# Cybersecurity awareness en skills in Nederland

# 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.

# 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.

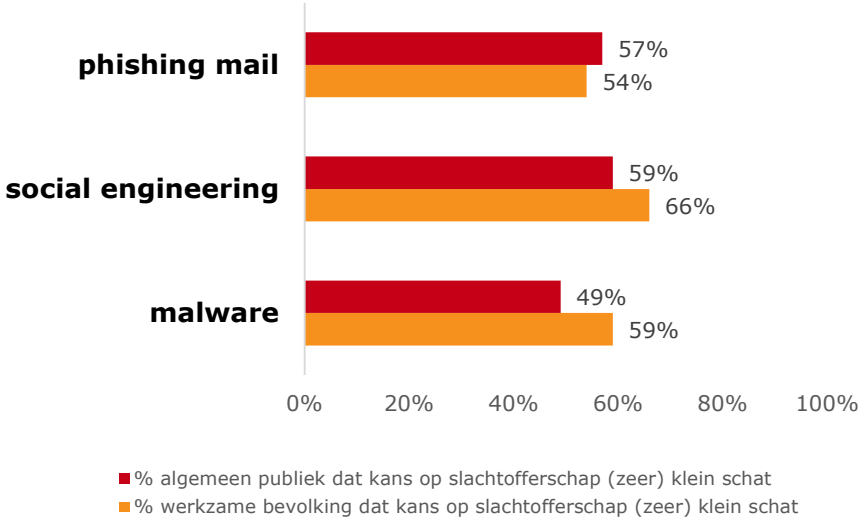
# Management summary in woord en beeld

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.

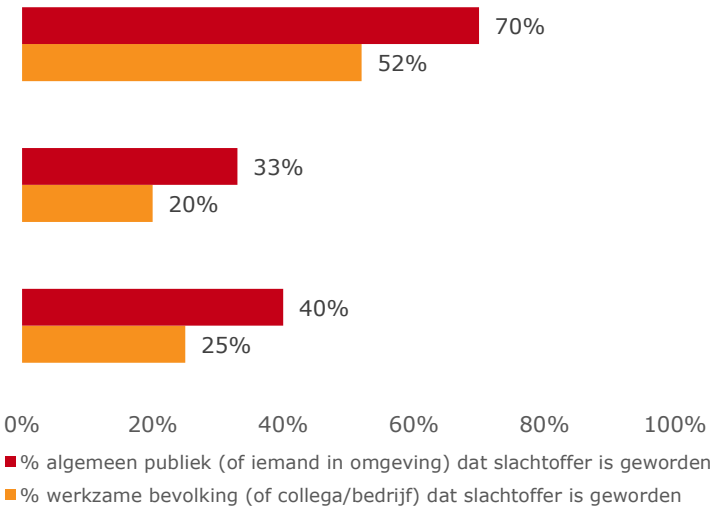
# Nederlanders maken zich (deels onterecht) weinig zorgen over hun digitale veiligheid

- 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.

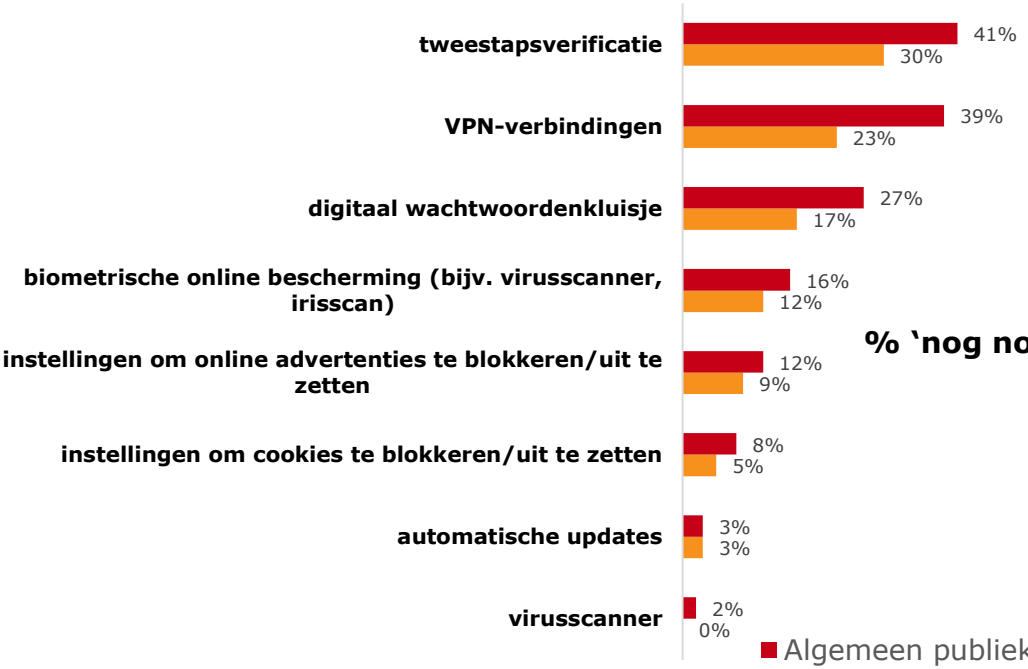
2. Onder ZZP'ers maakt ruim 1 op de 10 nooit een back-up omdat zij hier 'nooit eerder over nagedacht hebben'

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

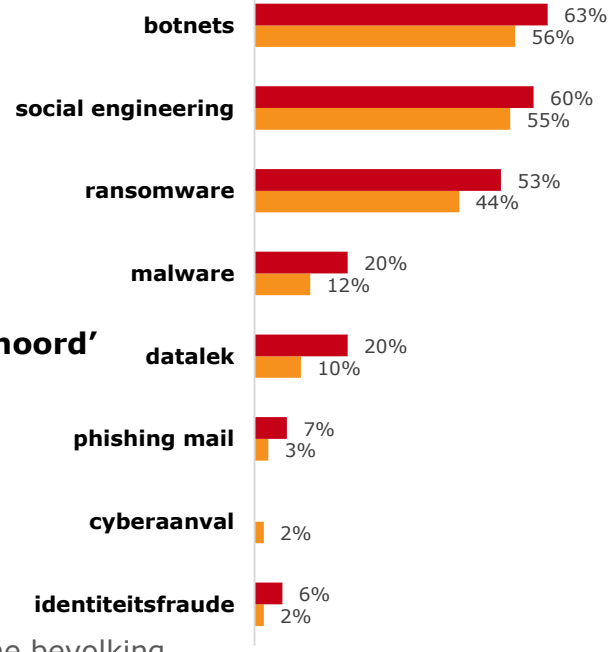
# Maatregelen ter preventie van cyber gevaren zijn bekender dan de gevaren zelf, dit is een mogelijke verklaring voor het omzeilen van veiligheidsmaatrelen

- 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**

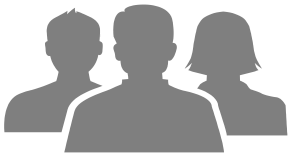



**Bekendheid cyber gevaren**



# 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%**

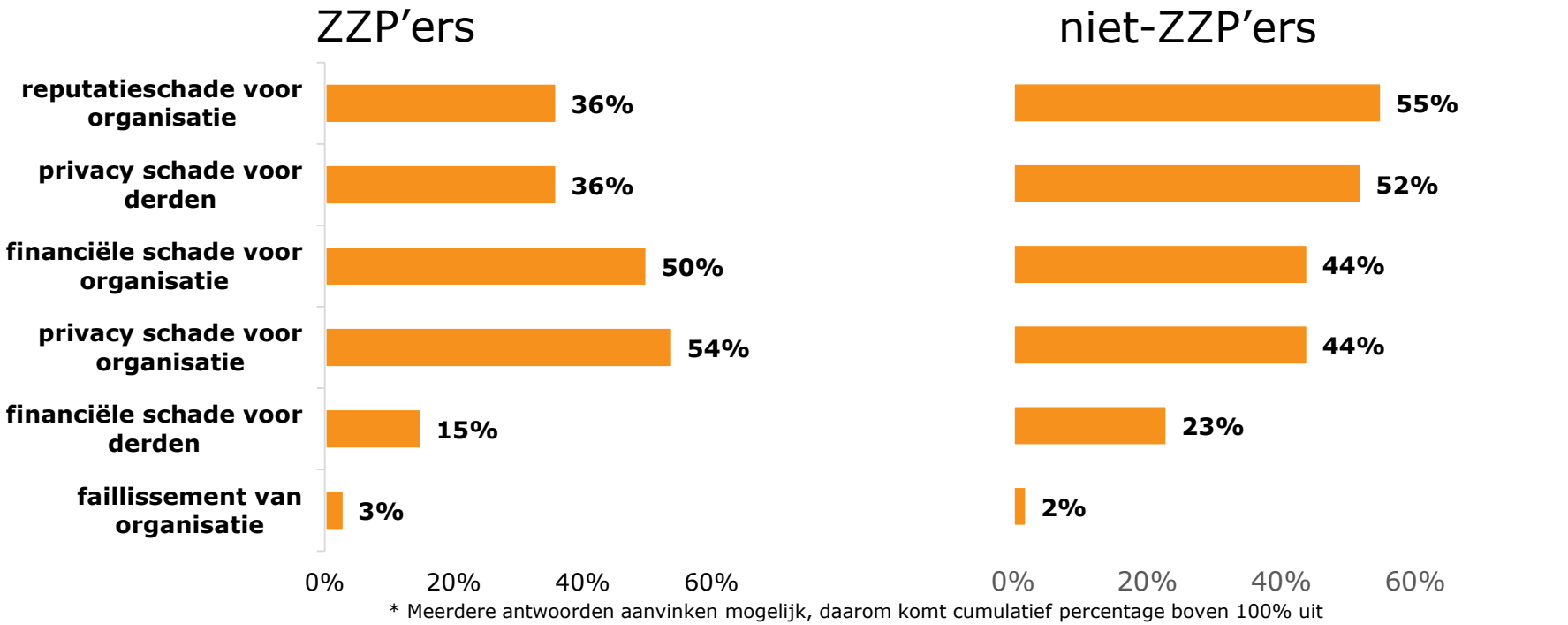
'wanneer ik actief ben op sociale media denk ik meestal **niet bewust** na over de eventuele gevolgen hiervan voor mijzelf en/of mijn vrienden en bekenden'

**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'