Cybersecurity 2015
Awareness, gedrag & digitaal verantwoord ondernemen

Tweede conceptrapportage van een kwantitatief onderzoek
in opdracht van de NCTV
- Resultaten van de 2015-meting

Uitgevoerd door: GfK bv
Uw contact: Peter van de Vijver
Tel.: +31 (0) 35-6258411 / Fax: +31 (0) 35-6248532
E-mail: peter.van.de.vijver@gfk.com
Projectnummer: 38282
Datum: 25-9-2015

INHOUD

1. Inleiding

1.1 Achtergrond en doel van het onderzoek

Achtergrond

Cybersecurity is van groot belang voor het goed functioneren van economie en maatschappij, want, zoals minister Van der Steur het verwoordde tijdens de Global Conference on CyberSpace 2015: 'It is important for us all to realize the full potential of cyberspace while at the same time reducing the risks involved. By working together, we can truly start working on creating a free, open and secure cyberspace'.

Daarvoor is niet alleen van belang hoe internet door experts zo veilig mogelijk wordt gemaakt en gehouden. Ook gebruikers zelf kunnen daar door besef (awareness) en gedrag een fundamentele bijdrage aan leveren. Dat laatste, het gebruikersperspectief (van consumenten en professionals), staat in dit onderzoek centraal.

De uitkomsten van het onderzoek zullen worden gebruikt als input voor de campagne Alert Online, die elk najaar wordt gevoerd. Doel van deze campagne is om de kennis van professionals en consumenten over digitale veiligheid te vergroten en zo een gedragsverandering te realiseren. Om de campagne optimaal aan te laten sluiten bij de doelgroepen, is kennis van die doelgroepen natuurlijk van essentieel belang. De - zo belangrijke - juiste accenten in de communicatie kunnen zo worden aangebracht.

In 2012, 2013 en 2014 zijn metingen van het Cybersecurity onderzoek uitgevoerd, waarvan de 2013- en 2014-metingen ook door GfK zijn uitgevoerd. Uit de voorgaande metingen blijkt dat er zeker nog winst valt te behalen als het gaat om de digitale veiligheid van verschillende doelgroepen.

In 2015 staat digitaal verantwoord ondernemen centraal. Hierin sluit de campagne aan bij een belangrijke hoofdconclusie van het onderzoek in 2014: de werkomgeving is een belangrijke stimulator voor cyber awareness en bijbehorend gedrag, ook in de privésituatie. Het onderzoek van afgelopen jaar heeft ons ook laten zien dat de risico's nog altijd worden onderschat, zowel in de werk- als in de privésituatie, en dat er behoefte is aan duidelijke, heldere informatie met een concreet handelingsperspectief.

Doel

Het hoofddoel van het onderzoek is in 2015: het verkrijgen van inzicht in hoe veilig of onveilig men zich online gedraagt (op basis van zelfgerapporteerd gedrag). In voorgaande jaren lag de nadruk in het onderzoek meer op cyber awareness (kennis en houding).

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) gebruikt de inzichten van dit onderzoek op de langere termijn voor het nog beter toespitsen van haar beleid en communicatie.

1.2 Opzet van het onderzoek

Doelgroepen

Een belangrijke verandering in het onderzoek ten opzichte van vorige metingen is dat in overleg met de opdrachtgevers minder differentiatie is aangebracht in de doelgroep publieke sector en meer differentiatie is aangebracht in de doelgroep bedrijfsleven. Dit mede op basis van een verschuiving van de beleidsmatige focus richting digitaal verantwoord ondernemen.
Een belangrijke verandering is verder een *inhoudelijke* verschuiving van de focus, van bewustzijn van cybersecurity (awareness) naar cybersecure gedrag. Dit heeft ook geleid tot een vernieuwde vragenlijst, waardoor vergelijkingen met voorgaande metingen slechts op hoofdlijnen kunnen worden getrokken.

Het onderzoek is in 2015 uitgevoerd onder de volgende zes doelgroepen:

Overheid

- Ambtenaren Rijksoverheid:
  Ambtenaren, werkzaam bij één van de Rijksoverheden (hieronder vallen ook inspecties, uitvoeringsorganisaties, agentschappen, ZBO's en diensten zoals de Belastingdienst, Rijkswaterstaat, DJI, IND, UWV, NZA, Hoge Colleges van Staat);
- Ambtenaren exclusief Rijksoverheid:
  Ambtenaren werkzaam bij één van de provincies, gemeenten of waterschappen.

Bedrijfsleven

- Bedrijfsleven klein-MKB:
  Medewerkers uit alle sectoren van het bedrijfsleven die werkzaam zijn voor een organisatie tot 10 medewerkers (inclusief ZZP'ers);
- Bedrijfsleven groot-MKB:
  Medewerkers uit alle sectoren van het bedrijfsleven die werkzaam zijn voor een organisatie met 10 tot en met 249 medewerkers;
- Bedrijfsleven grootbedrijf:
  Medewerkers uit alle sectoren van het bedrijfsleven die werkzaam zijn voor een organisatie met 250 medewerkers of meer.

Algemeen publiek 13+

- Burgers:
  Inwoners van Nederland van 13 jaar en ouder.

Binnen de professionele doelgroepen (overheid en bedrijfsleven) is onderscheid gemaakt tussen degenen die wel verantwoordelijk zijn voor ICT-zaken en degenen die hier niet voor verantwoordelijk zijn[1].

Zoals ook in de metingen van eerdere jaren geldt als aanvullende voorwaarde voor deelname aan het onderzoek dat men binnen de zakelijke doelgroep een door de werkgever beschikbaar gesteld apparaat

[1] Dit is in de plaats gekomen van een onderscheid naar wel en niet een leidinggevende functie in voorgaande metingen.

(desktop computer, laptop, tablet en/of smartphone) moest hebben om thuis of op kantoor werkzaamheden uit te voeren.
Deelnemers binnen het algemeen publiek moeten thuis minimaal beschikken over een dergelijk apparaat (desktop computer, laptop, tablet en/of smartphone).

ICT-gebruik van de doelgroepen in het onderzoek

Devices beschikbaar in thuissituatie
Een ruime meerderheid van de deelnemers aan het onderzoek beschikt thuis over een laptop en/of een smartphone (80%). Ook het tabletbezit is hoog te noemen: 69% van de ondervraagden beschikt hierover in de thuissituatie. Ongeveer zes op de tien deelnemers beschikt thuis nog over een 'klassieke' desktop. Een veel beperktere groep bezit wearables (zoals smart watches, Google Glass) of smart devices (zoals domotica, slimme thermostaat).

Devices via werkgever
De desktop computer, laptop en een smartphone zijn apparaten die regelmatig door een werkgever voor werkdoeleinden beschikbaar worden gesteld; ongeveer de helft van de werkenden is in het bezit van (één van) deze apparaten.

Mate verantwoordelijkheid voor ICT zaken / automatisering binnen de organisatie
Het overgrote deel (twee derde) van de werkende deelnemers geeft aan niet verantwoordelijk te zijn voor ICT-zaken/automatisering binnen hun organisatie: 18% is eindverantwoordelijk en 16% is mede-verantwoordelijk. Vooral de medewerkers werkzaam in het klein-MKB geven aan eindverantwoordelijk te zijn voor ICT-zaken/automatisering. Logisch natuurlijk: veel mensen zijn als ZZP'er eigen baas en dus hoofdverantwoordelijk.

Organisatie ICT-zaken binnen de organisatie
Voor een ruime meerderheid van de werkende deelnemers (59%) worden de ICT-zaken beheerd door een interne ICT'er / interne ICT-afdeling; 12% geeft aan dat er niemand specifiek verantwoordelijk is voor ICT-zaken (vooral medewerkers in het klein-MKB). Bij medewerkers in het grootbedrijf worden ICT-zaken vaker beheerd door een interne ICT'er / interne ICT-afdeling dan medewerkers in het klein- en groot-MKB. Bij medewerkers in het groot-MKB worden ICT-zaken vaker beheerd door een extern bedrijf dan medewerkers uit het klein-MKB en grootbedrijf. Daarnaast geven ambtenaren buiten de Rijksoverheid vaker aan dat ICT-zaken beheerd worden door een interne ICT'er / interne ICT-afdeling dan ambtenaren binnen de Rijksoverheid.

Instructies van werkgever voor veilig gebruik van devices
Ruim de helft van de werkenden (60%) geeft aan instructies te hebben ontvangen van de werkgever voor het veilig gebruik van een laptop, tablet of smartphone. Ambtenaren bij de Rijksoverheid geven vaker aan dergelijke instructies te hebben ontvangen ten opzichte van ambtenaren buiten de Rijksoverheid. Daarnaast zien we dat bij een grote bedrijfsomvang (groot-MKB en grootbedrijf) medewerkers vaker aangeven dergelijke instructies te hebben ontvangen.

Methode en veldwerk

Net als in eerdere jaren is er voor gekozen om het onderzoek volledig online uit te voeren, met behulp van een door GfK geprogrammeerde vragenlijst. Het veldwerk verliep als volgt: de respondent kreeg via e-mail een uitnodiging voor het onderzoek, waarin een link is opgenomen naar de online vragenlijst.

Het veldwerk vond plaats van 22 juni tot en met 12 juli 2015. Tijdens de veldwerkperiode zijn meerdere herinneringen gestuurd om de benodigde respons te halen.

Steekproef en respons

Voor dit onderzoek zijn in totaal zes steekproeven getrokken: voor elke doelgroep één. Onderstaande tabel geeft de omvang van de bruto en netto steekproef per doelgroep weer.

Tabel 1a. Overzicht bruto en netto steekproef en respons

Doelgroepen	Bruto steekproef	Netto n
Ambtenaren Rijksoverheid	700	301
Ambtenaren exclusief Rijksoverheid	700	301
Medewerkers klein-MKB	1.200	400
Medewerkers groot-MKB	1.400	401
Medewerkers grootbedrijf	900	401
Burgers 13+	3.250	1.344
Totaal	*8.150*	*3.148*

Het gemiddelde responspercentage, dat wil zeggen alle compleet ingevulde vragenlijsten als percentage van het totaal aantal voor het onderzoek uitgenodigde respondenten, bedraagt 39%.

Alle doelgroepen kregen aan het begin van de vragenlijst diverse selectievragen voorgelegd, zodat een-ieder met zekerheid werd toegewezen aan de voor hem of haar van toepassing zijnde doelgroep.
Alle respondenten die hebben deelgenomen aan het Cybersecurity onderzoek in 2014 zijn uitgesloten van deelname.

Representativiteit

Om de representativiteit van de steekproeven te waarborgen is gezorgd voor:

- Steekproeven van voldoende omvang om betrouwbare uitspraken te kunnen doen op basis van de netto respons (netto n).
- Een representatieve verdeling op relevante kenmerken[2]. Daartoe zijn de steekproeven uit het GfK-panel van tevoren verdeeld (gestratificeerd) naar verhoudingen van relevante kenmerken in de populatie en zijn ze hierop achteraf herwogen.

Meer informatie over de weging en de steekproefverdeling treft u aan in bijlage 8.2.

[2] Bij de ambtenaren buiten de Rijksoverheid gaat het bijvoorbeeld om een representatieve spreiding over provincie, gemeente en waterschap; bij het bedrijfsleven over een representatieve spreiding over onder meer branches en bedrijfsgrootte. Bij het algemene publiek gaat het om een representatieve spreiding over leeftijd, geslacht, opleidingsniveau, regio en internetgebruik.

1.3 Leeswijzer

Voordat we ingaan op de beschrijving van de resultaten, volgt eerst de management summary.

De hoofdstukken in deze rapportage die de resultaten beschrijven, zijn thematisch opgebouwd: per thema worden eerst de overall resultaten beschreven, dan de verschillen tussen de doelgroepen en tot slot de verschillen naar achtergrondkenmerken. Door de gewijzigde onderzoeksopzet (wijzigingen in de opbouw van de steekproef, als ook een nieuwe vragenlijst) is ervoor gekozen om de vergelijking met voorgaande jaren te beperken tot een vergelijking op enkele hoofdlijnen, in de management summary. In de rest van de rapportage wordt dus niet met eerdere metingen vergeleken.

In de bijlagen wordt ingegaan op de methodologische aspecten van het onderzoek.

Ten geleide bij het rapport

Aard van de resultaten
Alle resultaten betreffen *zelfgerapporteerde* kennis, houding en gedrag.

Weergave van significante verschillen
De gevonden percentages zijn getoetst op significantie van de verschillen:

- tussen de zes doelgroepen; hierbij kijken we naar verschillen tussen de twee groepen overheids-functionarissen, naar verschillen tussen de drie groepen medewerkers uit het bedrijfsleven, en specifiek naar verschillen tussen medewerkers klein-MKB en burgers (omdat een belangrijke vraag vooraf was of deze twee groepen vergelijkbare resultaten laten zien).
- naar geslacht, leeftijd en opleiding;
- naar wel of niet verantwoordelijk voor ICT-zaken en automatisering.

De tabellen met de significantievergelijkingen zijn separaat van dit rapport opgeleverd.

In het rapport is alleen melding gemaakt van verschillen wanneer deze significant zijn op het niveau van $p < 0,05$. Dit betekent dat de kans dat de gevonden verschillen in de steekproef op toeval berusten kleiner is dan vijf procent. Daar waar de som van percentages geen 100 bedraagt, wordt dit veroorzaakt door afrondingsverschillen.

Antwoorden op open vragen
De vragenlijst bevat een aantal open vragen, waarbij de respondent het gegeven antwoord letterlijk heeft ingetypt. De open antwoorden van sommige open vragen zijn per antwoord nagecodeerd, waardoor een percentering van de resultaten mogelijk is.

Tevens wordt separaat een overzicht geleverd van alle gegeven open antwoorden. Om recht te doen aan de sfeer en achtergrond waarin de antwoorden zijn gegeven, zijn stijl-, taal- en typefouten ondergeschikt gemaakt aan de context, waardoor gekozen is voor een letterlijke, ongecorrigeerde weergave van deze antwoorden.

2. Management Summary

Achtergrond en doel onderzoek

In opdracht van de NCTV heeft GfK onder in totaal 3.148 personen (online) onderzoek uitgevoerd naar cybersecurity awareness en gedrag. Het onderzoek in 2015 betreft inmiddels alweer de vierde meting: in 2013 en 2014 heeft GfK de tweede en derde meting uitgevoerd (1-meting en 2-meting) en in 2012 heeft Motivaction het onderzoek voor het eerst uitgevoerd (pilot, 0-meting). De meerjarige uitvoering is erg waardevol omdat op die manier de kennis rondom cybersecurity awareness en gedrag met elke meting kan worden verbreed en verdiept.

Het hoofddoel van het onderzoek is in 2015: het verkrijgen van inzicht in hoe veilig of onveilig men zich online gedraagt. In voorgaande jaren lag de focus meer op cyber awareness.
Belangrijk om te vermelden is dat het onderzoek is gebaseerd op de *zelfgerapporteerde* kennis, houding en gedrag van respondenten.

Onderzoeksopzet in vogelvlucht

In vergelijking met eerdere metingen van cybersecurity is dit jaar in overleg met de opdrachtgevers minder differentiatie aangebracht in de doelgroep publieke sector en meer differentiatie aangebracht in de doelgroep bedrijfsleven. De voornaamste reden hiervoor is de nadruk die in de campagne Alert Online dit jaar gelegd zal worden op digitaal verantwoord ondernemen.
Een belangrijke verandering is verder een *inhoudelijke* verschuiving van de focus, van bewustzijn van cybersecurity (awareness) naar cybersecure gedrag. Deze verschuiving heeft als primair doel om zicht te krijgen op hoe gedrag direct en indirect kan worden beïnvloed. Dit blijkt uit de aanpassingen in de vragenlijst, maar komt ook mede tot uitdrukking in de verdiepende analyse die is uitgevoerd.

Het online onderzoek heeft plaatsgevonden van 22 juni 2015 tot en met 12 juli 2015. Er is gebruik gemaakt van het GfK online panel.

De volgende doelgroepen zijn voor het onderzoek ondervraagd:

- Ambtenaren van de Rijksoverheid;
- Ambtenaren exclusief Rijksoverheid (provincies, gemeenten, waterschappen);
- Medewerkers van bedrijven in het klein-MKB (tot 10 medewerkers, inclusief ZZP'ers);
- Medewerkers van bedrijven in het groot-MKB (10 - 249 medewerkers);
- Medewerkers van grootbedrijven (250 of meer medewerkers);
- Tot slot: Nederlandse burgers van 13 jaar en ouder.

Deze management summary bestaat uit een samenvatting van de resultaten en een overzicht van de belangrijkste conclusies.

Belangrijkste inzichten

De andere insteek van het onderzoek heeft ertoe geleid dat er dit jaar binnen het onderzoek meer aandacht is geweest voor cybersecure gedrag.

De belangrijkste inzichten die uit dit onderzoek naar voren komen zijn:

1) *Meer awareness leidt niet vanzelf tot beter gedrag.*
   Vanuit eerdere metingen is bekend dat de awareness onder professionele doelgroepen over het algemeen groter is dan onder het algemeen publiek. En dat bijvoorbeeld doelgroepen als de Rijksambtenaren en de medewerkers grootbedrijf zich meer bewust zijn van de eigen digitale veiligheid dan andere groepen. Als we echter naar de verschillen kijken in het feitelijke gedrag, dan zijn die tussen de verschillende doelgroepen bijzonder klein. Dé uitdaging ligt dus in het feit om van awareness tot cybersecure gedrag te komen.

2) *Klein-MKB'ers zijn een bijzondere groep, maar niet net als burgers*
   Bij de doelgroep Klein-MKB komen eigenlijk twee werelden samen: privé en werk. Dat is voor hen vaak met elkaar vervlochten, waardoor er ook in termen van digitale veiligheid sprake is van een zekere overlap. Men realiseert zich dat onveilig gedrag privé impact kan hebben op de werksituatie en andersom. Dat maakt hen op dit moment, weliswaar met een gering verschil, de groep die het meest cybersecure handelt.

3) *Opleidingsniveau heeft weinig effect op de mate van cybersecure gedrag*
   Het blijkt dat er op basis van opleidingsniveau geen wezenlijke verschillen zijn aan te duiden in de mate van cybersecure gedrag. Geslacht en leeftijd wel spelen wel een rol: ouderen zijn meer cybersecure qua gedrag dan jongeren en mannen zijn het iets meer dan vrouwen.

Samenvatting en conclusies

Voor de leesbaarheid van het rapport is ervoor gekozen om de samenvatting volgens een soortgelijke structuur te laten verlopen als het tekstuele rapport, zodat in de hoofdstukken altijd relatief eenvoudig de specifiekere beschrijving kan worden teruggevonden.
In de samenvatting zijn tegelijkertijd de voornaamste conclusies verwerkt, die op basis van de resultaten getrokken kunnen worden.

Kennis & houding (inclusief bewustzijn en verantwoordelijkheden)

Ransomware, cryptoware en social engineering zijn nog maar in beperkte mate bekende begrippen: ruim de helft geeft aan hier nog nooit van gehoord te hebben. Phishing mails, virusscanners en firewalls zijn wel een stuk bekender.
Onder de bedrijfsdoelgroepen lijkt de omvang van de organisatie een rol te spelen in de (kennis van de) aanwezigheid van beleid rondom de digitale werkomgeving en het inwerken van nieuwe medewerkers in veilig digitaal werken; hoe groter de organisatie, des te vaker dit beleid aanwezig is volgens medewerkers.

De verantwoordelijkheid voor de veiligheid van internetgebruik wordt vooral in de thuissituatie, maar ook in de werksituatie, door een meerderheid van de respondenten bij zichzelf gelegd. De eigen verantwoordelijkheid wordt vooral gevoeld door mannen, 50-plussers en hoogopgeleiden. En door degenen die medeverantwoordelijk zijn voor ICT in hun organisatie.
Een aanzienlijke groep vindt een deel van die verantwoordelijkheid ook liggen bij internet providers (thuissituatie), de ICT'er/ICT-afdeling (werksituatie, indien aanwezig) en het management van de organisatie (werksituatie).

Als we inzoomen op de werksituatie, acht een ruime meerderheid zich voldoende bewust van het belang van digitale veiligheid en vindt zichzelf voldoende op de hoogte van de eigen verantwoordelijkheden. Ook het bewustzijn van de mogelijke gevaren voor de organisatie op het gebied van digitale veiligheid en kennis over bij wie incidenten te melden, worden hoog ingeschat. Men vindt zichzelf wel minder goed op de hoogte van *beleid* met betrekking tot digitale veiligheid (dit komt overigens overeen met de resultaten van het onderzoek van 2014).

Inschatting digitale veiligheid & zorgen
Binnen de professionele doelgroepen vinden vooral medewerkers bij de Rijksoverheid en medewerkers in het grootbedrijf dat hun organisatie aandacht heeft voor de digitale veiligheid. We zien dan ook dat deze groepen de digitale veiligheid van hun werksituatie over het algemeen hoger inschatten. Een algemene lijn is - nog steeds, want ook uit eerdere metingen bleek dit al - dat werknemers hun eigen digitale veiligheid hoger inschatten dan die van hun collega's.

Wat verder opvalt, is dat de professionele doelgroepen hun digitale veiligheid thuis hoger inschatten dan het algemeen publiek, alhoewel men zich er thuis over het algemeen wel meer zorgen over maakt dan op het werk. Ook geeft nog altijd bijna de helft van de respondenten aan zich niet voldoende beschermd te voelen tegen de risico's van internet. Men voelt zich dus redelijk veilig, maar maakt zich wel enige zorgen en voelt zich vaak toch eigenlijk nog niet voldoende beschermd.

Inschatting kans op persoonlijk slachtofferschap
Evenals in 2014 is de helft van de respondenten in de veronderstelling dat kwaadwillenden toch wel slagen in hun opzet en dat je je daarom tegen grote gevaren eigenlijk niet kunt weren. Ruim een derde geeft bijvoorbeeld aan bang te zijn voor identiteitsfraude.
De inschatting dat men zelf slachtoffer wordt van bepaalde vormen van cybercrime, wordt het grootst geacht bij zaken zoals een product kopen dat vervolgens niet wordt geleverd, het zonder toestemming gebruiken of verspreiden van persoonlijke gegevens en pogingen om gegevens te ontfutselen. De kans op zaken zoals gefilmd worden, geld van de rekening halen of het gebruik van de creditcard door een ander wordt door de meerderheid lager ingeschat. Tevens veronderstelt de helft phishing mails meteen te zullen herkennen bij ontvangst. De risicoperceptie is opmerkelijk vergelijkbaar tussen de doelgroepen.

Inschatting impact van incidenten
De impact van de mogelijke gevolgen van ongewenste inbreuk op de digitale veiligheid in het algemeen - in zowel de privésituatie als de werksituatie - worden doorgaans als (zeer) ernstig ingeschat.
In de werksituatie gaat het bij ambtenaren vooral om zorgen over reputatieschade voor de werkgever, gevolgd door privacy-schade voor derden en voor de werkgever. Bij bedrijven is financiële schade een belangrijkere zorg en speelt reputatieschade juist een minder grote rol.

In de privésituatie richt de zorg zich sterker op financiële schade voor de persoon in kwestie en de gevolgen voor anderen in de omgeving. Medewerkers in klein-MKB maken zich ook zorgen over de impact op de uitvoering van hun zakelijke activiteiten.
Toch leidt dit alles doorgaans niet tot veel meer veilig digitaal gedrag. Dat komt vermoedelijk doordat het gevaar voor mensen vaak niet concreet genoeg is en omdat men bovendien niet goed weet hoe men zich hiertegen moet wapenen.

Ondernomen maatregelen
De *spontaan* meest genoemde beschermingsmaatregel tegen misbruik van de desktop computer of laptop in de privésituatie is nog steeds de installatie van (goede) antivirussoftware, op ruime afstand gevolgd door het gebruik van een firewall. In de werksituatie gaat men er vaak van uit dat de IT'er/IT-afdeling dergelijke maatregelen neemt, maar worden veilig wachtwoordgebruik en antivirussoftware ook wel vaker genoemd, vooral door klein-MKB.

Werkelijk slachtofferschap
Ongewenste e-mail en phishing zijn een ruime meerderheid van de respondenten wel eens overkomen. Voor ongewenste e-mail (spam) is dit wellicht te verwachten. Voor phishing, een meer ingrijpende manier van slachtofferschap, mag dit als een fors aandeel worden beschouwd, maar wel moet worden toegevoegd dat dit niet betekent dat iedereen er ook daadwerkelijk 'ingetrapt' hoeft te zijn. Virussen komen ook regelmatig voor en een vijfde heeft wel eens te maken gekregen met mensen die gegevens opvragen onder valse voorwendselen (social engineering).

Gewenste gedragingen (zelfgerapporteerd)
Om het cybersecure gedrag te vergroten is er vooral nog winst te halen op de volgende punten: het gebruik van WiFi-verbindingen (automatisch verbinding maken en het gebrek aan het gebruik van een VPN-app), het regelmatig maken van back-ups, het instellen een van twee-staps authenticatie (waar mogelijk) en wachtwoordgedrag.
Daarnaast is websitebezoek in enige mate een aandachtspunt: circa een derde geeft aan niet te controleren of de juiste URL in de internetbrowser staat bij het bezoek van websites, of dat er een groen slotje aanwezig is bij websites waar gegevens ingevoerd moeten worden. Aangaande phishing mails wordt beduidend minder onveilig gedrag gerapporteerd; de overgrote meerderheid zegt verdachte mails direct te verwijderen (ook van een bekende afzender) en niet op links te klikken die men niet vertrouwt.

Op basis van de indexscore, berekend op basis van een binnen het onderzoek uitgevoerde inventarisatie van (de mate van) cybersecure gedrag, valt te concluderen dat Nederland een krappe voldoende scoort. Er is dus nog voldoende ruimte voor verbetering. Daarnaast is geconstateerd dat de verschillen in de mate van digitaal veilig gedrag tussen de doelgroepen zeer gering zijn.

Dit is interessant, omdat de professionele doelgroepen vaak wel een hoger *bewustzijnsniveau* hebben dan het algemeen publiek, zo blijkt ook uit eerdere metingen.

Bij het maken van cyberbeleid is het verder van belang om oog te hebben voor een aantal factoren die op meer indirecte wijze van invloed zijn op de mate van cybersecure gedrag:

- Leeftijd is een belangrijk element om rekening mee te houden: ouderen (50-plussers) gedragen zich digitaal doorgaans veiliger dan jongeren (vooral 13-17 jaar, maar ook 18-30 jaar). Jongeren gedragen zich minder cybersecure, waarschijnlijk omdat ze de risico's voor henzelf onderschatten.
- Andere elementen die van invloed zijn op de hoogte van (de indexscore voor) cybersecure gedrag zijn onder andere het feit of men zichzelf digitaal veilig voelt in de privé-situatie en of men zichzelf in staat acht om phishing mails te signaleren.
- In de werksituatie is aandacht voor cybersecurity bij nieuwe medewerkers een belangrijk middel om cybersecure gedrag door de hele organisatie te stimuleren. Dit geldt vooral voor overheden en grotere MKB bedrijven, waar dit gebruikelijker is dan bij klein-MKB.

Preventiegedrag op het werk

Het merendeel van de professionals geeft aan zakelijke devices niet door anderen te laten gebruiken en bij gebruik van openbare WiFi-verbindingen bewuste keuzes te maken over welke handelingen men wel of niet verricht. Zaken waar minder veilig mee wordt omgegaan zijn: het gebruik van beveiligde VPN-verbindingen (via token), bij gebruik van apparaten in een openbare ruimte maatregelen nemen (zoals een privacy screen) zodat anderen niet kunnen meekijken, en het laten controleren van een USB-stick op virussen als deze extern is geweest.

Wachtwoordgebruik

In het wachtwoordgedrag is dezelfde lijn zichtbaar als in het onderzoek van 2014: het wachtwoordgebruik is over het algemeen nog steeds niet erg veilig en er wordt veelal reactief gehandeld rondom het veranderen van wachtwoorden.

Op verschillende vlakken wordt risicogedrag gerapporteerd ten aanzien van wachtwoordgebruik. Een minderheid wijzigt de wachtwoorden (minimaal) 3-maandelijks en gebruikt wachtwoorden van meer dan 12 karakters. Daarnaast worden wachtwoorden nog regelmatig genoteerd op briefjes die verstopt worden (22%), voor meerdere accounts gebruikt (42%) en over het algemeen pas na een (automatische) melding gewijzigd (41%). Overigens leert 6 op de 10 mensen de wachtwoorden uit het hoofd.

Voorgenomen gedrag bij voorval

Bij ontvangst van een verdachte e-mail van de eigen bank zegt de meerderheid deze direct ongelezen te zullen verwijderen. Bij een dergelijke e-mail met een bekende als afzender, gaat het om twee vijfde dat dit zegt te gaan doen. Ook geeft een deel aan contact te zoeken met de afzender om te controleren of de mail geen phishing betreft (30% in geval van een bekende; 21% in geval van de eigen bank). Een kleine minderheid geeft aan uit nieuwsgierigheid verdachte mails toch te openen; bij mails afkomstig van een bekende zou men dit vaker doen dan bij mails van de eigen bank.

3. Hoe digitaal veilig zijn de doelgroepen en welke factoren beïnvloeden digitaal veilig gedrag?

Bij de analyse is in de eerste stap vastgesteld in welke mate de verschillende doelgroepen aangeven zich digitaal veilig te gedragen. De basis hiervoor werd gevormd door een door de NCTV opgestelde lijst met gewenste cybersecure gedragingen.

De eerste stap
De gewenste gedragingen zijn gerangschikt onder diverse thema's. Aan elk thema is door de NCTV een gewicht gehangen om onderscheid te kunnen maken tussen belangrijke en minder belangrijke wenselijke gedragingen. In tabel 3.1 is zichtbaar welke gewichten daar, op basis van de beleidsuitgangspunten, aan verbonden zijn.

Tabel 3.1: elementen cybersecure gedrag

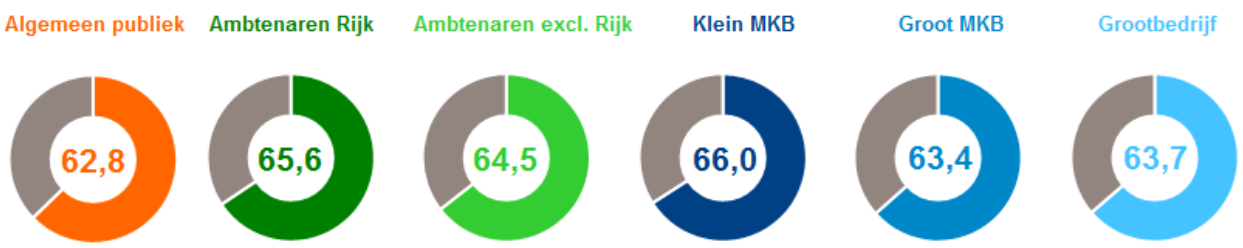
Thema	Gewicht
1. Wachtwoorden	18
2. Software-updates	18
3. Back-ups	14
4. Herkennen van phishing mails (om o.a. cryptoware- en ransomwarebesmetting te voorkomen)	12
5. WiFi – het gebruik van draadloos internetten	10
6. Gebruik smartphone	10
7. Websites bezoeken	5
8. Andere apparaten verbonden met internet (netwerk-opslag, beveiligingscamera's, etc.)	5
9. Bring your own device *(alleen voor professionals)*	5
10. Twee-factor authenticatie	4
11. Veilig online winkelen	4

Als we kijken naar waar men veilig en minder veilig gedrag vertoont, dan is de eerste conclusie dat er over de hele linie nog veel vooruitgang te boeken valt op de volgende aspecten:

1) het gedrag rondom WiFi-netwerken
2) het regelmatig maken van back-ups
3) verstandig wachtwoordgebruik (regelmatig vervangen en meer dan 12 karakters)

Op basis van deze zelfgerapporteerde gedragingen en bijbehorende gewichten is er vervolgens een indexscore berekend. Deze geeft de mate aan waarin iemand zich cybersecure gedraagt, op basis van de optelsom van de gedragingen. Hoe hoger de score, hoe meer cybersecure men is qua gedrag. De gemiddelden per doelgroep ziet u hieronder.

Indexscores Cybersecure Gedrag (per doelgroep,gemiddelde)



Er zijn twee conclusies te trekken op basis van de gemiddelde indexscores: het cybersecure gedrag valt te kwalificeren als een krappe voldoende: er is ook nog genoeg verbetering mogelijk. Daarnaast zien we dat de verschillen in de mate van digitaal veilig gedrag tussen de doelgroepen zeer gering zijn. Dit is interessant omdat de professionele doelgroepen (zeker de Rijksoverheid) vaak wel een hoger *bewustzijnsniveau* hebben dan andere doelgroepen, zo blijkt ook uit eerdere metingen.

De kleine verschillen in gedrag tussen de doelgroepen die zichtbaar zijn, wijzen erop dat professionele doelgroepen zich over de hele linie wel in iets sterkere mate cybersecure gedragen dan het algemeen publiek. Rijksambtenaren scoren iets beter ten opzichte van ambtenaren buiten de Rijksoverheid. Opmerkelijk is dat werknemers in klein-MKB zich in iets sterkere mate cybersecure gedragen dan werknemers in groot-MKB en grootbedrijf. Dit valt mogelijk te verklaren door het feit dat werknemers in klein-MKB zich beter bewust zijn van de risico's die ze lopen en omdat ze ook vaker zelf verantwoordelijk zijn voor de digitale veiligheid in hun bedrijf.

De tweede stap: welke factoren hebben invloed op cybersecure gedrag?
Naast de wetenschap hoe hoog iedere doelgroep scoort qua cybersecure gedrag, is de indexscore ook een goed uitgangspunt voor een verdiepende analyse. Het doel daarvan is te bepalen in hoeverre diverse factoren, verzameld binnen het onderzoek, een verklaring kunnen vormen voor de verschillen in hoogte van die indexscore. Dus: wat bepaalt in welke mate of iemand hoog of laag scoort op de onderdelen van cybersecure gedrag? We hebben hierbij zowel gekeken naar factoren op het gebied van kennis en houding, als naar achtergrondfactoren als leeftijd en opleidingsniveau.

De verdiepende analyses wijzen uit dat een veelheid aan factoren een rol speelt bij het verklaren van het gedrag. Dat wil dus ook zeggen dat een brede aanpak in principe helpt om cybersecure gedrag te stimuleren. De analyse levert een aantal aanvullende inzichten op (zie kader).

- Mannen handelen iets meer cybersecure dan vrouwen.
- Leeftijd speelt een rol: hoe ouder, des te meer cybersecure, is de stelregel.
- Opleiding speelt een opmerkelijk geringe rol, alhoewel er op gedragspecifieke elementen wel accentverschillen zijn. Hoogopgeleiden zijn bijvoorbeeld minder voorzichtig met WiFi-verbindingen en laagopgeleiden vertonen onveiliger wachtwoordgedrag.
- Als men denkt phishing-mails te kunnen herkennen, blijkt men ook meer cybersecure te handelen.
- Hoe hoger men de digitale veiligheid in de privé-situatie inschat, hoe meer cybersecure men ook blijkt te handelen. Of andersom geredeneerd: hoe meer cybersecure men handelt, hoe digitaal veiliger men zich privé voelt.
- Als de werkgever aandacht besteedt aan digitale veiligheid bij het inwerken van medewerkers, uit zich dat ook in meer cybersecure gedrag van werknemers binnen dat bedrijf.
- Slachtofferschap van een incident op het gebied van digitale veiligheid leidt niet automatisch tot meer cybersecure gedrag. Sterker nog: vaker lijkt er sprake van een licht negatief verband: mensen die iets hebben meegemaakt, gedragen zich wat minder cybersecure. Als voorbeeld ongewenste e-mail (SPAM): mensen die hiermee te maken hebben gekregen, vertonen minder cybersecure gedrag. Onverschilligheid of onvermogen staat actie blijkbaar in de weg.

4. Resultaten 2015: Kennis en houding

4.1 Beknopte samenvatting

Kennis & houding (incl. bewustzijn en verantwoordelijkheden)
Zaken zoals ransomware, cryptoware en social engineering zijn over het algemeen nog vrij onbekend onder respondenten; ruim de helft geeft aan nog nooit gehoord te hebben van deze zaken. Phishing mails, virusscanners en firewalls zijn echter wel een stuk bekender.
Bij bedrijven lijkt de omvang van de organisatie een rol te spelen voor de (kennis van de) aanwezigheid van beleid rondom de digitale werkomgeving en het inwerken van nieuwe medewerkers in veilig digitaal werken; des te groter de organisatie, des te vaker dit van toepassing is.

De verantwoordelijkheid voor de veiligheid van internetgebruik wordt vooral in de thuissituatie maar ook in de werksituatie door een meerderheid van de respondenten grotendeels bij henzelf gelegd. De eigen verantwoordelijkheid wordt vooral gevoeld door mannen, 50-plussers en hoogopgeleiden. En door degenen die medeverantwoordelijk zijn voor ICT in hun organisatie.
Een aanzienlijke groep vindt een deel van die verantwoordelijkheid ook liggen bij Internet providers (thuissituatie), de ICT'er/ICT-afdeling (werksituatie, indien aanwezig) en het management van de organisatie (werksituatie).

In de werksituatie acht een ruime meerderheid zich voldoende bewust van het belang van digitale veiligheid en vindt zichzelf tevens voldoende op de hoogte van de eigen verantwoordelijkheden. Ook het bewustzijn van de mogelijke gevaren voor de organisatie op het gebied van digitale veiligheid en kennis over bij wie incidenten te melden worden hoog ingeschat. Men acht zich minder goed op de hoogte van beleid met betrekking tot digitale veiligheid; circa een derde geeft aan *niet* goed op de hoogte te zijn hiervan (dit komt overigens overeen met de resultaten van het 2014-onderzoek).

4.2 Overall houding en kennis

Hieronder volgen de belangrijkste resultaten ten aanzien van overall houding en kennis.

Figuur B1: Kunt u aangeven in welke mate u bekend bent met onderstaande zaken?

	Algemeen publiek (n=1344)	Ambtenaren Rijk (n=301)	Ambtenaren excl. Rijk (n=301)	Klein MKB (n=400)	Groot MKB (n=401)	Grootbedrijf (n=401)
Phishing mails						
Ik weet wat het is	81%	94%	89%	92%	86%	84%
Wel eens van gehoord, maar weet niet wat het is	10%	4%	9%	4%	7%	10%
Nooit van gehoord	9%	2%	2%	3%	7%	6%
Malware						
Ik weet wat het is	56%	71%	63%	67%	64%	65%
Wel eens van gehoord, maar weet niet wat het is	24%	22%	25%	21%	22%	19%
Nooit van gehoord	20%	7%	12%	12%	14%	16%
Virusscanner						
Ik weet wat het is	95%	98%	97%	99%	98%	96%
Wel eens van gehoord, maar weet niet wat het is	3%	1%	3%	1%	1%	3%
Nooit van gehoord	2%	0%	0%	0%	1%	1%
Firewall						
Ik weet wat het is	83%	94%	90%	89%	90%	90%
Wel eens van gehoord, maar weet niet wat het is	13%	6%	9%	10%	8%	8%
Nooit van gehoord	4%	0%	1%	1%	2%	2%
Ransomware						
Ik weet wat het is	14%	21%	18%	19%	20%	21%
Wel eens van gehoord, maar weet niet wat het is	21%	29%	26%	24%	24%	19%
Nooit van gehoord	65%	51%	56%	57%	56%	60%
Cryptoware						
Ik weet wat het is	12%	29%	20%	17%	18%	20%
Wel eens van gehoord, maar weet niet wat het is	26%	32%	30%	31%	27%	30%
Nooit van gehoord	62%	39%	50%	52%	54%	51%
Social Engineering						
Ik weet wat het is	9%	18%	11%	13%	13%	15%
Wel eens van gehoord, maar weet niet wat het is	29%	34%	27%	31%	24%	31%
Nooit van gehoord	62%	49%	62%	55%	62%	54%

Overall beeld

Ruim driekwart van de respondenten weet wat een phishing-mail, een virusscanner en een firewall is. Van malware weet ruim de helft wat het is. Ransomware, cryptoware en social engineering zijn een stuk minder bekend; ruim de helft van de respondenten geeft zelfs aan nog nooit gehoord te hebben van deze zaken.

Vergelijking tussen doelgroepen

Ambtenaren Rijksoverheid weten beter wat cryptoware, social engineering en phishing mails zijn dan de Ambtenaren exclusief Rijksoverheid.

Tussen de verschillende bedrijfsgrootten in het bedrijfsleven zijn weinig verschillen zichtbaar, behalve op het gebied van phishing mails. Hier geven medewerkers klein-MKB vaker aan te weten wat phishing mails zijn dan medewerkers groot-MKB en grootbedrijf.

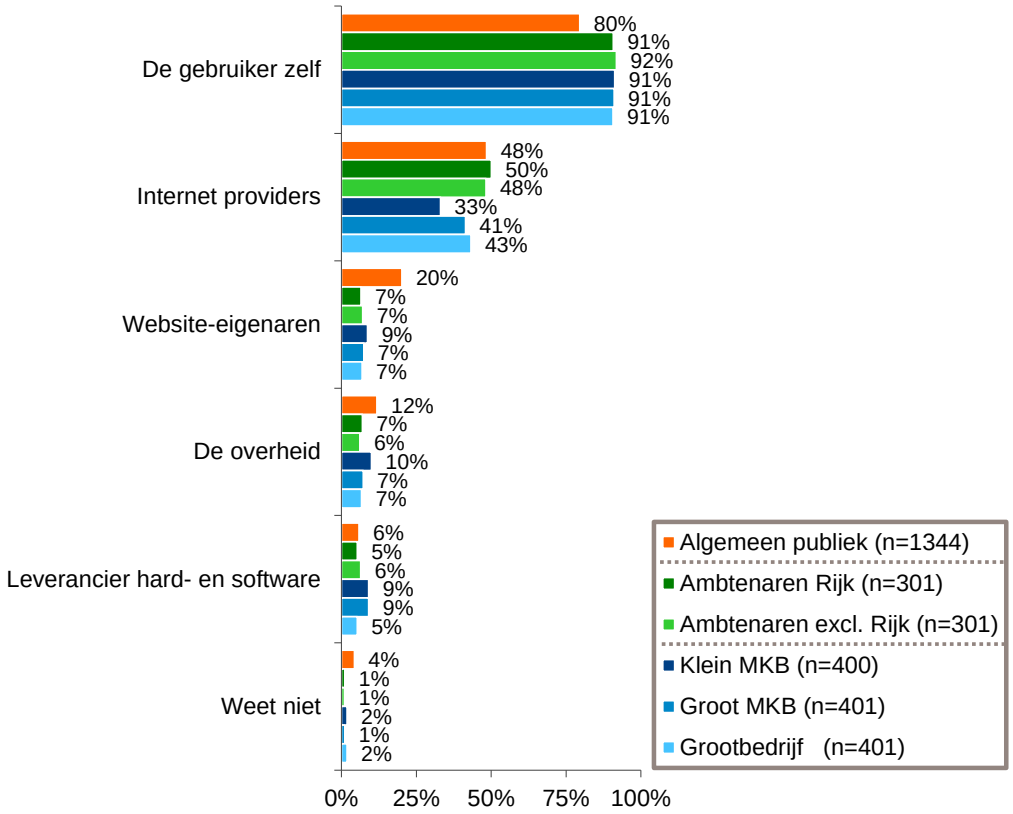
Het kennisniveau van de voorgelegde cybersecurity-gerelateerde zaken van medewerkers klein-MKB is over het algemeen hoger dan dat van burgers.

Verschillen in achtergrondkenmerken

Het kennisniveau van de voorgelegde cybersecurity-gerelateerde zaken is op nagenoeg alle punten hoger onder mannen dan onder vrouwen. Ook onder hoogopgeleiden en 30-plussers is het kennisniveau hoger dan onder midden- en laagopgeleiden en de leeftijdsgroepen t/m 30 jaar. Medewerkers die (mede-) verantwoordelijk zijn voor ICT-zaken hebben over het algemeen - logisch - een hoger kennisniveau van de voorgelegde cybersecurity-gerelateerde zaken dan medewerkers die niet verantwoordelijk zijn voor ICT-zaken (alleen voor firewall & virusscanner zijn geen verschillen zichtbaar).

Verantwoordelijk voor veiligheid internetgebruik (thuis)

Figuur B06: Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid op het gebied van internetgebruik in uw thuissituatie voornamelijk moet liggen?



Overall beeld
Wanneer het gaat over veiligheid op het gebied van internetgebruik thuis geven de meeste respondenten aan hier voornamelijk zelf (als gebruiker) voor verantwoordelijk te zijn. Ook de internetproviders worden als verantwoordelijk aangemerkt.

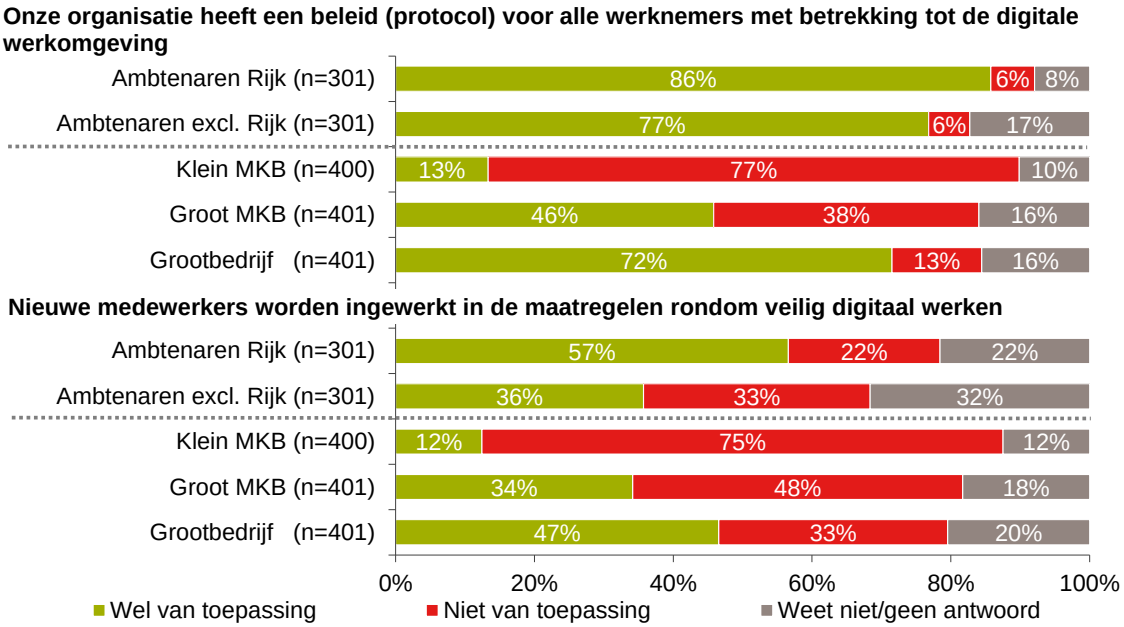
Vergelijking tussen doelgroepen
Medewerkers in grotere bedrijven (groot-MKB en grootbedrijf) zien vaker dan medewerkers uit het klein-MKB verantwoordelijkheid voor de veiligheid van internetgebruik in de thuissituatie mede bij Internet providers. Medewerkers uit het klein-MKB leggen vaker dan medewerkers grootbedrijf en burgers de verantwoordelijkheid voor de veiligheid van internetgebruik in de thuissituatie mede bij leveranciers van hard- en software. Medewerkers uit het klein-MKB geven overigens vaker dan burgers aan dat deze verantwoordelijkheid mede bij de gebruiker zelf zou moet liggen.

Verschillen in achtergrondkenmerken
Medewerkers die medeverantwoordelijk zijn voor ICT-zaken/automatisering, mannen, 50-plussers en hoogopgeleiden geven vaker aan dat de verantwoordelijkheid voor de veiligheid van internetgebruik in de thuissituatie mede bij de gebruiker zelf zou moet liggen. 50-plussers zien ook vaker (mede-) verantwoordelijkheid voor Internet providers, en hoogopgeleiden zien dit vaker voor leveranciers van hard- en software.

4.3 Houding en kennis in de zakelijke setting

Hieronder worden de belangrijkste resultaten weergegeven ten aanzien van houding en kennis in de zakelijke setting. Deze vragen zijn voorgelegd aan alle professionele doelgroepen.

Figuur B03: In hoeverre vindt u de volgende stellingen van toepassing op uw organisatie?



Overall beeld

Gemiddeld geeft een kleine meerderheid van de professionals aan dat de organisatie een beleid heeft voor alle werknemers omtrent de digitale werkomgeving. Een op de tien respondenten weet hier geen antwoord op te geven. Bij ruim een derde van de professionals worden nieuwe medewerkers ingewerkt in de maatregelen rondom veilig digitaal werken (bijna de helft geeft aan dat dit niet het geval is).

Vergelijking tussen doelgroepen

Ambtenaren Rijksoverheid geven vaker aan dat de organisatie een beleid heeft omtrent de digitale werkomgeving en dat nieuwe medewerkers worden ingewerkt in de maatregelen rondom veilig digitaal werken ten opzichte van ambtenaren exclusief Rijksoverheid.

Onder de bedrijfsgroepen lijkt de omvang van de organisatie van invloed te zijn op de (kennis van de) aanwezigheid van beleid rondom de digitale werkomgeving en het inwerken van nieuwe medewerkers in veilig digitaal werken; des te groter de organisatie, des te vaker dit van toepassing is.

Bekendheid en houding digitale veiligheid (op het werk)

Figuur B04: In hoeverre vindt u de volgende stellingen van toepassing op uzelf in uw werksituatie?

	Ambtenaren Rijk (n=301)	Ambtenaren excl. Rijk (n=301)	Klein MKB (n=400)	Groot MKB (n=401)	Grootbedrijf (n=401)
Ik weet bij wie ik een incident op het gebied van digitale veiligheid dien te melden					
Wel van toepassing	87%	78%	45%	77%	86%
Niet van toepassing	7%	13%	36%	17%	10%
Weet niet/geen antwoord	6%	9%	18%	5%	5%
Ik ben me voldoende bewust van het belang van digitale veiligheid					
Wel van toepassing	95%	92%	85%	87%	88%
Niet van toepassing	2%	2%	10%	8%	7%
Weet niet/geen antwoord	3%	5%	5%	4%	4%
Ik ben me voldoende bewust van de mogelijke gevaren op het gebied van digitale veiligheid die zich binnen onze organisatie kunnen voordoen					
Wel van toepassing	89%	80%	71%	76%	77%
Niet van toepassing	4%	8%	18%	14%	14%
Weet niet/geen antwoord	7%	12%	10%	10%	9%
Informatie over digitale veiligheid ervaar ik als helder en eenduidig					
Wel van toepassing	71%	58%	50%	62%	62%
Niet van toepassing	18%	22%	30%	22%	24%
Weet niet/geen antwoord	11%	20%	21%	16%	13%
Ik ben voldoende op de hoogte van mijn eigen verantwoordelijkheden rondom digitale veiligheid					
Wel van toepassing	92%	84%	83%	83%	86%
Niet van toepassing	5%	6%	10%	11%	9%
Weet niet/geen antwoord	3%	10%	7%	6%	5%
Ik ben voldoende op de hoogte van het beleid over digitale veiligheid					
Wel van toepassing	82%	61%	54%	64%	70%
Niet van toepassing	11%	20%	28%	23%	21%
Weet niet/geen antwoord	8%	18%	18%	13%	8%

Overall beeld

Een ruime meerderheid (ruim 8 op de 10) noemt zich voldoende bewust van het belang van digitale veiligheid in de werksituatie en zegt voldoende op de hoogte te zijn van de eigen verantwoordelijkheden. Ongeveer driekwart geeft aan voldoende bewust te zijn van de mogelijke gevaren voor de organisatie op het gebied van digitale veiligheid en geeft aan te weten bij wie ze een incident dienen te melden. Ongeveer een derde geeft aan *niet* goed op de hoogte te zijn van het beleid met betrekking tot digitale veiligheid en tevens de informatie over digitale veiligheid *niet* als helder en eenduidig te ervaren.

Vergelijking tussen doelgroepen

Ambtenaren Rijksoverheid geven vaker dan ambtenaren exclusief Rijksoverheid aan op de hoogte te zijn van het beleid over digitale veiligheid, de eigen verantwoordelijkheden rondom digitale veiligheid en bij wie een incident te melden. Ook zijn ambtenaren Rijksoverheid meer bewust van de mogelijke cybergevaren die zich kunnen voordoen binnen de organisatie.

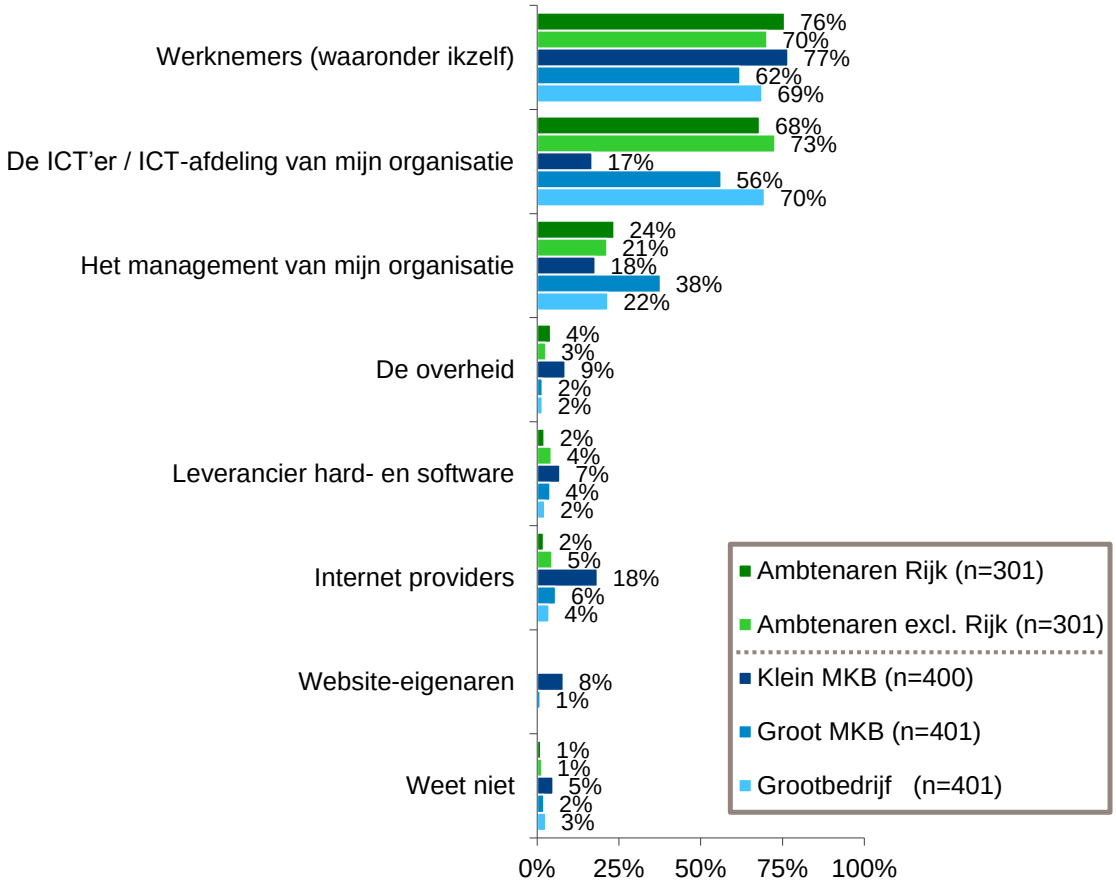
Tussen de bedrijfsdoelgroepen zijn slechts enkele verschillen zichtbaar. Medewerkers grootbedrijf geven vaker dan medewerkers klein- en groot-MKB aan te weten bij wie een incident te melden en voldoende op de hoogte te zijn van het beleid rondom digitale veiligheid.

Verschillen in achtergrondkenmerken

Vooral mannen, 50-plussers en degenen die medeverantwoordelijk zijn voor ICT-zaken/automatisering zijn zich bewust van het belang van digitale veiligheid in de werksituatie. Tevens geven mannen en 50-plussers vaker aan te weten bij wie een incident gemeld dient te worden.

Verantwoordelijk voor veiligheid internetgebruik (op het werk)

Figuur B05: Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid op het gebied van internetgebruik in uw werksituatie voornamelijk moet liggen?



Overall beeld

Qua veiligheid van internetgebruik in de werksituatie geven de meeste professionals aan zich hier voornamelijk zelf (als werknemers) voor verantwoordelijk te voelen. Ook de ICT-afdeling van de organisatie (door iets meer dan de helft van de professionals genoemd) en het management van de organisatie (door een kwart genoemd) wordt verantwoordelijkheid hiervoor toegedicht.

Vergelijking tussen doelgroepen

Tussen de twee ambtenarengroepen zijn nauwelijks verschillen zichtbaar; tussen de drie bedrijfsdoelgroepen zijn deze juist wel aanwezig. Medewerkers klein-MKB geven vaker dan medewerkers groot-MKB en grootbedrijf aan verantwoordelijkheid voor de veiligheid op het gebied van internetgebruik in de werksituatie te zien bij zichzelf, Internet providers, website-eigenaren en de overheid. Medewerkers groot-MKB en grootbedrijf leggen juist vaker verantwoordelijkheid bij de ICT-afdeling van de organisatie, terwijl medewerkers groot-MKB ook vaker verantwoordelijkheid leggen bij het management van de organisatie.

Verschillen in achtergrondkenmerken

Mannen, 50-plussers en hoogopgeleiden leggen vaker de verantwoordelijkheid voor de veiligheid op het gebied van internetgebruik in de werksituatie bij zichzelf. Jongeren (18-30 jaar) leggen vaker verantwoordelijkheid bij het management van de organisatie en de overheid.

5. Resultaten 2015: Risicoperceptie cybercrime

5.1 Beknopte samenvatting

Inschatting digitale veiligheid & zorgen
Binnen de professionele doelgroepen vinden vooral medewerkers bij de Rijksoverheid en medewerkers in het grootbedrijf dat hun organisatie aandacht heeft voor de digitale veiligheid. We zien dan ook dat deze groepen de digitale veiligheid van hun werksituatie over het algemeen hoger inschatten. Een algemene lijn is - nog steeds, want ook uit eerdere metingen bleek dit al - dat werknemers hun eigen digitale veiligheid hoger inschatten dan dat van hun collega's.

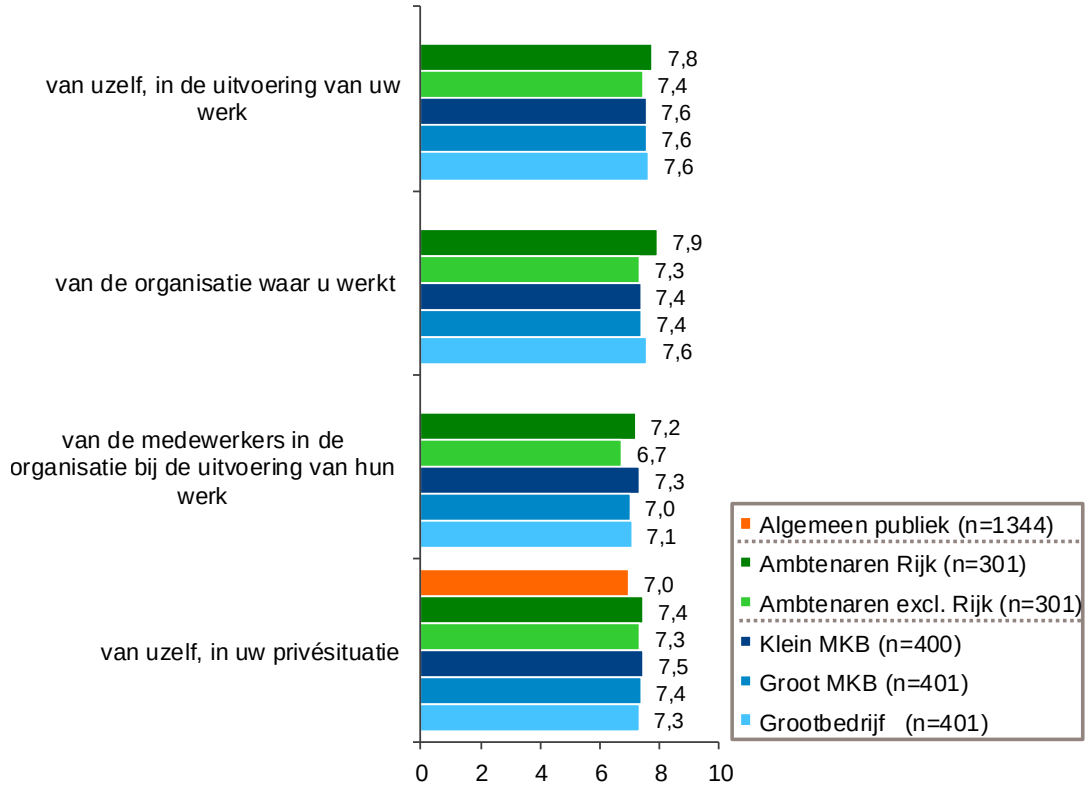
Wat verder opvalt is dat de professionele doelgroepen hun digitale veiligheid thuis hoger inschatten dan het algemeen publiek. Dat is des te opmerkelijker als gerealiseerd wordt dat binnen de doelgroep algemeen publiek ook veel mensen werkzaam zijn. Niet-werkende groepen (als studenten, werklozen, gepensioneerden) schatten hun digitale veiligheid thuis dus een stuk lager in, is de hoofdconclusie.
Professionele doelgroepen maken zich thuis over het algemeen wel meer zorgen over hun digitale veiligheid dan op het werk. Ook geeft nog altijd bijna de helft van de respondenten aan zich niet voldoende beschermd te voelen tegen de risico's van internet. Men voelt zich dus redelijk veilig, maakt zich wel enige zorgen en voelt zich vaak toch nog niet goed beschermd.

Kans op persoonlijk slachtofferschap
Evenals in 2014, is de helft van de respondenten in de veronderstelling dat kwaadwillenden toch wel slagen en dat je je daarom tegen grote gevaren niet kunt weren. Ruim een derde geeft bijvoorbeeld aan bang te zijn voor identiteitsfraude.
De inschatting dat men zelf slachtoffer wordt van bepaalde vormen van cybercrime, wordt het grootst geacht bij zaken zoals een product kopen dat vervolgens niet wordt geleverd, het zonder toestemming gebruiken of verspreiden van persoonlijke gegevens en pogingen om gegevens te ontfutselen. De kans op zaken zoals gefilmd worden, geld van de rekening halen of het gebruik van de creditcard door een ander worden door de meerderheid lager ingeschat. Tevens veronderstelt de helft phishing mails meteen te zullen herkennen bij ontvangst. De risicoperceptie is opmerkelijk vergelijkbaar tussen de doelgroepen.

Gevolgen van incidenten
De impact van de mogelijke gevolgen van ongewenste inbreuk op de digitale veiligheid in het algemeen - in zowel de privésituatie als de werksituatie - worden doorgaans als (zeer) ernstig ingeschat.
In de werksituatie gaat het bij ambtenaren vooral om zorgen over reputatieschade voor de werkgever, gevolgd door privacy-schade voor derden en voor de werkgever, bij bedrijven is financiële schade een belangrijkere zorg en speelt reputatieschade juist een minder grote rol.
In de privé-situatie richt de zorg zich sterker op financiële schade voor de persoon in kwestie en de gevolgen voor anderen in de omgeving. Klein-MKB maakt zich daar ook zorgen over de effecten op de uitvoering van hun zakelijke activiteiten.

5.2 Inschatting digitale veiligheid

Figuur C01: Op een schaal van 1 tot 10, hoe hoog schat u de digitale veiligheid in…



Overall beeld

De digitale veiligheid in de privésituatie wordt door de meerderheid van de respondenten ruim voldoende beoordeeld met een 7,2. Circa een op de tien respondenten schat de eigen digitale veiligheid in de privésituatie in als onvoldoende. De digitale veiligheid van professionals tijdens de uitvoering van hun werk wordt over het algemeen goed beoordeeld; het gemiddelde rapportcijfer wat hiervoor wordt gegeven is een 7,6. De helft van de professionals beoordeelt de digitale veiligheid van de organisatie met het cijfer 7,5. De digitale veiligheid van de medewerkers in de organisatie wordt als minst positief beoordeeld. Toch wordt hier gemiddeld nog altijd het cijfer 7,1 aan toegekend.

Vergelijking tussen doelgroepen

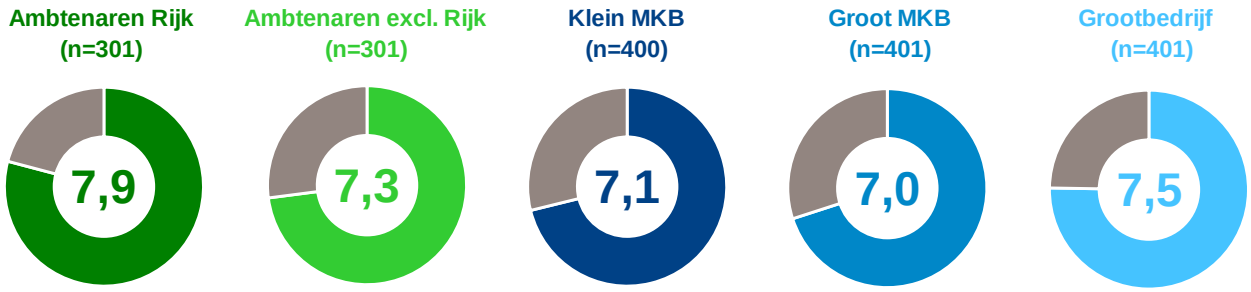
In de werksituatie geven ambtenaren Rijksoverheid op alle aspecten (digitale veiligheid van zichzelf, de organisatie, en medewerkers) gemiddeld hogere scores dan ambtenaren exclusief Rijksoverheid. In de privésituatie verschilt de veiligheidsbeleving voor die groepen niet.

Medewerkers grootbedrijf schatten de digitale veiligheid van de organisatie gemiddeld (iets) hoger in dan medewerkers in het klein en groot-MKB. De digitale veiligheid van de medewerkers in de organisatie wordt juist weer door medewerkers klein-MKB gemiddeld hoger ingeschat dan medewerkers groot-MKB en grootbedrijf.

Medewerkers klein-MKB geven gemiddeld een hoger rapportcijfer voor de eigen digitale veiligheid in de privésituatie ten opzichte van burgers (7,5 vs. 7,0). Het algemeen publiek geeft met een 7,0 de laagste score van alle doelgroepen voor de eigen digitale veiligheid in de privésituatie.

Verschillen in achtergrondkenmerken
Medewerkers die niet verantwoordelijk zijn voor ICT-zaken/automatisering schatten de digitale veiligheid van de organisatie gemiddeld hoger in dan medewerkers die hier (mede)verantwoordelijk voor zijn. Vrouwen, hoogopgeleiden, en jongeren (18-30 jaar) zijn iets kritischer over de digitale veiligheid van de organisatie en geven hiervoor een lager gemiddeld cijfer. In de privésituatie zijn het vooral mannen en laagopgeleiden die zichzelf digitaal veilig achten.

Figuur C02: Op een schaal van 1 tot 10, hoe beoordeelt u de mate waarin uw organisatie aandacht heeft voor digitale veiligheid?

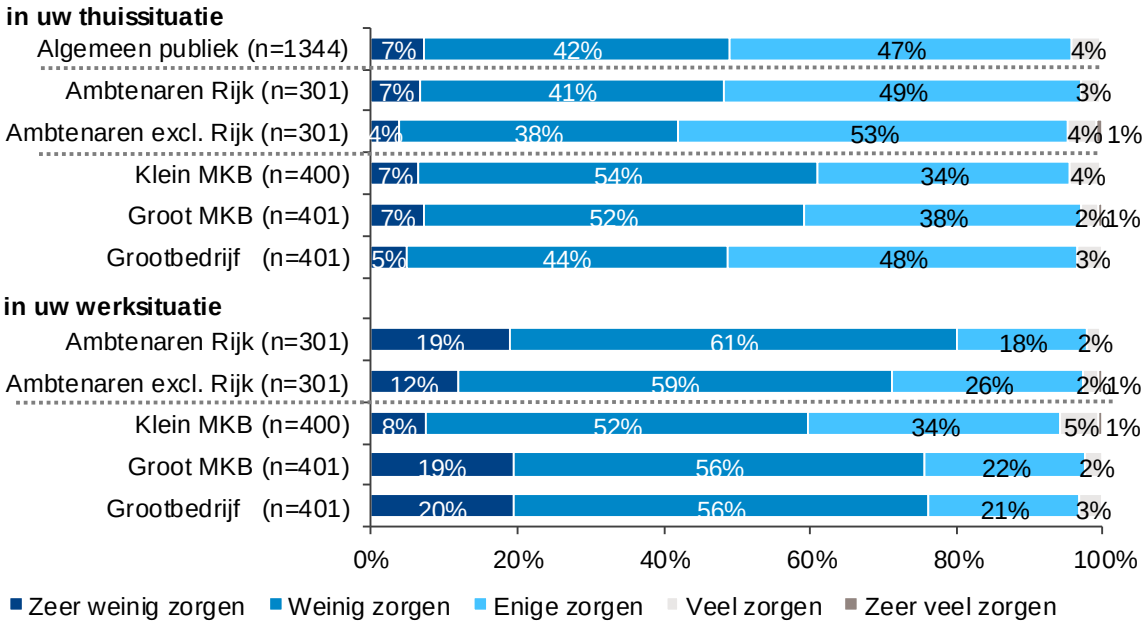


Overall beeld
De mate waarin de organisatie aandacht heeft voor digitale veiligheid wordt over het algemeen met een voldoende beoordeeld; gemiddeld scoort de organisatie hier een 7,4.

Vergelijking tussen doelgroepen
Volgens ambtenaren Rijksoverheid heeft de organisatie meer aandacht voor digitale veiligheid dan ambtenaren exclusief Rijksoverheid. In het bedrijfsleven is te zien dat medewerkers grootbedrijf de aandacht voor digitale veiligheid van de organisatie hoger beoordelen dan medewerkers in het klein- en groot-MKB.

Verschillen in achtergrondkenmerken
Vrouwen, jongeren (18-30 jaar) en hoogopgeleiden geven een lagere beoordeling voor de aandacht voor digitale veiligheid van de organisatie dan mannen, ouderen, en laag- en middelbaaropgeleiden. Ook medewerkers die eind- of medeverantwoordelijk zijn voor ICT-zaken/automatisering schatten de aandacht voor digitale veiligheid van de organisatie lager in dan medewerkers die niet verantwoordelijk zijn voor ICT-zaken/automatisering.

Figuur C03: In hoeverre maakt u zich zorgen over uw digitale veiligheid…?



Overall beeld

Ongeveer de helft van de respondenten maakt zich enige zorgen als het gaat over de eigen digitale veiligheid in de thuissituatie. Over de eigen digitale veiligheid in de werksituatie maakt men zich minder zorgen; bijna driekwart van de respondenten geeft aan zich (zeer) weinig zorgen te maken.

Vergelijking tussen doelgroepen

In de *thuissituatie* maken medewerkers grootbedrijf zich vaker enige zorgen over de eigen digitale veiligheid van de doelgroepen in het bedrijfsleven. In de werksituatie geldt dat medewerkers klein-MKB zich vaker enige zorgen maken over de eigen digitale veiligheid dan medewerkers groot-MKB en grootbedrijf.

In de werksituatie maken ambtenaren exclusief Rijksoverheid zich vaker enige zorgen over de eigen digitale veiligheid dan ambtenaren Rijksoverheid.

Bij medewerkers klein-MKB zijn de zorgen die men zich maakt in de thuissituatie en de werksituatie nagenoeg gelijk; dit kan te maken hebben met de dunne scheidslijn tussen werk en privé.

Verschillen in achtergrondkenmerken

In de thuissituatie maken 30-plussers zich vaker enige zorgen over de eigen digitale veiligheid dan de jongere leeftijdsgroepen. Ook maken hoogopgeleiden zich vaker enige zorgen over de eigen digitale veiligheid in de thuissituatie dan laagopgeleiden. Degenen die mede- of niet verantwoordelijk zijn voor ICT-zaken maken zich tevens vaker enige zorgen dan degenen die hier eindverantwoordelijk voor zijn.

In de werksituatie maken hoogopgeleiden zich vaker enige zorgen over de eigen digitale veiligheid dan laag- en middenopgeleiden. Degenen die eind- of medeverantwoordelijk zijn voor ICT-zaken maken zich vaker enige zorgen dan degenen die hier niet verantwoordelijk voor zijn.

Figuur B02: Stellingen risicoperceptie internet (percentage "zeer mee eens" + "mee eens")

	Algemeen publiek (n=1344)	Ambtenaren Rijk (n=301)	Ambtenaren excl. Rijk (n=301)	Klein MKB (n=400)	Groot MKB (n=401)	Grootbedrijf (n=401)
Bij online aankopen betaal ik het liefst met iDEAL	74%	72%	74%	75%	72%	72%
Ik heb vertrouwen in de veiligheid van internetbankieren	64%	70%	63%	67%	65%	69%
Ik zie geen gevaar bij het online aankopen van producten bij grote merken of bekende sites.	58%	59%	56%	57%	65%	64%
Als ik phishing mails zou ontvangen, zou ik deze meteen herkennen	56%	68%	57%	71%	65%	60%
Tegen grote gevaren op internet kun je je eigenlijk niet weren, kwaadwillenden slagen toch wel	52%	44%	52%	48%	52%	50%
Van iedereen zijn nu eenmaal veel gegevens bekend op internet, dat heb je zelf niet echt in de hand	46%	45%	43%	50%	48%	42%
Ik voel me voldoende beschermd tegen de risico's van internet.	43%	50%	45%	50%	49%	47%
Ik vertrouw erop dat internetbedrijven mijn gegevens niet zonder mijn toestemming aan derden verstrekken	38%	33%	30%	33%	36%	40%
Ik ben niet bang voor identiteitsfraude	22%	24%	22%	27%	28%	25%
Ik begrijp de zorgen over online betalen met een creditcard niet, als het mis gaat krijg je je geld toch wel terug.	17%	18%	15%	15%	20%	22%

Overall beeld

Minder dan de helft van de ondervraagden geeft aan zich voldoende beschermd te voelen tegen de risico's van internet, en circa de helft van de respondenten is in de veronderstelling dat kwaadwillenden toch wel slagen en dat je je daarom tegen grote gevaren niet kunt weren. Ongeveer de helft van de ondervraagden geeft aan vertrouwen te hebben in de veiligheid van internetbankieren, geen gevaar te zien bij online aankopen van producten bij grote merken of bekende sites en phishing mails meteen te herkennen bij ontvangst. Men is wel enigszins bang voor identiteitsfraude; slechts een kwart van de ondervraagden geeft aan hier *niet* bang voor te zijn.

Vergelijking tussen doelgroepen

Medewerkers groot-MKB en medewerkers grootbedrijf geven vaker aan geen gevaren te zien bij de online aankoop van producten bij grote merken of bekende sites ten opzichte van medewerkers klein-MKB. Medewerkers klein-MKB geven vaker aan meteen phishing mails te herkennen bij ontvangst ten opzichte van medewerkers grootbedrijf en burgers.

Wat blijkt uit de onderliggende cijfers is dat medewerkers klein-MKB zich vaker *on*voldoende beschermd voelen tegen de risico's van internet ten opzichte van medewerkers groot-MKB, medewerkers grootbedrijf en burgers.

Ambtenaren Rijksoverheid geven vaker aan meteen phishing mails te herkennen bij ontvangst ten opzichte van ambtenaren exclusief Rijksoverheid.

Verschillen in achtergrondkenmerken

Vooral 50-plussers en midden- en hoogopgeleiden betalen het liefst met iDEAL bij online aankopen (ter vergelijking: 50-plussers geven vaker aan de browser te gebruiken dan de app bij het bankieren via internet; tussen opleidingsgroepen zijn geen verschillen zichtbaar). Daarnaast voelen mannen, 30-plussers en hoogopgeleiden zich vaker goed beschermd tegen de risico's van internet dan vrouwen, jongeren (13-17 jaar) en laagopgeleiden.

Daarnaast geven medewerkers die (mede)verantwoordelijk zijn voor ICT-zaken vaker aan een phishingmail meteen te herkennen, alsmede mannen, hoogopgeleiden en 18–49 jarigen. Het zijn vooral de ouderen (50-plussers) die bang zijn voor identiteitsfraude.

Figuur C08: Hoe groot denkt u dat de kans is dat tegen uw zin het volgende op internet gebeurt? (de percentages van 'niet groot, niet klein' en 'weet niet/geen antwoord' zijn niet getoond).

	Algemeen publiek (n=1344)	Ambtenaren Rijk (n=301)	Ambtenaren excl. Rijk (n=301)	Klein MKB (n=400)	Groot MKB (n=401)	Grootbedrijf (n=401)
Er wordt zomaar geld van mijn rekening gehaald						
(Zeer) grote kans	11%	7%	11%	9%	9%	10%
(Zeer) kleine kans	52%	61%	49%	58%	59%	52%
Er wordt zomaar met mijn creditcard betaald door een ander						
(Zeer) grote kans	9%	13%	9%	8%	9%	10%
(Zeer) kleine kans	59%	59%	53%	59%	60%	52%
Er wordt iets gekocht uit mijn naam						
(Zeer) grote kans	16%	14%	14%	13%	11%	15%
(Zeer) kleine kans	43%	43%	40%	48%	46%	42%
Een product waarvoor ik betaald heb, wordt niet geleverd en de verkoper is niet meer te bereiken						
(Zeer) grote kans	23%	23%	22%	23%	22%	24%
(Zeer) kleine kans	38%	36%	33%	38%	43%	34%
Iemand doet alsof hij mij is						
(Zeer) grote kans	15%	15%	14%	14%	11%	14%
(Zeer) kleine kans	43%	43%	41%	44%	44%	44%
Persoonlijke gegevens die ik op internet heb gezet, worden zonder mijn toestemming door anderen gebruikt en verspreid						
(Zeer) grote kans	25%	30%	27%	27%	22%	23%
(Zeer) kleine kans	38%	37%	35%	40%	45%	35%
Anderen proberen persoonlijke gegevens van mij te ontfutselen						
(Zeer) grote kans	24%	29%	28%	26%	27%	29%
(Zeer) kleine kans	36%	32%	32%	38%	41%	34%
Ik word gefilmd via de webcam						
(Zeer) grote kans	7%	5%	6%	7%	6%	8%
(Zeer) kleine kans	69%	75%	67%	74%	77%	71%
Mijn computer wordt gebruikt om een misdaad te plegen (bijvoorbeeld door hackers)						
(Zeer) grote kans	8%	11%	8%	11%	9%	11%
(Zeer) kleine kans	48%	50%	44%	50%	52%	46%

Overall beeld

Als er wordt gekeken naar in hoeverre men inschat dat zij zelf risico lopen op bepaalde vormen van cybercrime, dan komt naar voren dat de meerderheid de kans *klein* acht dat ze gefilmd worden, dat er geld van hun rekening wordt gehaald of dat er met hun creditcard wordt betaald door een ander.

De kans dat men zelf te maken krijgt met andere voorvallen wordt hoger ingeschat; bijvoorbeeld dat men een product heeft gekocht en dit vervolgens niet wordt geleverd, dat persoonlijke gegevens zonder toestemming worden gebruikt of verspreid via internet en dat anderen proberen gegevens te ontfutselen (23% tot 26% schat dit risico als (zeer) groot in).

Vergelijking tussen doelgroepen

Over het algemeen achten medewerkers groot-MKB de kans op de voorgelegde incidenten groter dan medewerkers grootbedrijf.

De kans op de voorgelegde incidenten van medewerkers klein-MKB en burgers zijn nagenoeg gelijk; alleen de kans om gefilmd te worden via webcam en zomaar geld dat van de rekening af wordt gehaald wordt door medewerkers klein-MKB kleiner ingeschat dan burgers.

Verschillen in achtergrondkenmerken

Van veel van de voorgelegde incidenten schatten mannen de kans kleiner in dan vrouwen; bijvoorbeeld van iets kopen uit zijn naam, zomaar geld dat van de rekening wordt gehaald, iemand die doet alsof hij de respondent is, en het ontfutselen van persoonlijke gegevens.

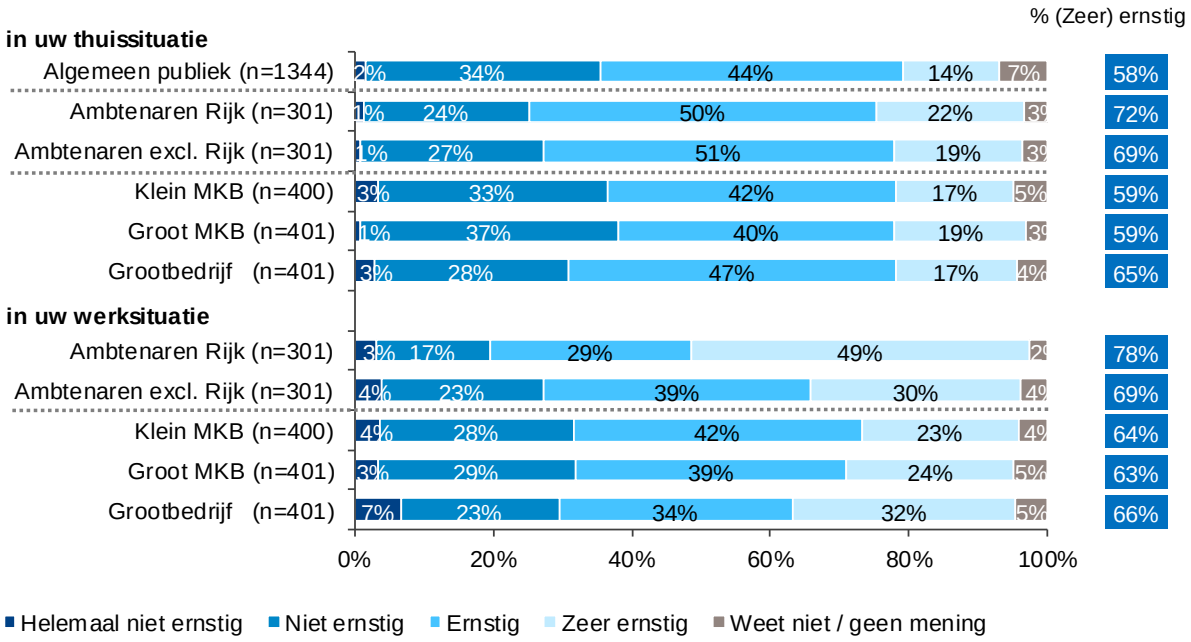
Van een aantal incidenten achten ook 50-plussers de kans kleiner in dan jongere leeftijdsgroepen. Zo achten zij bijvoorbeeld de kans op het gebruik of de verspreiding van hun persoonlijke gegevens en het niet leveren van een gekocht product kleiner in.

Jongeren (13–30 jaar) achten de kans dat de eigen computer wordt gebruikt om een misdaad te plegen (bijvoorbeeld door hackers) juist groter in dan 30-plussers.

5.3 Invloed en gevolgen van incidenten

Nu volgen de resultaten over de inschatting van de invloed en gevolgen van mogelijke incidenten op het gebied van digitale veiligheid.

Figuur C04: Hoe ernstig acht u de mogelijke gevolgen van ongewenste inbreuk op de digitale veiligheid?



Overall beeld

De mogelijke gevolgen van ongewenste inbreuk op de digitale veiligheid in het algemeen (in zowel de thuis- als de werksituatie) worden door het merendeel van de respondenten als (zeer) ernstig geacht.

Vooral in de werksituatie geldt dat in zeer sterke mate; de helft van de Rijksambtenaren schat de potentiële gevolgen van een inbreuk op de digitale veiligheid op het werk zelfs in als 'zeer ernstig'.

Vergelijking tussen doelgroepen
Medewerkers groot-MKB achten de mogelijke gevolgen van ongewenste inbreuk op de digitale veiligheid in de thuissituatie vaker in als (helemaal) niet ernstig dan medewerkers grootbedrijf.
In de werksituatie is enkel een verschil zichtbaar tussen de ambtenaren doelgroepen; ambtenaren Rijksoverheid achten de mogelijke gevolgen van ongewenste inbreuk op de digitale veiligheid vaker in als (zeer) ernstig in vergelijking met ambtenaren exclusief Rijksoverheid.

Verschillen in achtergrondkenmerken
In de thuissituatie zijn het vooral 50-plussers, hoogopgeleiden en werknemers die niet verantwoordelijk zijn voor ICT-zaken/automatisering die de mogelijke gevolgen van ongewenste inbreuk op de digitale veiligheid als (zeer) ernstig achten.
In de werksituatie achten hoogopgeleiden de mogelijke gevolgen van ongewenste inbreuk op de digitale veiligheid vaker als (zeer) ernstig dan de overige opleidingsgroepen.

Figuur C05: Hoeveel invloed zouden onderstaande zaken (voortkomend uit ongewenste inbreuk op uw digitale veiligheid) hebben op uw dagelijks leven? (weergave percentages "(heel) veel invloed")

	Algemeen publiek (n=1344)	Ambtenaren Rijk (n=301)	Ambtenaren excl. Rijk (n=301)	Klein MKB (n=400)	Groot MKB (n=401)	Grootbedrijf (n=401)
Gehackt worden in mijn thuissituatie waardoor mijn persoonlijke gegevens online veranderd worden	84%	92%	91%	87%	90%	90%
In mijn werksituatie geen toegang meer hebben tot al mijn bestanden		91%	90%	91%	80%	88%
Het niet werken van de interne IT-systemen van mijn werk		88%	86%	69%	80%	90%
Gehackt worden in mijn thuissituatie waardoor mijn gegevens en data gelekt worden	78%	86%	89%	79%	85%	84%
Een aantal dagen geen internetverbinding hebben in mijn werksituatie		84%	85%	85%	82%	84%
Gehackt worden in mijn werksituatie waardoor mijn gegevens en data gelekt		84%	81%	84%	73%	77%
In mijn thuissituatie geen toegang meer hebben tot al mijn bestanden	83%	81%	82%	82%	78%	85%
Een aantal dagen geen internetverbinding hebben in mijn thuissituatie	61%	61%	65%	72%	64%	66%

Overall beeld
Voor het merendeel van de respondenten zouden alle genoemde zaken voortkomend uit ongewenste inbreuk op digitale veiligheid (heel) veel invloed hebben op het dagelijks leven. Een aantal dagen thuis geen internetverbinding hebben zou het minst onoverkomelijk zijn; toch geeft nog ruim drie op de vijf respondenten aan dat dit (heel) veel invloed zou hebben op het dagelijks leven.

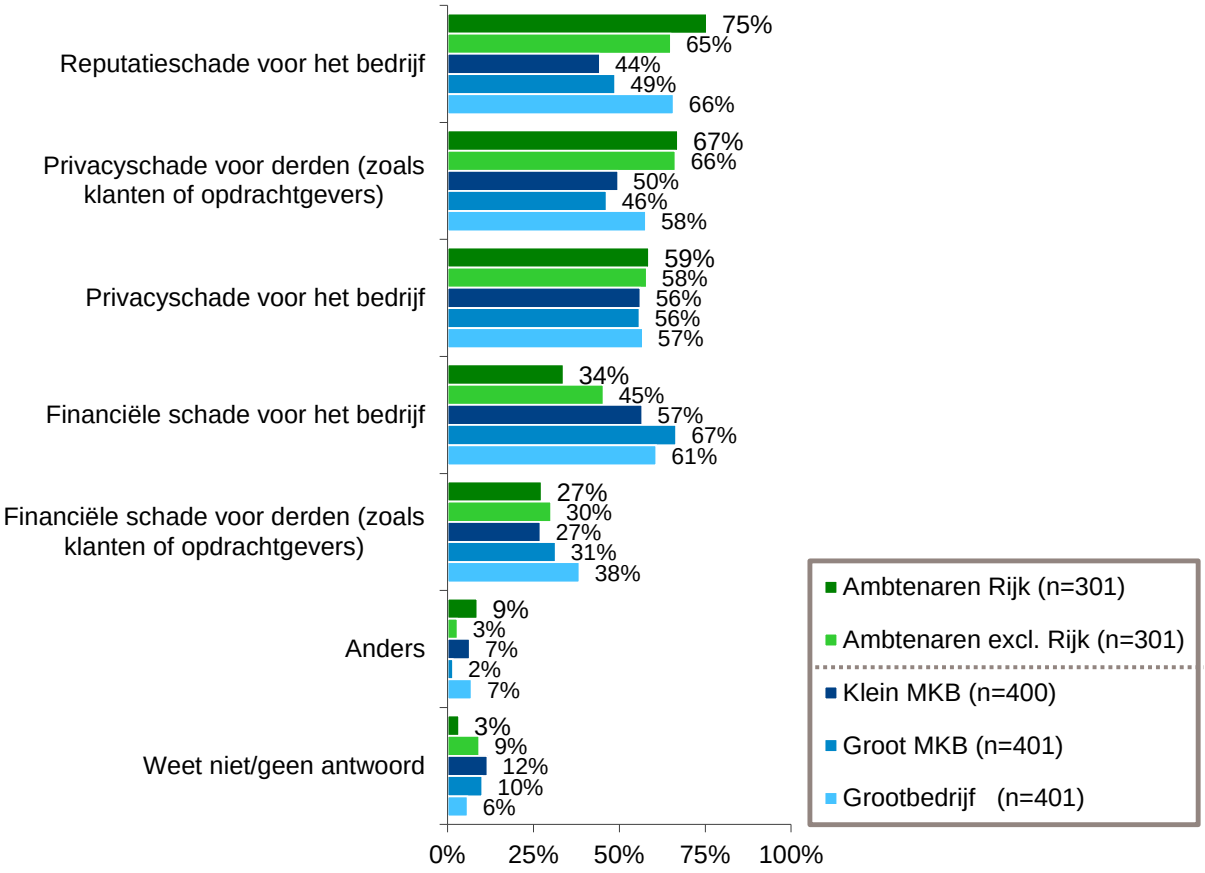
Vergelijking tussen doelgroepen
Tussen de twee ambtenarendoelgroepen zijn geen wezenlijke verschillen zichtbaar. Tussen de bedrijven-doelgroepen juist wel: medewerkers grootbedrijf schatten de impact van het niet-werken van interne IT-systemen van het werk hoog in, terwijl medewerkers klein-MKB vooral (heel) veel impact verwachten van gehackt worden in de werksituatie, waardoor gegevens en data gelekt worden.

Verschillen in achtergrondkenmerken

Over het algemeen achten vrouwen de invloed van de genoemde zaken voortkomend uit ongewenste inbreuk op digitale veiligheid groter dan mannen. Voor sommige (vooral werkgerelateerde) zaken achten hoogopgeleiden de invloed groter dan de overige opleidingsgroepen; bijvoorbeeld geen toegang hebben tot bestanden in zowel de werk- als thuissituatie, het niet-werken van interne IT-systemen van het werk, en een aantal dagen geen internetverbinding hebben in de werksituatie.

Daarnaast verwachten medewerkers die eindverantwoordelijk zijn voor ICT-zaken/automatisering vaak (heel) veel invloed van een aantal dagen geen internetverbinding hebben in de thuissituatie.

Figuur C06: Welke mogelijke gevolgen ziet u voor uw bedrijf of organisatie indien ongewenste inbreuk wordt gemaakt op de digitale veiligheid in uw werksituatie?



Overall beeld

Het meest genoemde mogelijke gevolg voor het bedrijf of organisatie van de respondent indien ongewenste inbreuk wordt gemaakt op de digitale veiligheid *in de werksituatie* is reputatieschade voor het bedrijf. Ook privacy-schade voor derden (zoals klanten en opdrachtgevers) en voor het bedrijf zelf worden veel genoemd, gevolgd door financiële schade.

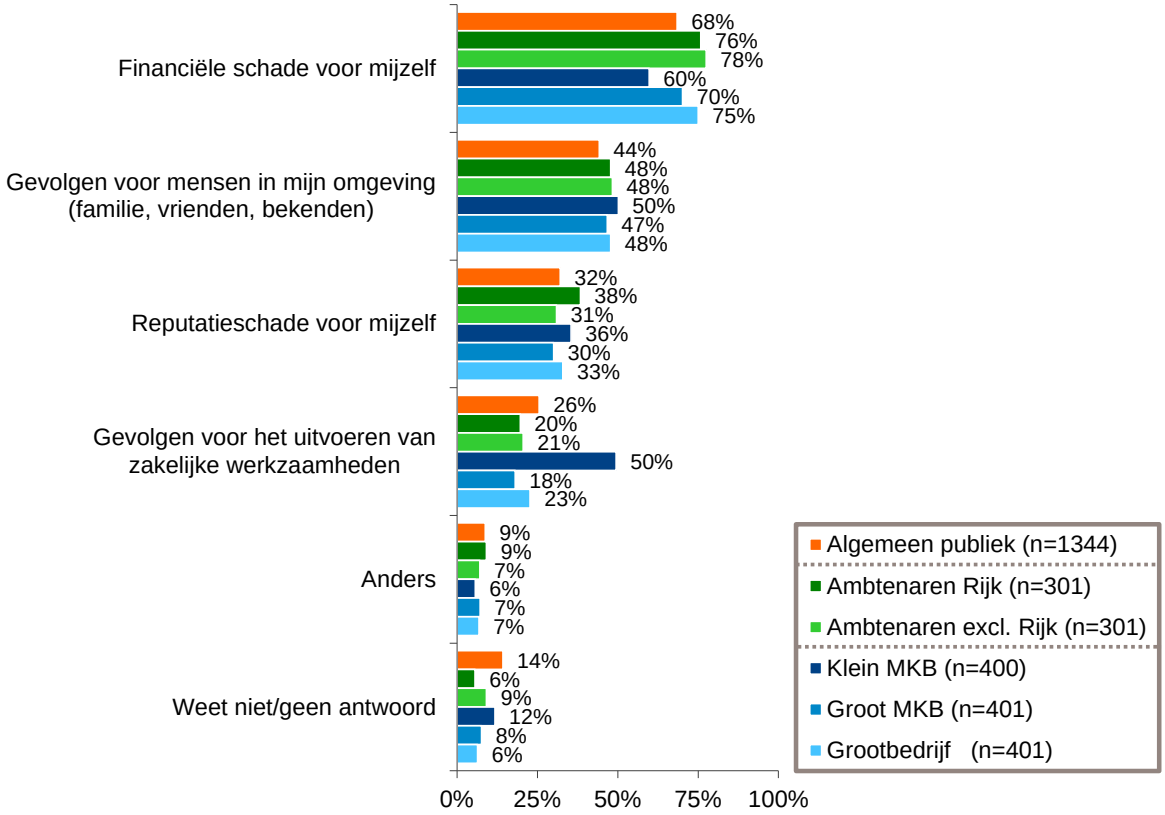
Vergelijking tussen doelgroepen

Reputatieschade voor het bedrijf wordt door ambtenaren Rijksoverheid, die de mogelijke gevolgen vaker als zeer ernstig inschatten, vaker genoemd dan door de ambtenaren exclusief Rijksoverheid, en vaker door medewerkers grootbedrijf dan andere bedrijfsleven doelgroepen. Ook financiële schade en privacy-schade voor derden worden vaker genoemd door medewerkers grootbedrijf dan overige bedrijfsleven doelgroepen.

Verschillen in achtergrondkenmerken

Vrouwen noemen vaker privacy-gerelateerde zaken, terwijl mannen vaker financieel-gerelateerde zaken noemen als mogelijke gevolgen voor de organisatie van ongewenste inbreuk op de digitale veiligheid. Daarnaast noemen hoogopgeleiden vaker reputatieschade voor het bedrijf en privacy-schade voor zowel het bedrijf als derden in vergelijking met de overige opleidingsgroepen.

Figuur C07: Welke mogelijke gevolgen ziet u voor uzelf indien er in uw thuissituatie ongewenste inbreuk wordt gemaakt op de digitale veiligheid?



Overall beeld

Het meest genoemde mogelijke gevolg voor de respondent zelf, indien ongewenste inbreuk wordt gemaakt op de digitale veiligheid *in de thuissituatie,* is financiële schade voor zichzelf. Ook ziet bijna de helft van de ondervraagden gevolgen voor mensen in de directe omgeving.

Vergelijking tussen doelgroepen

Medewerkers klein-MKB zien (veel) vaker gevolgen voor het uitvoeren van zakelijke werkzaamheden in het geval er in de thuissituatie ongewenst inbreuk op de digitale veiligheid wordt gedaan, in vergelijking met de overige bedrijfsleven doelgroepen en burgers. Logisch, want de scheidslijn tussen privé en werk zal in hun geval vaak minder strikt zijn. Echter zien medewerkers klein-MKB minder financiële schade voor henzelf als gevolg ten opzichte van overige bedrijfsleven doelgroepen.

Daarnaast zien medewerkers klein-MKB vaker gevolgen voor mensen in de omgeving dan burgers.

Verschillen in achtergrondkenmerken

Hoogopgeleiden zien vaker reputatieschade voor zichzelf, financiële schade voor zichzelf en gevolgen voor de mensen in de omgeving dan de overige opleidingsgroepen; laagopgeleiden geven vaker aan het niet te weten of geen antwoord te kunnen geven. 30-plussers geven vaker aan financiële schade voor zichzelf als mogelijk gevolg te zien ten opzichte van personen onder de dertig jaar.

6. Resultaten 2015: Preventiegedrag

6.1 Beknopte samenvatting

Ondernomen maatregelen
De *spontaan* meest genoemde beschermingsmaatregel tegen misbruik van de desktop computer of laptop in de privésituatie is de installatie van (goede) antivirussoftware, op ruime afstand gevolgd door het gebruik van een firewall. In de werksituatie gaat men er vaak vanuit dat de IT'er/IT-afdeling dergelijke maatregelen neemt, maar worden veilig wachtwoordgebruik en antivirussoftware wel genoemd, vooral door klein-MKB.

Gewenste gedragingen
Als we de mate van cybersecure gedrag willen verbeteren, dan is er met name nog winst te behalen op de volgende punten: het gebruik van WiFi-verbindingen (automatisch verbinding maken en het gebrek aan het gebruik van een VPN-app), het regelmatig maken van back-ups, het instellen een van twee-staps authenticatie (waar mogelijk) en wachtwoordgedrag.
Daarnaast is websitebezoek in mindere mate een aandachtspunt. Circa een derde controleert bij het bezoeken van websites niet of de juiste URL in de internetbrowser staat, of dat er een groen slotje aanwezig is bij websites waar gegevens ingevoerd moeten worden. Aangaande phishing mails wordt beduidend minder onveilig gedrag vertoond; de overgrote meerderheid zou verdachte mails direct verwijderen (ook van een bekende afzender) en niet op links klikken die men niet vertrouwt.

Preventiegedrag op het werk
Het merendeel van de professionals geeft aan zakelijke devices niet door anderen te laten gebruiken en bij gebruik van openbare WiFi-verbindingen bewuste keuzes te maken over welke handelingen men wel of niet verricht. Zaken waar minder veilig mee wordt omgegaan zijn: het gebruik van beveiligde VPN-verbindingen (via token), het, nemen van maatregelen bij gebruik van apparaten in een openbare ruimte (zoals een privacy screen) zodat anderen niet kunnen meekijken, en ten slotte: het laten controleren van een USB-stick op virussen als deze extern is geweest.

Wachtwoordgedrag in detail
De resultaten ten aanzien van wachtwoordgedrag zijn vergelijkbaar met de resultaten in 2014. Het wachtwoordgebruik is over het algemeen niet erg veilig en er wordt veelal reactief omgegaan met het wisselen van wachtwoorden.
Op verschillende vlakken wordt risicogedrag vertoond ten aanzien van wachtwoordgebruik. Een minderheid wijzigt de wachtwoorden 3-maandelijks en gebruikt wachtwoorden van meer dan 12 karakters. Daarnaast worden wachtwoorden genoteerd op briefjes die verstopt worden (22%), voor meerdere accounts gebruikt (42%) en over het algemeen pas na een melding gewijzigd (41%). Overigens leert 6 op de 10 de wachtwoorden uit het hoofd.

6.2 Ondernomen actie ter bescherming tegen misbruik

Nu volgen de resultaten ten aanzien van maatregelen die men neemt om zichzelf te beschermen tegen mogelijk digitaal misbruik.

Figuur D01: Wat doet u om uzelf te beschermen tegen misbruik van uw desktop computer of laptop via internet in uw thuissituatie (open vraag)?

	Algemeen publiek (n=1069)	Ambtenaren Rijk (n=271)	Ambtenaren excl. Rijk (n=284)	Klein MKB (n=344)	Groot MKB (n=370)	Grootbedrijf (n=376)
(Goede) beveiligingssoftware/antivirussoftware/virusscanner (Norton, McAfee, AVG, Kaspersky, etc.)	56%	66%	62%	53%	60%	64%
Firewall	22%	33%	35%	27%	25%	32%
Wachtwoorden (verschillende / moeilijk te raden / regelmatig veranderen / wachtwoordkluisje / wachtwoordgenerator)	11%	18%	15%	15%	11%	14%
Opletten / alert zijn / voorzichtig / zorgvuldig zijn (algemeen)	7%	5%	7%	5%	5%	6%
Beveiligen / beveiliging (algemeen)	5%	5%	5%	4%	4%	1%
Onbekende/verdachte/phishing mails niet openen / direct verwijderen	5%	7%	7%	5%	4%	5%
Malwarescanner / anti-malware programma	4%	5%	7%	4%	2%	6%
Geen onbekende websites bezoeken / links aanklikken	4%	3%	5%	3%	4%	3%
(Regelmatig/dagelijks) updaten van software	3%	4%	3%	2%	5%	4%
(Regelmatig/dagelijks) scannen van apparaat	3%	1%	1%	2%	1%	1%
Ik doe er niets aan	9%	7%	6%	14%	11%	10%
Weet niet / geen antwoord	12%	8%	11%	11%	7%	8%

Overall beeld

Het meest gegeven antwoord op de open vraag hoe men zichzelf *thuis* beschermt tegen misbruik van desktop computer of laptop via internet is het gebruik van (goede) beveiligingssoftware, antivirussoftware of virusscanners. Ook geeft een kwart van de respondenten aan zichzelf te beschermen met een firewall. Een op de 10 geeft aan niets te doen om zichzelf te beschermen tegen misbruik van de desktop computer of laptop via internet in de thuissituatie.

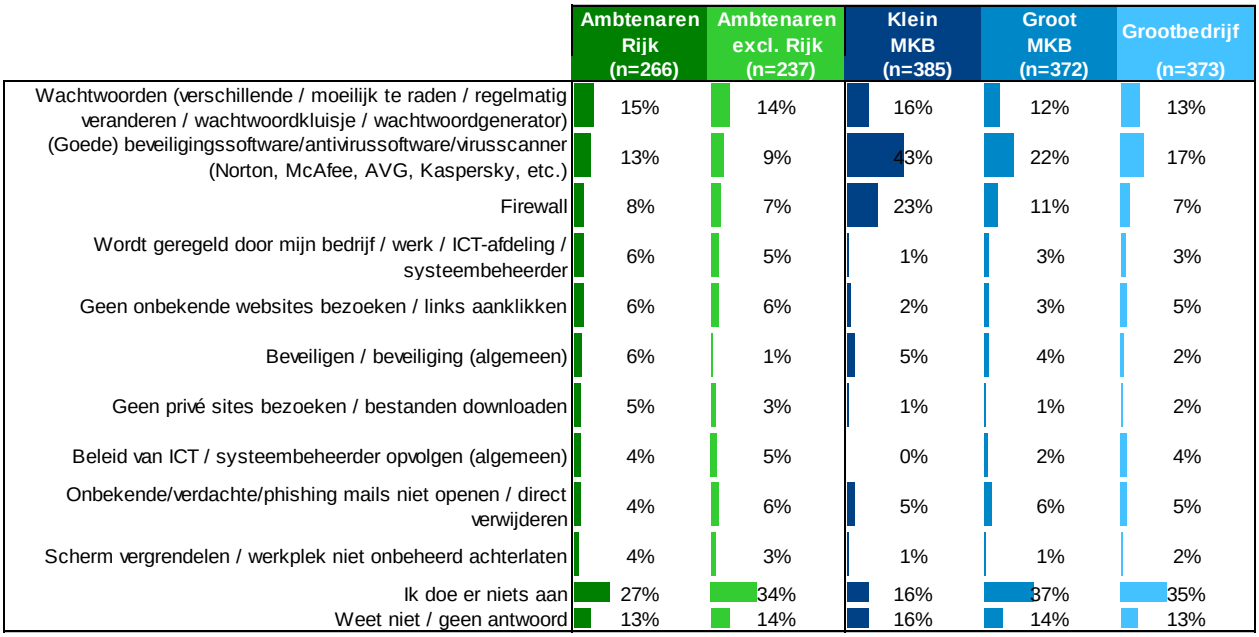
Vergelijking tussen doelgroepen

Medewerkers grootbedrijf geven vaker dan medewerkers klein-MKB spontaan aan zich te beschermen in de privésituatie door middel van (goede) antivirussoftware.

Verschillen in achtergrondkenmerken

Mannen geven vaker aan dan vrouwen dat ze zich beschermen in de privésituatie door middel van (goede) antivirussoftware, firewalls, malwarescanners en het regelmatig updaten van software. 30-plussers geven vaker spontaan dan jongeren onder de 30 jaar aan dat ze zich beschermen in de privésituatie door middel van (goede) antivirussoftware en firewalls. Hoger opgeleiden geven vaker dan laag- en middenopgeleiden aan dit te doen door middel van firewalls, verdachte of onbekende mails niet te openen dan wel te verwijderen, veilig om te gaan met wachtwoorden en regelmatig software te updaten.

Figuur D02: Wat doet u zelf om uzelf te beschermen tegen misbruik van uw desktop computer of laptop via internet in uw werksituatie (open vraag)?



Overall beeld

Het meest gegeven antwoord op de vraag hoe men zichzelf *op het werk* beschermt tegen misbruik van desktop computer of laptop via internet is middels (verschillende of moeilijke) wachtwoorden, (goede) beveiligingssoftware en antivirussoftware. Een aanzienlijk deel geeft aan zelf niets te doen; vermoedelijk omdat men ervan uitgaat dat dit door de IT'er/IT-afdeling van de organisatie wordt verzorgd.

Vergelijking tussen doelgroepen

Medewerkers klein-MKB geven vaker aan dan medewerkers groot-MKB en grootbedrijf dat ze zichzelf beschermen tegen misbruik in de werksituatie door middel van (goede) antivirussoftware en firewalls.

Verschillen in achtergrondkenmerken

Medewerkers die eindverantwoordelijk zijn voor ICT-zaken/automatisering geven vaker aan dan medewerkers die hier mede- of niet verantwoordelijk voor zijn dat ze zichzelf beschermen tegen misbruik in de werksituatie door middel van (goede) antivirussoftware, firewalls en beveiliging in het algemeen. Degenen die niet verantwoordelijk zijn voor ICT-zaken/automatisering geven vaker aan niets te doen (dan degenen die mede- of eindverantwoordelijk zijn). Mannen geven bij veel zaken aan dit vaker in te zetten dan vrouwen (bijvoorbeeld goede antivirussoftware, firewalls, geen onbekende sites bezoeken of links aanklikken). Ook hoogopgeleiden geven aan bepaalde zaken (firewalls, veilig wachtwoordgebruik) vaker in te zetten in de werksituatie dan laag- en middenopgeleiden.

Figuur D04: Kunt u voor de apparaten waar u thuis beschikking over heeft aangeven welke van de volgende uitspraken voor u gelden? (antwoordoptie 'niet op mij van toepassing/weet niet' is buiten beschouwing gelaten in de percentering)

	Algemeen publiek (n=1288)	Ambtenaren Rijk (n=294)	Ambtenaren excl. Rijk (n=289)	Klein MKB (n=386)	Groot MKB (n=389)	Grootbedrijf (n=383)
Ik heb een antivirusprogramma geïnstalleerd						
Ja	95%	96%	95%	91%	92%	91%
Nee	5%	4%	5%	9%	8%	9%
Ik laat mijn computer(s) maandelijks scannen op infecties						
Ja	77%	80%	72%	73%	73%	76%
Nee	23%	20%	28%	27%	27%	24%
Ik heb een firewall ingeschakeld						
Ja	91%	95%	93%	89%	91%	91%
Nee	9%	5%	7%	11%	9%	9%
Ik deïnstalleer software die ik niet gebruik						
Ja	74%	75%	70%	73%	78%	70%
Nee	26%	25%	30%	27%	22%	30%
Ik klik niet op ingekorte hyperlinks						
Ja	51%	51%	53%	48%	48%	48%
Nee	49%	49%	47%	52%	52%	52%
Ik verwijder spam direct en ongeopend						
Ja	94%	97%	96%	95%	95%	93%
Nee	6%	3%	4%	5%	5%	7%
Ik installeer apps alleen via de officiële applicatiewinkels en gebruik geen illegale kopieën						
Ja	91%	96%	93%	92%	92%	90%
Nee	9%	4%	7%	8%	8%	10%
Als ik een USB-stick vind, stop ik hem in mijn computer om te kijken wat er op staat.						
Ja	18%	14%	17%	10%	25%	17%
Nee	82%	86%	83%	90%	75%	83%
Mijn smartphone is vergrendeld met een code of wachtwoord.						
Ja	80%	88%	90%	83%	79%	84%
Nee	20%	12%	10%	17%	21%	16%
Ik heb met mijn kind(eren) afspraken gemaakt over het omgaan met digitale veiligheid tijdens het internetten						
Ja	73%	74%	66%	79%	73%	67%
Nee	27%	26%	34%	21%	27%	33%

Overall beeld

Gemiddeld geeft ruim 9 op de 10 respondenten aan een antivirussoftware te hebben geïnstalleerd op apparaten waar men thuis de beschikking over heeft. Ook spam wordt door de overgrote meerderheid direct en ongeopend verwijderd. Een kleiner deel (50%) geeft aan niet op ingekorte hyperlinks te klikken en een kwart (26%) de-installeert geen software die niet wordt gebruikt.

Vergelijking tussen doelgroepen

Ambtenaren Rijksoverheid geven vaker aan dan ambtenaren exclusief Rijksoverheid dat apparaten maandelijks worden gescand op infecties. Medewerkers groot-MKB geven vaker aan dan medewerkers klein-MKB en grootbedrijf dat ze een gevonden USB-stick in de computer zouden stoppen om te kijken wat er op staat.

Verschillen in achtergrondkenmerken

Op een aantal aspecten zijn het vooral mannen, 50-plussers en laag- en middenopgeleiden die veiliger gedrag vertonen (bijv. ten aanzien van het niet-klikken op hyperlinks, het scannen van apparaten op infecties, het inschakelen van firewalls). Hoogopgeleiden en vrouwen zijn daarentegen veiliger in het gebruik van apps en installeren deze vaker alleen via de officiële applicatiewinkels.

Figuur D07: Kunt u aangeven in hoeverre onderstaande stellingen voor u gelden in uw thuissituatie? (antwoordoptie 'niet op mij van toepassing/weet niet' is buiten beschouwing gelaten in de percentering)

	Algemeen publiek (n=1169)	Ambtenaren Rijk (n=273)	Ambtenaren excl. Rijk (n=273)	Klein MKB (n=362)	Groot MKB (n=376)	Grootbedrijf (n=373)
Ik maak doorgaans back-ups als systemen daarom vragen						
Ja	52%	60%	66%	65%	58%	65%
Nee	48%	40%	34%	35%	42%	35%
Ik maak doorgaans zelf back-ups zonder dat systemen daarom vragen						
Ja	46%	55%	41%	65%	50%	52%
Nee	54%	45%	59%	35%	50%	48%
Ik vergrendel mijn privé-apparaten met een beveiligingscode of een wachtwoord						
Ja	76%	81%	76%	75%	74%	78%
Nee	24%	19%	24%	25%	26%	22%
Wanneer ik gebruik maak van een openbare WiFi-verbinding, maak ik bewuste keuzes welke handelingen ik wel en welke ik niet verricht op mijn privé-apparaten						
Ja	79%	85%	75%	78%	78%	77%
Nee	21%	15%	25%	22%	22%	23%

Overall beeld

Op het gebied van het maken van back-ups in de thuissituatie valt nog terrein te winnen; de helft van de ondervraagden maakt doorgaans back-ups *zonder* dat systemen daarom vragen. Ruim driekwart van de respondenten vergrendelt de privé-apparaten met een beveiligingscode of een wachtwoord en maakt bewuste keuzes over handelingen die verricht worden op openbare WiFi-verbindingen.

Vergelijking tussen doelgroepen

Medewerkers klein-MKB zijn pro-actiever in het maken van back-ups in de thuissituatie en doen dit vaker zonder dat systemen daarom vragen ten opzichte van alle andere doelgroepen.

Ambtenaren Rijksoverheid maken vaker proactief back-ups in de thuissituatie en maken vaker bewuste keuzes over handelingen die verricht worden op openbare WiFi-verbindingen dan Ambtenaren exclusief Rijksoverheid.

Verschillen in achtergrondkenmerken

Vooral tussen leeftijdsgroepen zijn duidelijke verschillen; 50-plussers vertonen over het algemeen veiliger gedrag dan de overige leeftijdsgroepen. Ten aanzien van back-ups zien we ook dat vooral hoogopgeleiden hier vaker veilig gedrag vertonen dan laag- en middenopgeleiden. Tevens zijn mannen pro-actiever dan vrouwen in het maken van back-ups en doen dit vaker zonder dat systemen daarom vragen, terwijl vrouwen vaker aangeven dan mannen dat privé-apparaten vergrendeld zijn.

6.3 Gewenste gedragingen (mate van cybersecure gedrag)

Hieronder worden de resultaten getoond van de gewenste gedragingen (zoals opgesteld door de NCTV). Deze vragen zijn aan alle doelgroepen voorgelegd en deze zijn gebruikt voor het berekenen van de indexscore voor de mate van cybersecure gedrag.

De percentages in de tabel geven het aandeel respondenten aan die zich **veilig** gedragen met betrekking tot het betreffende aspect. Hoe hoger, hoe beter. Lage percentages duiden er dus op, dat er qua digitaal veilig gedrag op dat punt nog een flinke verbetering mogelijk is.

Figuur D03 (deel 1): Kunt u aangeven welke van de volgende uitspraken voor u gelden? (weergave percentages "veilig"- de respondenten die 'niet op mij van toepassing/weet niet' hebben geantwoord zijn buiten beschouwing gelaten in de percentering)

De weergegeven percentages zijn '% veilig gedrag'	Algemeen publiek	Ambtenaren Rijk	Ambtenaren excl. Rijk	Klein MKB	Groot MKB	Grootbedrijf
WiFi-het gebruik van draadloos internetten	(n=1163)	(n=277)	(n=272)	(n=366)	(n=381)	(n=365)
Ik maak doorgaans gebruik van het automatisch verbinding maken met vertrouwde WiFi-netwerken	19%	19%	15%	20%	17%	17%
Ik maak doorgaans gebruik van een Virtual Private Network (VPN)-app om verbinding te maken met WiFi-netwerken buitenshuis, waarmee mijn internetverkeer versleuteld wordt verstuurd	22%	26%	25%	20%	26%	33%
Als ik buitenshuis gebruik maak van WiFi-netwerken, maak ik doorgaans alleen verbinding met vertrouwde netwerken, waar je op moet inloggen	70%	71%	72%	74%	70%	72%
Ik heb een wachtwoord ingesteld op mijn WiFi-netwerk thuis dat bestaat uit minimaal 12 karakters	77%	77%	73%	74%	74%	75%
Back-ups	(n=1256)	(n=293)	(n=285)	(n=391)	(n=384)	(n=377)
Ik maak doorgaans minstens elke 4 weken een back-up van mijn bestanden op een externe harde schijf	36%	34%	35%	56%	37%	38%
Herkennen van phishingmails om o.a. cryptoware- en ransomwarebesmetting te voorkomen	(n=1308)	(n=295)	(n=293)	(n=397)	(n=391)	(n=391)
Ik verwijder doorgaans e-mails die ik niet vertrouw zonder deze te openen, ook als deze van een bekende afzender komen	90%	94%	92%	90%	89%	92%
Ik vermijd doorgaans op links te klikken die ik niet vertrouw	96%	98%	97%	99%	96%	96%
Wachtwoorden	(n=1241)	(n=287)	(n=282)	(n=379)	(n=385)	(n=372)
Ik verander mijn wachtwoorden doorgaans elke drie maanden	22%	27%	18%	24%	20%	24%
Mijn wachtwoorden bestaan doorgaans uit meer dan 12 karakters	31%	28%	23%	28%	30%	28%
Mijn wachtwoorden bevatten doorgaans minimaal 1 hoofdletter, 1 kleine letter en 1 speciaal teken	81%	82%	81%	80%	79%	83%
Mijn wachtwoorden bestaan doorgaans uit tussen de 8 en 12 karakters	82%	87%	82%	81%	84%	83%
Ik zet mijn wachtwoorden niet in een document op mijn computer en/of laptop	86%	81%	82%	82%	87%	84%
Twee-factor-authenticatie	(n=1032)	(n=261)	(n=249)	(n=329)	(n=346)	(n=337)
Waar het mogelijk is om een twee-staps-verificatie in te stellen, doe ik dit ook	49%	53%	54%	50%	52%	55%
Websites bezoeken	(n=1211)	(n=294)	(n=282)	(n=380)	(n=383)	(n=373)
Bij het bezoeken van websites controleer ik doorgaans of de juiste URL in mijn internetbrowser staat om vast te stellen of ik de juiste site bezoek	64%	68%	65%	64%	64%	62%
Bij het bezoeken van websites waar ik gegevens moet invoeren, controleer ik doorgaans eerst of er een groen slotje aanwezig is in mijn browser	69%	71%	72%	72%	74%	67%
Bij het bezoeken van websites waar ik gegevens moet invoeren, voer ik doorgaans alleen verplichte velden in en geen niet-verplichte velden	93%	95%	92%	95%	91%	91%

Overall beeld

Ten aanzien van WiFi-gebruik vertoont een ruime meerderheid onveilig gedrag ten aanzien van het automatisch verbinding maken met vertrouwde WiFi-netwerken en het gebrek aan gebruik van een VPN-app om verbinding te maken met WiFi-netwerken buitenshuis om internetverkeer versleuteld te versturen. Ruim de helft (61%) vertoont onveilig gedrag als het gaat om het maken van back-ups van bestanden minstens elke 4 weken en ook het instellen van een twee-staps authenticatie waar mogelijk wordt door de helft niet gedaan. Aangaande phishing mails wordt beduidend minder onveilig gedrag vertoond. Wat betreft wachtwoorden wordt vooral onveilig gedrag vertoond als het gaat om het 3-maandelijks wijzigen van wachtwoorden en wachtwoorden van meer dan 12 karakters gebruiken. Circa een derde controleert bij het bezoeken van websites niet of de juiste URL in de internetbrowser staat, of dat er een groen slotje aanwezig is bij websites waar gegevens ingevoerd moeten worden.

Vergelijking tussen doelgroepen

Medewerkers klein-MKB laten vaker *onveilig* gedrag zien als het gaat om het gebruik van een VPN-app om verbinding te maken met WiFi-netwerken buitenshuis om internetverkeer versleuteld te versturen in vergelijking met medewerkers grootbedrijf. Echter laten medewerkers klein-MKB vaker *veilig* gedrag zien ten opzichte van medewerkers groot-MKB en grootbedrijf met betrekking tot een aantal andere zaken (zoals het maken van back-ups minstens elke 4 weken, het niet-klikken op links die men niet vertrouwt en het invoeren van alleen verplichte velden bij websites waar gegevens ingevoerd moeten worden).

Verschillen in achtergrondkenmerken

Ten aanzien van WiFi-gebruik maken vooral hoogopgeleiden automatisch verbinding met vertrouwde WiFi-netwerken (onveilig gedrag), terwijl 50-plussers hier veiliger mee omgaan dan 18-49 jarigen. Vooral vrouwen maken geen gebruik van een VPN-app om verbinding te maken met WiFi-netwerken buitenshuis om internetverkeer versleuteld te versturen. Onveilig gedrag aangaande het maken van back-ups minstens elke 4 weken wordt vooral vertoond door laagopgeleiden, 18-30 jarigen, en werknemers die niet verantwoordelijk zijn voor ICT-zaken/automatisering. Bij het herkennen van phishing mails zijn het vooral jongeren (13-17 jaar) en laagopgeleiden die onveilig gedrag vertonen. Met betrekking tot wachtwoordgedrag zijn het juist de hoogopgeleiden die meer onveilig gedrag vertonen.

Figuur D03 (deel 2): Kunt u aangeven welk van de volgende uitspraken voor u gelden? (weergave percentages "veilig" - de respondenten die 'niet op mij van toepassing/weet niet' hebben geantwoord zijn buiten beschouwing gelaten in de percentering)

De weergegeven percentages zijn '% veilig gedrag'	Algemeen publiek	Ambtenaren Rijk	Ambtenaren excl. Rijk	Klein MKB	Groot MKB	Grootbedrijf
Veilig online winkelen	(n=1163)	(n=289)	(n=283)	(n=376)	(n=381)	(n=378)
Als ik online aankopen doe, controleer ik doorgaans of de webwinkel aangesloten is bij keurmerken	66%	71%	69%	68%	68%	70%
Als ik mijn betaling doe tijdens een online aankoop, controleer ik doorgaans of ik via een beveiligde internetverbinding betaal	79%	83%	85%	83%	79%	80%
Als ik online aankopen wil doen en de website niet helemaal vertrouw, verlaat ik doorgaans de website of ga ik op nader onderzoek uit	94%	95%	95%	94%	96%	93%
Software-updates	(n=1236)	(n=288)	(n=282)	(n=381)	(n=387)	(n=381)
Ik installeer doorgaans direct software-updates als mijn computer/laptop/tablet dit adviseert	67%	73%	76%	68%	70%	64%
Ik maak zoveel mogelijk gebruik van automatische software-updates	71%	75%	76%	71%	74%	71%
Bring your own device	(n=0)	(n=208)	(n=203)	(n=173)	(n=238)	(n=284)
Als ik mijn privé-apparaten ook voor het werk gebruik, zorg ik er doorgaans voor dat anderen die ook gebruikmaken van deze apparaten, een ander account gebruiken	-	66%	58%	61%	51%	58%
Ik houd me doorgaans aan de afspraken die er zijn vanuit mijn werk voor het gebruik van privé-apparaten op het werk	-	93%	92%	84%	84%	90%
Gebruik smartphone	(n=1113)	(n=270)	(n=269)	(n=348)	(n=369)	(n=361)
Ik kan op afstand apparaten lokaliseren, blokkeren en inhoud wissen	34%	50%	43%	44%	45%	40%
Ik geef apps doorgaans toegang tot gegevens waar ze om vragen	66%	64%	63%	65%	65%	68%
Ik heb locatiegegevens voor apps doorgaans aanstaan	73%	61%	66%	70%	67%	68%
Ik download apps doorgaans alleen uit de App Store / Google Play Store	90%	95%	97%	95%	93%	92%
Andere apparaten verbonden met internet	(n=1136)	(n=274)	(n=264)	(n=348)	(n=372)	(n=365)
Ik zorg dat alle apparaten in huis die met internet verbonden zijn een veilig wachtwoord hebben	61%	56%	52%	56%	58%	57%

Overall beeld

Circa een derde controleert niet of webwinkels aangesloten zijn bij keurmerken. Gedrag ten aanzien van software-updates is over het algemeen redelijk veilig (twee derde van de respondenten vertoont veilig gedrag). Bij het gebruik van de smartphone is het op afstand apparaten kunnen lokaliseren, blokkeren en inhoud wissen de gedraging waar het meest onveilig gedrag wordt vertoond (hoewel alsnog 40% hier veilig gedrag op vertoont). Ruim een derde geeft apps toegang tot de gegevens waar ze om vragen. Apparaten in huis die verbonden zijn met het internet zijn door 4 op de 10 respondenten niet voorzien van een veilig wachtwoord. Tevens vertonen 4 op de 10 professionals onveilig gedrag bij het gebruik van privé-apparaten die ook voor het werk worden gebruikt.

Vergelijking tussen doelgroepen

Ambtenaren exclusief Rijksoverheid zijn veiliger dan ambtenaren Rijksoverheid als het gaat om het direct installeren van software-updates wanneer dit geadviseerd wordt.

Verschillen in achtergrondkenmerken

Bij een aantal zaken vertonen mannen en 50-plussers veiliger gedrag dan vrouwen en jongere leeftijdsgroepen (ten aanzien van opleiding zijn veel minder verschillen). Bijvoorbeeld op het gebied van het direct installeren van software-updates wanneer dit geadviseerd wordt en het controleren van een beveiligde internetverbinding bij online betalingen.

Vrouwen en 18-30 jarigen gebruiken vaker de app dan de browser bij betaaltransacties via internet (bijv. bij online winkelen) dan mannen en de overige leeftijdsgroepen.

6.4 Preventiegedrag op het werk

Nu volgen de resultaten ten aanzien van preventiegedrag *op het werk en gerelateerd aan zakelijke devices*. Deze vragen zijn voorgelegd aan alle zakelijke doelgroepen.

Figuur D06: Kunt u aangeven of de volgende stellingen voor u gelden?

	Ambtenaren Rijk (n=215)	Ambtenaren excl. Rijk (n=222)	Klein MKB (n=305)	Groot MKB (n=257)	Grootbedrijf (n=262)
Ik laat mijn zakelijke tablet en/of smartphone niet door anderen gebruiken					
Ja	86%	84%	79%	78%	80%
Nee	14%	16%	21%	22%	20%
Ik laat mijn zakelijke desktop computer en/of laptop niet door anderen gebruiken					
Ja	84%	74%	76%	63%	72%
Nee	16%	26%	24%	37%	28%
Wanneer ik gebruik maak van een openbare WiFi-verbinding (bijv. in de trein, een café, etc.), maak ik bewuste keuzes welke handelingen ik wel en welke ik niet verricht op mijn zakelijke apparaten (laptop, tablet, smartphone)					
Ja	87%	80%	80%	72%	71%
Nee	13%	20%	20%	28%	29%
Ik maak voor mijn werk gebruik van een token om veilig te VPN'en					
Ja	62%	66%	17%	38%	52%
Nee	38%	34%	83%	62%	48%
Een USB-stick die buiten de organisatie is geweest, laat ik eerst door de systeembeheerder controleren op virussen					
Ja	50%	22%	31%	26%	26%
Nee	50%	78%	69%	74%	74%
Ik neem maatregelen zodat anderen niet mee kunnen kijken als ik mijn zakelijke laptop, smartphone en/of tablet gebruik in een openbare ruimte zoals een trein of café					
Ja	51%	42%	33%	37%	43%
Nee	49%	58%	67%	63%	57%
Ik vergrendel mijn zakelijke apparaten met een beveiligingscode					
Ja	95%	86%	74%	82%	85%
Nee	5%	14%	26%	18%	15%
Ik vergrendel mijn zakelijke computer of laptop als ik mijn werkplek verlaat					
Ja	89%	80%	68%	64%	82%
Nee	11%	20%	32%	36%	18%

Overall beeld

Gemiddeld geeft circa drie kwart van de professionals aan zakelijke devices niet door anderen te laten gebruiken en bij gebruik van openbare WiFi-verbindingen bewuste keuzes te maken over welke handelingen men wel of niet verricht. Zaken waar minder veilig mee wordt omgegaan zijn: het gebruik van beveiligde VPN-verbindingen (via token), bij gebruik van apparaten in een openbare ruimte

maatregelen te nemen (zoals een privacy screen) zodat anderen niet kunnen meekijken, en het laten controleren van een USB-stick op virussen als deze extern is geweest.

Vergelijking tussen doelgroepen

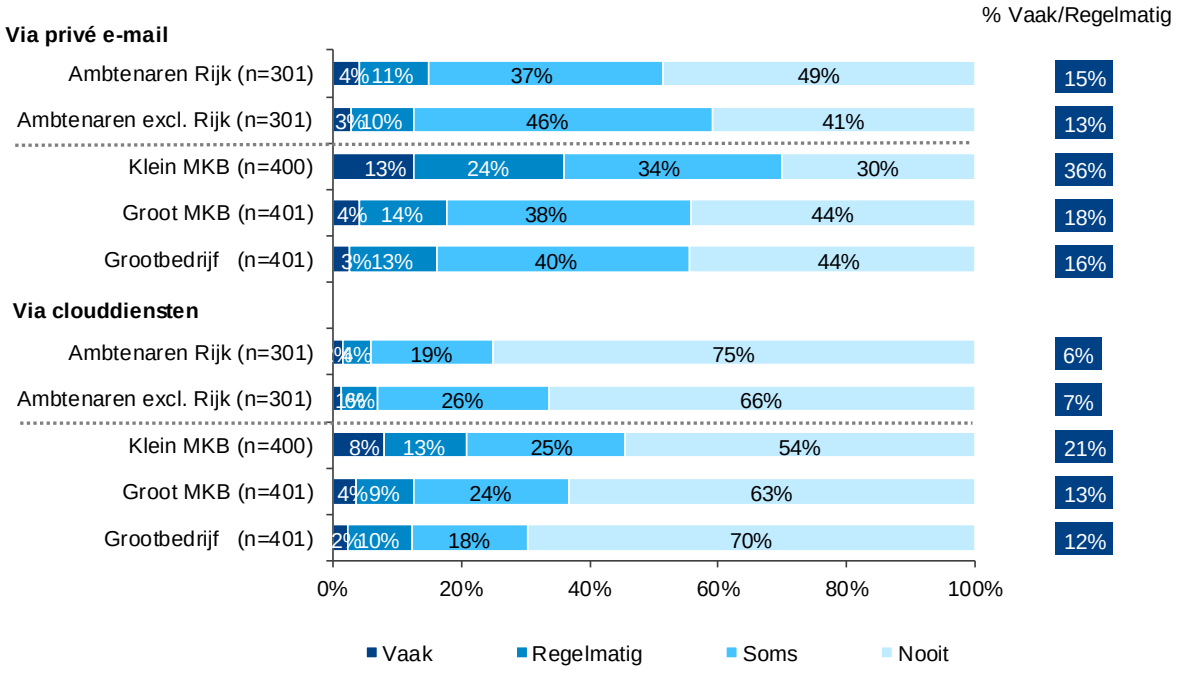
Ambtenaren Rijksoverheid laten op een aantal zaken veiliger gedrag zien dan ambtenaren exclusief Rijksoverheid. Bijvoorbeeld op het gebied van: zakelijke desktops en/of laptops *niet* door anderen gebruiken, USB-sticks die buiten de organisatie zijn geweest laten controleren op virussen, het vergrendelen van zakelijke apparaten met een beveiligingscode en het vergrendelen van zakelijke desktop computers/laptops als men de werkplek verlaat.

Medewerkers grootbedrijf vertonen op sommige vlakken veiliger gedrag dan medewerkers klein- en groot-MKB; ze maken vaker gebruik van een beveiligde VPN-verbinding (via token) en vergrendelen vaker zakelijke desktop computers/laptops als de werkplek wordt verlaten.

Verschillen in achtergrondkenmerken

50-plussers laten vaker dan de overige leeftijdsgroepen USB-sticks die buiten de organisatie zijn geweest controleren op virussen (ook laagopgeleiden doen dit vaker dan de andere opleidingsgroepen) en nemen vaker maatregelen zodat anderen niet mee kunnen kijken op devices in openbare ruimtes.

Figuur D05: Hoe vaak deelt u ten behoeve van uw werk documenten en bestanden via uw privé e-mail of via clouddiensten?



Overall beeld

Eén op de vijf professionals geeft aan regelmatig/vaak documenten en bestanden van het werk te delen via privé e-mail. Documenten en bestanden van het werk worden minder gedeeld via clouddiensten; één op de tien professionals geeft aan dit regelmatig/vaak te doen.

Vergelijking tussen doelgroepen

Ambtenaren Rijksoverheid geven vaker aan nooit documenten en bestanden van het werk te delen via clouddiensten dan ambtenaren exclusief Rijksoverheid.

Medewerkers klein-MKB delen vaker documenten en bestanden van het werk via privé e-mail en clouddiensten ten opzichte van medewerkers groot-MKB en grootbedrijf.

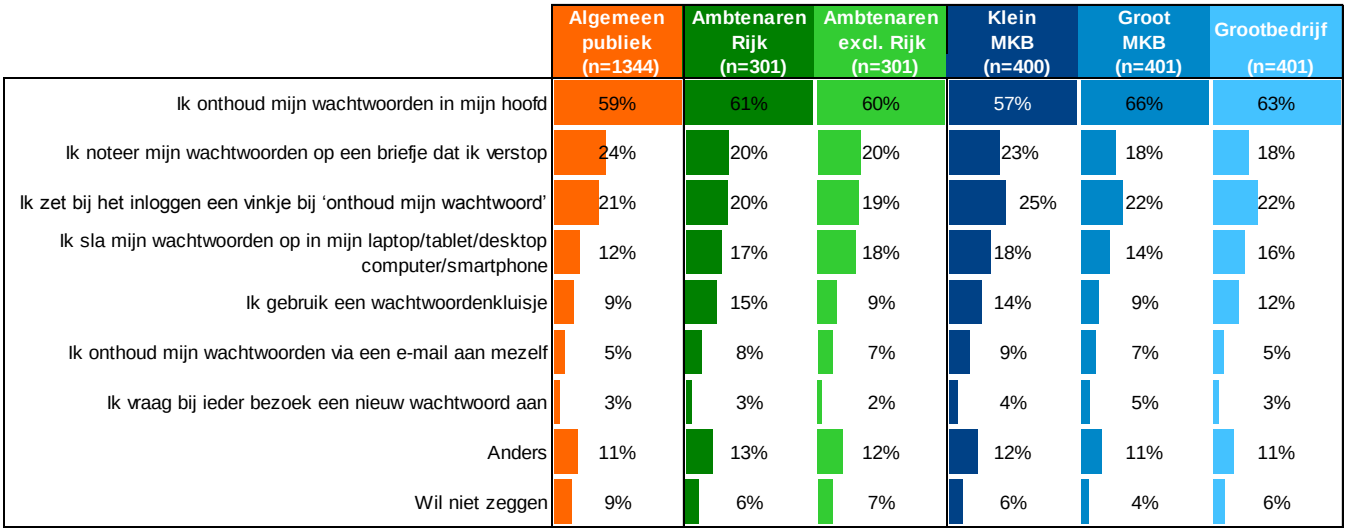
Verschillen in achtergrondkenmerken

Hoogopgeleiden delen vaker documenten en bestanden van het werk (via privé e-mail en clouddiensten) dan de overige opleidingsgroepen. Jongere werknemers (18-30 jaar) delen vaker bestanden van het werk via clouddiensten dan oudere werknemers (30-plus).

6.5 Wachtwoordgedrag in detail

Hieronder volgen de resultaten ten aanzien de details ten aanzien van wachtwoordgedrag. Deze vragen zijn aan alle doelgroepen voorgelegd.

Figuur D08: Hoe zorgt u ervoor dat u uw wachtwoorden kunt onthouden?



Overall beeld

De meerderheid van de respondenten geeft aan wachtwoorden uit het hoofd te leren. Ruim een vijfde van de respondenten geeft aan wachtwoorden te noteren op een briefje dat verstopt wordt of bij het inloggen het vinkje aan te zetten 'Onthoud mijn wachtwoord'.

Vergelijking tussen doelgroepen

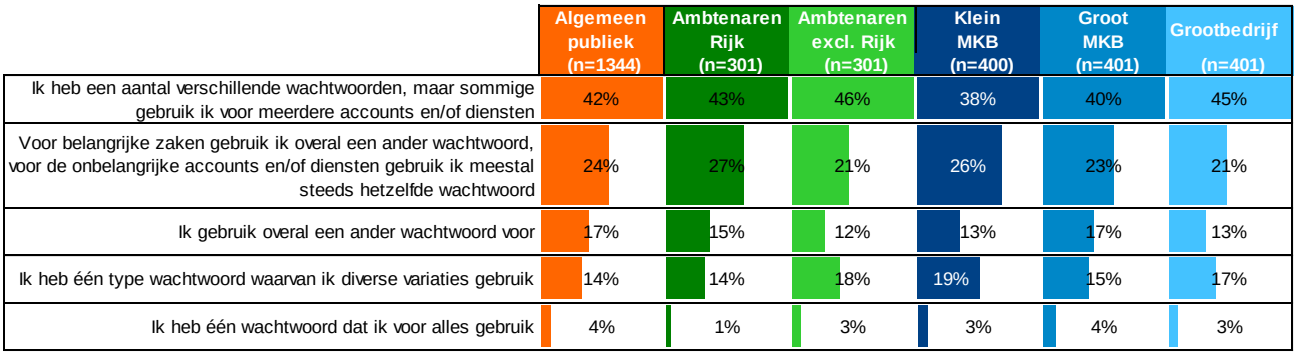
Tussen de ambtenaren doelgroepen zijn weinig verschillen op te merken; alleen ten aanzien van het gebruik van een wachtwoordenkluisje is te zien dat dit vaker voorkomt onder ambtenaren Rijksoverheid ten opzichte van ambtenaren exclusief Rijksoverheid.

Ook tussen de bedrijfsleven doelgroepen zijn weinig verschillen zichtbaar. Medewerkers groot-MKB onthouden wachtwoorden vaker in het hoofd dan medewerkers klein-MKB, en medewerkers klein-MKB gebruiken vaker een wachtwoordenkluisje dan medewerkers groot-MKB.

Verschillen in achtergrondkenmerken

Midden- en hoogopgeleiden, jongere personen (13–30 jaar) en werknemers die niet of medeverantwoordelijk zijn voor ICT-zaken/automatisering onthouden wachtwoorden vaker in het hoofd. Wachtwoordenkluisjes worden het vaakst gebruikt door hoogopgeleiden en 30-plussers. Het gebruik van een briefje dat wordt verstopt komt het vaakst voor onder 50-plussers en laagopgeleiden. Het vinkje 'Onthoud mijn wachtwoord' en een e-mail aan zichzelf komen vaker voor onder vrouwen, 18-30 jarigen en hoogopgeleiden.

Figuur D09: Hoeveel verschillende wachtwoorden gebruikt u voor de verschillende computers, programma's en/of websites die u gebruikt?



Overall beeld

Qua aantal verschillende wachtwoorden dat men heeft, geeft men vooral aan een aantal verschillende wachtwoorden te hebben, waarvan sommige voor meerdere accounts en/of diensten worden gebruikt. Bijna een kwart van de respondenten gebruikt voor belangrijke zaken iedere keer een ander wachtwoord en voor minder belangrijke zaken meestal steeds hetzelfde wachtwoord.

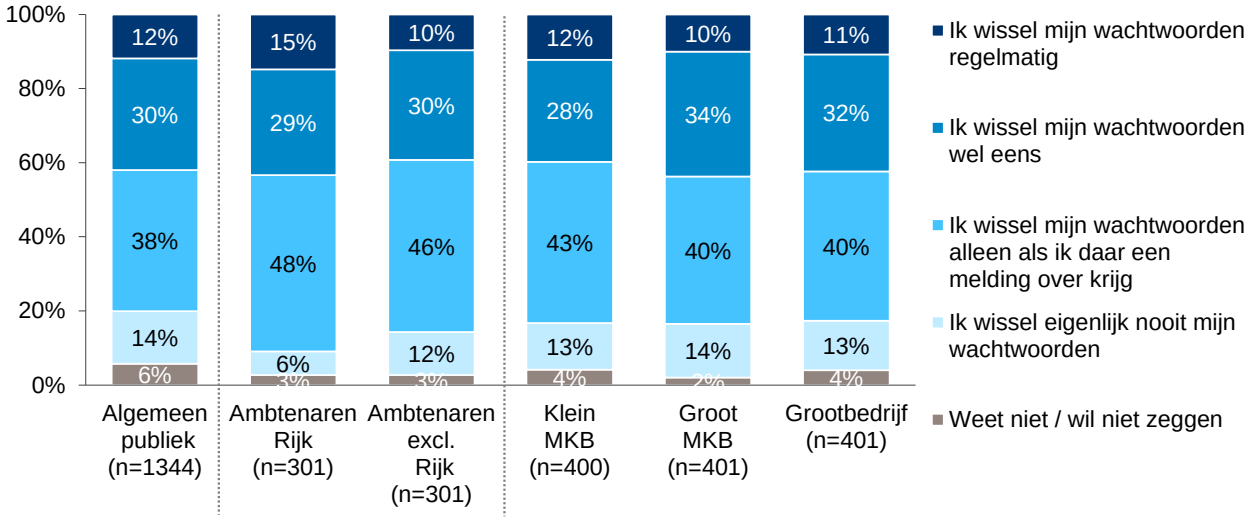
Vergelijking tussen doelgroepen

Er zijn geen wezenlijke verschillen tussen doelgroepen.

Verschillen in achtergrondkenmerken

50-plussers en laagopgeleiden geven vaker aan overal een ander wachtwoord voor te gebruiken dan 18-49 jarigen en midden- en hoogopgeleiden. Werknemers die niet verantwoordelijk zijn voor ICT-zaken/automatisering hebben vaker een aantal verschillende wachtwoorden, waarvan sommige voor meerdere accounts/diensten worden gebruikt (in vergelijking met werknemers die (mede) verantwoordelijk zijn voor ICT-zaken/automatisering).

Figuur D10: Hieronder staat een aantal uitspraken over het wisselen van wachtwoorden. Welke uitspraak is het meeste op uw wachtwoord(en) van toepassing? Met "regelmatig" wordt bedoeld: eens per drie maanden of vaker. Met "wel eens" wordt bedoeld: minder vaak dan eens per drie maanden.



Overall beeld

Men is veelal reactief als het gaat om het wisselen van wachtwoorden; men doet dit vaak alleen als er een melding over verschijnt. Drie op de tien respondenten geeft aan wachtwoorden wel eens te wisselen. Ruim een op de tien respondenten bekent wachtwoorden eigenlijk nooit te veranderen.

Vergelijking tussen doelgroepen

Ambtenaren exclusief Rijksoverheid geven vaker aan nooit wachtwoorden te wisselen ten opzichte van ambtenaren Rijksoverheid (12% vs. 6%).

Verschillen in achtergrondkenmerken

Jongeren (13-17 jaar) geven vaker dan de overige leeftijdsgroepen aan nooit hun wachtwoorden te wisselen, terwijl 50-plussers vaker dan de overige leeftijdsgroepen aangeven regelmatig hun wachtwoorden te wisselen. Laagopgeleiden vertonen wat betreft het wisselen van wachtwoorden veiliger gedrag dan hoog- en middenopgeleiden; zij geven vaker aan deze regelmatig te wisselen. Tevens geven hoogopgeleiden vaker aan dan de overige leeftijdsgroepen dat ze enkel wachtwoorden wisselen als daar een melding over verschijnt. Ook vrouwen zijn hier wat reactiever in dan mannen.

7. Resultaten 2015: Werkelijk slachtofferschap & voorgenomen gedrag bij een voorval

7.1 Beknopte samenvatting

Werkelijk slachtofferschap
Ongewenste e-mail en phishing is een ruime meerderheid wel eens overkomen. Voor ongewenste e-mail (spam) is dit wellicht te verwachten, voor phishing, een meer ingrijpende manier van slachtofferschap, mag dit als een fors aandeel worden beschouwd. Virussen komen ook regelmatig voor en een vijfde heeft wel eens te maken gekregen met mensen die gegevens opvragen onder valse voorwendselen.

Voorgenomen gedrag bij voorval
Bij ontvangst van een verdachte e-mail van de eigen bank zegt de meerderheid deze direct ongelezen te zullen verwijderen. Bij een dergelijke e-mail met een bekende als afzender gaat het om twee vijfde die dit zegt te gaan doen. Ruim een kwart zou de e-mail verifiëren bij de afzender.

Ook geeft een deel aan contact te zoeken met de verzender om te controleren of de mail geen phishing betreft (30% in geval van een bekende; 21% in het geval van de eigen bank). Een kleine minderheid geeft aan uit nieuwsgierigheid verdachte mails toch te openen; van een bekende zou men dit vaker doen dan van de eigen bank.

7.2 Werkelijk slachtofferschap

Hieronder ziet u de resultaten van cyberincidenten waar respondenten zelf, of mensen in hun directe omgeving, mee te maken hebben gehad.

Figuur F01: Heeft u zelf, of iemand in uw directe omgeving, ooit wel eens te maken gehad met één van onderstaande voorvallen? Let op: hierbij konden 'Ja, ikzelf' en 'Ja, iemand in mijn directe omgeving' beiden geselecteerd worden. Dus de percentages kunnen optellen tot meer dan 100%.

	Algemeen publiek (n=1344)	Ambtenaren Rijk (n=301)	Ambtenaren excl. Rijk (n=301)	Klein MKB (n=400)	Groot MKB (n=401)	Grootbedrijf (n=401)
Computervirus verspreid via e-mail						
Ja, ikzelf	19%	19%	21%	28%	20%	21%
Ja, iemand in mijn directe omgeving	18%	26%	24%	20%	24%	24%
Nee	58%	53%	54%	51%	57%	58%
Computervirus verspreid via het downloaden van geïnfecteerde software/bestanden						
Ja, ikzelf	23%	27%	30%	31%	28%	26%
Ja, iemand in mijn directe omgeving	17%	21%	23%	19%	21%	21%
Nee	55%	53%	47%	52%	52%	55%
Computeruitval door een virus of malware						
Ja, ikzelf	20%	21%	23%	29%	24%	21%
Ja, iemand in mijn directe omgeving	13%	16%	18%	17%	19%	18%
Nee	61%	63%	59%	57%	60%	61%
Identiteitsdiefstal / misbruik van uw persoonsgegevens						
Ja, ikzelf	3%	1%	2%	3%	1%	2%
Ja, iemand in mijn directe omgeving	3%	4%	4%	4%	5%	5%
Nee	88%	91%	90%	90%	90%	87%
Ongeoorloofde afschrijving via internetbankieren						
Ja, ikzelf	5%	5%	6%	5%	2%	6%
Ja, iemand in mijn directe omgeving	5%	7%	5%	5%	8%	5%
Nee	84%	86%	86%	88%	89%	87%
Mails met phishing						
Ja, ikzelf	56%	62%	62%	73%	61%	62%
Ja, iemand in mijn directe omgeving	19%	28%	24%	26%	25%	27%
Nee	30%	23%	26%	21%	29%	26%
Ongewenste e-mail (spam)						
Ja, ikzelf	82%	86%	87%	93%	84%	85%
Ja, iemand in mijn directe omgeving	25%	36%	28%	37%	30%	31%
Nee	10%	8%	8%	4%	10%	11%
Mensen die gegevens opvragen door zich voor te doen als telefonische helpdesk, een betrouwbare of bekende organisatie						
Ja, ikzelf	19%	22%	18%	25%	19%	22%
Ja, iemand in mijn directe omgeving	11%	14%	12%	17%	12%	13%
Nee	67%	67%	68%	64%	70%	66%
Online pesten						
Ja, ikzelf	2%	1%	2%	2%	2%	2%
Ja, iemand in mijn directe omgeving	6%	5%	5%	4%	7%	5%
Nee	87%	92%	91%	92%	89%	90%
Online chantage (ook wel ransomware genoemd)						
Ja, ikzelf	3%	2%	2%	4%	5%	4%
Ja, iemand in mijn directe omgeving	4%	6%	2%	5%	4%	3%
Nee	87%	89%	90%	88%	87%	89%
Oplichting bij online aankopen						
Ja, ikzelf	9%	12%	10%	13%	11%	11%
Ja, iemand in mijn directe omgeving	9%	10%	10%	12%	14%	14%
Nee	78%	78%	76%	75%	73%	74%
Online oplichting met behulp van een zielig verhaal						
Ja, ikzelf	12%	14%	16%	25%	16%	15%
Ja, iemand in mijn directe omgeving	6%	6%	6%	11%	9%	9%
Nee	78%	79%	78%	65%	77%	75%

Overall beeld

De meest genoemde voorvallen waarmee respondenten zelf te maken hebben gehad, zijn ongewenste e-mail (spam) en mails met phishing. De meest genoemde voorvallen waarmee iemand uit de directe omgeving ooit te maken heeft gekregen zijn, naast ongewenste e-mail (spam) en mails met phishing, ook computervirussen verspreid via e-mail en computeruitval door virussen. Met identiteitsdiefstal en online pesten/chantage heeft nagenoeg niemand (ook niet in de directe omgeving) te maken gekregen.

Vergelijking tussen doelgroepen

Tussen de twee ambtenaren doelgroepen zijn weinig verschillen op te merken, maar tussen de bedrijfsleven doelgroepen is dit wel het geval. Over het algemeen hebben medewerkers klein-MKB vaker zelf te maken gehad met veel van de voorgelegde voorvallen ten opzichte van zowel medewerkers groot-MKB en grootbedrijf, als burgers. Dit heeft ongetwijfeld te maken met het feit dat zij vaker zelf (mede) verantwoordelijk zijn voor ICT-zaken en dus zelf met voorvallen worden geconfronteerd.

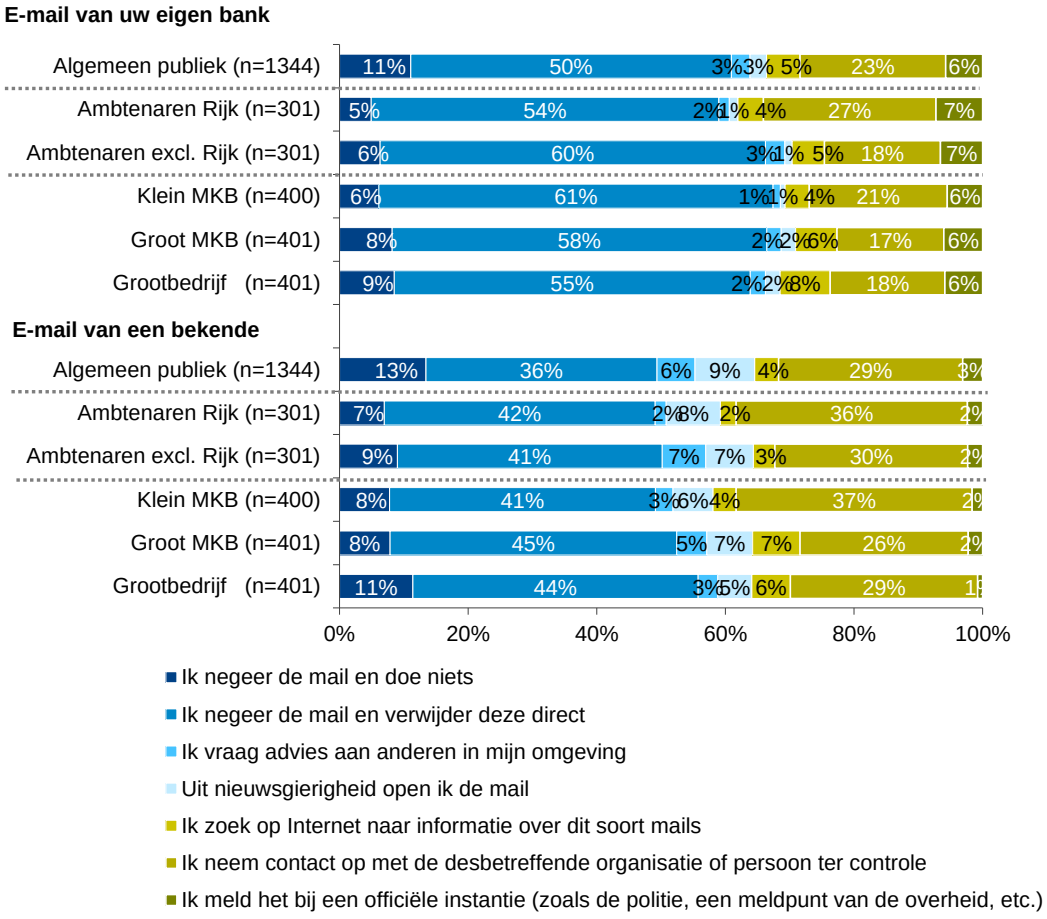
Verschillen in achtergrondkenmerken

Mannen, ouderen en hoogopgeleiden hebben vaker zelf te maken gehad met een aantal voorvallen (zoals computervirus verspreid via e-mail/downloaden van geïnfecteerde software of bestanden, computeruitval door een virus of malware) dan vrouwen, jongeren en laag- en middelbaaropgeleiden. Vooral 30-plussers, hoogopgeleiden en medewerkers die eindverantwoordelijk zijn voor ICT-zaken/automatisering hebben zelf te maken gehad met phishing mails. Jongeren (13-17 jaar) geven vaker aan zelf te maken hebben gehad met online pesten vergeleken met de overige leeftijdsgroepen.

7.3 Voorgenomen gedrag bij ontvangst van phishing mails

Nu volgen de resultaten van voorgenomen gedrag bij de ontvangst van vermoedelijke phishing mails (van zowel de eigen bank als een bekende).

Figuur E01: Stel dat u zelf een e-mail in uw mailbox ontvangt van onderstaande afzenders, maar u vertrouwt het niet helemaal en vermoedt dat het een e-mail met phishing is. Wat zou u dan doen?



Overall beeld

Indien men een mail van de eigen bank ontvangt maar deze niet helemaal vertrouwt, zou ruim de helft de mail negeren en direct verwijderen. Ook indien een dergelijke mail afkomstig is van een bekende zou het merendeel (40%) de mail negeren en direct verwijderen. Een op de drie respondenten geeft aan in het geval van een bekende contact op te nemen met de desbetreffende persoon om te controleren of de mail geen phishing betreft. Een minderheid geeft aan uit nieuwsgierigheid verdachte mails toch te openen; van een bekende zou men dit vaker doen dan van de eigen bank (8% vs. 2%).

Vergelijking tussen doelgroepen

Indien men een mail van de eigen bank ontvangt maar deze niet helemaal vertrouwt, zouden ambtenaren Rijksoverheid vaker contact opnemen met de desbetreffende persoon/organisatie ter controle ten opzichte van ambtenaren exclusief Rijksoverheid.

Indien een dergelijke mail afkomstig is van een bekende, geven ambtenaren exclusief Rijksoverheid vaker aan advies te vragen aan anderen in de omgeving in vergelijking met ambtenaren Rijksoverheid. Medewerkers klein-MKB zouden vaker contact opnemen met de desbetreffende organisatie of persoon ter controle ten opzichte van medewerkers groot-MKB en grootbedrijf.

Verschillen in achtergrondkenmerken

Jongeren (13-17 jaar) zouden vaker dan de overige leeftijdsgroepen mails die ze niet helemaal vertrouwen (van zowel de eigen bank als een bekende) toch openen uit nieuwsgierigheid. Ook 18-30 jarigen zouden dit vaker doen dan de oudere leeftijdsgroepen. 50-plussers zouden vaker dan 18-49 jarigen contact opnemen met de verzender (als de afzender de eigen bank is) en een melding doen bij een officiële instantie (als de afzender een bekende is). Hoogopgeleiden zouden dergelijke mails (van zowel de eigen bank als een bekende) vaker negeren en direct verwijderen ten opzichte van de overige leeftijdsgroepen.

8. Bijlagen

8.1 Responsoverzicht

De responsoverzichten zijn hieronder weergegeven, eerst voor de totale steekproef en vervolgens per doelgroep.

Totaal
De respons voor de totale steekproef is 39%.

Bruto steekproef		8.150
Non-respons (geen respons ontvangen)		3.857
Afvallers		1.145
Groep vol	342	
Niet volledig ingevulde vragenlijsten	196	
Voldoet niet aan de criteria / screeningseisen	607	
Complete vragenlijsten		3.148

Ambtenaren Rijksoverheid
De respons voor deze doelgroep is 43%.

Bruto steekproef		700
Non-respons (geen respons ontvangen)		294
Afvallers		105
Groep vol	27	
Niet volledig ingevulde vragenlijsten	10	
Voldoet niet aan de criteria / screeningseisen	68	
Complete vragenlijsten		301

Ambtenaren overig

De respons voor deze doelgroep is 43%.

Bruto steekproef		700
Non-respons (geen respons ontvangen)		258
Afvallers		141
Groep vol	51	
Niet volledig ingevulde vragenlijsten	17	
Voldoet niet aan de criteria / screeningseisen	73	
Complete vragenlijsten		301

Medewerkers 'klein-MKB'

De respons voor deze doelgroep is 33%.

Bruto steekproef		1.200
Non-respons (geen respons ontvangen)		584
Afvallers		216
Groep vol	9	
Niet volledig ingevulde vragenlijsten	49	
Voldoet niet aan de criteria / screeningseisen	158	
Complete vragenlijsten		400

Medewerkers 'groot-MKB'

De respons voor deze doelgroep is 29%.

Bruto steekproef		1.400
Non-respons (geen respons ontvangen)		744
Afvallers		255
Groep vol	54	
Niet volledig ingevulde vragenlijsten	30	
Voldoet niet aan de criteria / screeningseisen	171	
Complete vragenlijsten		401

Medewerkers grootbedrijf (overig bedrijfsleven)

De respons voor deze doelgroep is 45%.

Bruto steekproef		900
Non-respons (geen respons ontvangen)		306
Afvallers		193
Groep vol	24	
Niet volledig ingevulde vragenlijsten	32	
Voldoet niet aan de criteria / screeningseisen	137	
Complete vragenlijsten		401

Burgers 13+

De respons voor deze doelgroep is 41%.

Bruto steekproef		3.250
Non-respons (geen respons ontvangen)		1.671
Afvallers		235
Groep vol	177	
Niet volledig ingevulde vragenlijsten	58	
Voldoet niet aan de criteria / screeningseisen	0	
Complete vragenlijsten		1.344

8.2 Steekproeven en weging

Steekproeven en weging
Er is voor gekozen om het onderzoek volledig binnen het GfK Online panel uit te voeren en de eerdere combinatie met het Flitspanel van het Ministerie van BZK los te laten. Dat voorkomt enerzijds discussies over het gebruik van twee verschillende panels.

Onderstaande tabel geeft een overzicht van de steekproef- en weegkenmerken.

Doelgroepen	Kenmerken waarop de steekproef is gestratificeerd	Kenmerken waarop de steekproef wordt gewogen
Ambtenaren Rijksoverheid	Geslacht, leeftijd	Geslacht, leeftijd
Ambtenaren overig	Geslacht, leeftijd, verdeling gemeente/waterschap/provincie	Geslacht, leeftijd, verdeling gemeente/waterschap/provincie
Medewerkers 'klein-MKB'	Branche, bedrijfsgrootte, geslacht, leeftijd	Branche, bedrijfsgrootte, geslacht, leeftijd
Medewerkers 'Groot-MKB'	Branche, bedrijfsgrootte, geslacht, leeftijd	Branche, bedrijfsgrootte, geslacht, leeftijd
Medewerkers overig bedrijfsleven	Branche, bedrijfsgrootte, geslacht, leeftijd	Branche, bedrijfsgrootte, geslacht, leeftijd
Burgers 13+	Geslacht, leeftijd, opleiding, regio, internetgebruik	Geslacht, leeftijd , opleiding, regio, internetgebruik

8.3 Nadere informatie indexscore en verdiepende analyses

Indexscore
Om beter inzicht te krijgen in de mate van cybersecure gedrag, is het van belang om duidelijk te hebben wanneer men beschouwd mag worden als 'cybersecure' qua gedrag. Hiertoe heeft de NCTV verzocht om een aantal 'gewenste gedragingen' op te stellen. Deze gewenste gedragingen bestaan uit een aantal thema's, en voor elk thema zijn specifieke gedragstellingen geformuleerd. Vervolgens heeft de NCTV het belang van elk thema aangegeven voor de totale mate van cybersecure gedrag door een gewicht toe te kennen aan elk van de thema's.

De gewenste gedragingen zijn verwerkt in vraagblok D03, en op basis hiervan is een indicator berekend, die de mate aangeeft waarin de respondent 'cybersecure' gedrag vertoont. De indicator is als volgt berekend:

Per thema is een score berekend van minimaal 0 tot maximaal 1. Als een stelling niet van toepassing is, laten we deze buiten de berekening, de respondent in kwestie kan evenwel toch een maximale score van 1 behalen. Bijvoorbeeld: als een thema 4 stellingen omvat, telt elke stelling voor 0,25 mee. Als één van de vier stellingen niet van toepassing is, tellen we de stelling voor 0,334 mee enzovoort. Pas als geen van de stellingen van een thema van toepassing is, krijgt het gehele thema de kwalificatie "niet van toepassing".

Vervolgens worden de scores van elk thema vermenigvuldigd met de desbetreffende weging van dat thema en gesommeerd.

We delen vervolgens deze somscore door de maximaal haalbare score op de betreffende thema's en vermenigvuldigen deze met 100 om een indicator van 0-100 te verkrijgen. Om te voorkomen dat de indicator "Cybersecurity" op te weinig thema's is gebaseerd, moeten minimaal zes thema's op de respondent van toepassing zijn.

Om beter inzicht te krijgen in de mate van cybersecure gedrag (en eventuele verschuivingen in de tijd overzichtelijk te kunnen monitoren in de toekomst), zijn de indicatorscores ingedeeld in drie groepen:

1. **Laag**; gebaseerd op het laagste kwartiel (de laagste 25% van de respondenten, die het laagst scoren op de indicator) - score van 0 tot 53.25
2. **Midden**; gebaseerd op de middelste helft (de middelste 50% van de respondenten) - score tussen 53.25 en 75.30
3. **Hoog**; gebaseerd op het hoogste kwartiel (de hoogste 25% van de respondenten, die het hoogst scoren op de indicator) - score van 75.31 tot 100

Hieronder zijn de specifieke gedragstellingen weergegeven waar de indicator op gebaseerd is.

D03 [S per row]
Kunt u aangeven welk van de volgende uitspraken voor u gelden?

1. Ja
2. Nee
99. Niet op mij van toepassing / weet niet

1) WiFi-het gebruik van draadloos internetten

a. Ik heb een wachtwoord ingesteld op mijn WiFi-netwerk thuis dat bestaat uit minimaal 12 karakters
b. Als ik buitenshuis gebruik maak van WiFi-netwerken, maak ik doorgaans alleen verbinding met vertrouwde netwerken, waar je op moet inloggen
c. Ik maak doorgaans gebruik van het automatisch verbinding maken met vertrouwde WiFi-netwerken
d. Ik maak doorgaans gebruik van een Virtual Private Network (VPN)-app om verbinding te maken met WiFi-netwerken buitenshuis, waarmee mijn internetverkeer versleuteld wordt verstuurd

2) Back-ups

e. Ik maak doorgaans minstens elke 4 weken een back-up van mijn bestanden (bijv. belangrijke documenten, foto's, etc.) op een externe harde schijf

3) Herkennen van phishing mails om o.a. cryptoware- en ransomwarebesmetting te voorkomen Ik vermijd doorgaans op links te klikken (bijv. in e-mails) die ik niet vertrouw

f. Ik verwijder doorgaans e-mails die ik niet vertrouw zonder deze te openen, ook als deze van een bekende afzender komen

4) Wachtwoorden [SCRIPTER: do not show bold text]

g. Mijn wachtwoorden bestaan doorgaans uit meer dan 12 karakters
h. Mijn wachtwoorden bestaan doorgaans uit tussen de 8 en 12 karakters
i. Mijn wachtwoorden bevatten doorgaans minimaal 1 hoofdletter, 1 kleine letter en 1 speciaal teken (anders dan letters uit het alfabet of cijfers)
j. Ik zet mijn wachtwoorden in een document op mijn computer en/of laptop
k. Ik verander mijn wachtwoorden doorgaans elke drie maanden

5) Twee-factor-authenticatie

l. Waar het mogelijk is om een twee-staps-verificatie [*SCRIPTER show information text 1*] in te stellen, doe ik dit ook

6) Websites bezoeken

m. Bij het bezoeken van websites controleer ik doorgaans of de juiste URL in mijn internetbrowser staat om vast te stellen of ik de juiste site bezoek
n. Bij het bezoeken van websites waar ik gegevens moet invoeren (zoals bij webwinkels), controleer ik doorgaans eerst of er een groen slotje aanwezig is in mijn browser
o. Bij het bezoeken van websites waar ik gegevens moet invoeren (zoals bij webwinkels), voer ik doorgaans alleen verplichte velden in en geen niet-verplichte velden

7) Veilig online winkelen

p. Als ik online aankopen wil doen en de website niet helemaal vertrouw, verlaat ik doorgaans de website of ga ik op nader onderzoek uit
q. Als ik online aankopen doe, controleer ik doorgaans of de webwinkel aangesloten is bij keurmerken (zoals de Thuiswinkel Waarborg)
r. Als ik mijn betaling doe tijdens een online aankoop, controleer ik doorgaans of ik via een beveiligde internetverbinding betaal ('https://' in de browser en groen hangslotje)
s. Als ik betaaltransacties doe/als ik bankier via internet gebruik ik vaker de app dan de browser

8) Software-updates

t. Ik installeer doorgaans direct software-updates als mijn computer/laptop/tablet dit adviseert
u. Ik maak zoveel mogelijk gebruik van automatische software-updates

9) Bring your own device [only show if quota > 1 (PROFESSIONALS)]

v. Ik houd me doorgaans aan de afspraken die er zijn vanuit mijn werk voor het gebruik van privé-apparaten op het werk (Bring Your Own Device)
w. Als ik mijn privé-apparaten ook voor het werk gebruik (Bring Your Own Device), zorg ik er doorgaans voor dat anderen (zoals mijn partner, kinderen) die ook gebruikmaken van deze apparaten, een ander account gebruiken

10) Gebruik smartphone

x. Ik download apps doorgaans alleen uit de App Store / Google Play Store
y. Ik geef apps doorgaans toegang tot gegevens waar ze om vragen (mijn microfoon, contacten, etc.)
z. Ik heb locatiegegevens voor apps doorgaans aanstaan
aa. Ik kan op afstand apparaten lokaliseren, blokkeren en inhoud wissen (bijv. via de 'Find my iPhone' app)

11) Andere apparaten verbonden met internet (network-opslag, beveiligingscamera's, etc.)

bb. Ik zorg dat alle apparaten in huis die met internet verbonden zijn een veilig wachtwoord hebben (minimaal 12 tekens)

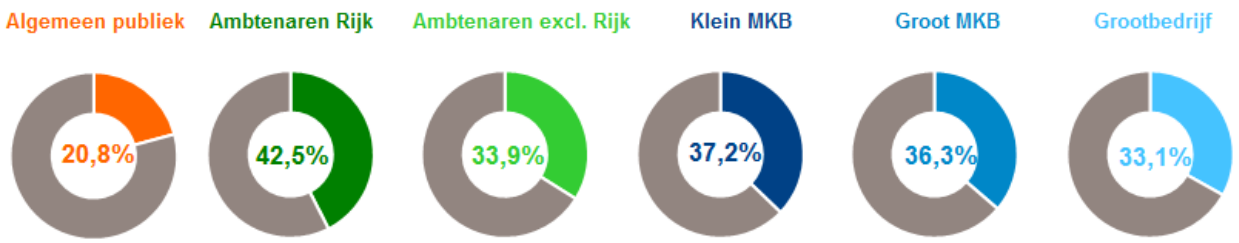
Verdiepende analyses

Naast de interessante wetenschap hoe hoog iedere doelgroep scoort op dit cybersecure gedrag, is de indexscore ook een uitstekend uitgangspunt voor een verdiepende analyse. Het doel daarvan is te bepalen in hoeverre informatie, verzameld binnen het onderzoek, een verklaring kan vormen voor de verschillen in hoogte van die indexscore. Dus: wat bepaalt in welke mate of iemand hoog of laag scoort op cybersecure gedrag?

Hiertoe is een verdiepende analyse uitgevoerd, waarbij eerst de onderlinge correlaties zijn bepaald tussen enerzijds enkele achtergrondkenmerken en vragenlijstvariabelen en anderzijds de indexscore cybersecure gedrag. Vervolgens is op basis van de uitkomsten hiervan een zogenaamde relative weights analyse uitgevoerd, om te bepalen in hoeverre de relevante variabelen een bijdrage leveren aan de verklaring van de verschillen in hoogte van de indexscore. Een dergelijke verklarende analyse is een nieuw element in het onderzoek naar cybersecurity.

Ten eerste is het belangrijk om de verklaringskracht te bekijken van de elementen die bij de analyse zijn betrokken. De verklaringskracht voor cybersecure gedrag.

Verklaringskracht op basis van verdiepende analyses Cyberscure Gedrag (per doelgroep)



Duidelijk is dat voor de professionele doelgroepen meer verklaring wordt gevonden voor de verschillen in de indexscore cybersecure gedrag dan voor het algemeen publiek. Dit was in zekere zin ook te verwachten, omdat er voor de professionele doelgroepen meer (werkspecifieke) informatie is verzameld en er hierdoor meer informatie in de verklarende analyse kon worden opgenomen. Vooral de verklaringskracht voor de groep Rijksambtenaren is, ook vanuit sociaalwetenschappelijk perspectief, aanzienlijk te noemen.

8.4 Certificering

Het onderzoek is uitgevoerd in overeenstemming met het quality systeem van GfK dat is gecertificeerd volgens de normen van NEN-EN-ISO 9001, ISO 20252 en ISO 26362. GfK onderschrijft de gedragsregels van E.S.O.M.A.R. (European Society for Opinion and Market Research) en is lid van de brancheorganisatie MOA (zie http://www.moaweb.nl).

Het is toegestaan de uitkomsten van onderzoek extern te publiceren. Wel dient in dat geval bij de onderzoeksresultaten als bron "GfK <opleveringsmaand en jaar onderzoek>" te worden vermeld.

Exclusiviteit van verzamelde gegevens is gebaseerd op de Gedragscode van de MOA, art. 5 (zie http://www.moaweb.nl).