Rapportage Cyber security

Kwantitatief onderzoek in opdracht van NCTV en DPC

Uitgevoerd door: Intomart GfK bv

Uw contact: Marjolein van Kouterik-Nijhof

Tel.: +31 (0)35-6258411 / Fax: +31 (0)35-6246532
E-mail: marjolein.van.kouterik-nijhof@gfk.com

Projectnummer: 32876

Datum: 18-10-2013

INHOUD **Pagina**

BIJLAGEN:

1. Responsoverzicht kwantitatief onderzoek
2. Kwantitatieve vragenlijst
3. Certificering

Samenvatting, conclusies en aanbevelingen

Achtergrond en doel onderzoek

In opdracht van NCTV en DPC heeft GfK Intomart een online onderzoek uitgevoerd onder netto 3.241 personen naar de cyber security awareness. Dit onderzoek betreft de 1-meting; in 2012 is de pilot (o-meting) door onderzoeksbureau Motivaction uitgevoerd.

Doel van dit onderzoek is het verkrijgen van inzicht in het huidige niveau van cyber security awareness vertaald naar kennis, houding en gedrag; de informatiebehoeften op dit gebied en verschillen in de resultaten tussen doelgroepen en in de tijd. Ook geeft het onderzoek inzicht in een jaarlijks wisselend thema, wat dit jaar Smart Security betreft. Smart Security bestaat uit drie subthema's: Smart Cities, Security by Design en Smart Coalitions.

Onderzoeksopzet in vogelvlucht

Het kwantitatieve onderzoek vond plaats van 10 tot en met 22 juli 2013 onder het online onderzoekspanel van GfK onder de volgende doelgroepen:

- medewerkers van de Rijksoverheid;
- medewerkers van gemeenten;
- medewerkers van vitale sectoren van het bedrijfsleven (energie, transport, telecommunicatie, financiële sector, drinkwater, keren en beheren van oppervlaktewater);
- medewerkers van het bedrijfsleven overig (organisaties met 10 medewerkers of meer, *exclusief* vitale sectoren);
- burgers van 13 jaar en ouder.

De respons van de totale steekproef is 50%. Tussen de doelgroepen varieert de respons van 26% voor gemeenten tot 71% voor het algemene bedrijfsleven. Om een representatief beeld te verkrijgen zijn de steekproeven op voorhand verdeeld naar de populatieverhoudingen op relevante kenmerken en zijn de resultaten achteraf waar nodig gewogen naar deze kenmerken.

Ten geleide voor de lezer

- In de management summary geven we eerst een overall samenvatting van het algemene deel van het onderzoek, gevolgd door een samenvatting van het themadeel (Smart Security) en de hoofdlijnen van de uitkomsten van de verdiepende analyses. Vervolgens komen de conclusies en aanbevelingen aan bod. Tot slot geven we per doelgroep de belangrijkste conclusies, gevolgd door een samenvatting van de resultaten.
- Daar waar in deze management summary gesproken wordt over verschillen betreft dit uitsluitend significante verschillen.
- Alle resultaten betreffen *zelfgerapporteerde* kennis, houding en gedrag.

Management samenvatting Cyber security 2013

Overall samenvatting

Beeld cyber security

- Alle doelgroepen hebben vaker een concreet beeld van cyber security dan vorig jaar. Beveiliging tegen bedreigingen van buitenaf via antivirussoftware en firewalls zijn nog steeds dominante elementen in de beeldvorming, boven bescherming van de privacy. Drie van de vijf doelgroepen associëren cyber security dit jaar vaker met privacy. Nog altijd een derde heeft echter spontaan geen beeld van cyber security.

Verantwoordelijkheidstoedeling

- Cyber security wordt ook dit jaar als een gedeelde verantwoordelijkheid beschouwd van de gebruiker zelf (als werknemer of burger) en andere partijen (respectievelijk de IT-afdeling en internetproviders). Opvallend is dat burgers de verantwoordelijkheid wat vaker buiten zichzelf leggen, namelijk bij website-eigenaren.

Risicoperceptie

- De meerderheid van de professionele doelgroepen en van burgers vindt zichzelf voldoende bewust van de gevaren van internet en maken zich hier niet erg druk over. Gemeenteambtenaren maken zich wat meer zorgen om de risico's van internet en voelen zich minder weerbaar hiertegen.
- Bij burgers is de risicoperceptie het laagst. Hoewel zij zichzelf voldoende bewust vinden, weet de meerderheid (bovendien ook méér dan vorig jaar) niet hoe er via internet misbruik van hun computer kan worden gemaakt. Burgers maken zich de minste zorgen van alle doelgroepen en een groot deel denkt dat de kans dat zij zelf met internetrisico's te maken krijgen klein is en schat privacyrisico's hoger in dan financieel-economische risico's. Zij voelen zich ook minder weerbaar tegen de risico's (beperkte locus of control) dan de professionele doelgroepen. Zo weet een derde niet hoe zich te beschermen tegen misbruik, een toename ten opzichte van vorig jaar. Het is niet verrassend dan een noemenswaardige groep (een kwart) behoefte heeft aan meer informatie over internetrisico's.

Cyber secure kennis en gedrag rondom veilig wachtwoordgebruik

- Wat betreft een veilig wachtwoordgebruik zijn er geen verschillen tussen groepen.
- Op een positieve ontwikkeling binnen de vitale setoren na (het vaker gebruiken van afzonderlijke wachtwoorden voor belangrijke zaken binnen de vitale sectoren), lijkt het gebruik van wachtwoorden wat aan veiligheid in te boeten ten opzichte van vorig jaar. Zo zien we bij alle doelgroepen dat ze minder vaak een ander wachtwoord voor ieder account gebruiken en minder vaak op eigen initiatief hun wachtwoorden periodiek wisselen.

Cyber security op het werk: aandacht voor digitale veiligheid door werkgever, verankering in beleid, uitvoering en naleving beleid

- Wat betreft cyber security awareness op het werk zijn er bij meerdere doelgroepen ontwikkelingen (positief en/of negatief) te zien ten opzichte van vorig jaar.
  - Daarbij springt de Rijksoverheid er positief uit: over de hele linie (aandacht voor digitale veiligheid op het werk, verankering in beleid, structurele uitvoering en naleving van het beleid) is hierin een stijging te zien.
  - Bij de vitale sectoren zijn de ontwikkelingen verdeeld. Het bewustzijn en de kennis van de medewerkers ligt nog steeds op een hoog niveau en soms is toegenomen in de tijd. En hoewel cyber security nog altijd hoog in het vaandel staat zijn hierin de nodige scheurtjes in zichtbaar ten opzichte van verleden jaar. Met name de aandacht in het beleid voor digitale veiligheid bij het personeel is wat verslapt ten opzichte van vorig jaar. Ook is het gedrag van medewerkers soms wat minder veilig geworden.
  - Hoewel binnen het algemene bedrijfsleven een aantal positieve ontwikkelingen gaande zijn, ligt het cyber security niveau grotendeels op hetzelfde niveau als vorig jaar. Daarin zijn nog stappen te maken.
  - Gemeenten scoren dit jaar ook relatief het laagst van de bevraagde professionele doelgroepen. Zo scoort de aandacht voor digitale veiligheid op het werk lager en vaker onvoldoende, is de digitale veiligheid minder vaak dan bij de andere doelgroepen en minder vaak dan verleden jaar in beleid geborgd, is er minder sprake van een structurele uitvoering en naleving van het beleid, is de cyber security awareness qua kennis en gedrag minder sterk dan bij andere doelgroepen en voelen gemeenteambtenaren zich het minst goed op de hoogte van het digitale veiligheidsbeleid.
- Leidinggevenden zijn doorgaans kritischer over de cyber security awareness in kennis en gedrag van medewerkers dan de medewerkers zelf zijn.

Beoordeling digitale veiligheid op het werk en thuis

- Ook dit jaar wordt de digitale veiligheid van de werkgever het hoogste beoordeeld, gevolgd door de eigen digitale veiligheid op het werk die men bovendien als hoger ingeschat dan de digitale veiligheid van collega's en de digitale veiligheid thuis. Rijksambtenaren, medewerkers van de vitale sectoren en medewerkers van het algemene bedrijfsleven zijn dit jaar (nog) positiever over de digitale veiligheid van hun werkgever en hun collega's. Rijksambtenaren zijn ook positiever over de eigen digitale veiligheid als werknemer. De beoordeling van de digitale veiligheid is bij gemeenten gelijk gebleven of iets minder positief geworden dan vorig jaar. Voorts zijn gemeenten hier negatiever over dan de andere zakelijke doelgroepen.

Samenvatting Thema 2013: Smart Security

- Uit de verdiepende analyses komt naar voren dat er weinig noemenswaardige verschillen tussen de doelgroepen zijn in de bekendheid met en beeldvorming over Smart Cities, in de perceptie en het belang van de digitale veiligheid van diverse activiteiten en locaties (Smart Design) en de perceptie van de rolverdeling van diverse partijen bij het tegengaan van Ddos-aanvallen en malware. Onderstaande bevindingen gelden derhalve voor alle vijf doelgroepen.

- Het concept *Smart Cities* is niet erg bekend onder de doelgroepen: bijna de helft kan geen Smart City noemen. Degenen die dat wel kunnen, beschouwen vooral Amsterdam en Eindhoven als een Smart City, vooral door de aanwezigheid van technische universiteiten, gerichtheid op innovatie en de toepassing van slimme digitale technologie en (in geval van burgers) vanwege de grootte van de stad (Amsterdam). Burgers vinden het belangrijker dan de overige doelgroepen dat een Smart City digitale veiligheid als voorwaarde stelt.
- Wat betreft *Security by design* hechten de ondervraagden veel waarde aan de digitale veiligheid thuis en op het werk (belang uitgedrukt in een rapportcijfer van 8,8 en 8,5) en ook nog veel, maar relatief iets minder, waarde aan de digitale veiligheid onderweg (7,5). Van de acht voorgelegde activiteiten en locaties waarvan respondenten de digitale veiligheid hebben beoordeeld in de vorm van een rapportcijfer tussen de 1 en de 10, scoort de digitale veiligheid van Wifi-thuis het hoogst (7,6) en die van het mobiele internetdiensten en het openbaar vervoer relatief het laagst (6,1 en 6). De digitale veiligheid van de overige aspecten (thuiswinkelen, nieuwssites, online reserveren van tickets en de energievoorziening) scoren daartussenin met cijfer tussen de 6,9 en 6,6.
- Wat betreft *Smart Coalitions* is bij het tegengaan van DDoS-aanvallen en malware in de ogen van alle doelgroepen de grootste rol weggelegd voor providers (8,4), software leveranciers en de (Rijks)overheid (beide 7,9) zelf en relatief de kleinste rol voor de Europese Commissie (7,1) en het bedrijfsleven en het MKB (7,0). De rol van de wetenschap (7,5), hardwareleveranciers en dienstverleners op het gebied van vitale infrastructuur (beide 7,2) bij bestrijding van Ddos-aanvallen en malware ligt hier in de ogen van de doelgroepen tussen in.

Samenvatting resultaten verdiepende analyses

- Uit de resultaten van de verdiepende analyses blijkt dat de resultaten voor een groot deel samengevat kunnen worden in zes onderliggende indicatoren, hierna aangeduid als “factoren”.
- De factoren van Cyber security geven inhoudelijk het volgende weer:
  - Factor 1: Cyber security op het werk. Deze factor heeft betrekking op alle doelgroepen, behalve burgers. Het omvat hoe de organisatie omgaat met cyber security, en de kennis, houding en gedrag van de respondent in de rol van werknemer ten aanzien van cyber security op het werk.
  - Factor 2: Het bewust omgaan met wachtwoorden. Deze factor behelst de eigen inschatting van de veiligheid van de wachtwoorden die men gebruikt en de manier waarop men omgaat met wachtwoorden wat betreft de eigenschappen van de wachtwoorden, het variëren en het vernieuwen van wachtwoorden.
  - Factor 3: De inschatting van de eigen digitale veiligheid. Hierbij gaat het om de digitale veiligheid op werkgebied en in de privésituatie, evenals de algemene grondhouding ten aanzien van de risico’s van internet voor de respondent zelf.
  - Factor 4: De wijze waarop men omgaat met e-mail (het versturen van vertrouwelijke informatie, het klikken op links in e-mail et cetera), het openen of verzenden van bestanden en gegevensdragers zoals usb-sticks.

- Factor 5: De alertheid op de betrouwbaarheid van websites en de mate waarin men zijn of haar apparaten beveiligt (via antivirus en anti-spywaresoftware, een personal firewall, het laten uitvoeren van automatische updates).
- Factor 6: De perceptie van de zinvolheid van beveiliging/ de eigen weerbaarheid, de eigen ervaring met cybercrime thuis of op het werk en de sterkte van de beveiliging van het draadloos netwerk thuis (indien men over zo'n netwerk beschikt).

- Als we kijken naar de samenstelling van de factoren dan zien we dat er een verband is tussen kennis en houding en kennis en gedrag: kennis en houding of kennis en gedrag gaan vaak samen in één factor.
- De verbanden tussen deze aspecten zijn binnen alle factoren, uitgezonderd factor 6, positief, oftewel een hoger kennisniveau gaat samen met het (vaker) vertonen van het gewenste, veilige gedrag. Binnen factor 6 zien we namelijk een negatief verband tussen de algemene houding versus de eigen ervaring met cyber security en de netwerkbeveiliging. Naarmate men meer ervaring met cyber criminaliteit heeft en minder van mening is dat je je als individu niet toch niet kunt weren tegen cyber criminaliteit, hoe beter de beveiliging van het draadloos netwerk thuis.
- Overkoepelend zien we dat de doelgroepen Rijksoverheid, vitale sectoren en het algemene bedrijfsleven in bredere zin cyber security aware zijn dan gemeenten en burgers: zij scoren vaker op meerdere (drie tot vijf van de zes) factoren hoog.

Conclusies

- De inhoudelijke bekendheid met cyber security is onder alle doelgroepen toegenomen ten opzichte van vorig jaar en wordt vaker dan vorig jaar geassocieerd met privacy. Toch is een aanzienlijk deel van alle doelgroepen spontaan nog niet inhoudelijk bekend met cyber security.
- Cyber security wordt gezien als een gedeelde verantwoordelijkheid: burgers en professionals zien hierin dus ook een rol voor zichzelf weggelegd.
- Ondanks de gestegen inhoudelijke bekendheid en het verantwoordelijkheidsbesef, is de risicoperceptie nog tamelijk beperkt.
  - De meerderheid van alle doelgroepen vindt zichzelf voldoende bewust van de risico's van internet, maar niet iedereen (ongeveer de helft) voelt zich hiertegen ook voldoende beschermd.
  - Bij burgers is de risico-perceptie lager dan bij professionele doelgroepen. Ook voelen zij zich minder weerbaar tegen internetrisico's. Ze vinden privacy-risico's nog altijd aannemelijker dan financieel-economische risico's.
- Wat betreft een veilig wachtwoordgebruik zijn er nauwelijks verschillen tussen de doelgroepen. Het gebruik van wachtwoorden is op meerdere aspecten minder veilig geworden dan vorig jaar, ook bij de vitale sectoren.

- In de cyber security awareness op het werk (aandacht voor digitale veiligheid op het werk, verankering in beleid, structurele uitvoering en naleving van beleid) zijn bij alle doelgroepen ontwikkelingen te zien ten opzichte van vorig jaar, die positief en/of negatief van aard zijn.
  - Bij alle professionals zijn in meer of mindere mate nog stappen te maken.
  - Er is een discrepantie tussen het beeld dat leidinggevenden van de cyber security awareness van hun medewerkers en het beeld dat leeft bij medewerkers zelf: medewerkers schatten hun eigen cyber security awareness rooskleurig in. Ook vinden ze hun digitale veiligheid beter dan die van collega's.
  - De rangordering van de professionals op de cyber security ladder (op basis van hun relatieve positie ten opzichte van elkaar op basis van de huidige onderzoeksresultaten) is als volgt:

1) De Rijksoverheid springt er wat dat aangaat positief uit: de cyber security awareness is over de hele linie gestegen en ligt vaak op het hoogste niveau van alle doelgroepen.
2) De vitale sectoren nemen nu de tweede plek in op de cyber security awareness ladder. Hoewel het bewustzijn en de kennis van medewerkers nog steeds op een hoog niveau ligt en soms is toegenomen, is hun gedrag soms wat onveiliger geworden. Voornaamste punt is echter gelegen in het organisatiebeleid: daarin is de aandacht voor de zachte factor "personeel" verslapt.
3) Het bedrijfsleven neemt de derde plaats in. Hoewel er binnen deze doelgroep een aantal verbeteringen zichtbaar zijn, ligt het cyber security niveau goeddeels op hetzelfde niveau als vorig jaar.
4) Gemeenten nemen een laatste plaats in. Ondanks hun sterkere bewustzijn van het belang van digitale veiligheid en de gevaren hiervoor en het feit dat er op een aantal aspecten een verbetering is te zien, is het niveau van cyber security awareness op het merendeel van de aspecten gelijk gebleven of verslechterd ten opzichte van vorig jaar. Dit niveau is structureel lager dan bij de andere professionals.

- De digitale veiligheid thuis en op het werk wordt door alle doelgroepen als voldoende ingeschat. De beoordelingen van de digitale veiligheid en het eigen bewustzijn lijken bij de Rijksambtenaren en medewerkers van vitale sectoren behoorlijk in lijn te liggen met de feitelijke situatie, maar de inschatting van de andere groepen lijkt wat optimistisch gezien hun "feitelijke" cyber security awareness.

Aanbevelingen

- Overkoepelend is het devies om vooral door te gaan met campagnes gericht op het vergroten van de cyber security awareness. Bij alle doelgroepen is immers nog lang niet iedereen voldoende doordrongen van het belang hiervan en is voldoende bekend met de risico's van internet en hoe zich hiertegen te beschermen. Gezien kennis, houding en gedrag met elkaar samenhangen is het zinvol om de communicatiedoelen hierop te richten. Een concreet aandachtspunt hierbij zou een veilig wachtwoordgebruik kunnen zijn: dit behoeft bij alle doelgroepen (in gelijke mate) verbetering.

- Een mogelijke drempel voor een effectieve campagne is het feit dat het gros zichzelf wel degelijk voldoende bewust vindt en dat de risicoperceptie tamelijk beperkt is. Dit kan worden doorbroken door mensen een spiegel voor te houden van hun “feitelijke” digitale veiligheid, zodat er (meer) een sense of urgency ontstaat en mensen meer doordrongen worden van de gevaren, het belang en de mogelijkheid om daar zelf wat aan te doen.
    - De huidige onderzoeksresultaten kunnen als “eye-opener” fungeren, maar wellicht zou ook een soort “test” ontwikkeld kunnen worden voor professionals en burgers die op een eenvoudige, snelle en ook “leuke” manier inzicht geeft in hun mate van digitale veiligheid en op basis van de uitkomsten concrete handelingsadviezen geef.
    - Hiernaast is en blijft voor professionals een belangrijke, zo niet de belangrijkste rol weggelegd voor hun leidinggevende. Zij moeten er meer op toezien dat medewerkers voldoende op de hoogte zijn en zich voldoende geïnformeerd voelen over het belang van digitale veiligheid op het werk en bedreigingen daarvoor (ongewenst gedrag), het organisatiebeleid, de uitwerking daarvan in regels en richtlijnen en hun eigen verantwoordelijkheden daarbinnen. Het is zaak zo concreet mogelijk aan te geven wat ongewenst/ onveilig en wat gewenst/veilig gedrag is en wat de consequenties van onveilig gedrag kunnen zijn. Tevens moeten leidinggevend structureler de vinger aan de pols houden wat betreft de naleving van de regels door hun medewerkers en hierop aanspreken.
- Kijken we naar de cyber security op het werk dan is er bij alle professionele doelgroepen in meer of mindere mate winst te behalen in de kennis over het organisatiebeleid, de verankering van digitale veiligheid in het organisatiebeleid, (toezien op) de naleving hiervan en het geven van feedback hierover. In de volgende paragraaf staan per doelgroep onder “conclusies” specifiek aangegeven welke aspecten verbetering behoeven. Duidelijk is in ieder geval dat de doelgroep gemeenten met prioriteit aandacht behoeven.
- Bij het eventuele gebruik van het thema Smart Security in de campagne is het van belang rekening te houden met het feit dat een groot deel van alle doelgroepen niet bekend is met de subthema’s Smart Cities en Smart Coalitions. Er is dus niet veel voorkennis aanwezig. De vraag is ook hoe het thema zich verhoudt tot de diverse doelgroepen: what’s in it for them?

Samenvatting per doelgroep ten aanzien van cyber security

Rijksoverheid

Conclusie

- Er is duidelijk sprake van een stijgende lijn binnen de Rijksoverheid op het gebied van digitale veiligheid.
- Toch is hierin nog wel een weg te gaan. Nuancering bij bovenstaande bevindingen is namelijk dat het absolute niveau van cyber security awareness bij Rijksambtenaren op een aantal aspecten nog zeker voor verbetering vatbaar is. Hierbij gaat het zowel om kennis, gedrag als beleid:

- *Kennis:*
  - De spontane bekendheid met cyber security en bedreigingen daarvan (ongeveer de helft is hier niet mee bekend);
  - De bekendheid met het organisatiebeleid rondom digitale veiligheid en zwakke plekken in de organisatie (respectievelijk een derde en de helft is hier niet mee bekend)
- *Beleid:*
  - De verankering van diverse aspecten van beleid in de organisatie zoals back-up beleid, beleid voor het updaten van beveiligingssoftware, beleid voor internetgebruik en beleid voor het gebruik van usb-sticks (dit is bij een kwart tot een derde nog niet geborgd);
- *Gedrag en uitvoering beleid:*
  - Een veilig gebruik van wachtwoorden.
  - Het structureel naleven van het beleid op diverse aspecten (een aanzienlijk deel geeft aan dat dit niet van toepassing is of niet te weten of het van toepassing is), zoals feedback bij incidenten, aandacht voor digitale veiligheid bij de komst en het vertrek van medewerkers, aandacht voor digitale veiligheid in functioneringsgesprekken, het naleven van veiligheidsprotocollen, voorzichtig omgaan met digitale netwerken (zoals openbare Wi-Fi-verbindingen en VPN) en apparaten die buiten de organisatie zijn geweest.
  - Toezien op naleving van de regels rondom digitale veiligheid bij collega's (ongeveer de helft doet dit nog niet).

Samenvatting

Beeld cyber security

- De meerderheid van de Rijksambtenaren heeft een concreet beeld bij cyber security. Zij associëren dit vooral met beveiliging tegen aanvallen van buitenaf (via antivirussoftware, bescherming van het netwerk) en bescherming van de privacy (via firewalls en wachtwoorden).

Verantwoordelijkheidstoedeling

- Cyber security wordt als een gedeelde verantwoordelijkheid gezien van vooral de IT-afdeling en de werknemers zelf. Toch legt een aanzienlijke groep Rijksambtenaren de verantwoordelijkheid voor digitale veiligheid buiten zichzelf.

Risicoperceptie

- Het leeuwendeel van de Rijksambtenaren vindt zichzelf voldoende bewust van de gevaren van internet en ongeveer de helft voelt zich op dit moment voldoende beschermd tegen internetrisico's.
- Het merendeel is niet heel veel zorgen hierover.

Cyber secure kennis en gedrag rondom veilig wachtwoordgebruik

- Rijksambtenaren zijn dit jaar iets minder uitgesproken over hun wachtwoordveiligheid dan vorig jaar; ze beoordeling dat vaker met een voldoende (6-7) in plaats van een ruim voldoende of onvoldoende. De gemiddelde beoordeling is onveranderd (7,1).
- Hun wachtwoordsterkte, wat betreft het toepassen van drie eigenschappen (het gebruiken van fictieve woorden, speciale tekens en meer dan tien karakters) van wachtwoorden is echter op hetzelfde niveau als vorig jaar gebleven. Ook nu voldoen de wachtwoorden niet altijd aan deze drie eigenschappen. Weliswaar gebruikt de meerderheid (vijf tot zes op de tien) wachtwoorden met fictieve woorden en met speciale tekens, minder dan de helft (vier op de tien) hanteert wachtwoorden met meer dan tien karakters.
- Het gebruik van wachtwoorden, wat betreft het gebruiken van afzonderlijke wachtwoorden voor accounts en het wisselen van wachtwoorden, is – net als bij andere doelgroepen - wat onveiliger geworden ten opzichte van vorig jaar. Zo hebben Rijksambtenaren vaker verschillende wachtwoorden waarvan ze sommige voor meerdere accounts gebruiken en hebben ze minder vaak een ander wachtwoord voor ieder account. Bovendien wisselen ze minder vaak hun wachtwoorden op eigen initiatief maar vaker alleen na een melding. Ook wisselen ze minder regelmatig de belangrijkste wachtwoorden dan vorig jaar.
- Kortom: de wachtwoorden van Rijksambtenaren zijn niet altijd even sterk en nog lang niet iedereen gaat op een veilige manier met wachtwoorden om.

Cyber security op het werk: aandacht voor digitale veiligheid door werkgever, verankering in beleid, uitvoering en naleving beleid

- Zowel binnen de Rijksoverheid als de andere professionele doelgroepen kan een groot deel (nagenoeg de helft) niet spontaan aangeven welke online handelingen een risico voor de digitale veiligheid van de werkgever vormen.
- Los van deze beperkte spontane bekendheid met voor de werkgever risicovolle online handelingen van medewerkers, is binnen de Rijksoverheid over de hele linie een stijging te zien rondom cyber security op het werk.
    - Zowel de aandacht voor digitale veiligheid op het werk (rapportcijfer 8,5) als het verankeren van diverse aspecten van digitale veiligheid in het organisatiebeleid is toegenomen ten opzichte van verleden jaar. Zo is er nu bij de *ruime* meerderheid beleid voor de omgang met apparaten, internet, back-ups, incidenten, wachtwoordgebruik en beveiligingssoftware.
    - Het beleid wordt ook vaker structureel uitgevoerd en nageleefd dan verleden jaar. Zo krijgen nagenoeg alle Rijksambtenaren uitleg over het digitaal veilig gebruik van hun apparaten en worden er onder meer vaker maatregelen rondom de digitale veiligheid uitgevoerd bij het vertrek van medewerkers, worden nieuwe medewerkers vaker ingewerkt op dit gebied en zorgen leidinggevenden er vaker voor dat medewerkers op de hoogte zijn van het digitale veiligheidsbeleid. Bovendien maakt naleving van het beleid vaker deel uit van functioneringsgesprekken.
    - Net als vorig jaar is de cyber security awareness van medewerkers qua kennis en gedrag op het werk (op enkele aspecten na) op een hoog niveau en op meerdere aspecten toegenomen.

Kennis:

- Vrijwel alle ondervraagden weten bijvoorbeeld welke informatie gevoelig is, het leeuwendeel weet waar een incident te melden en hoe hierbij te handelen, waar op te letten bij links in ontvangen e-mails en welke websites al dan niet te bezoeken.
- Ook is in de ogen van medewerkers hun bewustzijn van de gevaren rondom digitale veiligheid toegenomen, evenals hun bekendheid met waar een incident te melden.

Gedrag:

- Er is een toename te zien in de omvang van de groep Rijksambtenaren die nooit bedrijfsgevoelige informatie deelt via e-mail, de cloud en/of een usb-stick, de groep die zijn computer niet door anderen laat gebruiken en de groep die zijn usb-stick laat checken op virussen als die buiten de organisatie is geweest.
- Verder zien Rijksambtenaren vaker dan vorig jaar toe op de onderlinge naleving van het beleid: zij stimuleren collega's meer zich volgens de regels te gedragen en wijzen collega's erop wanneer zij de regels niet goed naleven.

- Ook in de ogen van leidinggevenden is een verbetering te zien bij medewerkers: zo zijn medewerkers zich volgens leidinggevenden bewuster van het belang en de gevaren van digitale veiligheid, zijn zij beter op de hoogte van hun eigen verantwoordelijkheden en het organisatiebeleid en leven zij het beleid strikter na.

Beoordeling digitale veiligheid op het werk en thuis

- De verbetering in de cyber security van Rijksambtenaren worden weerspiegeld in het beeld dat zij hebben van de digitale veiligheid op het werk: ze zijn dit jaar positiever over de digitale veiligheid van hun werkgever, zichzelf als werknemer én hun collega's van (8,5, 8,2, 7,7).
- De digitale veiligheid thuis wordt ook dit jaar als relatief minder veilig beschouwd dan de digitale veiligheid op het werk en ligt op hetzelfde niveau als vorig jaar (7,4).

Gemeenten

Conclusie

- Bij gemeenteambtenaren is op een aantal aspecten van cyber security awareness een verbetering in de tijd te zien (een toename van het geïnstrueerd zijn over een veilig digitaal gebruik van apparaten, een zorgvuldige omgang met het werken in een digitale omgeving; verankering in beleid op twee aspecten). Toch is op het merendeel van de aspecten is het niveau gelijk gebleven of afgenomen ten opzichte van vorig jaar. Des te opvallender is het, dat medewerkers zelf van mening zijn dat hun bewustzijn is verbeterd.
- Het absolute niveau van gemeenteambtenaren is veelal structureel lager dan bij andere professionals. Gemeenten hebben dan ook nog een behoorlijke stap te maken als het gaat om hun cyber security awareness. Hierbij gaat het zowel om kennis en bewustzijn, gedrag als beleid:

- *Kennis:*
  - De spontane bekendheid met cyber security en de bedreigingen daarvan (respectievelijk een vijfde en een derde is hier niet mee bekend).
  - De bekendheid met het organisatiebeleid met betrekking tot digitale veiligheid, hoe te handelen en waar zich in de organisatie zwakke plekken bevinden.
- *Beleid:*
  - De verankering van diverse aspecten van beleid in de organisatie zoals beleid voor de omgang met apparaten, beleid voor het melden van incidenten, beleid voor internetgebruik, back-upbeleid, beleid voor het updaten van beveiligingssoftware en beleid voor de omgang met usb-sticks (dit is bij een derde tot tweederde nog niet geborgd).
- *Gedrag en uitvoering beleid:*
  - Een veilig gebruik van wachtwoorden.
  - Een structurele uitvoering en naleving van het beleid: bij meerdere aspecten geeft een aanzienlijk deel geeft aan dat dit niet van toepassing is of niet te weten of het van toepassing is). Hierbij gaat het onder meer om: (toezien op) het voldoende bewust en op de hoogte zijn van medewerkers rondom het belang van digitale veiligheid, de bedreigingen hiervoor, het organisatiebeleid en hun eigen verantwoordelijkheid, het feedback bij incidenten, aandacht voor digitale veiligheid bij de komst en het vertrek van medewerkers, aandacht voor digitale veiligheid in functioneringsgesprekken, het naleven van veiligheidsprotocollen, voorzichtig omgaan met digitale netwerken en apparaten die extern zijn geweest.
  - Toezien op naleving van de regels rondom digitale veiligheid bij collega's.

Samenvatting

Beeld cyber security

- De ruime meerderheid van de gemeenteambtenaren heeft een concreet beeld bij Cyber Security; zij hebben hier het vaakst een beeld bij van alle doelgroepen. Het accent in hun associaties ligt minder dan bij de andere groepen op antivirussoftware en wat vaker bij andere aspecten zoals wachtwoorden, privacy, hacken, beveiliging computer en netwerk.

Verantwoordelijkheidstoedeling

- Gemeenteambtenaren beschouwen digitale veiligheid als een gedeelde verantwoordelijkheid van de IT-afdeling en zichzelf, waarbij zij het vaker als de eigen verantwoordelijkheid beschouwen dan medewerkers van vitale sectoren en het bedrijfsleven.

Risicoperceptie

- Ruim tweederde van de gemeenteambtenaren acht zichzelf voldoende bewust van de risico's van internet en de meerderheid (méér dan vorig jaar) vindt zichzelf voldoende bewust van de gevaren rondom digitale veiligheid.
- Zij maken zich – vaker dan de andere doelgroepen- zorgen over hun digitale veiligheid in het algemeen en over de bescherming van hun privacy in het bijzonder en voelen ze zich minder beschermd tegen de risico's van internet. Ze zien de risico's ook meer als een bedreiging voor henzelf dan burgers en medewerkers van de vitale sectoren.

Cyber secure kennis en gedrag rondom veilig wachtwoordgebruik

- Gemeenteambtenaren zijn dit jaar positiever (gemiddeld rapportcijfer dit jaar 6,9 versus een 6,6 in 2012) over hun wachtwoordveiligheid dan in 2012; ze beoordelen dit minder vaak met een onvoldoende dan vorig jaar.
- Hun wachtwoordsterkte, wat betreft het toepassen van drie eigenschappen (het gebruiken van fictieve woorden, speciale tekens en meer dan tien karakters) van wachtwoorden is op één aspect verbeterd ten opzichte van verleden jaar: ze bevatten vaker speciale tekens. Ook nu voldoen de wachtwoorden echter nog lang niet altijd aan deze drie eigenschappen. Weliswaar gebruikt de meerderheid (tussen de vijf en zes op de tien) wachtwoorden met fictieve woorden en met speciale tekens, minder dan de helft (een derde) hanteert wachtwoorden met meer dan tien karakters.
- Het gebruik van wachtwoorden, wat betreft het gebruiken van afzonderlijke wachtwoorden voor accounts en het wisselen van wachtwoorden, is – net als bij andere doelgroepen - wat onveiliger geworden ten opzichte van vorig jaar. Gemeenteambtenaren hanteren vaker verschillende wachtwoorden waarvan ze sommige voor meerdere accounts gebruiken en hebben minder vaak een ander wachtwoord voor ieder account. Bovendien wisselen ze minder vaak hun wachtwoorden op eigen initiatief maar vaker alleen na een melding. Ook wisselen ze minder regelmatig de belangrijkste wachtwoorden dan vorig jaar.
- Kortom: de wachtwoorden van Gemeenteambtenaren zijn niet altijd even veilig sterk. Bovendien gaat een aanzienlijk deel nog niet op een veilige manier met wachtwoorden om.

Cyber security op het werk: aandacht voor digitale veiligheid door werkgever, verankering in beleid, uitvoering en naleving beleid

- Zowel binnen de gemeenten als de andere professionele doelgroepen kan een groot deel niet spontaan aangeven welke online handelingen een risico vormen voor de digitale veiligheid van de werkgever. De spontane bekendheid hiermee is echter wel hoger onder gemeenten dan bij de andere doelgroepen (een derde versus de helft weet niet).
- Afgezien van deze hogere spontane bekendheid met voor de werkgever risicovolle online handelingen, is de cyber security op het werk bij gemeenten gelijk gebleven ten opzichte van vorig jaar of indien deze veranderd is, vaker af- dan toegenomen.

- De aandacht voor digitale veiligheid door de werkgever is weliswaar op een gelijk en voldoende niveau gebleven als vorig jaar (7,5), maar is lager en minder vaak *ruim* voldoende dan de aandacht hiervoor bij werkgevers in de andere doelgroepen. Dit strookt met de mate waarin digitale veiligheid in de gemeentelijke organisaties is verankerd en wordt uitgevoerd: gemeenten doen het op dit gebied vaak minder goed dan andere doelgroepen en waar er sprake is van ontwikkelingen in de tijd gaat het vaker om een afname dan een toename. Zo is er bij gemeenten sprake van een afname van het hebben van een beleid voor alle werknemers rondom de digitale omgeving. Wat betreft het vastleggen van specifieke aspecten van digitale veiligheid in organisatiebeleid, zien we een toename wat betreft beleid voor veilig wachtwoordgebruik en voor de omgang met apparaten, maar een afname wat betreft het back-up beleid.
- Het beleid wordt bovendien minder structureel uitgevoerd dan bij de andere doelgroepen: gemeentemedewerkers vinden voorgelegde aspecten die te maken hebben met de uitvoering van het beleid minder vaak van toepassing op hun werkgever dan de andere professionals. Zo weet de meerderheid niet hoe te handelen bij incidenten, worden nieuwe medewerkers in de meeste gevallen niet ingewerkt op dit gebied en worden bij vertrekkende medewerkers in de meeste gevallen geen digitale veiligheidsmaatregelen uitgevoerd. Van alle zakelijke doelgroepen voelen gemeenten zich ook het minst goed geïnformeerd over het digitale veiligheidsbeleid. Wat betreft de feedback na een incident en het toezien van leidinggevenden op het voldoende op de hoogte zijn van medewerkers over het beleid, is bovendien een daling te zien ten opzichte van vorig jaar. Positieve uitschieter is de informatievoorziening over een veilig gebruik van apparaten voor het werk: driekwart van de gemeenteambtenaren heeft hier een instructie voor gehad en dat is een toename in de tijd.

- Net als vorig jaar is de cyber security awareness van gemeenteambtenaren qua kennis over veilig digitaal gedrag op het werk en gedrag zelf lager dan bij andere professionals en vaak op een tamelijk laag niveau.
  Kennis:
  - Net als vorig jaar weet een aanzienlijk deel van de gemeenteambtenaren (en meer dan bij andere doelgroepen) niet of er een organisatiebeleid voor diverse aspecten van de digitale veiligheid is.
  - Ook zijn gemeentemedewerkers minder goed dan andere professionals op de hoogte van welke informatie gevoelig is, wat te doen bij een incident, waar ze op moeten letten bij een link in een e-mail, welke websites al dan niet te bezoeken en van de zwakke plekken in de organisatie.
  - Dit staat enigszins in contrast met de perceptie van medewerkers over zichzelf: zoals eerder geconcludeerd vindt de meerderheid zichzelf voldoende cyber aware en is deze groep zelfs iets gestegen in de tijd.

Gedrag:

- Het digitale gedrag van gemeenteambtenaren is op twee aspecten verbeterd ten opzichte van vorig jaar (het zorgvuldig omgaan met handelingen bij gebruik van een openbare Wi-Fi-verbinding en het gebruik van een VPN verbinding voor het werk) en verder op een gelijk niveau gebleven qua veiligheid. Een niveau dat lager ligt dan bij andere professionals; gemeenteambtenaren: delen vaker dan anderen gevoelige informatie via e-mail, laten hun zakelijke tablet of smartphone vaker door anderen gebruiken, laten vaker computers onbeheerd achter en laten een usb-stick van buiten de organisatie minder vaak op virussen controleren. Zij zijn ook minder geneigd om hun collega's aan te zetten tot en aan te spreken op het opvolgen van de regels.

- In de ogen van gemeentelijke leidinggevenden zijn medewerkers op diverse gebieden minder cyber security aware dan verleden jaar; niet alleen zijn zij minder goed op de hoogte, minder bewust en verantwoordelijk ten aanzien van digitale veiligheid, ook leven ze afspraken minder goed na. Dit staat in contract met de perceptie van medewerkers over zichzelf: de meerderheid vindt zichzelf voldoende bewust van het belang en de gevaren voor digitale veiligheid, voldoende op de hoogte van de eigen verantwoordelijkheden en is van mening dat hij of zij het beleid strikt naleeft.
- Overigens kunnen leidinggevenden ook een hand in eigen boezem steken wat betreft het huidige niveau van cyber security awareness van hun medewerkers, aangezien leidinggevenden er zelf nog altijd weinig (en ook minder dan vorig jaar) op toezien dat medewerkers op de hoogte zijn van het digitale veiligheidsbeleid en dit ook naleven.

Beoordeling digitale veiligheid op het werk en thuis

- Bovenstaand beeld komt ook naar voren in de beoordeling van gemeenteambtenaren van de digitale veiligheid van hun werkgever, van collega's en zichzelf: deze is ook dit jaar lager dan die van de andere professionele doelgroepen. Terwijl het oordeel bij de andere doelgroepen is gestegen, is dit bij gemeenteambtenaren onveranderd gebleven ten opzichte van verleden jaar.

Vitale sectoren

Conclusie

- Hoewel security awareness nog steeds tamelijk hoog in het vaandel staat bij vitale sectoren, zijn hierin tegelijkertijd scheurtjes (een afname) zichtbaar. Als gevolg van de verslechtering op meerdere aspecten van cyber security ten opzichte van vorig jaar, zijn de vitale sectoren wat betreft het absolute niveau van cyber security dit jaar geen koploper meer. De Rijksoverheid heeft dat stokje dit jaar overgenomen en de vitale sectoren bevinden zich tussen de Rijksoverheid en bedrijfsleven in.
- De vitale sectoren hebben dus zeker nog stappen te maken om de dalende trend om te buigen en het absolute niveau van cyber security awareness te verbeteren. Hierbij gaat het zowel om kennis, gedrag en beleid:

- *Kennis:*
  - De spontane bekendheid met cyber security en de bedreigingen daarvan (respectievelijk een derde en de helft is hier niet mee bekend).
  - Het bewustzijn van het belang van digitale veiligheid en de risico's hieromtrent, de bekendheid met het organisatiebeleid met betrekking tot digitale veiligheid, hun eigen verantwoordelijkheid, hoe te handelen en waar zich in de organisatie zwakke plekken bevinden. Werknemers hebben een rooskleurig beeld hiervan met betrekking tot zichzelf dan leidinggevenden.
- *Beleid:*
  - Het borgen van een adequaat niveau van cyber security awareness bij het personeel via eenduidige informatie/kennisdeling over: het belang van en de risico's voor digitale veiligheid, de eigen rol, een veilig gebruik van apparaten.
  - Het verankeren van regels en protocollen in organisatiebeleid.
- *Gedrag en uitvoering beleid:*
  - Een veilig gebruik van wachtwoorden.
  - Een structurele uitvoering en naleving van het beleid; dit is het grootste pijnpunt binnen de vitale sectoren: bij meerdere beleidsaspecten geeft een aanzienlijk deel aan dat dit niet ten uitvoer wordt gebracht in de praktijk. Hierbij gaat het onder meer om: (toezien op) het voldoende bewust en op de hoogte zijn van medewerkers rondom het belang van digitale veiligheid, de bedreigingen hiervoor, het organisatiebeleid en hun eigen verantwoordelijkheid, het geven van feedback bij incidenten, aandacht voor digitale veiligheid bij de komst en het vertrek van medewerkers, aandacht voor digitale veiligheid in functioneringsgesprekken, het naleven van veiligheidsprotocollen, voorzichtig omgaan met openbare digitale netwerken en apparaten die buiten de organisatie zijn geweest.
  - Toezien op naleving van de regels rondom digitale veiligheid bij collega's.

Samenvatting

Beeld cyber security

- Het merendeel van de medewerkers van vitale sectoren heeft een beeld bij cyber security. Dominante elementen hierin zijn beveiliging tegen aanvallen van buitenaf en bescherming van de privacy. Privacy is een sterkere associatie dan vorig jaar.

Verantwoordelijkheidstoedeling

- Cyber security wordt vooral als een gedeelde verantwoordelijkheid gezien van de IT-afdeling en werknemers.

Risicoperceptie

- Het overgrote deel van de werknemers van vitale sectoren (driekwart) vindt zichzelf voldoende bewust van de risico's van internet en ongeveer de helft voelt zich voldoende beschermd tegen de internetrisico's.
- Verder is het gros niet erg bezorgd om de risico's. Het feit dat men in een vitale sector werkt, uit zich dus niet in meer zorgen om de digitale veiligheid dan bij andere, niet-vitale sectoren.

Cyber secure kennis en gedrag rondom veilig wachtwoordgebruik

- De beoordeling van de wachtwoordsterkte is bij medewerkers van vitale sectoren hetzelfde als vorig net als vorig jaar met een voldoende (2013 en 2012: 7,1).
- Verder gaan ze al met al nog altijd zorgvuldig met hun wachtwoorden om. Zij gebruiken voor belangrijke zaken vaker afzonderlijke wachtwoorden dan verleden jaar, maar het regelmatig wisselen van de belangrijkste wachtwoorden is afgenomen.
- Hun wachtwoordsterkte, wat betreft het toepassen van drie eigenschappen (het gebruiken van fictieve woorden, speciale tekens en meer dan tien karakters) van wachtwoorden is op hetzelfde niveau als vorig jaar. Ook dit jaar voldoen de wachtwoorden nog lang niet altijd aan deze drie eigenschappen. Weliswaar gebruikt de meerderheid (tussen de vijf en zes op de tien) wachtwoorden met fictieve woorden en met speciale tekens, minder dan de helft (vier op de tien) hanteert wachtwoorden met meer dan tien karakters.
- Het gebruik van wachtwoorden, wat betreft het gebruiken van afzonderlijke wachtwoorden voor accounts en het wisselen van wachtwoorden, is – net als bij andere doelgroepen - wat onveiliger geworden ten opzichte van vorig jaar. Werknemers in vitale sectoren hanteren vaker dan vorig jaar verschillende wachtwoorden waarvan ze sommige voor meerdere accounts gebruiken, gebruiken nu minder vaak voor belangrijke zaken een ander wachtwoord gebruikt en voor onbelangrijke accounts één wachtwoord en hebben minder vaak een ander wachtwoord voor ieder account. Bovendien wisselen ze minder vaak hun wachtwoorden op eigen initiatief maar vaker alleen na een melding. Ook wisselen ze minder regelmatig de belangrijkste wachtwoorden dan vorig jaar.
- Kortom: wachtwoorden van medewerkers van vitale sectoren zijn niet altijd even veilig. Bovendien gaat een aanzienlijk deel nog niet op een veilige manier met wachtwoorden om.

Cyber security op het werk: aandacht voor digitale veiligheid door werkgever, verankering in beleid, uitvoering en naleving beleid

- Zowel binnen de vitale sectoren als de andere professionele doelgroepen kan een groot deel niet spontaan aangeven welke online handelingen een risico vormen voor de digitale veiligheid van de werkgever. De spontane bekendheid hiermee is binnen vitale sectoren op een gelijk niveau als binnen de Rijksoverheid en het bedrijfsleven (de helft weet het niet).

- Los van deze wat beperkte spontane bekendheid met voor de werkgever risicovolle online handelingen, ligt de cyber security op het werk bij vitale sectoren op veel aspecten op hetzelfde (tamelijk hoge) niveau als vorig jaar. Dat geldt echter niet voor alle aspecten: op een aantal aspecten is een verslechtering te zien ten opzichte van 2012.
    - De aandacht voor digitale veiligheid op het werk (in 2013 en 2012 een 8,3) en de verankering voor een veilig gebruik van apparaten, internet, wachtwoorden et cetera ("harde aspecten") in beleid is binnen de vitale sectoren onveranderd op een relatief hoog niveau.
    - Opvallend is echter dat de aandacht voor "zachte aspecten", namelijk het personeel, wat is verslapt. Zo is er minder vaak beleid voor alle werknemers met betrekking tot de digitale werkomgeving, worden nieuwe medewerkers minder vaak ingewerkt rondom veilig digitaal werken, ontvangen medewerkers minder vaak instructies over een veilig gebruik van apparatuur, zien leidinggevenden minder toe op bekendheid bij medewerkers met het organisatiebeleid en maakt het naleven van de regels in minder gevallen deel uit van functioneringsgesprekken.
- Net als vorig jaar is de cyber security awareness van medewerkers qua kennis en gedrag op het werk (op enkele aspecten na) op een hoog niveau. De kennis is op enkele aspecten toegenomen, terwijl het gedrag op een aantal aspecten is verbeterd en op enkele aspecten is verslechterd.

  Kennis:
    - Werknemers in de vitale sectoren zijn net als vorig jaar goed op de hoogte van welke informatie gevoelig is, hoe te handelen bij een incident, waar op te letten bij links in e-mails en welke websites al dan niet te bezoeken. Hierin lijkt sprake te zijn van een stijging ten opzichte van verleden jaar. Kennis over de zwakke plekken in de organisatie is echter nog niet alom aanwezig.
    - Het bewustzijn van het belang van en de gevaren voor digitale veiligheid, de kennis van het organisatiebeleid en de eigen verantwoordelijkheden en de naleving van het beleid is op hetzelfde hoge niveau als vorig jaar.

  Gedrag:
    - Werknemers in de vitale sectoren gaan zorgvuldiger dan vorig jaar om met het delen van gevoelige informatie: ze delen minder vaak gevoelige informatie per e-mail, in de cloud en via usb-sticks.
    - Daarentegen gaan ze wat minder bewust om met openbare wifi-verbindingen en laten ze usb-sticks van buiten minder vaak controleren op virussen.
    - Ook attenderen ze collega's minder vaak op de regels en stimuleren ze hen minder vaak zich eraan te houden.
- In de ogen van leidinggevenden in vitale sectoren is het bewustzijn, de kennis en het gedrag van medewerkers op een gelijk niveau als vorig jaar. Opvallend is dat werknemers een positiever beeld van hun eigen bewustzijn, kennis en gedrag hebben dan leidinggevenden.

Beoordeling digitale veiligheid op het werk en thuis

- De op sommige aspecten wat afgenomen cyber security awareness komt niet tot uiting in de beoordeling van de respondenten van de digitale veiligheid van de werkgever, collega's en zichzelf als werknemer: hierover zijn zij nog steeds positief, over hun werkgever en collega's zijn zij op dit gebied zelfs nog wat positiever dan vorig jaar. Over hun digitale veiligheid thuis zijn ze juist minder te spreken dan vorig jaar.

Bedrijfsleven

Conclusie

- Hoewel op een aantal aspecten van cyber security een positieve ontwikkeling te zien is binnen het bedrijfsleven, ligt het cyber security niveau grotendeels op gelijk niveau als vorig jaar. Daarmee neemt het bedrijfsleven de derde plaats in ten opzichte van de andere professionele doelgroepen. Kijkend hiernaar en het absolute niveau van cyber security awareness in kennis, beleid en gedrag dan is zijn er nog de nodige stappen te maken.

    - *Kennis:*
        - De spontane bekendheid met cyber security en de bedreigingen daarvan (respectievelijk een derde en de helft is hier niet mee bekend).
        - Het bewustzijn van het belang van digitale veiligheid en de risico's hiervoor, de bekendheid met het organisatiebeleid en de eigen verantwoordelijkheid, hoe te handelen en waar zich in de organisatie zwakke plekken bevinden. Werknemers hebben een rooskleuriger beeld hiervan met betrekking tot zichzelf dan leidinggevenden.
    - *Beleid:*
        - Het zorgen voor voldoende kennis bij het personeel over het organisatiebeleid en hoe te handelen.
        - Het verankeren van regels en protocollen in organisatiebeleid.
    - *Gedrag en uitvoering beleid:*
        - Een veilig gebruik van wachtwoorden.
        - Een structurele uitvoering en naleving van het beleid. Hier kan winst worden geboekt aangezien bij meerdere beleidsaspecten een aanzienlijk deel meldt dat dit niet wordt uitgevoerd. Hierbij gaat het onder andere om: toezien door leidinggevende op het voldoende bewust en op de hoogte zijn van medewerkers rondom het organisatiebeleid en dit op de agenda zetten in functionerings-gesprekken, het geven van feedback bij incidenten, aandacht voor digitale veiligheid bij de komst en het vertrek van medewerkers, het strikt naleven van veiligheidsprotocollen, voorzichtig omgaan met openbare digitale netwerken en apparaten die buiten de organisatie zijn geweest.
        - Toezien op naleving van de regels rondom digitale veiligheid bij collega's.

Samenvatting

Beeld cyber security

- De meerderheid van de medewerkers van het bedrijfsleven heeft een beeld bij cyber security. Men denkt hierbij vooral aan antivirussoftware en firewalls. Bescherming van de privacy wordt wat vaker genoemd dan in 2012.

Verantwoordelijkheidstoedeling

- Medewerkers van het bedrijfsleven vinden cyber security zowel de verantwoordelijkheid van de IT-afdeling als de werknemers zelf, waarbij het accent ligt op de IT-afdeling.

Risicoperceptie

- Tweederde van de medewerkers van het bedrijfsleven vindt zichzelf voldoende bewust van de gevaren van internet en ongeveer de helft voelt zich voldoende beschermd tegen internetrisico's. Zij zijn niet erg bezorgd om hun digitale veiligheid.

Cyber secure kennis en gedrag rondom veilig wachtwoordgebruik

- Wat betreft veilig wachtwoordgebruik geven medewerkers van het bedrijfsleven zichzelf vaker een ruim voldoende (8 of hoger) dan een voldoende, al blijft het gemiddelde gelijk aan vorig jaar.
- Hun wachtwoordsterkte, wat betreft het toepassen van drie eigenschappen (het gebruiken van fictieve woorden, speciale tekens en meer dan tien karakters) van wachtwoorden is op hetzelfde niveau als vorig jaar. Ook dit jaar voldoen de wachtwoorden nog lang niet altijd aan deze drie eigenschappen. Weliswaar gebruikt de meerderheid (tussen de vijf en zes op de tien) wachtwoorden met fictieve woorden en met speciale tekens, minder dan de helft (vier op de tien) hanteert wachtwoorden met meer dan tien karakters.
- Het gebruik van verschillende wachtwoorden voor accounts is onveranderd ten opzichte van vorig jaar en ligt nu op een lijn met de andere doelgroepen. Relatief de grootste groep (twee vijfde) heeft een aantal verschillende wachtwoorden waarvan ze sommige gebruiken voor meerdere accounts of een ander wachtwoord bij belangrijke zaken (een kwart). Het gebruik wat betreft het wisselen van wachtwoorden is net als bij de andere groepen onveiliger geworden; er wordt minder vaak van wachtwoord gewisseld en dit gebeurt bovendien vaker alleen naar aanleiding van een melding.
- Kortom: wachtwoorden van medewerkers van het bedrijfsleven niet altijd even veilig. Bovendien gaat een aanzienlijk deel nog niet op een veilige manier met wachtwoorden om.

Cyber security op het werk: aandacht voor digitale veiligheid door werkgever, verankering in beleid, uitvoering en naleving beleid

- Zowel binnen het bedrijfsleven als de andere professionele doelgroepen kan een groot deel niet spontaan aangeven welke online handelingen een risico vormen voor de digitale veiligheid van de werkgever. De spontane bekendheid hiermee is op een gelijk niveau als binnen de Rijksoverheid en de vitale sectoren (de helft weet het niet).
- Binnen het bedrijfsleven ligt de cyber security op het werk op een gelijk of soms hoger niveau dan vorig jaar:
  - Zowel de aandacht voor digitale veiligheid op het werk (rapportcijfer 8) als het verankeren van diverse aspecten van digitale veiligheid in het organisatiebeleid is toegenomen ten opzichte van verleden jaar. Zo is er nu vaker beleid voor wachtwoord-gebruik, de omgang met apparaten, het updaten van beveiligingssoftware en de omgang met USB-sticks.
  - De uitvoering van beleid ligt hoofdzakelijk op hetzelfde niveau als vorig jaar: diverse aspecten van het beleid (zoals het inwerken van nieuwe medewerkers, het informeren van medewerkers) wordt in ongeveer de helft van de gevallen uitgevoerd. Op enkele aspecten is een verbetering te zien: medewerkers worden vaker geïnstrueerd over een veilig gebruik van apparaten en gaan bewuster om met werken in een digitale omgeving.
- De cyber security awareness qua kennis en gedrag van medewerkers ligt zowel in de ogen van medewerkers zelf als hun leidinggevenden op een gelijk niveau als vorig jaar.
  Kennis:
  - Het bewustzijn van het belang van en de gevaren voor digitale veiligheid, de kennis van het organisatiebeleid en de eigen verantwoordelijkheden ligt op hetzelfde niveau als vorig jaar: bij de meerderheid van de werknemers is deze kennis aanwezig en evenzo is deze bij een aanzienlijk groep (een derde of meer) nog niet aanwezig.
  - Medewerkers van het bedrijfsleven zijn (net als gemeenteambtenaren) minder goed dan Rijksambtenaren en medewerkers van vitale sectoren op de hoogte van hoe te handelen bij een incident dat de digitale veiligheid in gevaar brengt, waar op te letten bij links in e-mails, welke websites te bezoeken en van waar de zwakke plekken in de digitale veiligheid van de organisatie zich bevinden.

  Gedrag:
  - De naleving van regels en veiligheidsprotocollen ligt op hetzelfde niveau als vorig jaar. Collega's attenderen elkaar nog lang niet altijd op de regels en veiligheidsprotocollen en werknemers voeren dit zelf ook niet altijd uit.
  - Wel gaan werknemers bewuster om met openbare Wi-Fi-verbindingen.

Beoordeling digitale veiligheid

- De beoordeling van de digitale veiligheid van de werkgever is toegenomen ten opzichte van vorig jaar (8,1 dit jaar versus een 7,6 in 2012). Collega's krijgen vaker een ruim voldoende dan vorig jaar, het gemiddelde is echter gelijk gebleven (7,4). Werknemers beoordelen hun eigen digitale veiligheid op het werk (net als in andere sectoren) hoger (7,9) dan die van collega's. Deze beoordeling is tegelijkertijd lager dan die van Rijksambtenaren en werknemers in vitale sectoren. De digitale veiligheid thuis krijgt vaker een onvoldoende dan vorig jaar, het gemiddelde is onveranderd (7,5).

Burgers 13+

Conclusies

- Burgers zijn net als gemeenteambtenaren relatief het minst cyber security aware.
- Burgers vinden zichzelf meer bewust van de risico's van internet dan ze in werkelijkheid zijn getuige hun risico-perceptie, kennis en gedrag.

  Risico-perceptie en locus of control
  - Burgers hebben een tamelijk passieve houding ten aanzien van de risico's van internet. Een groot deel denkt dat ze zelf weinig kans hebben om met internetrisico's te maken te krijgen, maakt zich hier niet veel zorgen over en denkt zich hier toch niet tegen te kunnen verweren.

  Kennis:
  - Er is onder een aanzienlijke groep onbekendheid met hoe er misbruik van computers kan worden gemaakt en hoe je hiertegen te beschermen. Burgers weten minder goed dan de professionele doelgroepen hoe cookies te verwijderen.

  Gedrag:
  - Wachtwoorden van burgers zijn nog lang niet bij iedereen veilig. Bovendien gaat een aanzienlijk deel nog niet op een veilige manier met wachtwoorden om.
  - Hoewel het merendeel van de burgers bewust omgaat met het prijsgeven van persoonlijke informatie op social media, doet een noemenswaardige groep dit nog niet.
  - Burgers openen vaker dan de professionele doelgroepen e-mail van onbekenden. Ze laten juist minder vaak automatische updates van beveiligingssoftware installeren.
- Burgers zijn nog niet verzadigd wat betreft informatie over internetrisico's. drie op de tien burgers hebben hieraan behoefte of weten dat nog niet zeker (een op de tien).

Samenvatting

Beeld cyber security

- Burgers hebben vaker dan vorig jaar een beeld cyber security. Zij denken hierbij vooral aan bescherming tegen virussen door middel van firewalls en wachtwoorden. Bescherming van privacy wordt ook vaker genoemd. Een derde heeft geen beeld van cyber security.

Verantwoordelijkheidstoedeling

- Burgers leggen de verantwoordelijkheid voor privacy iets vaker buiten zichzelf dan vorig jaar, maar zien zichzelf en providers nog altijd als primair verantwoordelijken. Ze beoordelen digitale veiligheid in huis vaker met een ruim voldoende dan vorig jaar.

Risicoperceptie

- Ruim tweederde zegt zich voldoende bewust te zijn van de risico's van internet en twee vijfde voelt zich voldoende beschermd hiertegen. Opvallend is dat burgers zich vrij passief en passiever dan andere doelgroepen opstellen: de helft denkt zich toch niet te kunnen verweren tegen de gevaren van internet en is van mening dat de ontwikkelingen te snel gaan om bij te houden. Vrouwen, ouderen en hoogopgeleiden zijn zich beter bewust van risico's van internet dan mannen, jongeren en laagopgeleiden.

- Burgers maken zich dan ook niet veel zorgen om hun digitale veiligheid. Een derde maakt zich helemaal geen zorgen.
- Dat de risicoperceptie bij burgers beperkt is, blijkt ook uit het feit dat een groot deel van hen denkt dat de kans dat zij zelf met internetrisico's te maken krijgen klein is, het meest waarschijnlijk achten zij de kans op het ongewenst delen van privé-informatie met derden. Wel acht men de kans op diefstal of fraude via internet iets groter dan vorig jaar, maar nog altijd klein. Burgers zien privacyrisico's dus nog steeds als een reëlere bedreiging dan financieel-economische risico's.

Cyber secure kennis en gedrag rondom veilig wachtwoordgebruik

- Burgers beoordelen de veiligheid van hun wachtwoorden iets minder vaak met een onvoldoende dan vorig jaar, het gemiddelde is op een gelijk niveau met vorig jaar (7,1).
- Hun wachtwoordsterkte, wat betreft het toepassen van drie eigenschappen (het gebruiken van fictieve woorden, speciale tekens en meer dan tien karakters) van wachtwoorden laat een tegenstrijdige ontwikkeling zien. Ten opzichte van vorig jaar bestaan hun wachtwoorden vaker uit meer dan tien karakters, maar minder vaak uit fictieve woorden. Al met al voldoen de wachtwoorden nog lang niet altijd aan deze drie eigenschappen. Hoewel de meerderheid (zes op de tien) wachtwoorden met fictieve woorden gebruikt, gebruikt iets minder dan de helft wachtwoorden met speciale tekens en meer dan tien karakters.
- Het gebruik van wachtwoorden, wat betreft het gebruiken van afzonderlijke wachtwoorden voor accounts en het wisselen van wachtwoorden, is – net als bij andere doelgroepen - wat onveiliger geworden ten opzichte van vorig jaar. Burgers hanteren vaker dan vorig jaar verschillende wachtwoorden waarvan ze sommige voor meerdere accounts gebruiken, gebruiken nu minder vaak voor belangrijke zaken een ander wachtwoord gebruikt en voor onbelangrijke accounts één wachtwoord en hebben minder vaak een ander wachtwoord voor ieder account. Bovendien wisselen ze minder vaak hun wachtwoorden op eigen initiatief maar vaker alleen na een melding. Ook wisselen ze minder regelmatig de belangrijkste wachtwoorden dan vorig jaar.
- Kortom: wachtwoorden van burgers zijn niet altijd even veilig. Bovendien gaat een aanzienlijk deel nog niet op een veilige manier met wachtwoorden om.

Cyber secure kennis en gedrag

Kennis

- Hoewel burgers zichzelf dus behoorlijk bewust vinden van digitale veiligheid, weet tweederde niet hoe er via internet misbruik kan worden gemaakt van hun computer (een stijging ten opzichte van vorig jaar).
- Bovendien weet één op de drie niet wat te doen om zich te beschermen tegen misbruik, dit was in 2012 één op de vijf. Alleen het afschermen van privacy gevoelige informatie op sociale media wordt vaker genoemd.
- Wel is het gros van de burgers bekend met cookies.

Gedrag:

- Het merendeel van de burgers gaat bewust om met het prijsgeven van persoonlijke informatie op social media. Steeds meer mensen stellen op social media een privacy filter in en men weet ook goed hoe een dergelijk filter aangepast dient te worden. Ook wordt minder vaak online vermeld wanneer men op vakantie gaat. Daarentegen is het aantal mensen dat zoveel mogelijk persoonlijke informatie op hun profiel weergeeft dit jaar toegenomen en is deze groep noemenswaardig qua omvang net als de groep die zijn profiel voor iedereen zichtbaar maakt (beid een vijfde) en deelt waar hij of zij werkt (een derde).
- Burgers hebben vaker een Wi-Fi-netwerk thuis dan verleden jaar en beveiligen dit netwerk vaker met WPA2. De wel beveiliging heeft maar niet weet welk type, is toegenomen.
- Ondanks de grote bekendheid met cookies, weten burgers minder goed dan de overige doelgroepen hoe die verwijderd kunnen worden. Ook opent men vaker dan de andere groepen e-mail van onbekenden en laat men minder vaak automatische updates van beveiligingssoftware installeren.

Informatiebehoefte

- Ruim een kwart van de burgers heeft behoefte aan extra informatie over internetrisico's.
- Er is geen duidelijke voorkeur voor een bepaalde afzender van deze informatie. Zowel providers, consumentenorganisaties en de overheid worden door tweederde genoemd.
- Burgers gebruiken vaker wachtwoorden met minimaal 10 tekens, maar minder vaak wachtwoorden zonder woorden erin. Men geeft de eigen wachtwoorden minder vaak een onvoldoende dan vorig jaar.
- Een op de vijf schrijft zijn/haar wachtwoorden op een verstopt briefje. Men gebruikt steeds vaker meerdere wachtwoorden waarvan voor sommige diensten steeds dezelfde. Een op de vijf wisselt nooit van wachtwoord en meer dan een derde alleen als ze een melding krijgen, dat aantal is gestegen sinds 2012.

1. Inleiding

1.1 Achtergrond en doel van het onderzoek

Achtergrond
Het aantal cybermisdrijven neemt toe en cybercrime internationaliseert en criminaliseert steeds verder. Ook ons land - dat tot de top behoort wat betreft de internetpenetratie en daardoor kwetsbaar is - wordt hiermee geconfronteerd. De soms dagenlange onbereikbaarheid van onder andere DigiD, Rijksoverheid.nl, de site van de Belastingdienst en het online betalingsverkeer van de ING door DDoS-aanvallen staan nog scherp op ons netvlies.

Het is duidelijk dat digitale veiligheid, oftewel cyber security van eminent belang is om te voorkomen dat cybercrime onze samenleving en economie verstoort. Er zijn dan ook tal van initiatieven om cybercrime in te dammen, waarbij vaak sprake is van een publiek-private samenwerking om te komen tot een integrale aanpak. Iedereen heeft een aandeel in het “cyber secure” houden van de samenleving: consumenten, bedrijven en overheden. Hoewel er met diverse campagnes breed wordt ingezet op het bewustmaken van burgers, overheden en bedrijven van het belang van cyber security en hun rol daarin, is het cyber security bewustzijn en het besef dat je zelf maatregelen (zoals gedragsregels en technische maatregelen) kunt nemen om je weerbaarheid te vergroten nog niet volop aanwezig.
Er is nog veel winst te halen als het gaat om de digitale veiligheid van verschillende doelgroepen. De tiendaagse campagne Alert Online, van de NCTV, die dit najaar voor de tweede keer plaats vindt, zet hierop in.

Doel
Ter voorbereiding op en als input voor de komende campagne en de PR daaromheen heeft GfK Intomart in opdracht van NCTV en DPC een representatief onderzoek uitgevoerd dat inzicht biedt in de ontwikkelingen en de wijze waarop zowel de zakelijke doelgroepen als de doelgroep burgers omgaan met digitale veiligheid. De nulmeting van dit onderzoek vond plaats in 2012 en is uitgevoerd door onderzoeksbureau Motivaction B.V.

Specifiek geeft dit onderzoek ieder jaar inzicht in:
- Het huidige niveau van cyber security awareness vertaald naar kennis, houding en gedrag;
- De informatiebehoefte rondom cyber security awareness;
- De verschillen tussen de doelgroepen;
- Ontwikkelingen in de tijd, welke een indicatie vormen voor het effect van inspanningen rondom het vergroten van de cyber security awareness.

Daarnaast heeft het onderzoek een jaarlijks wisselend thema, dat kan worden gebruikt om meer focus aan te brengen in de brede campagne Alert Online. Dit jaar is gekozen voor het thema “Smart Security”. NCTV kan de inzichten van dit onderzoek gebruiken voor het nog beter toespitsen van haar beleid en communicatiestrategie rondom digitale veiligheid op diverse doelgroepen.

1.2 Opzet van het onderzoek

Doelgroepen
De onderzoeksdoelgroepen bestaan uit de volgende vijf groepen:

- Rijksoverheid: ambtenaren werkzaam bij een van de elf departementen, uitvoeringsorganisaties, agentschappen, ZBO's, Hoog College van Staat, Adviescollege, Rechterlijke macht, onderwijs- en onderzoeksinstellingen, politie of Defensie;
- Gemeenten: ambtenaren werkzaam bij gemeenten in onder meer beleids-, uitvoerings-, staf-, administratieve- en loketfuncties;
- Bedrijfsleven: medewerkers uit alle sectoren van het bedrijfsleven die werkzaam zijn voor een organisatie met 10 medewerkers of meer, exclusief medewerkers van organisaties binnen de vitale sectoren;
- Vitale sectoren: medewerkers van organisaties binnen de vitale sectoren energie, transport, telecommunicatie, financiële sector, drinkwater, keren en beheren van oppervlaktewater;
- Burgers: inwoners van Nederland van 13 jaar en ouder.

Binnen de vier zakelijke doelgroepen is onderscheid gemaakt naar leidinggevenden (een medewerker die leiding geeft aan een groep medewerkers vanuit een formele rol) en overige medewerkers. Verder geldt voor de zakelijke doelgroepen dat alle respondenten door hun werkgever een computer (pc, laptop, tablet en/of smartphone) ter beschikking gesteld hebben gekregen voor het uitvoeren van hun werkzaamheden (thuis of op kantoor).

Voor de doelgroep burgers geldt dat zij thuis beschikken over een privécomputer (pc, laptop, tablet en/of smartphone).

Methode en veldwerk
Gekozen is voor een kwantitatief online onderzoek. Ter voorkoming van paneleffecten, is het onderzoek uitgevoerd onder alle doelgroepen, behalve gemeenten, uitgevoerd onder het GfK onderzoekspanel. Het onderzoek onder gemeenten is, net als vorig jaar, uitgevoerd onder het Flitspanel[1] van het ministerie van BZK, in de vragenlijstomgeving van het GfK onderzoekspanel. Hiernaast zijn er 26 medewerkers van de doelgroep vitale sectoren uit het relatienetwerk van NCTV uitgenodigd voor deelname.

De vragenlijst is aan de hand van een door GfK Intomart geprogrammeerde vragenlijst (CAWI) afgenomen. De respondent krijgt via e-mail een uitnodiging voor het onderzoek, in de e-mail is een link opgenomen naar de vragenlijst. Door op de link te klikken opent het onderzoek automatisch en kan de respondent zelf via de computer de vragenlijst invullen.

[1] Het Flitspanel bestaat uit medewerkers van verschillende overheidssectoren. Zij zijn geworven door middel van het Personeels- en Mobiliteitsonderzoek, waarvoor zij aselect zijn geselecteerd via het ABP. Zo is geborgd dat het panel een afspiegeling is van de populatie per sector.

Het veldwerk onder het GfK panel vond plaats van 10 juli tot en met 22 juli 2013. Het veldwerk onder het Flitspanel vond plaats van 5 juli tot en met 22 juli 2013. Tijdens de veldwerkperiode is eenmaal (op 11 juli) een herinnering gestuurd naar de respondenten van het Flitspanel en tweemaal (op 16 juli en op 19 juli) een herinnering verstuurd naar een deel van de mensen van het GfK panel, die de vragenlijst op dat moment nog niet (volledig) hadden ingevuld.

Steekproef en respons

Voor dit onderzoek zijn in totaal 7 steekproeven getrokken: voor elke doelgroep één plus twee extra bruto steekproeven onder de doelgroepen Rijksoverheid en Vitale sectoren (op 18 juli). De steekproef voor gemeenten is getrokken uit het Flitspanel van het ministerie van BZK en de steekproeven voor de andere vier doelgroepen zijn getrokken uit het GfK online panel.
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
Rijksoverheid	1.140 (890+ 250)	523
Gemeenten	3.060	538
Bedrijfsleven overig	612	371
Bedrijfsleven vitale sectoren	1.418 (942+450+26)	524
Burgers 13+	2.181	1.285
Totaal	*8.411*	*3.241*

Alle doelgroepen kregen aan het begin van de vragenlijst diverse selectievragen voorgelegd, op basis waarvan zij – met het oog op de kwaliteit van de data - uiteindelijk zijn toegewezen aan één doelgroep. Dit in tegenstelling tot de meting van 2012, waarbij respondenten die tot meerdere doelgroepen behoorden zowel als consument als medewerker van het bedrijfsleven zijn bevraagd.

Representativiteit

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

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

Meer informatie over de weging en de steekproefverdeling treft u aan in bijlage 1.

Leeswijzer

De rapportage is thematisch opgebouwd; dit betekent dat per thema telkens zowel de overall resultaten voor de doelgroepen als verschillen in de resultaten tussen doelgroepen, binnen doelgroepen en in de tijd worden beschreven.

De indeling van de rapportage is als volgt:

- Voorafgaand aan dit inleidende hoofdstuk 1 zijn de samenvatting, de conclusies en aanbevelingen opgenomen;
- In hoofdstuk 2 komen de resultaten aan bod, waarbij we achtereenvolgens ingegaan op het beeld van cyber security bij de doelgroepen; de risicoperceptie; de kennis en het gedrag rondom digitale veiligheid in het algemeen en in het bijzonder rondom een veilig gebruik van wachtwoorden en tot slot de gepercipieerde verantwoordelijkheid rondom cyber security;
- In hoofdstuk 3 komt het themadeel van dit jaar aan bod: Smart Security;
- In hoofdstuk 4 gaan we in op de belangrijkste resultaten van verdiepende analyses die we hebben uitgevoerd op de onderzoeksdata.

De tabellen van alle vragen tezamen zijn bij dit rapport geleverd als tien afzonderlijke tabellenrapportages. Verder is in dit rapport achtereenvolgens als bijlage opgenomen:

- Onderzoeksverantwoording inclusief responsoverzicht;
- Kwantitatieve vragenlijst;
- Certificering.

Ten geleide bij het rapport

Aard van de resultaten

Alle resultaten betreffen *zelfgerapporteerde* kennis, houding en gedrag.

Vergelijkbaarheid resultaten in de tijd

De vragenlijst van het huidige Cyber security onderzoek is aangescherpt ten opzichte van de vragenlijst van de nulmeting / pilot van vorig jaar (2012). In sommige gevallen zijn er op basis van betrouwbaarheids- en factoranalyses op het bestand van 2012 een aantal items bij vragen weggelaten, zijn er soms enkele items of een hele vraag toegevoegd of is de tekst van een item wat aangescherpt. Verder is de volgorde van een aantal vragen aangepast zodat deze logischer is voor respondenten, volgorde-effectenen en het geven van sociaal-wenselijke antwoorden zoveel mogelijk voorkomt. Wijzigingen zijn alleen aangebracht indien deze geen drempel vormden voor een vergelijking in de tijd; dit betekende dat bewust van sommige mogelijke wijzigingen is afgezien. Met deze vragenlijst is de basis gelegd voor de toekomstige metingen.

Weergave van significante verschillen

De gevonden percentages zijn getoetst op significantie van de verschillen:

- tussen de vijf doelgroepen;
- binnen elk van de vijf doelgroepen op geslacht, leeftijd, opleiding en voor de zakelijke doelroepen ook naar leidinggevendheid;
- in de tijd.

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 zijn procentueel per antwoord nagecodeerd. Een uitdraai van alle antwoorden is in een afzonderlijk Excel-bestand opgeleverd. Om recht te doen aan de sfeer en achtergrond waarin de antwoorden zijn gegeven, zijn stijl-, taal- en typefouten ondergeschikt gemaakt aan de context, zodat in het tabellenrapport gekozen is voor een letterlijke, ongecorrigeerde weergave van deze antwoorden.

2. Resultaten 2013

Inleiding

In dit hoofdstuk gaan we eerst in op het beeld dat bij de diverse doelgroepen leeft ten aanzien van cyber security. Vervolgens zetten we uiteen hoe het gesteld is met hun risicoperceptie, aan bod komen onder meer hoe ze de digitale veiligheid op het werk en thuis inschatten en wat hun algemene grondhouding ten aanzien van de risico's van internet is. Daarna gaan we in op diverse aspecten van cyber security awareness, vertaald naar kennis, houding en gedrag, gevolg door de verantwoordelijkheidstoedeling voor cyber security. Bij elke vraag staan onder subkopjes eventuele significante verschillen tussen groepen, in de tijd en binnen groepen.

2.1 Beeld cyber security

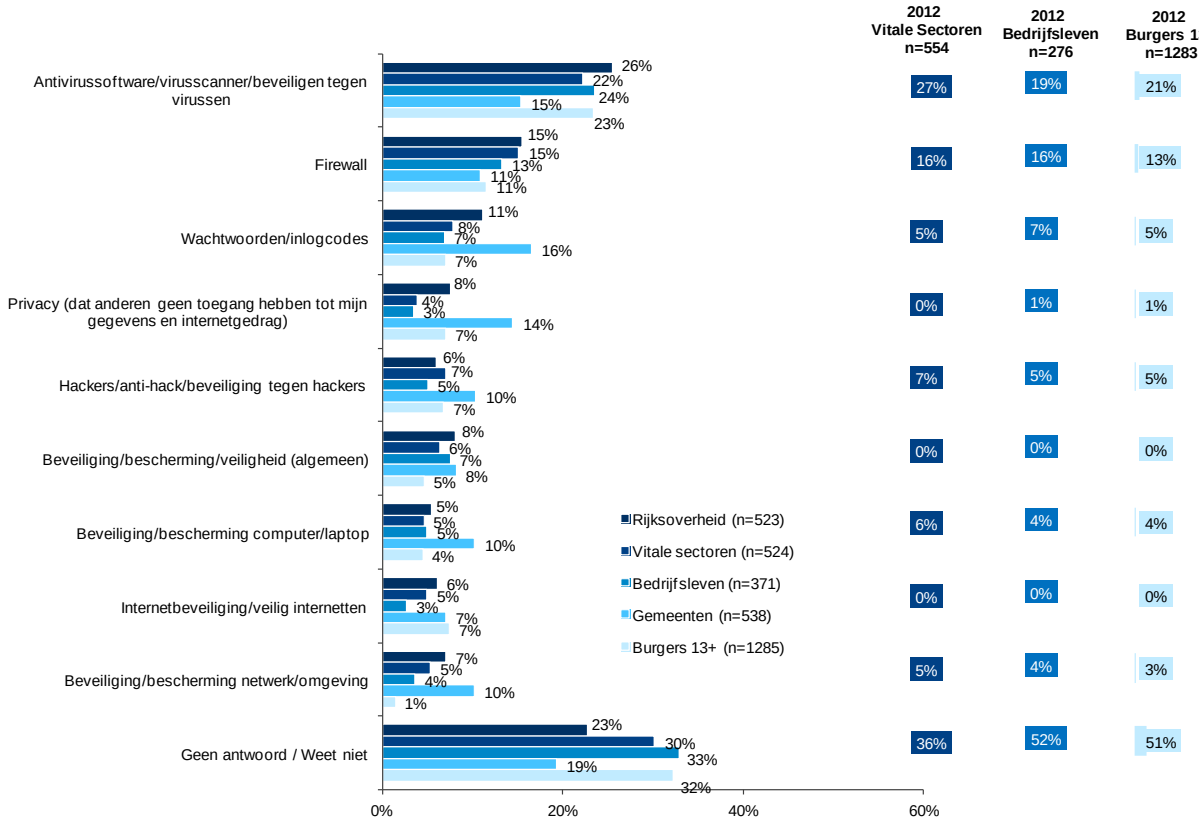
In deze paragraaf komt het beeld dat de verschillende doelgroepen hebben met betrekking tot cyber security aan bod. Eerst gaan we in op de spontane associaties bij cyber security, vervolgens op het beeld dat de doelgroepen hebben van de mate van cyber security op het werk en thuis.

Overall zien we dat de bescherming tegen virussen nog altijd het dominante element in beeldvorming ten aanzien van cyber security is.
Verder blijkt dat de digitale veiligheid op het werk en thuis met een (ruim) voldoende wordt beoordeeld, waarbij de digitale veiligheid op het werk hoger wordt ingeschat dan de digitale veiligheid thuis.

2.1.1 Bij digitale veiligheid denkt men vooral aan bescherming tegen virussen en firewalls

In vergelijking met vorig jaar weten de ondervraagden beter een antwoord te geven op de vraag waar ze aan denken bij een veilige digitale omgeving. Waar in 2012 nog gemiddeld 47% aangaf geen antwoord te kunnen geven op deze vraag, is dit in 2013 gezakt naar 28%. Men denkt bij cyber security vooral aan beveiliging tegen aanvallen van buitenaf zoals door virussen en hackers, maar ook aan bescherming van de privacy via firewalls en wachtwoorden.

Figuur B1: Als we het hebben over cyber security oftewel een veilige digitale omgeving, waar denkt u dan aan?



Vergelijking met 2012

Burgers en medewerkers van het bedrijfsleven en de vitale sectoren noemen allemaal vaker privacy. Ook noemen burgers vaker internetbankieren, wachtwoorden en McAfee. Beveiliging van het netwerk, identiteitsroof en malware worden minder vaak door burgers genoemd. Niet-leidinggevenden noemen vaker dan in 2012 beveiliging tegen internetcriminelen, bescherming van de netwerkomgeving, privacy en wachtwoorden. Deze laatste twee worden ook vaker dan vorige keer genoemd door de leidinggevenden.

Vergelijking tussen groepen

Gemeentemedewerkers (15%) noemen minder vaak antivirussoftware dan de overige doelgroepen, maar vaker wachtwoorden, privacy, hackers, beveiliging van de computer, bescherming van de netwerkomgeving en dat het belangrijk is goed op te letten. Ook geven gemeentemedewerkers het minst vaak aan dat ze geen antwoord op deze vraag kunnen geven. Rijksambtenaren noemen vaker dan burgers beveiliging van de netwerkomgeving, wachtwoorden en encryptie.

Vergelijking binnen groepen

- Bij de burgers kunnen vijftigplussers minder vaak bepaalde voorzorgsmaatregelen noemen dan jongere groepen, zoals bijvoorbeeld antivirussoftware, een firewall, wachtwoorden of encryptie. Van de laagopgeleiden kan 46% niet uitleggen wat er met cyber security bedoeld wordt tegenover 19% van de hoogopgeleiden.
- Hoogopgeleiden kunnen vaker dan laagopgeleiden zaken opnoemen als beveiliging tegen hackers, malware, phishing en wachtwoorden. Mannen noemen internetcriminelen, beveiliging tegen hacken, malware en encryptie vaker dan vrouwen.
- Rijksambtenaren van 31-49 jaar noemen malware en firewalls vaker dan vijftigplussers. Laagopgeleide Rijksambtenaren kiezen in 36% van de gevallen voor het antwoord 'weet niet'. Hoogopgeleide gemeentemedewerkers noemen vaker wachtwoorden en dat het nodig is om goed op te letten, maar middenopgeleiden noemen juist weer vaker Https en Norton. Jongere medewerkers van vitale sectoren noemen vaker McAfee en hoogopgeleide medewerkers van het bedrijfsleven vaker encryptie.

2.1.2 De digitale veiligheid van de werkgever wordt met gemiddeld een 8,1 het hoogst ingeschat

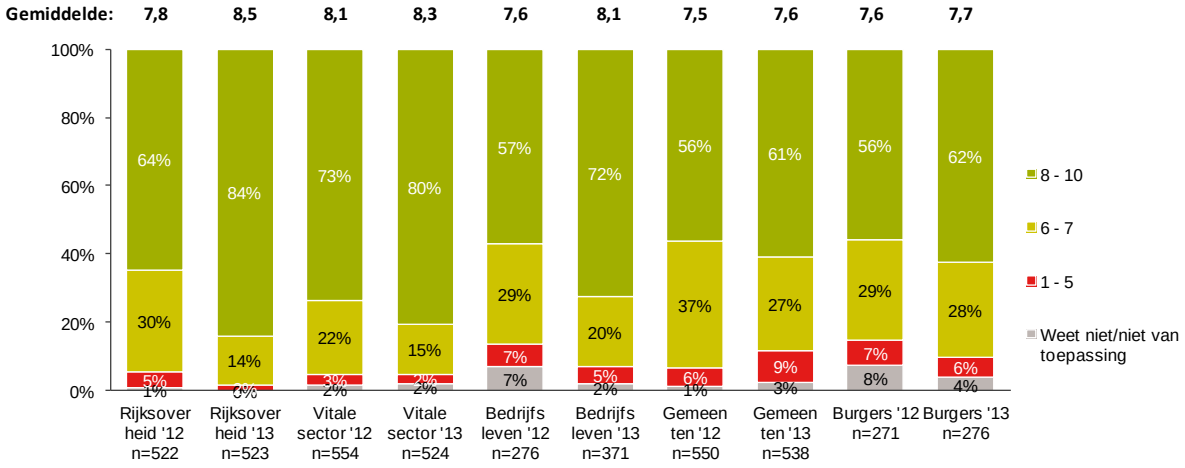
Om inschatting te krijgen in de perceptie van respondenten van de mate van digitale veiligheid van de werkgever, de medewerkers, de respondent zelf in de rol van werknemer en de respondent zelf als privépersoon, is respondenten gevraagd de digitale veiligheid in een rapportcijfer uit te drukken. Bij de burgers is deze vraag alleen gesteld aan degenen die thuis een door de werkgever ter beschikking gestelde computer hebben.

De digitale veiligheid van de werkgever wordt gemiddeld over alle doelgroepen heen het hoogst ingeschat (8,1), gevolgd door de digitale veiligheid van de respondent zelf op het werk (7,9) en tot slot op een gedeelde laatste plaats de digitale veiligheid thuis en van collega's (7,4). We bespreken nu de resultaten in deze volgorde.

2.1.2.1 Digitale veiligheid werkgever scoort het hoogst met gemiddeld een 8,1

Gemiddeld wordt de digitale veiligheid van de werkgever beoordeeld met een 8,1. De meerderheid van de doelgroepen (73%) geeft een hoge score van 8-10. Een minderheid van 5% geeft een onvoldoende. De digitale veiligheid van de werkgever wordt relatief het hoogste ingeschat door Rijksambtenaren (8,5) en relatief het laagst door burgers (7,7).

Figuur B2_1: Rapportcijfer digitale veiligheid werkgever



Vergelijking met 2012

Medewerkers van de Rijksoverheid, de vitale sectoren en het bedrijfsleven beoordelen hun werkgever significant beter dan in 2012. Dit geldt zowel voor het gemiddelde rapportcijfer, als voor het aandeel dat een ruim voldoende geeft versus het aandeel dat een voldoende of een onvoldoende geeft. Zowel bij de leidinggevenden als de niet-leidinggevenden is de waardering voor de digitale veiligheid van de werkgever gestegen.

Vergelijking tussen groepen

In vergelijking met de overige professionele doelgroepen beoordelen de gemeentemedewerkers de digitale veiligheid van hun werkgever lager.

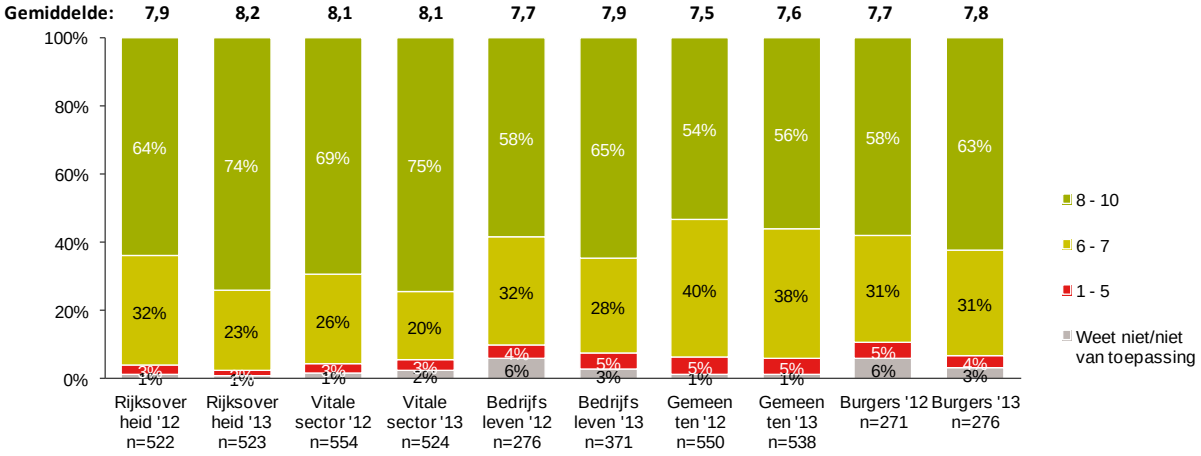
Vergelijking binnen groepen

Van de burgers geven de vijftigplussers (73%) vaker een hoge beoordeling aan hun werkgever dan de groep 31-49 jaar (62%). Bij de gemeentemedewerkers geven middenopgeleiden (74%) vaker een hoge score dan hoogopgeleiden (55%). Van de medewerkers van de vitale sectoren geven hoogopgeleiden (83%) vaker een score van 8-10 dan de laagopgeleiden (70%).

2.1.3 Eigen digitale veiligheid op het werk scoort gemiddeld een 7,9

Men beoordeelt de eigen digitale veiligheid op het werk hoger (7,9) dan die van collega's (7,4). Gemiddeld geeft tweederde (67%) een hoge score van 8-10 en geeft een minderheid van 4% een onvoldoende. De gemiddelde score loopt van een 7,6 bij gemeentemedewerkers tot een 8,2 bij Rijksambtenaren.

Figuur B2_3: Rapportcijfer digitale veiligheid uzelf op werk



Vergelijking met 2012

Rijksambtenaren en medewerkers van het bedrijfsleven geven vaker aan dan vorig jaar dat hun eigen digitale gedrag op het werk zeer veilig is. De gemiddelde beoordeling is ook (wat) gestegen ten opzichte van vorig jaar. Zowel bij de leidinggevenden als de niet-leidinggevenden is de beoordeling van de eigen digitale veiligheid op het werk gestegen ten opzichte van 2012.

Vergelijking tussen groepen

Rijksambtenaren en medewerkers van de vitale sectoren geven zichzelf een hogere beoordeling dan burgers, medewerkers van gemeenten en van het bedrijfsleven.

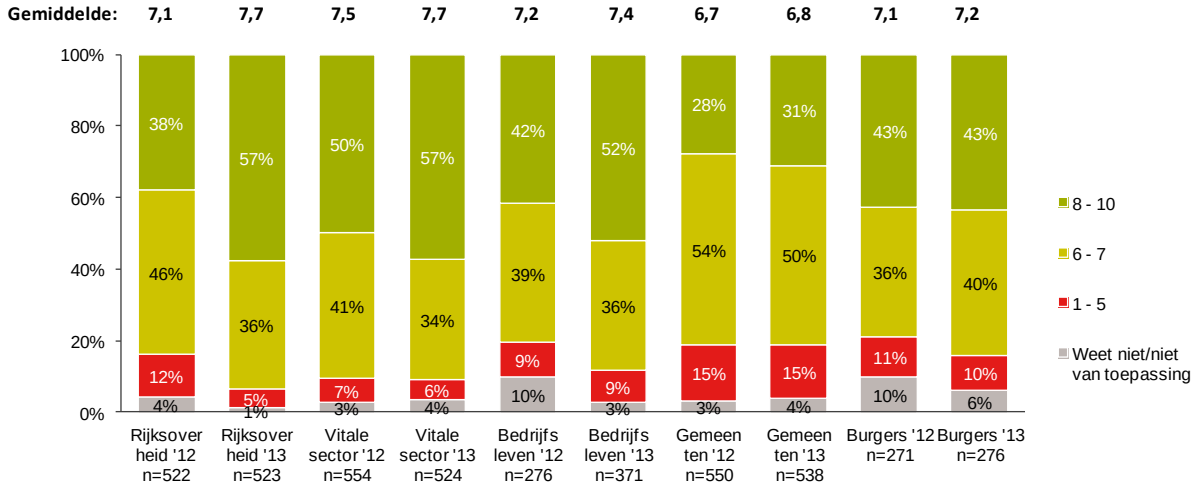
Vergelijking binnen groepen

Voor alle professionele doelgroepen geldt dat hoogopgeleide medewerkers zichzelf minder vaak een hoge score geven dan middenopgeleide medewerkers. Bij medewerkers van het bedrijfsleven beoordeelden vijftigplussers (73%) zichzelf vaker goed dan jongere medewerkers.

2.1.3.1 Digitale veiligheid collega's scoort een gemiddeld een 7,4

De digitale veiligheid van collega's wordt op hetzelfde niveau ingeschat als de eigen digitale veiligheid thuis, namelijk met een rapportcijfer 7,4. Gemiddeld beoordeelt 48% de collega's met een hoge score van 8-10 en geeft 9% hun digitale veiligheid een onvoldoende. De beoordelingen variëren van een gemiddelde van 6,8 voor gemeentemedewerkers tot een 7,7 voor Rijksambtenaren en medewerkers van de vitale sectoren.

Figuur B2_2: Rapportcijfer digitale veiligheid collega's



Vergelijking met 2012

Medewerkers van de Rijksoverheid, vitale sectoren en het bedrijfsleven geven hun collega's vaker een hoge score dan in 2012. Ook de gemiddelde beoordeling is gestegen ten opzichte van vorig jaar. Deze stijging is gelijk verdeeld over de leidinggevenden en niet-leidinggevenden.

Vergelijking tussen groepen

Rijksambtenaren en medewerkers van de vitale sectoren geven hun collega's vaker een hoge beoordeling dan burgers en gemeentemedewerkers. Gemeentemedewerkers beoordelen de digitale veiligheid van hun collega's vaker dan de Rijksambtenaren en medewerkers van de vitale sectoren met een onvoldoende.

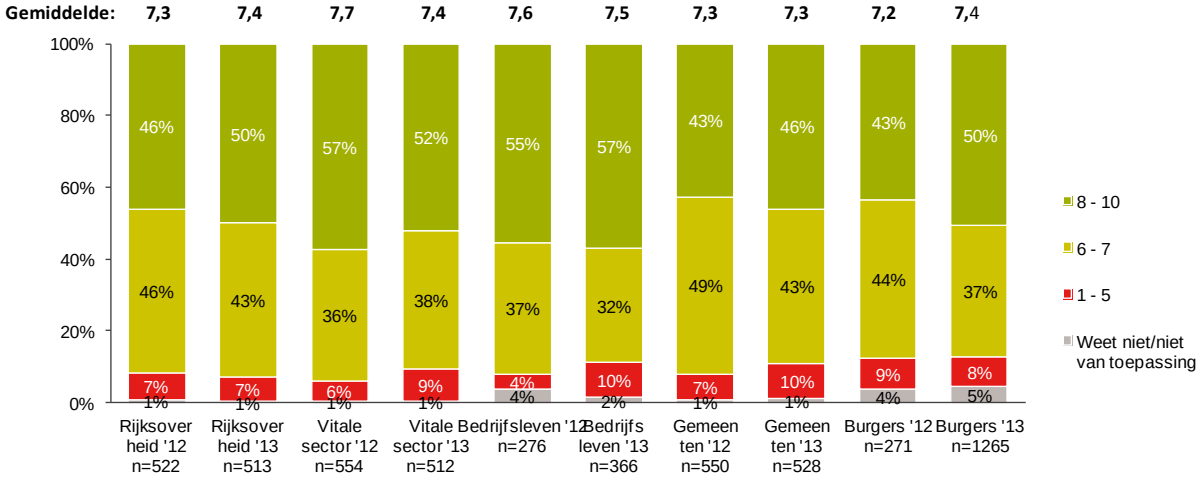
Vergelijking binnen groepen

De Rijksambtenaren en medewerkers van gemeenten en vitale sectoren beoordelen hun collega's hoger als ze middenopgeleid zijn dan hoogopgeleid. Bij medewerkers van het bedrijfsleven en de vitale sectoren geven de vijftigplussers vaker een hoge score aan hun collega's dan de jongere medewerkers.

2.1.3.2 Digitale veiligheid thuis scoort gemiddeld een 7,4

Thuis schat men de digitale veiligheid als minder hoog in dan op het werk. Dat blijkt uit het gemiddelde rapportcijfer van een 7,4 en het aandeel respondenten dat zichzelf een hoge score (gemiddeld geeft 51% zichzelf een score van 8-10) of een onvoldoende (9%) geeft. De scores liggen dicht bij elkaar tussen de doelgroepen, en lopen uiteen van een 7,3 van gemeenteambtenaren tot een 7,5 van medewerkers uit het bedrijfsleven.

Figuur B2_4: Rapportcijfer digitale veiligheid uzelf thuis



Vergelijking met 2012

Burgers geven zichzelf significant vaker een hoge beoordeling dan in 2012; ook de gemiddelde beoordeling is gestegen. Medewerkers van het bedrijfsleven en de vitale sectoren beoordelen hun digitale veiligheid thuis juist vaker met een onvoldoende dan verleden jaar. De gemiddelde beoordeling van medewerkers van vitale sectoren is wat gedaald ten opzichte van 2012. Zowel de leidinggevenden als de niet-leidinggevenden geven zichzelf vaker een onvoldoende.

Vergelijking tussen groepen

Medewerkers van het bedrijfsleven geven zichzelf vaker een hoge score dan gemeentemedewerkers. Burgers geven vaker dan de professionele groepen aan niet te weten hoe het met hun digitale veiligheid thuis gesteld is.

Vergelijking binnen groepen

Bij de burgers geven mannen (56%) geven zichzelf vaker een score van 8-10 dan vrouwen (45%). Hoogopgeleide burgers (15%) geven zichzelf vaker een onvoldoende dan lageropgeleiden. Voor de professionele doelgroepen geldt dat vijftigplussers zichzelf een significant hogere beoordeling geven dan de groep 18-30. Bij het bedrijfsleven en de vitale sectoren schatten middenopgeleide medewerkers hun eigen digitale veiligheid thuis hoger in dan hoogopgeleiden.

2.2 Risicoperceptie

In deze paragraaf komt de risicoperceptie aan bod. Allereerst gaan we in op de algemene houding ten aanzien van de risico's van internet en de eigen invloed ("locus of control") daarop, gevolgd door de mate waarin men zich zorgen maakt over de eigen digitale veiligheid. Vervolgens zoomen we in op de risicoperceptie onder de doelgroep burgers: hoe is het gesteld met hun spontane bekendheid over mogelijkheden om via internet misbruik van hun computer te maken en hoe groot schatten zij de kans in dat zij zelf te maken krijgen met internetrisico's.

Tot slot gaan we in op de risicoperceptie onder professionals: hoe beoordelen ze de aandacht van hun werkgever voor digitale veiligheid, hoe is het gesteld met hun spontane bekendheid van risico's voor de digitale veiligheid van hun werkgever, in hoeverre is digitale veiligheid verankerd in beleid en wordt dit beleid structureel uitgevoerd en nageleefd?

Overall zien we dat de risicoperceptie op diverse aspecten is toegenomen maar op andere aspecten nog beperkt is. Hoewel het merendeel van de respondenten zichzelf voldoende bewust vindt van de risico's van internet, is een aanzienlijk deel spontaan niet bekend met de risico's van internet voor zichzelf of de werkgever. Ook is het merendeel niet echt bezorgd over hun eigen digitale veiligheid.

2.2.1 Meerderheid respondenten vindt zichzelf voldoende bewust van de risico's van internet en aanzienlijke groep maakt zich geen zorgen

Dit jaar is een aantal stellingen voorgelegd om de algemene basishouding ten aanzien van de risico's van internet en perceptie van de eigen weerbaarheid/invloed ten aanzien van deze risico's in kaart te brengen. Onderstaande tabel geeft de resultaten per doelgroep weer, op volgorde van veel naar weinig instemming met de stellingen. Opvallend is dat het merendeel (ongeveer driekwart) van de respondenten zichzelf voldoende bewust vindt van de risico's van internet, maar dat tegelijkertijd ongeveer vier op de tien respondenten zich weinig zorgen over deze risico's maken.

Wellicht komt dit, doordat ze zich veilig achten (nagenoeg de helft voelt zich voldoende beschermd tegen de internetrisico's) in combinatie met het feit dat een groot deel van de respondenten (de helft) het idee hebben dat hun eigen invloed beperkt is (tegen grote gevaren en nieuwe risico's kun je je toch niet (tijdig) weren. Wel maken ongeveer vier op de tien respondenten zich zorgen om de bescherming van hun privacy op internet. Verder valt op dat ongeveer één op de vijf respondenten denkt zelf minder risico te lopen dan anderen.

Figuur B3a: Stellingen risicoperceptie internet (weergave percentage "zeer mee eens" + "mee eens")

	Rijksoverheid n=523	Vitale sectoren n=524	Bedrijfsleven n=371	Gemeenten n=538	Burgers 13+ n=1285
Ik ben niet huiverig voor internetbankieren.	77%	76%	76%	71%	70%
Ik ben me voldoende bewust van de risico's van internet.	73%	72%	68%	69%	69%
Ik heb met mijn kind(eren) afspraken gemaakt over omgaan met digitale veiligheid tijdens het internetten.	60%	60%	68%	68%	60%
Ik zie geen gevaar bij het online aankopen van producten bij grote merken of bekende sites.	59%	57%	66%	56%	59%
Tegen grote gevaren op internet kun je je eigenlijk niet weren, kwaadwillenden slagen toch wel.	52%	52%	56%	53%	57%
De privacy voorwaarden bij het verstrekken van gegevens op internet lees ik meestal niet of nauwelijks.	49%	52%	55%	53%	46%
Er komen telkens nieuwe risico's bij op internet, dat kun je toch niet bijbenen.	49%	48%	53%	46%	52%
Bij online aankopen betaal ik liever niet met een creditcard.	43%	41%	41%	50%	45%
Ik voel me voldoende beschermd tegen de risico's van internet.	46%	48%	49%	38%	44%
Van iedereen zijn nu eenmaal veel gegevens bekend op internet, dat heb je zelf niet echt in de hand.	40%	38%	45%	39%	46%
Ik maak me meestal weinig zorgen over de risico's van internet.	41%	45%	45%	39%	41%
Ik maak me zorgen om de bescherming van mijn privacy op internet.	39%	39%	39%	52%	38%
Risico's van internet zijn vervelend, maar niet echt bedreigend voor mij.	38%	40%	36%	35%	40%
Ik vertrouw er op dat internetbedrijven mijn gegevens niet zonder mijn toestemming aan derden verstrekken.	35%	34%	36%	28%	41%
Ik loop minder risico dan anderen op een nare ervaring met internet.	19%	23%	22%	20%	19%
Ik begrijp de zorgen over online betalen met een creditcard niet, als het mis gaat krijg je je geld toch wel	11%	16%	16%	8%	13%

Vergelijking tussen groepen

Gemeentemedewerkers zijn het vaker dan de overige doelgroepen oneens met de stelling dat internetbedrijven zonder toestemming geen persoonlijke gegevens aan derden verstrekken, burgers zijn het hier daarentegen vaker dan gemeentemedewerkers wel mee eens. Ook zijn burgers vaker dan medewerkers van vitale sectoren en gemeenten van mening dat je toch niet zelf in de hand hebt dat je gegevens bekend zijn op internet. 8% van de burgers weet niet of het risicovol is om met een creditcard online aankopen te betalen, dat is meer dan bij de professionele doelgroepen.

Zeven op de tien gemeentemedewerkers zijn het oneens met de stelling dat je je geld toch wel terug krijgt als online betalen met een creditcard misgaat tegenover ongeveer ruim de helft bij de overige doelgroepen. Ook zijn gemeentemedewerkers vaker dan burgers en medewerkers van het bedrijfsleven geneigd om de privacyvoorwaarden te lezen. Verder maken gemeentemedewerkers zich meer dan de overige doelgroepen zorgen over de bescherming van hun privacy op internet en voelen zich ook minder beschermd tegen de risico's van internet. Ook zijn ze het vaker dan burgers en medewerkers van de vitale sectoren oneens dat de risico's van internet niet echt bedreigend voor hen zijn.

Rijksambtenaren en gemeentemedewerkers zijn het vaker dan burgers oneens met de stelling dat de risico's van internet niet bij te benen zijn. Rijksambtenaren zijn vaker dan burgers niet huiverig voor internetbankieren.

Medewerkers van het bedrijfsleven geven vaker dan gemeentemedewerkers aan geen gevaar te zien bij online aankopen bij grote en bekende merken. Burgers zijn het minder vaak oneens dan Rijksambtenaren en gemeentemedewerkers met de stelling dat ze zelf minder risico lopen op internet dan anderen of dat je je niet kunt weren tegen de gevaren van het internet.

Vergelijking binnen groepen

In het algemeen kan bij de burgers gesteld worden dat mannen minder bewust zijn van de risico's van internet en ook meer risico's nemen dan vrouwen. Zo denken mannen (25%) bijvoorbeeld vaker dan vrouwen (13%) dat ze minder risico lopen op nare ervaringen dan anderen. Burgers jonger dan 30 jaar maken zich veel minder zorgen over de risico's van internet dan burgers ouder dan 30 jaar. Vooral de groep van 13-17 jaar maakt zich weinig zorgen over de gevaren van internet (58%). Van deze groep geeft ook 68% aan (bijna) geen privacyvoorwaarden te lezen en 32% weet niet of het veilig is om bij online aankopen met een creditcard te betalen. Driekwart (76%) van de vijftigplussers denkt zich al voldoende bewust te zijn van de risico's van internet. Hoogopgeleide burgers zijn zich vaak beter bewust van de risico's dan lageropgeleiden, vooral wat betreft privacy en het doorverkopen van persoonlijke data aan derden. Maar hoogopgeleiden hebben wel meer vertrouwen dan lageropgeleiden in internetbankieren, betalen met een creditcard en online aankoop bij grote merken of bekende sites. Hoogopgeleiden zijn het vaker oneens dat je de gevaren van internet niet goed kunt bijbenen en dat je je hier niet goed tegen kunt weren.

Van de Rijksambtenaren voelen vooral de vijftigplussers zich zeker op het internet, ze denken alle risico's goed afgedekt te hebben. De groep van 18-30 jaar geeft vaker aan onzeker te zijn over de risico's van internet (13%), 26% geeft aan het oneens te zijn dat ze minder risico lopen op internet dan anderen tegenover 50% van de groep 31-49 jaar. Ook is 61% van de jongste groep het eens dat je je toch niet goed kunt weren tegen de gevaren van internet. Ook bij Rijksambtenaren zijn hoogopgeleiden (28%) het er vaker mee oneens dat je je niet kan weren dan de laagopgeleiden (12%).

Bij de gemeenten maken vijftigplussers (60%) zich vaker dan de groep 31-49 jaar (48%) zorgen over hun privacy op internet, zij lezen dan ook vaker de privacyvoorwaarden voor ze hun gegevens opgeven (38%).

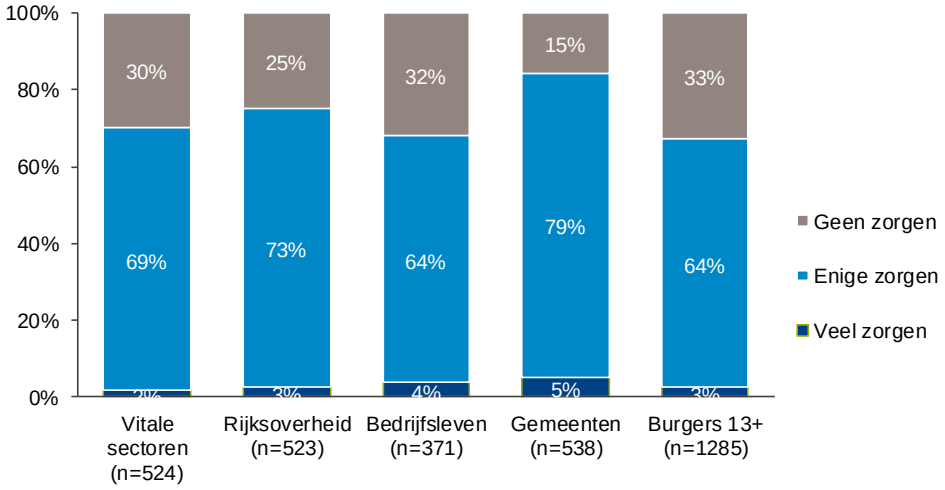
Hoogopgeleide gemeentemedewerkers (33%) hebben er vaker geen problemen mee om online te betalen met een creditcard dan middenopgeleide medewerkers (24%).Hoogopgeleide medewerkers van de vitale sectoren hebben vaker geen vertrouwen (41%) dat hun gegevens niet doorgespeeld worden aan derden, ze zijn ook vaker van mening dat je het wel in de hand kan houden of je gegevens bekend zijn (41%). Hoe jonger men is, hoe minder problemen men heeft met online aankopen bij grote en bekende sites en hoe ouder des te meer men de privacyvoorwaarden leest en zich zorgen maakt over de risico's van internet.

Bij medewerkers van het bedrijfsleven vertrouwen vooral laagopgeleiden (52%) erop dat bedrijven hun gegevens niet verstrekken aan derden. Net als bij de burgers denkt 76% van de vijftigplussers zich voldoende bewust te zijn van de risico's van internet.

2.2.2 Tweederde van de respondenten maakt zich enige zorgen over de digitale veiligheid

Het grootste deel van de respondenten (ongeveer tweederde) maakt zich enige zorgen over hun digitale veiligheid en een minderheid maakt zich veel zorgen. Een aanzienlijke groep (een kwart tot een derde) maakt zich echter geen zorgen

Figuur B3b:In hoeverre maakt u zich zorgen over uw digitale veiligheid?



Vergelijking tussen groepen

Gemeentemedewerkers maken zich vaker enige zorgen over hun digitale veiligheid dan de niet-overheid groepen. Burgers maken zich vaker helemaal geen zorgen dan de overheidsmedewerkers.

Vergelijking binnen groepen

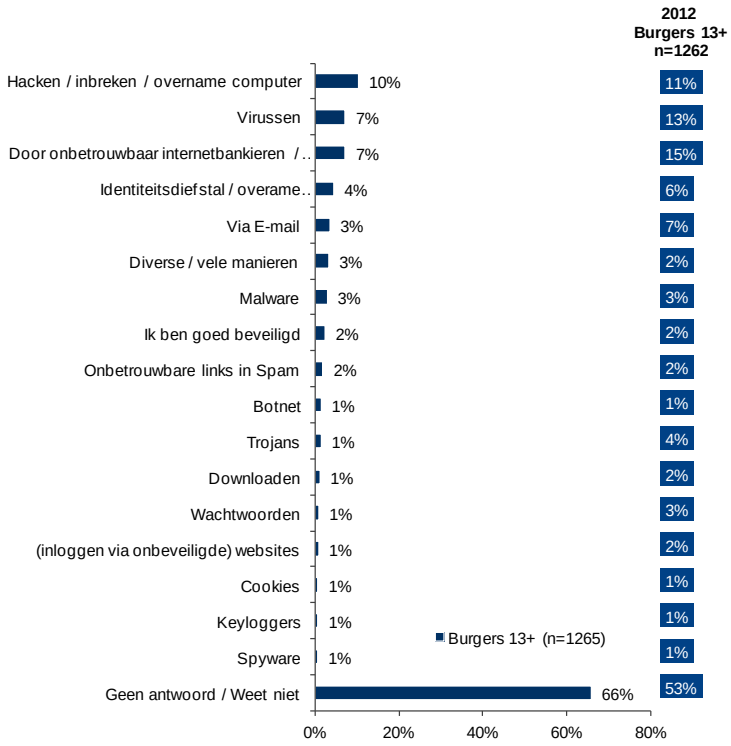
Bij de burgers maakt men zich minder zorgen naarmate de ondervraagde jonger is. Zo maakt 52% van de groep 13-17 jaar zich geen zorgen, tegenover 26% van de groep 50+. Ook voor de overige doelgroepen afgezien van het bedrijfsleven geldt dat oudere medewerkers zich meer zorgen maken over hun digitale veiligheid dan jongere medewerkers. Voor de medewerkers van het bedrijfsleven geldt dat laagopgeleiden (49%) zich minder vaak enige zorgen maken dan hoogopgeleiden (68%).

2.2.3 Risicoperceptie onder burgers beperkt

2.2.3.1 Tweederde van de burgers weet niet spontaan te noemen hoe er via internet misbruik van hun computer kan worden gemaakt.

Het merendeel van de respondenten (66%) kan niet aangeven op welke manieren er via internet misbruik van hun computer kan worden gemaakt. Van de gegeven antwoorden, worden net als vorig jaar virussen, inbraak op de computer en onbetrouwbaar internetbankieren of phishing het meest genoemd als vormen van cybercrime.

Figuur D3: Op welke manieren kan er via internet misbruik gemaakt worden van uw computer?



Vergelijking met 2012

Het aantal burgers dat geen antwoord kan geven op deze vraag is gestegen ten opzichte van 2012. De volgende zaken worden minder vaak genoemd dan verleden jaar: via e-mail, door gebrek aan beveiliging, door onbetrouwbaar internetbankieren en phishing, identiteitsdiefstal, Trojans, virussen, downloaden, inloggen via onbeveiligde websites en wachtwoorden.

Vergelijking binnen Burgers 13+

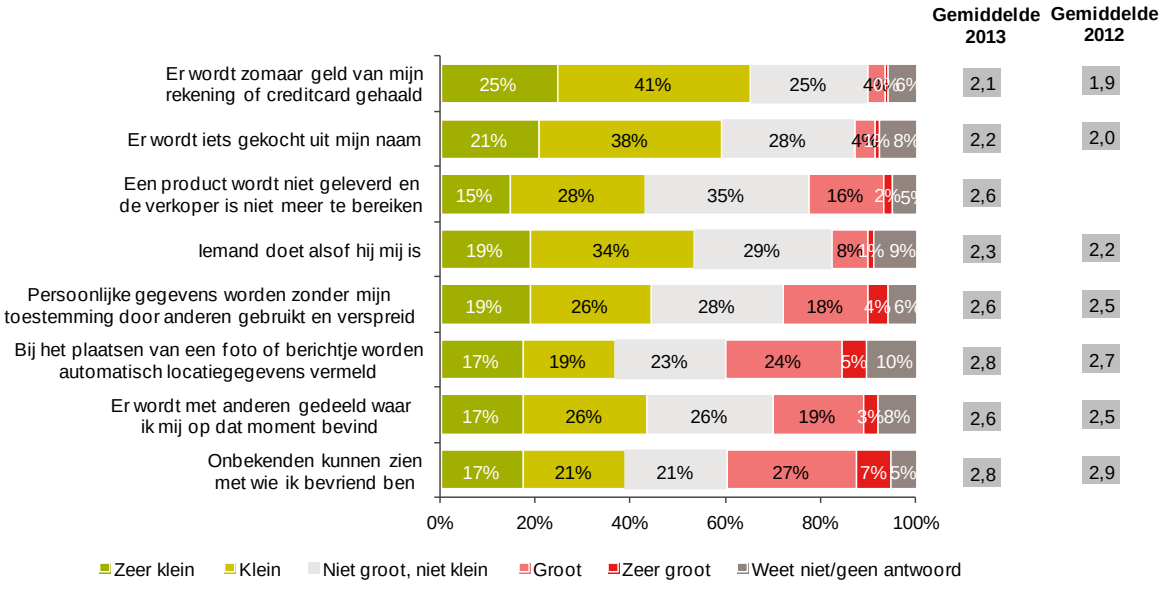
Vrouwen noemen vaker identiteitsdiefstal, maar mannen noemen vaker malware, spyware en Trojans. De groep 18-30 jaar noemt vaker identiteitsdiefstal, virussen en wachtwoorden dan oudere burgers. Hoogopgeleiden noemen vaker hacken, phishing, identiteitsdiefstal, en virussen dan laagopgeleiden. 5% van de hoogopgeleiden geeft aan goed beveiligd te zijn. Ruim driekwart (78%) van de laagopgeleiden geeft het antwoord ‘weet niet’.

2.2.3.2 Een groot deel van de burgers denkt dat de kans op internetrisico's voor henzelf klein is; het meest waarschijnlijk achten ze de kans op het ongewenst delen van privé-informatie met derden.

Wanneer we kijken in hoeverre burgers inschatten dat zij zelf risico lopen op bepaalde vormen van cybercrime dan zien we dat burgers de kans klein achten dat er geld van hun rekening of creditcard wordt gehaald, dat er iets gekocht wordt uit hun naam en dat hun identiteit wordt gestolen.

Ook de overige risico's worden door een aanzienlijke groep als klein ingeschat, maar hierbij zien we ook een aanzienlijke groep die de risico's als groot beschouwen. Het risico dat onbekenden kunnen zien met wie de respondent bevriend is en het automatisch vermelden van locatiegegevens worden dan relatief het vaakst als groot beschouwd. Wat verder opvalt is dat bij alle risico's circa een kwart geen inschatting van de kans dat dit hen overkomt, kan maken.

Figuur D5: Hoe groot denkt u dat de kans is dat tegen uw zin in het volgende op internet gebeurt:



Vergelijking met 2012

Ten opzichte van 2012 schatten burgers de kans groter in dat er zomaar geld van hun rekening of creditcard wordt gehaald, dat er iets wordt gekocht uit hun naam, dat persoonlijke gegevens (zoals vakantiefoto's, persoonlijke berichten of persoonsgegevens) zonder toestemming door anderen worden verspreid en dat hun locatie met anderen wordt gedeeld. De stelling 'een product wordt niet geleverd en de verkoper is niet meer te bereiken' is dit jaar voor het eerst gesteld. Daardoor is geen vergelijking in de tijd mogelijk.

Vergelijking binnen Burgers 13+

Mannen schatten de genoemde internetrisico's in ongeveer de helft van de gevallen lager in dan vrouwen. In tegenstelling tot de overige resultaten zien vijftigplussers deze risico's juist als minder groot dan jongeren. Zo denken minder burgers van boven de 50 jaar dat onbekenden kunnen zien met wie ze bevriend zijn, dat persoonlijke gegevens zonder hun toestemming worden verspreid of dat hun locatie met anderen wordt gedeeld. Dit komt waarschijnlijk doordat jongeren veel meer ervaring met sociale media hebben.

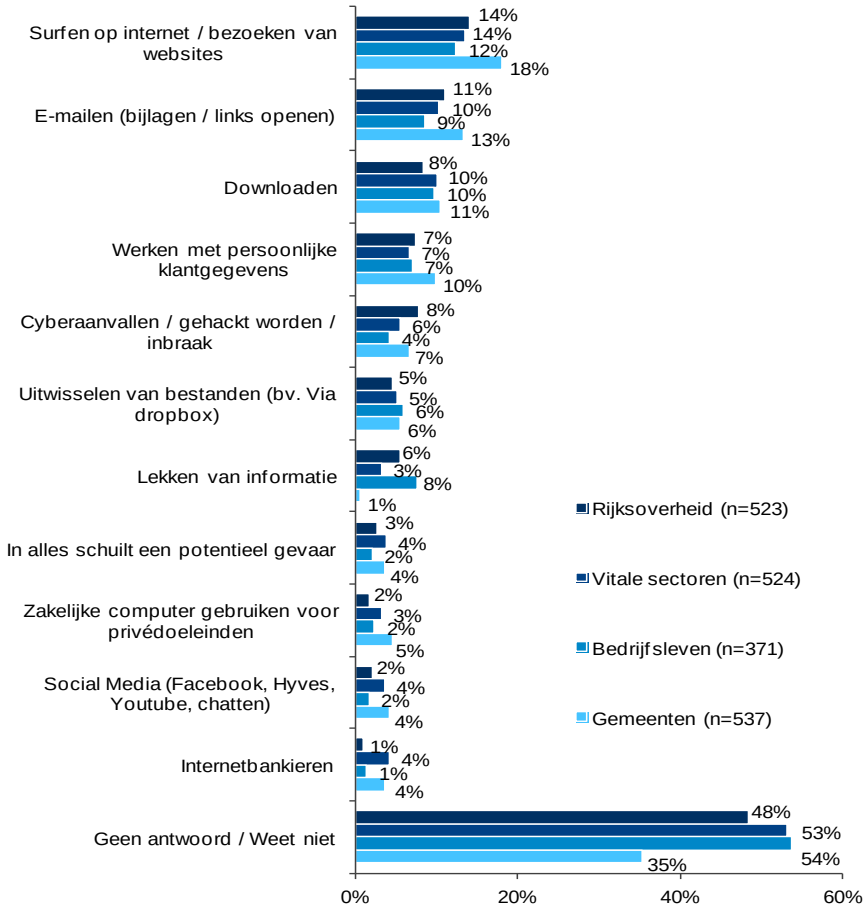
Hoogopgeleiden schatten de kans van identiteitsdiefstal of dat iets gekocht wordt uit hun naam vaker als (zeer) klein in dan lageropgeleiden. Maar ze zijn zich er wel vaker van bewust dat op sociale media gedeelde informatie bij onbekenden terecht kan komen.

2.2.4 Werkgever heeft veel aandacht voor digitale veiligheid, maar risicoperceptie onder professionals verdeeld

2.2.4.1 Spontane bekendheid professionals met risico's voor digitale veiligheid werkgever beperkt; surfen op het werk wordt relatief het meest genoemd

Opvallend is dat gemiddeld 47% van de ondervraagden geen antwoord kan geven op de open vraag welke online handelingen een risico voor de digitale veiligheid van hun werkgever kunnen vormen. Kijken we naar de gegeven antwoorden dan worden surfen op het internet, e-mailen en het downloaden van bestanden relatief het meest als risico genoemd.

Figuur B4: Kunt u aangeven welke werkzaamheden en handelingen op internet een risico kunnen vormen voor de digitale veiligheid van de organisatie waar u voor werkt?



Vergelijking tussen groepen

Gemeentemedewerkers geven minder vaak dan de overige professionele doelgroepen aan het niet te weten. Ook noemen ze minder vaak het lekken van informatie als een mogelijk risico voor de digitale veiligheid op het werk.

In 2012 is deze vraag niet gecodeerd, daarom is er niet met deze data vergeleken.

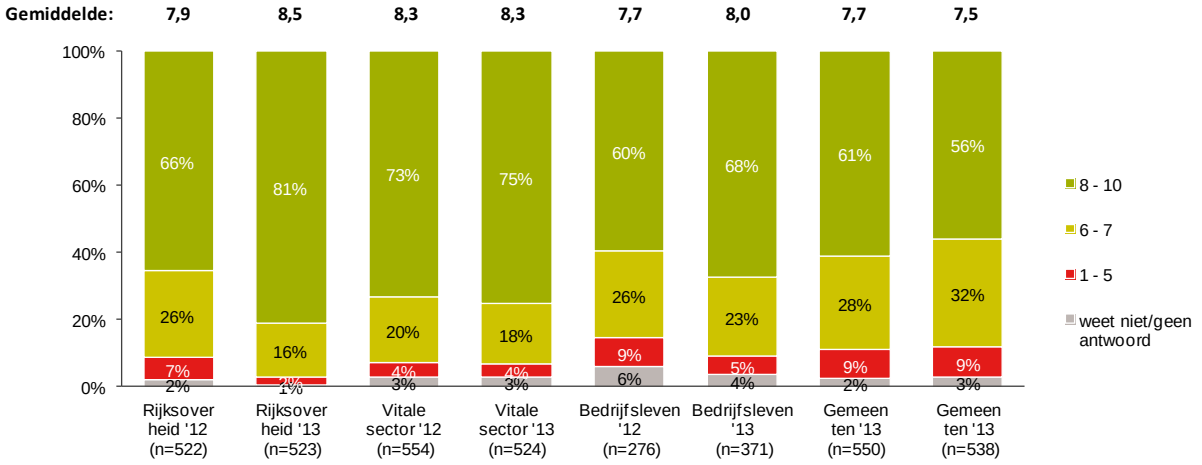
Vergelijking binnen groepen

Bij de Rijksambtenaren noemen de hoogopgeleiden vaker e-mailen (15%) en cyberaanvallen (11%). Bij de gemeentemedewerkers noemen de hoogopgeleiden vaker de zakelijke computer gebruiken voor privédoeleinden (6%). E-mailen (13%) en cyberaanvallen (9%) worden ook vaker genoemd door hoogopgeleide medewerkers van vitale sectoren. Laagopgeleiden van alle doelgroepen geven vaker het antwoord ‘weet niet’.

2.2.4.2 De aandacht voor de digitale veiligheid door de werkgever wordt positief beoordeeld en is sterk gestegen bij de Rijksoverheid.

Onder de professionele doelgroepen geeft men aan dat het goed gesteld is met de aandacht van de werkgever voor de digitale veiligheid. De gemiddelde score is een 8,1 en varieert van een 7,5 voor de gemeentemedewerkers tot een 8,5 voor de Rijksambtenaren. Gemiddeld geeft 70% een score van 8-10 en 5% een onvoldoende.

Figuur B3: Rapportcijfer aandacht werkgever voor digitale veiligheid



Vergelijking met 2012

De beoordeling van de digitale veiligheid van de werkgever is bij de Rijksoverheid zeer sterk gestegen ten opzichte van 2012, maar ook de beoordeling van de medewerkers van het bedrijfsleven is hoger dan vorig jaar. Dit geldt zowel voor de gemiddelde beoordeling als het aandeel dat een ruim voldoende geeft. De beoordeling van de aandacht voor de digitale veiligheid bij de werkgever is vooral gestegen bij de niet-leidinggevenden.

Vergelijking tussen groepen

De Rijksambtenaren geven vaker hun werkgever een hoge score voor aandacht voor digitale veiligheid dan de gemeentemedewerkers en medewerkers van het bedrijfsleven. Gemeentemedewerkers geven minder vaak een hoge score dan de andere doelgroepen.

Vergelijking binnen groepen

Oudere Rijksambtenaren geven een hogere score dan jongere Rijksambtenaren, maar liefst 87% van de groep 50+ geeft een score van 8-10 tegenover 66% van de groep 18-30 jaar. Ook bij de medewerkers van de gemeenten en het bedrijfsleven worden vaker hoge scores gegeven voor de aandacht voor digitale veiligheid bij de werkgever door de ouderen dan de jongeren.

2.3 Cyber secure kennis en gedrag

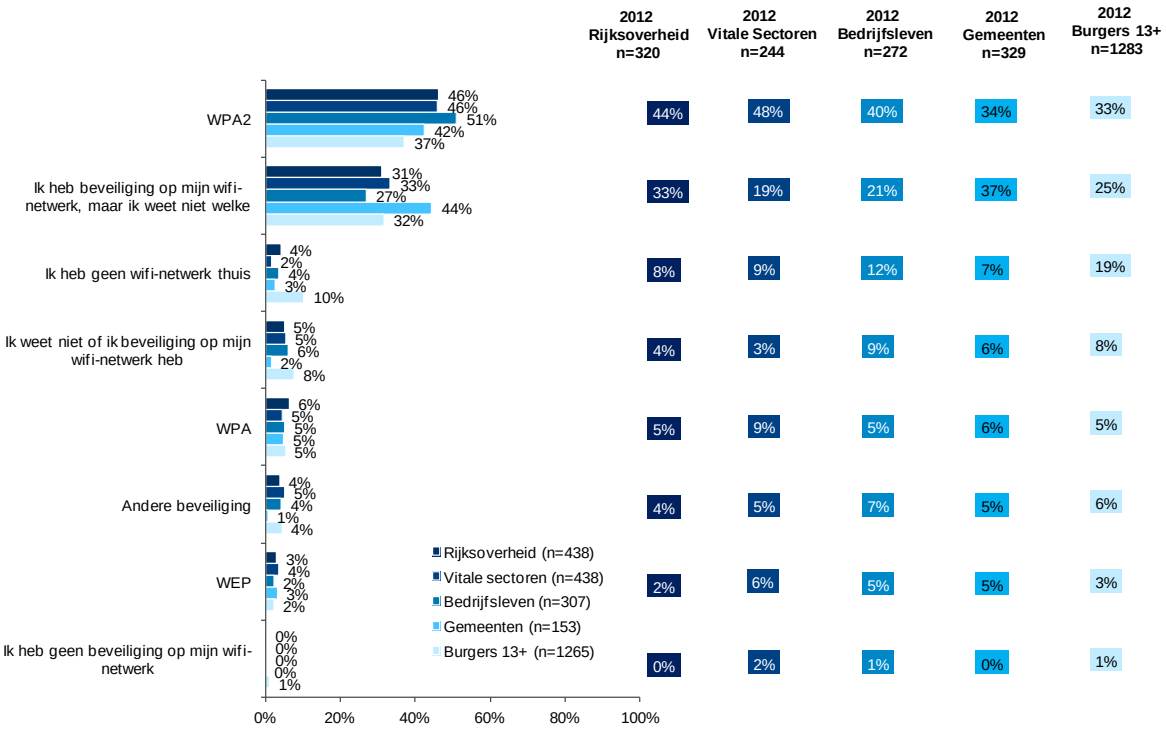
In deze paragraaf gaan we in op hoe het qua bewustzijn, kennis en gedrag gesteld is met de security awareness. Allereerst komen de algemene kennis en gedrag van burgers rondom digitale veiligheid aan de orde, gevolgd door hun behoefte aan informatie over de risico's van internet. Daarna gaan we in op de algemene kennis en gedrag van professionals ten aanzien van cyber security op het werk.

2.3.1 Algemene kennis en gedrag rondom digitale veiligheid

2.3.1.1 Iedereen heeft Wi-Fi-netwerk thuis beveiligd maar een derde weet niet hoe

Beveiliging via WPA2 is nog steeds de meest toegepaste beveiliging. Gemiddeld een derde van de ondervraagden weet niet wat voor beveiliging er op het wifi-netwerk thuis zit.

Figuur D7: Welke beveiliging staat er thuis aan op uw wifi-netwerk (draadloos netwerk)?



Vergelijking met 2012

Burgers en medewerkers van het bedrijfsleven gebruiken vaker WPA2 dan in 2012. Burgers en medewerkers van vitale sectoren weten vaker dan vorig jaar niet wat voor beveiliging er op het wifi-netwerk zit. Het gebruik van WEP of andere beveiliging in het algemeen is afgenomen. Alle doelgroepen zeggen minder vaak dat ze geen wifi-netwerk thuis te hebben. Dit geldt voor zowel de leidinggevenden als de niet-leidinggevenden.

Vergelijking tussen groepen
Gemeentemedewerkers weten vaker dan de andere doelgroepen niet wat voor beveiliging ze op hun wifi-netwerk hebben. Burgers hebben vaker dan de professionele doelgroepen helemaal geen wifi-netwerk thuis.

Vergelijking binnen groepen
Vrouwen (41%) weten veel vaker dan mannen (21%) niet welke beveiliging ze op hun wifi-netwerk hebben. Mannen (50%) geven veel vaker aan WPA2 te hebben dan vrouwen (24%). 17% van de vijftigplussers zegt thuis geen wifi-netwerk te hebben. Hoogopgeleiden en burgers jonger dan 50 jaar geven vaker aan dat ze WPA2 hebben. Laagopgeleide Rijksambtenaren geven relatief vaak aan dat ze niet weten of ze beveiliging op hun netwerk hebben. Medewerkers van boven de 50 jaar van de Rijksoverheid en het bedrijfsleven zeggen vaker dat ze andere beveiliging hebben dan jongere medewerkers.

2.3.1.2 Cookies zijn dit jaar alom bekend geraakt

Door het nieuwe beleid waarbij men toestemming moet geven om online gevolgd te worden door cookies is vrijwel iedereen nu op de hoogte van wat cookies zijn.

Figuur D8: Weet u wat cookies zijn? (weergave percentage "ja")

2012 Rijksoverheid n=320	2013 Rijksoverheid n=438	2012 Vitale sectoren n=244	2013 Vitale sectoren n=438	2012 Bedrijfsleven n=272	2013 Bedrijfsleven n=307	2012 Gemeenten n=329	2013 Gemeenten n=153	2012 Burgers 13+ n=1283	2013 Burgers 13+ n=1265
93%	99%	92%	98%	91%	98%	93%	98%	86%	93%

Vergelijking met 2012
Alle doelgroepen zijn gestegen wat betreft hun kennis van cookies. Deze stijging geldt zowel voor leidinggevenden als niet-leidinggevenden.

Vergelijking tussen groepen
De professionele doelgroepen geven vaker aan te weten wat cookies zijn dan de burgers.

Vergelijking binnen groepen
Bij de burgers weten hoog- en middenopgeleiden vaker wat cookies zijn dan de laagopgeleiden (89%).

2.3.1.3 Op de PC en laptop vertoont men veiliger gedrag dan op de tablet en smartphone

Als gekeken wordt naar verstandig of minder verstandig gedrag valt op dat men over het algemeen verstandiger om gaat met PC's en laptops dan met tablets en smartphones. Aan de andere kant zijn er natuurlijk ook een hoop handelingen die men niet uitvoert op de tablet of smartphone waardoor soms ook veilig gedrag minder noodzakelijk is.

Vraag D9:Kunt u voor de apparaten waar u thuis beschikking over heeft aangeven welke van de volgende uitspraken op u van toepassing zijn? (weergave percentage "van toepassing"

Deze tabel is weergegeven op de volgende bladzijde.

	Op de PC					Op de laptop					Op de tablet					Op de smartphone				
	Rijksoverheid (n=268)	Vitale sectoren (n=254)	Bedrijfsleven (n=185)	Gemeenten (n=125)	Burgers 13+ (n=844)	Rijksoverheid (n=372)	Vitale sectoren (n=354)	Bedrijfsleven (n=233)	Gemeenten (n=102)	Burgers 13+ (n=850)	Rijksoverheid (n=269)	Vitale sectoren (n=265)	Bedrijfsleven (n=181)	Gemeenten (n=73)	Burgers 13+ (n=503)	Rijksoverheid (n=262)	Vitale sectoren (n=278)	Bedrijfsleven (n=181)	Gemeenten (n=62)	Burgers 13+ (n=638)
Terughoudendheid gezond verstand																				
Ik ga voorzichtig om met e-mails, websites of aanbieders die ik niet vertrouw of niet ken	91%	84%	83%	93%	81%	86%	78%	82%	93%	81%	76%	70%	69%	76%	66%	68%	68%	67%	76%	65%
Ik open soms wel eens bestanden waarvan ik de zender niet ken	9%	14%	17%	32%	15%	10%	11%	9%	42%	11%	4%	8%	5%	28%	7%	7%	7%	3%	24%	6%
Ik ga nooit in op ongevraagde verzoeken per e-mail om in te loggen op een website of om mijn gegevens te bevestigen	78%	72%	69%	88%	72%	77%	71%	70%	82%	70%	67%	69%	64%	66%	60%	70%	63%	61%	67%	58%
Ik klik niet op links in e-mails, want die kunnen mij naar gevaarlijke websites sturen	46%	50%	42%	72%	43%	47%	49%	41%	66%	43%	41%	43%	40%	48%	35%	41%	42%	37%	52%	36%
Ik meld verdachte zaken op mijn apparaat bij een helpdesk	26%	21%	18%	72%	23%	19%	20%	18%	48%	21%	11%	15%	8%	28%	13%	9%	11%	4%	32%	10%
Ik weet hoe ik cookies in mijn browser kan verwijderen	81%	75%	81%	89%	64%	73%	71%	70%	77%	64%	47%	47%	54%	47%	44%	38%	41%	44%	50%	36%
Minder verstandig gedrag																				
Uit nieuwsgierigheid kijk ik bij spam meestal wel even waar het over gaat	7%	14%	17%	32%	13%	10%	11%	11%	35%	11%	4%	9%	5%	37%	5%	6%	3%	3%	23%	4%
Ik vind e-mail voldoende veilig om vertrouwelijke informatie te versturen	51%	51%	57%	77%	55%	46%	50%	53%	65%	52%	38%	37%	35%	38%	36%	33%	37%	36%	47%	38%
Wanneer ik vertrouwelijke informatie in een e-mail meestuur als bijlage, loop ik geen gevaar dat de inhoud door kwaadwillende bekeken wordt	19%	20%	23%	43%	26%	18%	17%	22%	41%	25%	13%	15%	13%	20%	13%	13%	12%	10%	28%	15%
Als ik een usb-stick als relatiegeschenk krijg, stop ik hem in het apparaat om te kijken wat er op staat.	40%	38%	39%	62%	33%	28%	34%	34%	61%	32%	5%	6%	6%	14%	5%	3%	4%	3%	19%	3%
Als ik ergens een verloren usb-stick vind, stop ik hem niet in het apparaat om te kijken wat er op staat	50%	43%	37%	76%	41%	42%	40%	37%	59%	38%	28%	28%	24%	43%	28%	24%	23%	18%	38%	24%
Laatste updates																				
Ik maak zo veel mogelijk gebruik van de mogelijkheden om automatische updates te laten installeren	69%	65%	66%	85%	65%	64%	59%	61%	73%	63%	49%	49%	49%	60%	41%	44%	46%	44%	59%	40%
Als ik op het apparaat een melding krijg dat er software-updates beschikbaar zijn, dan voer ik deze meestal niet uit	12%	12%	20%	34%	19%	10%	13%	16%	43%	19%	9%	12%	15%	32%	13%	13%	11%	15%	40%	14%
Ik controleer nooit bij de softwareleverancier of er updates beschikbaar zijn en installeer deze	11%	14%	15%	34%	14%	14%	15%	17%	44%	13%	9%	14%	13%	34%	10%	14%	10%	15%	47%	9%
Anti virussoftware en firewall																				
Op mijn apparaat is anti-virussoftware geactiveerd	88%	83%	83%	93%	85%	84%	78%	79%	85%	83%	38%	36%	38%	49%	41%	29%	27%	30%	45%	30%
Op mijn apparaat is geen anti-spywaresoftware geactiveerd	12%	12%	11%	31%	12%	9%	10%	12%	36%	10%	27%	26%	31%	42%	26%	38%	30%	37%	61%	31%
Op mijn apparaat is geen personal firewall geactiveerd	12%	13%	11%	33%	12%	10%	16%	16%	35%	12%	24%	28%	32%	48%	24%	33%	35%	33%	48%	29%
Ik zorg dat ik altijd beschik over de up-to-date versies van anti-virussoftware, anti-spywaresoftware en /of personal firewall	83%	70%	72%	89%	70%	71%	68%	66%	83%	68%	36%	35%	33%	46%	36%	27%	25%	26%	39%	28%
Weten bij wie je je gegevens achterlaat																				
Voordat ik inlog of mij registreer op een andere website dan die van de bank, controleer ik altijd het certificaat van de website (https/ slotje)	54%	50%	52%	84%	48%	46%	50%	47%	69%	47%	34%	38%	38%	53%	30%	28%	28%	21%	42%	21%
Voordat ik inlog of mij registreer op een website van de bank, controleer ik altijd het certificaat van de website (https/ slotje)	65%	64%	66%	83%	61%	58%	62%	61%	81%	57%	42%	46%	43%	47%	35%	34%	35%	31%	45%	28%
Als ik inlog of mij registreer op een website waar ik mijn persoonsgegevens moet invullen (veilingsite, webwinkel, etc.) controleer ik meestal niet het certificaat van de website (https/ slotje)	32%	34%	35%	48%	28%	33%	30%	34%	51%	31%	22%	30%	26%	43%	21%	22%	21%	26%	38%	20%

Vergelijking met 2012
Dit jaar zijn zeven uitspraken op negatieve wijze geherformuleerd, bijvoorbeeld ‘op mijn apparaat is een personal firewall geactiveerd’ is geworden ‘op mijn apparaat is geen personal firewall geactiveerd’. Hierdoor kunnen de uitspraken minder goed vergeleken worden met 2012. Maar in het algemeen valt wel op dat het gedrag niet veiliger is geworden. Zo checkt men veel minder vaak dan vorig jaar het certificaat van een website (https/slotje). Ook laat men minder vaak de software automatisch updaten en meldt men minder vaak verdachte zaken bij de helpdesk. Het zijn vooral de niet-leidinggevenden die lager scoren dan in 2012.

Vergelijking tussen groepen
De gemeentemedewerkers zijn bij deze vraag een zeer opvallende groep, ze hebben bijna overal een veel hogere score dan de overige doelgroepen op zowel de positieve als de negatieve statements. Dit suggereert dat een deel van de gemeentemedewerkers de uitspraken heeft aangevinkt zonder ze goed te lezen. Rijksambtenaren scoren goed op voorzichtig omgaan met e-mails van onbekende zenders, het niet openen van spam en zorgen dat de anti-virussoftware, anti-spysoftware en personal firewall up-to-date is.
Burgers lopen op een aantal punten achter op de professionele doelgroepen. Zo weten ze minder goed hoe ze cookies moeten verwijderen, laten ze minder vaak automatisch updates installeren en openen ze sneller e-mail van onbekende zenders.

Vergelijking binnen groepen
Bij de burgers zien we dat mannen vaker verstandig gedrag vertonen dan vrouwen. Verder vertoont men veiliger gedrag naarmate men ouder en hoger opgeleid is. Ook is er in een aantal gevallen een regionaal effect te zien, burgers uit de Randstad beveiligen zich beter dan burgers uit andere streken. Dit wordt wellicht veroorzaakt doordat men meer criminaliteit in de buurt gewend is en daarom minder goed van vertrouwen.

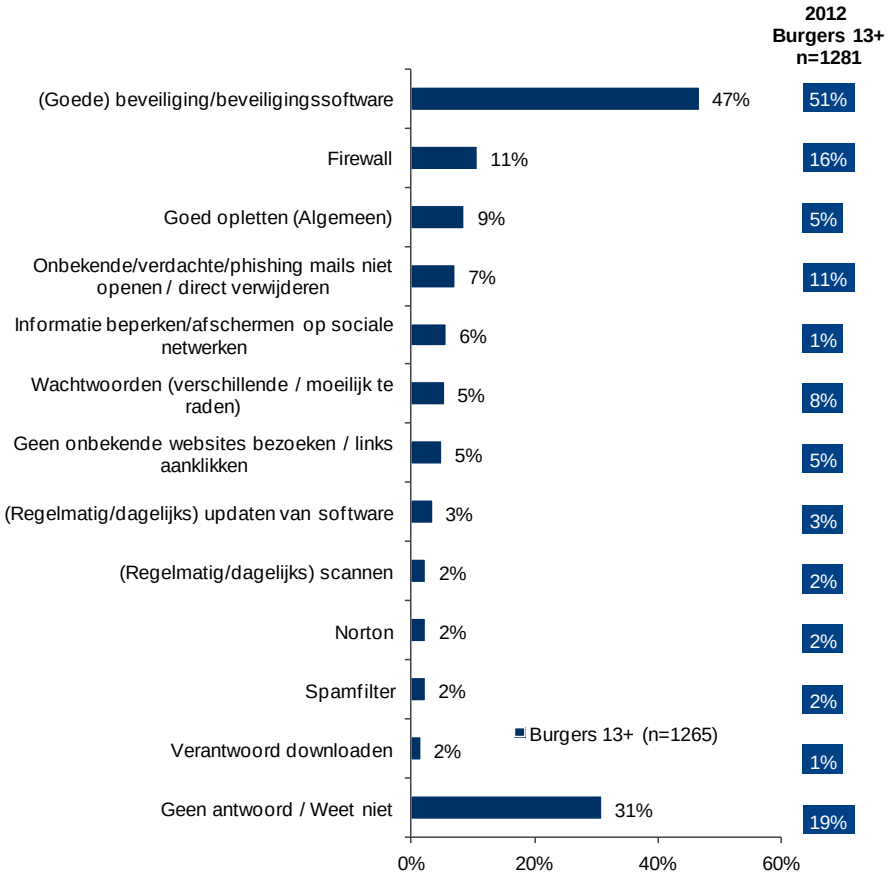
Bij Rijksambtenaren is voornamelijk een leeftijdseffect zichtbaar, medewerkers van onder de 30 vertonen minder verstandig gedrag dan medewerkers van boven de 30. Bij de gemeentemedewerkers is het vooral de groep 50+ die relatief hoog scoort op zowel verstandig als onverstandig gedrag. Voor medewerkers van de vitale sectoren geldt dat oudere medewerkers veiliger gedrag vertonen dan jongere medewerkers, met name beschikken ze vaker over up-to-date beveiligingssoftware. Bij de werknemers van het bedrijfsleven vertonen de hoogopgeleiden vaker verstandig gedrag, maar met name hun smartphone is vaak minder goed beveiligd.

2.3.2 Algemene kennis en gedrag burgers

2.3.2.1 De burger beschermt zichzelf hoofdzakelijk via beveiligingssoftware; een derde weet spontaan niet te noemen hoe hij zichzelf beschermt

Verder noemt men vooral de firewall en het niet openen van verdachte e-mails als goede methodes om jezelf te beschermen tegen misbruik, maar ook gewoon goed opletten in het algemeen.

Figuur D4: Wat doet u zelf om uzelf te beschermen tegen dergelijk misbruik?



Vergelijking met 2012

Het aantal burgers dat aangeeft deze vraag niet te kunnen beantwoorden is toegenomen ten opzichte van 2012. De volgende zaken worden minder vaak genoemd dan vorig jaar: beveiligingssoftware, firewall, verdachte mails niet openen en betere wachtwoorden. Beveiligingsmaatregelen die wel vaker genoemd worden zijn het afschermen of beperken van informatie op sociale media en goed opletten.

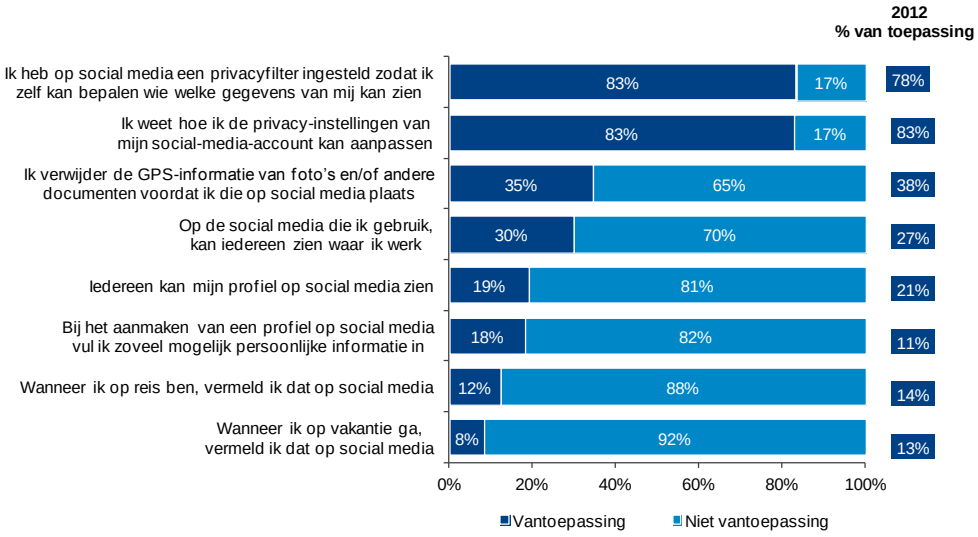
Vergelijking binnen Burgers 13+

Mannen noemen vaker beveiligingssoftware, firewall en updaten van software en vrouwen vaker verdachte mails niet openen en informatie op sociale netwerken afschermen. Burgers jonger dan 50 noemen vaker verantwoord downloaden en informatie op sociale netwerken afschermen. Hoogopgeleiden kunnen veel meer maatregelen noemen dan laagopgeleiden. 38% van de laagopgeleiden kiest voor het antwoord 'weet niet'.

2.3.2.2 Meerderheid burgers gaat zorgvuldig om met weergave van persoonlijke informatie op sociale media

De meerderheid van de burgers gaat zorgvuldig om met de weergave van persoonlijke informatie op social media. Steeds meer mensen stellen op social media een privacy filter in en men weet ook goed hoe een dergelijk filter aangepast dient te worden. Een op de vijf vult zijn profiel(en) zo volledig mogelijk in.

Figuur D6: Welke van de volgende uitspraken met betrekking tot uw social media gebruik zijn op u van toepassing?



Vergelijking met 2012

Ten opzichte van 2012 zijn er een aantal positieve ontwikkelingen te zien: zo is er een toename bij burgers wat betreft het instellen van een privacy filter op social media en een afname van het vermelden van vakanties op social media. Echter dit jaar vullen meer burgers dan in 2012 zoveel mogelijk persoonlijke informatie in op hun social media profiel.

Vergelijking binnen Burgers 13+

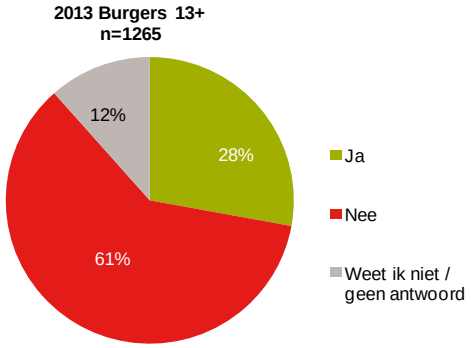
Vrouwen (13%) vullen minder vaak dan mannen (26%) zoveel mogelijk persoonlijke informatie in op hun profiel en ze hebben ook vaker een privacyfilter ingesteld dan mannen. 94% van de groep 18-30 heeft een privacyfilter ingesteld staan tegenover 76% van de vijftigplussers. 28% van de oudste groep heeft zijn profiel zichtbaar staan voor iedereen tegenover 10% van de groep 18-30 jaar. Burgers van onder de 30 zijn wel veel vaker geneigd om het op social media te melden als ze op vakantie of op reis gaan dan ouderen.

Hoogopgeleiden vermelden hun reizen en de plek waar ze werken ook vaker dan laagopgeleiden. De groep van 18-30 jaar weet vaker dan de groep 50+ hoe ze hun privacysettings aan moeten passen en verwijderen vaker de GPS-informatie van hun foto's voor ze die online plaatsen.

2.3.2.3 Ruim een kwart van de burgers heeft behoefte aan informatie over de risico's van internet

61% van de burgers heeft hier geen behoefte aan en 12% weet het niet zeker.

Figuur D10: Heeft u behoefte aan informatie over hoe u zich kunt beschermen tegen de risico's van internet?



Vergelijking met 2012

Vorig jaar werd een gelijke uitkomst gevonden als dit jaar.

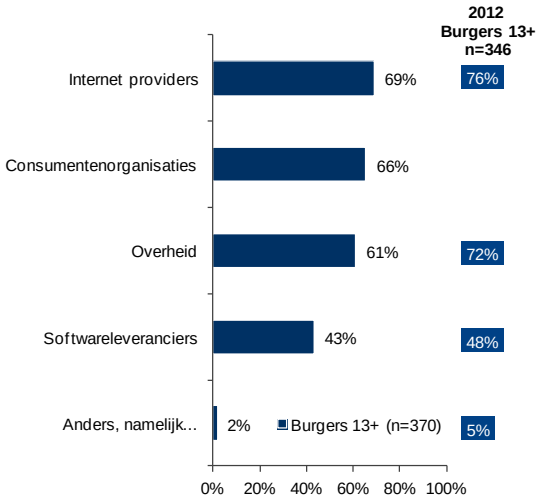
Vergelijking binnen Burgers 13+

Vrouwen (15%) geven vaker aan dan mannen (8%) geen antwoord op deze vraag te weten. Oudere burgers hebben meer behoefte dan jongere burgers aan extra informatie over de risico's van internet. Ook hebben hoogopgeleiden (40%) hier beduidend meer behoefte aan dan laag- en middenopgeleiden.

2.3.2.4 Burgers willen vooral informatie ontvangen van internet providers

Ook consumentenorganisaties lijkt tweederde van de burgers een geschikte bron voor meer informatie over hoe men zich kan beschermen tegen de risico's van internet, de overheid komt met 61% op de derde plaats.

Figuur D11: Van welke partijen wilt u informatie over hoe zich kunt beschermen tegen de risico's van internet?



Vergelijking met 2012
Consumentenorganisaties is er dit jaar nieuw bijgekomen als antwoordcategorie, mede hierdoor worden internet providers en de overheid minder vaak genoemd dan vorig jaar.

Vergelijking binnen Burgers 13+
Mannen noemen sofware leveranciers (53%) en internet providers (76%) vaker dan vrouwen. Vijftigplussers (76%) willen vaker informatie van internet providers ontvangen dan jongere burgers. Hoogopgeleiden kiezen liever voor consumentenorganisaties (81%) en de overheid (71%).

2.3.3 Algemene kennis en gedrag van professionals rondom digitale veiligheid

2.3.3.1 De diverse aspecten van digitale veiligheid zijn volgens de meerderheid vastgelegd in organisatiebeleid, digitaal veiligheidsbeleid is het vaakst vastgelegd bij de Rijksoverheid en het bedrijfsleven.

Volgens driekwart of meer van de respondenten is er binnen hun organisatie beleid voor een veilig wachtwoord gebruik en voor de omgang met apparaten (pc's, laptops, tablets, smartphones). Ongeveer tweederde geeft aan dat er beleid is voor het melden van incidenten, voor het bezoeken van websites en voor het updaten van antivirussoftware. Relatieve hekkensluiter is het beleid voor het gebruik van usb-sticks: gemiddeld geeft ongeveer de helft van de respondenten aan dat hun organisatie daarover beschikt.

Figuur C4: Zijn onderstaande zaken binnen uw organisatie vastgelegd in een beleid?

C4 % 'ja'	2012 Rijksoverheid n=522	2013 Rijksoverheid n=523	2012 Vitale sectoren n=554	2013 Vitale sectoren n=524	2012 Bedrijfsleven n=276	2013 Bedrijfsleven n=371	2012 Gemeenten n=550	2013 Gemeenten n=538
Beleid voor veilig wachtwoordgebruik	79%	90%	78%	81%	63%	79%	65%	84%
Beleid voor omgang met apparaten	75%	85%	68%	76%	50%	69%	57%	67%
Beleid voor melden incidenten	n.a.	82%	n.a.	72%	n.a.	64%	n.a.	56%
Beleid voor internetgebruik	64%	74%	70%	69%	51%	58%	64%	59%
Back-upbeleid	63%	67%	68%	71%	60%	65%	67%	58%
Beleid voor updaten antivirussoftware	56%	68%	63%	67%	53%	63%	51%	52%
Beleid voor omgang met usb-sticks	59%	73%	57%	55%	34%	43%	33%	33%

Vergelijking met 2012

In bovenstaande tabel is een significante stijging ten opzichte van vorig jaar met groen aangegeven en een significante daling met rood. Zowel de medewerkers van de Rijksoverheid als het bedrijfsleven geven aan op meerdere punten vaker beleid te hebben voor wat betreft de omgang met digitale veiligheid. Zowel voor leidinggevenden als niet-leidinggevenden is de kennis van het bestaan van beleid op de meeste punten gestegen, maar dit is vaker significant voor de leidinggevenden.

Vergelijking tussen groepen

De Rijksoverheid heeft vaker dan de overige doelgroepen een beleid voor veilig wachtwoordgebruik, internetgebruik, beleid voor de omgang met usb-sticks en computers en voor het melden van incidenten. Bijna vier op de tien (38%) gemeentemedewerkers weet niet of er een beleid is voor het updaten van antivirussoftware.

Rijksambtenaren en medewerkers bij de vitale sectoren hebben vaker dan de andere groepen beleid over welke websites ze op het werk mogen bezoeken en welke niet. Ruim een kwart (28%) van de Rijksambtenaren en 34% van de gemeentemedewerkers weet niet of er sprake is van een back-upbeleid. Ook is 45% van de gemeentemedewerkers zich er niet van bewust of er een beleid geldt voor de omgang met usb-sticks en 32% weet niet of er een beleid is voor het melden van incidenten.

Vergelijking binnen groepen

Voor de meeste punten geldt dat de oudere Rijksambtenaren beter op de hoogte zijn of er beleid bestaat dan de groep van 18-30 jaar. Dit wordt waarschijnlijk veroorzaakt doordat de meeste leidinggevenden ouder dan 30 jaar zijn. Ook voor de medewerkers van de vitale sectoren geldt dat de ouderen beter weten of er beleid bestaat dan de jongeren, verder geldt ook dat men zich meer bewust is van het beleid als men hoger opgeleid is. Bij de medewerkers van het bedrijfsleven geeft de groep 50+ vaker aan dat er beleid bestaat voor de omgang met usb-sticks en computers en het melden van incidenten.

2.3.3.2 Volgens zeven op de tien werknemers heeft hun werkgever een beleid voor de digitale omgeving voor alle werknemers

Gemiddeld geeft 69% van de ondervraagden aan dat de organisatie voor alle werknemers een beleid heeft op het gebied van de digitale omgeving. De helft geeft aan dat medewerkers weten hoe te handelen bij incidenten en dat er maatregelen worden uitgevoerd bij vertrek van medewerkers. 46% zegt dat alle medewerkers een terugkoppeling ontvangen na een incident en 43% dat nieuwe medewerkers worden ingewerkt op de maatregelen rondom veilig digitaal werken. Vier op de tien (41%) respondenten geeft aan dat leidinggevenden erop toe zien dat alle medewerkers op de hoogte zijn van het beleid en 26% dat het naleven van regels rondom digitale veiligheid deel uitmaakt van de functioneringsgesprekken.

Figuur C5: In hoeverre vindt u de volgende stellingen van toepassing op uw organisatie? (weergave percentage "wel van toepassing" + "meer wel dan niet van toepassing")

	Rijksoverheid		Vitale sectoren		Bedrijfsleven		Gemeenten	
	2013 n=523	2012 n=522	2013 n=524	2012 n=554	2013 n=371	2012 n=276	2013 n=538	2012 n=550
Onze organisatie heeft een beleid voor alle werknemers m.bt. tot de digitale omgeving	78%	76%	66%	75%	62%	58%	52%	65%
De medewerkers weten hoe te handelen bij incidenten	60%	56%	59%	64%	53%	51%	33%	39%
Bij vertrek van medewerkers worden maat-regelen uitgevoerd t.a.v. digitale veiligheid	55%	34%	56%	55%	49%	47%	33%	34%
Na een incident ontvangen alle medewerkers hier direct een terugkoppeling over	52%	58%	52%	58%	47%	51%	32%	52%
Nieuwe medewerkers worden ingewerkt in de maatregelen rondom veilig digitaal werken	52%	35%	52%	60%	46%	42%	22%	27%
De leidinggevenden zien er op toe dat alle medewerkers op de hoogte zijn van beleid m.b.t. de digitale werkomgeving	51%	41%	52%	61%	43%	43%	20%	34%
Het naleven van regels rondom digitale veiligheid maakt deel uit van functioneringsgesprekken	37%	22%	31%	46%	29%	30%	9%	10%

Vergelijking met 2012

Een significante stijging ten opzichte van vorig jaar is met groen aangegeven en een significante daling met rood. Bij de Rijksambtenaren is er op vier punten sprake van een verbetering ten opzichte van 2012. Voor de medewerkers van de vitale sectoren geldt dat er sprake is van een daling op vier punten. Bij gemeentemedewerkers is er een daling te zien op drie punten.

Niet-leidinggevenden geven minder vaak aan dat er een beleid met betrekking tot de digitale omgeving is, dat alle medewerkers terugkoppeling ontvangen na een incident en dat leidinggevenden erop toe zien dat alle werknemers het beleid kennen. Bij de stelling dat er maatregelen worden uitgevoerd bij het vertrek van een medewerker is juist een stijging te zien onder niet-leidinggevenden ten opzichte van 2012.

Vergelijking tussen groepen
De gemeentemedewerkers geven voor alle stellingen aan dat ze minder van toepassing zijn dan de overige professionele doelgroepen. Ambtenaren van de Rijksoverheid hebben vaker dan de overige groepen een beleid voor alle werknemers met betrekking tot de digitale omgeving.

Vergelijking binnen groepen
De stellingen worden vaker onderschreven door Rijksambtenaren uit de groep 50+ dan door jongere Rijksambtenaren, waarschijnlijk omdat dit vaker leidinggevenden zijn. Ook bij gemeentemedewerkers en medewerkers van het bedrijfsleven geven de vijftigplussers eerder aan dat de stellingen van toepassing zijn. Verder scoren bij de gemeenten de middenopgeleiden ook hoger dan de hoogopgeleiden. Jongeren van 18-30 jaar en laagopgeleiden geven bij de medewerkers van de vitale sectoren significant vaker aan dat de stellingen niet van toepassing zijn.

2.3.3.3 Vitale sectoren krijgen het minst vaak uitleg over veilig gebruik van apparatuur

Deze vraag is gesteld aan medewerkers die een laptop, tablet of smartphone bezitten via hun werkgever en deze zowel voor zakelijke als privédoeleinden gebruiken. Gemiddeld heeft 74% van de ondervraagden een instructie van zijn werkgever gekregen over veilig gebruik van hun apparatuur.

Figuur S3e: Heeft u van uw werkgever instructies ontvangen voor het veilig gebruik van uw laptop, tablet of smartphone?

S3e	2013 Rijksoverheid n=147	2012 Rijksoverheid n=148	2013 Vitale sectoren n=186	2012 Vitale sectoren n=196	2013 Bedrijfsleven n=110	2012 Bedrijfsleven n=65	2013 Gemeenten n=153	2012 Gemeenten n=133
% 'Ja'	93%	82%	68%	80%	81%	58%	74%	64%

Vergelijking met 2012
Rijksambtenaren, gemeentemedewerkers en medewerkers van het bedrijfsleven geven vaker dan in 2012 aan een instructie van hun werkgever te hebben ontvangen. Medewerkers van de vitale sectoren hebben juist minder vaak een instructie ontvangen dan verleden jaar.

Vergelijking tussen groepen
De Rijksambtenaren geven vaker aan een instructie te hebben ontvangen dan de overige professionele doelgroepen. 31% van de gemeentemedewerkers geeft aan geen instructie te hebben ontvangen, dat is meer dan bij de Rijksambtenaren en de medewerkers van vitale sectoren.

Vergelijking binnen groepen
40% van de laagopgeleide medewerkers van vitale sectoren die in het bezit zijn van een laptop, tablet of smartphone geeft aan geen instructie te hebben ontvangen voor het veilige gebruik hiervan. Verder zijn er geen significante verschillen door de grootte van de groepen.

2.3.3.4 Bewustzijn van digitale veiligheid is sterk gestegen volgens leidinggevenden Rijksoverheid

Volgens de ruime meerderheid van de werknemers (ongeveer twee derde of meer) zijn medewerkers zich bewust van het belang en de gevaren rondom digitale veiligheid, zijn zij voldoende op de hoogte van hun eigen verantwoordelijkheden en weten zij de weg naar informatie hierover te vinden. Vijf tot zes op de tien medewerkers geven aan dat werknemers in hun organisatie goed op de hoogte zijn van het organisatiebeleid aangaande digitale veiligheid, de informatie hierover als eenduidig ervaren en dat zij de indruk hebben dat medewerkers de afspraken rondom protocollen strikt opvolgen.
Daarentegen hebben vier op de tien respondenten de indruk dat medewerkers die op de hoogte zijn niet altijd alle protocollen toepassen en denken drie op de tien respondenten dat medewerkers niet op de hoogte zijn van het beleid rondom digitale veiligheid.

Figuur C6: In hoeverre vindt u de volgende stellingen van toepassing op de medewerkers in uw organisatie? (weergave percentage "wel van toepassing" + "meer wel dan niet van toepassing")

	Rijksoverheid		Vitale sectoren		Bedrijfsleven		Gemeenten	
	2013 n=105	2012 n=84	2013 n=117	2012 n=155	2013 n=97	2012 n=62	2013 n=92	2012 n=101
Medewerkers weten waar zij terecht kunnen voor informatie over digitale veiligheid	82%	n.a.	68%	n.a.	72%	n.a.	70%	n.a.
Medewerkers zijn op de hoogte van hun eigen verantwoordelijkheden	84%	63%	69%	73%	67%	65%	46%	59%
Medewerkers zijn zich voldoende bewust belang digitale veiligheid	83%	68%	71%	66%	66%	63%	41%	54%
Medewerkers zijn zich voldoende bewust van gevaren die zich binnen organisatie kunnen voordoen	79%	60%	66%	66%	66%	60%	39%	50%
Medewerkers zijn goed op de hoogte van het organisatiebeleid	76%	41%	62%	60%	65%	53%	28%	38%
Medewerkers ervaren informatie over digitale veiligheid als helder en eenduidig	67%	35%	57%	59%	62%	50%	29%	41%
Medewerkers houden zich strikt aan afspraken rondom uitvoering van protocollen	69%	44%	58%	58%	59%	47%	24%	36%
Medewerkers die op de hoogte zijn, passen niet alle veiligheidsprotocollen toe	43%	36%	41%	44%	48%	52%	36%	41%
Medewerkers zijn niet op de hoogte van beleid over digitale veiligheid	30%	35%	33%	37%	37%	36%	46%	39%

Vergelijking met 2012

Deze vraag is alleen gesteld aan leidinggevenden waardoor de subgroepen vrij klein zijn en de verschillen minder snel significant zijn. Significante stijgingen ten opzichte van vorig jaar zijn met groen aangegeven in de tabel; er zijn alleen significante verschillen te zien bij de werknemers van de Rijksoverheid. Bij de leidinggevenden van de Rijksoverheid is er een sterke stijging op zes statements omtrent het bewustzijn en het naleven van beleid ten aanzien van de digitale veiligheid op het werk te zien.

De uitspraak *Medewerkers weten waar zij terecht kunnen voor informatie over digitale veiligheid* is dit jaar voor het eerst gesteld en kan daarom niet in de tijd worden vergeleken.

Vergelijking tussen groepen
De leidinggevenden van de gemeenten geven hun medewerkers een lagere score voor zes van de negen statements dan de leidinggevenden van de overige professionele doelgroepen. Leidinggevenden van gemeenten geven vaker (39%) aan dat medewerkers de informatie over digitale veiligheid niet als helder en eenduidig ervaren ten opzichte van leidinggevende van de Rijksoverheid (13%).

Vergelijking binnen groepen
Van de leidinggevenden van de gemeente van boven de 50 geeft 40% aan dat de medewerkers goed op de hoogte zijn van het organisatiebeleid tegenover 19% van de leidinggevenden van 31-49 jaar. Een dergelijk verschil is ook zichtbaar bij drie andere uitspraken, leidinggevenden van 50+ zijn daar positiever dan jongere bij de gemeenten. Ook de leidinggevenden van de vitale sectoren en het bedrijfsleven zijn vaak positiever over het bewustzijn van het digitale veiligheidsbeleid bij medewerkers naarmate ze ouder zijn. Wellicht valt dit verschil te verklaren doordat oudere leidinggevenden vaak hoger geplaatst zijn en verder afstaan van de dagelijkse werkzaamheden van jongere uitvoerenden.

2.3.3.5 Merendeel professionals acht zich voldoende bewust van het belang van digitale veiligheid

Gemiddeld 86% van de professionals vindt zich voldoende bewust van het belang van digitale veiligheid, 82% zegt voldoende op de hoogte te zijn van de eigen verantwoordelijkheden en 78% dat ze voldoende bewust zijn van de gevaren op het gebied van digitale veiligheid. Ruim driekwart weet bij wie ze een incident dienen te melden en 71% zegt zich strikt aan de afspraken rondom de uitvoering van de protocollen te houden. Informatie over digitale veiligheid ervaart 62% als helder en eenduidig. Iets minder dan de helft stimuleert collega's om zich volgens de regels te gedragen. Wanneer een collega een regel veronachtzaamt, wijst 43% zijn collega hierop. Een derde geeft toe niet goed op de hoogte te zijn van het beleid met betrekking tot digitale veiligheid.

Figuur C7: In hoeverre vindt u de volgende stellingen van toepassing op uzelf in uw werksituatie? (weergave percentage "wel van toepassing" + "meer wel dan niet van toepassing")

	2013 Rijksoverheid n=523	2012 Rijksoverheid n=522	2013 Vitale sectoren n=524	2012 Vitale sectoren n=554	2013 Bedrijfsleven n=371	2012 Bedrijfsleven n=276	2013 Gemeenten n=538	2012 Gemeenten n=550
Ik ben me voldoende bewust van het belang van digitale veiligheid	88%	90%	84%	82%	83%	77%	88%	85%
Ik ben voldoende op de hoogte van mijn eigen verantwoordelijkheden	86%	85%	82%	82%	79%	78%	80%	80%
Ik ben me voldoende bewust van de gevaren op het gebied van digitale veiligheid	86%	75%	77%	78%	72%	69%	75%	63%
Ik weet bij wie ik een incident dien te melden	79%	73%	75%	78%	75%	76%	79%	74%
Ik houd me strikt aan de afspraken rondom de uitvoering van de protocollen	77%	73%	73%	75%	66%	67%	67%	62%
Informatie over digitale veiligheid ervaar ik als helder en eenduidig	70%	n.a.	69%	n.a.	63%	n.a.	45%	n.a.
Ik stimuleer mijn collega's zich volgens de regels te gedragen	52%	41%	51%	58%	46%	47%	37%	35%
Ik maak collega's er op attent wanneer ze een regel veronachtzamen	48%	37%	47%	54%	43%	43%	33%	33%
Ik ben niet goed op de hoogte van het beleid over digitale veiligheid	30%	n.a.	31%	n.a.	32%	n.a.	44%	n.a.

Vergelijking met 2012

De significante verschillen met 2012 per doelgroep zijn in de tabel aangegeven met groen bij een stijging en met rood bij een daling. Gemiddeld is men zich vaker bewust van het belang van digitale veiligheid dan in 2012 (84%). Ook het bewustzijn van de gevaren is gestegen ten opzichte van vorig jaar (71%). De stellingen 'Informatie over digitale veiligheid ervaar ik als helder en eenduidig' en 'Ik ben niet goed op de hoogte van het beleid over digitale veiligheid' worden dit jaar voor het eerst gesteld.

Vergelijking tussen groepen

Rijksambtenaren zijn zich vaker bewust van de mogelijke gevaren op het gebied van digitale veiligheid dan de overige professionele doelgroepen. Informatie over digitale veiligheid wordt door de gemeentemedewerkers minder vaak als helder en eenduidig ervaren dan door de overige groepen. Werknemers van het bedrijfsleven en de gemeenten vinden zichzelf minder vaak dan de Rijksambtenaren voldoende op de hoogte van de eigen verantwoordelijkheden rondom digitale veiligheid. Ook houden Rijksambtenaren zich vaker strikt aan de regels dan de medewerkers van gemeenten en het bedrijfsleven. Gemeentemedewerkers maken hun collega's minder vaak dan de andere ondervraagden erop attent wanneer ze een bepaalde regel veronachtzamen en ze stimuleren ze ook minder om zich volgens de regels te gedragen. De gemeentemedewerkers geven ook het vaakst aan niet goed op de hoogte te zijn van het beleid over digitale veiligheid.

Vergelijking binnen groepen

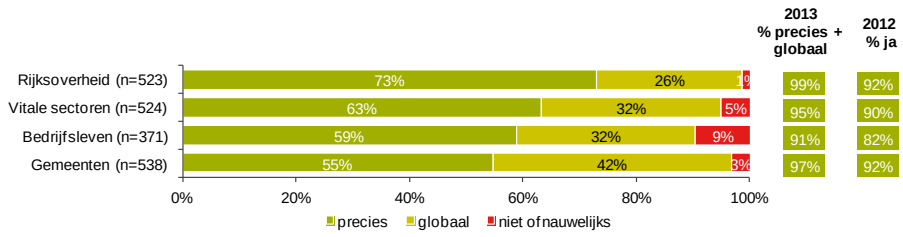
Jongere medewerkers van de Rijksoverheid en de vitale sectoren weten minder goed bij wie ze een incident moeten melden dan oudere medewerkers. Naarmate medewerkers van de Rijksoverheid, gemeenten en vitale sectoren ouder zijn, geven ze eerder aan zich bewust te zijn van het belang van digitale veiligheid en dat ze zich voldoende bewust zijn van de mogelijke gevaren. Ook vinden Rijksambtenaren en medewerkers van vitale sectoren die ouder zijn dan 50 jaar de beschikbare informatie vaker helder en eenduidig.

Deze zelfde groep zegt ook vaker voldoende op de hoogte te zijn van de eigen verantwoordelijkheden en dat ze zich strikt aan de afspraken rondom de uitvoering van de protocollen houden. Hoogopgeleide gemeentemedewerkers wijzen collega's er minder vaak op dat ze een regel veronachtzamen en geven ook minder vaak aan dat ze collega's stimuleren om zich volgens de regels te gedragen dan middenopgeleide gemeentemedewerkers. Medewerkers van vitale sectoren van 18-30 jaar doen beide zaken ook minder snel dan medewerkers van boven de 30 jaar. Hoogopgeleide medewerkers van het bedrijfsleven stimuleren hun collega's minder om zich volgens de regels te gedragen dan laagopgeleide medewerkers.

2.3.3.6 Vrijwel alle Rijksambtenaren weten welke informatie gevoelig is

Doordat de antwoordcategorieën van de volgende vijf vragen dit jaar zijn aangepast van 'ja' naar 'precies' en 'globaal', zijn ze niet goed te vergelijken met 2012.
Gemiddeld weet 63% precies welke informatie binnen de organisatie gevoelig is, 4% weet dit niet.

Figuur C1_1:In hoeverre weet u welke informatie binnen uw organisatie gevoelig is?



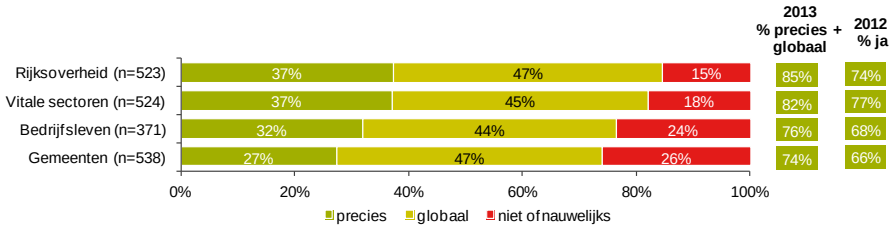
Vergelijking tussen groepen
De Rijksambtenaren geven vaker het antwoord 'precies' en de gemeentemedewerkers vaker het antwoord 'globaal' dan de overige professionele doelgroepen.

Vergelijking binnen groepen
Gemeentemedewerkers van 50+ geven vaker het antwoord 'niet of nauwelijks' (5%). Hoog- en middenopgeleide medewerkers van de vitale sectoren weten vaker welke informatie gevoelig is dan de laagopgeleiden. Dit geldt ook voor de medewerkers van het bedrijfsleven.

2.3.3.7 Een kwart van de gemeentemedewerkers weet niet welke actie te ondernemen bij een incident

Gemiddeld een derde van de ondervraagden weet precies wat ze moeten doen als er een incident plaats vindt, een vijfde heeft hier in het geheel geen idee van.

Figuur C1_2:In hoeverre weet u wat u moet doen wanneer er een incident plaatsvindt die de digitale veiligheid in het gevaar brengt?



Vergelijking tussen groepen

De Rijksambtenaren en medewerkers van de vitale sectoren geven vaker het antwoord ‘precies’ dan de gemeentemedewerkers. De gemeentemedewerkers en medewerkers van het bedrijfsleven zeggen vaker ‘niet of nauwelijks’ dan de Rijksambtenaren.

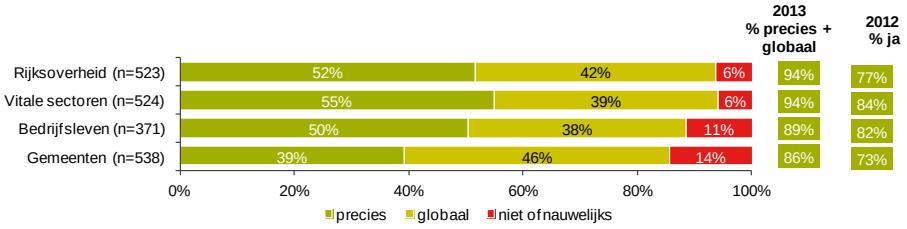
Vergelijking binnen groepen

Bij de Rijksambtenaren geeft men vaker aan precies te weten wat te doen bij een incident naarmate men ouder is. Ook bij de gemeentemedewerkers geeft de groep 50+ (18%) minder vaak aan niet te weten wat te doen dan de groep 31-49 jaar (28%). Wat wel opvallend is, is dat juist 29% van de hoogopgeleide gemeentemedewerkers kiest voor ‘niet of nauwelijks’.

2.3.3.8 De helft van de professionals weet precies waar op te letten bij een link in e-mail

Gemiddeld weet bijna de helft van de medewerkers precies waar ze op moeten letten bij een link in een e-mail, maar 9% weet dit niet.

Figuur C1_3:In hoeverre weet u waar u op moet letten wanneer u een e-mail ontvangt met daarin een link?



Vergelijking tussen groepen

Gemeentemedewerkers kiezen minder vaker voor ‘precies’ en vaker voor ‘niet of nauwelijks’ dan de Rijksambtenaren en medewerkers van de vitale sectoren. Ook de medewerkers van het bedrijfsleven weten vaker niet waar ze op moeten letten als ze een e-mail met een link krijgen.

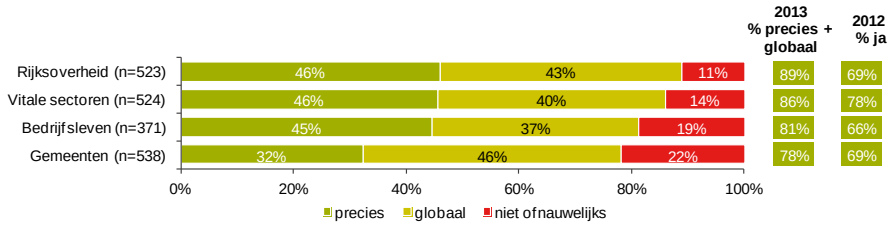
Vergelijking binnen groepen

Rijksambtenaren weten weer beter waar ze op moeten letten bij oplopende leeftijd. Bij de medewerkers van het bedrijfsleven weten leidinggevenden (49%) vaker precies hoe ze naar een link in een e-mail moeten kijken dan de niet-leidinggevenden (26%).

2.3.3.9 Meer dan driekwart weet welke websites men mag bezoeken

Gemiddeld weet 46% precies welke websites bezocht mogen worden op de zakelijke computer. 16% is hier niet van op de hoogte.

Figuur C1_4:In hoeverre weet u welke websites u wel en niet mag bezoeken op uw zakelijke computer?



Vergelijking tussen groepen

Meer dan een vijfde van de gemeentemedewerkers en bijna een vijfde van de medewerkers van het bedrijfsleven geeft aan niet te weten welke websites ze wel en niet mogen bezoeken op hun zakelijke computer, dit is vaker dan bij de Rijksambtenaren en medewerkers van de vitale sectoren.

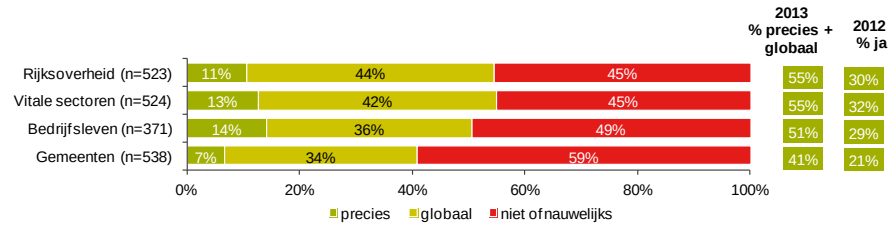
Vergelijking binnen groepen

De Rijksambtenaren geven weer vaker aan precies te weten welke websites ze mogen bezoeken naarmate ze ouder zijn. Hoogopgeleide Rijksambtenaren (38%) weten dit minder vaak precies dan laagopgeleide Rijksambtenaren (63%). Bij medewerkers van het bedrijfsleven zijn leidinggevenden vaker precies op de hoogte dan niet-leidinggevenden.

2.3.3.10 Men is niet goed bekend met de zwakke plekken in de organisatie

Gemiddeld weet slechts 11% van de ondervraagden waar de zwakke plekken in de digitale veiligheid van de organisatie zitten. De helft is hier niet of nauwelijks van op de hoogte.

Figuur C1_5:In hoeverre weet u wat de zwakke plekken zijn in de digitale veiligheid van uw organisatie?



Vergelijking tussen groepen

Gemeentemedewerkers zijn minder vaak op de hoogte van waar de zwakke plekken zitten dan de overige professionele doelgroepen.

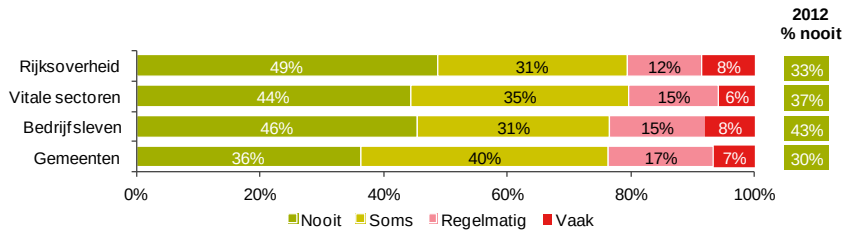
Vergelijking binnen groepen

Voor alle groepen geldt dat niet-leidinggevenden vaker niet of nauwelijks op de hoogte zijn van zwakke plekken in de digitale veiligheid dan leidinggevenden.

2.3.3.11 Men deelt minder vaak bedrijfsgevoelige informatie via e-mail

Gemiddeld deelt 44% van de ondervraagden nooit bedrijfsgevoelige informatie via e-mail, 35% doet dit soms, 15% regelmatig en 7% vaak.

Figuur C2_1: Hoe vaak deelt u gevoelige bedrijfsinformatie via e-mail?



Vergelijking met 2012

De medewerkers van de Rijksoverheid, de gemeenten en de vitale sectoren geven vaker aan dan in 2012 dat ze nooit bedrijfsgevoelige informatie delen via e-mail.

Vergelijking tussen groepen

Gemeentemedewerkers geven minder vaak aan nooit e-mail hiervoor te gebruiken dan de overige professionele doelgroepen.

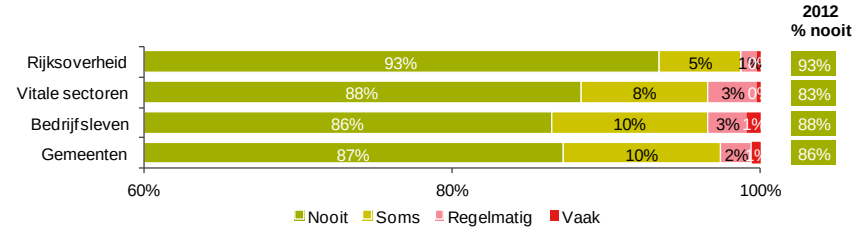
Vergelijking binnen groepen

Jonge en laagopgeleide medewerkers delen vaker gevoelige informatie per e-mail dan ouderen en hoogopgeleiden.

2.3.3.12 Minder dan 15% deelt gevoelige informatie via de cloud

Gemiddeld deelt 89% van de ondervraagden nooit bedrijfsgevoelige informatie via de cloud, 8% doet dit soms en 2% regelmatig en 1% vaak .

Figuur C2_2: Hoe vaak deelt u gevoelige bedrijfsinformatie via de cloud?



Vergelijking met 2012

De medewerkers van de vitale sectoren geven vaker aan dan in 2012 dat ze nooit bedrijfsgevoelige informatie delen via de cloud.

Vergelijking tussen groepen

Rijksambtenaren geven vaker aan nooit de cloud te gebruiken dan de overige doelgroepen.

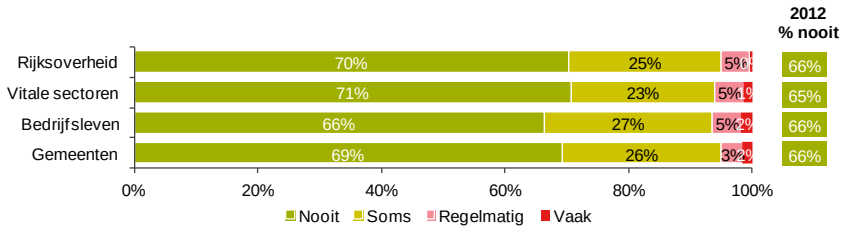
Vergelijking binnen groepen

Bij de gemeenten, vitale sectoren en het bedrijfsleven delen de leidinggevenden vaker bedrijfsgevoelige informatie via de cloud dan de niet-leidinggevenden.

2.3.3.13 Een derde van het bedrijfsleven deelt wel eens gevoelige informatie via een usb-stick

Gemiddeld deelt 69% van de ondervraagden nooit bedrijfsgevoelige informatie via een usb-stick, 25% doet dit soms, 4% regelmatig en 1% vaak.

Figuur C2_3: Hoe vaak deelt u gevoelige bedrijfsinformatie via een usb-stick?



Vergelijking met 2012

De Rijksambtenaren en medewerkers van vitale sectoren delen minder vaak bedrijfsgevoelige informatie via een usb-stick dan in 2012. Er zijn geen significante verschillen tussen de doelgroepen.

Vergelijking binnen groepen

Hoogopgeleide en leidinggevende medewerkers van de Rijksoverheid, vitale sectoren en het bedrijfsleven delen vaker bedrijfsgevoelige informatie via een usb-stick dan middenopgeleide en niet-leidinggevende medewerkers.

2.3.3.14 Vitale sectoren krijgen het minst vaak uitleg over veilig gebruik van apparatuur

Deze vraag is gesteld aan medewerkers die een laptop, tablet of smartphone bezitten via hun werkgever en deze zowel voor zakelijke als privédoeleinden gebruiken. Gemiddeld heeft 74% van de ondervraagden een instructie van zijn werkgever gekregen over veilig gebruik van hun apparatuur.

Figuur S3e: Heeft u van uw werkgever instructies ontvangen voor het veilig gebruik van uw laptop, tablet of smartphone? (weergave percentage "ja")

S3e	2013 Rijksoverheid n=147	2012 Rijksoverheid n=148	2013 Vitale sectoren n=186	2012 Vitale sectoren n=196	2013 Bedrijfsleven n=110	2012 Bedrijfsleven n=65	2013 Gemeenten n=153	2012 Gemeenten n=133
% 'Ja'	93%	82%	68%	80%	81%	58%	74%	64%

Vergelijking met 2012

Rijksambtenaren, gemeentemedewerkers en medewerkers van het bedrijfsleven geven vaker dan in 2012 aan een instructie van hun werkgever te hebben ontvangen. Medewerkers van de vitale sectoren hebben juist minder vaak een instructie ontvangen dan verleden jaar.

Vergelijking tussen groepen

De Rijksambtenaren geven vaker aan een instructie te hebben ontvangen dan de overige professionele doelgroepen. 31% van de gemeentemedewerkers geeft aan geen instructie te hebben ontvangen, dat is meer dan bij Rijksambtenaren en medewerkers van vitale sectoren.

Vergelijking binnen groepen

40% van de laagopgeleide medewerkers van vitale sectoren die in het bezit zijn van een laptop, tablet of smartphone geeft aan geen instructie te hebben ontvangen voor het veilige gebruik hiervan. Verder zijn er geen significante verschillen door de grootte van de groepen.

2.3.3.15 De vitale sectoren gaan minder voorzichtig om met openbare wifi dan in 2012

Gemiddeld laat 80% zijn zakelijke smartphone of tablet niet door anderen gebruiken. Evenmin wil tweederde zijn pc of laptop delen. Een beveiligde verbinding wordt door 60% gebruikt voor het werk. Bij een openbare wifi-verbinding denkt 46% van de ondervraagden na over welke handelingen men wel of niet kan verrichten. 30% laat zijn computer wel eens onbeheerd achter en 16% laat een usb-stick controleren op virussen als deze extern is geweest. Na gebruik van een openbare wifi verbinding past een kleine minderheid 6%) zijn wachtwoorden aan.

Figuur C3: Zijn de volgende stellingen op u van toepassing? (weergave percentage "van toepassing")

	2013 Rijksoverheid n=523	2012 Rijksoverheid n=522	2013 Vitale sectoren n=524	2012 Vitale sectoren n=554	2013 Bedrijfsleven n=371	2012 Bedrijfsleven n=276	2013 Gemeenten n=538	2012 Gemeenten n=550
Ik laat mijn zakelijke tablet of smartphone niet door anderen gebruiken	83%	81%	80%	75%	81%	76%	75%	75%
Ik laat mijn pc of laptop niet door anderen gebruiken	68%	59%	69%	66%	60%	55%	n.a.	49%
Ik maak voor mijn werk gebruik van een VPN-verbinding of een andere beveiligde verbinding	63%	64%	65%	60%	53%	44%	57%	43%
Wanneer ik gebruik maak van een openbare wifiverbinding, maak ik bewuste keuzes welke handelingen ik verricht	46%	46%	44%	52%	50%	42%	43%	35%
Ik laat wel eens een PC of laptop onbeheerd achter	25%	n.a.	26%	n.a.	34%	n.a.	35%	n.a.
Een usb-stick die buiten de organisatie is geweest, laat ik door de systeembeheerder controleren op virussen	19%	12%	16%	23%	16%	20%	11%	13%
Wanneer ik een openbare wifiverbinding heb gebruikt, wijzig ik daarna mijn wachtwoord(en)	5%	7%	7%	17%	8%	13%	4%	4%

Vergelijking met 2012

De significante verschillen per doelgroep staan in de tabel met rood en groen aangegeven. Wachtwoorden worden minder dan in 2012 (10%) gewijzigd na gebruik te hebben gemaakt van een openbare wifi verbinding. Wel maakt men vaker gebruik van een beveiligde verbinding zoals VPN dan verleden jaar (53%). De stelling 'ik laat wel eens een PC of laptop onbeheerd achter' is dit jaar voor het eerst gesteld. De stelling 'ik laat mijn pc of laptop niet door anderen gebruiken' is door een programmeerfout niet gesteld aan gemeentemedewerkers.

Vergelijking tussen groepen
De gemeentemedewerkers geven vaker dan de andere doelgroepen aan dat ze hun zakelijke tablet of smartphone door anderen laten gebruiken. Medewerkers van het bedrijfsleven maken minder vaak gebruik van een beveiligde verbinding dan medewerkers van de Rijksoverheid en de vitale sectoren. Rijksambtenaren laten vaker dan gemeentemedewerkers een usb-stick die buiten de organisatie is geweest controleren op virussen. Computers worden vaker onbeheerd achtergelaten door medewerkers van gemeenten en het bedrijfsleven dan door medewerkers van de Rijksoverheid en de vitale sectoren.

Vergelijking binnen groepen
Hoogopgeleide en leidinggevende Rijksambtenaren letter beter op wat voor handelingen ze verrichten wanneer ze gebruik maken van een openbare wifi-verbinding. Bij de vitale sectoren laten medewerkers een usb-stick eerder controleren naarmate ze ouder zijn, ook laten oudere medewerkers minder vaak hun computers onbeheerd achter. Dit geldt ook voor oudere medewerkers van het bedrijfsleven, zij laten ook minder snel hun computer door anderen gebruiken. Hoogopgeleide medewerkers van het bedrijfsleven maker vaker gebruik van een VPN verbinding.

2.4 Kennis en gedrag rondom veilig wachtwoordgebruik

2.4.1 Burgers en gemeenten gebruiken sterkere wachtwoorden dan in 2012.
Er zijn drie eigenschappen van wachtwoorden die de sterkte daarvan ten goede komen: geen “echte” woorden opnemen, wachtwoorden langer dan tien karakters gebruiken en wachtwoorden met speciale tekens gebruiken.

Net als in 2012, zien we dat deze eigenschappen niet alledrie even vaak gehanteerd worden. Zo wordt de eigenschap het vermijden van echte woorden nog steeds het vaakst gehanteerd (gemiddeld 61%), gevolgd door het bevatten van speciale tekens (50%) en het bevatten van meer dan 10 karakters (43%).

Tabel E1: Samenstelling van wachtwoorden (weergave percentage “van toepassing”)

	Rijksoverheid		Gemeenten		Bedrijfsleven		Vitale sectoren		Burgers 13+	
	2013 n = 523	2012 n = 522	2013 n = 538	2012 n = 550	2013 n = 371	2012 n = 276	2013 n = 524	2012 n = 554	2013 n = 1283	2012 n = 1285
Mijn wachtwoorden bestaan uit meer dan 10 karakters	42%	36%	36%	31%	42%	39%	41%	45%	47%	37%
Mijn wachtwoorden bevatten geen woorden	62%	62%	58%	57%	63%	64%	63%	66%	60%	65%
Mijn wachtwoorden bevatten speciale tekens	56%	53%	51%	43%	51%	53%	54%	59%	46%	48%

E1a: Mijn wachtwoorden bestaan uit meer dan 10 karakters
E1b: Mijn wachtwoorden bevatten geen woorden die in het woordenboek voorkomen
E1c: Mijn wachtwoorden bevatten speciale tekens (anders dan letters uit het alfabet of cijfers)

Verschillen met 2012
Gemeentemedewerkers gebruiken vaker speciale tekens dan in 2012 en burgers gebruiken vaker wachtwoorden die bestaan uit meer dan tien karakters, maar minder vaak wachtwoorden die geen woorden uit het woordenboek bevatten.

Verschillen tussen groepen
Burgers hebben vaker wachtwoorden die uit 10 karakters bestaan dan gemeentemedewerkers, terwijl Rijksambtenaren en medewerkers van de vitale sectoren vaker speciale tekens gebruiken dan burgers.

Verschillen binnen groepen
Binnen de groep burgers zien we de volgende verschillen: vijftigplussers hebben minder vaak (41%) wachtwoorden met minimaal 10 karakters dan mensen van 18-30 jaar (52%) en 31-49 jaar (50%). Vijftigplussers en laagopgeleiden hebben vaker (47% en 50%) wachtwoorden die bestaan uit echte woorden dan mensen van 31-49 jaar (35%), middenopgeleiden (37%) en hoogopgeleiden (30%). Mannen, burgers van onder de 50 en midden- en hoogopgeleiden hebben vaker wachtwoorden met speciale tekens dan vrouwen, vijftigplussers en laagopgeleiden.

Jongere Rijksambtenaren gebruiken vaker wachtwoorden die bestaan uit meer dan 10 karakters dan Rijksambtenaren van boven de 30.

Hoogopgeleide gemeentemedewerkers hebben vaker (55%) wachtwoorden met speciale tekens dan middenopgeleiden (43%).

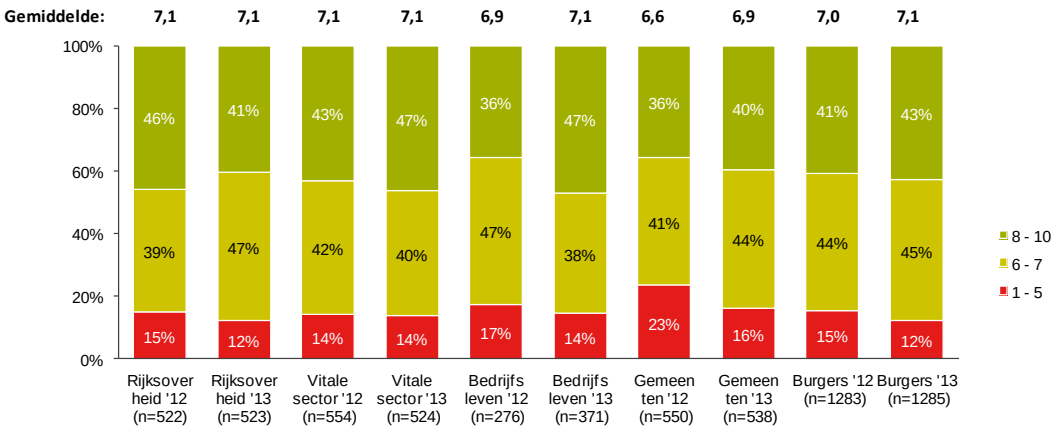
Laagopgeleide medewerkers uit het bedrijfsleven gebruiken vaker (54%) wachtwoorden die bestaan uit echte woorden en minder vaak (29%) speciale tekens en dan midden- en hoogopgeleiden.

Hoogopgeleiden werkzaam in vitale sectoren hebben minder vaak (35%) wachtwoorden die bestaan uit meer dan 10 tekens dan middenopgeleiden (47%).

2.4.2 Alle doelgroepen beoordelen de veiligheid van hun wachtwoorden nog steeds met gemiddeld een 7

Aan alle groepen is gevraagd om hun wachtwoorden te beoordelen op een tienpuntschaal (zeer onveilig - zeer veilig). Het gros van de respondenten beoordeelt de veiligheid van hun wachtwoorden met een voldoende of ruim voldoende; een minderheid geeft een onvoldoende. De gemiddelde beoordeling is gelijk voor alle groepen en ligt rond de 7.

Grafiek E2: Hoe veilig ('sterk') denkt u dat (de meeste) wachtwoorden van u zijn? Uiteenlopend van '1= zeer onveilig/zwak' - tot '10= zeer veilig/sterk'



Verschillen met 2012

Bij gemeenten en bedrijven is de gemiddelde beoordeling van hun wachtwoordsterkte toegenomen ten opzichte van 2012. Verder geven gemeentemedewerkers de sterkte van hun wachtwoorden in 2013 minder vaak met een onvoldoende (16% geeft een 1 tot 5) dan in 2012 (23%). Medewerkers van het bedrijfsleven beoordelen de sterkte van hun wachtwoorden vaker met een ruim voldoende (47%) dan in 2012 (36%).

Rijksambtenaren zijn wat minder uitgesproken over de veiligheid/sterkte van hun wachtwoorden: zij beoordelen hun wachtwoorden dit jaar vaker (47%) met een voldoende (6 of 7) dan in 2012 (39%) en minder vaak met een ruim voldoende of onvoldoende dan in 2012.

Burgers beschouwen de sterkte van hun wachtwoorden minder vaak (12%) als onvoldoende dan in 2012 (15%).

Leidinggevenden schatten de sterkte van hun wachtwoorden hoger in dan in 2012: 49% (versus 39% in 2012) geeft deze nu een ruim voldoende en 12% (versus 17% in 2012) een onvoldoende.

Verschillen tussen groepen

Binnen de Rijksoverheid geven lager opgeleide ambtenaren vaker (55%) aan dat ze een sterk wachtwoord hebben dan hoogopgeleiden (37%). Ook oudere medewerkers (50+) beoordelen de sterkte van hun wachtwoord hoger (48%) dan jongere medewerkers (18-30 jaar, 26%).

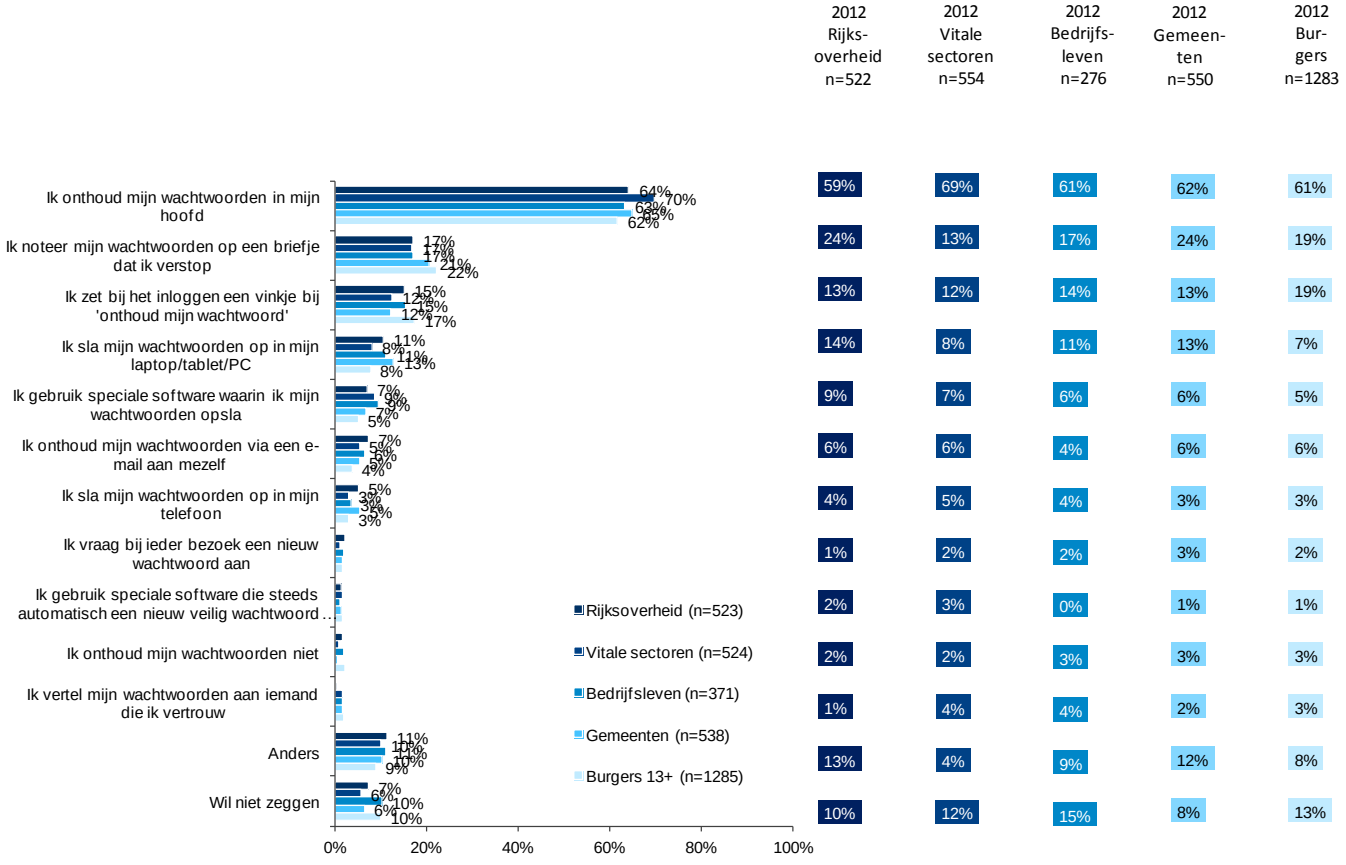
Verschillen binnen groepen

Onder burgers geeft 48% van de mannen de wachtwoordsterkte een ruim voldoende, tegenover 39% van de vrouwen. Evenzo beoordelen vrouwen hun wachtwoorden vaker (15%) als onvoldoende sterk dan mannen (10%).

2.4.3 De meeste mensen onthouden wachtwoorden in hun hoofd of gebruiken een verstopt briefje als geheugensteuntje

De meerderheid van de respondenten onthoudt hun wachtwoorden in hun hoofd. Het meest gebruikte geheugensteuntje is het noteren van wachtwoorden op een briefje dat wordt verstopt, gevolgd door het laten onthouden van het wachtwoord op de website. De andere geheugensteuntjes (opslaan in telefoon, opslaan op laptop/ tablet/ pc, delen van wachtwoorden met een vertrouwd persoon, e-mail naar eigen account) worden minder vaak genoemd.

Grafiek E3: Hoe zorgt u ervoor dat u uw wachtwoorden kunt onthouden?



Verschillen met 2012

Gemeentemedewerkers slaan hun wachtwoorden vaker (5%) in telefoons op dan in 2012 (3%). Rijksambtenaren noteren nu minder vaak (17%) dan in 2012 (24%) hun wachtwoorden op een verstopt briefje. Leidinggevenden delen iets minder vaak wachtwoorden met personen die zij vertrouwen en sturen wachtwoorden minder vaak naar het eigen e-mailaccount dan in 2012.

Verschillen tussen groepen

Het bedrijfsleven (vitale sectoren en overig) gebruikt vaker (9%) speciale software waarin wachtwoorden kunnen worden opgeslagen dan burgers (5%).

Burgers (8%) slaan minder vaak dan gemeentemedewerkers(13%) hun wachtwoorden op in hun computer. Verder onthouden zij minder vaak (4%) wachtwoorden door een e-mail naar hun eigen account te sturen dan Rijksambtenaren (7%).

Verschillen binnen groepen

Bij burgers onthouden vrouwen hun wachtwoorden vaker (66%) in hun hoofd dan mannen (57%). Mannen gebruiken vaker speciale software bij het genereren en opslaan van hun wachtwoorden. Vijftigplussers hebben meer moeite (46%) met het onthouden van hun wachtwoorden in hun hoofd dan de andere leeftijdsgroepen.

De leeftijdsgroep 18-30 jaar onthoudt ook beter (82%) hun wachtwoorden dan de leeftijdsgroep 50+ (46%). Vijftigplussers gebruiken vaker (30%) een verstopt briefje als hulpmiddel dan jongeren. De jongste groep (13-17 jaar) gebruikt vaker (5%) speciale software die steeds automatisch een nieuw veilig wachtwoord genereert dan de oudere groep.

De leeftijdsgroep 18-30 jaar vraagt iets vaker (3%) dan 50plussers (1%) bij ieder bezoek een nieuw wachtwoord aan. Hoogopgeleiden slaan vaker hun wachtwoorden op hun computer (11%) of met speciale software (8%) op dan laagopgeleiden (5%, 4%). Ook vragen zij vaker (4%) dan middenopgeleiden bij ieder bezoek een nieuw wachtwoord aan (1%). Middenopgeleiden geven vaker (65%) aan hun wachtwoorden in hun hoofd te kunnen onthouden dan laagopgeleiden (57%).

Jonge Rijksambtenaren onthouden vaker (85%) hun wachtwoorden in hun hoofd dan ambtenaren die ouder dan 30 jaar zijn. Rijksambtenaren van 31-49 jaar onthouden vaker (68%) hun wachtwoorden dan 50+ collega's (52%). Daarentegen schrijven medewerkers ouder dan 50 jaar vaker (25%) hun wachtwoorden op een verstopt briefje dan de jongere medewerkers. Ook gebruiken oudere Rijksambtenaren minder vaak (5%) een e-mail naar hun eigen e-mailadres om hun wachtwoorden te onthouden dan jongeren (13%). Hoogopgeleiden (18%) laten vaker de website het wachtwoord onthouden dan laag- en middenopgeleiden.

Bij gemeentemedewerkers is hetzelfde patroon te zien als bij Rijksambtenaren: ouderen onthouden minder vaak (56%) wachtwoorden in hun hoofd en gebruiken vaker (25%) een briefje dat verstopt wordt dan jongeren. Daarnaast vertellen oudere gemeentemedewerkers vaker (4%) hun wachtwoorden aan iemand die ze vertrouwen dan de groep van 31-49 jaar (1%).

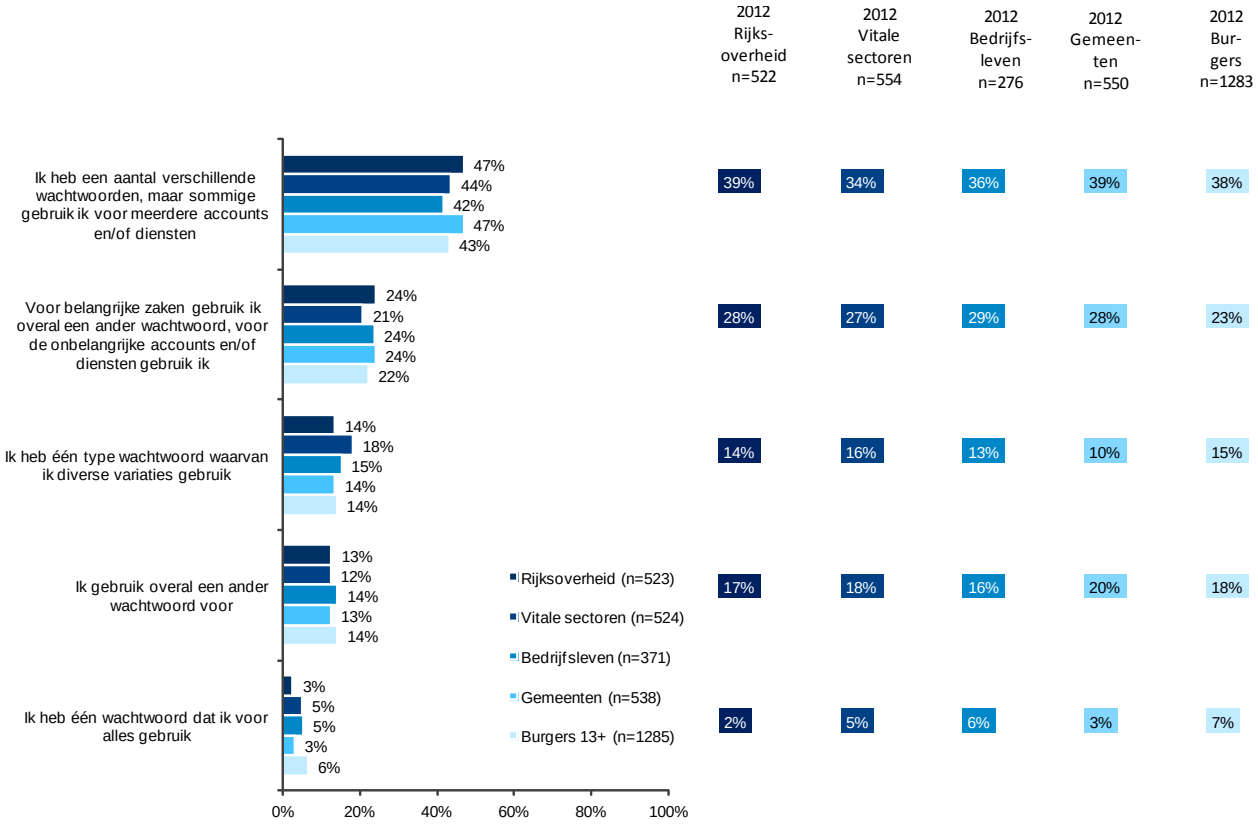
Jonge medewerkers (18-30 jaar) in vitale sectoren laten hun wachtwoord vaker door de website onthouden dan oudere medewerkers. Hoger opgeleiden slaan hun wachtwoorden vaker (12%) op in hun computer dan laag- of middenopgeleiden (8%, 4%).

Net als bij de vitale sectoren laten jonge medewerkers in het bedrijfsleven vaker (36%) hun wachtwoord door de website opslaan dan oudere medewerkers. Ook hoger opgeleiden doen dit vaker (20%) dan laagopgeleiden (6%). Daarnaast e-mailen jonge medewerkers vaker hun wachtwoorden naar hun eigen account (16%) dan medewerkers in de leeftijdscategorie 31-49 jaar. Net als bij de ambtenaren is te zien dat jonge mensen vaker (75%) hun wachtwoorden in hun hoofd onthouden dan oudere mensen. Daarentegen geven de jonge medewerkers vaker (9%) aan dan de andere leeftijdsgroepen dat ze hun wachtwoorden niet onthouden.

2.4.4 Het gebruik van verschillende wachtwoorden waarvan sommige voor meerdere accounts neemt toe en het gebruik van een ander wachtwoord voor ieder account daalt

Tussen de 42% en 47% van de respondenten gebruikt een aantal verschillende wachtwoorden waarvan sommige wachtwoorden voor meerdere accounts worden gebruikt. Bijna een kwart van de respondenten gebruikt voor belangrijke zaken iedere keer een ander wachtwoord en voor onbelangrijke zaken meestal steeds hetzelfde wachtwoord.

Grafiek E4: Hoeveel verschillende wachtwoorden gebruikt u voor de verschillende computers, programma's en/of websites die u gebruikt?



Verschillen met 2012

Alle doelgroepen, behalve het bedrijfsleven, hebben vaker verschillende wachtwoorden waarvan sommige gebruikt worden voor meerdere accounts, dan in 2012. Zij maken juist minder vaak gebruik van een ander wachtwoord voor ieder account dan in 2012. Binnen vitale sectoren wordt minder vaak (21%) dan in 2012 (27%) voor belangrijke zaken een ander wachtwoord gebruikt en voor onbelangrijke accounts één wachtwoord. Onder leidinggevenden is het gebruik van verschillende wachtwoorden voor belangrijke zaken afgenomen. Daarentegen worden er vaker verschillende wachtwoorden gebruikt, die voor meerdere accounts en/of diensten worden toegepast.

Verschillen tussen groepen
Burgers gebruiken vaker (7%) één wachtwoord voor alle accounts dan de ambtenaren (3%).

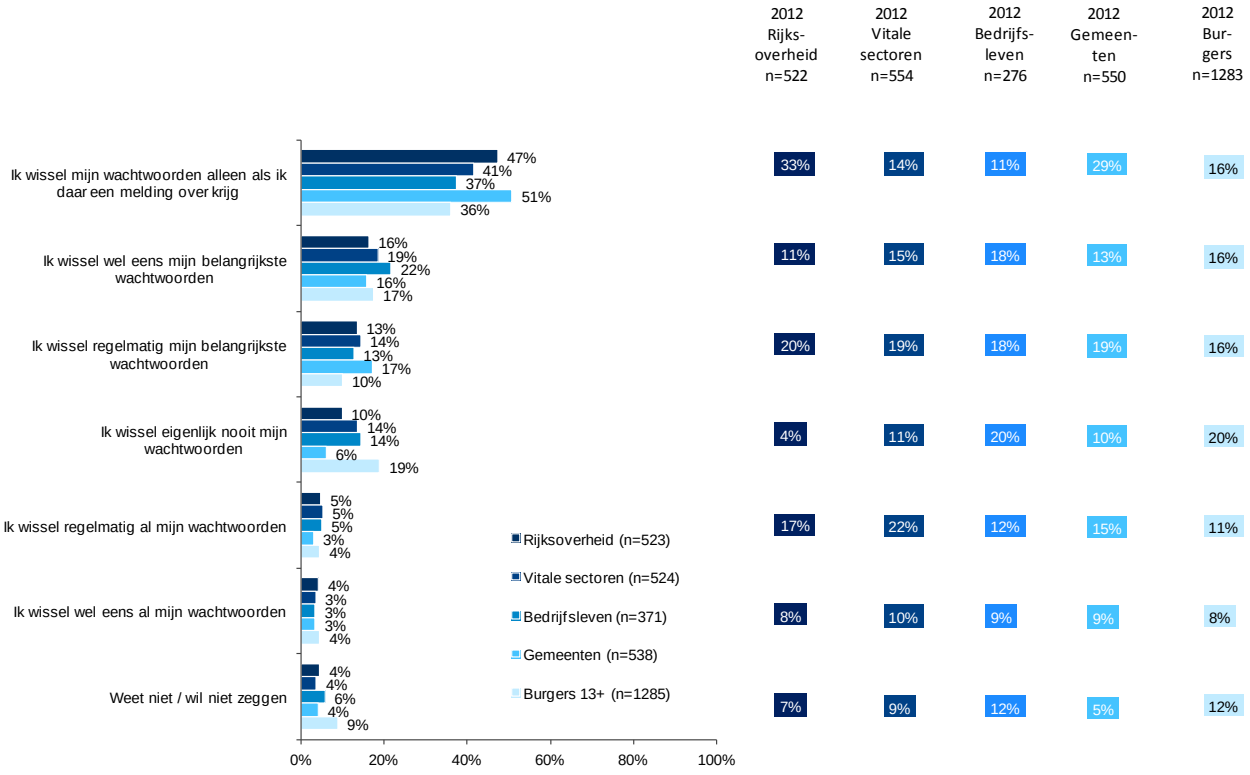
Verschillen binnen groepen
Onder burgers zien we dat vrouwen vaker (47%) verschillende wachtwoorden waarvan soms dezelfde voor meerdere accounts gebruiken dan mannen (40%). Mensen ouder dan 30 gebruiken vaker (16%) overal een ander wachtwoord dan de groep 18-30 jaar (7%). Laag- en middenopgeleiden gebruiken vaker één wachtwoord voor alle accounts dan hoogopgeleiden (12%). Daarentegen gebruiken midden- en hoogopgeleiden vaker verschillende wachtwoorden, soms voor meerdere accounts, dan laagopgeleiden (18%).

Middenopgeleiden en hoogopgeleiden in het bedrijfsleven gebruiken vaker een ander wachtwoord voor belangrijke accounts (behalve bij onbelangrijke zaken) dan laagopgeleide medewerkers (13%). Laagopgeleiden gebruiken vaker (9%) één wachtwoord voor alles dan hoogopgeleiden (25%).

2.4.5 Respondenten wisselen minder vaak op eigen initiatief hun wachtwoorden

Ongeveer vier op de tien respondenten wisselen alleen hun wachtwoorden als ze daar een melding over krijgen. Op afstand wordt dit gevolgd door het wel eens wisselen van de belangrijkste wachtwoorden (18%), het nooit wisselen van wachtwoorden (14%) en het regelmatig wisselen van de belangrijkste wachtwoorden (13%).

Grafiek E5: 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".



Verschillen met 2012

Binnen alle groepen is het wisselen van wachtwoorden afgenomen ten opzichte van 2012.

Ook is er bij alle doelgroepen sprake van een afname van het wel eens of regelmatig wisselen van alle wachtwoorden. Verder geven Rijksambtenaren, medewerkers van vitale sectoren en burgers minder vaak aan dat zij regelmatig hun belangrijkste wachtwoorden wisselen. Daarentegen is er bij alle doelgroepen sprake van een toename van het alleen wisselen van hun wachtwoord naar aanleiding van een melding daartoe. Binnen de Rijksoverheid wordt er vaker aangegeven dat wachtwoorden nooit gewisseld worden. Bij gemeenten en het bedrijfsleven is het tegenovergestelde te zien.

Onder leidinggevenden zien we hetzelfde patroon als onder de verschillende groepen: wachtwoorden worden vaker alleen gewisseld als daar een melding over verschijnt en minder uit eigen initiatief.

Verschillen tussen groepen
Het bedrijfsleven (zowel vitale sectoren als overig) en burgers wisselen vaker nooit hun wachtwoorden nooit dan de gemeentemedewerkers (6%). Burgers wisselen hun wachtwoorden vaker nooit (19%) dan Rijksambtenaren (10%). Gemeentemedewerkers wisselen vaker (51%) alleen hun wachtwoorden als ze daar een melding over krijgen dan medewerkers uit de vitale sectoren (41%), het bedrijfsleven (37%) en burgers (36%).
Rijksambtenaren wisselen vaker alleen hun wachtwoord na een melding (47%) dan medewerkers in het bedrijfsleven (37%) en burgers (36%).

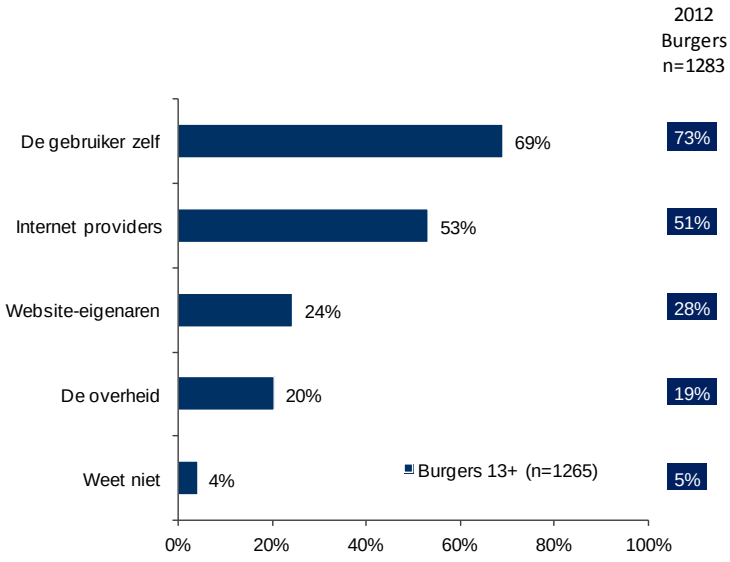
Verschillen binnen groepen
Onder Rijksambtenaren zien we dat de oudste twee leeftijdsgroepen vaker regelmatig hun belangrijkste wachtwoorden wisselen dan de jongste leeftijdsgroep (3%).
Jonge gemeentemedewerkers geven vaker aan (32%) dat ze wel eens hun belangrijkste wachtwoorden wisselen dan hun oudere collega's. In het bedrijfsleven zijn er verschillen te zien tussen de jongste en de oudste leeftijdsgroepen. Jonge medewerkers wisselen vaker alleen hun wachtwoorden wanneer ze daar een melding over krijgen (54%), terwijl oudere medewerkers vaker wel eens alle wachtwoorden wisselen (6%).
Laagopgeleide burgers zeggen vaker (25%) hun wachtwoorden nooit te wisselen dan midden- (16%) en hoogopgeleide (13%) burgers. Hier tegenover staat dat midden- en hoogopgeleide burgers vaker alleen hun wachtwoorden wisselen wanneer ze daar een melding over ontvangen (30%).

2.5 De verantwoordelijkheid voor Cyber security ligt volgens medewerkers vooral bij de IT-afdeling en medewerkers; burgers zien vooral zichzelf en internetproviders als verantwoordelijken

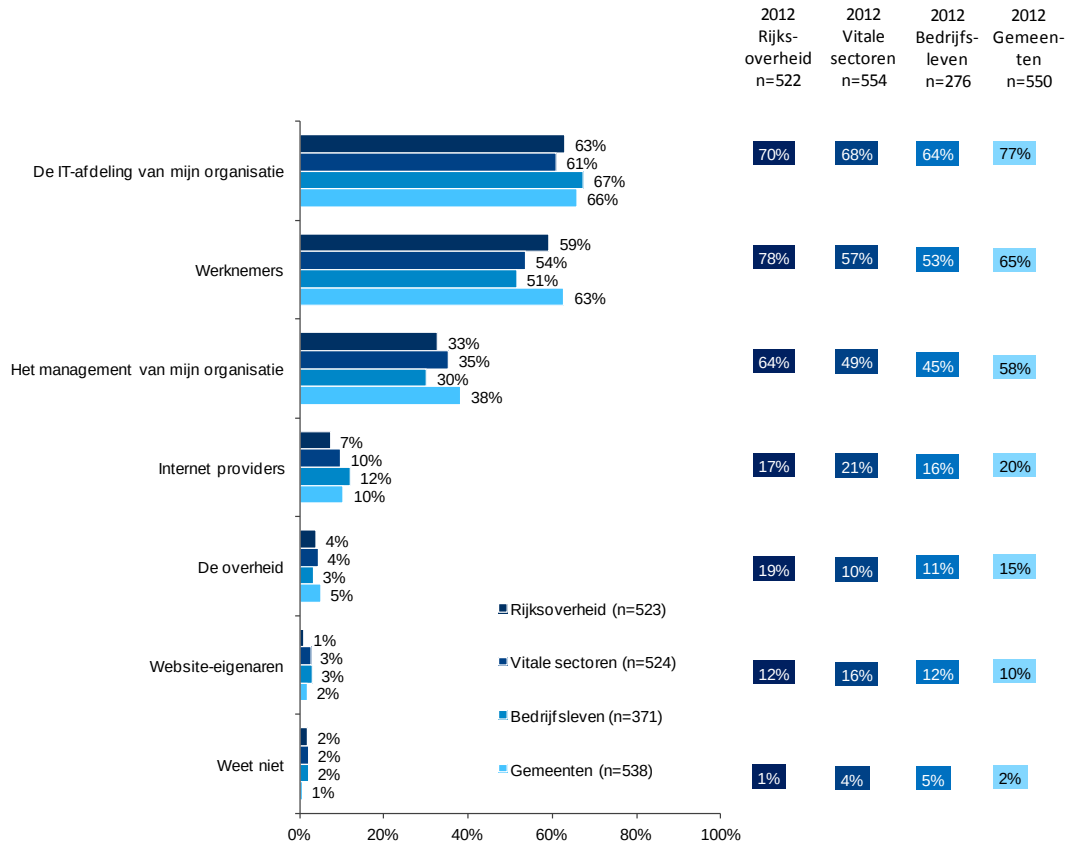
De meerderheid van de professionele respondenten vindt dat de verantwoordelijkheid voor een veilig internetgebruik op de werkplek vooral moet liggen bij de IT-afdeling. Vervolgens worden de medewerkers en het management als verantwoordelijken aangeduid.

Wanneer het gaat over internetveiligheid thuis geven de meeste burgers aan dat zij hier voornamelijk zelf voor verantwoordelijk zijn. Ook internetproviders (door ongeveer de helft van de burgers genoemd) en website-eigenaren (door een kwart genoemd) wordt verantwoordelijkheid hiervoor toegedicht.

Figuur D12: Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid op het gebied van internetgebruik voornamelijk moet liggen?



Figuur C8: Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid op het gebied van internetgebruik voornamelijk moet liggen? Er zijn maximaal twee antwoorden mogelijk



Verschillen met 2012
Bij burgers is een afname te zien in het aandeel dat zichzelf voornamelijk verantwoordelijk beschouwt voor de veiligheid van internetgebruik thuis. Burgers leggen de verantwoordelijkheid vaker bij website-eigenaren. Door een verandering in de vragenlijst bij vraag C8 (meerdere antwoorden mogelijk in 2012 versus maximaal 2 antwoorden mogelijk in 2013) is een vergelijking in de tijd voor de zakelijke doelgroepen indicatief.

Verschillen tussen groepen
In tegenstelling tot de vitale sectoren en het bedrijfsleven, geven gemeentemedewerkers vaker (63%) aan dat de verantwoordelijkheid voor veilig internetgebruik bij medewerkers zelf ligt.

Verschillen binnen groepen
Onder burgers vinden mannen vaker (56%) dat internetproviders verantwoordelijk zijn voor cyber security dan vrouwen (50%). De oudere leeftijdsgroepen noemen vaker internetproviders als verantwoordelijk voor de veiligheid van internetgebruik dan de jongere leeftijdsgroepen. Website eigenaren worden vaker (28%) verantwoordelijk gesteld voor de veiligheid door burgers van 31-49 jaar dan vijftigplussers (20%). Hoogopgeleiden noemen de gebruikers van het internet vaker (78%) als verantwoordelijke voor veilig internet dan laag- en middenopgeleiden.

Rijksambtenaren van 31-49 jaar geven vaker (63%) aan dat medewerkers verantwoordelijk zijn voor een veilig internetgebruik dan jonge Rijksambtenaren. Hoogopgeleiden vinden vaker (40%) dan middenopgeleiden dat het management verantwoordelijk is voor de cyber security (21%). Daarentegen zien de middenopgeleiden vaker (70%) de IT-afdeling als verantwoordelijke (57%).

Onder gemeentemedewerkers vinden middenopgeleiden vaker internetproviders en de overheid verantwoordelijk voor de cyber security op hun werkplek dan hoogopgeleiden. Hoogopgeleiden zien vaker (67%) de medewerkers als verantwoordelijk dan middenopgeleiden (53%).

Binnen de vitale sectoren geven jonge medewerkers vaker (77%) dan oudere medewerkers aan dat de IT-afdeling de veiligheid van het internetgebruik op zich moet nemen. De middelste leeftijdsgroep is juist vaker (58%) van mening dat medewerkers zelf de verantwoordelijkheid moeten nemen dan de jongste leeftijdsgroep. Verder vinden hoopopgeleide medewerkers uit het bedrijfsleven vaker (59%) dat de veiligheid van internetgebruik bij de medewerkers zou moeten liggen dan de laag- en middenopgeleide medewerkers. Laag- en middenopgeleide medewerkers wijzen juist vaker dan de hoogopgeleiden (6%) internet providers als verantwoordelijke partij aan.

3. Resultaten thema 2013: Smart Security

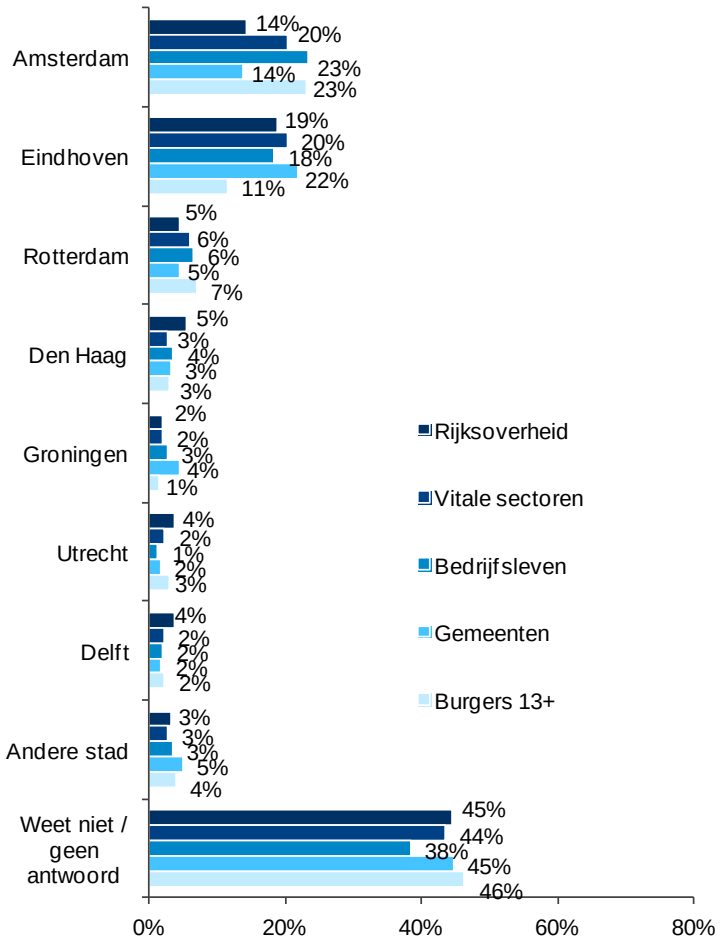
3.1 Subthema 1: Smart Cities

Smart Cities zijn (stedelijke) gebieden waar slimme, nieuwe ICT-toepassingen worden ontwikkeld en ingezet. Smart Cities gebruiken groene technologie, ontwikkelen apparaten en apps voor beter vervoer en recreatie en gebruiken nieuwe ICT-toepassingen voor bijvoorbeeld gezondheid, bedrijvenparken en onderwijs. Alle ondervraagden kregen eerst deze uitleg te zien voor het beantwoorden van de vragen.

3.1.1 Bijna de helft van alle respondenten kan geen Smart City noemen

Bijna vijf op de tien (45%) van de ondervraagden geeft aan geen Nederlandse stad als Smart City te kunnen aanwijzen, dit aantal ligt ongeveer gelijk voor alle groepen. Amsterdam wordt het vaakst genoemd als een voorbeeld van een Smart City.

Figuur G1: Welke stad in Nederland ziet u als een Smart City?



Verschillen tussen groepen
Amsterdam wordt vooral door burgers en medewerkers in het algemene bedrijfsleven spontaan als Smart City genoemd. Ook Eindhoven wordt door ongeveer een vijfde van de professionele doelgroepen genoemd, bij burgers is dit minder met 11%. Groningen wordt vaker genoemd door medewerkers van gemeenten.

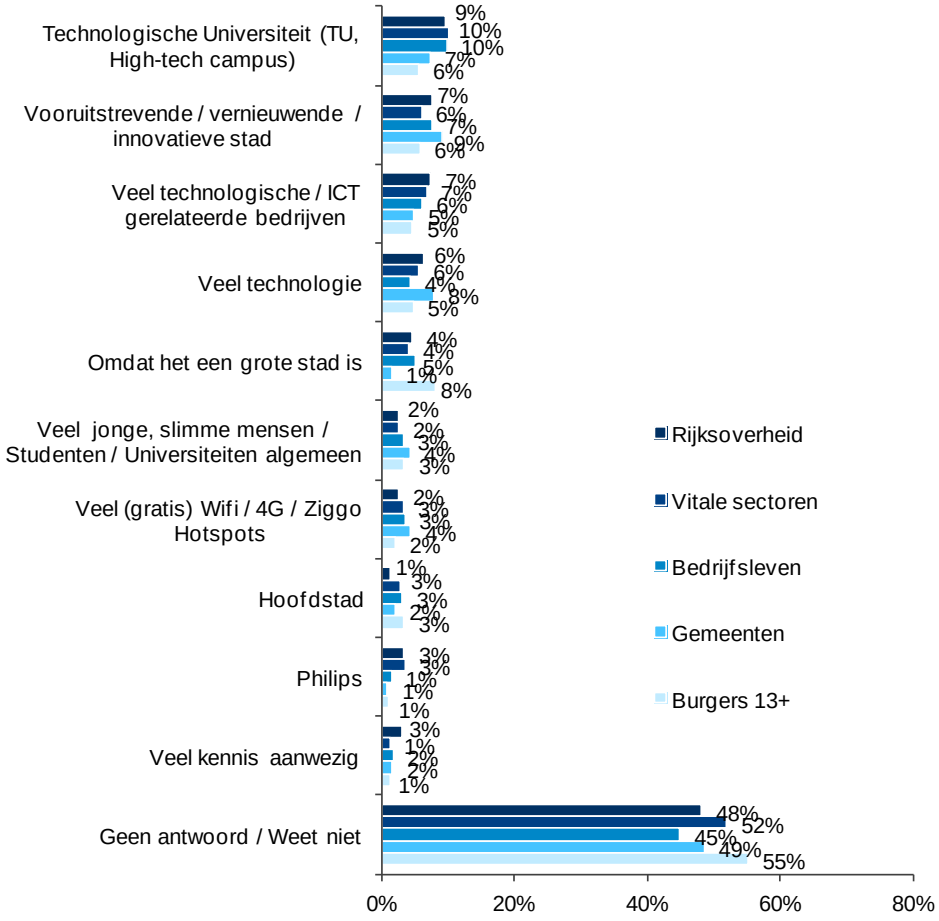
Verschillen binnen groepen
Bij de medewerkers van vitale sectoren noemen laagopgeleiden vaker Rotterdam (12%) en Groningen (5%) dan hoogopgeleiden. Bij medewerkers van het bedrijfsleven wordt Groningen juist vaker genoemd door hoogopgeleiden (5%). Men is sterk geneigd om de grootste stad uit de eigen regio te noemen. Burgers uit de drie grootste steden noemen vaker Den Haag (12%) en Rotterdam (12%), in het Zuiden noemt men vaker Eindhoven (27%) en in het Noorden Groningen (8%). Amsterdam wordt vaker genoemd door vrouwen (28%) dan door mannen (17%) en Eindhoven juist vaker door mannen (16%) dan door vrouwen (7%).

3.1.2 In een Smart City werken en studeren veel mensen met technologische kennis

Meer dan de helft van de ondervraagden geeft aan geen reden aan te kunnen geven waarom ze een stad als Smart City noemen. Steden worden vooral als Smart City genoemd, omdat ze (technische) universiteiten hebben of bedrijven waar men zich bezig houdt met de ontwikkeling van ICT en technologie. Op deze plekken is immers veel technische kennis aanwezig. Verder noemt men vooral grotere steden die een innovatief imago hebben. Amsterdam wordt ook wel simpelweg genoemd omdat het de hoofdstad is. Tussen de doelgroepen zijn geen grote verschillen zichtbaar.

Verschillen binnen groepen
Bij de medewerkers van de vitale sectoren noemen hoogopgeleiden vaker innovativiteit (9%) en laagopgeleiden vaker de grootte van een stad (8%) als reden dat het een Smart City is. Bij de burgers noemen mannen (7%) vaker de aanwezigheid van een technologische universiteit als reden dan vrouwen (4%).

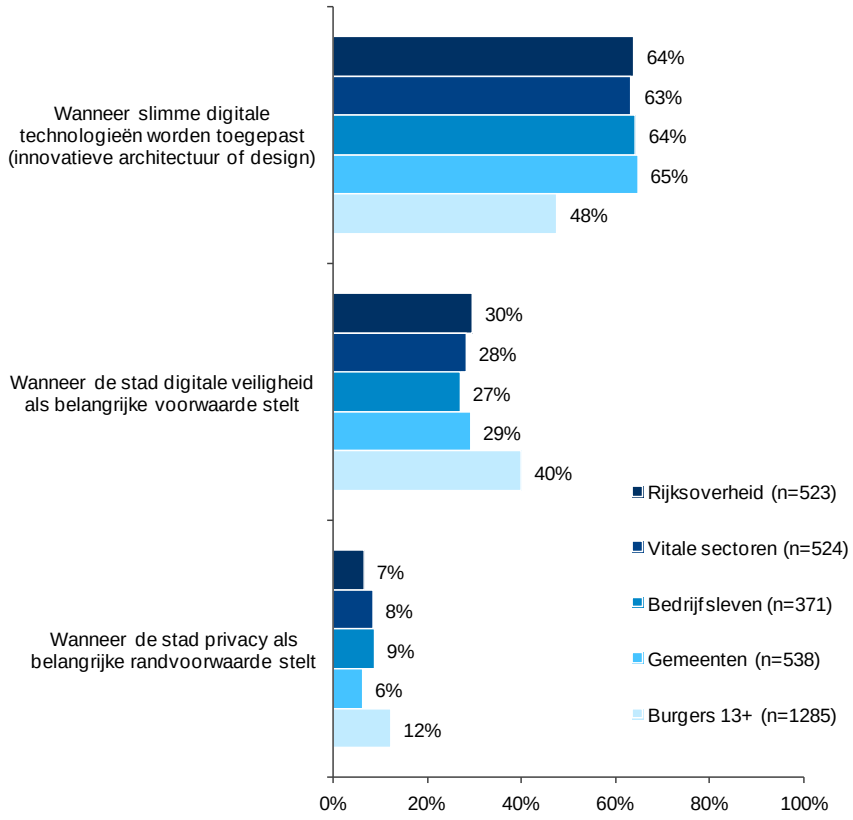
Figuur G2: Waarom vindt u deze stad een smart city?



3.1.3 In een Smart City worden slimme digitale technologieën toegepast

Bijna tweederde van de professionele doelgroepen vindt een stad met name een Smart City wanneer er slimme digitale technologieën worden toegepast. Voor burgers is het belangrijker dat een stad digitale veiligheid als belangrijkste voorwaarde stelt (40%). Ook kiezen burgers vaker voor privacy en dus minder vaak voor slimme digitale technologieën als belangrijke randvoorwaarde dan de professionele doelgroepen.

Figuur G3: Wanneer vindt u dat een stad een smart city is? 1 antwoord mogelijk



Verschillen binnen groepen

Bij Rijksambtenaren kiezen medewerkers van 31-49 jaar vaker voor slimme digitale technologieën (69%) en 50 plussers vaker dan jongeren voor digitale veiligheid (36%). Een vergelijkbaar leeftijdsverschil is ook te zien bij medewerkers van gemeenten en vitale sectoren. Bij de burgers kiest zelfs 49% van de vijftig plussers voor veiligheid boven innovatie.

3.2 Subthema 2: Security by design / Smart design

3.2.1 Wi-Fi-thuis scoort het hoogste op digitale veiligheid (7,6), het openbaar vervoer scoort relatief het laagst (6)

Respondenten is gevraagd om met behulp van een rapportcijfer tussen de 1 en de 10 uit te drukken hoe het is gesteld met de digitale veiligheid van een aantal aspecten van hun IT-omgeving thuis, onderweg en op hun werk. In deze paragraaf geven we de aspecten weer in de volgorde van hoogste naar (relatief) laagste beoordeling.

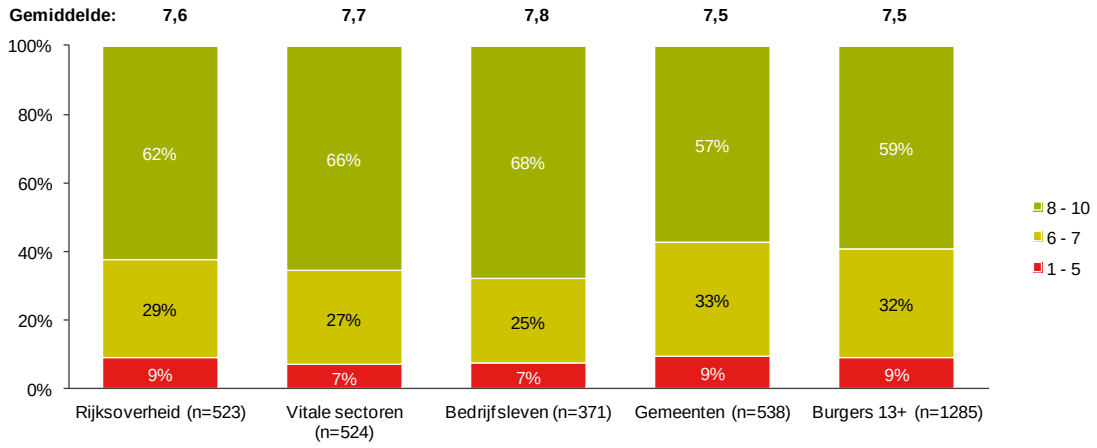
De digitale veiligheid van alle acht voorgelegde aspecten wordt gemiddeld met een voldoende beoordeeld. De beoordelingen lopen uiteen van een 7,6 (voor Wifi-thuis) tot een 6 (voor het Openbaar vervoer).

In de beoordeling van de diverse aspecten zijn weinig verschillen tussen de vijf doelgroepen onderling te zien.

3.2.1.1 De digitale veiligheid van Wifi-thuis scoort gemiddeld een 7,6

Respondenten schatten de veiligheid van Wifi-thuis het hoogst in van alle 8 voorgelegde aspecten van de IT-omgeving. Gemiddeld scoort dit een 7,6 en bij de doelgroepen liggen de rapportcijfers tussen de 7,5 en 7,8. Ongeveer zes op de tien respondenten beoordelen de veiligheid met een 8 tot 10, een kwart tot een derde met een 6 tot 8 en een minderheid met een onvoldoende.

Figuur G4_2: Beoordeling digitale veiligheid Wifi-thuis



Verschillen tussen groepen

Medewerkers van het bedrijfsleven schatten deze veiligheid vaker hoog (8-10) in dan burgers en medewerkers van gemeenten. De gemiddelde beoordeling verschillen niet significant van elkaar.

Verschillen binnen groepen

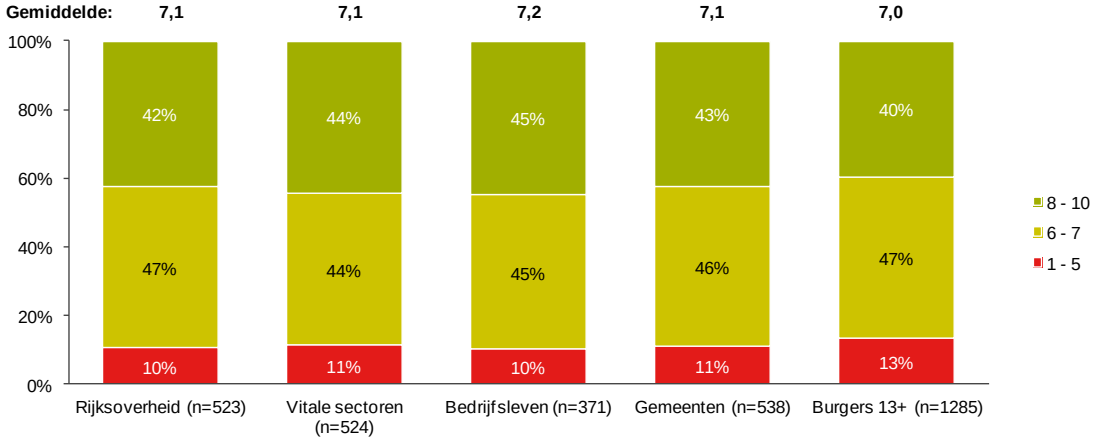
Bij de rijksoverheid geven jongeren (18-30) minder vaak een hoge beoordeling (42%) van de veiligheid van Wifi-thuis dan Rijksambtenaren van boven de 30. Bij de gemeenten geeft 16% van de vijftigplussers een onvoldoende tegenover 6% in de leeftijdscategorie 31-49. Bij de burgers van boven de 50 is dit 12%, hoe ouder, hoe minder vertrouwen men heeft in de veiligheid. Laagopgeleide burgers geven de veiligheid vaker (12%) een onvoldoende dan hoogopgeleiden (6%).

3.2.1.2 De digitale veiligheid van administratieve zaken scoort gemiddeld een 7

De digitale veiligheid van het beheer van administratieve zaken scoort gemiddeld een 7 en tussen de doelgroepen een 7 tot 7,2, waarmee het de tweede plaats inneemt. Tussen de 40 en 45% geeft de veiligheid een ruim voldoende (8-10) en 10 tot 13% geeft een onvoldoende.

Er zijn geen verschillen tussen groepen.

Figuur G4_5: Beoordeling digitale veiligheid Beheren van administratieve zaken



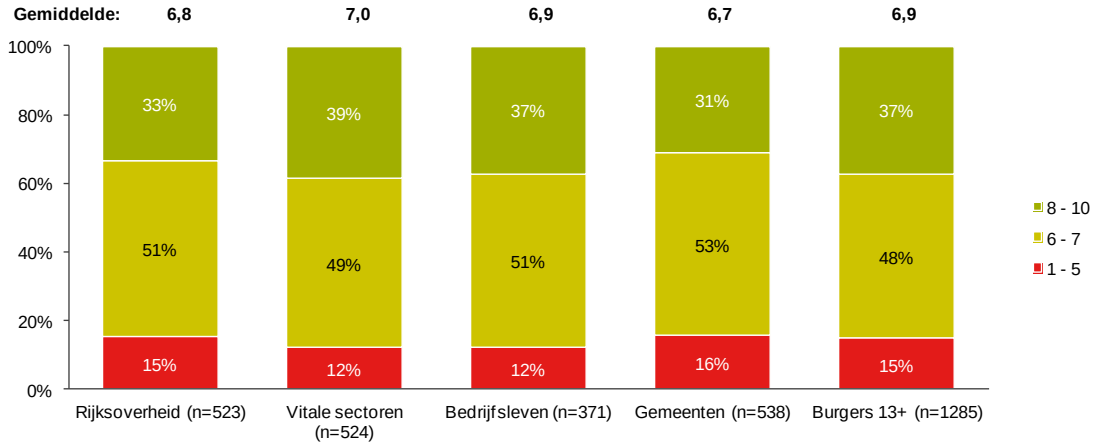
Verschillen binnen groepen

Bij burgers van 18-30 jaar oud beoordeelt 45% de veiligheid met 8-10 tegenover 35% van de vijftig plussers, het vertrouwen neemt af met leeftijd. Bij medewerkers van de vitale sectoren beoordelen de laagopgeleiden de digitale veiligheid van administratieve zaken met een 6,2 tegenover een 5,7 bij de middenopgeleiden. Ook bij het algemene bedrijfsleven is een opleidingsverschil te zien, laag- en middenopgeleiden geven de veiligheid een 7,4 ten opzichte van een 6,9 bij laagopgeleiden.

3.2.1.3 De digitale veiligheid van thuiswinkelen scoort gemiddeld een 6,9

Op de derde plaats wordt de digitale veiligheid van thuiswinkelen gemiddeld met een ruim voldoende beoordeeld, overall met een 6,9 en door de doelgroepen tussen de 6,7 en de 7.

Figuur G4_1: Beoordeling digitale veiligheid Thuiswinkelen



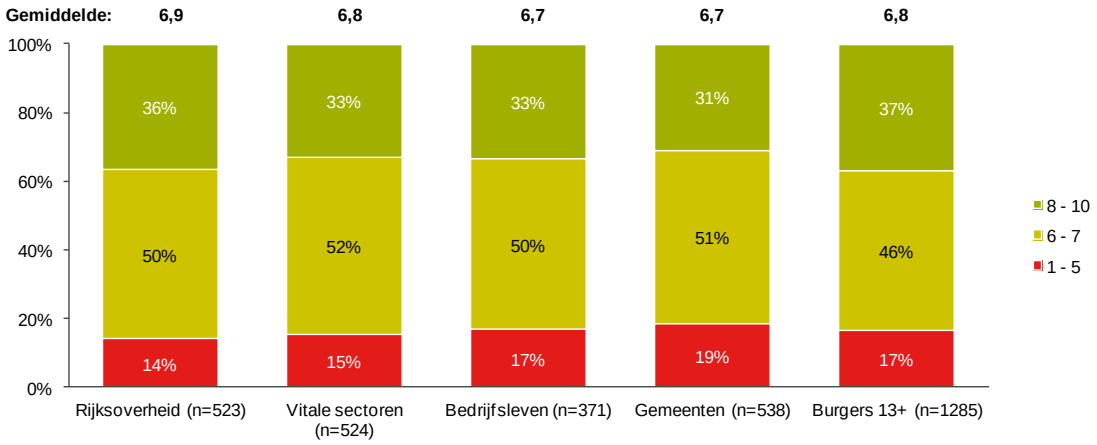
Verschillen tussen groepen
De gemiddelde beoordeling van vitale sectoren is wat hoger dan die van gemeenten.

Verschillen binnen groepen
Vijftigplussers geven de digitale veiligheid van thuiswinkelen vaker een onvoldoende dan jongeren, dat geldt zowel voor burgers (18%), als voor medewerkers van gemeenten (22%) en vitale sectoren (17%).

3.2.1.4 De digitale veiligheid van nieuwssites scoort gemiddeld een 6,8

De digitale veiligheid van nieuwssites scoort gemiddeld een 6,8. Gemiddeld geeft 35% een score van 8-10 en 16% een onvoldoende. Er zijn geen verschillen tussen de doelgroepen.

Figuur G4_3: Beoordeling digitale veiligheid Nieuwssites



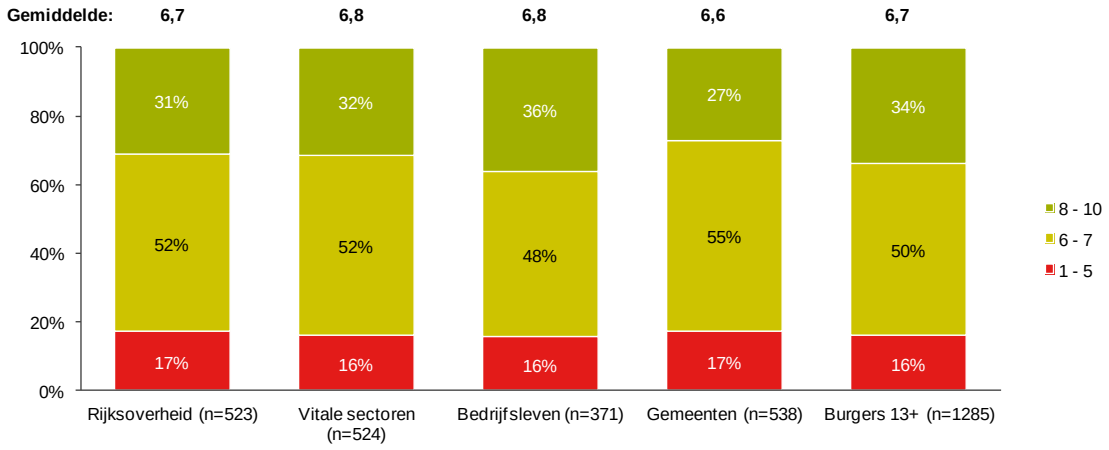
Verschillen binnen groepen

Dit vertrouwen loopt bij burgers af per leeftijdsgroep, in de categorie 13-17 heeft 50% een score van 8-10, bij vijftigplussers is dit 33%. Bij de medewerkers van gemeenten beoordeelt 34% van de hoogopgeleiden de digitale veiligheid van nieuwssites als goed tegenover 21% van de middenopgeleiden. Het tegenovergestelde is het geval bij het algemene bedrijfsleven, 22% van de hoogopgeleiden geeft de veiligheid een onvoldoende vergeleken met 9% van de middenopgeleiden.

3.2.1.5 De digitale veiligheid van het online reserveren van tickets scoort gemiddeld een 6,7

Bij het reserveren van tickets en kaartjes, ongeacht of het hier om bioscoopkaartjes of bijvoorbeeld vliegtickets gaat, beoordeelt men de digitale veiligheid gemiddeld met een 6,7; de beoordeling van de doelgroepen loopt uiteen van een 6,6 tot 6,8. Gemiddeld bijna een derde geeft een score van 8-10 en 16% een onvoldoende.

Figuur G4_6: Beoordeling digitale veiligheid Reserveren van tickets



Verschillen tussen groepen

Burgers en medewerkers van het bedrijfsleven geven hierbij significant vaker een score van 8-10 dan medewerkers van de gemeenten.

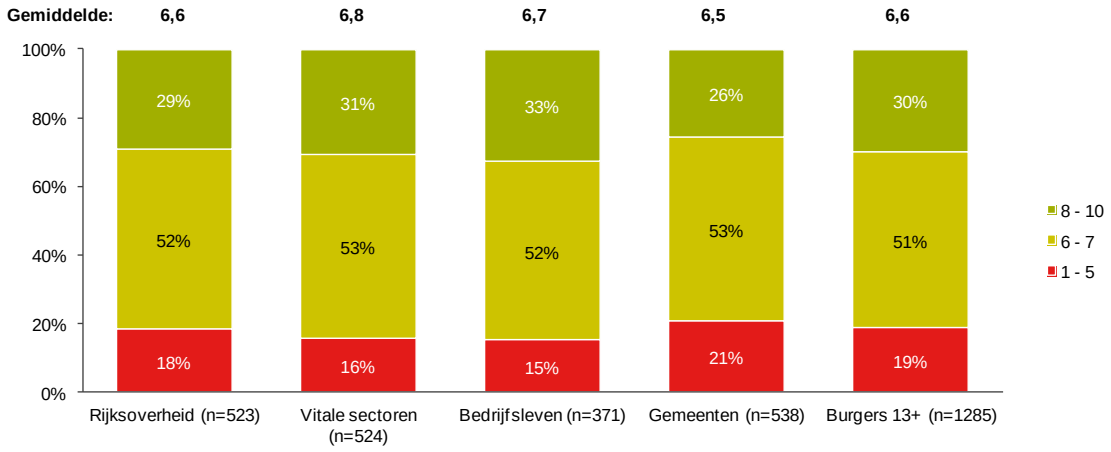
Verschillen binnen groepen

Van de burgers geven mannen (19%) vaker een onvoldoende dan vrouwen (14%). Ook vijftigplussers geven vaker een onvoldoende (21%) dan jongere leeftijdsgroepen. Van de laagopgeleide medewerkers van vitale sectoren geeft 23% een 8-10 vergeleken met 11% van de middenopgeleiden. Hoogopgeleiden van het algemene bedrijfsleven geven een 6,9 voor de digitale veiligheid van tickets reserveren ten opzichte van een 7,4 bij laag- en middenopgeleiden.

3.2.1.6 De digitale veiligheid van Energievoorziening scoort gemiddeld een 6,6

De beoordeling van de digitale veiligheid van de energievoorziening is overall gemiddeld een 6,6 en varieert van gemiddeld een 6,5 bij medewerkers van gemeenten tot een 6,8 bij medewerkers van vitale sectoren. Gemiddeld geeft 30% een score van 8-10 en 18% een onvoldoende. Er zijn geen verschillen tussen de doelgroepen.

Figuur G4_8: Beoordeling digitale veiligheid Energievoorziening



Verschillen tussen groepen

De gemiddelde beoordeling van vitale sectoren is iets hoger dan die van gemeenten.

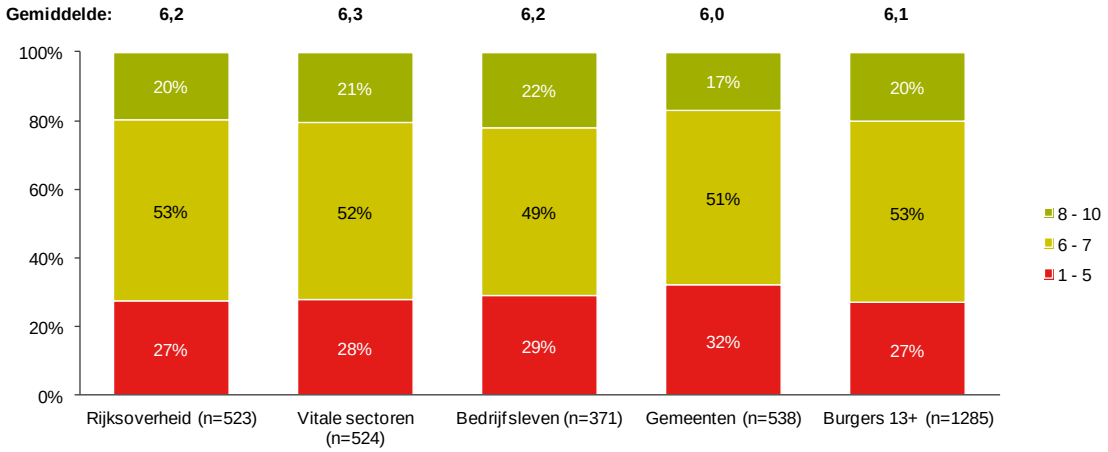
Verschillen binnen groepen

Bij de burgers neemt het vertrouwen in de veiligheid af met leeftijd. 42% van de tieners geeft een score van 8-10 ten opzichte van 26% van de vijftigplussers. Weer zien we het omgekeerde effect bij Rijksambtenaren, hier geeft 32% van de vijftigplussers een score van 8-10 wat lager is dan 16% van de leeftijdscategorie 18-30 jaar. De laagopgeleide medewerkers van het algemene bedrijfsleven geven in 49% van de gevallen een 8-10 voor de digitale veiligheid van de energievoorziening terwijl dit bij hoopopgeleide medewerkers bij 28% het geval is.

3.2.1.7 De digitale veiligheid van Mobiele internetdiensten scoort gemiddeld een 6,1

De digitale veiligheid van apps en andere mobiele internetdiensten wordt met een gemiddelde score van een 6,1 op één na laagste beoordeeld van de voorgelegde aspecten van de IT-omgeving. Eén op de vijf geeft een score van 8-10 en een relatief grote groep van gemiddeld 28% geeft de veiligheid van apps een onvoldoende. Bij de verschillende doelgroepen scoort het gemiddeld een krappe voldoende van 6 tot 6,3. Er zijn geen wezenlijke verschillen tussen de groepen.

Figuur G4_7: Beoordeling digitale veiligheid Mobiele internetdiensten zoals apps



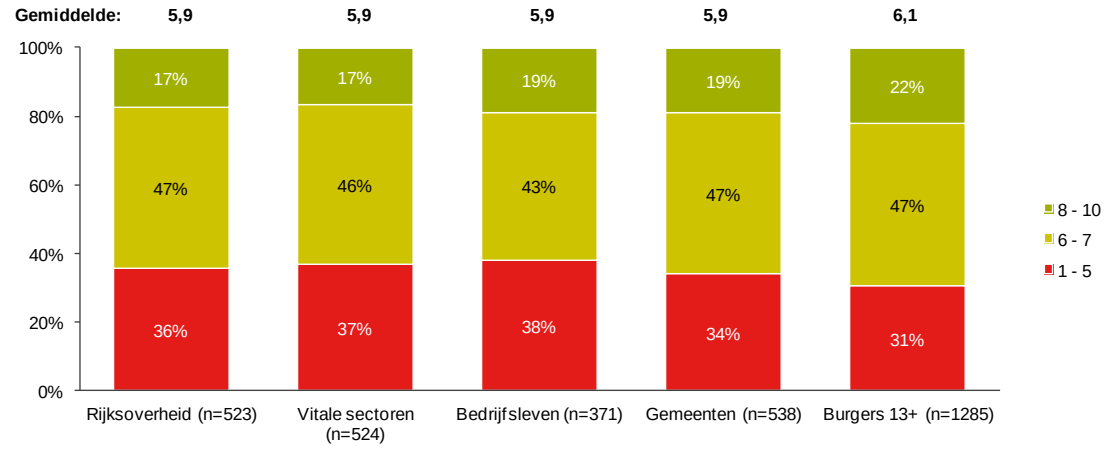
Verschillen binnen groepen

Van de burgers beoordelen mannen (32%) deze veiligheid vaker met een onvoldoende dan vrouwen (22%). Bij de vijftigplussers geeft 33% een onvoldoende ten opzichte van 18% bij de leeftijdscategorie 18-30 jaar. Bij de Rijksambtenaren neemt het vertrouwen in de veiligheid van apps juist toe met leeftijd, 25% van de vijftigplussers geeft een 8-10 vergeleken met 8% van de groep 18-30 jaar oud. 23% van de laagopgeleide medewerkers van vitale sectoren geeft een hoge beoordeling ten opzichte van 11% van de middenopgeleiden.

3.2.1.8 De digitale veiligheid van het openbaar vervoer scoort gemiddeld een 6

Met een gemiddelde score van 6,0 wordt de digitale veiligheid van het openbaar vervoer als net voldoende beoordeeld. Daarmee wordt de digitale veiligheid van het openbaar vervoer als laagste beoordeeld. Een relatief omvangrijke groep van ruim een derde geeft een onvoldoende en gemiddeld 20% geeft een score van 8-10. Tussen de groepen lopen de scoren licht uiteen van een 5,8 tot een 6,1. Er zijn geen significante verschillen tussen de groepen onderling.

Figuur G4_4: Beoordeling digitale veiligheid Openbaar vervoer



Verschillen binnen groepen

Bij de burgers zijn de mannen vaker negatief dan de vrouwen, 35% van de mannen geeft een onvoldoende vergeleken met 27% van de vrouwen. Bij Rijksambtenaren neemt het vertrouwen in de digitale veiligheid van het openbaar vervoer toe met de leeftijd, de jongste leeftijdscategorie geeft een 5,2 en de oudste een 6,2. Laagopgeleide medewerkers van de vitale sectoren geven een 6,2 tegenover een 5,7 bij middenopgeleiden. Ook bij het algemene bedrijfsleven hebben laagopgeleiden meer vertrouwen in de veiligheid, 33% geeft een score van 8-10 ten opzichte van 14% van de hoogopgeleiden.

3.2.2 Beoordeling van het belang van digitale veiligheid

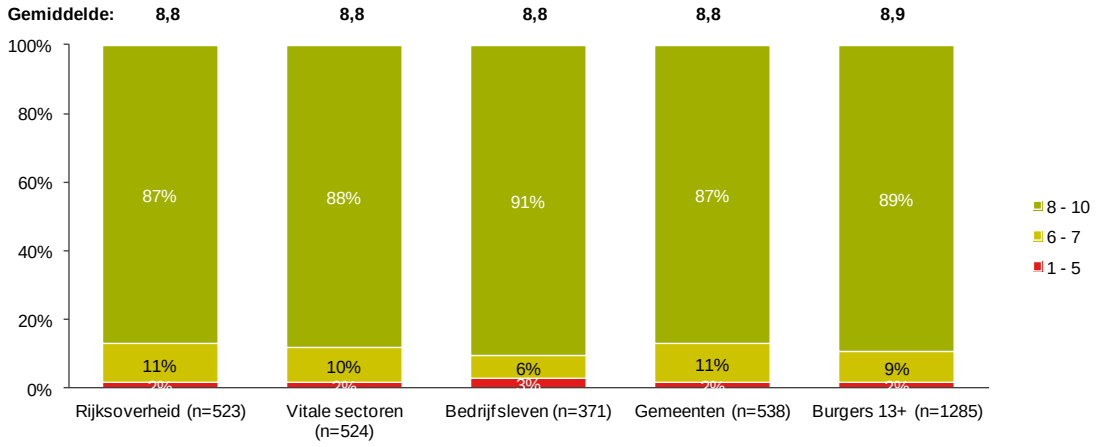
Respondenten hebben via een rapportcijfer aangegeven hoe belangrijk zij de digitale veiligheid thuis, onderweg en op het werk vinden. Zij blijken op alle drie deze gebieden veel waarde te hechten aan de digitale veiligheid, waarbij ze relatief de meeste waarde hechten aan de veiligheid thuis (8,8) en op het werk (8,5) en iets minder waarde hechten aan de digitale veiligheid onderweg (7,5).

3.2.2.1 Belang van digitale veiligheid thuis scoort een 8,8

Alle doelgroepen vinden het extreem belangrijk dat het thuis digitaal veilig is met gemiddelde scores tussen de 8,8 en 8,9 en een overall gemiddelde van 8,8. Slechts 2% van alle ondervraagden geeft dit belang een onvoldoende en 89% geeft een score van 8-10.

Er zijn geen significante verschillen tussen de doelgroepen.

Figuur G5_1: Beoordeling belang van digitale veiligheid Thuis



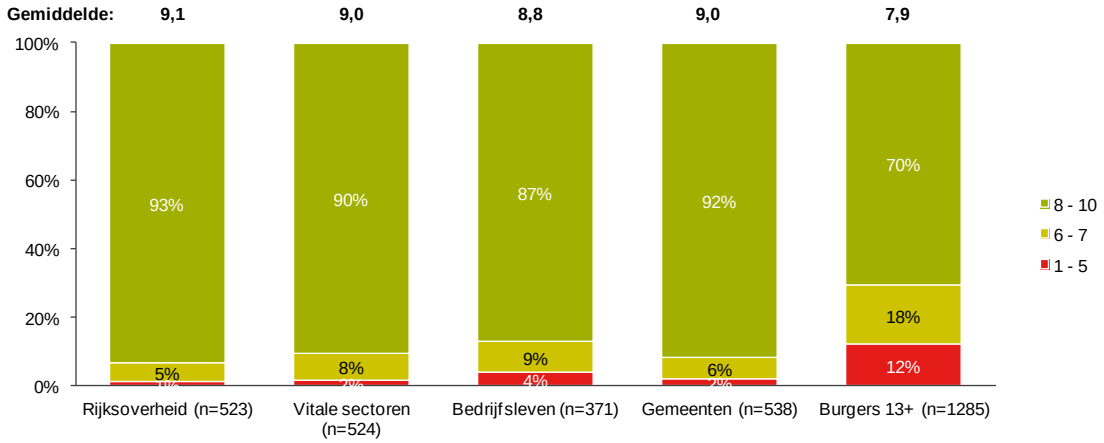
Verschillen binnen groepen

Van de burgers vindt 92% van de vrouwen dit met een score van 8-10 nog iets belangrijker dan mannen (87%). In de leeftijd van 13-17 jaar bevindt zich met 5% het hoogste aantal burgers die dit belang een onvoldoende geeft. Bij medewerkers van de vitale sectoren is ook een leeftijdseffect zichtbaar, bij 18-30 jaar vindt 80% dit zeer belangrijk ten opzichte van 91% bij de categorie van 31-49 jaar.

3.2.2.2 Belang van digitale veiligheid op het werk scoort een 8,5

Ook het belang van digitale veiligheid op het werk wordt zeer hoog bevonden met een overall gemiddelde van een 8,5, gemiddelde scores van 8,8 tot 9,1 voor de professionele doelgroepen en significant lager door burgers met een gemiddelde van 7,9. Van de professionele groepen geeft gemiddeld 2% dit belang een onvoldoende tegenover 12% van de burgers. Dit komt doordat veel burgers zelf niet werkzaam zijn.

Figuur G5_3: Beoordeling belang van digitale veiligheid op het werk



Verschillen tussen groepen

De gemiddelde beoordeling van het belang van digitale veiligheid op het werk is bij alle professionele groepen hoger dan bij burgers. Verder is het gemiddelde oordeel van Rijksambtenaren wat hoger dan dat van medewerkers van het bedrijfsleven.

Verschillen binnen groepen

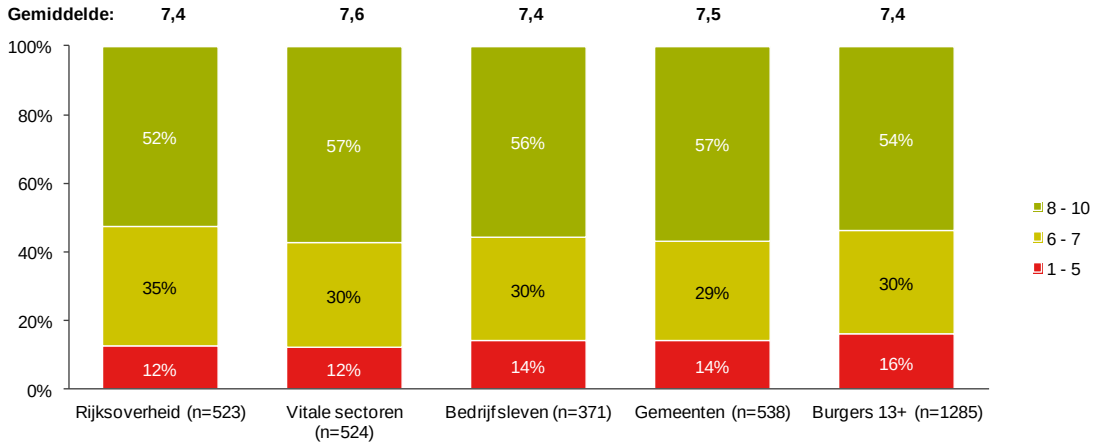
Oudere burgers vinden het belang van digitale veiligheid op het werk belangrijker dan jongere burgers, afgezien van de vijftigplussers waarvan er al veel met pensioen zijn. Voor de Rijksoverheid weegt dit belang ook zwaarder dan voor medewerkers van het algemene bedrijfsleven. Middenopgeleide Rijksambtenaren scoren dit item vaker met 8-10 (63%) dan hoogopgeleide Rijksambtenaren (44%). Dit geldt ook voor de overige professionele doelgroepen, zowel bij de medewerkers van gemeenten, van vitale sectoren en van het algemene bedrijfsleven hechten middenopgeleide medewerkers meer belang aan digitale veiligheid op het werk dan hoogopgeleide medewerkers.

3.2.2.3 Belang van digitale veiligheid onderweg scoort een 7,5

De digitale veiligheid onderweg vindt men van deze drie relatief het minst belangrijk, maar het krijgt gemiddeld nog altijd een overall score van 7,5 en scores van 7,4 tot 7,6 van de diverse doelgroepen. Meer dan de helft geeft een score van 8-10 en gemiddeld 14% geeft een onvoldoende.

Er zijn hierbij geen verschillen tussen de doelgroepen.

Figuur G5_2: Beoordeling belang van digitale veiligheid Onderweg



Verschillen binnen groepen

Mannen (19%) hechten hier vaker weinig belang aan dan vrouwen (14%). Laagopgeleide burgers (20%) beoordelen dit belang ook vaker met een onvoldoende dan middenopgeleiden (13%). Bij de Rijksambtenaren zijn het juist de hoogopgeleiden die het minder vaak (44%) zeer belangrijk vinden dan middenopgeleiden (63%). Het belang van digitale veiligheid onderweg wordt vaker met een onvoldoende beoordeeld door medewerkers van vitale sectoren van boven de 50 (18%) dan van tussen de 31 en 49 (9%). Voor het bedrijfsleven vinden de hoogopgeleide medewerkers (49%) de veiligheid minder vaak zeer belangrijk dan de middenopgeleiden (64%).

3.3 Subthema 3: Smart Coalitions

Bij dit subthema wordt eerst ingegaan op de bestrijding van DDoS-aanvallen, vervolgens op de bestrijding van malware en tot slot op het belang dat respondenten hechten aan samenwerking in diverse branches voor het verhogen van digitale veiligheid.

3.3.1 Grootste rol weggelegd voor provides bij bestrijding DDoS-aanvallen, relatief kleinste rol voor het bedrijfsleven/het MKB

Voorafgaand aan de vragen over de rollen van de diverse partijen bij de bestrijding van DDoS-aanvallen, kregen de ondervraagden eerst de volgende uitleg te zien: DDoS-aanvallen zijn pogingen om een computer, netwerk, website of dienst onbruikbaar te maken. Dergelijke aanvallen leiden doorgaans tot een overbelasting van de server, waardoor reguliere gebruikers geen toegang meer hebben.

Van alle genoemde partijen verwacht men dat providers de grootste rol spelen bij de bestrijding van DDoS-aanvallen (8,4), gevolgd door softwareleveranciers en de (Rijks)overheid (beide 7,9), de wetenschap (7,5), hardwareleveranciers en dienstverleners op het gebied van vitale infrastructuur (beide 7,2), de Europese Commissie (7,1) en tot slot het bedrijfsleven/MKB (7,0).

3.3.2 Providers scoren met gemiddeld een 8,4 het hoogst voor hun rol in de bestrijding van DDoS-aanvallen

Providers krijgen een gemiddelde score van 8,4 overall en van 8,2 tot 8,7 tussen de diverse groepen. Gemiddeld geeft 81% van de ondervraagden een score van 8-10 en 6% een onvoldoende.

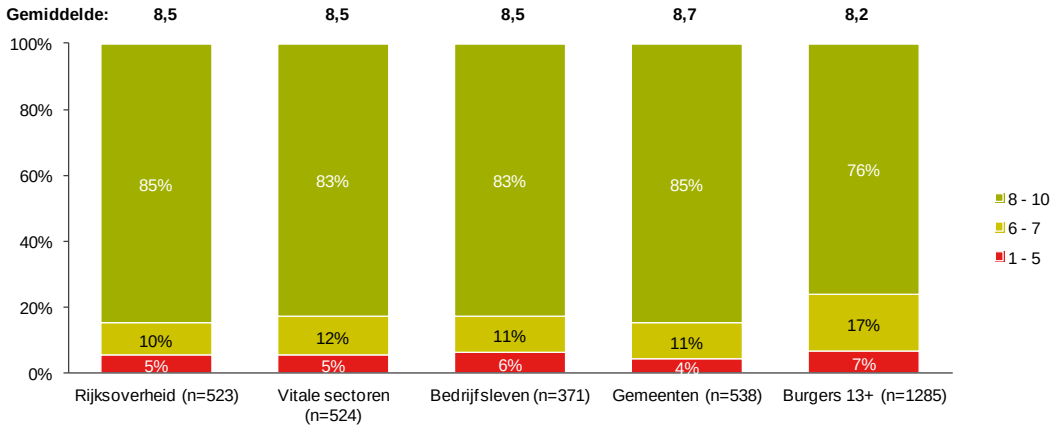
Verschillen tussen groepen

Ambtenaren en medewerkers van vitale sectoren verwachten vaker een grote rol van providers rondom het tegengaan van DDoS-aanvallen dan burgers. Hun gemiddelde beoordeling is hoger dan dat van burgers.

Verschillen binnen groepen

Bij oplopende leeftijd geldt dat de burger meer verwacht van de providers, de groep 13-17 scoort gemiddeld een 7,8 en de groep 31-49 een 8,4. Middenopgeleiden vinden dit vaker (81%) belangrijk dan laagopgeleiden (71%). Ook voor de Rijksambtenaren en medewerkers van vitale sectoren geldt dat ouderen de rol van de providers belangrijker vinden dan jongeren.

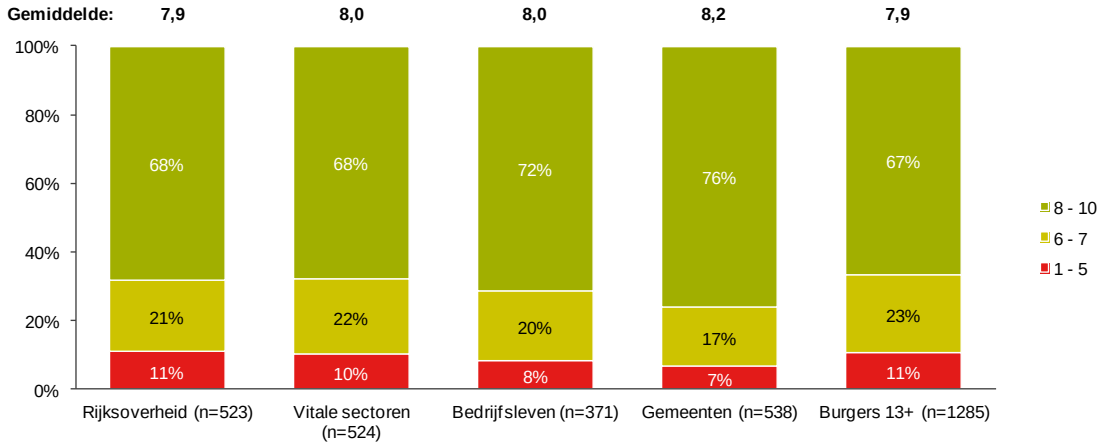
Figuur G6_3: Belang rol bij bestrijding DDoS-aanvallen Providers



3.3.2.1 Software leveranciers scoren gemiddeld een 7,9 voor hun rol in de bestrijding van DDoS-aanvallen

Op de tweede plaats vinden we softwareleveranciers met een gemiddelde score van 7,9 en tussen de 7,9 en de 8,2 onder de doelgroepen. Gemiddeld geeft 69% een ruim voldoende (8-10) en 10% een onvoldoende.

Figuur G6_7: Belang rol bij bestrijding DDoS-aanvallen Software leveranciers



Verschillen tussen groepen

Gemeenten zijn significant vaker van mening dan de overige doelgroepen dat software leveranciers een belangrijke rol moeten spelen bij de verdediging tegen DDoS-aanvallen. De gemiddelde beoordeling van gemeenten is hoger dan die van de Rijksoverheid en burgers.

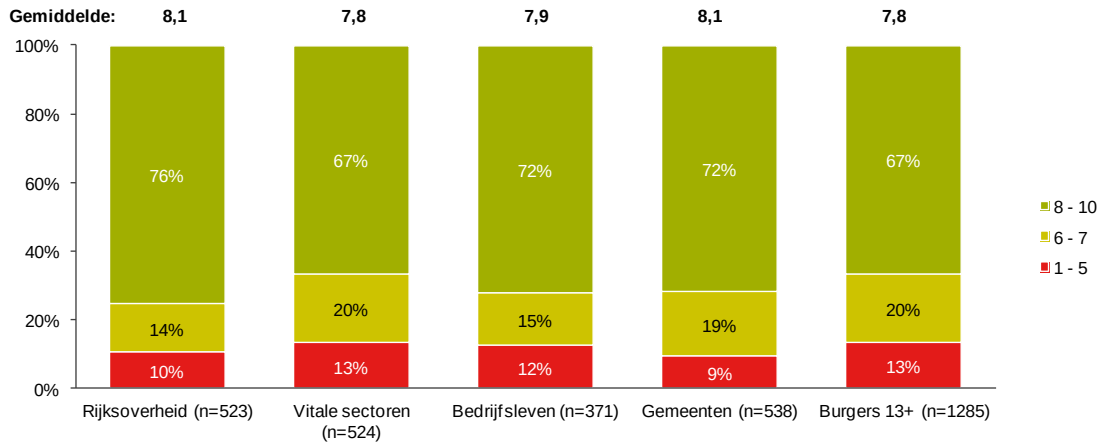
Verschillen binnen groepen

Wederom is het belang bij burgers weer in hoge mate gebonden aan de leeftijd van de ondervraagden, dit loopt op van gemiddeld 7,4 bij de groep 13-17 jaar tot 8,1 bij vijftigplussers. Dit leeftijdsverband is ook zichtbaar bij alle vier de professionele doelgroepen, zo scoort bijvoorbeeld bij de Rijksambtenaren de groep 18-30 jaar gemiddeld een 7,2 en de groep 50+ een 8,2.

3.3.2.2 (Rijks)overheid scoort gemiddeld een 7,9 voor hun rol in de bestrijding van DDoS-aanvallen

De overheid neemt een gedeelde tweede plaats in wat betreft de rol die zij in de ogen van de respondenten spelen bij het bestrijden van DDoS-aanvallen. Deze partij scoort gemiddeld een 7,9 en tussen de doelgroepen een 7,8 en 8,1.

Figuur G6_1: Belang rol bij bestrijding DDoS-aanvallen (Rijks)overheid



Verschillen tussen groepen

Vooral de Rijksambtenaren zelf vinden dit belangrijker dan de burgers en de medewerkers van vitale sectoren. Gemiddeld geeft 70% van de ondervraagden een score van 8-10 en 12% een onvoldoende. Er zijn geen verschillen in de gemiddelde beoordelingen tussen de doelgroepen.

Verschillen binnen groepen

Mannen geven vaker (16%) een onvoldoende dan vrouwen (11%) en burgers van boven de 30 vinden significant vaker dat de (Rijks)overheid een belangrijke rol hierbij moet spelen dan burgers van onder de 30. Middenopgeleide medewerkers van gemeenten (83%) geven dit belang vaker een score van 8-10 dan hoogopgeleide medewerkers (67%).

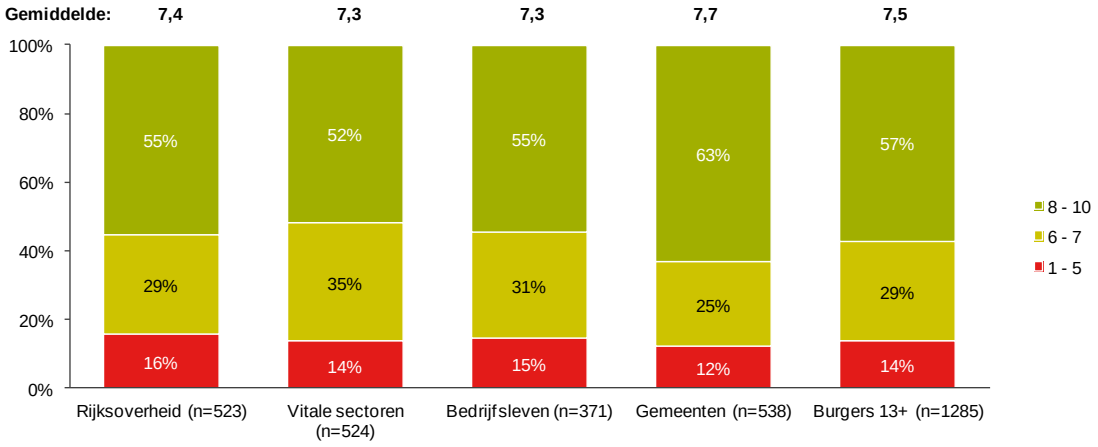
3.3.2.3 De wetenschap scoort gemiddeld een 7,5 voor zijn rol in de bestrijding van DDoS-aanvallen

De wetenschap neemt de derde plaats in wat betreft de gepercipieerde bijdrage die ze leveren aan bestrijding van DDoS-aanvallen. De gemiddelde overall score is een 7,5 en tussen de doelgroepen is dat tussen de 7,3 en 7,7. Gemiddeld geeft 57% een score van 8-10 en 14% een onvoldoende.

Verschillen tussen groepen

Medewerkers van gemeenten zien vaker dan medewerkers van vitale sectoren een belangrijke rol voor de wetenschap weg gelegd. Verder zien we dat de gemiddelde beoordeling van gemeenten hoger is dan die van vitale sectoren en het bedrijfsleven.

Figuur G6_8: Belang rol bij bestrijding DDoS-aanvallen Wetenschap



Verschillen binnen groepen

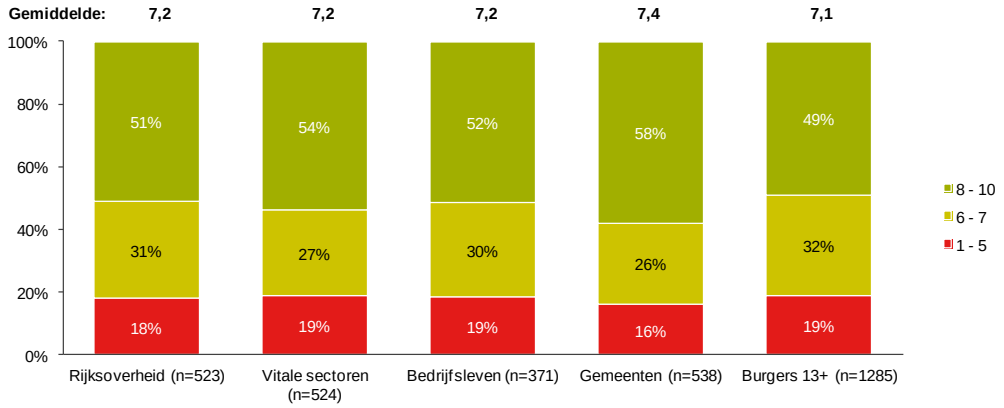
Van de burgers boven de 50 jaar oud geeft 65% een score van 8-10, dat is significant meer dan de drie jongere leeftijdscategorieën waarvan de jongste maar 42% deze score geeft. Voor de medewerkers van de vitale sectoren geldt dat hoe hoger men opgeleid is, hoe kleiner de verwachting is die men koestert ten opzichte van de wetenschap wat betreft het aandragen van oplossingen voor het verweer tegen DDoS-aanvallen. Gemiddeld scoren laagopgeleiden een 7,9 en hoogopgeleiden een 7,0.

Voor de Rijksambtenaren en de medewerkers van het algemene bedrijfsleven geldt weer dat men vaker een belangrijke rol toedicht aan de wetenschap bij een hogere leeftijd.

3.3.2.4 Dienstverleners op het gebied van de vitale infrastructuur scoren gemiddeld een 7,2 voor hun rol in de bestrijding van DDoS-aanvallen

Men geeft de rol die dienstverleners op het terrein van de vitale infrastructuur spelen gemiddeld een 7,2; dit is een score van 7,1 tot 7,4 onder de doelgroepen. Gemiddeld geeft 52% een score van 8-10 en 18% een onvoldoende.

Figuur G6_4: Belang rol bij bestrijding DDoS-aanvallen Dienstverleners vitale infrastructuur



Verschillen tussen groepen

Medewerkers van gemeenten schatten de rol van dienstverleners op het gebied van vitale infrastructuur bij het tegengaan van DDoS-aanvallen groter in dan de burgers. Er zijn geen verschillen in de gemiddelde beoordelingen tussen de doelgroepen.

Verschillen binnen groepen

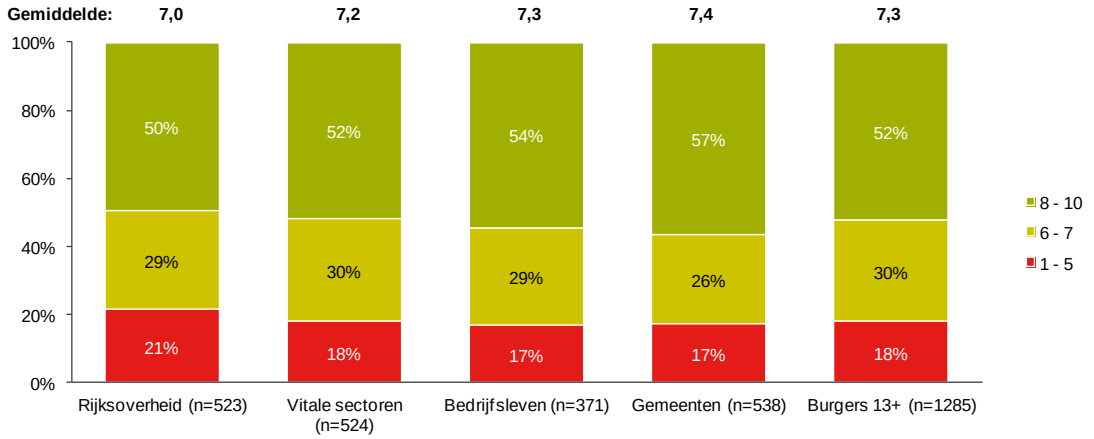
Bij de burgers zien we weer een sterk verband met leeftijd, hoe ouder, hoe groter men verwacht dat de rol zal zijn van de dienstverleners. De groep 18-30 jaar scoort gemiddeld een 6,4 en de vijftigplussers een 7,5. Middenopgeleiden (7,3) verwachten ook meer van de vitale sector dan de hoogopgeleiden (6,8). Bij alle professionele doelgroepen is hetzelfde verband te zien, hoe ouder de ondervraagden, hoe meer men verwacht van de rol van dienstverleners in de vitale infrastructuur. En ook hier wordt een belangrijkere rol toegekend door de middenopgeleiden dan door de hoogopgeleiden.

3.3.2.5 Hardware leveranciers scoren gemiddeld een 7,2 voor hun rol in de bestrijding van DDoS-aanvallen

Hardwareleveranciers krijgen gemiddeld een score van 7,2 en tussen de doelgroepen een 7 tot 7,4. Ruim de helft van de ondervraagden wil graag dat hardwareleveranciers een belangrijke rol gaan spelen bij het weren van DDoS-aanvallen en gemiddeld 18% geeft dit belang een onvoldoende.

Er zijn geen verschillen tussen de doelgroepen.

Figuur G6_6: Belang rol bij bestrijding DDoS-aanvallen Hardware leveranciers



Verschillen binnen groepen

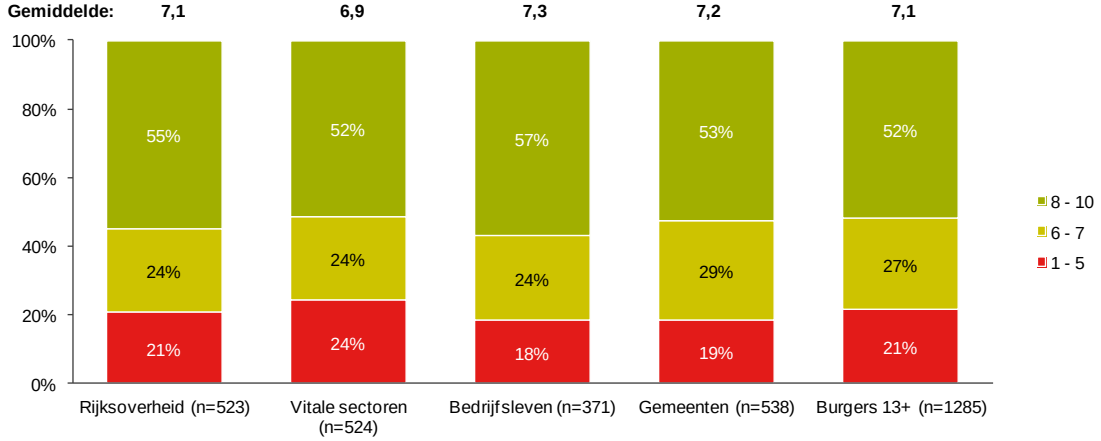
Bij de burgers verwachten vrouwen (55%) dit vaker dan mannen (49%). Van de oudste groep burgers scoort 59% een 8-10 ten opzichte van 46% van de groep 18-30 jaar. Zware internetgebruikers verwachten minder van de rol van hardwareleveranciers dan lichte of medium internetgebruikers. 44% van de hoogopgeleide medewerkers van vitale sectoren geeft een score van 8-10 ten opzichte van 59% van de laagopgeleide medewerkers.

3.3.2.6 De Europese Commissie scoort gemiddeld een 7,1 voor zijn rol in de bestrijding van DDoS-aanvallen

De Europese commissie scoort gemiddeld een 7,1 en tussen de doelgroepen een 6,9 tot 7,3 voor de belangrijkheid van hun rol bij de bestrijding van DDoS-aanvallen. Gemiddeld geeft 53% een score van 8-10 en 21% een onvoldoende.

Er zijn geen significante verschillen tussen de doelgroepen.

Figuur G6_2: Belang rol bij bestrijding DDoS-aanvallen Europese commissie



Verschillen binnen groepen

Bij de burgers zijn vrouwen (55%) hier vaker voorstander van dan mannen (49%). In de leeftijdscategorie 18-30 jaar ziet men het minst vaak (39%) een belangrijke rol weg gelegd voor de Europese commissie. Bij de Rijksambtenaren zijn hoogopgeleiden (47%) minder vaak een sterke voorstander dan middenopgeleiden (65%). Bij de medewerkers van de gemeenten en de vitale sectoren is eenzelfde verband te zien: hoogopgeleiden hebben significant minder vaak een score van 8-10 dan middenopgeleiden.

3.3.2.7 Het bedrijfsleven en het MKB scoren gemiddeld een 7 voor hun rol in de bestrijding van DDoS-aanvallen

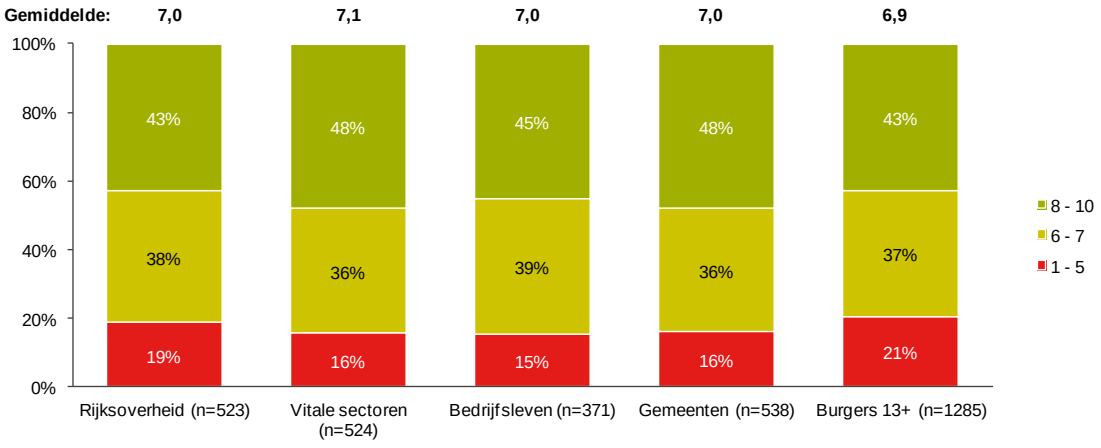
Met een gemiddelde score van een 7 overall en tussen de groepen van 6,9 tot 7,1 zijn het bedrijfsleven en het MKB relatief gezien de hekkensluiter wat betreft hun gepercipieerde aandeel in het tegengaan van DDoS-aanvallen. Gemiddeld geeft 45% een score van 8-10 en 18% een onvoldoende.

Er zijn geen significante verschillen tussen de doelgroepen.

Verschillen binnen groepen

Hoogopgeleide burgers (34%) geven minder vaak dan laagopgeleide burgers (43%) een score van 8-10. 51% van de vijftigplussers geeft een hoge beoordeling wat significant meer is dan bij ondervraagden onder de 30 jaar. Laagopgeleide Rijksambtenaren beoordelen de belangrijkheid van de rol van het bedrijfsleven gemiddeld met een 7,4, voor de hoogopgeleide Rijksambtenaren is dit 6,7. Dit verschil is ook te zien bij middenopgeleide (7,5) en hoogopgeleide (6,9) medewerkers van gemeenten.

Figuur G6_5: Belang rol bij bestrijding DDoS-aanvallen Bedrijfsleven + MKB



3.3.3 Ook bij de bestrijding van malware grootste rol weggelegd door providers; relatief kleinste rol voor het bedrijfsleven/MKB en de Europese Commissie

Naast hun perceptie van de rollen van de hiervoor besproken partijen bij het tegengaan van DDoS-aanvallen is de respondenten ook gevraagd naar hun beeld van de rol die deze partijen spelen bij de bestrijding van malware. Alvorens hier hun mening over te geven, kregen alle ondervraagden de volgende tekst te zien: Malware is kwaadaardige en/of schadelijke software. Er zijn veel verschillende varianten van malware, het 'virus' is de meest bekende vorm.

De verwachtingen over de rol die de diverse partijen spelen bij de bestrijding van malware, liggen grotendeels in lijn met de eerder besproken verwachtingen bij het bestrijden van DDoS-aanvallen. Van alle genoemde partijen verwacht men ook hierbij dat providers ook de grootste rol spelen bij de bestrijding van malware (8,1), gevolgd door softwareleveranciers (7,9), de (Rijks)overheid (7,3), de wetenschap (7,1), hardwareleveranciers (6,9), het bedrijfsleven/MKB (6,8) en de Europese commissie (6,8) en tot slot dienstverleners op het gebied van vitale infrastructuur (6,7).

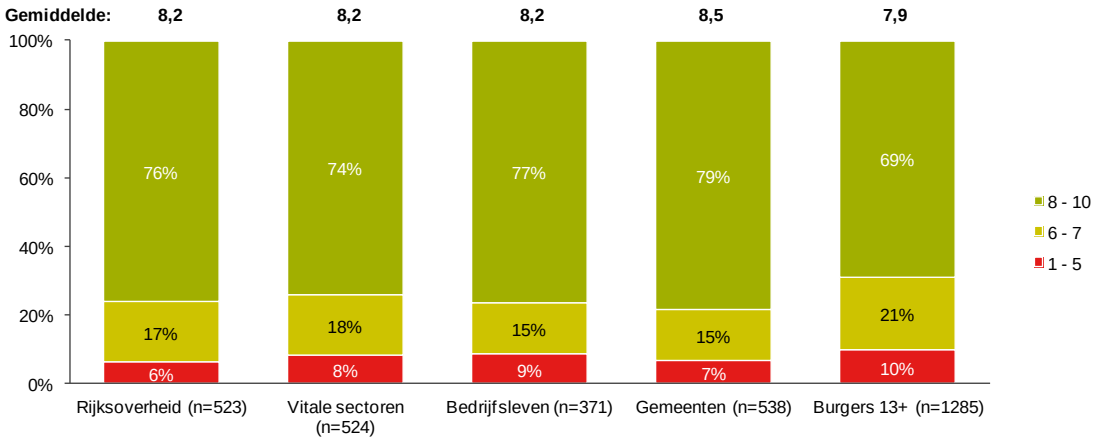
3.3.3.1 Providers scoren gemiddeld met een 8,1 het hoogst voor hun rol in de bestrijding van malware

Ook bij de bestrijding van malware verwacht men dat providers de allerbelangrijkste rol zullen spelen. De gemiddelde score is een 8,1 en varieert van 7,9 tot 8,5 tussen de doelgroepen. Gemiddeld geeft 73% een score van 8-10 en 8% een onvoldoende.

Verschillen tussen groepen

Ambtenaren verwachten vaker een rol van providers dan burgers, hun gemiddelde score is hoger. Gemeenten hebben een hogere gemiddelde score dan vitale sectoren.

Figuur G7_3: Belang rol bij bestrijding malware Providers



Verschillen binnen groepen

Van de burgers verwachten ouderen vaker dat de rol van de providers belangrijk zal zijn dan de jongeren, in de groep 13-17 geeft 53% een score van 8-10 tegenover 74% van de groep 31-49. Dit leeftijdseffect is ook zichtbaar bij de Rijksambtenaren, de groep 18-30 geeft gemiddeld een 7,6 en de groep 50+ een 8,5.

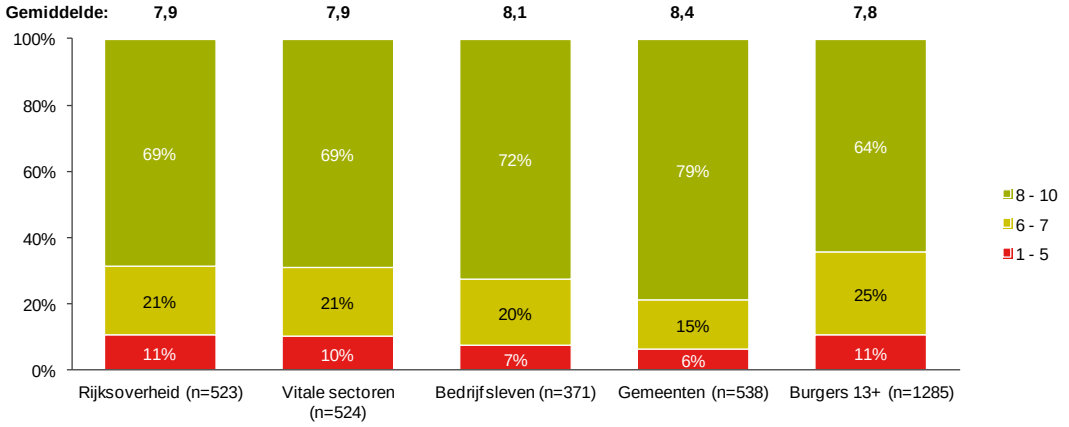
3.3.3.2 Software leveranciers scoren gemiddeld een 7,9 voor hun rol in de bestrijding van malware

Men schrijft ook een belangrijke rol toe aan de software leveranciers voor de bestrijding van malware, met een gemiddelde score van 7,9 en onder de doelgroepen variërend van 7,8 tot 8,4. Gemiddeld geeft 69% een score van 8-10 en 10% een onvoldoende.

Verschillen tussen groepen

De medewerkers van de gemeenten scoren hierop hoger dan de medewerkers van Rijksoverheid, de vitale sectoren en dan burgers. Medewerkers van het bedrijfsleven scoren hierop ook hoger dan burgers.

Figuur G7_7: Belang rol bij bestrijding malware Software leveranciers



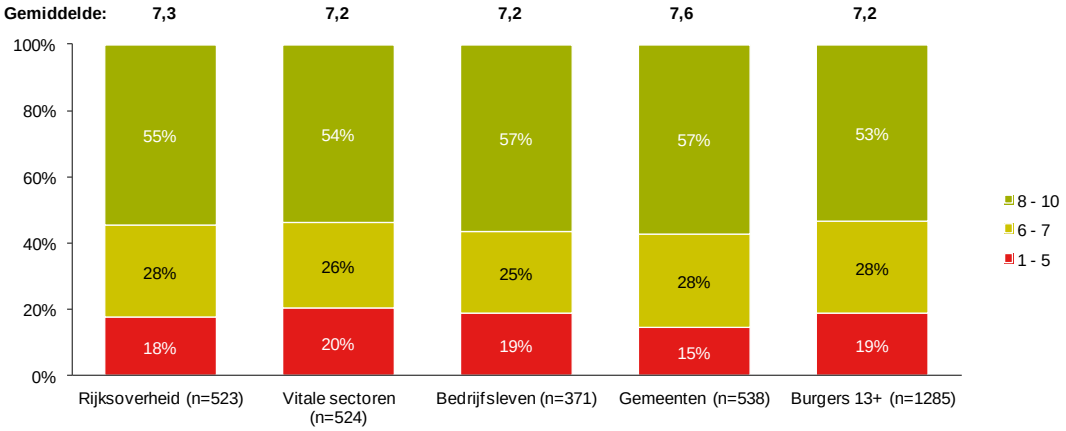
Verschillen binnen groepen

Burgers van boven de 30 jaar hebben een hogere verwachting van de rol van de software leveranciers dan als men onder de 30 jaar is. Hoogopgeleiden (69%) geven vaker een score van 8-10 dan laagopgeleiden (60%). Rijksambtenaren in de leeftijd 18-30 jaar geven gemiddeld een 7,3 voor de belangrijkheid van de rol van software leveranciers ten opzichte van een 8,1 voor vijftigplussers.

3.3.3.3 De (Rijks)overheid scoort gemiddeld een 7,9 voor zijn rol in de bestrijding van malware

Op de derde plaats komt de Rijksoverheid met een score van 7,3 overall en 7,2 tot 7,6 onder de doelgroepen. Gemiddeld geeft 55% een score van 8-10 en 18% een onvoldoende.

Figuur G7_1: Belang rol bij bestrijding malware (Rijks)overheid



Verschillen tussen groepen

Gemeenten scoren gemiddeld hoger dan burgers.

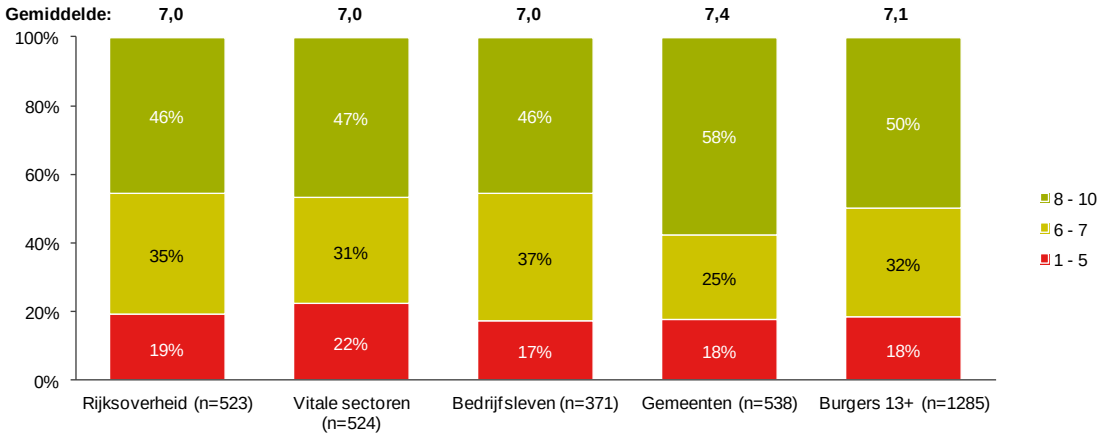
Verschillen binnen groepen

Van de burgers geven de mannen (22%) dit belang iets vaker een onvoldoende dan de vrouwen (16%). Middenopgeleide burgers (57%) geven dit belang vaker een score van 8-10 dan hoogopgeleide burgers (46%). Dit verschil zien we ook terug bij hoogopgeleide Rijksambtenaren (47%) ten opzichte van laag- en middenopgeleiden (66 en 63%). Ook voor de medewerkers van gemeenten geldt dat de hoogopgeleiden dit belang minder onderschrijven.

3.3.3.4 De wetenschap scoort gemiddeld een 7,1 voor zijn rol in de bestrijding van malware

Het belang van de rol van de wetenschap wordt ingeschat met een gemiddelde van 7,1 en tussen de 7 en 7,4 bij de doelgroepen. Gemiddeld geeft 50% een score van 8-10 en 19% een onvoldoende.

Figuur G7_8: Belang rol bij bestrijding malware Wetenschap



Verschillen tussen groepen

De medewerkers van de gemeenten schatten dit belang gemiddeld hoger in dan alle andere doelgroepen.

Verschillen binnen groepen

Vooral burgers ouder dan vijftig verwachten veel van de wetenschap, 58% geeft een score van 8-10. Zware internetgebruikers van 14 uur of meer per week schatten de rol van wetenschap significant lager in dan gemiddelde internetgebruikers, 24% geeft een onvoldoende. Bij Rijksambtenaren en medewerkers van vitale sectoren zijn het ook weer vooral de vijftigplussers die de rol van de wetenschap als zeer belangrijk beschouwen. Bij de gemeenten beoordelen hoogopgeleide medewerkers (20%) de rol van de wetenschap vaker met een onvoldoende dan middenopgeleide medewerkers (11%).

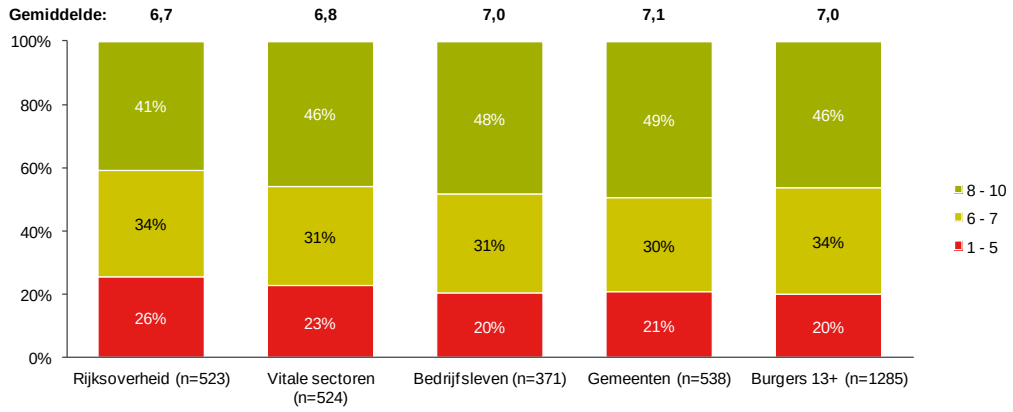
3.3.3.5 Hardwareleveranciers scoren gemiddeld een 6,9 voor hun rol in de bestrijding van malware

De rol die hardware leveranciers spelen bij de bestrijding van malware wordt uitgedrukt met een voldoende (9,9); tussen de doelgroepen loopt dit uiteen van een 6,7 tot een 7,1. Gemiddeld geeft 46% een score van 8-10 en 22% een onvoldoende.

Verschillen tussen groepen

Ambtenaren van de Rijksoverheid schatten de rol van hardwareleveranciers bij de bestrijding van malware het minst hoog in met een 6,7, dit is lager dan gemeenteambtenaren (7,1).

Figuur G7_6: Belang rol bij bestrijding malware Hardware leveranciers



Verschillen binnen groepen

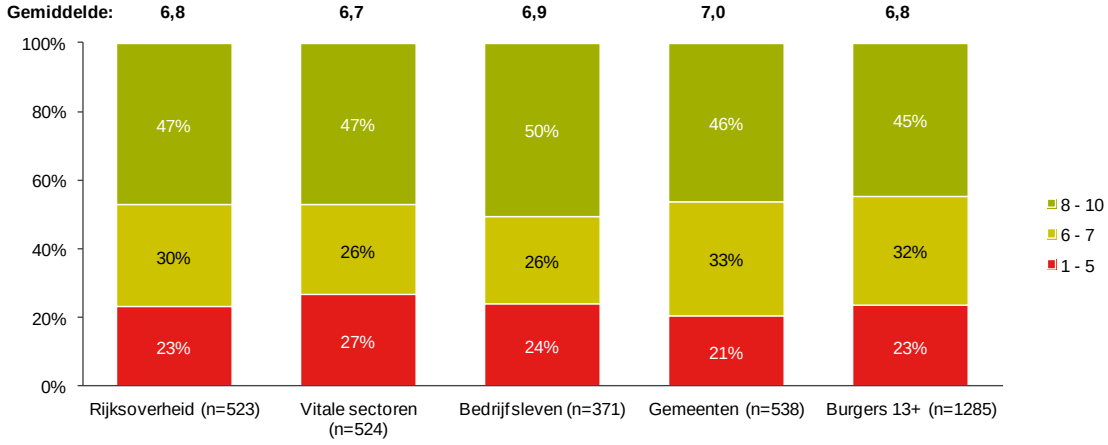
Van de burgers schatten vrouwen (7,3) dit belang hoger in dan mannen (6,7). Jongeren van onder de 30 jaar (6,7 en 6,6) vinden de rol van hardwareleveranciers minder belangrijk dan dertigplussers. Bij de Rijksambtenaren en medewerkers van het bedrijfsleven denken laagopgeleiden dat het belang van hardwareleveranciers hoger is dan hoogopgeleiden. Zo geeft 30% van de hoogopgeleide Rijksambtenaren een onvoldoende ten opzichte van 15% van de laagopgeleide Rijksambtenaren.

3.3.3.6 De Europese Commissie scoort gemiddeld een 6,8 voor zijn rol in de bestrijding van malware

Het belang van de rol van de Europese commissie varieert van een score van 6,7 bij de medewerkers van vitale sectoren tot een 7 bij gemeentemedewerkers; de overall score is een 6,8. Gemiddeld geeft 46% een score van 8-10 en 24% een onvoldoende.

Er zijn geen verschillen tussen de doelgroepen.

Figuur G7_2: Belang rol bij bestrijding malware Europese commissie



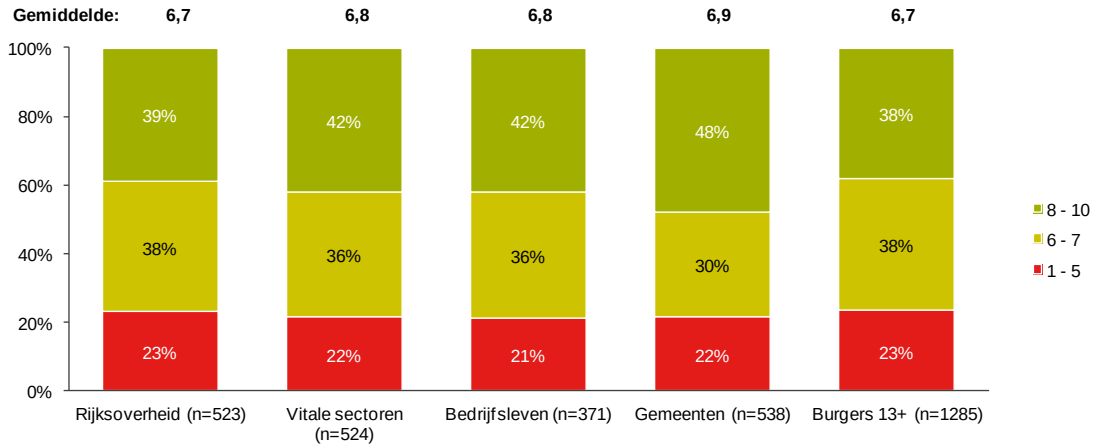
Verschillen binnen groepen

Dit belang wordt vaker met een onvoldoende beoordeeld door mannelijke burgers (27%) dan vrouwelijke (20%). Jongeren van onder de 30 jaar vinden de rol van de Europese Commissie minder belangrijk dan burgers van boven de 30 jaar. Hoogopgeleide Rijksambtenaren (28%) geven dit belang vaker een onvoldoende dan laagopgeleide Rijksambtenaren (12%). Ook voor medewerkers van vitale sectoren geldt dat hoogopgeleiden minder vaak een score van 8-10 geven dan laag- en middenopgeleiden.

3.3.3.7 Het bedrijfsleven / MKB scoort gemiddeld een 6,8 voor zijn rol in de bestrijding van malware

Voor het bedrijfsleven en MKB ligt de score tussen de 6,7 en 6,9, overall bezien een 6,8. Gemiddeld geeft 41% een score van 8-10 en 23% een onvoldoende.

Figuur G7_5: Belang rol bij bestrijding malware Bedrijfsleven + MKB



Verschillen tussen groepen

De medewerkers van gemeenten kennen significant vaker een belangrijke rol toe aan het bedrijfsleven en MKB bij de bestrijding van malware dan de overige doelgroepen. Er zijn geen verschillen in de gemiddelde beoordeling tussen groepen.

Verschillen binnen groepen

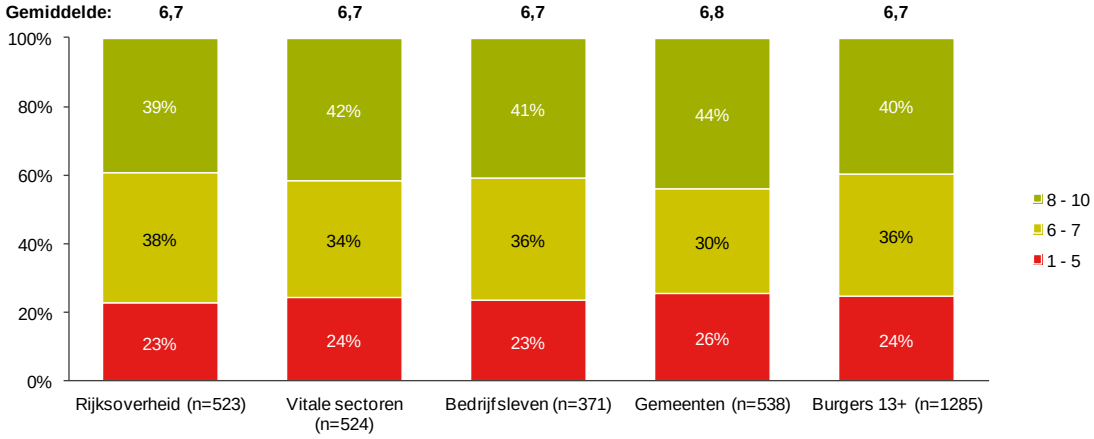
Oudere burgers verwachten eerder een belangrijke rol van het bedrijfsleven dan jongere, van de groep 18-30 jaar geeft 23% een score van 8-10, voor de groep 50+ is dit 45%. Hoogopgeleiden (32%) geven verder minder vaak een hoge score dan middenopgeleiden (42%). Voor alle vier de professionele doelgroepen geldt ook weer dat de belangrijkheid van de rol hoger wordt ingeschat naarmate men ouder en lager opgeleid is. Zo scoren laagopgeleide Rijksambtenaren gemiddeld een 7,3 tegenover een 6,4 bij hoogopgeleide Rijksambtenaren.

3.3.3.8 Dienstverleners van de vitale infrastructuur hebben gemiddeld met een 6,7 de laagste score voor hun aandeel in de bestrijding van malware

De gemiddelde score voor dienstverleners van de vitale infrastructuur zoals energie- en watervoorziening bij het weren van malware ligt tussen de 6,7 en 6,8; overall gemiddeld een 6,7. Gemiddeld geeft 41% een score van 8-10 en 24% een onvoldoende.

Er zijn geen significante verschillen tussen de doelgroepen.

Figuur G7_4: Belang rol bij bestrijding malware Dienstverleners vitale infrastructuur



Verschillen binnen groepen

Bij de burgers gaat het dan vooral om ouderen, vijftigplussers geven gemiddeld een 7,1 tegenover een 6 bij de groep 18-30. Hoogopgeleiden denken minder vaak dan lageropgeleiden dat de vitale sectoren een grote rol spelen. Bij alle vier de professionele doelgroepen zijn dezelfde verschillen te zien. Jongeren denken minder vaak dan ouderen dat deze dienstverleners een belangrijke rol spelen en hoogopgeleiden denken dit minder vaak dan laag- en middenopgeleiden.

3.3.4 Samenwerking voor het verhogen van de digitale veiligheid wordt als het belangrijkste beschouwd in de financiële sector en als relatief het minst belangrijk in de oppervlaktewatersector

Achtereenvolgens hechten respondenten het meeste belang aan samenwerking voor het verhogen van digitale veiligheid in de financiële sector (8,5), op de voet gevolgd door de telecommunicatie (8,2) en op enige afstand gevolgd door energie en drinkwater (beide 7,3), transport (7,1) en tot slot oppervlaktewater (6,9).

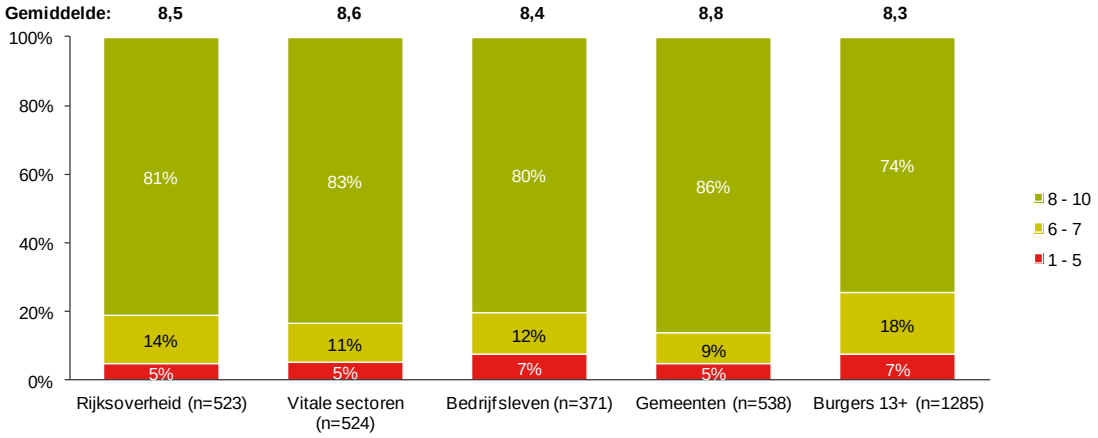
3.3.4.1 Het belang van samenwerking voor verhoging van de digitale veiligheid scoort het hoogst voor de financiële sector (8,5)

Samenwerking binnen de financiële sector voor de verbetering van de digitale veiligheid wordt het allerbelangrijkst gevonden van alle sectoren, de gemiddelde score is tussen de 8,3 en 8,8 en overall een 8,5. Gemiddeld geeft 80% een score van 8-10 en 6% een onvoldoende.

Verschillen tussen groepen

Burgers vinden deze samenwerking minder vaak zeer belangrijk dan de professionele doelgroepen. Verder zien we dat de gemiddelde beoordeling van gemeenten hoger is dan die van de Rijksoverheid, het bedrijfsleven en burgers. De gemiddelde beoordeling van vitale sectoren is hoger dan die van burgers.

Figuur G8_3: Belang samenwerking binnen de financiële sector



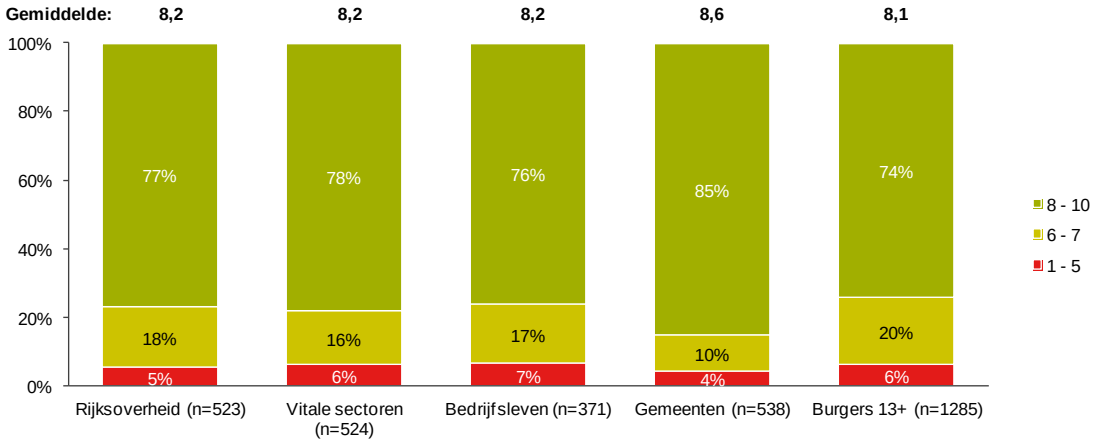
Verschillen binnen groepen

Bij de burgers vinden mannen (78%) het belangrijker dan vrouwen (71%) en vijftigplussers (83%) belangrijker dan jongeren. Hoe ouder Rijksambtenaren en medewerkers van het bedrijfsleven zijn, hoe meer men van mening is dat het nodig is dat er binnen de financiële sector aan de digitale veiligheid wordt gewerkt.

3.3.4.2 Het belang van samenwerking voor verhoging van de digitale veiligheid scoort een 8,2 voor de telecommunicatie sector

Op de tweede plaats vindt men het zeer belangrijk dat er wordt samengewerkt binnen de telecommunicatiesector op het gebied van digitale veiligheid. Men geeft gemiddeld een score van 8,2, uiteenlopend van 8,1 tot 8,6 onder de vijf doelgroepen. Gemiddeld geeft 77% een score van 8-10 en 6% een onvoldoende.

Figuur G8_2: Belang samenwerking binnen de telecommunicatie sector



Verschillen tussen de groepen
Gemeentemedewerkers vinden dit wederom belangrijker dan de overige doelgroepen.

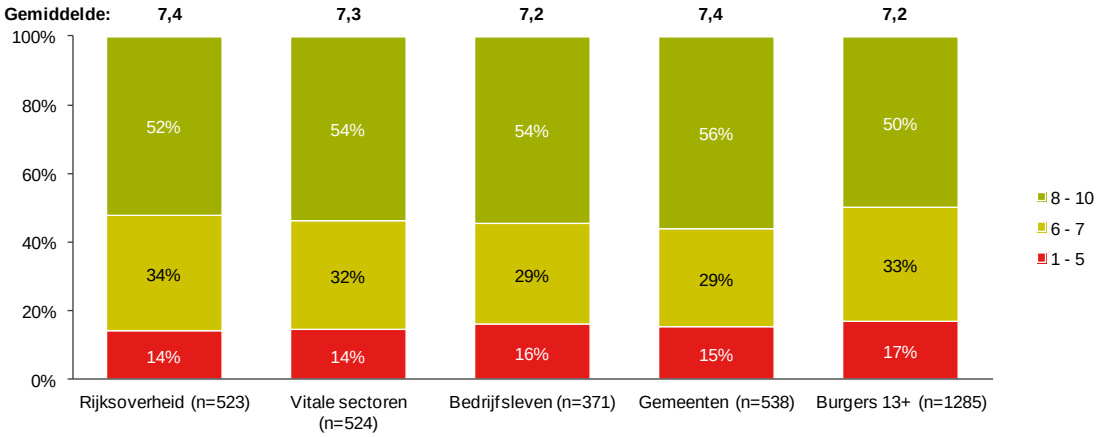
Verschillen binnen groepen
Mannen (78%) vinden dit vaker zeer belangrijk dan vrouwen (71%). Van de vijftigplussers geeft 82% een score van 8-10. Midden- en hoogopgeleiden vinden de samenwerking binnen telecommunicatie belangrijker dan laagopgeleiden. Voor de Rijksambtenaren, gemeentemedewerkers en medewerkers van het bedrijfsleven geldt weer dat men samenwerking belangrijker vindt naarmate de leeftijd van de ondervraagde hoger is.

3.3.4.3 Het belang van samenwerking voor verhoging van de digitale veiligheid scoort een 7,3 voor de energiesector

Het belang van samenwerking binnen de energiesector scoort gemiddeld tussen de 7,2 en 7,4, overall gemiddeld een 7,3. Gemiddeld geeft 53% een score van 8-10 en 16% een onvoldoende.

Er zijn geen significante verschillen tussen de doelgroepen.

Figuur G8_1: Belang samenwerking binnen de energie sector



Verschillen binnen groepen

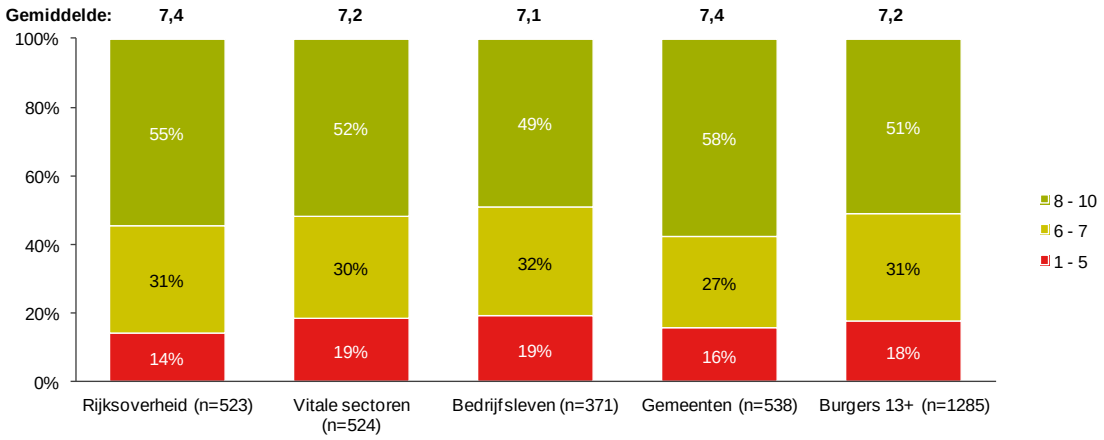
Onder burgers is er een sterk leeftijdseffect voor de mate waarin men het belangrijk vindt dat er samen gewerkt wordt binnen de energiesector om de digitale veiligheid te verhogen. De groep 13-17 jaar geeft hier gemiddeld een 6,2 voor, bij de groep 50+ loopt dit op tot een 7,7. Hoogopgeleiden geven met 24% vaker een onvoldoende dan laag- en middenopgeleiden. Ook voor de vier professionele doelgroepen geldt dat het percipieerde belang van samenwerking binnen de energiesector zeer sterk toeneemt met leeftijd.

3.3.4.4 Het belang van samenwerking voor verhoging van de digitale veiligheid scoort een 7,3 voor de drinkwatersector

Voor de drinkwatersector ligt de score gemiddeld tussen de 7,1 en 7,4; overall een 7,3. Gemiddeld geeft 53% een score van 8-10 en 17% een onvoldoende.

Er zijn geen significante verschillen tussen de doelgroepen.

Figuur G8_4: Belang samenwerking binnen de drinkwatersector



Verschillen binnen groepen

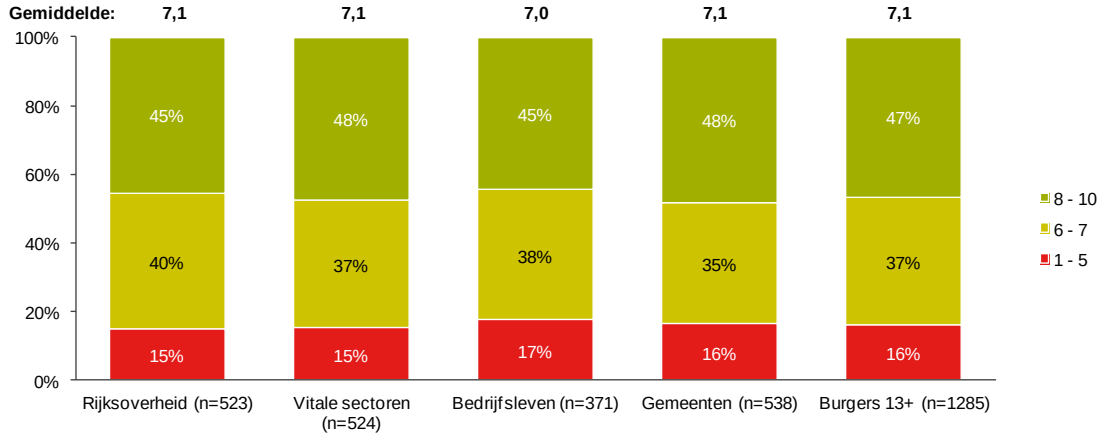
Burgers vinden het naarmate ze ouder zijn belangrijker dat er wordt samengewerkt binnen de drinkwatersector om de digitale veiligheid te verhogen. Hoogopgeleiden (24%) geven hiervoor vaker een onvoldoende dan laag- en middenopgeleiden. Voor alle professionele doelgroepen geldt weer dat jongere medewerkers minder vaak het belang inzien van samenwerking binnen de drinkwatersector dan oudere medewerkers.

3.3.4.5 Het belang van samenwerking voor verhoging van de digitale veiligheid scoort een 7,1 voor de transportsector

Voor de transportsector ligt de score gemiddeld tussen de 7,0 en 7,1; overall gemiddeld een 7.1. Gemiddeld geeft 47% een score van 8-10 en 16% een onvoldoende.

Er zijn geen significante verschillen tussen de doelgroepen.

Figuur G8_6: Belang samenwerking binnen de transportsector



Verschillen binnen groepen

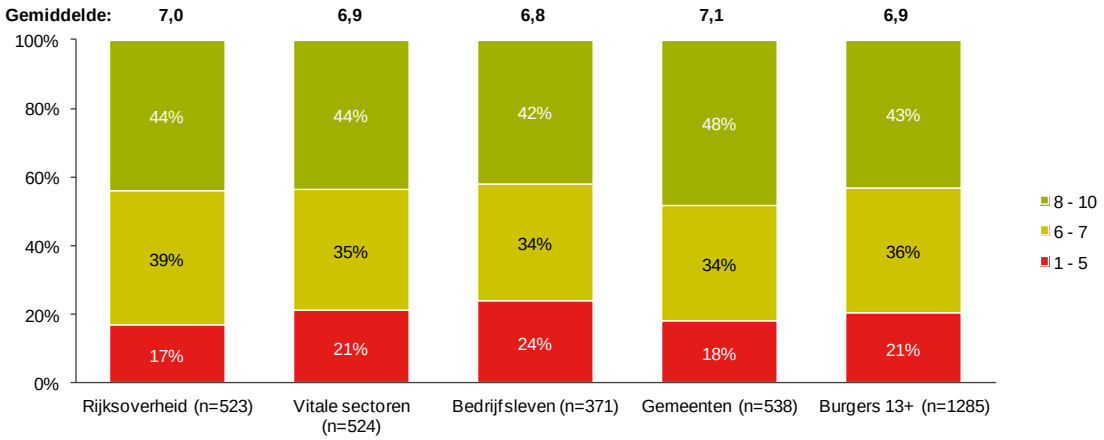
Voor wat betreft het belang van samenwerking binnen de transportsector om de digitale veiligheid te vergroten geldt voor zowel de burgers als voor de professionele doelgroepen dat oudere ondervraagden dit belang hoger inschatten dan jongere ondervraagden en dat middenopgeleide ondervraagden het belangrijker vinden dan hoogopgeleide ondervraagden.

3.3.4.6 Het belang van samenwerking voor verhoging van de digitale veiligheid scoort relatief het laagst voor de oppervlaktewatersector (6,9)

Men vindt de oppervlaktewatersector relatief de minst belangrijke voor wat betreft samenwerken aan het verhogen van de digitale veiligheid. De score ligt gemiddeld tussen de 6,8 en 7,1; overal gemiddeld is dit een 6,9. Gemiddeld geeft 44% een score van 8-10 en 20% een onvoldoende.

Er zijn geen significante verschillen tussen de doelgroepen.

Figuur G8_5: Belang samenwerking binnen de oppervlaktewatersector



Verschillen binnen groepen

Van de burgers uit de groep 18-30 geeft 24% een score van 8-10 ten opzichte van 54% van de vijftigplussers. Hoogopgeleide burgers geven met 27% vaker een onvoldoende voor de belangrijkheid van samenwerking binnen de oppervlaktewatersector dan laag- en middenopgeleiden. Bij alle professionele doelgroepen zien de jongere medewerkers minder vaak het belang in dan oudere medewerkers. Bij de gemeenten geven hoogopgeleide medewerkers (20%) het belang vaker een onvoldoende dan middenopgeleide medewerkers (11%).

3.3.4.7 De bekendheid met samenwerkingsverbanden in het teken van digitale veiligheid is (zeer) beperkt

Het gros van de ondervraagden (88%) kan in het geheel geen samenwerkingsverband van organisaties noemen die werken aan digitale veiligheid. Voor burgers is dit meer dan bij ambtenaren met 92%. Slechts 3% noemt de overheid en 2% het Nationaal Cyber Security Centrum (onder gemeentemedewerkers is dit 4%). Het interbancair overleg wordt door 1% van de Rijksambtenaren genoemd en het VNG door 1% van de gemeentemedewerkers.

4. Resultaten verdiepende analyse

Inleiding

Het onderzoek naar de cyber security awareness van vijf doelgroepen is een omvangrijk onderzoek dat bestaat uit een groot aantal vragen, die de kennis, houding en het gedrag van de doelgroepen rondom digitale veiligheid in kaart brengen. Naast het weergeven van de resultaten van alle vragen, kan het voor de lezer inzichtelijk zijn als deze veelheid van data geaggregeerd zou kunnen worden tot een aantal kernelementen oftewel “factoren”. Met behulp van verdiepende analyse zijn we nagegaan of en zo ja welke onderliggende “factoren” er uit de data gedestilleerd kunnen worden.

In dit hoofdstuk geven we de resultaten van deze analyses beknopt weer. Voor een goed begrip van de resultaten, gaan we daarbij eerst kort in op de opzet van de analyse en vervolgens op het uiteindelijke resultaat ervan.

4.1 Opzet databewerking en analyse

Samengevat bestaat de analyse bestaat uit de volgende stappen:

- *Variabelen in dezelfde richting brengen.* Om respondenten scherp te houden en een antwoordcadans te voorkomen, zijn diverse items “omgekeerd” gesteld, wat betekent dat als men het ermee eens is, dit bijvoorbeeld blijk geeft van ongewenst gedrag. Voor een eenduidige interpretatie van de analyses, is het van belang dat alle variabelen in dezelfde richting staan, dat wil zeggen: een lage score getuigt van een lage cyber security awareness, een hoge score van een hoge cyber security awareness qua kennis, houding of gedrag. Om dit te bewerkstellingen hebben we een aantal stellingen omgepoold/hergecodeerd.

- *Standaardiseren van variabelen.* Dit is noodzakelijk omdat de originele variabelen niet allemaal op dezelfde manier gemeten zijn. Om de variabelen onderling goed met elkaar te kunnen vergelijken en voor dezelfde analyses te kunnen benutten, hebben we ze omgerekend naar een schaal van 0 tot 10. De kennis, houding of het gedrag van de respondent wordt dus uitgedrukt in een schaalscore tussen de 0 en 10. Hoe hoger de score, hoe beter de cyber security awareness voor de betreffende vraag. Dit kan bij verschillende vragen dus verschillende zaken betekenen: bij een kennisvraag betekent een hoge schaalscore dat de respondent een hoog kennisniveau heeft wat betreft digitale veiligheid. Bij een gedragsvraag betekent een hoge schaalscore dat de cyber security awareness van de respondent zich vertaalt naar het vertonen van het gewenste, veilige gedrag.

- *Ontwikkelen van sterke, betekenisvolle schalen.* Om de data verder te aggregeren, hebben we de volgende stappen genomen:
    - *Factoranalyse* op vragen die bestaan uit meerdere items (bijvoorbeeld stellingen, aspecten) om na te gaan of items één of meerdere factoren meten.

- *Betrouwbaarheidsanalyse* op de items die samen één factor vormen om na te gaan op basis van welke items we de meest betrouwbare, robuuste schalen kunnen maken. Daartoe is telkens gekeken naar: de betrouwbaarheid van de totale schaal (met behulp van Cronbach's Alpha) en vervolgens naar de bijdrage van de individuele items aan de schaal. Items die de schaalbetrouwbaarheid naar beneden halen, zijn niet opgenomen in de schaal. Hiernaast is voor de items van vraag D9 op inhoudelijke gronden besloten om de items aan "factoren" toe te wijzen, omdat de factoranalyse slecht interpreteerbare factoren opleverde.
- *Berekenen gemiddelde schaalscores.* Voor de geconstrueerde "optimale" schalen hebben we vervolgens voor elke respondent de gemiddelde score op de schaal gemeten en deze opgenomen in een nieuwe variabele. Deze score is een getal tussen de 1 en de 10. Een voorwaarde bij factoranalyse is dat alle respondenten die in deze analyse bestrokken worden een waarde (antwoord) op de betreffende vragen hebben. Vanwege selecties in de vragenlijst is dit niet altijd voor iedereen bij elke vraag het geval. Als oplossing hiervoor is het gemiddelde als waarde ingevuld in geval van missende waarden. In totaal zijn op deze manier 29 variabelen geconstrueerd.

- *Nagaan of er onderliggende factoren zijn.* Via een factoranalyse op de nieuwe variabelen (met voor elke respondent een gemiddelde schaalscore) zijn we nagegaan of er in de data onderliggende componenten/factoren aanwezig zijn. In totaal kwamen er 7 factoren uit deze analyse naar voren.

- *Interpreteren en aanscherpen resultaten factoranalyse.* Om na te gaan in hoeverre de gevonden factoren betekenisvol zijn, hebben we:
  - Berekend op hoeveel factoren elke respondent hoog scoort en dit afgezet tegen alle nieuwe variabelen. Zo konden we zien in hoeverre een hoge score op meerdere factoren samenvalt met een hoge score op de variabele.
  - Variabelen die hierin niet of nauwelijks variatie lieten zien uit de analyse gehaald. In totaal zijn er 9 variabelen verwijderd.
  - Opnieuw factoranalyse uitgevoerd op de resterende variabelen en vervolgens de gemiddelde factorscore per respondent berekend. Dit resulteert in 6 factoren.

- *Indelen van de factorscores naar een ordinale schaal.* Uit praktische overwegingen hebben we de factorscores omgezet naar een ordinale schaal met 3 categorieën: laag, midden en hoog.

- *Berekenen van de score op het totaal van factoren.* Om inzicht te krijgen in hoeverre er bepaalde groepen zijn die cyber bewust zijn op meerdere gebieden, hebben we voor elke respondent het aantal keren berekend dat deze hoog, midden of hoog, of laag scoort over de zes factoren.

4.2 Belangrijkste resultaten analyses

4.2.1 Er zijn zes factoren die ten grondslag liggen aan de cyber security awareness en die tezamen 54% van de variantie verklaren

Uiteindelijk zijn er zes duidelijk benoembare, betrouwbare factoren uit de data gedestilleerd, die ten grondslag liggen aan de cyber security awareness. Uiteindelijk blijkt een groot deel van de informatie uit de vragen over kennis, houding en gedrag samen te vatten in zes factoren, die samen 53,8% van de variantie verklaren.

Onderstaande tabel geeft een overzicht van de zes factoren, de bijbehorende variabelen en items. Tevens hebben we de zogeheten componentladingen vermeld; deze geven aan hoe sterk de variabele samenhangt met de component (= de achterliggende factor/concept). Hoe hoger de componentlading, des te groter de samenhang van de vraag met de component.

Tabel 4.1 Overzicht factoren en componentladingen

Factor		Variabele	Items	Factor 1	2	3	4	5	6
1	Cyber security bewustzijn op het werk	kennis&gedrag c7	1,2,3,4,5,6	,796					
		beleid&gedrag c5	alles	,792					
		houding c7	7,8	,744					
		kennis c1	alles	,709					
		gedrag c3	alles	,544					
2	Gedrag: bewust omgaan met wachtwoorden	gedrag e1	alles		,660				
		gedrag e5	alles behalve 7		,634				
		risico-inschatting e2	alles		,601				
		gedrag e4	alles behalve 7		,575				
3	Risicoperceptie/inschatting digitale veiligheid	risico-inschatting b2	1,2,3			,644			
		risico-inschatting b2	4			,643			
		houding b3a	1,6,7,8,10,11,13			,575			
4	Gedrag: bewust omgaan met e-mail, bestanden, gegevensdragers	gedrag d9	10,15,18,19,20				,841		
		gedrag d9	4,14,16,17,18				,800		
5	Gedrag: bewust omgaan met websites en beveiliging apparaat	gedrag d9	1,2,3,5,6,7,8,9					,746	
		gedrag d9	11,12,13					,633	
6	Locus of control, ervaring, netwerkbeveiliging	gedrag d7	alles behalve 8						,687
		houding b3a	2,12,15						-,523
		ervaring b5	B5, alles			-,420			,496

De factoren geven inhoudelijk het volgende weer:

- **Factor 1** gaat over het cyber security bewustzijn op het werk en heeft betrekking op alle doelgroepen, behalve burgers. Het omvat hoe de organisatie omgaat met cyber security, en de kennis, houding en gedrag van de respondent in de rol van werknemer ten aanzien van cyber security op het werk.
- **Factor 2** heeft betrekking op het bewust omgaan met wachtwoorden. Deze factor behelst de eigen inschatting van de veiligheid van de wachtwoorden die men gebruikt en de manier waarop men omgaat met wachtwoorden wat betreft de eigenschappen van de wachtwoorden, het variëren en het vernieuwen van wachtwoorden.
- **Factor 3** gaat over de inschatting van de eigen digitale veiligheid op werkgebied en in de privésituatie, evenals de algemene grondhouding ten aanzien van de risico's van internet voor de respondent zelf.

- **Factor 4** omvat de wijze waarop men omgaat met e-mail (het versturen van vertrouwelijke informatie, het klikken op links in e-mail et cetera), het openen of verzenden van bestanden en gegevensdragers zoals usb-sticks.
- **Factor 5** behelst de alertheid op de betrouwbaarheid van websites en de mate waarin men zijn of haar apparaten beveiligt (via antivirus en anti-spywaresoftware, een personal firewall, het laten uitvoeren van automatische updates).
- **Factor 6** heeft betrekking op de algemene houding ten aanzien van de zinvolheid van beveiliging/perceptie van de eigen weerbaarheid ("locus of control"), de eigen ervaring met cybercrime thuis of op het werk en de sterkte van de beveiliging van het draadloos netwerk thuis (indien men over zo'n netwerk beschikt). Tussen de algemene houding versus de eigen ervaring en de netwerkbeveiliging is bestaat een negatief verband: naarmate men meer ervaring met cyber criminaliteit heeft en minder van mening is dat je je als individu niet toch niet kunt weren tegen cyber criminaliteit, hoe beter de beveiliging van het draadloos netwerk thuis.

Als we kijken naar de samenstelling van de factoren, dan zien we het volgende:
- Kennis en houding of kennis en gedrag gaan vaak samen in één factor. Dit betekent dat deze twee constructen met elkaar samenhangen.
- De zesde factor is het minst goed benoembaar/eenduidig te interpreteren, dit zien we over het algemeen vaker bij de laatste "restfactor".

4.2.2 De groepen Rijksoverheid, Vitale sectoren en bedrijfsleven scoren vaker op meerdere factoren hoog dan Gemeenten en Burgers

Om inzicht te krijgen in hoeverre er groepen bestaan die "breed" cyber security aware zijn, hebben we gekeken welke respondenten op meerdere factoren een hoge score laten zien. Daartoe zijn de zes factorscores ingedeeld in drie even grote groepen: laag (1/3), midden (1/3) en hoog (1/3). Hoe groter het aantal factoren waarop men hoog scoort, hoe breder men zich bewust is van digitale veiligheid.

Tabel 4.2 Cyber security awareness, aantal keren hoge score op factoren

Aantal keren hoog	Totaal	Rijksoverheid	Gemeenten	Vitale sectoren	Bedrijfsleven	Burgers 13+
0	7,6%	5,5%	11,7%	5,0%	7,9%	7,8%
1	27,9%	18,1%	35,6%	22,9%	21,8%	32,5%
2	34,3%	33,3%	33,9%	30,5%	30,0%	37,6%
3	20,5%	26,1%	15,1%	26,7%	25,0%	16,7%
4	8,0%	14,2%	3,2%	11,1%	12,1%	5,2%
5	1,5%	2,7%	,5%	3,4%	3,0%	,2%
6	,1%	,2%	0,0%	,4%	,2%	0,0%
Totaal	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Zoals tabel 4.2.2 laat zien, scoort de meerderheid (ongeveer de helft van de respondenten) op twee factoren hoog en een vijfde tot een kwart scoort op drie factoren hoog. Iets minder dan een op de tien respondenten laat een hoge score zien op vier factoren.

Een hoge score op veel (5 of meer) factoren komt niet of nauwelijks voor. Ook relatief weinig, maar wel vaker (in 5 tot 12% van de gevallen), zien we dat respondenten op geen enkele factor hoog scoren.

Verschillen tussen groepen
Ambtenaren van de Rijksoverheid en werknemers van vitale sectoren en het bedrijfsleven hebben vaker een hoge score op drie, vier of vijf van de in totaal zes factoren van cyber security awareness dan gemeenteambtenaren en burgers. Dit duidt op een minder breed aanwezig cyber security bewustzijn bij gemeenten en burgers. Ook de bevinding dat gemeenteambtenaren vaker op geen enkele factor hoog scoren of op één factor hoog scoren en dat burgers vaker een of twee keer hoog scoren, wijst in die richting.

4.2.3 Op vijf van de zes factoren hebben gemeenteambtenaren minder vaak een hoge score dan de andere doelgroepen

In deze paragraaf kijken we per factor naar de verdeling van de scores hierop bij de diverse doelgroepen. Dit geeft een overkoepelend beeld van hoe het gesteld is met de cyber security awareness van de doelgroepen op het betreffende gebied.

Tabel 4.3 Percentage hoge scores factor 1 Cyber security bewustzijn op het werk, uitgesplitst naar de vier onderzoeksdoelgroepen

Score	Totaal	Rijksoverheid	Gemeenten	Vitale sectoren	Bedrijfsleven
Laag	33,5%	32,6%	62,4%	37,6%	43,2%
Midden	33,5%	11,7%	12,3%	9,0%	10,2%
Hoog	32,9%	55,8%	25,3%	53,4%	46,5%
Totaal	100,0%	100,0%	100,0%	100,0%	100,0%

Het cyber security bewustzijn op het werk loopt uiteen tussen de vier zakelijke doelgroepen en is het laagst bij gemeenteambtenaren:

- Rijksambtenaren, medewerkers van de vitale sectoren en medewerkers van het algemene bedrijfsleven hebben vaker een hoge score dan gemeenteambtenaren.
- Gemeenteambtenaren hebben vaker een lage score dan de andere drie zakelijke doelgroepen.

Tabel 4.4 Percentage hoge scores factor 2 Bewust omgaan met wachtwoorden, uitgesplitst naar de vijf onderzoeksdoelgroepen

Score	Totaal	Rijksoverheid	Gemeenten	Vitale sectoren	Bedrijfsleven	Burgers 13+
Laag	32,9%	32,5%	29,5%	36,3%	32,2%	33,4%
Midden	33,6%	36,8%	34,3%	31,5%	31,6%	33,5%
Hoog	33,5%	30,7%	36,2%	32,3%	36,1%	33,2%
Totaal	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

In de wijze waarop de diverse doelgroepen omgaan met hun wachtwoorden zijn geen verschillen te zien tussen de vijf doelgroepen. Bij alle groepen zien we dat ongeveer een derde hier op een onveilige wijze mee omgaat (lage score), een derde hier op een gemiddelde wijze mee omgaat wat betreft de veiligheid (niet slecht, maar kan beter) en evenzo een derde hier op een veilige manier meer omgaat (hoge score).

Tabel 4.5 Percentage hoge scores factor 3 Risicoperceptie/inschatting digitale veiligheid, uitgesplitst naar de vijf onderzoeksdoelgroepen

Score	Totaal	Rijksoverheid	Gemeenten	Vitale sectoren	Bedrijfsleven	Burgers 13+
Laag	33,1%	30,3%	45,8%	29,2%	34,7%	30,1%
Midden	33,7%	33,0%	32,3%	32,8%	30,5%	35,8%
Hoog	33,2%	36,8%	21,9%	38,0%	34,8%	34,1%
Totaal	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

De inschatting van de digitale veiligheid op het werk en privé en de algemene basishouding rondom risico's van internet loopt uiteen tussen gemeenten versus de andere vier doelgroepen en is (wederom) het laagst bij gemeenteambtenaren:

- Rijksambtenaren, medewerkers van de vitale sectoren, medewerkers van het algemene bedrijfsleven en burgers hebben vaker een hoge score dan gemeenteambtenaren.
- Gemeenteambtenaren hebben vaker een lage score dan de andere vier doelgroepen. Zij zijn zich dus minder bewust van de gevaren van internet en de risico's die dit voor hen zelf met zich mee kan brengen.

Tabel 4.6. Percentage hoge scores factor 4 Bewust omgaan met e-mail, bestanden en gegevensdragers, uitgesplitst naar de vijf onderzoeksdoelgroepen

Score	Totaal	Rijksoverheid	Gemeenten	Vitale sectoren	Bedrijfsleven	Burgers 13+
Laag	33,0%	27,8%	18,7%	33,0%	37,8%	39,8%
Midden	33,1%	30,7%	63,3%	30,3%	29,7%	23,5%
Hoog	33,9%	41,6%	18,0%	36,6%	32,4%	36,7%
Totaal	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

De cyber security awareness vertaald in de manier waarop men omgaat met e-mail, bestanden en gegevensdragers zoals usb-sticks verschilt tussen de doelgroepen:

- Gemeenteambtenaren scoren vaker in het midden en hebben minder vaak een lage of hoge score dan de andere vier doelgroepen.
- Medewerkers van de Rijksoverheid en van de Vitale sectoren scoren vaker in het midden dan burgers.
- Medewerkers van het bedrijfsleven en burgers hebben vaker een lage score dan Rijksambtenaren.

Tabel 4.7 Percentage hoge scores factor 5 Bewust omgaan met websites en beveiliging apparaten, uitgesplitst naar de vijf onderzoeksdoelgroepen

Score	Totaal	Rijksoverheid	Gemeenten	Vitale sectoren	Bedrijfsleven	Burgers 13+
Laag	35,1%	35,5%	22,1%	37,6%	33,8%	39,7%
Midden	33,6%	31,6%	53,3%	33,6%	30,4%	27,2%
Hoog	31,3%	32,9%	24,6%	28,8%	35,9%	33,1%
Totaal	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

De wijze waarop men omgaat met websites en de beveiliging van zijn of haar apparaten verschilt tussen de doelgroepen:

- Gemeenteambtenaren scoren vaker in het midden en hebben minder vaak een lage of hoge score dan de andere vier doelgroepen en vice versa

Tabel 4.8 Percentage hoge scores factor 6 Locus of control, ervaring met cybercrime, netwerkbeveiliging, uitgesplitst naar de vijf onderzoeksdoelgroepen

Score	Totaal	Rijksoverheid	Gemeenten	Vitale sectoren	Bedrijfsleven	Burgers 13+
Laag	33,0%	28,8%	26,2%	30,7%	27,9%	40,0%
Midden	33,3%	34,6%	35,8%	30,5%	36,6%	31,9%
Hoog	33,7%	36,6%	38,0%	38,7%	35,5%	28,1%
Totaal	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Kijken we naar de cyber security in de zin van de eigen ervaring, het gevoel van weerbaarheid/eigen invloed en de sterkte van de netwerkbeveiliging thuis, dan zien we dat:

- Burgers hier vaker laag op scoren dan de vier zakelijke doelgroepen.
- De zakelijke doelgroepen laten vaker een hoge score zien dan burgers.

BIJLAGE 1
Responsoverzicht
kwantitatief onderzoek

Onderzoeksverantwoording kwantitatief onderzoek

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

Totaal

De respons voor de totale steekproef is 50%.

Bruto steekproef Totaal		**8949**
Vers sample / niet gereageerd		**4391**
Non-respons		**1317**
Groep vol / quotafail	183	
Niet volledig ingevulde vragenlijsten	213	
Voldoet niet aan criteria/screeningseisen	921	
Complete vragenlijsten		**3241**

Rijksoverheid

De respons voor deze doelgroep is 50%.

Bruto steekproef		**1140**
Vers sample / niet gereageerd		**561**
Non-respons		**56**
Groep vol / quotafail	26	
Niet volledig ingevulde vragenlijsten	30	
Voldoet niet aan criteria/screeningseisen	0	
Complete vragenlijsten		**523**

Gemeenten

De respons voor deze doelgroep is 26%.

Bruto steekproef		**3060**
Vers sample / niet gereageerd		**2257**
Non-respons		**265**
Groep vol / quotafail	0	
Niet volledig ingevulde vragenlijsten	265	
Voldoet niet aan criteria/screeningseisen	0	
Complete vragenlijsten		**538**

Vitale sectoren

De respons voor deze doelgroep is 40%.

Bruto steekproef		**1418**
Vers sample / niet gereageerd		**845**
Non-respons		**49**
Groep vol / quotafail	0	
Niet volledig ingevulde vragenlijsten	49	
Voldoet niet aan criteria/screeningseisen	0	
Complete vragenlijsten		**524**

Bedrijfsleven

De respons voor deze doelgroep is 71%.

Bruto steekproef		**612**
Vers sample / niet gereageerd		**155**
Non-respons		**86**
Groep vol / quotafail	70	
Niet volledig ingevulde vragenlijsten	16	
Voldoet niet aan criteria/screeningseisen	0	
Complete vragenlijsten		**371**

Burgers 13+

De respons voor deze doelgroep is 64%.

Bruto steekproef		**2181**
Vers sample / niet gereageerd		**748**
Non-respons		**148**
Groep vol / quotafail	87	
Niet volledig ingevulde vragenlijsten	60	
Voldoet niet aan criteria/screeningseisen	1	
Complete vragenlijsten		**1285**

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

Doelgroepen	Kenmerken waarop de steekproef is gestratificeerd	Kenmerken waarop de steekproef is gewogen
Rijksoverheid	Leeftijd, geslacht, leidinggevendheid	Leeftijd, geslacht
Gemeenten	Geen (dit was niet mogelijk binnen het Flitspanel)	Leeftijd, geslacht
Bedrijfsleven overig	Leeftijd, geslacht, bedrijfsgrootte, branche, leidinggevendheid	bedrijfsgrootte
Bedrijfsleven vitale sectoren	Leeftijd, geslacht, branche, leidinggevendheid	geen
Burgers 13+	Leeftijd, geslacht, opleiding, werkzaamheid, regio, internetgebruik	Leeftijd, geslacht, opleiding, werkzaamheid, regio, internetgebruik

BIJLAGE 2:

Vragenlijst

32876 Cyber security 2013
Online vragenlijst

QUOTA:

Total net n = **1283 + 550 for the target group "gemeenten"**

S. Selection questions

<display text>

Om te bepalen of u tot de doelgroep van dit onderzoek behoort, volgt nu eerst een aantal selectievragen.

S1.(0.0) Welke van de volgende omschrijvingen past bij uw persoonlijke situatie? (S)

1. Ik ben schoolgaand/studerend *(indien Flitspanel > einde vragenlijst)*
2. Ikben werkloos/werkzoekend/werkzaam in een niet-betaalde baan/niet werkzaam/gepensioneerd *(indien Flitspanel > einde vragenlijst)*
3. Ik werk in een betaalde baan bij een organisatie met meer dan 10 medewerkers (met een vaste aanstelling)
4. Ik werk in een betaalde baan bij een organisatie met minder dan 10 medewerkers
5. Ik ben een zelfstandige zonder personeel (ZZP'er) *(indien Flitspanel > einde vragenlijst)*

Selection: S1 = 3, 4 or 5

S2. In welke sector bent u werkzaam? (S)

1. Landbouw, bosbouw en visserij
2. Delfstoffenwinning
3. Industrie
4. Energievoorziening
5. Waterbedrijven en afvalbeheer
6. Bouwnijverheid
7. Handel
8. Vervoer en opslag
9. Horeca
10. Informatie en communicatie
11. Financiële dienstverlening
12. Verhuur en handel van onroerend goed
13. Specialistische zakelijke diensten
14. Verhuur en overige zakelijke diensten
15. Openbaar bestuur en overheidsdiensten
16. Onderwijs
17. Gezondheids- en welzijnszorg
18. Cultuur, sport en recreatie
19. Overige dienstverlening
20. Huishoudens
21. Extraterritoriale organisaties
22. Anders, namelijk…(O)

Selection: S2 = 15

S2a. Waar bent u werkzaam? (S)

1. Rijksoverheid
2. Provincie
3. Gemeente → *<if a irpd respondent chooses this category: end of questionnaire. Only respondents from the MWM2 "flitspanel" can take part in this questionnaire>*
4. Overige overheid/overig openbaar bestuur

Selection: S2 = 8

S2b. U geeft aan dat u werkzaam bent in de sector 'vervoer en opslag'.
Bent u werkzaam binnen de transportsector? (S)

1. Ja
2. Nee

Selection: S2 = 5

S2c. Op welk gebied bent u werkzaam? (S)

1. Drinkwater
2. Keren en beheren oppervlaktewater
3. Geen van bovenstaande

Selection: S2 = 10, 13, 14 or 22

S2d. Bent u werkzaam binnen de telecommunicatie? (S)

1. Ja
2. Nee

<Scripter: if S2 = 4, S2 = 11, S2a = 1 or 3, S2b = 1, S2c = 1 or 2, S2d = 1, the respondent cannot be appointed to quota group "Bedrijfsleven overig">

Selection: S1 = 3 or 4

S3a. (0.1) Welke van de volgende omschrijvingen past bij uw werksituatie? (S)

1. Ik geef leiding aan een groep medewerkers vanuit een formele rol
2. Ik werk als medewerker en geef zelf geen leiding

Selection: S1 = 3 or 4

S3b. (0.2) Heeft uw werkgever u een computer (pc, laptop, tablet en/of smartphone) ter beschikking gesteld voor het uitvoeren van uw werkzaamheden?

1. Ja
2. Nee *(Indien Flitspanel of S1 =3 end of questionnaire)*

Selection: S3b = 1

S3c. (0.3) Welke van onderstaande apparaten heeft uw werkgever aan u ter beschikking gesteld (thuis of op kantoor) voor werkgerelateerde doeleinden? Er zijn meerdere antwoorden mogelijk. (M)

1. Pc
2. Laptop
3. Tablet
4. Smartphone
5. Geen van deze (S)

Selection: S3c = 1,2,3 or 4

S3d. (0.4) Welke van deze apparaten, door uw werkgever aan u ter beschikking gesteld, gebruikt u tevens voor privézaken? (M)

<Show answer(s) S3c 1 – 4>

1. Pc
2. Laptop
3. Tablet
4. Smartphone
5. Ik gebruik deze apparaten niet voor privézaken [S]

Selection: S3d = 2,3 or 4

S3e. (0.5) Heeft u van uw werkgever instructies ontvangen voor het veilig gebruik van uw laptop, tablet of smartphone? (S)

1. Ja
2. Nee
3. Weet niet

ALL

S4a. (0.6) Heeft u thuis de beschikking over een computer (pc, laptop, tablet, smartphone)? (M)

1. Ja, een pc (niet van mijn werk)
2. Ja, een laptop (niet van mijn werk)
3. Ja, een tablet (niet van mijn werk)
4. Ja, een smartphone (niet van mijn werk)
5. Ja, een computer (pc, laptop, tablet, smartphone) van mijn werk
6. Nee *<if respondent is an IRPD member and does not belong to the target group 2 'bedrijfsleven vitale sectoren' or 3 'bedrijfsleven overig' (S1 = 1, 2, 4 or 5 OR S3b =2) > exit questionnaire)*

ALL

S4b. (0.7) Heeft u thuis beschikking over een internetverbinding? (S)

1. Ja
2. Nee *<if respondent is an IRPD member and does not belong to the target group 2 'bedrijfsleven vitale sectoren' or 3 'bedrijfsleven overig' (S1 = 1, 2, 4 or 5 OR S3b =2) > exit questionnaire)*

ALL

S5a. (0.8) Maken er weleens anderen gebruik van deze computer(s) die u thuis ter beschikking heeft? (S)

<show as a grid question>

Answers in column
1. Ja, zij gebruiken hiervoor hetzelfde account om in te loggen als ik
2. Ja, zij gebruiken hiervoor een ander account om in te loggen dan ik
3. Nee, ik ben de enige die dit apparaat gebruikt

Answers in row
<show answer(s) S4a = 1,2,3,4. If S4a=5, also show answers 1 through 4 of S3c that are not mentioned in S4a >

a. Pc
b. Laptop
c. Tablet
d. Smartphone

Selection: S5a = 1 or 2 (for pc, laptop, tablet or smartphone)

S5b. Wie maken er dan weleens gebruik van deze computer (pc, laptop, tablet, smartphone)?
(M)

1. Mijn partner
2. Mijn kind(eren)
3. Vriendjes van mijn kind(eren)
4. Familieleden
5. Vrienden/bekenden
6. Collega's

ALL

S5c. (0.9) Kunt u aangeven voor welke doeleinden u deze apparaten gebruikt? (S)

Answers in column
1. Alleen voor privédoeleinden
2. Alleen voor zakelijke doeleinden
3. Voor zowel privé als zakelijke doeleinden
4. Ik gebruik dit apparaat niet

Answers in row
<show answer(s) S4a = 1,2,3,4. If S4a= 5, also show answers 1 through 4 of S3c that are not mentioned in S4a>

a. Pc
b. Laptop
c. Tablet
d. Smartphone

<define the appointment to target groups on the basis of the previous selection questions, conform the quota description at the beginning of this document.

<if respondent belongs to target group “consumenten” AND S5c a,b,c, and d are all 4 > exit questionnaire>

<if the respondent belongs to both the target group “consumenten” as well as the target group “bedrijfsleven overig”:

- please appoint the respondent to the target group for which the relatively the most net respons is needed at that moment>
- depending on the target group to which the respondent is appointed, show the following text at the beginning of the questionnaire:
  <if target group = “consumenten”:> Wilt u deze vragenlijst invullen als consument en niet zozeer als werknemer.
  <if target group = “bedrijfsleven overig”:> Wilt u deze vragenlijst invullen als werknemer en niet zozeer als consument.

ALL

S5d Kunt u aangeven wie verantwoordelijk is voor (eventuele) beveiliging van deze apparaten? (S)

Answers in column

1. Niemand, het apparaat is niet beveiligd
2. Ikzelf
3. Mijn partner
4. Mijn kind(eren)
5. Familie of vrienden
6. Een professioneel bedrijf

Answers in row
<show answer(s) S4a = 1,2,3,4 If S4a=5, also show answers 1 through 4 of S3c that are not mentioned in S4a >

a. Pc
b. Laptop
c. Tablet
d. Smartphone

Basisvragenlijst

ALL

<DISPLAY TEXT>

Bedankt voor het beantwoorden van enkele vragen over uw computergebruik.
Welkom bij het hoofddeel van het onderzoek naar *cyber security*. Met dit onderzoek willen we in kaart brengen hoe Nederlanders op het werk en in hun privésituatie aankijken tegen veilig omgaan met hun digitale omgeving. Meewerken gebeurt zoals altijd <if s_bron = 2: bij Intomart GfK> op anonieme basis.
<only display the following text to the target groups Rijksoverheid", "Gemeenten", "Bedrijfsleven vitale sectoren", "Bedrijfsleven overig":>Waar we in de vragenlijst spreken over "organisatie" bedoelen we: de organisatie, overheidsinstantie of het bedrijf waar u werkzaam bent.

SELECTION: target groups "Rijksoverheid", "Gemeenten", "Bedrijfsleven vitale sectoren", "Bedrijfsleven overig"

A. Computergebruik werk

<display text>

De volgende vragen gaan over het gebruik van computers in uw werksituatie

A1 (1.1). Hoeveel uur per week maakt u gemiddeld gebruik van uw computer (pc, laptop, tablet en/of smartphone) voor het uitvoeren van uw betaalde werkzaamheden? (S)

1. Minder dan 1 uur per week
2. 1 tot en met 5 uur per week
3. 6 tot en met 10 uur per week
4. 11 tot en met 20 uur per week
5. 21 uur en meer per week

SELECTION: target groups "Rijksoverheid", "Gemeenten", "Bedrijfsleven vitale sectoren", "Bedrijfsleven overig"

A2 (1.2) Waarvoor gebruikt u de computer (pc, laptop, tablet en/of smartphone) die u voor uw werk ter beschikking is gesteld? (M) *<randomize>*

1. Tekstverwerking, rekenen en tekenen (offline software)
2. Tekstverwerking, rekenen en tekenen online in een zogenaamde cloud (Google Drive, iCloud e.d.)
3. Online bankieren
4. Online aankoop artikelen
5. Online verkoop artikelen
6. E-mailen
7. Chatten
8. Skype
9. Surfen op het internet om informatie te zoeken
10. Surfen op het internet voor vermaak
11. Downloaden van software, muziek, films e.d
12. Online gamen
13. Gebruik van netwerksites zoals Facebook, Hyves, LinkedIn
14. Anders, namelijk…(O)

B. Inschatting eigen mate van cyber security

ALL

B1 (2.1). Als we het hebben over cyber security oftewel een veilige digitale omgeving, waar denkt u dan aan? (O)

1. (O)
2. Weet niet/geen antwoord

ALL

B2 (2.2) Op een schaal van 1 tot 10, hoe hoog schat u de digitale veiligheid in: (O)
(Hierbij staat 1 voor heel laag en een 10 voor heel hoog)

Answers in column:

1. <1 – 10>
2. Weet niet/niet van toepassing (S)

Answers in row:

a. van de organisatie waar u werkt *<do not show to target group "consumers" who haven't got a company computer at home S3b = 2>*
b. van de medewerkers in de organisatie bij de uitvoering van hun werk *<do not show to target group "consumers" who haven't got a company computer at home S3b = 2>*
c. van uzelf, in de uitvoering van uw werk *<do not show to target group "consumers"who haven't got a company computer at home S3b = 2>*
d. van uzelf, in uw privésituatie *<only show if the person has a computer at home S4a = 1, 2, 3 of 4>*

ALL

B3a. Hieronder staat een aantal stellingen over het gebruik van internet. Kunt u aangeven in hoeverre u het (on)eens bent met de stellingen? (S)

Answers in column:

1. Zeer mee eens
2. Mee eens
3. Neutraal
4. Mee oneens
5. Zeer mee oneens
6. Weet niet

Answers in row, randomize:

a) Ik vertrouw er op dat internetbedrijven mijn gegevens niet zonder mijn toestemming aan derden verstrekken.
b) Van iedereen zijn nu eenmaal veel gegevens bekend op internet, dat heb je zelf niet echt in de hand.
c) Bij online aankopen betaal ik liever niet met een creditcard.
d) Ik begrijp de zorgen over online betalen met een creditcard niet, als het mis gaat krijg je je geld toch wel terug.
e) De privacy voorwaarden bij het verstrekken van gegevens op internet lees ik meestal niet of nauwelijks.
f) Ik ben niet huiverig voor internetbankieren.
g) Ik maak me meestal weinig zorgen over de risico's van internet.
h) Ik maak me zorgen om de bescherming van mijn privacy op internet.
i) Ik ben me voldoende bewust van de risico's van internet
j) Ik voel me voldoende beschermd tegen de risico's van internet.
k) Risico's van internet zijn vervelend, maar niet echt bedreigend voor mij.
l) Er komen telkens nieuwe risico's bij op internet, dat kun je toch niet bijbenen
m) Ik zie geen gevaar bij het online aankopen van producten bij grote merken of bekende sites.
n) Ik loop minder risico dan anderen op een nare ervaring met internet
o) Tegen grote gevaren op internet kun je je eigenlijk niet weren, kwaadwillenden slagen toch wel
p) Ik heb met mijn kind(eren) afspraken gemaakt over omgaan met digitale veiligheid tijdens het internetten <*only show if S5b = 2*>

ALL

B3b. In hoeverre maakt u zich zorgen over uw digitale veiligheid?

1. Veel zorgen
2. Enige zorgen
3. Geen zorgen

SELECTION: target groups: "Rijksoverheid", "Gemeenten", "Bedrijfsleven vitale sectoren", "Bedrijfsleven overig"

B3 (2.3) Op een schaal van 1 tot 10, hoe beoordeelt u de mate waarin de organisatie waarvoor u werkt aandacht heeft voor digitale veiligheid? (O)
(Hierbij staat een 1 voor heel laag en een 10 voor heel hoog)

1. <1 – 10
2. Weet niet/geen antwoord (S)

SELECTION: target groups: "Rijksoverheid", "Gemeenten", "Bedrijfsleven vitale sectoren", "Bedrijfsleven overig"

B4. (2.4) Kunt u aangeven welke werkzaamheden en handelingen op internet een risico kunnen vormen voor de digitale veiligheid van de organisatie waar u werkt? (O)

1. <OPEN>
2. Weet niet/geen antwoord

<*Not back*>

SELECTION: target groups all: “Rijksoverheid”, “Gemeenten”, “Bedrijfsleven vitale sectoren”, “Bedrijfsleven overig”, “Consumenten”

B5. (2.5) Heeft u op uw werk of thuis wel eens last gehad van: (S)

Answers in column, roulate
1. Computervirus verspreid via e-mail
2. Computervirus verspreid via het downloaden van geïnfecteerde software/bestanden
3. Computeruitval door een virus of malware
4. Identiteitsdiefstal / misbruik van uw persoonsgegevens
5. Ongeoorloofde afschrijving via telebankieren
6. Mails met phishing
7. Ongewenste e-mail (SPAM)
8. Mensen die gegevens opvragen door zich voor te doen als telefonische helpdesk

Answers in row
a. Ja , ikzelf
b. Nee, ik zelf niet maar wel een familielid/vriend/kennis/collega
c. Nee
d. Weet niet / geen antwoord

<show the following information balloon at 6 “mails met phishing”:>
Phishing is een verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan direct worden misbruikt voor het doen van bijvoorbeeld grote uitgaven (in het geval van creditcardnummers) of voor wat in het Engels 'identity theft' wordt genoemd, het stelen van een identiteit. In dit geval zijn bijvoorbeeld gegevens als sofi-nummers, adressen en geboortedata nodig.

<show the following information balloon at 3. “computeruitval door een virus of malware”:>
Malware is een verzamelnaam voor kwaadaardige en/of schadelijke software.

C. Wijze van vorm en inhoud geven aan cyber security op het werk

SELECTION: target groups: “Rijksoverheid”, “Gemeenten”, “Bedrijfsleven vitale sectoren”, “Bedrijfsleven overig”

C1. (3.7) In hoeverre weet u:

Answers in column
1. precies
2. globaal
3. niet of nauwelijks

Answers in row <randomize>

a. Welke informatie binnen uw organisatie gevoelig/vertrouwelijk is?
b. Wat u moet doen wanneer er een incident plaatsvindt die de digitale veiligheid in het gevaar brengt?
c. Waar u op moet letten wanneer u een e-mail ontvangt met daarin een link?
d. Welke websites u wel en niet mag bezoeken op uw zakelijke computer?
e. Wat de zwakke plekken zijn in de digitale veiligheid van uw organisatie?

SELECTION: target groups: "Rijksoverheid", "Gemeenten", "Bedrijfsleven vitale sectoren", "Bedrijfsleven overig"

C2. (3.5) Hoe vaak deelt u gevoelige bedrijfsinformatie via e-mail, de cloud of usb-stick?

Answers in column

1. Nooit
2. Soms
3. Regelmatig
4. Vaak

Answers in row

a. E-mail
b. De cloud
c. Usb-stick

<display information balloon at b. "De cloud':>
Informatie delen via de cloud: informatie via internet beschikbaar stellen, bijvoorbeeld via sites als WeTransfer.

SELECTION: target groups: "Rijksoverheid", "Gemeenten", "Bedrijfsleven vitale sectoren", "Bedrijfsleven overig"

C3. (3.8) Zijn de volgende stellingen op u van toepassing?

Answers in column

1. Wel van toepassing
2. Niet van toepassing

Answers in row <randomize>

a. Ik laat mijn zakelijke tablet en/of smartphone niet door anderen gebruiken *<only show if S3c = 3. "tablet" and/or 4. "smartphone">*
b. Ik laat mijn pc en/of laptop niet door anderen gebruiken *<only show if S3c = 1. "pc" and/or 2." Laptop">*
c. Wanneer ik gebruik maak van een openbare wifiverbinding (bijv. in de trein, een café, etc.), maak ik bewuste keuzes welke handelingen ik wel en welke ik niet verricht op mijn zakelijke computer (pc, laptop, tablet, smartphone)
d. Wanneer ik een openbare wifiverbinding heb gebruikt (bijv. in de trein, een café, etc.), wijzig ik daarna mijn wachtwoord(en)
e. Ik maak voor mijn werk gebruik van een VPN-verbinding of een andere beveiligde verbinding met bijvoorbeeld een authenticatietoken
f. Een usb-stick die buiten de organisatie is geweest, laat ik eerst door de systeembeheerder controleren op virussen
g. Ik laat wel eens een PC of laptop onbeheerd achter

SELECTION: target groups: “Rijksoverheid”, “Gemeenten”, “Bedrijfsleven vitale sectoren”, “Bedrijfsleven overig”

C4. (3.2) Zijn onderstaande zaken binnen uw organisatie vastgelegd in een beleid?

Answers in column
1. Ja
2. Nee
3. Weet niet/geen antwoord

Answers in row <randomize>
a. Beleid voor veilig wachtwoordgebruik
b. Beleid voor updaten antivirussoftware
c. Beleid voor internetgebruik: welk type websites wel/niet te bezoeken
d. Back-upbeleid
e. Beleid voor omgang met usb-sticks
f. Beleid voor omgang met pc’s, laptops, tablets en/of smartphones
g. Beleid voor melden van incidenten

SELECTION: target groups: “Rijksoverheid”, “Gemeenten”, “Bedrijfsleven vitale sectoren”, “Bedrijfsleven overig”

C5. (3.1) In hoeverre vindt u de volgende stellingen van toepassing op uw organisatie?

Answers in column
1. Niet van toepassing
2. Meer niet dan wel van toepassing
3. Meer wel dan niet van toepassing
4. Wel van toepassing
5. Weet niet/geen antwoord

Answers in row <randomize>
a. Onze organisatie heeft een beleid (protocol) voor alle werknemers met betrekking tot de digitale omgeving
b. De medewerkers weten hoe te handelen bij incidenten op het gebied van digitale veiligheid
c. Nieuwe medewerkers worden ingewerkt in de maatregelen rondom veilig digitaal werken
d. Bij ontslag en/of vertrek van medewerkers worden maatregelen uitgevoerd in het kader van digitale veiligheid
e. Het naleven van de regels rondom digitale veiligheid maakt binnen onze organisatie onderdeel uit van de functionerings-/beoordelingsgesprekken
f. Na een incident op het gebied van digitale veiligheid is het de gewoonte dat alle medewerkers hier direct een terugkoppeling over ontvangen
g. De leidinggevenden zien er op toe dat alle medewerkers op de hoogte zijn van het bestaan en de inhoud van het beleid met betrekking tot de digitale werkomgeving

SELECTION: target groups: "Rijksoverheid", "Gemeenten", "Bedrijfsleven vitale sectoren", "Bedrijfsleven overig" AND **S3a = 1**

C6. (3.3) In hoeverre vindt u de volgende stellingen van toepassing op de medewerkers in uw organisatie?

Answers in column
1. Niet van toepassing
2. Meer niet dan wel van toepassing
3. Meer wel dan niet van toepassing
4. Wel van toepassing
5. Weet niet/geen antwoord
6. Onze organisatie heeft geen beleid/protocol op dit gebied

Answers in row <randomize>
a. Medewerkers zijn goed op de hoogte van het organisatiebeleid over digitale veiligheid
b. Medewerkers zijn zich voldoende bewust van het belang van digitale veiligheid
c. Medewerkers zijn zich voldoende bewust van de mogelijke gevaren op het gebied van digitale veiligheid die zich binnen onze organisatie kunnen voordoen
d. Medewerkers ervaren de informatie over digitale veiligheid als helder en eenduidig
e. Medewerkers zijn op de hoogte van hun eigen verantwoordelijkheden rondom digitale veiligheid
f. Medewerkers houden zich strikt aan de afspraken rondom de uitvoering van de protocollen op het gebied van digitale veiligheid; zij volgen consequent de regels die hieraan verbonden zijn op
g. Medewerkers zijn niet op de hoogte van het beleid over digitale veiligheid
h. Medewerkers die op de hoogte zijn van het beleid over digitale veiligheid, passen niet alle veiligheidsprotocollen toe
i. Medewerkers weten waar zij terecht kunnen voor informatie over digitale veiligheid

SELECTION: target groups: "Rijksoverheid", "Gemeenten", "Bedrijfsleven vitale sectoren", "Bedrijfsleven overig"

C7. (3.4) In hoeverre vindt u de volgende stellingen van toepassing op uzelf in uw werksituatie?

Answers in column
1. Niet van toepassing
2. Meer niet dan wel van toepassing
3. Meer wel dan niet van toepassing
4. Wel van toepassing
5. Weet niet/geen antwoord
6. Onze organisatie heeft geen beleid/protocol op dit gebied

Answers in row <randomize>
a. Ik weet bij wie ik een incident op het gebied van digitale veiligheid dien te melden
b. Ik ben me voldoende bewust van het belang van digitale veiligheid
c. Ik ben me voldoende bewust van de mogelijke gevaren op het gebied van digitale veiligheid die zich binnen onze organisatie kunnen voordoen
d. Informatie over digitale veiligheid ervaar ik als helder en eenduidig

e. Ik ben voldoende op de hoogte van mijn eigen verantwoordelijkheden rondom digitale veiligheid
f. Ik houd me strikt aan de afspraken rondom de uitvoering van de protocollen op het gebied van digitale veiligheid; ik volg consequent de regels die hieraan verbonden zijn op
g. Ik maak collega's er (bijna) altijd op attent wanneer deze een bepaalde regel op het gebied van digitale veiligheid veronachtzamen
h. Ik stimuleer mijn collega's zich volgens de regels op het gebied van digitale veiligheid te gedragen
i. Ik ben niet goed op de hoogte van het beleid over digitale veiligheid

SELECTION: target groups: "Rijksoverheid", "Gemeenten", "Bedrijfsleven vitale sectoren", "Bedrijfsleven overig"

C8. (3.6) Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid op het gebied van internetgebruik voornamelijk moet liggen? Er zijn maximaal twee antwoorden mogelijk. (M)

TPM: max 2 answers

1. Werknemers
2. Het management van mijn organisatie
3. De IT-afdeling van mijn organisatie
4. Internet providers
5. Website-eigenaren
6. De overheid
7. Weet niet [S]

D. Kennis over cyber security

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4 Target groups: "gemeenten", "rijksoverheid", "bedrijfsleven vitale sectoren", "bedrijfsleven overig" with a private computer which is also used for work purposes S5c = 2 or 3.

<display text>

De volgende vragen gaan over uw privésituatie en het gebruik van uw privécomputer.

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4

D1. (4.2b) Hoeveel uur per week maakt u gemiddeld gebruik van uw computer(s) (pc, laptop, tablet en/of smartphone) in uw privétijd?

1. Minder dan 1 uur per week
2. 1 tot en met 5 uur per week
3. 6 tot en met 10 uur per week
4. 11 tot en met 20 uur per week
5. 21 uur en meer per week

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4

D2. (4.3) Welke van de onderstaande activiteiten onderneemt u op internet? (M)

<randomize, but always show category 13 as last one>

1. Tekstverwerking, rekenen en tekenen online in een zogenaamde cloud (Google Drive, iCloud e.d.)
2. Online bankieren
3. Online aankoop artikelen
4. Online verkoop artikelen
5. E-mailen
6. Chatten
7. Skype
8. Surfen op het internet om informatie te zoeken
9. Surfen op het internet voor vermaak
10. Downloaden van software, muziek, films e.d
11. Online gamen
12. Gebruik van netwerksites / social media, zoals twitter, facebook, LinkedIn
13. Anders, namelijk…(O)

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4

D3 (4.1) Op welke manieren kan er via internet misbruik gemaakt worden van uw computer? (O)

1. <O>
2. Weet niet/geen antwoord (S)

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4

D4. (4.2) Wat doet u zelf om uzelf te beschermen tegen dergelijk misbruik? (O)

1. <O>
2. Niets [S]
3. Weet niet/geen antwoord (S)

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4

D5. (4.4) Hoe groot denkt u dat de kans is dat tegen uw zin in het volgende op internet gebeurt: (S)

Answers in column

1. Zeer klein
2. Klein
3. Niet groot, niet klein
4. Groot
5. Zeer groot
6. Weet niet/geen antwoord

Answers in row, randomize

a. Er wordt zomaar geld van mijn rekening of creditcard gehaald
b. Er wordt iets gekocht uit mijn naam
c. Een product waarvoor ik betaald heb, wordt niet geleverd en de verkoper is niet meer te bereiken

d. Iemand doet alsof hij mij is
e. Persoonlijke gegevens (zoals vakantiefoto's, persoonlijke berichten of persoonsgegevens) die ik op internet heb gezet, worden zonder mijn toestemming door anderen gebruikt en verspreid
f. Bij het plaatsen van een foto of berichtje op social media worden automatisch locatiegegevens vermeld
g. Er wordt met anderen gedeeld waar ik mij op dat moment bevind
h. Onbekenden kunnen zien met wie ik bevriend ben

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4 AND D2 = 12

D6. (4.11) Welke van de volgende uitspraken met betrekking tot uw social media gebruik zijn op u van toepassing: (S)
Indien u meerdere typen social media gebruikt en een uitspraak is van toepassing voor minimaal één daarvan, antwoordt u dan 'van toepassing'.

Answers in column
1. Van toepassing
2. Niet van toepassing

Answers in row
a. Bij het aanmaken van een profiel op social media (twitter, facebook, LinkedIn) vul ik zoveel mogelijk persoonlijke informatie in
b. Ik heb op social media een privacyfilter ingesteld zodat ik zelf kan bepalen wie welke gegevens van mij kan zien
c. Wanneer ik op vakantie ga, vermeld ik dat op social media
d. Wanneer ik op reis ben, vermeld ik dat op social media
e. Iedereen kan mijn profiel op social media zien
f. Op de social media die ik gebruik, kan iedereen zien waar ik werk
g. Ik verwijder de GPS-informatie van foto's en/of andere documenten voordat ik die op social media plaats
h. Ik weet hoe ik de privacy-instellingen van mijn social-media-account kan aanpassen

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4 Target groups: "gemeenten", "rijksoverheid", "bedrijfsleven vitale sectoren", "bedrijfsleven overig" with a private computer which is also used for work purposes S5c = 2 or 3.

D7. (4.9) Welke beveiliging staat er thuis aan op uw wifi-netwerk (draadloos netwerk)? (S)

1. WPA
2. WPA2
3. WEP
4. Andere beveiliging
5. Ik heb beveiliging op mijn wifi-netwerk, maar ik weet niet welke
6. Ik weet niet of ik beveiliging op mijn wifi-netwerk heb
7. Ik heb geen beveiliging op mijn wifi-netwerk
8. Ik heb geen wifi-netwerk thuis

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4 Target groups: "gemeenten", "rijksoverheid", "bedrijfsleven vitale sectoren", "bedrijfsleven overig" with a private computer which is also used for work purposes S5c = 2 or 3.

D8. (4.8b) Weet u wat cookies zijn? (S)

1. Ja
2. Nee

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4
Target groups: "gemeenten", "rijksoverheid", "bedrijfsleven vitale sectoren", "bedrijfsleven overig" with a private computer which is also used for work purposes S5c = 2 or 3.

D9. (4.8) Kunt u voor het apparaat/de apparaten waar u thuis beschikking over heeft aangeven welke van de volgende uitspraken op u van toepassing zijn? (Multiple Grid)

Answers in column <only show the answers given at S4a = 1,2,3 and/or 4>

1. Pc
2. Laptop
3. Tablet
4. Smartphone
5. Geen van deze apparaten [S]

Rows <randomize>

a. Ik maak zo veel mogelijk gebruik van de mogelijkheden om automatische updates te laten installeren
b. Als ik op het apparaat een melding krijg dat er software-updates beschikbaar zijn, dan voer ik deze meestal niet uit
c. Ik controleer nooit bij de softwareleverancier of er updates beschikbaar zijn en installeer deze
d. Ik ga voorzichtig om met e-mails, websites of aanbieders die ik niet vertrouw of niet ken
e. Ik meld verdachte zaken op mijn apparaat bij een helpdesk
f. Op mijn apparaat is anti-virussoftware geactiveerd
g. Op mijn apparaat is geen anti-spywaresoftware geactiveerd
h. Op mijn apparaat is geen personal firewall geactiveerd
i. Ik zorg dat ik altijd beschik over de up-to-date versies van anti-virussoftware, anti-spywaresoftware en /of personal firewall
j. Ik open soms wel eens bestanden waarvan ik de zender niet ken
k. Voordat ik inlog of mij registreer op een andere website dan die van de bank, controleer ik altijd het certificaat van de website (https/ slotje)
l. Voordat ik inlog of mij registreer op een website van de bank, controleer ik altijd het certificaat van de website (https/ slotje)
m. Als ik inlog of mij registreer op een website waar ik mijn persoonsgegevens moet invullen (veilingsite, webwinkel, etc.) controleer ik meestal niet het certificaat van de website (https/ slotje)
n. Ik ga nooit in op ongevraagde verzoeken per e-mail om in te loggen op een website of om mijn gegevens te bevestigen
o. Uit nieuwsgierigheid kijk ik bij spam meestal wel even waar het over gaat
p. Ik vind e-mail voldoende veilig om vertrouwelijke informatie te versturen
q. Wanneer ik vertrouwelijke informatie in een e-mail meestuur als bijlage~~,~~ loop ik geen gevaar dat de inhoud door kwaadwillende bekeken wordt
r. Ik klik niet op links in e-mails, want die kunnen mij naar gevaarlijke websites sturen
s. Als ik een usb-stick als relatiegeschenk krijg, stop ik hem in het apparaat om te kijken wat er op staat.
t. Als ik ergens een verloren usb-stick vind, stop ik hem niet in het apparaat om te kijken wat er op staat.
u. Ik weet hoe ik cookies in mijn browser kan verwijderen

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4

D10. (4.5) Heeft u behoefte aan informatie over hoe u zich kunt beschermen tegen de risico's van internet? (S)

1. Ja
2. Nee
3. Weet ik niet / geen antwoord

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4 AND **D10 = 1.**

D11. (4.6) Van welke partijen wilt u informatie over hoe zich kunt beschermen tegen de risico's van internet? (M)

<Roulate, but always show category 6 as the last one>

1. Overheid
2. Softwareleveranciers
3. Internet providers
4. Consumentenorganisaties
5. Anders, namelijk…(O)

SELECTION: Target group: "consumenten" with a private computer S4a= 1,2,3 or 4

D12.(4.7) Bij wie vindt u dat de verantwoordelijkheid voor de veiligheid op het gebied van internetgebruik voornamelijk moet liggen? (M)

1. De gebruiker zelf
2. Internet providers
3. Website-eigenaren
4. De overheid
5. Weet niet [S]

ALL

E. Wachtwoord kennis en gedrag

ALL

E1. (5.2) Welke van onderstaande eigenschappen zijn van toepassing op de meeste van uw wachtwoorden?

Answers in column

1. Van toepassing
2. Niet van toepassing

Answers in row

a. Mijn wachtwoorden bestaan uit meer dan 10 karakters
b. Mijn wachtwoorden bevatten geen woorden die in het woordenboek voorkomen
c. Mijn wachtwoorden bevatten speciale tekens (anders dan letters uit het alfabet of cijfers)

ALL

<display text>

Sterke wachtwoorden bestaan uit minimaal 8 tekens, bevatten geen herkenbare woorden (of verschillende woorden achter elkaar), bevatten zowel hoofdletters als kleine letters, vreemde tekens en cijfers.

E2. (5.1) Hoe veilig ('sterk') denkt u dat (de meeste) wachtwoorden van u zijn? (Q)
Uiteenlopend van '1=zeer onveilig/zwak' - tot '10=zeer veilig/sterk'

<Range:> [cijfer 1 / 10]

ALL

E3. (5.3) Hoe zorgt u ervoor dat u uw wachtwoorden kunt onthouden? (M)

<Roulate>

1. Ik noteer mijn wachtwoorden op een briefje dat ik verstop
2. Ik sla mijn wachtwoorden op in mijn telefoon
3. Ik sla mijn wachtwoorden op in mijn laptop/tablet/PC
4. Ik zet bij het inloggen een vinkje bij 'onthoud mijn wachtwoord'
5. Ik vertel mijn wachtwoorden aan iemand die ik vertrouw
6. Ik onthoud mijn wachtwoorden via een e-mail aan mezelf
7. Ik vraag bij ieder bezoek een nieuw wachtwoord aan
8. Ik gebruik speciale software die steeds automatisch een nieuw veilig wachtwoord genereert
9. Ik gebruik speciale software waarin ik mijn wachtwoorden opsla
10. Ik onthoud mijn wachtwoorden in mijn hoofd
11. Ik onthoud mijn wachtwoorden niet
12. Anders fixed as the single last category
13. Wil niet zeggen [S] fixed as the last category

ALL

E4. (5.5) Hoeveel verschillende wachtwoorden gebruikt u voor de verschillende computers, programma's en/of websites die u gebruikt? (S)
Kiest u het antwoord dat het best bij uw situatie past.

Roulate

1. Ik heb één wachtwoord dat ik voor alles gebruik
2. Ik heb één type wachtwoord waarvan ik diverse variaties gebruik
3. Ik heb een aantal verschillende wachtwoorden, maar sommige gebruik ik voor meerdere accounts en/of diensten
4. Voor belangrijke zaken gebruik ik overal een ander wachtwoord, voor de onbelangrijke accounts en/of diensten gebruik ik meestal steeds hetzelfde wachtwoord
5. Ik gebruik overal een ander wachtwoord voor

ALL

E5. (5.4) 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”. (S)

1. Ik wissel eigenlijk nooit mijn wachtwoorden
2. Ik wissel mijn wachtwoorden alleen als ik daar een melding over krijg
3. Ik wissel wel eens mijn belangrijkste wachtwoorden
4. Ik wissel regelmatig mijn belangrijkste wachtwoorden
5. Ik wissel wel eens al mijn wachtwoorden
6. Ik wissel regelmatig al mijn wachtwoorden
7. Weet niet / wil niet zeggen

Subthema 1. Smart cities

SELECTION: All

DISPLAY

Smart cities zijn (stedelijke) gebieden waar slimme, nieuwe ICT-toepassingen worden ontwikkeld en ingezet. Smart cities gebruiken groene technologie, ontwikkelen apparaten en apps voor beter vervoer en recreatie en gebruiken nieuwe ICT-toepassingen voor bijvoorbeeld gezondheid, bedrijvenparken en onderwijs.

SELECTION: All

G1. Welke stad in Nederland ziet u als een Smart City? [O]

TPM: normal size open answer field

SELECTION: All

G2. Waarom vindt u deze stad een smart city? [O]

TPM: big open answer field

SELECTION: All

G3. Wanneer vindt u dat een stad een smart city is? [S]

1. Wanneer slimme digitale technologieën worden toegepast (innovatieve architectuur of design)
2. Wanneer de stad privacy als belangrijke randvoorwaarde stelt
3. Wanneer de stad digitale veiligheid als belangrijke voorwaarde stelt

Subthema 2. Security by design / Smart design

SELECTION: All

G4. De volgende vraag gaat over uw IT-omgeving thuis, onderweg (op straat) en op uw werk. Wilt u voor de onderstaande activiteiten en locaties met een rapportcijfer aangeven hoe het gesteld is met de digitale veiligheid? (10 staat voor volkomen veilig, 1 staat voor volkomen onveilig)

TPM: range 1 through 10

1. Thuiswinkelen [Q]
2. Wifi-thuis [Q]
3. Nieuwssites [Q]
4. Openbaar vervoer [Q]
5. Beheren van administratieve zaken [Q]
6. Reserveren van kaartjes en tickets voor de bioscoop tot vliegtickets [Q]
7. Mobielen internetdiensten zoals apps [Q]
8. Energie voorziening [Q]

SELECTION: All

G5. Kunt u van de volgende locaties met een rapportcijfer aangeven hoe belangrijk u digitale veiligheid daar vindt? (10 staat voor uitermate belangrijk, 1 staat voor uitermate onbelangrijk)

TPM: range 1 through 10

Thuis: [Q]
Onderweg: [Q]
Op het werk: [Q]

Subthema 3. Smart coalitions

SELECTION: All

G6. Kunt u met een rapportcijfer aangeven in welke mate onderstaande partijen een rol spelen bij het tegengaan van DDOS-aanvallen? (10 staat voor een zeer belangrijke rol, 1 staat voor een zeer onbelangrijke rol)

Informatie ballon: DDos-aanvallen zijn pogingen om een computer, netwerk, website of dienst onbruikbaar te maken. Dergelijke aanvallen leiden doorgaans tot een overbelasting van de server, waardoor reguliere gebruikers geen toegang meer hebben.

TPM: range 1 through 10

1 (Rijks)overheid [Q]
2 Europese commissie [Q]
4 providers [Q]
5 Dienstverleners (de vitale infrastructuur: energie, water, etc) [Q]
6 Bedrijfsleven + MKB [Q]
7 Hardware leveranciers [Q]
8 Software leveranciers [Q]
9 Wetenschap [Q]

SELECTION: All

G7 Kunt u met een rapportcijfer aangeven welke partijen een rol spelen bij de bestrijding van malware? (10 staat voor een zeer belangrijke rol, 1 staat voor een zeer onbelangrijke rol)

Informatie ballon: Malware is kwaadaardige en/of schadelijke software. Er zijn veel verschillende varianten van malware, het ‘virus’ is de meest bekende vorm.

TPM: range 1 through 10

1 (Rijks)overheid [Q]
2 Europese commissie [Q]
4 providers [Q]
5 Dienstverleners (de vitale infrastructuur: energie, water, etc) [Q]
6 Bedrijfsleven + MKB [Q]
7 Hardware leveranciers [Q]
8 Software leveranciers [Q]
9 Wetenschap [Q]

SELECTION: All

G8 Kunt u met een rapportcijfer aangeven in welke mate u samenwerking voor het verhogen van digitale veiligheid belangrijk vindt binnen de onderstaande sectoren? [S]

TPM: range 1 through 10

1. Energie [Q]
2. Telecommunicatie [Q]
3. Financiële sector [Q]
4. Drinkwater [Q]
5. Oppervlaktewater [Q]
6. Transport [Q]

SELECTION: All

G9 Welk(e) samenwerkingsverbanden in het teken van digitale veiligheid kent u? [O]

Z. Achtergrondgegevens

Selection: target group = gemeenten

Z1.(6.1) Wat is uw geslacht? (S)

1. Man
2. Vrouw

Selection: target group = gemeenten

Z2. (6.2) Wat is uw leeftijd? (O)

<Open> <*max. = 99*>

Selection: target group = gemeenten

Z3. (6.3) Wat is uw hoogst genoten opleiding?

1. Geen opleiding
2. Lager onderwijs
3. Lager beroepsonderwijs
4. Middelbaar algemeen
5. Middelbaar beroepsonderwijs
6. Hoger algemeen en voorbereidend wetenschappelijk onderwijs
7. Hoger beroepsonderwijs
8. Universiteit

Selection: target group = gemeenten

Z4. (6.4) Wat zijn de vier cijfers van uw postcode? (Q)

<Open> ……(Q)

Selection: target group = Rijksoverheid

Z5. (6.5) Waar bent u werkzaam? (S)

1. Departement
2. Uitvoeringsorganisatie of Inspectie
3. Agentschap of ZBO
4. Hoog College van Staat of Adviescollege
5. Medewerkers Rechterlijke macht
6. Medewerkers onderwijs (primair, voortgezet, middelbaar, hbo, wetenschappelijk) en onderzoeksinstellingen
7. Medewerkers politie
8. Medewerkers defensie: burgerpersoneel en militair personeel
9. Anders, namelijk.. (O)

Selection: Z5=1

Z6 Op welk departement bent u werkzaam?

1. Algemene Zaken
2. Binnenlandse Zaken en Koninkrijksrelaties
3. Buitenlandse Zaken
4. Defensie
5. Economische Zaken
6. Financiën
7. Infrastructuur en Milieu
8. Onderwijs, Cultuur en Wetenschap
9. Sociale Zaken en Werkgelegenheid
10. Veiligheid en Justitie
11. Volksgezondheid, Welzijn en Sport

Selection: target group = Gemeenten

Z7. (6.5) Wat voor soort functie heeft u?

1. Beleidsfunctie
2. Uitvoeringsfunctie
3. Staffunctie
4. Administratieve functie
5. Loketfunctie
6. Anders, namelijk…(O)

ALL

Hartelijk dank voor uw medewerking!

BIJLAGE 3

Certificering

Certificering

Het onderzoek is uitgevoerd in overeenstemming met het kwaliteitssysteem van GfK Intomart dat is gecertificeerd volgens de normen van NEN-EN-ISO 9001, ISO 20252 en ISO 26362. GfK Intomart 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 Intomart <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).