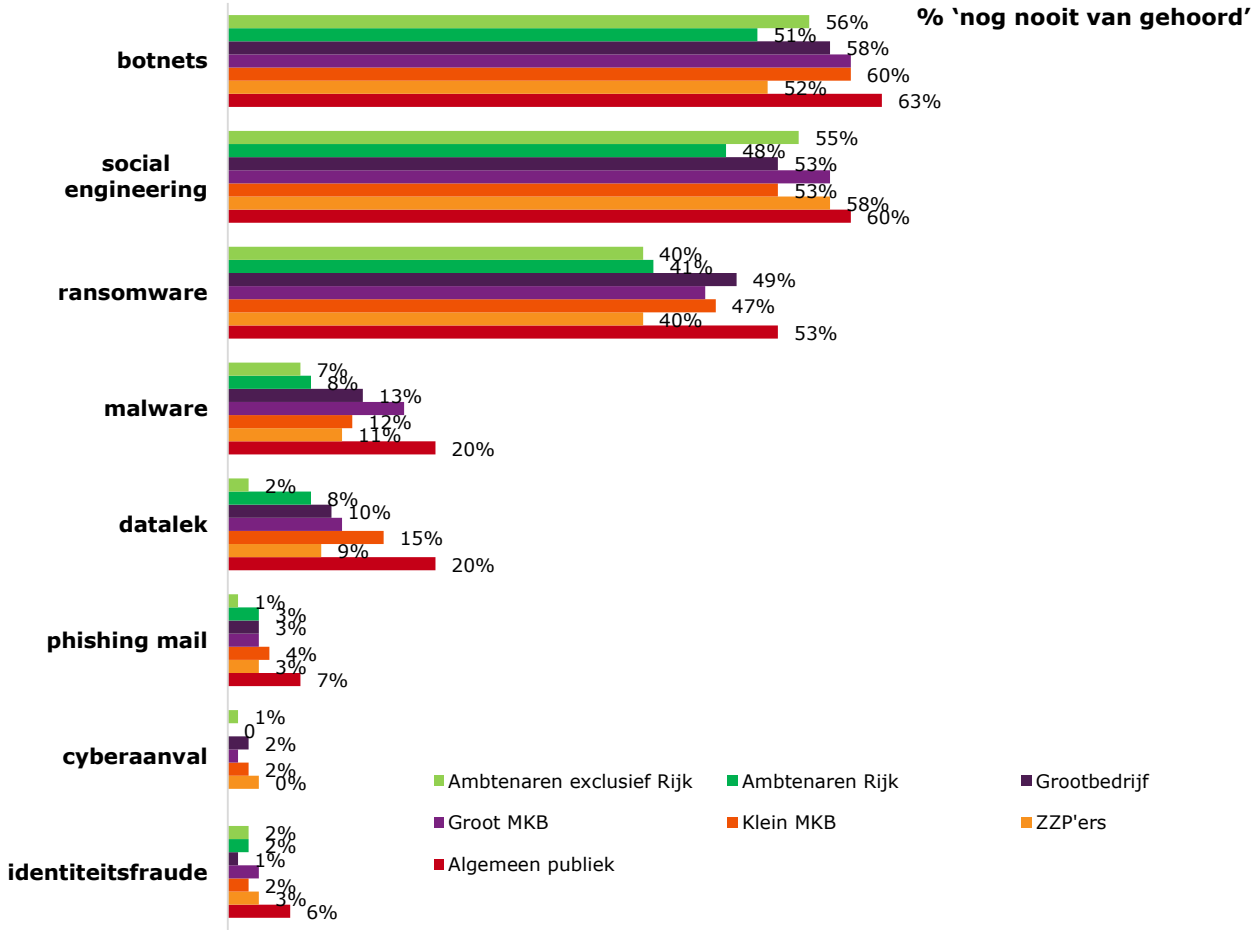


Algemeen publiek (n=963): Kunt u aangeven in welke mate u bekend bent met onderstaande zaken?
Werkzame bevolking (n=1711): Kunt u aangeven in welke mate u bekend bent met onderstaande zaken?

Algemeen publiek is minder bekend met cybergevaren dan werkzame bevolking

Voor alle groepen zijn botnets, social engineering en ransomware de meest onbekende cybergevaren. En in mindere mate malware, datalek, phishing mail en identiteitsfraude.

- Het percentage 'nog nooit van gehoord' is bij bijna alle cybergevaren het laagst voor ambtenaren. Dit betekent dat deze groep over het algemeen beter op de hoogte is dan de overige groepen.



Algemeen publiek (n=963): Kunt u aangeven in welke mate u bekend bent met onderstaande zaken?
Werkzame bevolking (n=1711): Kunt u aangeven in welke mate u bekend bent met onderstaande zaken?

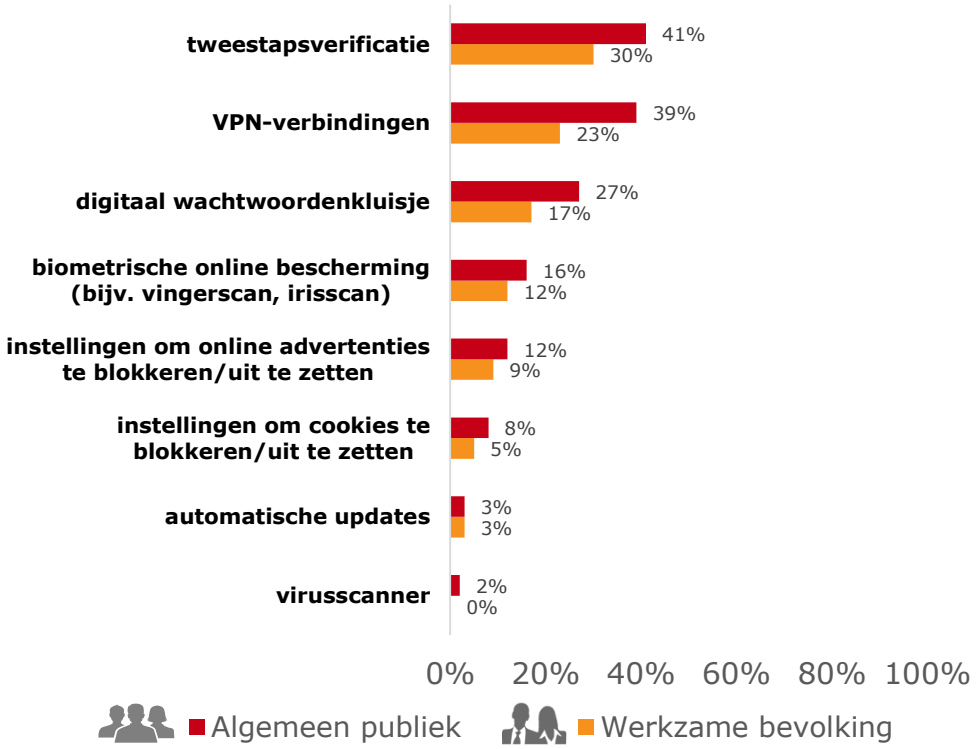
Verschillende vormen van bescherming tegen cybergevaren zijn bekender dan de cybergevaren zelf

Voor alle beschermingstermen geldt dat deze ofwel in gelijke mate ofwel minder bekend zijn bij algemeen publiek dan bij werkzame bevolking. Tweestapsverificatie, VPN-verbindingen en digitaal wachtwoordenkluisje zijn het minst bekend.

Verschillen op sociaal-demografische kenmerken:

- Mannen zijn bekender met beschermingstermen tegen cybergevaren (digitaal wachtwoordenkluisje, tweestapsverificatie, VPN, biometrische online bescherming en online advertenties) dan vrouwen. Dit geldt voor zowel algemeen publiek als werkzame bevolking.
- Met de begrippen VPN en tweestapsverificatie zijn 50+ers minder bekend dan 50-ers, binnen algemeen publiek en werkzame bevolking.
- Hoogopgeleiden zijn, net als met cybergevaren zelf, bekender met beschermingstermen tegen deze gevaren. Alleen bij virusscanner zijn geen significante verschillen te zien. Dit geldt voor beide groepen.

% 'nog nooit van gehoord'

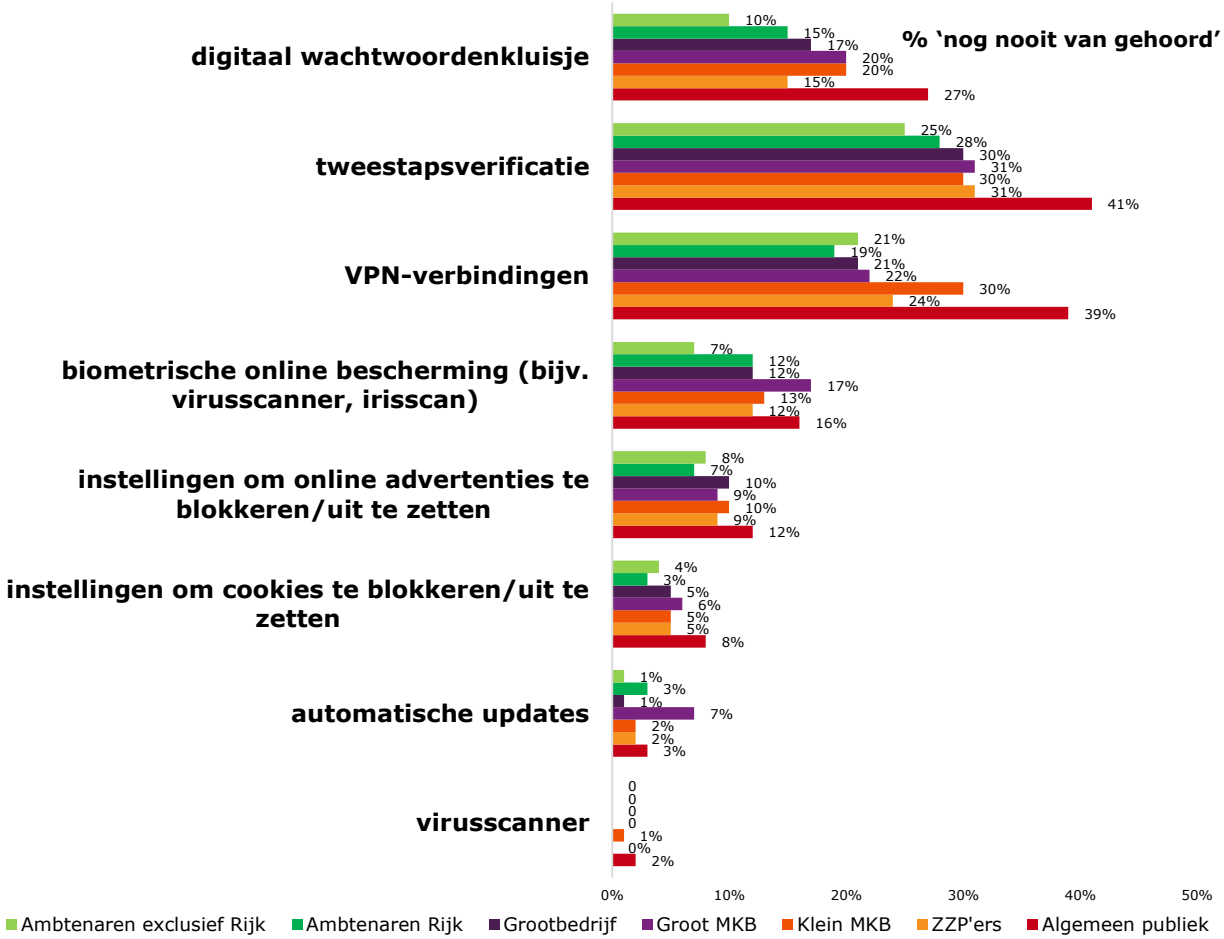


Algemeen publiek (n=963): Kunt u aangeven in welke mate u bekend bent met onderstaande zaken?
Werkzame bevolking (n=1711): Kunt u aangeven in welke mate u bekend bent met onderstaande zaken?

Werkzame bevolking is beter op de hoogte van bescherming tegen cybergevaar dan algemeen publiek

Digitaal wachtwoordenkluisje, tweestapsverificatie en VPN-verbindingen zijn bij alle doelgroepen het minst bekend.

- Net als bij de bekendheid met cybergevaren scoren ook hier beide groepen ambtenaren goed, er bestaat namelijk weinig onwetendheid over de verschillende beschermingstermen.
- Medewerkers binnen het groot MKB hebben vaker 'nooit gehoord' van de verschillende beschermingstermen



Algemeen publiek (n=963): Kunt u aangeven in welke mate u bekend bent met onderstaande zaken?
Werkzame bevolking (n=1711): Kunt u aangeven in welke mate u bekend bent met onderstaande zaken?

7 op de 10 maken zich (zeer) weinig zorgen over hun digitale veiligheid, dit is fors meer dan vorig jaar

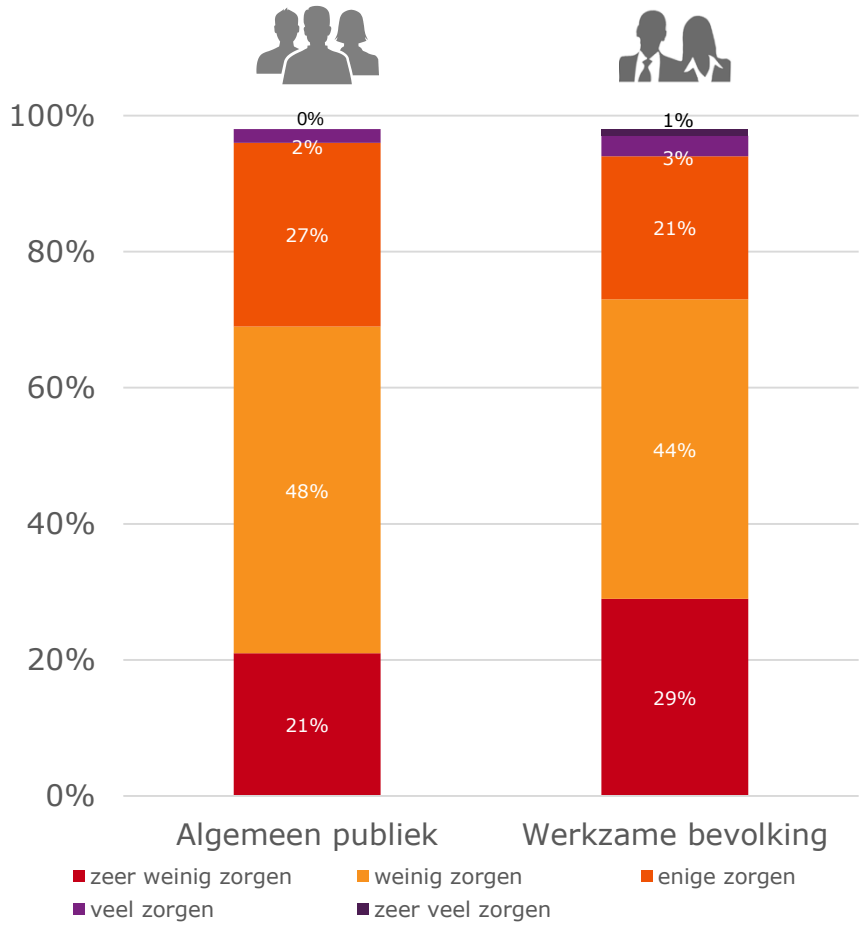
Wat valt op in vergelijking met de vorige meting (2015):

- In vergelijking met vorig jaar maakt een grotere groep van algemeen publiek zich (zeer) weinig zorgen. In 2016 is dat 69% terwijl dat in 2015 nog 47% was.
- Onder de werkzame bevolking is het percentage gelijk aan vorig jaar. Toen maakte 72,5% zich (zeer) weinig zorgen. In 2016 is dit 73%.

Verschillen op sociaal-demografische kenmerken:

- Jong algemeen publiek (18-30jr) geven vaker aan zich (zeer) weinig zorgen te maken over hun digitale veiligheid in vergelijking met 30+ers. Bij de werkzame bevolking maakt de groep 30-50jarigen zich vaker (zeer) weinig zorgen in vergelijking met de jongeren (18-30jr) en ouderen (50+).

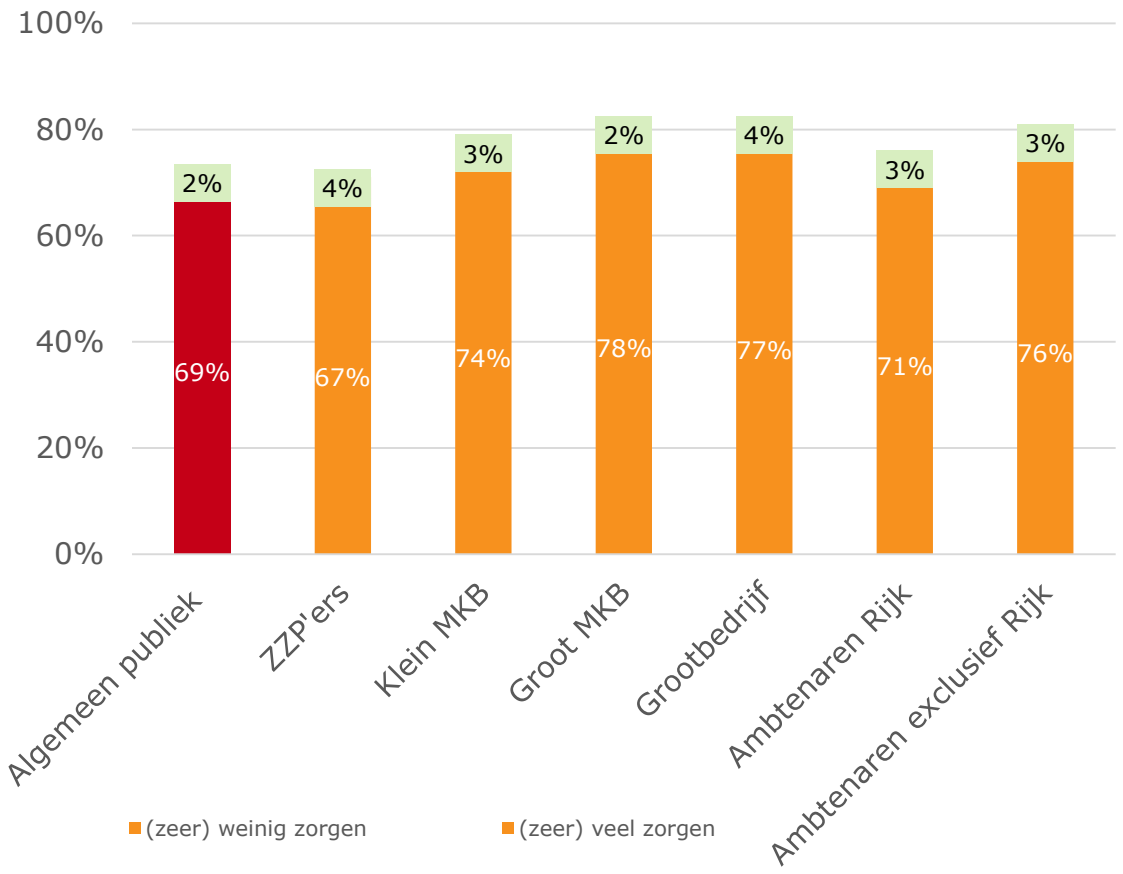
- Van de werkzame bevolking geven mannen vaker aan zich (zeer) veel zorgen te maken dan vrouwen. Hoogopgeleiden van de werkzame bevolking maken zich meer zorgen dan laag en middelbaar opgeleiden.



Algemeen publiek (n=963): In hoeverre maakt u zich zorgen over uw digitale / online veiligheid in uw thuissituatie?
Werkzame bevolking (n=1711): In hoeverre maakt u zich zorgen over uw digitale / online veiligheid in uw werksituatie?

In alle groepen is er slechts een zeer klein gedeelte dat zich (zeer) veel zorgen maakt over de digitale veiligheid

- Ambtenaren Rijk bevat (onder de werkzame bevolking) de kleinste groep personen die zich (zeer) weinig zorgen te maken.



* Grafiek loopt niet tot 100%, overige percentage is 'enige zorgen'

Algemeen publiek (n=963): In hoeverre maakt u zich zorgen over uw digitale / online veiligheid in uw thuissituatie?
Werkzame bevolking (n=1711): In hoeverre maakt u zich zorgen over uw digitale / online veiligheid in uw werksituatie?

Gemiddeld genomen, schatten beide groepen in dat ze (zeer) goede tot uitstekende cyber skills hebben

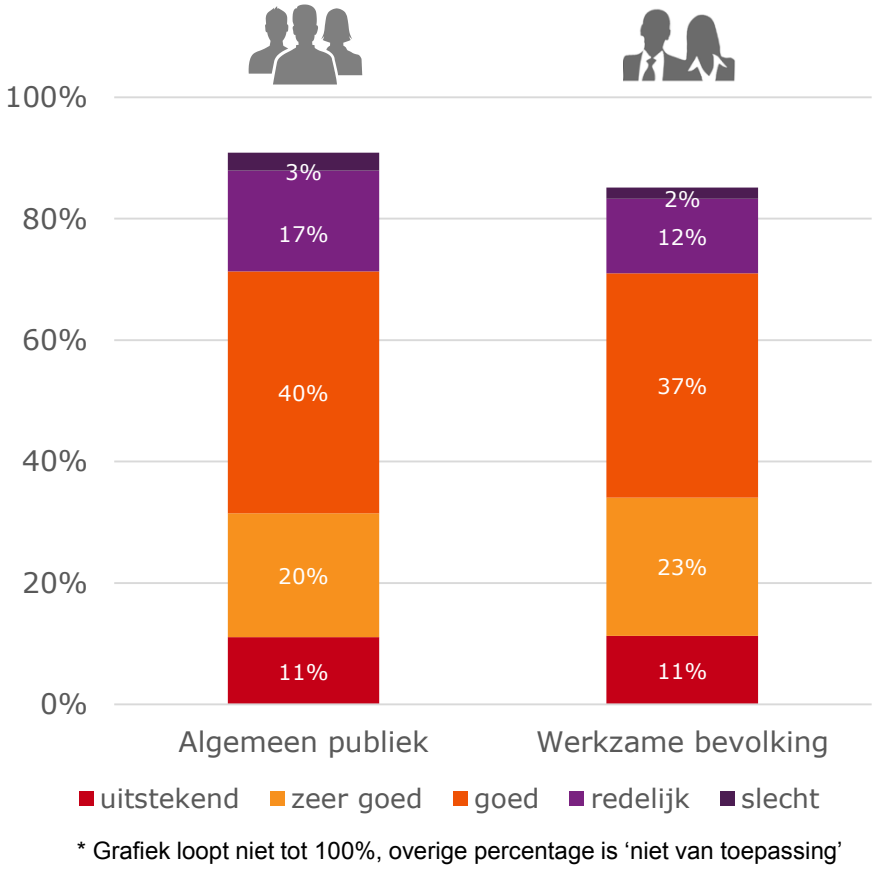
Dit is het gemiddelde van de eigen inschatting om op veilige wijze om te gaan met o.a. beheren en inhoud van wachtwoorden, wifi verbinding, cloud, phishing mails, software, diefstal/verlies/schade en sociale media.

Verschillen op sociaal-demografische kenmerken:

- Binnen algemeen publiek schatten mannen hun eigen cyberskills (beheren & inhoud van wachtwoorden, omgaan met wifi verbinding, cloud, phishing mail en software) hoger in dan vrouwen. Op gebruik sociale media is geen verschil te zien. Binnen de werkzame bevolking schatten mannen zichzelf ook hoger in dan vrouwen. In de beleidsgroep is geen verschil te zien tussen mannen en vrouwen.

- Binnen algemeen publiek geven 13-30jarigen aan veiliger gebruik te kunnen maken van sociale media dan 30+ers. Ook bij werkzame bevolking (niet-ZZP) schatten 20-50jarigen zich hoger in op veilig gebruikmaken van sociale media dan 50+ers. Zelfs oudere beleidmakers (50+) schatten zichzelf lager in op het gebruik van en het beleid maken omtrent sociale media.

- Op sommige cyber skills schatten hoogopgeleiden zichzelf slechter (beheren en inhoud van wachtwoorden, wifi verbinding, cloud, back-up en sociale media) in, op andere juist beter (phishing mail). Bij de werkzame bevolking zijn geen significante trends te zien.



* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Algemeen publiek (n=963): Gemiddelde van alle stellingsvragen: In hoeverre denkt u op een veilige wijze om te gaan met de volgende zaken in de digitale / online omgeving?
Werkzame bevolking (n=1711): Gemiddelde van alle stellingsvragen: In hoeverre denkt u op een veilige wijze om te gaan met de volgende zaken in de digitale / online omgeving?

Ongeveer 4 op de 10 zegt over weinig kennis te beschikken om cybergevaren te bestrijden

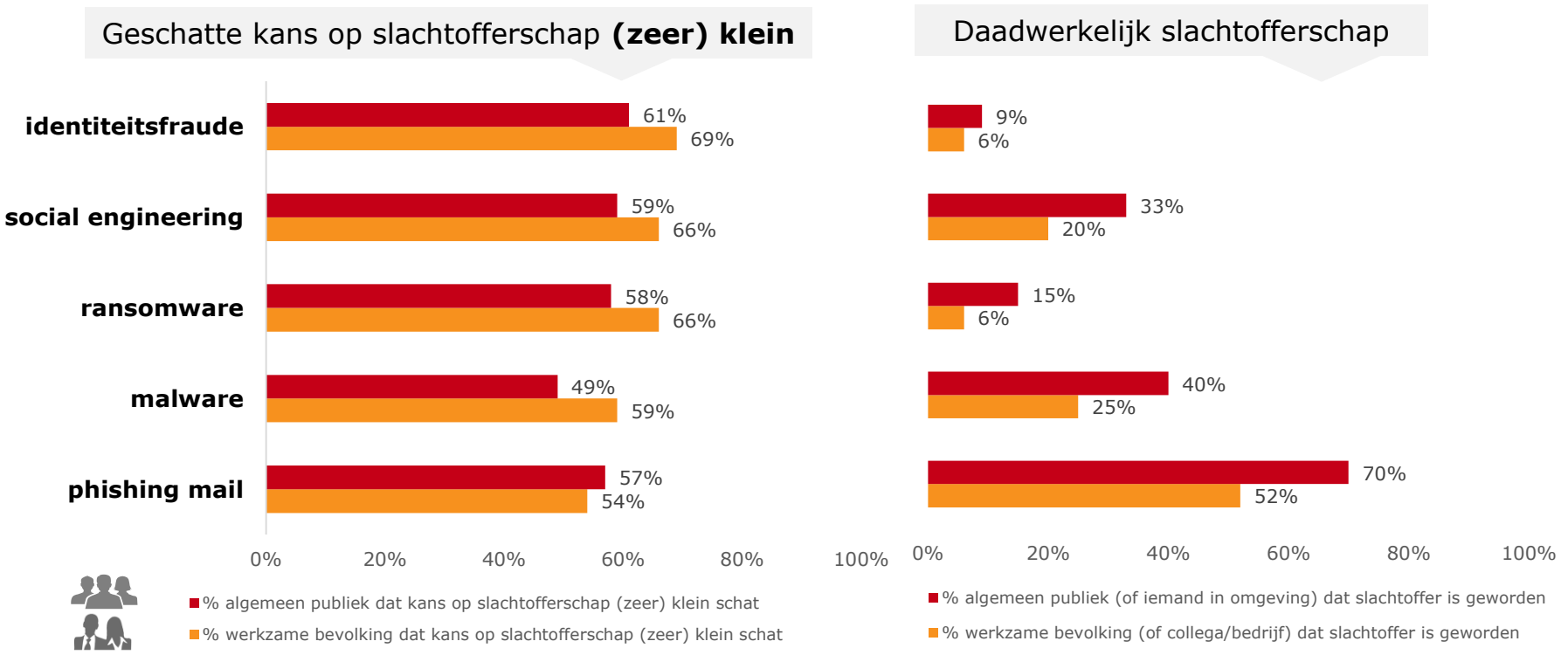
Van deze groep met 'niet zo veel kennis' zeggen stelt ruim 3 op de 10 deze kennis 'nauwelijks toe te kunnen passen'.

Verschillen op sociaal-demografische kenmerken: Mannen (zowel algemeen publiek als de werkzame bevolking) schatten hun kennis en toepasbaarheid van deze kennis hoger in dan vrouwen. Eenzelfde beeld zien we terug bij hoger opgeleiden, ook deze groep schat beide zaken hoger in dan lager en middelbaar opgeleiden. Onder leeftijdsgroepen valt het volgende op: 50+'ers zeggen over minder kennis te beschikken en ook in mindere mate toe te kunnen passen dan de jongere groepen, dit zowel onder de werkenden als het algemeen publiek.

Algemeen publiek (n=963), Werkzame bevolking (n=1711): In welke mate denkt u over de kennis te beschikken om gevaren in de digitale / online omgeving te kunnen bestrijden? In hoeverre denkt u de kennis die u hebt over de bestrijding van gevaren in de digitale / online omgeving ook op een goede manier toe te kunnen passen?

Onder het algemeen publiek (thuis) vallen meer ‘slachtoffers’ dan onder de werkzame bevolking

Hoewel meer dan de helft van het algemeen publiek en werkzame bevolking de kans op slachtofferschap van phishing mails als (zeer) klein schatten, liggen de percentages van daadwerkelijk slachtofferschap boven de 50%. Ook de percentages van daadwerkelijke slachtoffers van social engineering en malware zijn fors te noemen.

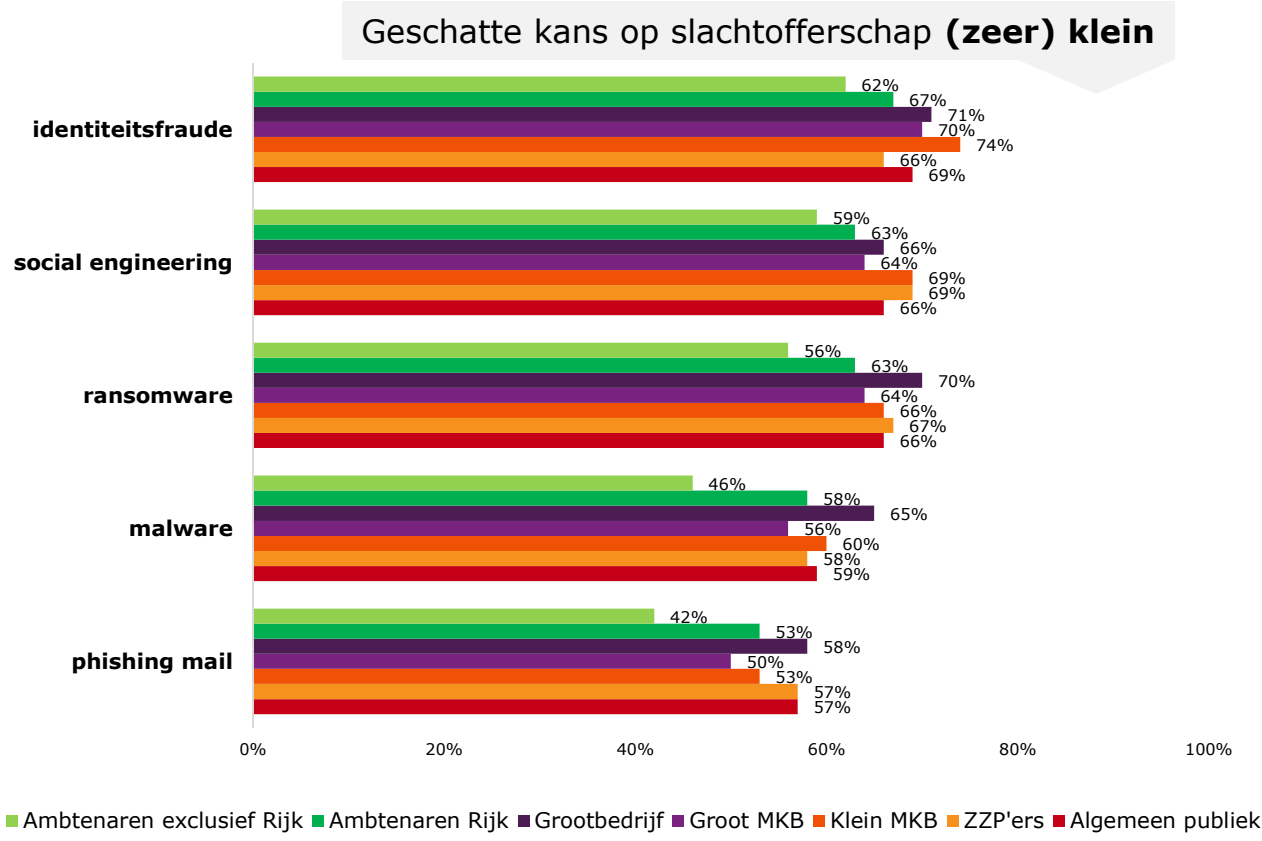


Algemeen publiek (n=963): Hoe groot acht u de kans dat u slachtoffer wordt van de volgende zaken? Heeft u zelf of iemand in uw directe omgeving ooit wel eens te maken gehad met één van de onderstaande voorvallen?
Werkzame bevolking (n=1711): Hoe groot acht u de kans dat u slachtoffer wordt van de volgende zaken? Heeft u of uw bedrijf ooit wel eens te maken gehad met één van onderstaande voorvallen?

Meerderheid van algemeen publiek en werkzame bevolking schat kans op slachtofferschap als (zeer) klein

Beide groepen ambtenaren schatten de kans op slachtofferschap minder vaak in als (zeer) klein.

- Onder werkzame bevolking schatten werknemers grootbedrijf en klein MKB de kans op slachtofferschap het vaakst in als (zeer) klein.

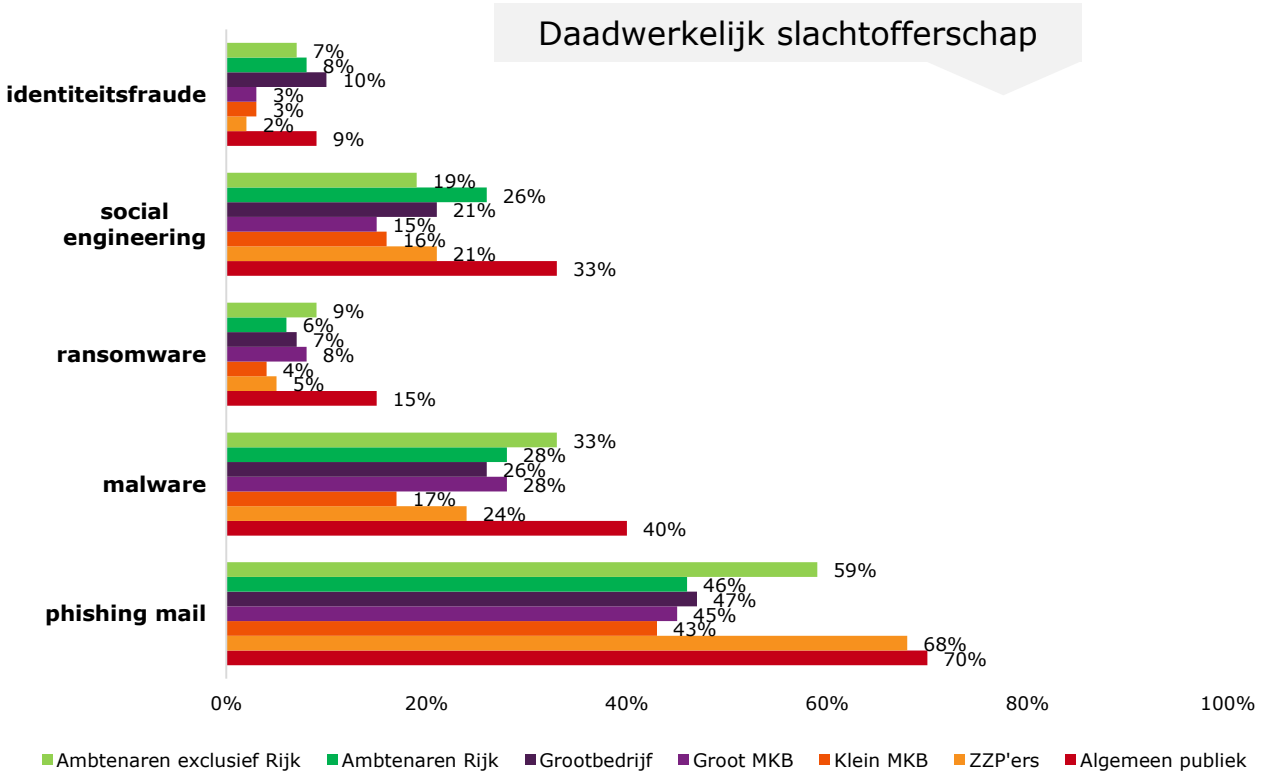


Algemeen publiek (n=963): Hoe groot acht u de kans dat u slachtoffer wordt van de volgende zaken? Heeft u zelf of iemand in uw directe omgeving ooit wel eens te maken gehad met één van de onderstaande voorvallen?
Werkzame bevolking (n=1711): Hoe groot acht u de kans dat u slachtoffer wordt van de volgende zaken? Heeft u of uw bedrijf ooit wel eens te maken gehad met één van onderstaande voorvallen?

In de thuissituatie (algemeen publiek) vallen meer ‘slachtoffers’ dan in de werksituatie (werkzame bevolking)

Hoewel meer dan de helft van het algemeen publiek en werkzame bevolking de kans op cybergevaren als (zeer) klein schatten, liggen de percentages van daadwerkelijk slachtofferschap (van bijv. malware en phishing) hoger dan de inschatting

- Onder de werkzame bevolking zijn ambtenaren (vooral exclusief rijk) relatief vaker slachtoffer, vooral van ransomware, malware en phishing mail. Dit komt ook overeen met hun eigen inschatting die negatiever is dan de andere groepen (zie vorige slide).



Algemeen publiek (n=963): Heeft u zelf of iemand in uw directe omgeving ooit wel eens te maken gehad met één van de onderstaande voorvallen?
Werkzame bevolking (n=1711): Heeft u of u of uw organisatie ooit wel eens te maken gehad met één van onderstaande voorvallen?

Verschillen op sociaal-demografische kenmerken met betrekking tot slachtofferschap van cybergevaren

Verschillen op sociaal-demografische kenmerken:

Geschatte kans op slachtofferschap

- Onder algemeen publiek schatten mannen de kans op slachtofferschap op cybergevaren (phishing mail, malware, identiteitsfraude en datalek) kleiner in dan vrouwen. Bij de werkzame bevolking is het tegenovergestelde te zien; hier schatten mannen de kans slachtoffer te worden van cybergevaren (malware, identiteitsfraude, botnets, ransomware, datalek, cyberaanval) groter in.
- Oudere werkzame bevolking (50+) denken sneller slachtoffer te worden van phishing, datalek en cyberaanval dan 18-30jarigen.
- Hoogopgeleiden binnen algemeen publiek denken minder snel slachtoffer te worden van phishing mail, maar sneller van botnets in vergelijking met laagopgeleiden. Bij de werkzame bevolking denken laagopgeleiden minder snel slachtoffer te worden van cybergevaren (alle) dan hoogopgeleiden.

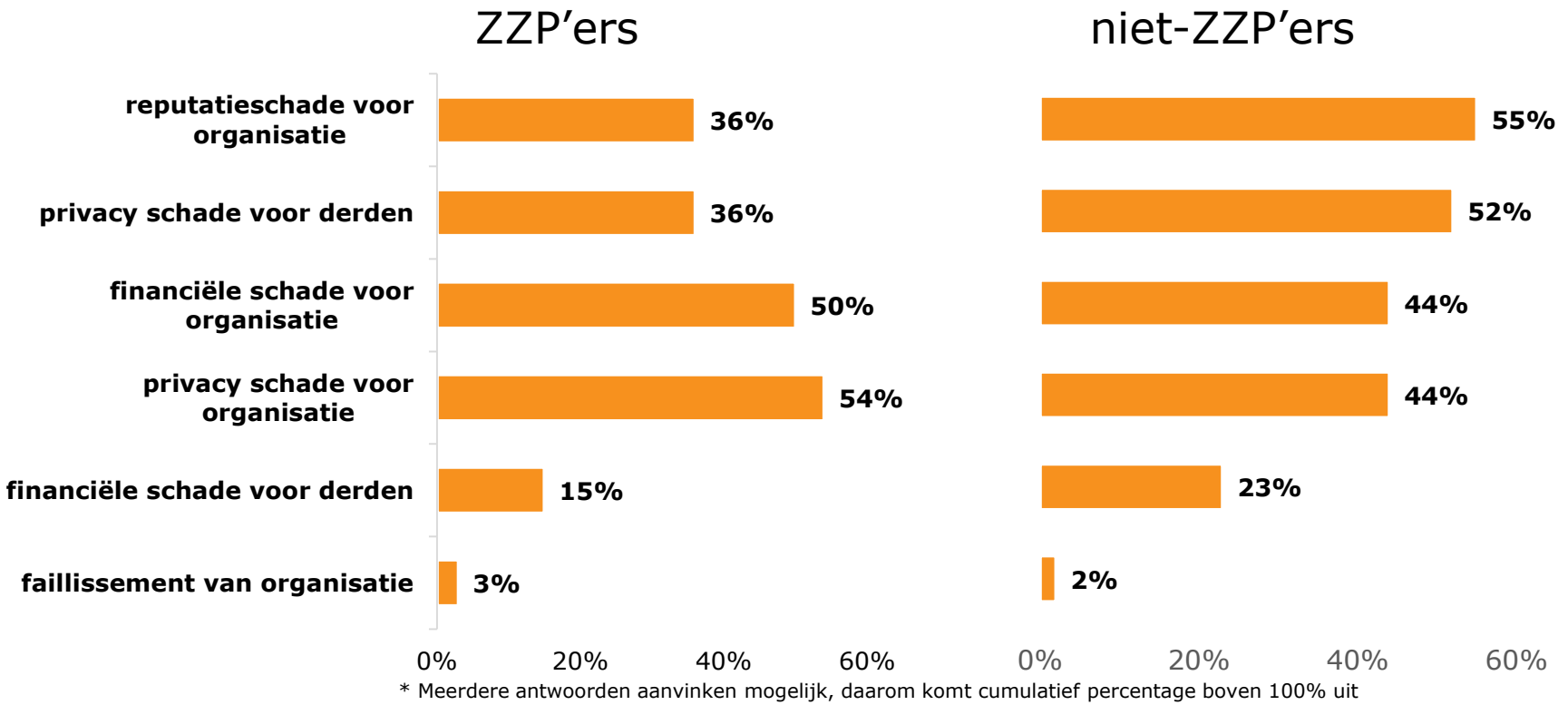
Daadwerkelijk slachtofferschap

- Hoewel mannen binnen algemene publiek de kans op slachtofferschap lager inschatten, worden ze zelf sneller slachtoffer dan vrouwen van cybergevaren (malware, computeruitval door virus, identiteitsfraude, social engineering, ransomware, oplichting bij online aankopen). Voor de werkzame bevolking niet-ZZP groep is dit ook het geval, bij ZZP'ers is geen significant verschil tussen mannen en vrouwen in daadwerkelijk slachtofferschap.
- 50+ers worden sneller slachtoffer van social engineering in vergelijking met 18-30 jarigen binnen algemeen publiek. Bij de werkzame bevolking is vooral het aantal 50+ slachtoffers binnen de ZZP groep opvallend: dit is op malware, phishing mail, spam, social engineering en acquisitie fraude.
- Hoogopgeleiden worden vaker slachtoffer van malware, spam, phishing mail en social engineering in zowel algemeen publiek en werkzame bevolking. Bij niet-ZZP'ers komen hier nog acquisitie fraude, botnets en identiteitsfraude bij.

Algemeen publiek (n=963) Werkzame bevolking (n=1711): Hoe groot acht u de kans dat u slachtoffer wordt van de volgende zaken? Heeft u zelf of iemand / Heeft u of uw bedrijf in uw directe omgeving ooit wel eens te maken gehad met één van de onderstaande voorvallen?

ZZP’ers zien vooral de directe schade voor henzelf en hebben minder oog voor de schade in de keten

ZZP’ers zien meer schade voor zichzelf/hun bedrijf. Opvallend is dat bijna de helft van de niet-ZZP’ers aangeeft dat financiële, privacy en reputatieschade het gevolg kunnen zijn van inbreuk op digitale veiligheid in hun werksituatie, heeft 37% van hen geen instructies van hun werkgever gekregen over het veilig gebruik maken van laptop, tablet of smartphone.



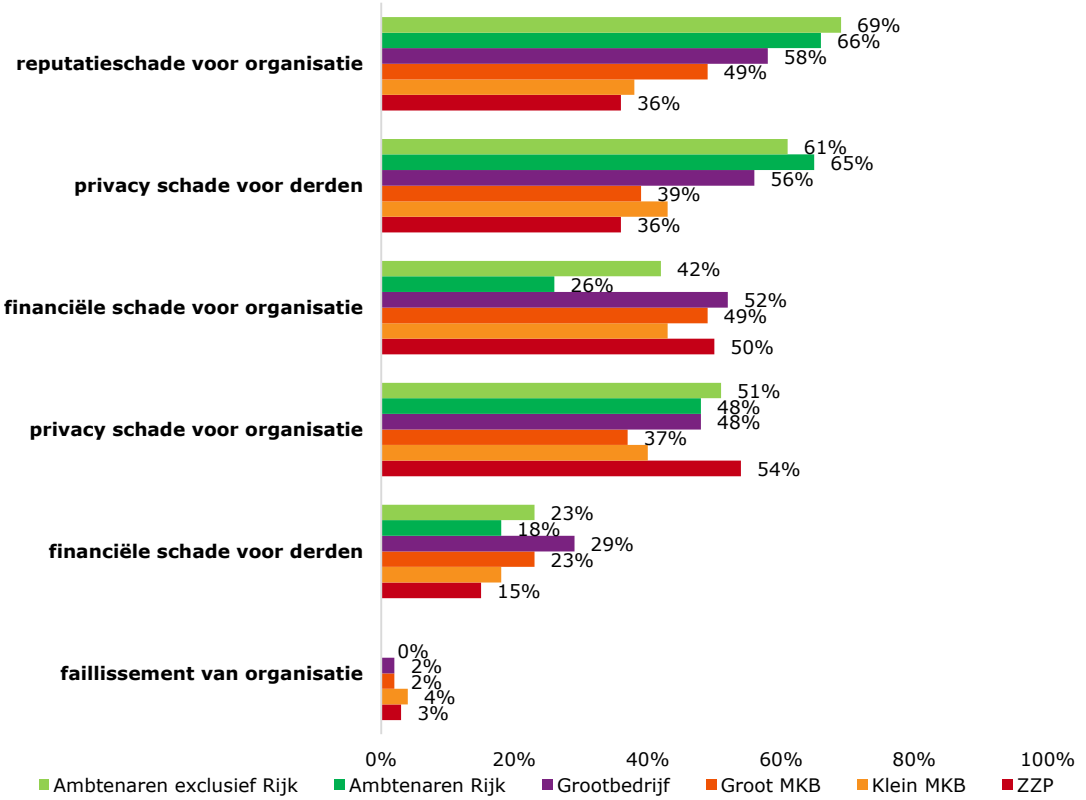
* Meerdere antwoorden aanvinken mogelijk, daarom komt cumulatief percentage boven 100% uit

ZZP (n=393) Niet-ZZP (n=1318): Welke mogelijke gevolgen ziet u (vooral) voor u of uw organisatie indien ongewenste inbreuk wordt gemaakt op de digitale veiligheid in uw werksituatie?
Niet-ZZP (n=1318): Heeft u van uw werkgever instructies ontvangen voor het veilig gebruik van uw laptop, tablet of smartphone? Ja 63% Nee 37%

Faillissement wordt door werknemers binnen commercie zelden gezien als een gevolg van de inbreuk op digitale veiligheid

Ambtenaren schatten gevolgen hoog in op het gebied van reputatie en privacy voor organisatie. Ook de privacy schade voor derden wordt vaak genoemd door de (Rijks)ambtenaren.

- ZZP'ers zien vooral financiële en privacy schade voor zichzelf/hun bedrijf.
- Opvallend is dat reputatieschade voor de organisatie minder vaak wordt genoemd door groot MKB, klein MKB en ZZP'ers.



* Meerdere antwoorden aanvinken mogelijk, daarom komt cumulatief percentage boven 100% uit

ZZP (n=393) Niet-ZZP (n=1318): Welke mogelijke gevolgen ziet u (vooral) voor u of uw organisatie indien ongewenste inbreuk wordt gemaakt op de digitale veiligheid in uw werksituatie? Niet-ZZP (n=1318)

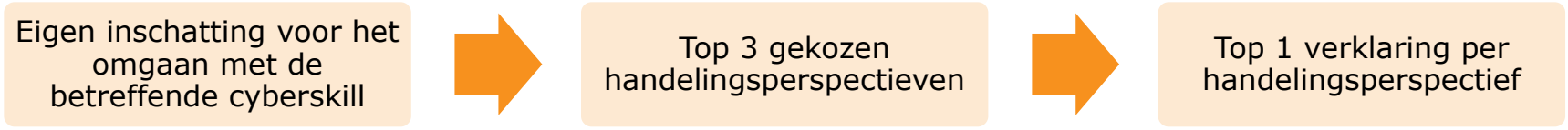
3

Het niveau van cybersecurity skills in Nederland

Leeswijzer

In dit hoofdstuk geven we een overzicht van de gekozen handelingsperspectieven (en verklaringen) ten opzichte van eigen inschatting van cybersecurity skills. Er worden 8 thema's behandeld: gebruik wifi verbinding, omgaan met phishing mail, updaten van software, gebruik sociale media, beleid sociale media, gebruik cloud, maken van back-ups, beheren van wachtwoorden, inhoud van wachtwoorden en omgaan met persoons- en klantgegevens. Enkele thema's zijn doelgroep specifiek (bijv. persoons- en klantgegevens alleen voor werkzame bevolking), dit is aangegeven in de conclusie van de slide.

Op elke slide worden drie 'stappen' behandeld met betrekking tot de cybersecurity skill (in het rood de werkzame bevolking, in het geel - zoals hieronder - het algemeen publiek en in het groen de overige opvallende bevindingen):



Er zijn dus 3 vragen gesteld om tot deze indeling te komen, hier volgt het voorbeeld van 'het beheren van wachtwoorden'.

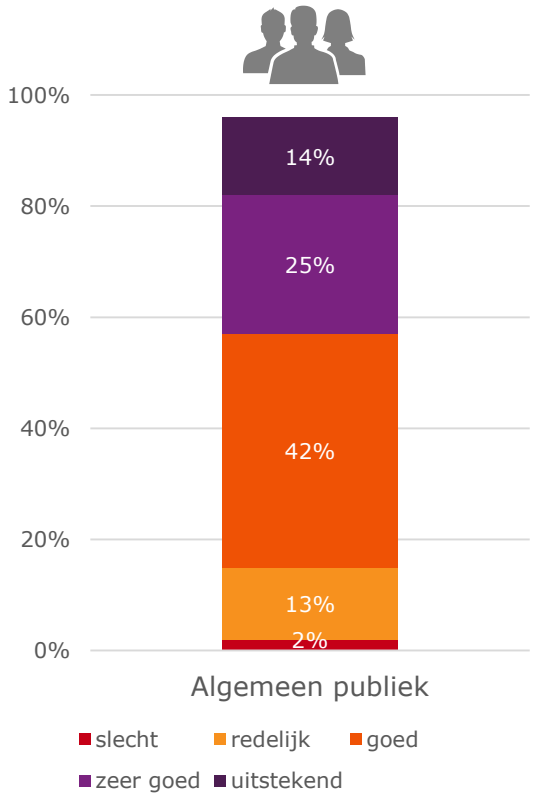
Voor de eigen inschatting is de volgende vraag gesteld: *In hoeverre denkt u op een veilige wijze om te gaan met 'het beheren van wachtwoorden' in de digitale / online omgeving? Slecht – redelijk – goed – zeer goed – uitstekend*.

De Top 3 gekozen handelingsperspectieven komt voort uit een aantal stellingen die worden voorgelegd met de vraag: *Kunt u aangeven welke stelling op u het meest van toepassing is?* In dit hoofdstuk zijn de top 3 meest gekozen handelingsperspectieven beschreven.

Na het beantwoorden van zo'n stellingvraag is de vraag *Kunt u aangeven waarom u kiest voor deze optie in de beschreven situatie?* gesteld waarna er 7 mogelijke antwoordopties volgden. In het overzicht is de meest beantwoorde antwoordoptie (top 1) weergegeven.

Van het algemeen publiek heeft 1 op de 10 zijn/haar wifi verbinding thuis niet beveiligd

Eigen inschatting gebruik wifi verbinding	Top 3 gekozen handelingsperspectieven	Top 1 verklaring per handelingsperspectief



55%
‘mijn wifi verbinding thuis is vergrendeld met een zelfverzonnen (en dus zelf gewijzigd) wachtwoord’

57%
hiervan zegt dit de meest veilige optie te vinden

40%
‘mijn wifi verbinding thuis is vergrendeld met een standaardwachtwoord (bijv. die op mijn router stond)’

32%
hiervan denkt dat deze optie voldoende veiligheid biedt

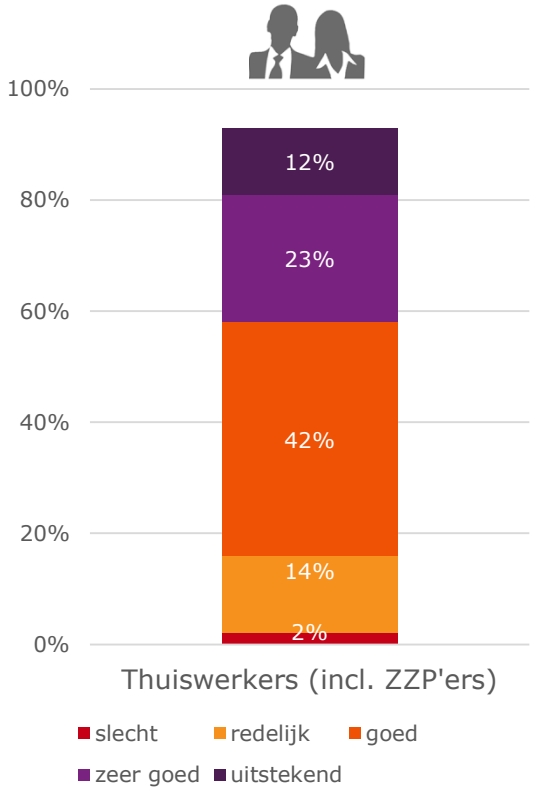
10%
‘mijn wifi verbinding thuis is niet beveiligd maar mijn apparaten die zijn verbonden zijn wel beveiligd met een wachtwoord’

41%
hiervan denkt dat deze optie voldoende veiligheid biedt

* Grafiek loopt niet tot 100%, overige percentage is ‘niet van toepassing’

Bij de thuiswerkers (incl. ZZP'ers) is het percentage onbeveiligde wifi verbindingen aanzienlijk lager

Eigen inschatting gebruik wifi verbinding → Top 3 gekozen handelingsperspectieven → Top 1 verklaring per handelingsperspectief



66%
'mijn verbinding thuis is vergrendeld met een zelfverzonnen (en dus zelf gewijzigd) wachtwoord'

58%
hiervan zegt dit de meest veilige optie te vinden

17%
'mijn verbinding thuis is vergrendeld met een standaardwachtwoord (bijv. die op mijn router stond)'

37%
hiervan denkt dat deze optie voldoende veiligheid biedt

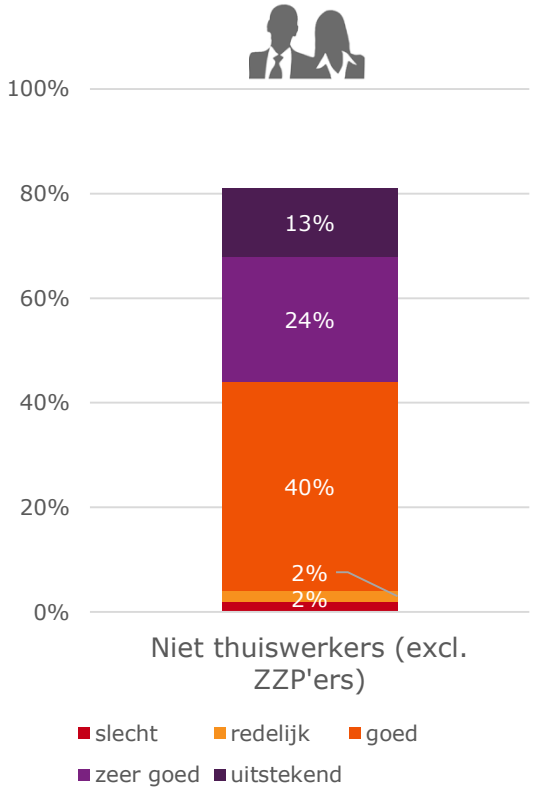
2%
'mijn verbinding is niet beveiligd maar mijn apparaten die zijn verbonden zijn wel beveiligd met een wachtwoord'

32%
hiervan zegt dit de meest veilige optie te vinden

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

1/5e van mensen die onderweg werken denkt dat inloggen op openbare netwerken zonder inlog voldoende veilig is

Eigen inschatting gebruik wifi verbinding → Top 3 gekozen handelingsperspectieven → Top 1 verklaring per handelingsperspectief



35%
'ik maak doorgaans geen gebruik van openbare netwerken'

→ **60%** hiervan zegt dit de meest veilige optie te vinden

20%
'ik maak doorgaans gebruik van openbare netwerken waar je op moet inloggen'

→ **38%** hiervan denkt dat deze optie voldoende veiligheid biedt

18%
'ik maak doorgaans gebruik van openbare netwerken die op dat moment beschikbaar zijn (zowel met als zonder inlog)'

→ **23%** hiervan denkt dat deze optie voldoende veiligheid biedt

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Wifi: ZZP'ers en Ambtenaren exclusief Rijksoverheid vinden openbare netwerken onveiliger dan overige werkenden

Eigen inschatting gebruik wifi verbinding → Handelingsperspectieven → Verklaring voor gekozen handelingsperspectief

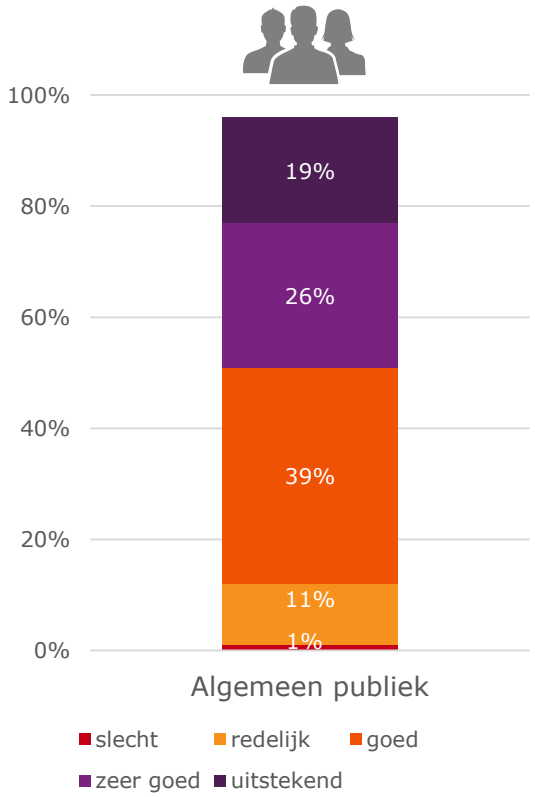
- ZZP'ers en MKB medewerkers schatten hun eigen skills om een veilige wifi verbinding te realiseren lager in dan medewerkers grootbedrijf en ambtenaren.

- Ongeveer 40% van de ZZP'ers en Ambtenaren exclusief Rijksoverheid geven aan doorgaans geen gebruik van openbare netwerken te maken. Onder de overige werkenden (MKB, grootbedrijf en Rijksambtenaren) is dit 30%.

- De ZZP'ers en Ambtenaren exclusief Rijksoverheid die aangeven doorgaans geen gebruik te maken van openbare netwerken geven als verklaring dit onveilig te vinden. Deze wijze van internetverbinding is voor een groot gedeelte van deze groep dus onacceptabel.

Meer dan de helft van het algemeen publiek verwijdert verdachte/mogelijke phishing mail direct

Eigen inschatting omgaan met phishing mail



Top 3 gekozen handelingsperspectieven

57%
'ik negeer de mail en verwijder deze direct'

22%
'ik neem contact op met de desbetreffende organisatie of persoon om te checken of de mail inderdaad is verstuurd door deze organisatie of persoon'

8%
'ik negeer de mail en doe niets'

Top 1 verklaring per handelingsperspectief

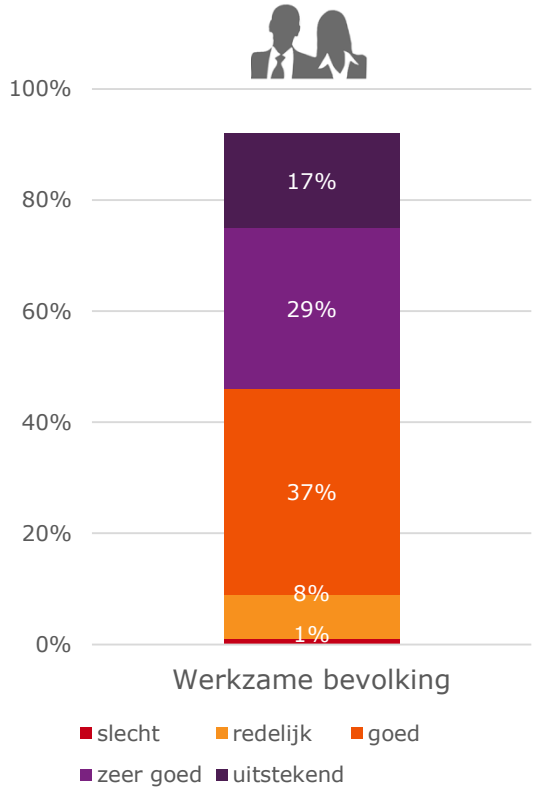
56% hiervan zegt dit de meest veilige optie te vinden

58% hiervan zegt dit de meest veilige optie te vinden

37% hiervan zegt dit de meest veilige optie te vinden

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

De werkzame bevolking meldt of checkt verdachte mail eerder bij iemand binnen of buiten de organisatie

Eigen inschatting omgaan met phishing mail	Top 3 gekozen handelingsperspectieven	Top 1 verklaring per handelingsperspectief
	**36%** ‘ik negeer de mail en verwijder deze direct’	**55%** hiervan zegt dit de meest veilige optie te vinden
	23% ‘ik neem contact op met de desbetreffende organisatie of persoon om te checken of de mail inderdaad is verstuurd door deze organisatie of persoon’	**62%** hiervan zegt dit de meest veilige optie te vinden
	18% ‘ik meld het bij de verantwoordelijke binnen mijn organisatie en buiten de organisatie (bv. politie, spamklacht, fraudehelpdesk, etc)’	**49%** hiervan zegt dit de meest veilige optie te vinden

* Grafiek loopt niet tot 100%, overige percentage is ‘niet van toepassing’

Phishing mail: merendeel algemeen publiek en ZZP'ers zijn voor bescherming op zichzelf aangewezen en verwijderen mail direct

Eigen inschatting omgaan met phishing mail → Handelingsperspectieven → Verklaring voor gekozen handelingsperspectief

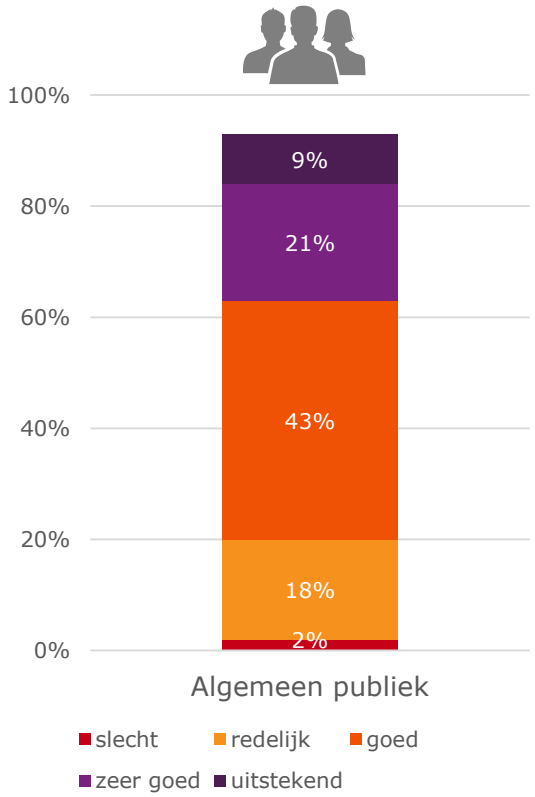
- MKB medewerkers en Ambtenaren exclusief Rijksoverheid schatten hun eigen skills om veilig met phishing mails om te gaan lager in dan de overige doelgroepen (het algemeen publiek, medewerkers grootbedrijf en Rijksambtenaren).

- Het type organisatie blijkt invloed te hebben op hoe werkenden omgaan met phishing mails. Het merendeel van de ZZP'ers zeggen de mail te verwijderen of na te gaan of de mail authentiek is. Medewerkers van bedrijven of ambtenaren maken eerder melding van een verdachte mail bij de verantwoordelijke binnen organisatie en buiten de organisatie (bv. politie, spamklacht, fraudehelpdesk).

- In de gegeven verklaringen zitten geen opvallende verschillen tussen de doelgroepen.

Bij algemeen publiek wordt automatisch updaten van software als meest gekozen

Eigen inschatting omgaan met software → Top 3 gekozen handelingsperspectieven → Top 1 verklaring per handelingsperspectief



48%
'ik heb automatisch updaten aangezet/ingesteld'

45%
hiervan zegt dit de meest veilige optie te vinden

23%
'ik stel het uit tot een gelegen moment (en doe het dan wel)'

32%
hiervan zegt dit de meest veilige optie te vinden

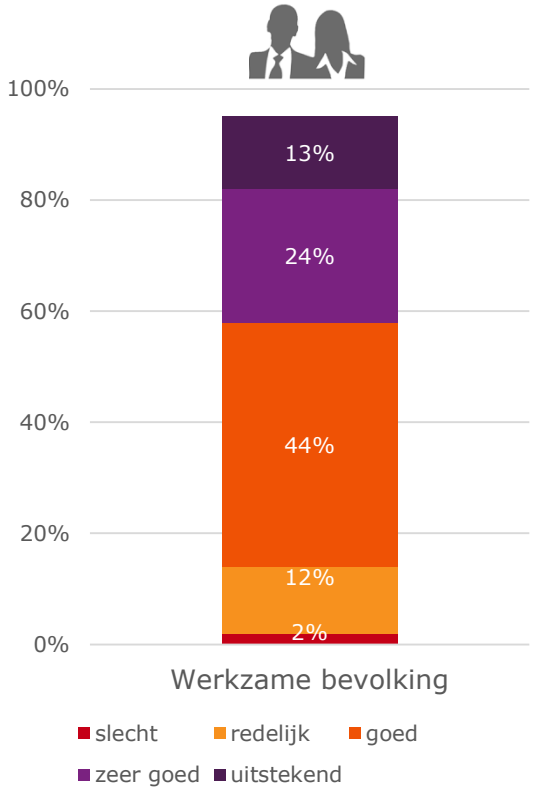
18%
'ik update direct als ik een melding krijg'

40%
hiervan zegt dit de meest veilige optie te vinden

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Bij ZZP'ers wordt de software bij een melding geupdate of wordt hiermee gewacht tot een gelegen moment

Eigen inschatting omgaan met software → Top 3 gekozen handelingsperspectieven → Top 1 verklaring per handelingsperspectief



37%
'ik stel het uit tot een gelegen moment (en doe het dan wel)'

69%
hiervan denkt dat deze optie voldoende veiligheid biedt

29%
'ik update direct als ik een melding krijg'

50%
hiervan zegt dit de meest veilige optie te vinden

25%
'ik heb automatisch updaten aangezet/ingesteld'

51%
hiervan zegt dit de meest veilige optie te vinden

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Omgaan met software: algemeen publiek kiest vaker voor automatisch updaten van software dan ZZP'ers

Eigen inschatting omgaan met software → Handelingsperspectieven → Verklaring voor gekozen handelingsperspectief

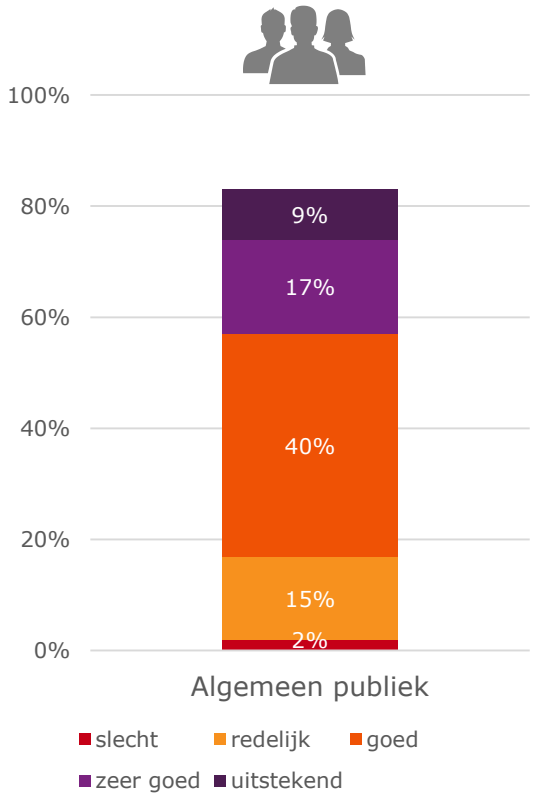
- Tussen het algemene publiek en de ZZP'ers zit geen verschil in de eigen inschatting over omgang met software (onder andere het doen van updates). Overige werkenden hebben deze vraag niet gekregen omdat de omgang met software vaak door een andere persoon of afdeling wordt gedaan.

- Onder algemeen publiek kiest bijna de helft voor het automatisch updaten van software terwijl dit onder ZZP'ers een kwart is. Verder geven bijna 4 op de 10 ZZP'ers aan dit op een beter gelegen moment te doen.

- In de gegeven verklaringen zitten geen opvallende verschillen tussen de twee doelgroepen.

Algemeen publiek: 16% denkt niet bewust na over de gevolgen tijdens sociaal media gebruik

Eigen inschatting gebruik sociale media → Top 3 gekozen handelingsperspectieven → Top 1 verklaring per handelingsperspectief



69%
'wanneer ik actief ben op sociale media (bv. berichten plaats) denk ik meestal **bewus**t na over de eventuele gevolgen hiervan voor mijzelf en/of mijn vrienden en bekenden'

42%
hiervan zegt dit de meest veilige optie te vinden

16%
'wanneer ik actief ben op sociale media (bv. berichten plaats) denk ik meestal **niet bewust** na over de eventuele gevolgen hiervan voor mijzelf en/of mijn vrienden en bekenden'

49%
hiervan zegt hier nooit eerder over nagedacht te hebben

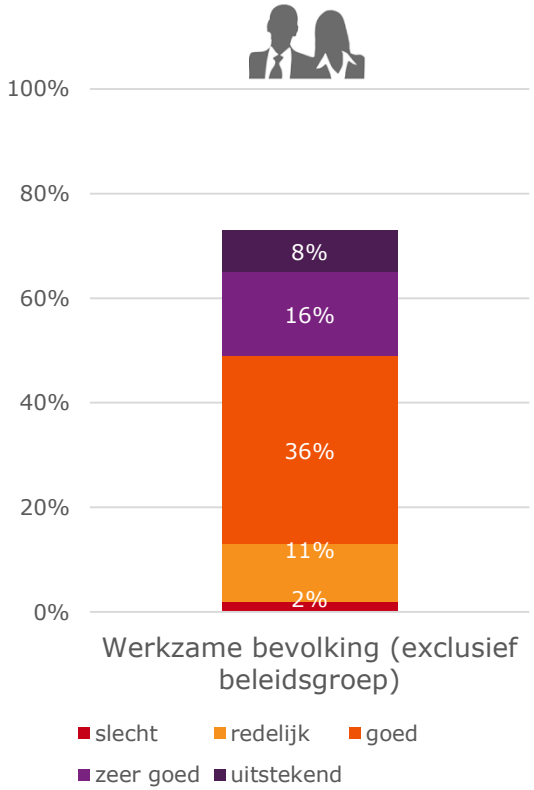
6%
'ik maak geen gebruik van sociale media'

28%
hiervan zegt dit de meest veilige optie te vinden

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Dit is vergelijkbaar voor de aantallen die te zien zijn bij de werkzame bevolking

Eigen inschatting gebruik sociale media → Top 3 gekozen handelingsperspectieven → Top 1 verklaring per handelingsperspectief



68%
'wanneer ik actief ben op sociale media (bv. berichten plaats) denk ik meestal **bewus**t na over de eventuele gevolgen hiervan voor mijzelf en/of mijn vrienden en bekenden'

49%
hiervan zegt dit de meest veilige optie te vinden

12%
'wanneer ik actief ben op sociale media (bv. berichten plaats) denk ik meestal **niet bewust** na over de eventuele gevolgen hiervan voor mijzelf en/of mijn vrienden en bekenden'

36%
hiervan zegt hier nog nooit eerder over nagedacht te hebben

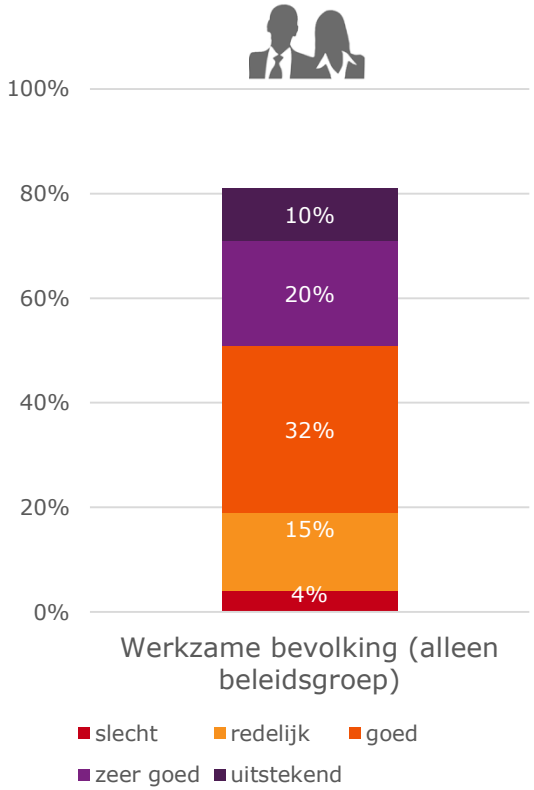
11%
'ik maak geen gebruik meer van sociale media'

23%
hiervan zegt dit de meest veilige optie te vinden

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Beleidsmakers ‘weten niet waarom’ ruim een derde van hun bedrijven geen sociaal media beleid hebben

Eigen inschatting beleid sociale media → Top 3 gekozen handelingsperspectieven → Top 1 verklaring per handelingsperspectief



44%
‘mijn bedrijf heeft een sociale media beleid en controleert ook regelmatig op basis van dit beleid’

43%
hiervan zegt dat dit de meest veilige optie is volgens mij(n organisatie)

40%
‘mijn bedrijf heeft (zover ik weet) geen sociaal media beleid’

32%
hiervan zegt niet te weten waarom

16%
‘mijn bedrijf heeft een sociale media beleid en controleert dit nooit’

29%
hiervan zegt niet te weten waarom

* Grafiek loopt niet tot 100%, overige percentage is ‘niet van toepassing’

Gebruik sociale media: ambtenaren exclusief Rijksoverheid bevat grootste groep die zegt geen gebruik meer maken van sociale media

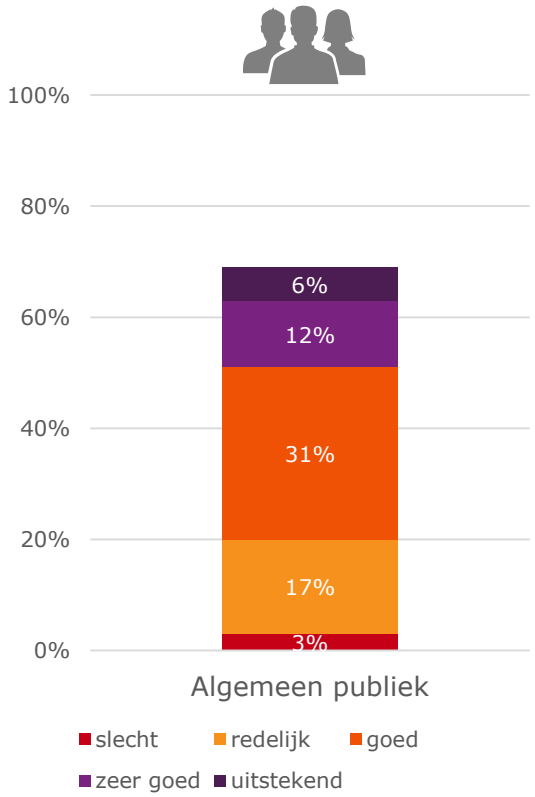
Eigen inschatting gebruik sociale media → Handelingsperspectieven → Verklaring voor gekozen handelingsperspectief

- In de gegeven inschattingen zitten geen opvallende verschillen tussen de doelgroepen.

- Onder de werkzame bevolking (11%) zitten meer mensen die zeggen geen gebruik meer te maken van sociale media dan onder het algemene publiek (6%). Dit percentage is hoogst onder ambtenaren exclusief Rijksoverheid (14%).

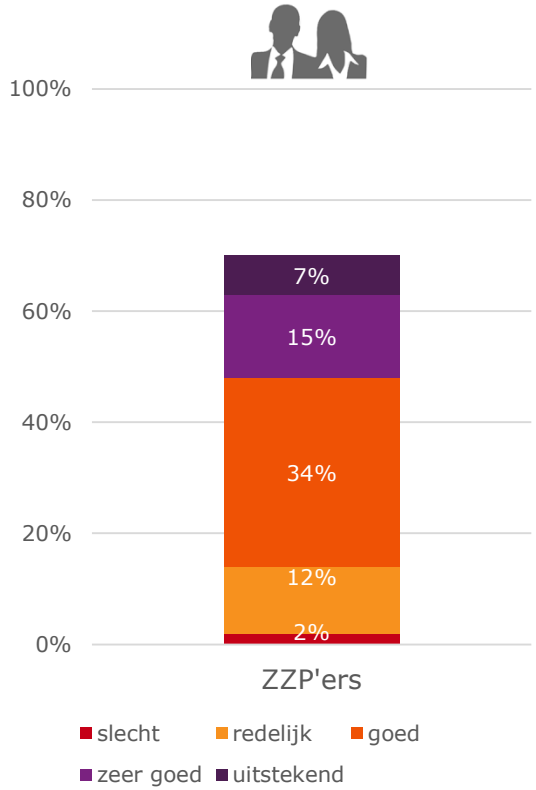
- In de gegeven verklaringen zitten geen opvallende verschillen tussen de doelgroepen.

Van het algemeen publiek gebruikt 1 op de 10 meestal een cloud zonder inloggegevens of wachtwoord

Eigen inschatting gebruik cloud	Top 3 gekozen handelingsperspectieven	Top 1 verklaring per handelingsperspectief
	**42%** ‘ik maak geen gebruik van een cloud’	**34%** hiervan zegt hier nooit eerder over nagedacht te hebben
	36% ‘ik maak meestal gebruik van een cloud met wachtwoord’	**49%** hiervan denkt dat deze optie voldoende veiligheid biedt
	12% ‘ik maak meestal gebruik van een cloud zonder dat ik inloggegevens en wachtwoord in moet voeren’	**30%** hiervan zegt hier nooit eerder over te hebben nagedacht

* Grafiek loopt niet tot 100%, overige percentage is ‘niet van toepassing’

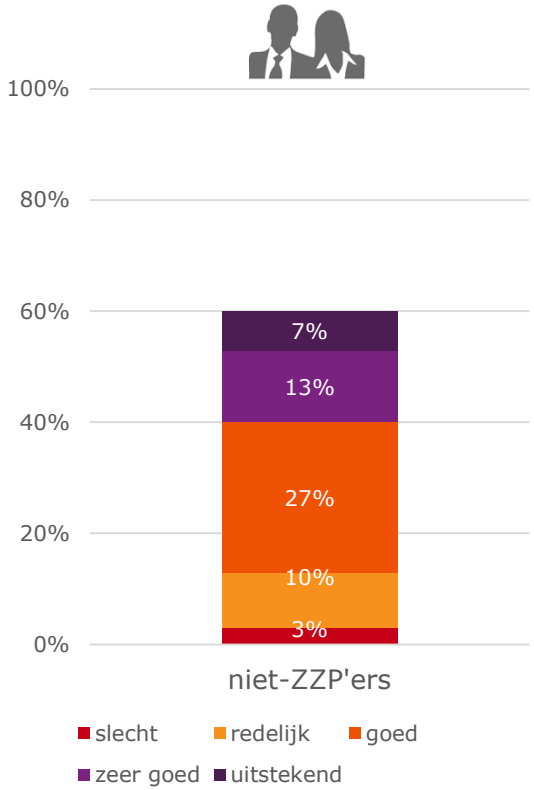
Bij ZZP'ers lijkt het niet gebruiken van een cloud een bewuste en volgens hen veilige keuze

Eigen inschatting gebruik cloud	Top 3 gekozen handelingsperspectieven	Top 1 verklaring per handelingsperspectief
	**42%** 'ik maak meestal gebruik van een cloud met wachtwoord'	**46%** hiervan denkt dat deze optie voldoende veiligheid biedt
	33% 'ik maak geen gebruik van een cloud'	**28%** hiervan zegt dit de meest veilige optie te vinden
	12% 'ik maak meestal gebruik van een cloud zonder dat ik inloggegevens en wachtwoord in moet voeren'	**20%** hiervan wist niet dat er andere opties dan deze waren

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Bij de niet-ZZP'ers maakt 2 op 10 alleen gebruik van een cloud aangeboden/aanbevolen door hun werkgever

Eigen inschatting gebruik cloud	Top 3 gekozen handelingsperspectieven	Top 1 verklaring per handelingsperspectief



49%
'ik maak geen gebruik van een cloud'

69%
hiervan zegt hier nooit over te hebben nagedacht

20%
'ik maak alleen gebruik van een cloud die wordt aangeboden/aanbevolen (zoals een gemeenschappelijke opslag op het intranet) door mijn werkgever/bedrijf'

32%
hiervan zegt dit de meest veilige optie te vinden

12%
'ik maak meestal gebruik van een cloud met wachtwoord'

23%
hiervan denkt dat deze optie voldoende veiligheid biedt

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Gebruik cloud: Meer dan de helft van de Rijksambtenaren en medewerkers grootbedrijf maken geen gebruik van een cloud tijdens het werk

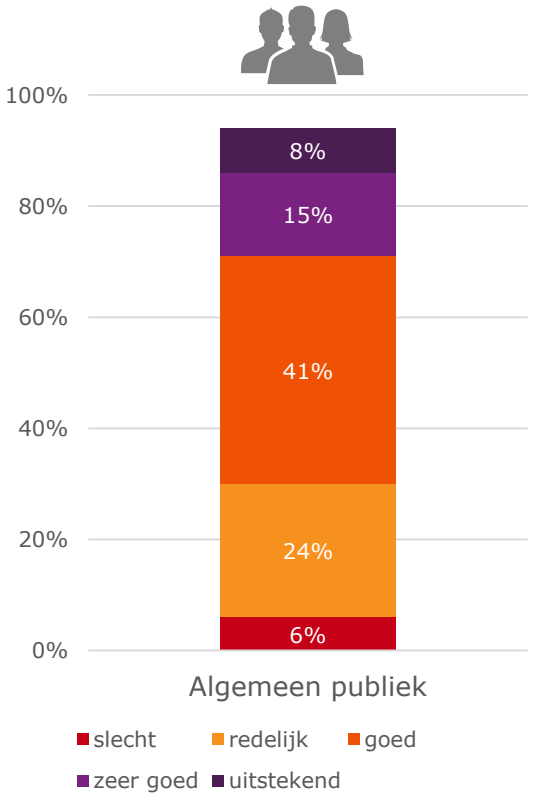
- In de gegeven inschattingen zitten geen opvallende verschillen tussen de doelgroepen.

- 55% van de Rijksambtenaren en medewerkers grootbedrijf maken geen gebruik van een cloud tijdens het werk. Bij de overige groepen werknemers ligt dit percentage rond de 45%

- In de gegeven verklaringen zitten geen opvallende verschillen tussen de doelgroepen.

Een kwart van het algemeen publiek maakt nooit een back-up omdat ze hier 'nooit over nagedacht hebben'

Eigen inschatting maken van back-ups



Top 3 gekozen handelingsperspectieven

29%
'ik maak eens in de 4 weken een back-up van mijn bestanden op een externe harde schijf/USB-stick'

28%
'ik maak eens per half jaar een back-up van mijn bestanden op een externe harde schijf/USB-stick'

24%
'ik maak nooit een back-up van mijn bestanden'

Top 1 verklaring per handelingsperspectief

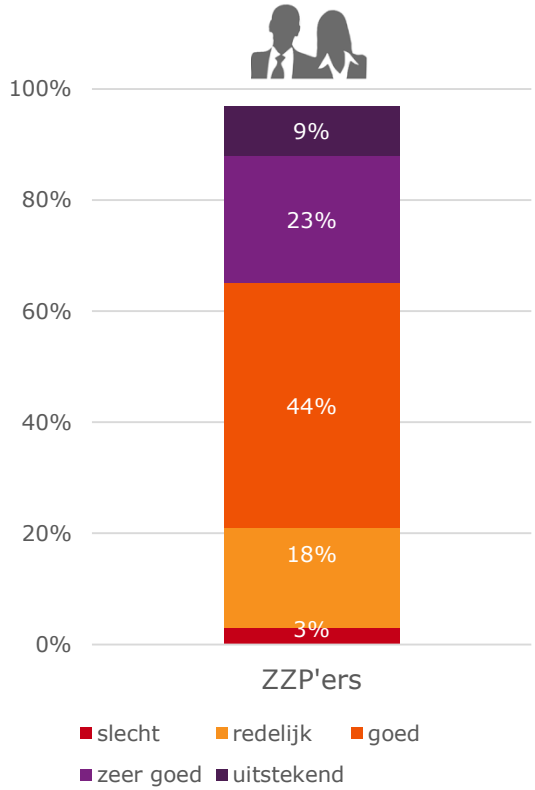
48%
hiervan zegt dit de meest veilige optie te vinden

42%
hiervan denkt dat deze optie voldoende veiligheid biedt

37%
hiervan zegt hier nooit eerder over te hebben nagedacht

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

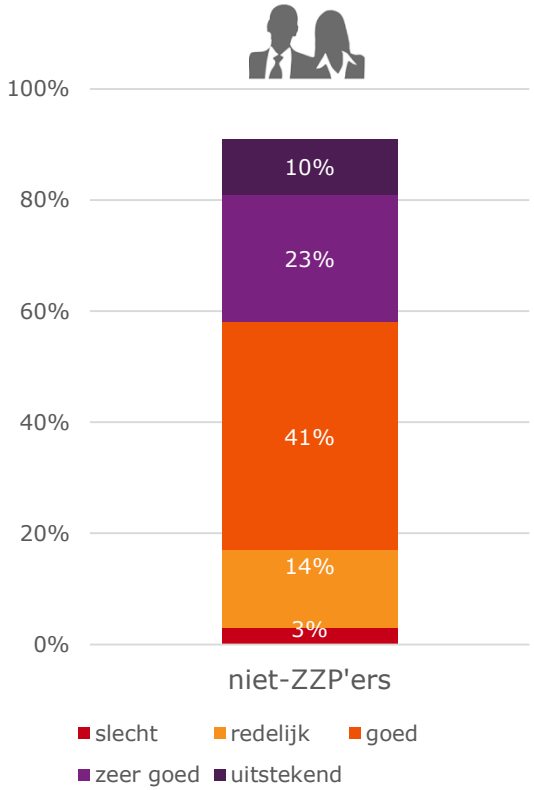
Bij ZZP'ers maakt ruim 1 op de 10 nooit een back-up omdat zij hier 'nooit eerder over nagedacht hebben'

Eigen inschatting maken van back-ups	Top 4 gekozen handelingsperspectieven	Top 1 verklaring per handelingsperspectief
	**35%** 'ik maak maandelijks een back-up van mijn werk gerelateerde bestanden op een externe harde schijf/USB-stick'	**39%** hiervan denkt dat deze optie voldoende veiligheid biedt
	30% 'ik maak dagelijks een back-up van mijn werk gerelateerde bestanden op een externe harde schijf/USB-stick'	**54%** Hiervan zegt dit de meest veilige optie te vinden
	24% 'ik maak wekelijks een back-up van mijn werk gerelateerde bestanden op een externe harde schijf/USB-stick'	**51%** hiervan zegt dit de meest veilige optie te vinden
	13% 'ik maak nooit een back-up van mijn werk gerelateerde bestanden'	**38%** hiervan zegt hier nooit eerder over nagedacht te hebben

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Bij 1 op de 10 niet-ZZP'ers worden er nooit back-ups gemaakt, ook (zover bekend) niet door de organisatie

Eigen inschatting maken van back-ups → Top 3 gekozen handelingsperspectieven → Top 1 verklaring per handelingsperspectief



67%
'back-ups van mijn werk gerelateerde bestanden worden automatisch opgeslagen door iemand anders binnen het bedrijf'

34%
hiervan zegt dit de meest veilige optie te vinden

16%
'ik maak zelf back-ups van mijn werkgerelateerde bestanden op een externe harde schijf of USB stick'

40%
hiervan zegt dit de meest veilige optie te vinden

9%
'ik maak zelf geen back-ups van mijn werkgerelateerde bestanden en (naar mijn weet) wordt dit ook niet door iemand anders in het bedrijf gedaan'

32%
hiervan zegt hier nooit eerder over nagedacht te hebben

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Back-ups: 1 op de 10 ZZP'ers en overige werknemers stelt dat er geen back-ups worden gemaakt

Eigen inschatting maken van back-ups → Handelingsperspectieven → Verklaring voor gekozen handelingsperspectief

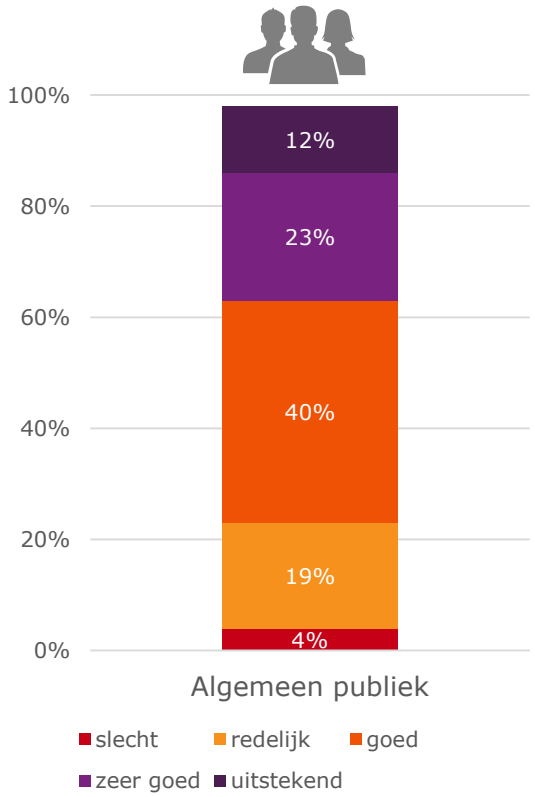
- Werknemers in het MKB (klein en groot) geven aan minder goed in staat te zijn om gegevens te beschermen tegen diefstal, verlies en schade doormiddel van back-ups dan de werknemers binnen het grootbedrijf en de overheid.

- Onder ZZP'ers maakt 13% nooit een back-up. Onder de overige werknemers (MKB, grootbedrijf en overheid) stelt 10% dat ook zij of hun organisatie (voor zover bekend) nooit back-ups maken.

- Een derde van de groep die nooit back-ups (laten) maken geeft aan dat ze hier nooit over nagedacht hebben.

Digitaal wachtwoordenkluisje wordt nauwelijks gebruikt (geen top 3) terwijl 41% aangeeft het wel te kennen

Eigen inschatting beheren wachtwoorden → Top 3 gekozen handelingsperspectieven → Top 1 verklaring per handelingsperspectief



46%
'ik onthoud mijn wachtwoorden'

62%
hiervan zegt dit de meest veilige optie te vinden

25%
'ik noteer ww op een briefje dat ik verstop'

49%
hiervan zegt de kennis niet te hebben dit anders te doen

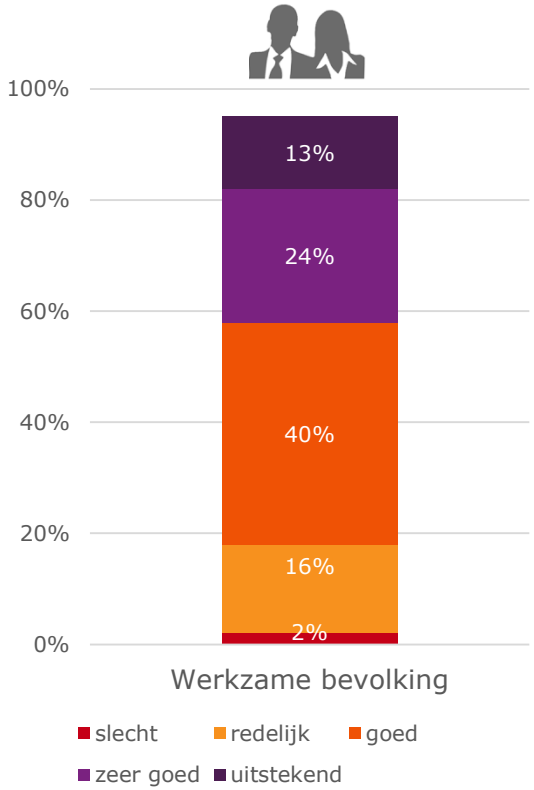
10%
'ik zet bij het inloggen een vinkje bij 'onthoud mijn wachtwoord''

28%
hiervan vindt een andere optie teveel tijd/moeite kosten

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Een derde van de werkzame bevolking schrijft wachtwoorden op een (digitaal) briefje

Eigen inschatting beheren wachtwoorden → Top 3 gekozen handelingsperspectieven → Top 1 verklaring per handelingsperspectief



50%
'ik onthoud mijn wachtwoorden'

→ **51%** hiervan zegt dit de meest veilige optie te vinden

17%
'ik noteer ww op een briefje dat ik verstop'

→ **36%** hiervan denkt dat deze optie voldoende veiligheid beidt

12%
'ik sla ww op in tablet/smartphone/etc'

→ **32%** hiervan denkt dat deze optie voldoende veiligheid biedt

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Beheren wachtwoorden: zowel onder algemeen publiek als werkzame bevolking schrijven veel mensen hun wachtwoorden op een briefje

Eigen inschatting beheren wachtwoorden → Handelingsperspectieven → Verklaring voor gekozen handelingsperspectief

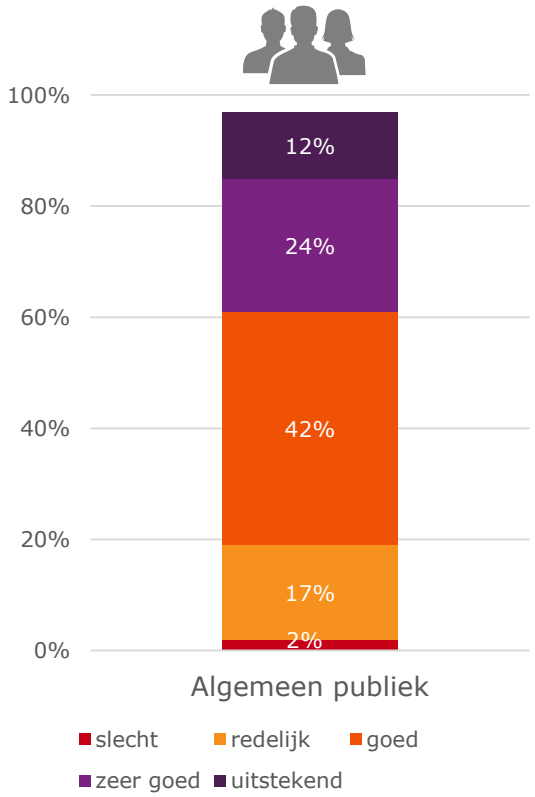
- Bijna de helft van de Rijksambtenaren stelt uitstekend of zeer groep in staat te zijn om hun wachtwoorden te beheren. Bij de overige werknemers en de algemene bevolking is dit percentage 35%.

- Onder algemeen publiek (25%) en werkzame bevolking (17%) zit nog een relatief grote groep die de wachtwoorden op verstopt briefje bewaren. Onder de werkenden zitten deze over de hele linie van organisaties.

- In de gegeven verklaringen zitten geen opvallende verschillen tussen de doelgroepen.

Twee derde van het algemeen publiek gebruikt wachtwoorden inclusief hoofdletter en speciaal teken

Eigen inschatting inhoud wachtwoorden



Top 3 gekozen handelingsperspectieven

67%
'mijn wachtwoorden bestaan doorgaans uit meer dan 8 karakters met minimaal 1 hoofdletter, 1 kleine letter en 1 speciaal teken (@, &, %, =)'

25%
'mijn wachtwoorden bestaan doorgaans uit meer dan 8 karakters'

8%
'mijn wachtwoorden bestaan doorgaans uit minder dan 8 karakters'

Top 1 verklaring per handelingsperspectief

53%
hiervan zegt dit de meest veilige optie te vinden

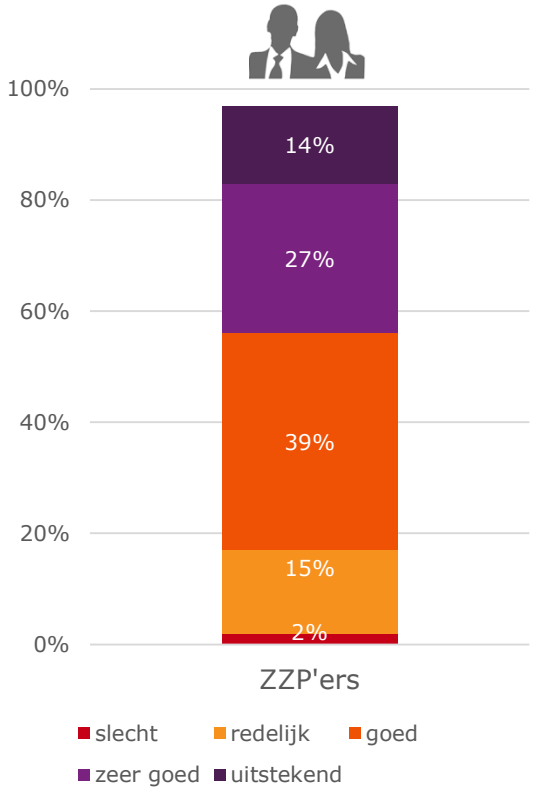
40%
hiervan denkt dat deze optie voldoende veiligheid biedt

38%
hiervan denkt dat deze optie voldoende veiligheid biedt

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Bij ZZP'ers gebruikt bijna driekwart wachtwoorden inclusief hoofdletter en speciaal teken

Eigen inschatting inhoud wachtwoorden	Top 3 gekozen handelingsperspectieven	Top 1 verklaring per handelingsperspectief



74%
'mijn wachtwoorden bestaan doorgaans uit meer dan 8 karakters met minimaal 1 hoofdletter, 1 kleine letter en 1 speciaal teken (bv. @, &, %, =)'

57%
hiervan zegt dit de meest veilige optie te vinden

21%
'mijn wachtwoorden bestaan doorgaans uit meer dan 8 karakters'

41%
hiervan denkt dat deze optie voldoende veiligheid biedt

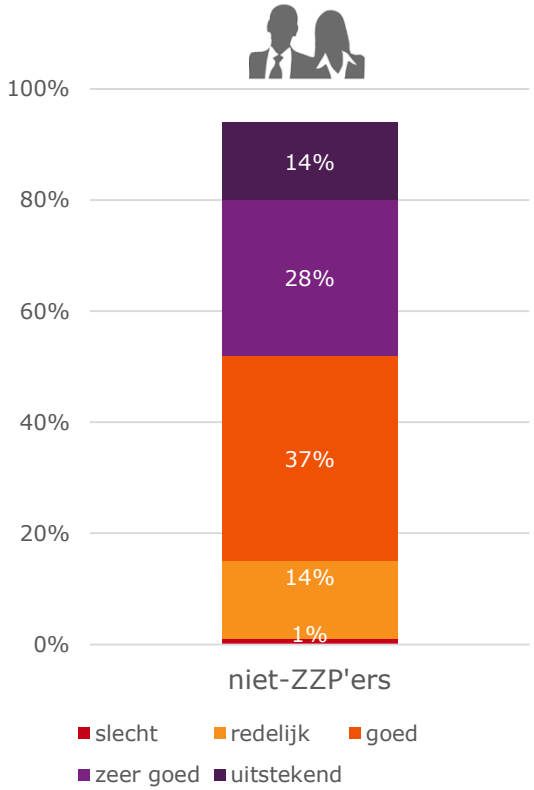
6%
'mijn wachtwoorden bestaan doorgaans uit minder dan 8 karakters'

43%
hiervan denkt dat deze optie voldoende veiligheid biedt

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Bij niet-ZZP'ers is aantal dat veilig wachtwoord gebruikt lager dan bij ZZP'ers

Eigen inschatting inhoud wachtwoorden	Top 3 gekozen handelingsperspectieven	Top 1 verklaring per handelingsperspectief



65%
'mijn wachtwoorden bestaan doorgaans uit meer dan 8 karakters met minimaal 1 hoofdletter, 1 kleine letter en 1 speciaal teken (bv. @, &, %, =)'

54%
hiervan zegt dit de meest veilige optie te vinden

21%
'mijn wachtwoorden bestaan doorgaans uit meer dan 8 karakters'

43%
hiervan denkt dat deze optie voldoende veiligheid biedt

8%
'mijn wachtwoorden bestaan doorgaans uit minder dan 8 karakters'

27%
hiervan denkt dat deze optie voldoende veiligheid biedt

* Grafiek loopt niet tot 100%, overige percentage is 'niet van toepassing'

Inhoud wachtwoorden: zowel onder algemeen publiek als werkzame bevolking schrijven veel mensen hun wachtwoorden op een briefje

Eigen inschatting Inhoud wachtwoorden → Handelingsperspectieven → Verklaring voor gekozen handelingsperspectief

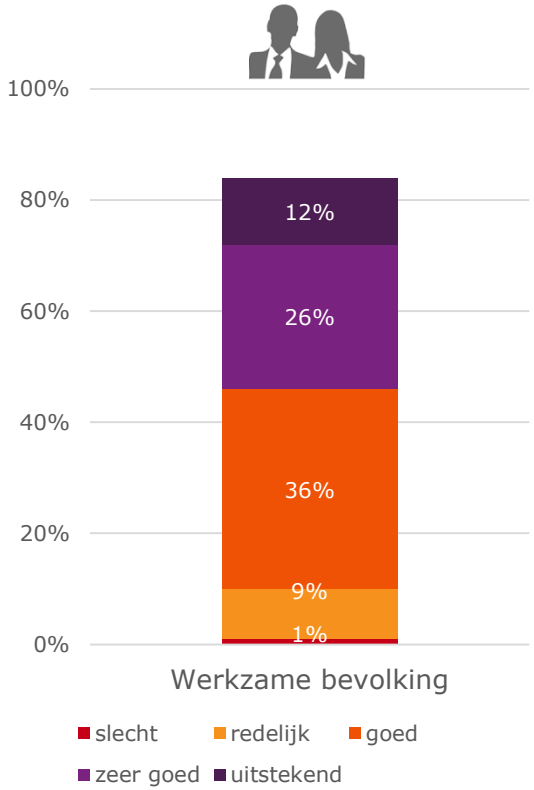
- MKB'ers blijken minder vertrouwen te hebben in deze skill. Onder MKB medewerkers schatten 3 op de 10 hun eigen skills om veilige wachtwoorden te kiezen in als uitstekend tot zeer goed. Onder de overige groepen medewerkers is dit ruim 4 op de 10. Algemeen publiek zit hier tussenin met 36%.

- Bij alle groepen werknemers is aantal dat hoofdletter en speciaal teken in wachtwoorden gebruikt (rond 65%) lager dan bij ZZP'ers (74%).

- In de gegeven verklaringen zitten geen opvallende verschillen tussen de doelgroepen.

Bijna 1 op de 10 geeft aan dat persoons- en/of klantgegevens niet extra beschermd zijn

Eigen inschatting omgaan met persoons- en klantgegevens



Top 3 gekozen handelingsperspectieven

34%
‘mijn organisatie maakt gebruik van een beveiligde opslag van persoons- en klantgegevens en er is beleid over op welke manier deze gebruikt mogen worden’

19%
‘mijn organisatie maakt gebruik van een beveiligde opslag en van een beveiligde verbinding waar persoonsgegevens worden verwerkt’

8%
‘de persoons- en / of klantgegevens binnen mijn organisatie zijn (naast de standaardbeveiliging van host/netwerk) niet extra beschermd’

Top 1 verklaring per handelingsperspectief

49%
hiervan zegt dit de meest veilige optie te vinden

44%
hiervan zegt dit de meest veilige optie te vinden

34%
hiervan denkt dat deze optie voldoende veiligheid biedt

* Grafiek loopt niet tot 100%, overige percentage is ‘niet van toepassing’

Omgaan met persoons- en klantgegevens: in de organisatie van ambtenaren is hiervoor vaker beleid en middelen

Eigen inschatting omgaan met persoons- en klantgegevens → Handelingsperspectieven → Verklaring voor gekozen handelingsperspectief

- 4 op de 10 ambtenaren zeggen uitstekend tot zeer goed om te kunnen gaan met persoons- en klantgegevens. Onder MKB'ers is dit 3 op de 10. ZZP'ers zitten hier tussenin met 35%.

- Onder ambtenaren geeft een fors hoger percentage (45%) aan dat de organisatie maakt gebruik van een beveiligde opslag van persoons- en klantgegevens en dat er beleid over de wijze waarop persoons- en klantgegevens verstuurd en gebruikt mogen worden. Bij de overige groepen werkenden ligt dit percentage rond de 30%.

- In de gegeven verklaringen zitten geen opvallende verschillen tussen de doelgroepen.

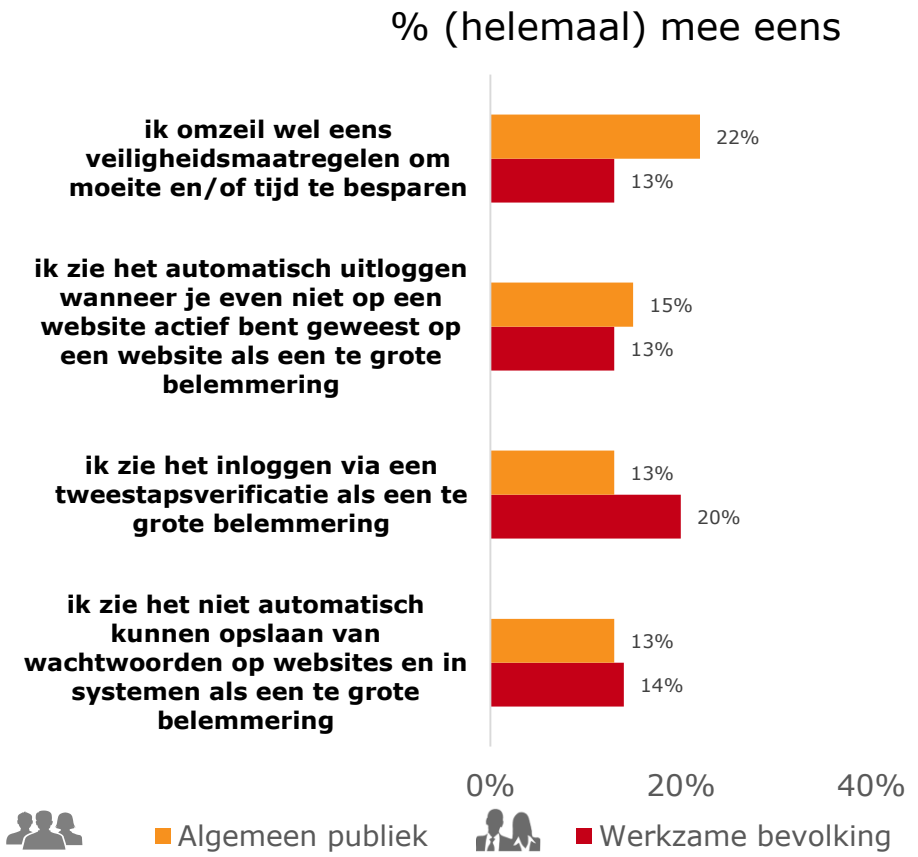
4

Waar liggen de kansen en bedreigingen voor de ontwikkeling van cybersecurity skills

Algemeen publiek omzeilt vaker veiligheidsmaatregelen dan werkzame bevolking om moeite/tijd te besparen

Verschillen op sociaal-demografische kenmerken:

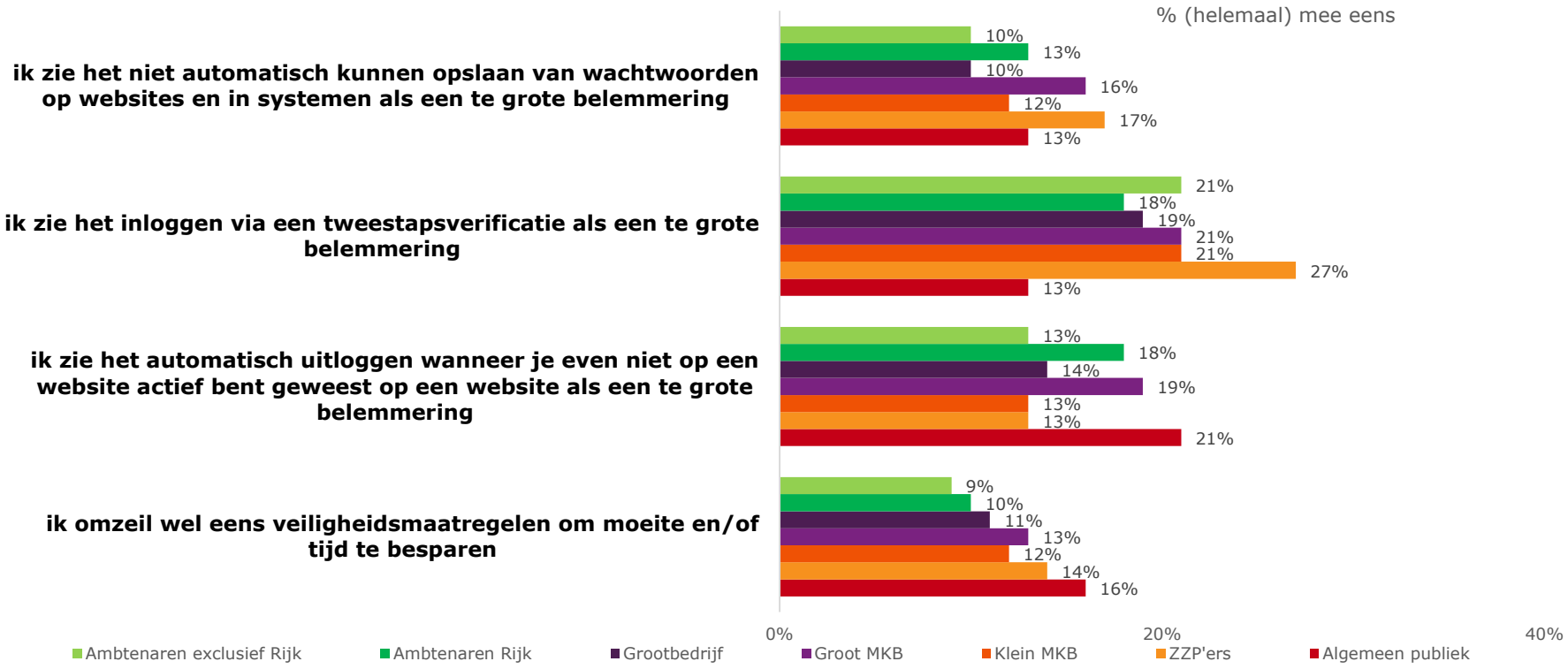
- Mannen zien het inloggen via een tweestapsverificatie en het automatisch uitloggen wanneer je even niet actief bent geweest op een website minder snel als een te grote belemmering dan vrouwen. Dit geldt voor zowel algemeen publiek als voor werkzame bevolking.
- 30-50jarigen binnen algemeen publiek omzeilen vaker veiligheidsmaatregelen om moeite en/of tijd te besparen dan 20-30jarigen en 50+ers. De oudere werkzame bevolking (30+) zijn minder geneigd veiligheidsmaatregelen te omzeilen dan de jongere (20-30jarigen).
- Hoogopgeleiden binnen algemeen publiek zien automatisch uitloggen en het niet automatisch kunnen opslaan van wachtwoorden minder vaak als een te grote belemmering in vergelijking met laagopgeleiden. Voor zowel algemeen publiek en werkzame bevolking geldt dat hoogopgeleiden minder snel veiligheidsmaatregelen omzeilen dan laagopgeleiden.



Algemeen publiek (n=963), Werkzame bevolking (n=1711): Hieronder staan een aantal mogelijke belemmeringen als gevolg van beleid en/of maatregelen die u moeten beschermen tegen digitale / online gevaren. Kunt u aangeven in hoeverre u het eens bent met de volgende stellingen.

ZZP’ers zien meeste belemmeringen bij ‘niet automatisch opslaan wachtwoorden’ en ‘inloggen via tweestapsverificatie’

Algemeen publiek ziet meeste belemmeringen als gevolg van ‘automatisch uitloggen bij inactiviteit’. Algemeen publiek omzeilt ook het vaakst veiligheidsmaatregelen om tijd te besparen. Ambtenaren exclusief Rijks ervaren over het algemeen de minste belemmeringen.



Algemeen publiek (n=963), Werkzame bevolking (n=1711): Hieronder staan een aantal mogelijke belemmeringen als gevolg van beleid en/of maatregelen die u moeten beschermen tegen digitale / online gevaren. Kunt u aangeven in hoeverre u het eens bent met de volgende stellingen.

Internet service providers volgens algemeen publiek en ZZP'ers belangrijke verantwoordelijke voor digitale veiligheid

Niet-zzp'ers geven aan dat deze verantwoordelijkheid in eerste instantie bij de ICT'er/ICT afdeling van de organisatie ligt en pas in tweede instantie bij de werknemers.

Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid in de digitale / online omgeving in uw thuissituatie voornamelijk moet liggen?

Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid in de digitale / online omgeving in uw werksituatie voornamelijk moet liggen?

Algemeen publiek	ZZP'ers	Niet-ZZP'ers
1 De gebruiker	1 De gebruiker	1 De ICT-afdeling van mijn organisatie
2 Internet service providers	2 Internet service providers	2 Werknemers
3 Website eigenaren	3 Leverancier hard- en software	3 Management van mijn organisatie

Algemeen publiek (n=963): Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid in de digitale / online omgeving in uw thuissituatie voornamelijk moet liggen?
ZZP (n=393), niet-ZZP (n=1318): Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid in de digitale / online omgeving in uw werksituatie voornamelijk moet liggen?

Werkzame bevolking (niet-ZZP) stelt de ICT-afdeling verantwoordelijk voor het ontwikkelen van cyberskills

Algemeen publiek en ZZP'ers vinden dat de gebruiker zelf verantwoordelijk is voor de ontwikkeling van cyberskills (net als bij de digitale veiligheid).

Wie zijn volgens u verantwoordelijk voor de ontwikkeling van uw kennis en vaardigheden ter bescherming van gevaren in de digitale / online omgeving in de thuissituatie?

Wie zijn volgens u verantwoordelijk voor de ontwikkeling van uw kennis en vaardigheden ter bescherming van gevaren in de digitale / online omgeving in de werksituatie?

Algemeen publiek	ZZP'ers	Niet-ZZP'ers
1 De gebruiker	1 De gebruiker	1 De ICT-afdeling van mijn organisatie
2 Internet service providers	2 Internet service providers	2 Management van mijn organisatie
3 Leverancier hard- en software	3 Leverancier hard- en software	3 De gebruiker

Algemeen publiek (n=963): Wie zijn volgens u verantwoordelijk voor de ontwikkeling van uw kennis en vaardigheden ter bescherming van gevaren in de digitale / online omgeving in de thuissituatie?
ZZP (n=393), niet-ZZP (n=1318): Wie zijn volgens u verantwoordelijk voor de ontwikkeling van uw kennis en vaardigheden ter bescherming van gevaren in de digitale / online omgeving in de werksituatie?

Volgens de werkzame bevolking is de ICT-afdeling de voornaamste verantwoordelijke voor digitale veiligheid

Algemeen publiek en ZZP'ers stellen dat de gebruiker zelf verantwoordelijk is voor zijn/haar digitale veiligheid. De gebruiker zelf en het management van de organisatie zijn de andere partijen waar ook verantwoordelijkheid zou moeten liggen.

	Algemeen publiek	ZZP'ers	Klein MKB	Groot MKB	Grootbedrijf	Ambtenaren Rijk	Ambtenaren exclusief Rijk
1	De gebruiker	De gebruiker	het management van mijn organisatie	De ICT-afdeling van mijn organisatie	De ICT-afdeling van mijn organisatie	De ICT-afdeling van mijn organisatie	De ICT-afdeling van mijn organisatie
2	Internet service providers	Internet service providers	De gebruiker	het management van mijn organisatie	De gebruiker	De gebruiker	De gebruiker
3	Website eigenaren	Leverancier hard- en software	Internet service providers	De gebruiker	het management van mijn organisatie	het management van mijn organisatie	het management van mijn organisatie

Algemeen publiek (n=963): Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid in de digitale / online omgeving in uw thuissituatie voornamelijk moet liggen?
ZZP (n=393), niet-ZZP (n=1318): Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid in de digitale / online omgeving in uw werksituatie voornamelijk moet liggen?

Werkzame bevolking van mening dat de ICT-afdeling verantwoordelijk is voor het ontwikkelen van cyberskills

Werkzame bevolking en ZZP'ers vinden dat de gebruiker zelf verantwoordelijk is voor de ontwikkeling van cyberskills (net als bij de digitale veiligheid). Volgens medewerkers uit het klein MKB heeft het management de voornaamste verantwoordelijkheid, ook de overige groepen werknemers meent dat het management verantwoordelijkheid draagt.

	Algemeen publiek	ZZP'ers	Klein MKB	Groot MKB	Grootbedrijf	Ambtenaren Rijk	Ambtenaren exclusief Rijk
1	De gebruiker	De gebruiker	het management van mijn organisatie	De ICT-afdeling van mijn organisatie	De ICT-afdeling van mijn organisatie	De ICT-afdeling van mijn organisatie	De ICT-afdeling van mijn organisatie
2	Internet service providers	Internet service providers	De gebruiker	het management van mijn organisatie	het management van mijn organisatie	De gebruiker	het management van mijn organisatie
3	Leverancier hard- en software	Leverancier hard- en software	De ICT-afdeling van mijn organisatie	De gebruiker	De gebruiker	het management van mijn organisatie	De gebruiker

Algemeen publiek (n=963): Wie zijn volgens u verantwoordelijk voor de ontwikkeling van uw kennis en vaardigheden ter bescherming van gevaren in de digitale / online omgeving in de thuissituatie?
ZZP (n=393), niet-ZZP (n=1318): Wie zijn volgens u verantwoordelijk voor de ontwikkeling van uw kennis en vaardigheden ter bescherming van gevaren in de digitale / online omgeving in de werksituatie?

Wat men nodig zou hebben om kennis tegen cybergevaren toepasbaar te maken is: meer ‘kennis’

Ook hulp, voorlichting en cursus zijn veelgenoemde punten om kennis tegen cybergevaren meer toepasbaar te maken. Bij werkzame bevolking komt hier ICT (afdeling) nog bij.

Algemeen publiek

Werkzame bevolking

Quotes

*“Betere **voorlichting**. Een Teleac **cursus** ofzo... Het verandert allemaal zo belachelijk snel dat ik het gevoel heb altijd achter de feiten aan te lopen.”*

*“Een dummy handleiding die overzicht geeft over alle opties en **gevaren**.”*

*“Meer **informatie** hierover verzamelen en me laten bijstaan door vertrouwd persoon die hier meer **kennis** van heeft.”*

*“**Voorlichting** via internet en/of senior web enz.”*

*“Te weinig **kennis** van de **gevaren** en hoe mee om te gaan.”*

*“Een computer **cursus** met de nadruk op veilig online zijn.”*

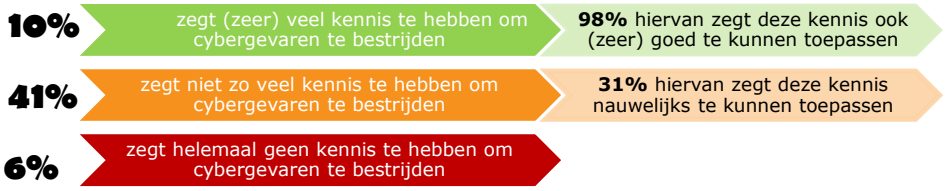
*“Vraag meestal **hulp** aan mijn zoon.”*

*“Werk bij een grote organisatie, waar alles door **ICT** geregeld wordt. Denk er zelf niet zo bij na.”*

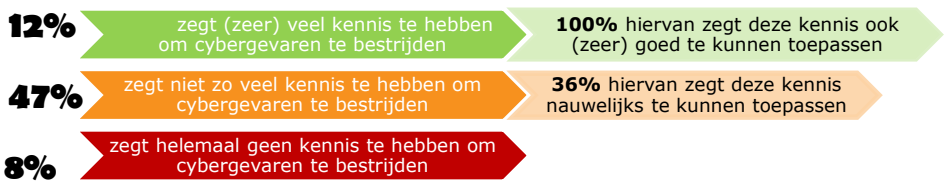
Algemeen publiek (692 open antwoorden), Werkzame bevolking (1166 open antwoorden): U heeft aangegeven dat u de kennis over bestrijding van gevaren in de digitale / online omgeving niet altijd goed toe te kunnen passen. Kunt u hieronder in het kort aangeven wat u nodig zou hebben om deze kennis beter toepasbaar te maken?

Groot MKB en grootbedrijf bevat de grootste groep die zeggen (zeer) veel kennis te hebben maar niet toe te kunnen passen

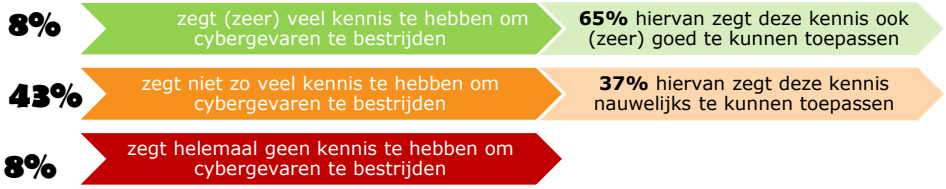
ZZP



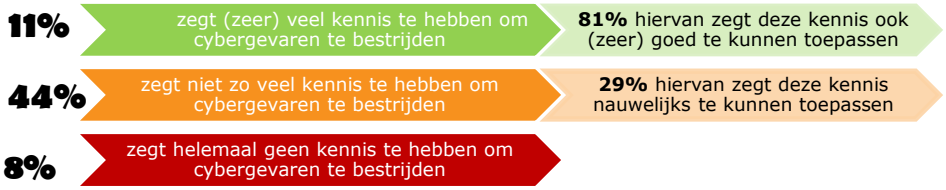
Klein MKB



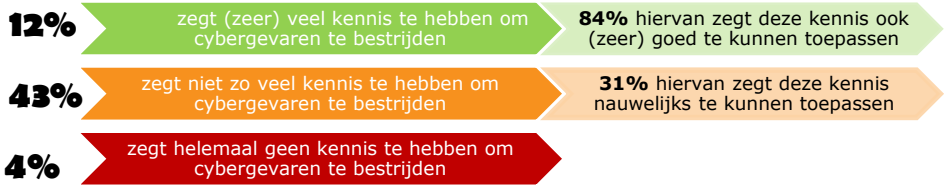
Groot MKB



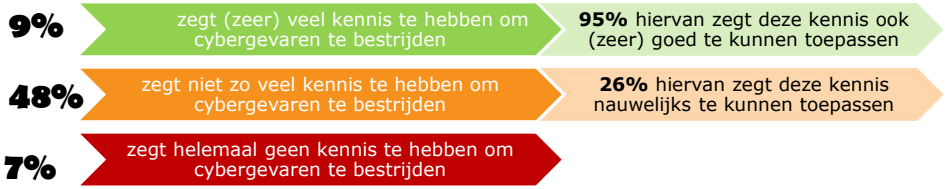
Grootbedrijf



Ambtenaren Rijk



Ambtenaren exclusief Rijk



Algemeen publiek (n=963): In welke mate denkt u over de kennis te beschikken om gevaren in de digitale / online omgeving te kunnen bestrijden? In hoeverre denkt u de kennis die u hebt over de bestrijding van gevaren in de digitale / online omgeving ook op een goede manier toe te kunnen passen?
Werkzame bevolking (n=1711): In welke mate denkt u over de kennis te beschikken om gevaren in de digitale / online omgeving op en tijdens uw werk te kunnen bestrijden? In hoeverre denkt u de kennis die u hebt over de bestrijding van gevaren in de digitale / online omgeving op en tijdens uw werk ook op een goede manier toe te kunnen passen?

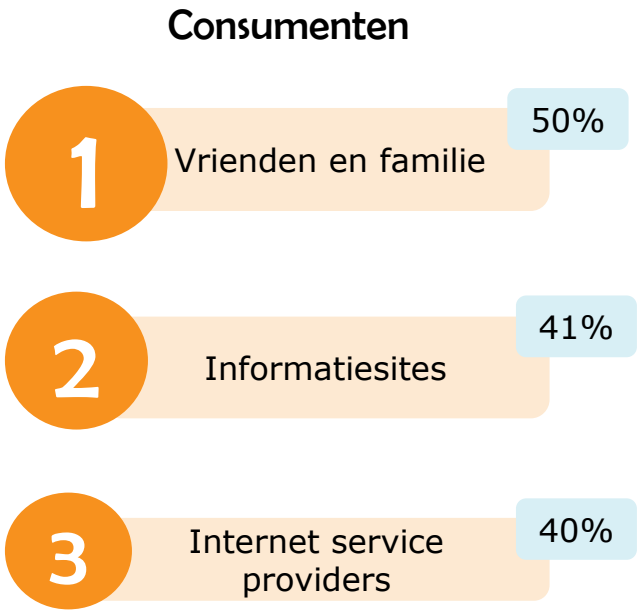
Algemeen publiek zou het liefst via vrienden en familie hun kennis en vaardigheden (verder) willen ontwikkelen

Gevolgd door internet service providers (incl. webhosting partijen) en informatiesites.

*Via welke kanalen en partijen zou u de kennis en vaardigheden ter bescherming van digitale / online omgeving willen ontwikkelen?**

Verschillen op sociaal-demografische kenmerken:

- Vrouwen zouden hun kennis en vaardigheden liever via vrienden en familie willen ontwikkelen in vergelijking met mannen. Mannen kiezen eerder voor internetserviceproviders, online fora en leverancier hard- en software.
- De optie informatiesites wordt meer gekozen door 30-50jarigen dan door jongeren (13-18jarigen) en ouderen (50+).
- Tussen opleidingsniveaus is ook een duidelijke scheiding te zien. Laagopgeleiden kiezen eerder voor vrienden en familie in vergelijking met hoogopgeleiden. Hoogopgeleiden zouden hun kennis en vaardigheden willen ontwikkelen via informatiesites, internetservice providers, online fora, belangenorganisaties, leverancier hard- en software en de bibliotheek.



* Meerdere antwoorden aanvinken mogelijk, daarom komt cumulatief percentage boven 100% uit

Algemeen publiek (n=963): Via welke kanalen en partijen zou u de kennis en vaardigheden ter bescherming van digitale / online omgeving willen ontwikkelen?

5

Onderzoeksverantwoording

Onderzoeksverantwoording

Methode	Online
Doelgroep(en)	Algemeen publiek en werkzame bevolking (onder wie ZZP, beleidmakers, werknemers)
Steekproefgrootte	Totale n = 2674 (963 Algemeen publiek , 1711 werkzame bevolking)
Respons	Algemeen publiek: 60% en werkzame bevolking: 51%
Steekproef(bron)	Voor dit onderzoek zijn er TNS NIPOBASE in totaal 7 steekproeven getrokken, voor elke doelgroep één.
Stratificatie	Werkzame bevolking getrokken op verdeling binnen sector, aantal werknemers, bedrijfsgrootte. Consumenten op representatieve verdeling voor geslacht, leeftijd, opleiding, gezinsgrootte, sociaal- economische status, provincie en regio.
Veldwerkperiode	12 t/m 28 juli 2016
Vragenlijstlengte	Gemiddeld 13 minuten
Open vragen	Gerapporteerd door middel van wordclouds en quotes
Vragenlijst	Twee (één voor algemeen publiek en één voor werkzame bevolking)
Toonmateriaal	Nee
Weging	Nee
Rapportage	Percentages zijn in de tabellen aan gegeven

*Meer gedetailleerde informatie over dit onderzoek is beschikbaar via uw contactpersoon bij TNS NIPO