TNO Informatie- en Communicatietechnologie

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek / Netherlands Organisation for Applied Scientific Research

Brassersplein 2
Postbus 5050
2600 GB Delft

www.tno.nl

T +31 15 285 70 00
F +31 15 285 70 57
info-ict@tno.nl

TNO-rapport

34982

Perceptieonderzoek Veilig Internet
Onderzoek naar de ruimte tussen wat (on)veilig ís en wat als zodanig gepercipieerd wordt

Datum	april 2009
Auteur(s)	S.G. Huveneers J.M.E. Geers
Reviewer	S.G.E. De Munck J. Wester
Opdrachtgever	Digivaardig & Digibewust (belegd bij ECP-EPN)
Projectnummer	035.33031
Aantal pagina's	45 (incl. bijlagen)

Alle rechten voorbehouden. Niets uit dit rapport mag worden vermenigvuldigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande schriftelijke toestemming van TNO.

Indien dit rapport in opdracht werd uitgebracht, wordt voor de rechten en verplichtingen van opdrachtgever en opdrachtnemer verwezen naar de Algemene Voorwaarden voor onderzoeksopdrachten aan TNO, dan wel de betreffende terzake tussen de partijen gesloten overeenkomst.

Het ter inzage geven van het TNO-rapport aan direct belanghebbenden is toegestaan.

© 2009 TNO

Inhoudsopgave

Managementsamenvatting

Het programma *Digivaardig & Digibewust* stimuleert veilig internetgebruik onder haar doelgroepen. Dit onderzoek bestaat uit twee delen. Enerzijds is gekeken wat we weten over de veiligheid van het internet. Met welke dreigingen worden de doelgroep geconfronteerd en welke risico's lopen zij bij het gebruik van digitale middelen? Anderzijds is door middel van een gebruikersonderzoek bevraagd hoe de doelgroepen zelf hun veiligheid bij het gebruik van online diensten percipiëren. Kort vatten we hieronder de belangrijkste bevindingen samen.

Veilig internet: wat weten we precies?

- Informatie over internet veiligheid kan worden opgesplitst in kwantitatieve informatie over de hoeveelheid dreigingen (*malware*, kinderporno, *phishing* etc) en in (vaak meer kwalitatieve) informatie over het risico dat gebruikers lopen en de schade die zij lijden bij confrontatie met een dreiging. Pas wanneer beiden bekend zijn ontstaat een compleet dreigingsbeeld.
- Beide soorten informatie worden door verschillende partijen verzameld (bijvoorbeeld commerciële organisaties, overheidsinstanties, ISP's en banken). Toch is er maar beperkt informatie beschikbaar. Het is vaak niet in het directe belang van commerciële partijen om de informatie die zij bezitten openbaar te maken.
- Om tot een compleet dreigingsbeeld te komen is het enerzijds noodzakelijk dat informatie beter gedeeld wordt en er een totaal beeld gevormd wordt, anderzijds is meer informatieverzameling nodig over met name over de impact en risico's van dreigingen.

Perceptie van gebruikers: hoe veilig voelen zij zich online?

Het perceptieonderzoek richtte zich op in totaal 1249 respondenten verdeeld over drie doelgroepen; ouders (opgesplitst in groepen met jongere en oudere kinderen), senioren en een controle groep van Nederlanders van vijftien jaar en ouder. Aan hen zijn vragen voorgelegd over o.a. de beveiliging van de computer, dienstengebruik, ondervonden hinder van dreigingen en veiligheidsbeleving.

- Meer dan 90% van de Nederlanders gebruikt een virusscanner. 75% installeerde in de week voorafgaand aan het onderzoek beveiligingsupdates van deze software.
- Veel gebruikers hebben ervaringen met dreigingen. Spam is daarbij het meest genoemd.
- Filters om schadelijke content te weren worden door een minderheid van de ouders gebruikt. Veel ouders vinden dit niet nodig.
- Er wordt vooral veel gebruik gemaakt van internet bankieren en marktplaatsen. Gebruikers hebben veel vertrouwen in deze diensten, maar maken zich meer zorgen over de beveiliging van persoonlijke gegevens.
- Bijna de helft van de ouders maakt zich wel eens zorgen over de veiligheid van hun kind online. Deze zorgen hebben vooral betrekking op de confrontatie met ongewenste informatie en het gegeven dat kinderen benaderd kunnen worden door onbekenden met slechte bedoelingen.
- Van de ouders vindt 80% dat ze zelf goed op de hoogte zijn en 95% van de ouders met kinderen in de leeftijd 13-18 jaar praat de kinderen over diverse onderwerpen. Wat niet uit dit onderzoek blijkt is of kinderen goed op de hoogte zijn van

dreigingen en risico's en hoe ze omgaan met de kennis die zij hebben over het onderwerp.
- Er is weinig behoefte aan extra informatie over veiligheid op internet. Huidige kennis wordt vooral opgedaan via de massamedia.
- Ouderen maken zich minder zorgen over de veiligheid van internetdiensten en de impact van malware en beschermen zich minder goed tegen dreigingen. Toch wijkt de groep niet erg veel af van de groep Nederlanders.

Conclusies en aanbevelingen
- Hoewel er informatie verzameld wordt over de hoeveelheid dreigingen online en soms ook over de risico's en impact, ontbreekt het aan een compleet dreigingsbeeld. Hierdoor is het niet voldoende mogelijk om in te schatten waar gebruikers risico lopen, of eventuele zorgen terecht zijn en waarmee het programma haar doelgroepen precies kan ondersteunen. Er ligt een grote uitdaging om een completer beeld te krijgen van de hoeveelheid dreigingen, de risico's en de impact voor gebruikers. Het programma zou initiatieven om dit beeld aan te vullen, met name op het gebied van impactmeting, kunnen ondersteunen of initiëren. Hierdoor kunnen de doelgroepen hun afwegingen maken op basis van feitelijke risico's en impact. Nu is de perceptie nog te veel incidentgedreven. Waar nodig kan het programma met de kennis van de feitelijke risico's voor gebruikers de doelgroepen extra voorlichten. Ook biedt een realistisch dreigingsbeeld mogelijkheden om urgente risico's (gezamenlijk) te bestrijden en beter te voorkomen in de toekomst.

- Uit het gebruikersonderzoek bleek dat veel ouders met hun kinderen praten over de dreigingen die online bestaan, vaak incident gedreven naar aanleiding van een bericht in de media. Uit dit onderzoek blijkt niet wat het effect is van deze voorlichting en hoe het gesteld is met het kennisniveau van de kinderen. Ook zeggen de ouders zelf niet veel meer behoefte te hebben aan voorlichting. Er is in de laatste jaren ook al voorlichting geweest voor ouders. Interessant zou zijn om te kijken welke invloed de voorlichting van de ouders heeft op het gedrag van de kinderen. Het hoeft helemaal niet vanzelfsprekend te zijn dat een goed voorgelichte ouder de kinderen ook heeft kunnen overtuigen van het belang van bewust internetgebruik. Mogelijk schatten kinderen de risico's anders in en verkiezen zij het nut of plezier van een dienst boven eventuele veiligheidsrisico's. Om hier uitspraken over te doen is meer onderzoek nodig.

- De senioren die in dit onderzoek ondervraagd zijn, zijn veelal actieve internetgebruikers. Over het algemeen blijken ouderen minder goed op de hoogte van veiligheidsrisico's en lopen ze iets achter in het gebruik van beveiligingen. Deze groep ondervindt ook minder last van risico's, waardoor het gevoel van urgentie mogelijk niet zo hoog is als bij de andere groepen. Ze vinden het ook moeilijker om de juiste informatiekanalen te vinden dan de andere doelgroepen. Hoewel er geen sprake is van een grote kloof tussen ouderen en de Nederlandse bevolking, zou het programma ouderen kunnen ondersteunen bij het vinden van de juiste informatiekanalen, of nieuwe kanalen inrichten.

1 Inleiding

Achtergrond- Digibewust

In 2006 is het programma *Digibewust* gestart om bij te dragen aan een beter ‘digitaal bewustzijn’ in Nederland. Het programma had een tweeledige doelstelling. Ten eerste wilde het gebruikers stimuleren om de kansen die digitale middelen bieden optimaal te benutten. Ten tweede wilde het de gebruiker bewust maken van eventuele risico’s die hiermee gepaard gaan. Door een goed digibewustzijn zijn mensen mogelijk in staat hun eigen digitale veiligheid goed in te schatten en zo op een verantwoorde manier te profiteren van allerhande digitale diensten. *Digibewust* heeft in de afgelopen drie jaar vele activiteiten gesteund met als doel aan die doelstelling bij te dragen. Hierbij heeft het programma zich in het bijzonder gericht op drie doelgroepen; kinderen en hun ouders/opvoeders, senioren en mkb-ers.

In 2009 krijgt het programma een vervolg in het nieuwe programma *Digivaardig & Digibewust*, waarmee beoogd wordt om gebruikers niet alleen digibewuster te maken, maar ook vaardiger in de omgang met digitale middelen en diensten.

Veiligheid op internet

Een van de thema’s die ook in het nieuwe programma een belangrijke plek krijgt, is veiligheid bij internetgebruik. Een digibewuste internetgebruiker is beter op de hoogte van risico’s en wordt in staat gesteld zijn handelen hier op aan te passen. In het kader van het *Digibewust* programma zijn er dan ook diverse initiatieven geweest die verschillende doelgroepen hebben ondersteund bij het bewust en veilig gebruik van digitale diensten. Om veilig en verantwoordelijk gebruik te maken van digitale middelen is het noodzakelijk dat gebruikers een waarheidsgetrouwe inschatting kunnen maken van de mate van veiligheid van een dienst. Hierbij is er dan mogelijk nog een onderscheid te maken tussen wat feitelijk veilig/onveilig ís op internet en wat de doelgroepen als veilig/onveilig percipiëren. Hierin schuilen twee gevaren: 1) de gebruiker voelt zich veilig in een onveilige omgeving en loopt daarmee risico’s zonder zich daarvan bewust te zijn of 2) de gebruiker waant zich onveilig in een veilige omgeving en voelt zich daardoor gehinderd om gebruik te maken van de dienst met als gevolg dat hij kansen mis loopt(2). Beiden staan optimalisering van het benutten van kansen die het gebruik van digitale diensten met zich mee kan brengen in de weg. Meer inzicht in de perceptie van gebruikers en de manier waarop die aansluit bij de werkelijkheid, geeft het nieuwe programma handvatten voor het bepalen van geschikte activiteiten.

Om inzicht te kunnen geven in zowel de perceptie van veiligheid van de gebruiker, als de feitelijke veiligheid, wordt het onderzoek in twee delen gesplitst. In hoofdstuk twee wordt verkend welke conclusies er getrokken kunnen worden over de feitelijke veiligheid van het internet in Nederland. Door middel van deskresearch en interviews met relevante partijen wordt er gekeken welke gegevens over internetveiligheid beschikbaar zijn en welke waarde er aan die gegevens toegekend kan worden. Op basis van deze uitkomsten kijken we welke inschatting er gemaakt kan worden over de veiligheid van het internet.

Het tweede deel van het onderzoek bespreekt de resultaten van een perceptieonderzoek bij gebruikers. Aan drie doelgroepen (internetgebruikers, ouders en senioren) zijn

vragen gesteld over de beveiliging van computers, de manier waarop mensen zich informeren over veiligheid de inschatting van de eigen kennis en ervaring en de beleving van veiligheid in het algemeen.

Aan het eind van het onderzoek wordt gekeken hoe de resultaten van het perceptieonderzoek zich verhouden tot de conclusies over de feitelijke veiligheid.

2 Veilig Internet: wat weten we nu precies?

ICT heeft zich in de afgelopen decennia ontwikkeld tot een essentieel onderdeel van onze (informatie)maatschappij. Internet in het bijzonder kan daarbij als vitale infrastructuur voor vrijwel alle economische en sociale processen worden beschouwd. Maar met de toenemende mogelijkheden en impact van ICT op economisch en maatschappelijk vlak, nemen ook de mogelijkheden voor kwaadwillenden toe om misbruik te maken van dit medium. Cybercrime-activiteiten (waaronder kinderporno, identiteitsfraude en de verspreiding van diverse vormen van malware) nemen snel toe (Govcert, 2008)[1], met zowel financiële als emotionele schade tot gevolg. Een studie van McAfee (2009)[2] begrootte de economische schade als gevolg van cybercrime (met name herstelwerkzaamheden en verloren intellectueel eigendom) voor bedrijven wereldwijd jaarlijks op ca. 1 biljoen dollar. Cybercrime beïnvloedt daarnaast ook het vertrouwen van gebruikers (burgers en bedrijven) in het internet en toepassingen daarvan. Vertrouwen is een belangrijke voorwaarde voor de verdere verspreiding en adoptie van ICT-diensten en -voorzieningen, en daarmee voor de ontwikkeling van de informatiemaatschappij als geheel.

De meeste van bovengenoemde gevaren worden inmiddels breed onderkend. Desondanks blijft het lastig ze objectief op hun risico's te beoordelen. Dit leidt soms tot onderschatting van mogelijke gevolgen door gebrek aan kennis, maar mogelijk ook tot overschatting van risico's op basis van extremen. Een goed overzicht van de daadwerkelijke risico's kan het programma Digivaardig & Digibewust helpen om voorlichting en andere activiteiten beter te richten, waardoor het programma als geheel effectiever wordt. Ook geeft een overzicht van de risico's inzicht in welke actoren het best in positie zijn of mogelijkheden hebben de internetveiligheid te verbeteren en wat ze daarvoor zouden kunnen doen. Daarnaast kunnen cijfers over internetrisico's een basis vormen voor beleidsmakers, bedrijven en individuen voor het nemen van (investerings)beslissingen.

2.1 Dreigingen en risico's

Veilig internet omvat een hoop verschillende aspecten. Zo kunnen zowel zakelijke als particuliere gebruikers geconfronteerd worden met verschillende vormen van Cybercrime. Volgens de definitie van de Europese Commissie[3] omvat dit begrip de volgende aspecten:

- Computercriminaliteit: dit begrip beslaat traditionele vormen van criminaliteit zoals fraude of oplichting, maar in een cybercrime context relateert het begrip specifiek aan criminaliteit gepleegd via elektronische communicatie netwerken en informatiesystemen (vanaf nu elektronische netwerken).
- Computergerelateerde criminaliteit: dit betreft publicatie van illegale content op elektronische media (bijvoorbeeld kinderporno, haat zaaien, discriminatie e.d.).

[1] Govcert, 2008 Trendrapport Inzicht in cybercrime: trends en cijfers, http://www.govcert.nl/render.html?it=156

2 McAfee (2009) Virtual criminality report 2008. Cybercrime vs Cyberlaw.

[3] European Commission (2007) Towards a general policy on the fight against cyber crime. Brussels, 22.5.2007, COM(2007) 267 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

- High-tech crime: betreft criminaliteit uniek voor elektronische netwerken, zoals aanvallen op informatiesystemen, *Denial of Service* en aanvallen die de vitale infrastructuur bedreigen, zoals ook verschillende vormen van malware.

In overleg met de opdrachtgever is besloten om dit onderzoek met name te richten op die veiligheidsaspecten die invloed hebben op de privégebruiker[4], derhalve besteden we in dit onderzoek geen aandacht aan veiligheidsrisico's voor overheden en bedrijven.

Wanneer we het hebben over internetveiligheid, is het belangrijk om een onderscheid te maken tussen een dreiging en een risico. Niet alle dreigingen hebben evenveel impact en daardoor loopt een gebruiker bij sommige dreigingen meer risico's dan bij anderen. Om het risico van een dreiging te bepalen is het van belang om te weten wat de impact van een potentiële dreiging is en hoe groot de kans is dat de dreiging zich voordoet. De impact kan in veel gevallen uitgedrukt worden als financiële schade. Zeker bij frauduleuze financiële transacties is dit duidelijk. Ook als bedrijven slachtoffer zijn is de schade meestal uit te drukken in een getal. Daarbij worden dan inschattingen gemaakt voor onproductieve uren, gederfde inkomsten en imagoschade. De impact is moeilijker te kwantificeren als het gaat om zaken als het bekend worden van privacygevoelige informatie, een tragere computer, tijd die het een privégebruiker kost de computer weer werkend te krijgen, enz.

Wanneer we het hebben over de veiligheid van internet vanuit het gebruikersperspectief, is het vooral interessant om een inschatting te kunnen maken van het risico. Uit onderzoek van verschillende producenten van anti-malware producenten blijkt dat de hoeveelheid gesignaleerde *malware* explosief groeit. In 2008 is bijna zeven keer meer malware gesignaleerd dan in 2007. Het grootste deel van deze malware bestaat uit *spyware* en Trojaanse paarden.[5] Toch moeten deze absolute cijfers in perspectief geplaatst worden. De toename van dreigingen leidt niet automatisch tot een evenredige groei van de risico's die gebruikers lopen. Wanneer het een toename betreft in dreigingen die reeds werden opgevangen door beschermende software, kan het risico voor de gebruiker hetzelfde zijn, of wellicht kleiner. En zo kan het ook zijn dat een minder voorkomende dreiging in potentie een grotere impact heeft en dus een groter risico vormt. Daarnaast is het door de continue ontwikkeling van dreigingen aannemelijk dat niet alle dreigingen in de beschikbare cijfers zijn opgenomen.

2.2 Beschikbare informatie over dreigingen en risico's

Door deskresearch en interviews is een beeld gemaakt van de partijen in het veld die op enige manier informatie verzamelen rondom veilig internet.
In tabel 1 wordt aangegeven welke instanties informatie verzamelen, of ze zich toespitsen op dreigingen en/of risico's en of de informatie openbaar beschikbaar is.

[4] In het gebruikersonderzoek is gekozen voor een focus op ouders en senioren, daarom beperkt dit hoofdstuk zich tot veiligheidsaspecten met invloed op privégebruikers.
[5] GData. *Malware-rapport. Halfjaarlijks rapport juli-december 2008.* http://www.gdata.nl/uploads/media/MalwareReport_2008_7-12_NL.pdf,
MessageLabs. *Messagelabs Intelligence kwartaal 1/maart 2009 http://www.messagelabs.nl/intelligence.aspx*

Type dataverzamelaar		**Dreigingen (kwantitatief**	**Risico's en impact**	**Openbaar beschikbaar (j/n)**	**Commercieel / Publiek belang (c / p)**
Commerciële partijen[6]		x		j	C
Overheid	KLPD		x	N (soms beperkt)	P
	SurfCert	x		n	P
	Govcert	x	x	J	P
Banken[7]		x	x	n	C
ISPs		x		n	C

Tabel 1: Soorten partijen met informatie over Internet-dreigingen.

Anti Malware producenten

De meest toegankelijke cijfers over internetdreigingen zijn die van anti-malware producenten. Voorbeelden zijn rapportages zoals die van G-Data[8] en MessageLabs[9] die informeren over aantallen SPAM- en *phishing*-emails, aantallen virussen en het aantal zombie computers in botnets dat zij detecteren. MessageLabs relateert deze aantallen ook aan het totaal aantal e-mails en computers. Voor de cijfers zoals die beschikbaar zijn bij de anti-malware producenten is het niet altijd duidelijk hoe de cijfers tot stand komen en in hoeverre nieuwe ontwikkelingen hierin meegenomen zijn. Het gaat hierbij om cijfers die aangeven hoe vaak een bepaalde dreiging voorkomt, niet om de kans dat de dreiging impact heeft en hoe groot die impact dan is. Over het risico van deze dreigingen geven deze cijfers dus geen informatie. Kleuring bij selectie en presentatie van data is met het oog op het bedrijfsbelang op basis van de huidige beschikbare gegevens niet uit te sluiten.

In de rapportages van GData wordt behalve aan kwantitatieve gegevens, ook aandacht geschonken aan opkomende trends. GData stelt dat vooral gebruikers van sociale netwerken, fora, blogs, andere web 2.0 toepassingen en online games voorzichtig moeten zijn. Dit omdat malware steeds vaker via de browser verspreidt wordt. "Gekraakte webservers, gemanipuleerde zoekresultaten en typefouten bij het invoeren van de URL kunnen naar sites leiden die de computer van de bezoeker ongemerkt infecteren op de achtergrond."[10]

[6] Zoals o.a. producenten van anti malware software

[7] Hoewel banken getypeerd zouden kunnen worden als commerciële partij, is er voor gekozen om ze hier apart in het overzicht op te nemen, omdat zij over informatie beschikken over specifieke dreigingen met vaak een hoge impact voor de gebruiker.

[8] GData. *Malware-rapport. Halfjaarlijks rapport juli-december 2008.* http://www.gdata.nl/uploads/media/MalwareReport_2008_7-12_NL.pdf

[9] MessageLabs. *Messagelabs Intelligence kwartaal 1/maart 2009* *http://www.messagelabs.nl/intelligence.aspx*

[10] GData. *Malware-rapport. Halfjaarlijks rapport juli-december 2008.* http://www.gdata.nl/uploads/media/MalwareReport_2008_7-12_NL.pdf

MessageLabs[11], ook producent van anti-malware software, rapporteert ook over de gemeten risico's als percentage van het totale internetverkeer. In maart 2009 bedroeg het aandeel van spammails in het totale e-mailverkeer wereldwijd maar liefst 75,7%. Voor Nederland lag dat percentage iets lager op 68,8%. Via 0,36% van de e-mailberichten werd in maart een virus verspreid. Hoewel dit percentage erg laag ligt, is hier wel sprake van en stijging ten opzichte van de maand ervoor. *Phishing*, het vaak ongemerkt kopiëren van persoonlijke gegevens, is volgens MessageLabs iets afgenomen (0,35% van het emailverkeer). Het aandeel van *phishing* in het totaal aantal gemeten gevaren, neemt echter wel toe. [12]

Ook Symantic[13] presenteert cijfers en trends over internetdreigingen. In hun rapport over 2008 is te lezen dat zij in 2008 met hun monitoringssysteem ruim 1,6 miljoen schadelijke dreigingen signaleerden. Ter vergelijking: in 2006 waren dat er nog ruim 140.000. De nieuwe geavanceerde technieken en het toenemende dreigingsniveau vragen volgens Symantec om nieuwe samenwerkingen tussen betrokken partijen om deze problematiek gezamenlijk aan te pakken.[14]

De cijfers van verschillende anti-malware producenten en de stijgingen die zij waarnemen, komen niet één op één overeen. Dit is vooral te verklaren door verschillende meetwijzen die zij hanteren; hierdoor is het niet duidelijk welke dreigingen precies worden gemeten en in hoeverre de resultaten van de metingen generaliseerbaar zijn.

Overheidsinstanties

In Nederland wordt door verschillende overheidsgerelateerde instanties informatie verzameld over dreigingen en risico's. Een van de partijen in dit veld is GovCert GovCert rapporteert over de trends die ze waarneemt in haar jaarlijkse Trendrapportage[15]. Voor de cijfers maakt GovCert gebruik van een eigen monitoringsysteem. Door middel van een steekproef wordt via dit systeem een inschatting gemaakt van de hoeveelheid malware dreigingen in Nederland. Ook relateert GovCert deze dreigingen aan de impact. Zo staat in de trendrapportage bijvoorbeeld beschreven dat 89% van virussen en spam wordt tegengehouden door anti-malware software. De kans dat deze dreiging de consument bereikt is kleiner dan de omvang van het probleem.

Zoals de naam van de rapportage al doet vermoeden, signaleert ook GovCert nieuwe trends. Ook in deze rapportage is aandacht gegeven aan recente ontwikkelingen rond zogenaamde web2.0 initiatieven. Kwaadwillenden maken steeds vaker gebruik van het vertrouwen wat heerst op sociale netwerken en chatprogramma's. Een klik van een gebruiker kan leiden tot een aanval op zijn of haar complete netwerk.

---

[11] www.messagelabs.nl

[12] MessageLabs. *Messagelabs Intelligence kwartaal 1/maart 2009*
http://www.messagelabs.nl/intelligence.aspx

[13] www.symantic.com

[14] Symantec.Symantec Global Internet Security Threat Report. Trends for 2008. Volume XIV, Published April 2009

[15] http://www.govcert.nl/render.html?it=156

De dienst nationale recherche van de KLPD (Team High Tech Crime) houdt zich bezig met cybercrime. Zij hebben criminaliteitsbeeld analyses[16] waarin ontwikkelingen op het gebied van cybercrime beschreven worden. Deze criminaliteitsbeeld analyses zijn niet openbaar. Uit interviews kwam naar voren dat het beeld dat in deze rapportages geschetst wordt, gebaseerd is op de aangiftes die worden gedaan met betrekking tot cybercrime. De getallen zoals de politie die beschikbaar heeft uit aangiftes zijn moeilijk te interpreteren omdat niet te zeggen is in hoeveel procent van de gevallen aangifte gedaan wordt. Er wordt vanzelfsprekend alleen melding gedaan van de gevallen waarbij de gebruiker zich zelf bewust is van een strafbaar feit en hiermee ook daadwerkelijk naar de politie stapt. In tegenstelling tot de meer kwantitatieve bronnen, kan op basis van de criminaliteitsbeeld analyses van het KLPD, wel een betere inschatting worden gemaakt van de impact die bepaalde dreigingen op de gebruiker hebben gehad. In de criminaliteitsbeeld analyses wordt verder gerapporteerd over de prijs voor gestolen data op Internet, zoals credit card gegevens, en over de prijs van op Internet aangeboden malware. Het team verkrijgt deze gegevens door het volgen van internetfora en chatrooms. Dit geeft in de eerste plaats een goede indruk van de soort dreigingen en nieuwe ontwikkelingen daarin. Daarnaast vertoont de prijs van de aangeboden gegevens, producten en diensten een relatie met de mogelijke opbrengst ervan (en daarmee met de impact voor de gebruiker). Deze relatie is echter lastig te leggen.

ISP's

Veel informatie over Internetdreigingen, zeker als het gaat om aantallen zombie-computers en de hoeveelheid SPAM, is beschikbaar bij de Internet Service Providers (ISPs). Deze informatie is echter niet openbaar. Ook voor ISP's geldt dat er een commercieel belang is en dat openbaarheid van bepaalde informatie ongunstig kan uitpakken voor het imago en de concurrentiepositie. Ook is het mogelijk dat het vanwege wettelijke aansprakelijkheidsproblemen minder aantrekkelijk is om de gegevens over risico's anders te gebruiken dan voor de eigen bedrijfsvoering. Wel werken een groot aantal Nederlandse ISP's samen om geïnfecteerde computers in quarantaine te plaatsen totdat de problemen verholpen zijn. De ISP's werken ook samen met GovCert, buitenlandse ISP's en de banken. De ISP's zijn vaak de eerste die een *phishing* aanval op een bank detecteren. De bank wordt daar dan van in kennis gesteld, zodat de bank zijn klanten kan waarschuwen. De ISPs kunnen lang niet alle zombie-computers in hun netwerk detecteren doordat deze tegenwoordig meestal lange tijd gebruikt worden om vertrouwelijke informatie te achterhalen en zeer gedoceerd berichten te versturen en pas op het eind van hun levenscyclus voor het versturen van een grote hoeveelheid SPAM. ISP's bevinden zich in de beste positie om getallen over de hoeveelheid SPAM en zombie-computers op Internet te verzamelen, maar de ISP's hebben geen inzicht op de impact van de dreigingen.

De OPTA en de ISP's hebben onlangs afspraken gemaakt over het verbeteren van voorlichting over internetveiligheid, dit in het kader van de informatieplicht van

[16] KLPD, Dienst Nationale Recherche, Cybercrime – focus op High Tech Crime, Deelrapport Criminaliteitsbeeld 2007.
E.R. Leukfeldt, M.M.L. Domenie, W. Ph. Stol, Criminialiteitsbeeldanalyse Cybercrime; Een verkennend onderzoek naar cybercrime in Nederland, Februari 2009 (voorlopige versie)

aanbieders in de Telecomwet. Voorlopig zijn er acht dreigingen[17] genoemd die in de voorlichting naar de klant dienen te worden meegenomen.

Banken
Het is niet openbaar hoeveel fraude plaatsvindt bij online bankieren en internet aankopen en wat de schade is van *phishing* aanvallen op bankgegevens. De banken zelf beschikken vaak wel over deze informatie. De gegevens van de banken over internet fraude zijn belangrijke gegevens om de risico's van Internet te bepalen. De banken hebben niet alleen inzicht in de dreigingen, maar ook in de impact ervan en daarmee in het risico dat ze vormen. Internetbankieren en online aankopen doen behoren tot de meest gebruikte diensten (zie Hoofdstuk 4). Deze gegevens zijn niet openbaar. Het is ook de vraag of het commercieel belang van de bank past om gegevens over risico's naar buiten te brengen in verband met mogelijke imagoschade.

2.3 Hiaten en mogelijkheden om deze in te vullen

Tabel 1 laat zien dat relatief veel informatie bekend is over het aantal instanties van de verschillende soorten dreigingen, maar veel minder over de risico's die ze veroorzaken. Ook is snel duidelijk dat de partijen die wel (zij het beperkt) inzicht hebben in het risico en de impact van bepaalde dreigingen, deze vaak om uiteenlopende redenen niet beschikbaar stellen.

De cijfers en informatie die wel beschikbaar is over veilig internet is dus nauwelijks in perspectief te plaatsen en daarom is het in de meeste gevallen onduidelijk hoe groot risico's zijn voor privé gebruikers. Een compleet dreigingsbeeld ontstaat alleen als de informatie rondom dreigingen en risico's rond verschillende veiligheidsaspecten samenkomen.

Het komen tot een volledig dreigingsbeeld vereist een verbreding van de scope. Door verschillende partijen bij elkaar te brengen kan het gat tussen dreigingen en impact met de informatie die er nu is al deels worden opgevuld, maar kan ook gezocht worden naar nieuwe initiatieven om op de nog lege terreinen deze informatie aan te vullen. Hierbij is er vooral behoefte aan impactmetingen die de kwantitatieve gegevens in perspectief kunnen plaatsen en een realistisch beeld kunnen geven van de risico's die gebruikers lopen bij het gebruik van digitale middelen.

2.4 Kernbevindingen

- Informatie over internet veiligheid kan worden opgesplitst in kwantitatieve informatie over de hoeveelheid dreigingen (malware, kinderporno, *phishing* etc) en in (vaak meer kwalitatieve) informatie over het risico dat gebruikers lopen en de schade die zij lijden bij confrontatie met een dreiging. Pas wanneer beiden bekend zijn ontstaat een compleet dreigingsbeeld.
- Beide soorten informatie worden door verschillende partijen verzameld (bijvoorbeeld commerciële organisaties, overheidsinstanties, ISP's en banken). Toch is er maar beperkt informatie beschikbaar. Het is vaak niet in het directe belang van commerciële partijen dat informatie openbaar is.

[17] Spam, botnets, phishing, spyware, trojans en overige malware, beveiliging van draadloze router, identiteitsdiefstal (-kaping) en ongewenste websites

- Om tot een compleet dreigingsbeeld te komen is het enerzijds noodzakelijk dat informatie beter gedeeld wordt en er een totaal beeld gevormd wordt, anderzijds is meer informatieverzameling nodig over met name over de impact en risico’s van dreigingen.

3 Onderzoeksopzet perceptieonderzoek

Voordat over wordt gegaan naar de resultaten, bespreken we in dit hoofdstuk kort de onderzoeksopzet. Paragraaf 3.1 geeft verdere toelichting op de gekozen doelgroepen. Paragraaf 3.2 gaat in op de opzet van de vragenlijst.

3.1 Doelgroepen

Het *Digibewust* programma dat liep van 2006-2008 richtte zich met name op drie doelgroepen; kinderen (en hun opvoeders), senioren en het MKB. In overleg met het programmabureau is ervoor gekozen om in het onderzoek de nadruk te leggen op de perceptie van senioren en ouders. Om de doelgroepen op sommige vragen te kunnen vergelijken met de gemiddelde Nederlandse internetgebruiker, is er ook een steekproef genomen onder Nederlanders met internet van 15 jaar en ouder[18].

De steekproef kent de volgende aantallen in de verschillende panels:

Tabel 3.1 Aantal respondenten per doelgroep

Doelgroep	**N**
Nederlanders (met internet) 15 jaar en ouder	288
Ouders van kinderen 6 – 12 jaar	310
Ouders van kinderen 13 – 18 jaar	302
Leden van community Ouders Online	228
Ouderen 65 jaar en ouder	349
Totaal	**1.249**

Bron: Synovate 2009

De ondervraagde ouders zijn in drie categorieën in te delen. Synovate benaderde twee representatieve groepen ouders met kinderen van 6-12 jaar (1) en 13-18 jaar (2). Op verzoek van het programmabureau is er ook een extern panel ouders ondervraagd. Deze ouders maken regelmatig gebruik van de website Ouders Online[19], een website waarop ouders terecht kunnen met allerhande vragen die hun kinderen betreffen. De website heeft een apart gedeelte over media en games, waarop onder andere informatie te vinden is over veilig internet. Door dit panel op te nemen in dit onderzoek, willen we kijken of er een verschil bestaat tussen de ouders van Ouders Online en de gemiddelde Nederlandse ouder.

[18] De steekproef onder Nederlanders met internet is representatief naar leeftijd, geslacht en opleidingsniveau. Het feit dat het hier een online vragenlijst betreft, maakt dat de groep naar alle waarschijnlijkheid wel boven gemiddeld ervaring heeft met internet en dienstengebruik.
[19] http://www.oudersonline.nl

3.2 Vragenlijst

Om een goede afweging te maken welke vragen gesteld moesten worden, zijn enkele interviews gehouden met experts op het gebied van internetgebruik bij de bovengenoemde doelgroepen. In deze interviews is kennis gedeeld en zijn thema's en problemen geïdentificeerd voor de uiteindelijke vragenlijst.

De vragenlijst is opgedeeld in drie delen. Er is een algemeen deel voor alle doelgroepen, een deel voor ouders en een deel voor senioren. De groep Nederlanders beantwoordt vragen in het algemene deel en in het deel voor senioren om de resultaten vergelijkbaar te maken. De resultaten, die in het volgende hoofdstuk aan bod komen, zullen langs dezelfde lijnen besproken worden.

3.2.1 Deel 1: Algemeen

Het de vragen in het algemene deel zijn voorgelegd aan alle respondenten.

In het algemene deel van de vragenlijst is ingegaan op de volgende onderwerpen:

- Het gebruik van internetdiensten
- Het vertrouwen in de veiligheid van internetdiensten
- Beveiliging van de computer tegen risico's
- Ondervonden hinder van dreigingen
- Algemene veiligheidsbeleving

3.2.2 Deel 2: Ouders

Het tweede deel van de vragenlijst richt zich op drie groepen ouders; ouders met kinderen op basisschoolleeftijd van 6-12 jaar, ouders van kinderen in de leeftijdscategorie 13-18 jaar en een panel van Ouders Online met kinderen in de leeftijd 6-18 jaar.

De onderwerpen die aan ouders zijn voorgelegd zijn de volgende:

- Ouders en hun zorgen
- Internet gebruik van de kinderen
- Gebruik van filters en controle
- Eigen kennis en informatievergaring
- Voorlichting van kinderen

3.2.3 Deel 3: Senioren

Het deel van het onderzoek dat zich richt op Nederlanders van 65 jaar en ouder raakt de volgende onderwerpen:

- Informatievergaring
- Eigen kennis
- Algemene veiligheidsbeleving

Dezelfde vragen zijn voorgelegd aan de groep Nederlanders van alle leeftijden om een vergelijking te kunnen maken.

4 Resultaten perceptieonderzoek

In dit hoofdstuk zullen de resultaten van het door Synovate uitgevoerde gebruikersonderzoek uitvoerig worden besproken en geanalyseerd. Eerst worden de resultaten uit het algemene deel van het onderzoek weergegeven. De overige resultaten worden per doelgroep besproken.

4.1 Algemeen

Steeds meer diensten zijn online beschikbaar. Veel Nederlanders maken daar dankbaar gebruik van. Van de Nederlandse bevolking heeft 86% toegang tot internet, 52% van de bevolking zoekt online naar informatie op overheidssites, 74% maakt gebruik van internet bankieren en bijna 67% van de internetgebruikers kocht in 2008 frequent iets via het internet.[20] “Gemak dient de mens”, gaat hier vaak op. Toch is het niet altijd duidelijk of de diensten die we gebruiken wel veilig zijn. Een groot deel van de verantwoordelijkheid ligt bij onszelf, door goed af te wegen wat wel en niet verstandig is wanneer wij ons online begeven, denk hierbij bijvoorbeeld aan het prijsgeven van persoonlijke informatie op openbare bronnen. Voor een deel van de dreigingen kunnen we ook technische hulp gebruiken, zoals virusscanners en spamfilters.

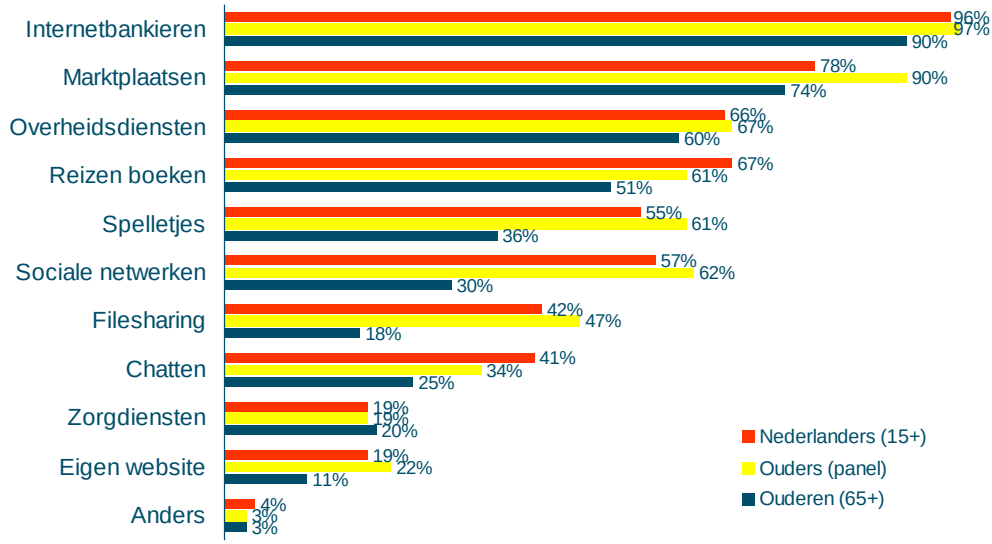
Het algemene deel van de vragenlijst vraagt gebruikers naar het gebruik van diensten en de motivatie die daarachter zit. Ook beantwoordden zij vragen over de beveiliging van hun computer en de hinder die zij zelf ondervinden van de risicovolle aspecten van het internet.

4.1.1 Het gebruik van internetdiensten

Het internet kent tal van diensten, de een veiliger dan de ander. Om een idee te krijgen van het gedrag van de respondenten, is aan alle respondenten een selectie van diensten voorgelegd met de vraag welke diensten zij weleens gebruikten. Het resultaat is weergegeven in Figuur 4.1.

[20] De Digitale Economie 2008. Centraal Bureau voor de Statistiek. Den Haag, 2008. www.cbs.nl

Figuur 4.1Van welke van onderstaande diensten heeft u wel eens gebruik gemaakt?



Bron: Synovate
Basis: groep Nederlanders 15+ (n=288); groep ouders uit het Online Interview Panel (n=612); groep ouderen 65+ (n=349)

Internetbankieren wordt door bijna alle internetgebruikers gebruikt. Dit is voor alle groepen het geval (Figuur 4.1)[21]. Ook het Centraal Bureau van de Statistiek publiceert cijfers over het gebruik van diverse internetdiensten. Volgens deze cijfers gebruikte 74% van de Nederlandse internetters in 2008 een dienst om online te betalen.[22] Het grote verschil is te verklaren door een zogenaamde '*selection bias*'. De respondenten van dit onderzoek nemen deel aan een online panel voor onderzoeken en het is waarschijnlijk dat zij daardoor actievere internetgebruikers zijn dan de gemiddelde Nederlander.

Ook Marktplaatsen en overheidsdiensten worden door een grote meerderheid gebruikt. Opvallend hierbij is dat ouders veruit het meest gebruik maken van marktplaatsen.

Wat ook opvalt is dat de groep senioren van de doelgroepen het minst gebruikt maakt van elektronische diensten Deze groep maakt wel relatief veel gebruik van zorgdiensten, maar hierbij is het verschil met de overige doelgroepen minimaal. Ouders zijn het meest actief bij het gebruik van online diensten.

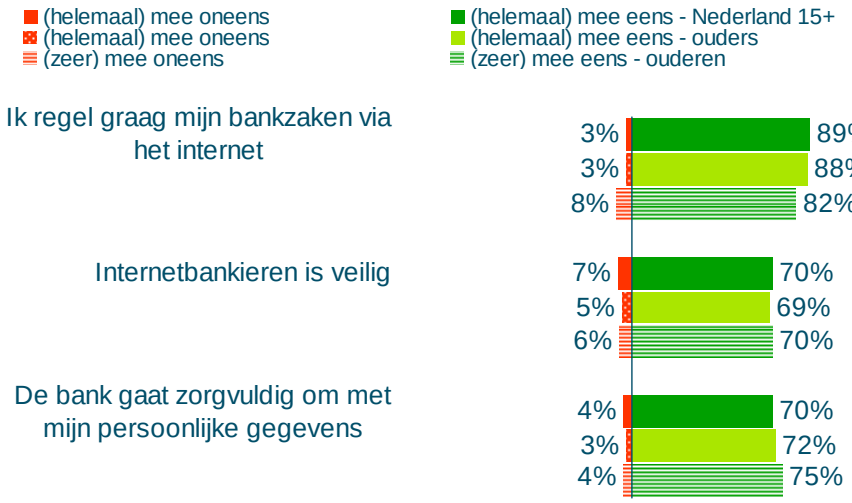
4.1.2 Het vertrouwen in de veiligheid van internetdiensten

Door middel van verschillende stellingen is doorgevraagd naar het vertrouwen in de diensten die ook in Figuur 4.1 aan bod kwamen.

[21] De twee groepen ouders (kinderen 6-12 jaar en kinderen 13-18 jaar) ondervraagd in het Online Interview Panel zijn samengevoegd voor de overzichtelijkheid. Er zijn geen grote verschillen tussen deze groepen.

[22] De Digitale Economie 2008. Centraal Bureau voor de Statistiek. Den Haag, 2008. www.cbs.nl

Figuur 4.2 Geef aan in hoeverre u het eens bent met de volgende stellingen



Bron: Synovate

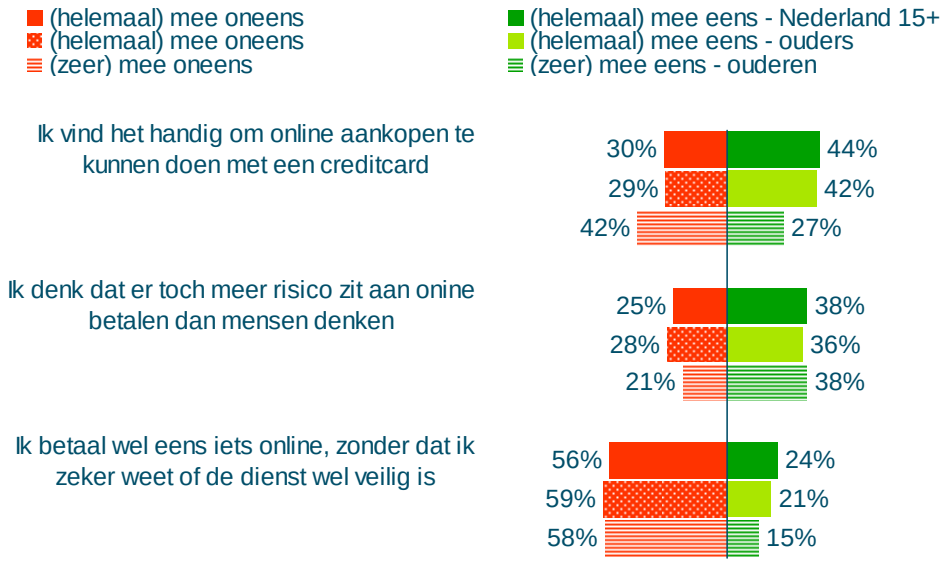
Basis: groep Nederlanders 15+ (n=288); groep ouders uit het Online Interview Panel (n=612); groep ouderen 65+ (n=349)

Internetbankieren wordt door vrijwel alle respondenten graag gebruikt (Figuur 4.2). Het vertrouwen in de veiligheid ervan is groot: zeven van de tien Nederlanders vindt internetbankieren veilig, slechts een klein percentage ziet de dienst als onveilig. Een klein percentage Nederlanders die de dienst als onveilig bestempelden, maakt toch gebruik van internet bankieren.

Meer dan driekwart van alle respondenten heeft vertrouwen in de manier waarop banken met hun gegevens omgaan. Er zijn hierbij geen grote verschillen tussen de doelgroepen.

In de volgende stellingen (Figuur 4.3) is gevraagd naar de motivatie om online te betalen en het risico dat men daarbij inschat.

Figuur 4.3 Geef aan in hoeverre u het eens bent met de volgende stellingen



Bron: Synovate

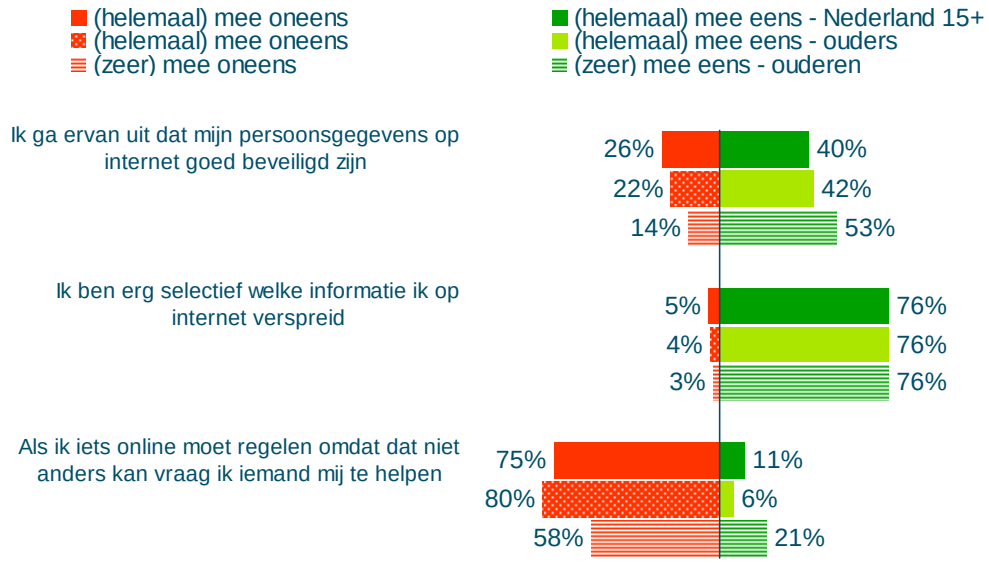
Basis: groep Nederlanders 15+ (n=288); groep ouders uit het Online Interview Panel (n=612); groep ouderen 65+ (n=349)

Ouderen maken bij het betalen online het minste gebruik van een creditcard: ongeveer een kwart van hen vindt het handig hiermee online aankopen te doen en 42% gebruikt liever geen creditcard bij online betalingen (Figuur 4.3). Ruim 40% van de Nederlanders en ouders geeft aan het handig te vinden om online met een creditcard te betalen.

De meningen over risico's van online betalen zijn verdeeld: iets minder dan vier op de tien denkt dat er meer risico's hieraan vastzitten dan vaak gedacht, terwijl een kwart dit bestrijdt. Van alle doelgroepen ontkent bijna 60% wel eens iets online te betalen, zonder zeker te weten of de dienst veilig is. Toch zegt 24% van de Nederlanders dit wel eens te doen. Voor de andere twee doelgroepen ligt dit percentage iets lager.

In de volgende stellingen is onder andere gevraagd naar het vertrouwen in de beveiliging van persoonlijke informatie (Figuur 4.4).

Figuur 4.4 Geef aan in hoeverre u het eens bent met de volgende stellingen



Bron: Synovate

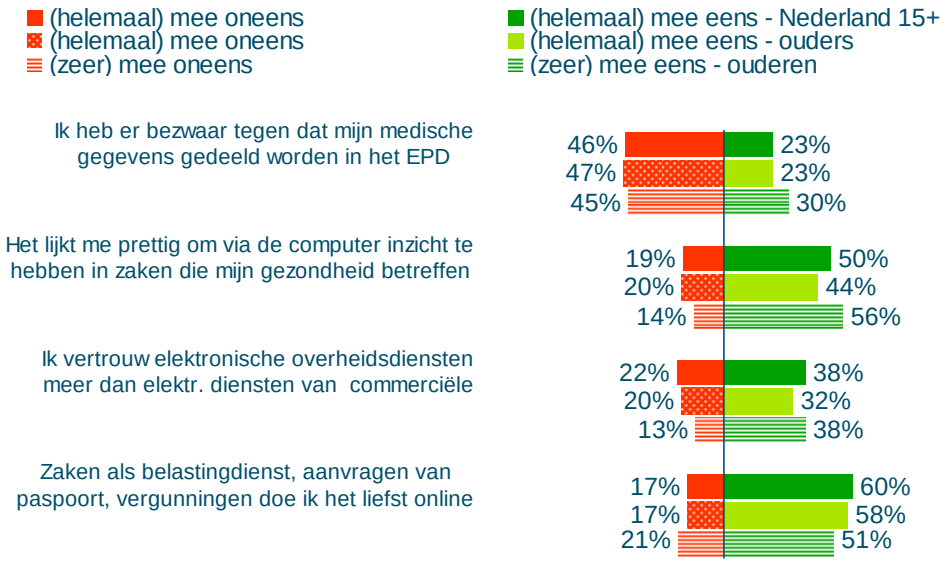
Basis: groep Nederlanders 15+ (n=288); groep ouders uit het Online Interview Panel (n=612); groep ouderen 65+ (n=349)

Een groot deel van de ondervraagde doelgroepen geeft aan vertrouwen te hebben in de beveiliging van persoonsgegevens online, bij ouderen is dit vertrouwen het grootst. Een kwart van de Nederlanders geen vertrouwen in de bescherming van haar persoonlijke gegevens. Drie kwart van alle doelgroepen geeft aan voorzichtig om te gaan met persoonlijke informatie. Ongeveer twintig procent staat neutraal ten opzichte van deze stelling.

Sommige diensten zijn alleen nog digitaal toegankelijk, denk hierbij bijvoorbeeld aan de belastingaangifte. Van de Nederlanders en ouders, geeft meer dan 75% aan hier geen hulp bij nodig te hebben. Voor de ouderen ligt dit percentage lager, 58% komt er zelf uit, 21% vraagt hulp aan een ander.

In de volgende stellingen wordt doorgegaan op het vertrouwen in diverse diensten.

Figuur 4.5 Geef aan in hoeverre u het eens bent met de volgende stellingen



Bron: Synovate

Basis: groep Nederlanders 15+ (n=288); groep ouders uit het Online Interview Panel (n=612); groep ouderen 65+ (n=349)

In 2009 worden grote stappen genomen in de richting van een Elektronisch Patiënten Dossier, waarin zorgverleners medische informatie over de patiënt bewaren en makkelijk toegankelijk maken voor collega's. Het is mogelijk om bezwaar te maken tegen het delen van deze informatie.
Bijna een kwart van de internetgebruikers heeft er bezwaar tegen dat medische gegevens gedeeld worden via het Elektronische Patiëntendossier (EPD) (Figuur 4.5). Dit is een opvallend hoog percentage gezien het feit dat slechts enkele procenten van de Nederlanders een bezwaarformulier tegen het EPD ingestuurd heeft. Ongeveer de helft van de internetgebruikers lijkt het wel prettig om zelf medische gegevens online in te kunnen zien. Voor ouderen ligt dit percentage het hoogst.

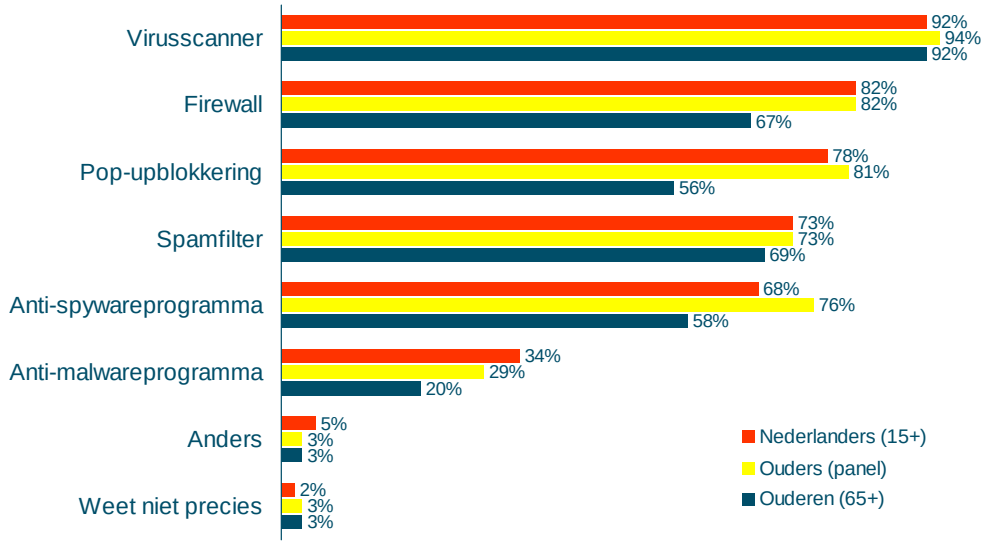
Op de vraag of men meer vertrouwen heeft in commerciële diensten of overheidsdiensten, antwoordde het grootste deel van de respondenten neutraal. Van de overige respondenten geven alle groepen aan het meest vertrouwen te hebben in digitale overheidsdiensten.

Een meerderheid geeft aan om zaken als belastingdienst, aanvragen van een paspoort en vergunningen, het liefst online te willen regelen. Voor ongeveer 20% geldt dat zij liever 'offline' deze zaken regelen. Ook ouderen geven aan het prettig te vinden om veel online te regelen, wel liggen de percentages hier iets lager dan voor de andere twee doelgroepen.

4.1.3 Beveiliging van computer tegen dreigingen

Alle groepen maken gebruik van meerdere internetdiensten. In welke mate zetten zij echter beveiligingsmiddelen in om het gebruik van deze diensten veilig te laten verlopen (Figuur 4.6)?

Figuur 4.6 Op welke manieren beveiligt u uw computer?[23]



Bron: Synovate

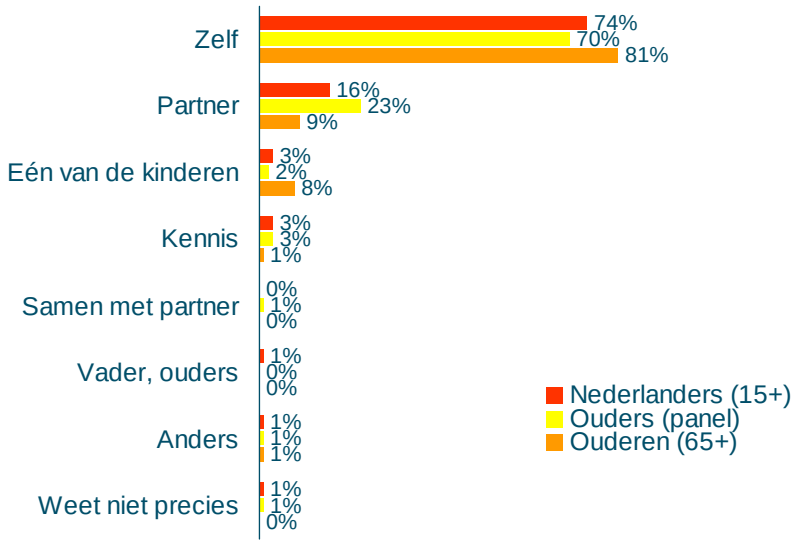
Basis: groep Nederlanders 15+ (n=288); groep ouders uit het Online Interview Panel (n=612); groep ouderen 65+ (n=349)

Bijna iedereen gebruikt een virusscanner en ook hebben veel internetgebruikers een firewall om de risico's bij internetten te verkleinen De laatste wordt wel minder gebruikt door ouderen. Ouderen maken van alle genoemde applicaties het minst gebruik. Ouders wijken weinig af van de gemiddelde Nederlanders. Opvallend is wel dat zij vaker software installeren om *spyware* te bestrijden.

Aan de respondenten is gevraagd wie er in het huishouden verantwoordelijk werd gehouden voor de beveiliging van de computer (Figuur 4.7).

[23] De functionaliteiten van de verschillende genoemde producten overlappen elkaar. Een virusscanner doet vaak meer dan alleen virussen weren en functioneert vaak als een anti-malware programma. Gekozen is om termen te gebruiken die voor mensen herkenbaar zijn.

Figuur 4.7 Wie is er thuis verantwoordelijk voor de beveiliging van uw computer?



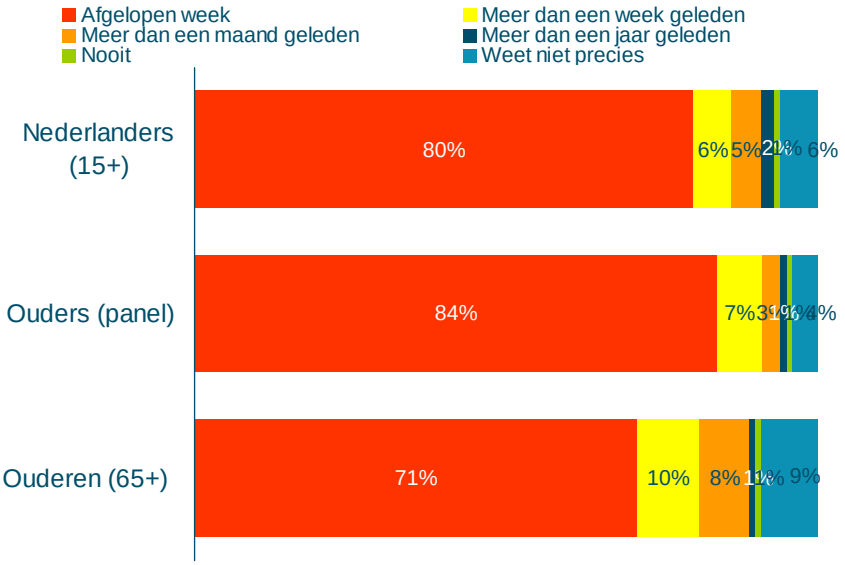
Bron: Synovate

Basis: groep Nederlanders 15+ (n=288); groep ouders uit het Online Interview Panel (n=612); groep ouderen 65+ (n=349)

Het merendeel van de respondenten geeft aan zelf verantwoordelijk te zijn voor de beveiliging van de pc. Bij ouderen ligt dit percentage het hoogst. In de meeste andere gevallen zijn dat de partners. Opvallend is dat 8% van de ouderen geeft te kennen dat de kinderen de beveiliging van de computer regelen.

Ook vroegen we de respondenten wanneer zij hun computer voor het laatst controleerden op gevaren van buitenaf (Figuur 4.8).

Figuur 4.8 Wanneer is uw computer voor het laatst gecontroleerd op virussen etc.?



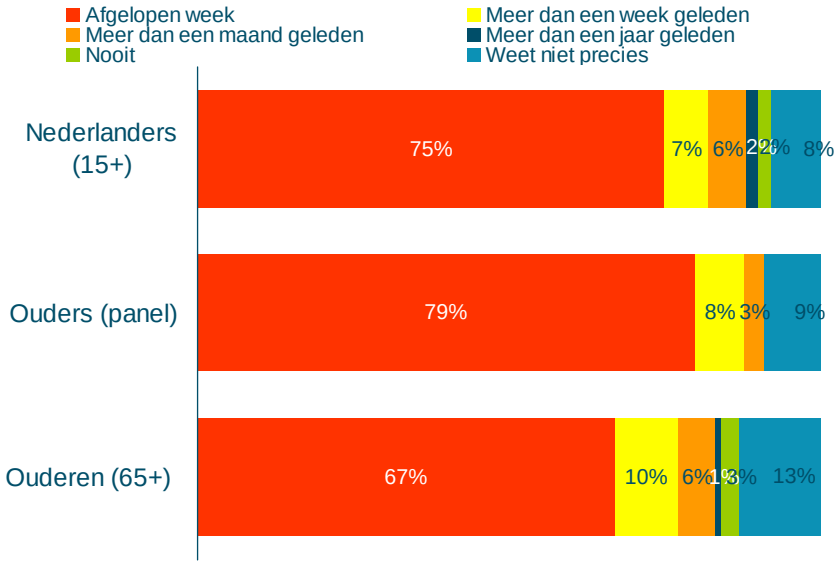
Bron: Synovate

Basis: groep Nederlanders 15+ (n=288); groep ouders uit het Online Interview Panel (n=612); groep ouderen 65+ (n=349)

In de week voorafgaand aan het onderzoek heeft 80% van de respondenten inde doelgroep Nederlanders de computer gecontroleerd op virussen. Bij ouders lag dit percentage nog iets hoger (84%) en bij ouderen lager (71%). Van de ouderen gaf 10% aan niet precies te weten wanneer de computer voor het laatst gescand was.

Ook updates van beveiligingssoftware zijn bij de meeste gebruikers van internet recent uitgevoerd (Figuur 4.9). Ook voor updates geldt dat ouderen deze iets minder gebruiken dan andere groepen. Dit is opvallend omdat ouderen het vaakst zelf verantwoordelijk zijn voor de beveiliging van de computer.

Figuur 4.9 Wanneer zijn er voor het laatst updates (of patches) van uw beveiligingssoftware gedownload?



Bron: Synovate

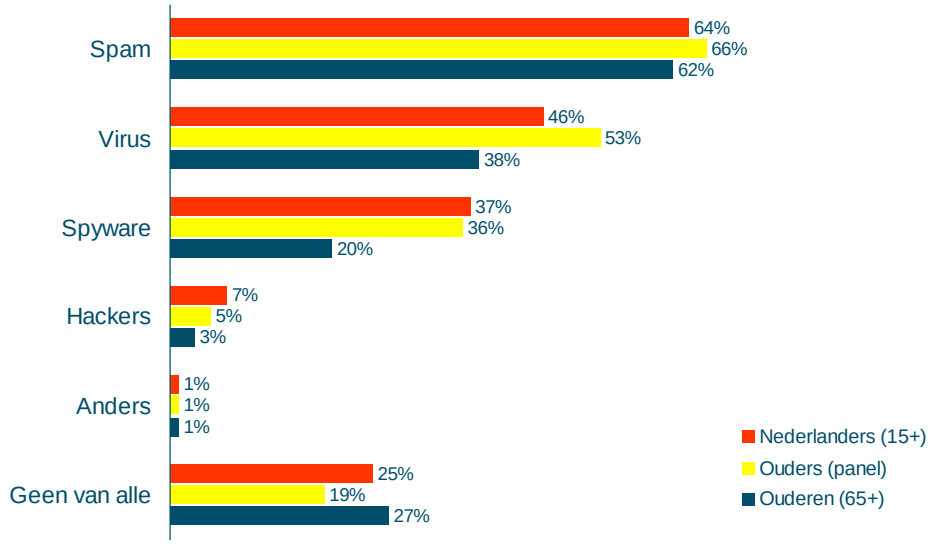
Basis: groep Nederlanders 15+ (n=288); groep ouders uit het Online Interview Panel (n=612); groep ouderen 65+ (n=349)

Een groot deel van de ondervraagden weert zich tegen dreigingen door het gebruik van een virusscanner. Het installeren van dergelijke software is echter niet genoeg. Om goed beveiligd te zijn is het noodzakelijk om zeer regelmatig de updates van de beveiliging te installeren. Ongeveer 10% van de respondenten geeft aan niet precies te weten wanneer dat voor het laatst gebeurd is.

4.1.4 Ondervonden hinder van dreigingen

Dreigingen worden vaak pas tastbaar als men er zelf ook hinder van ondervindt. In de vorige paragraaf is ingegaan op de manier waarop mensen hun computer beveiligen om zich te wapenen tegen schadelijke invloeden van buitenaf. Toch is dit mogelijk niet altijd afdoende. In deze paragraaf lichten we toe in hoeverre mensen, ondanks de vormen van beveiliging ook daadwerkelijk last hebben van verschillende veiligheidsdreigingen.

Figuur 4.10 Heeft u wel eens last gehad van...

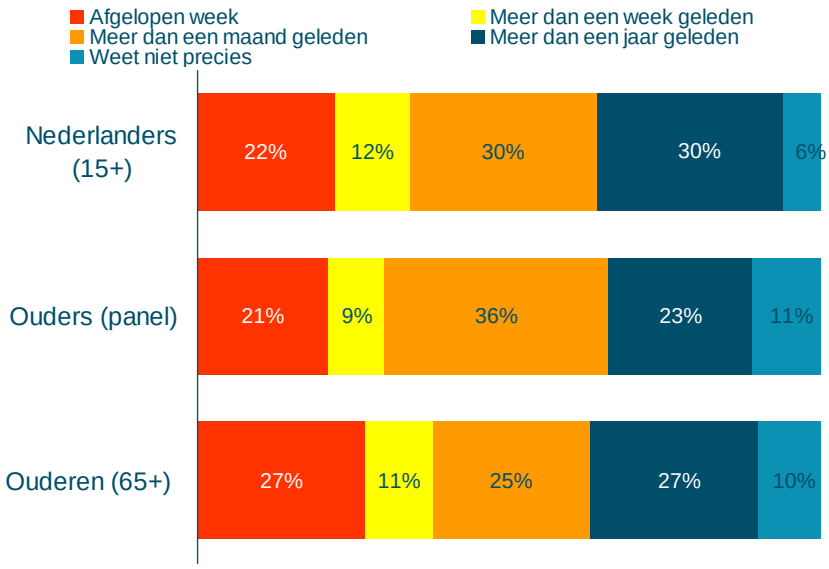


Bron: Synovate
Basis: groep Nederlanders 15+ (n=288); groep ouders uit het Online Interview Panel (n=612); groep ouderen 65+ (n=349)

Onder alle doelgroepen heeft ongeveer twee derde wel eens last gehad van spam. Een kwart van de Nederlanders en ouderen geeft aan nog nooit last te hebben gehad van een van bovenstaande dreigingen (of zich daar niet bewust van te zijn). Verder valt op dat ouders meer last hebben gehad van virussen en spam dan de andere doelgroepen. Dit zou te verklaren kunnen zijn door de toenemende hoeveelheid malware bij web2.0 toepassingen en games, wat vooral populair is onder kinderen en jongeren.

Aan de respondenten die te kennen gaven wel eens last te hebben van deze dreigingen, is gevraagd wanneer zij voor het laatst hiermee geconfronteerd zijn (Figuur 4.11).

Figuur 4.11 Wanneer heeft u voor het laatst gehad van een van onderstaande dreigingen?



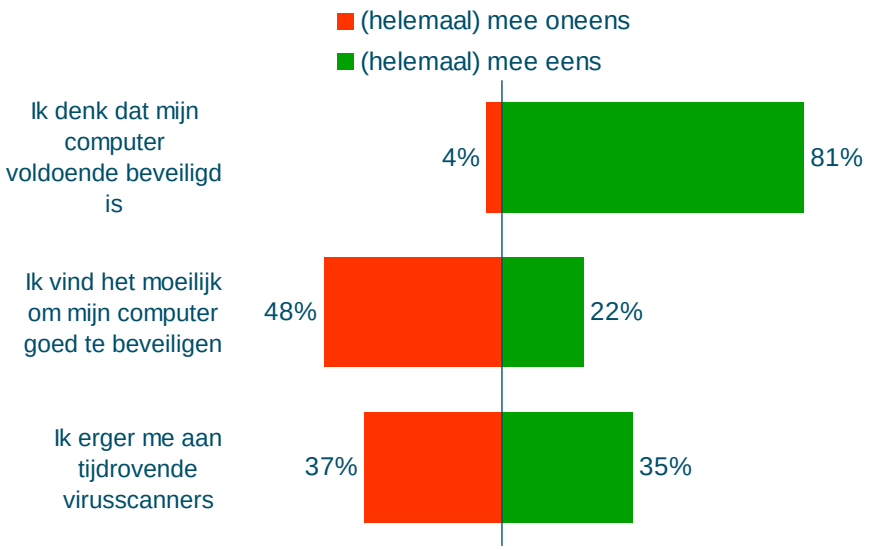
Bron: Synovate
Basis: heeft wel eens last gehad van een of meer dreigingen. Groep Nederlanders 15+ (n=217); groep ouders uit het Online Interview Panel (n=495); groep ouderen 65+ (n=255)

Voor alle doelgroepen geldt dat meer dan 20% van de respondenten in de week voorafgaand aan het onderzoek last heeft gehad van spam, virussen, spyware, hackers, of andere dreigingen. In 20-30% van de gevallen geldt dat dit al langer dan een jaar geleden was.

4.1.5 Algemeen veiligheidsgevoel

In bovenstaande paragrafen is onder andere gevraagd naar de hinder die de respondenten ondervonden van spam en virussen, hoe zij hun computer beschermen en welke diensten zij zoal gebruiken. In de komende stellingen wordt verder doorgevraagd hoe zij zelf hun veiligheid beleven en ervaren.[24]

Figuur 4.12 Geef aan in hoeverre u het eens bent met de volgende stellingen



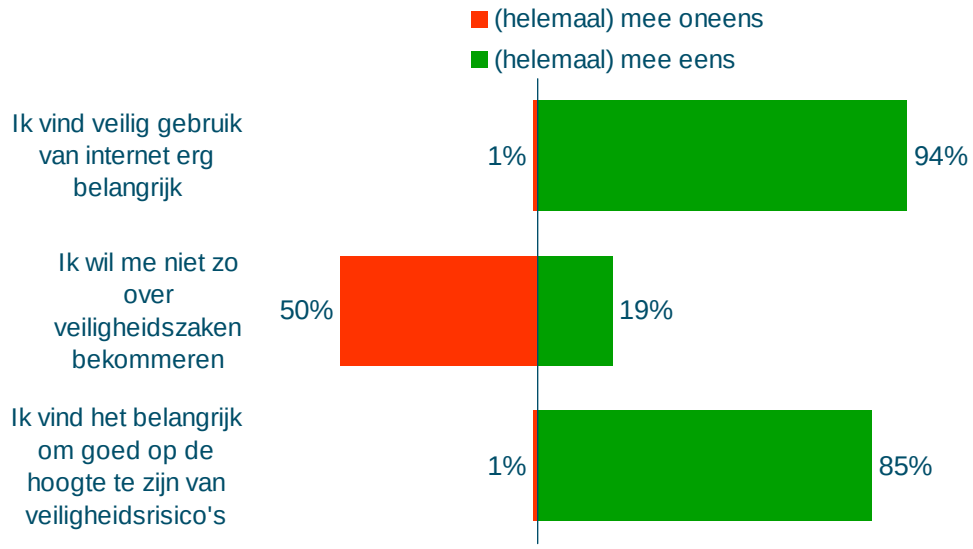
Bron: Synovate
Basis: Nederlanders 15+ (n=288)

Van de Nederlandse internetgebruikers geeft 81% aan voldoende vertrouwen te hebben in de beveiliging van de eigen computer (Figuur 4.12). Slechts 4% denkt dat de beveiliging onvoldoende is, 15% stemde neutraal. Bijna de helft van de internetgebruikers geeft aan geen moeite te hebben om de computer goed te beveiligen. Voor 22% van de internetgebruikers is dit nog wel lastig. Tijdrovende virusscanners zijn in 35% van de gevallen een storende factor, maar een kleine meerderheid geeft aan hier geen last van te hebben.

Hoe belangrijk zijn veiligheidszaken voor de internetgebruikers?

[24] De vragen zijn voorgelegd aan alle doelgroepen, maar er ontstonden hier geen significante verschillen. We bespreken de resultaten van de groep ‘Nederlanders’.

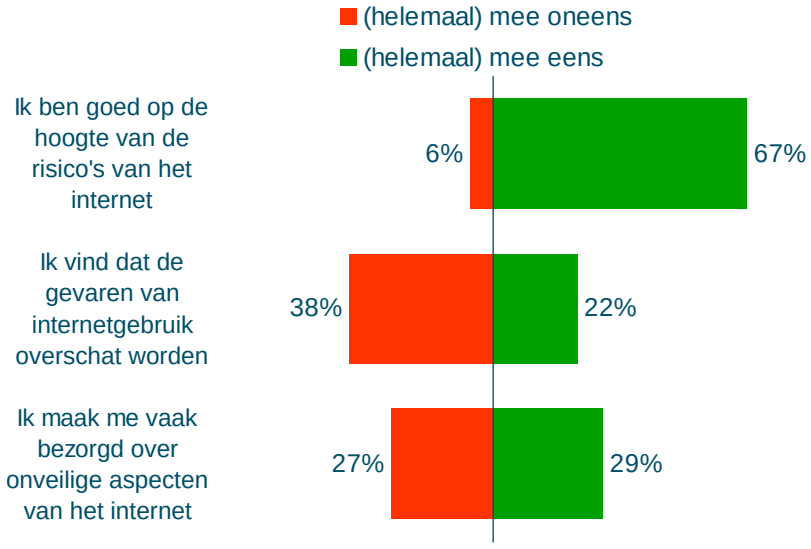
Figuur 4.13 Geef aan in hoeverre u het eens bent met de volgende stellingen



Bron: Synovate
Basis: Nederlanders 15+ (n=288)

Uit Figuur 4.13 blijkt dat een zeer groot deel van de internet gebruikers het belangrijk vindt om op de hoogte te zijn van veiligheidsrisico's (85%). Van de internetters vindt 94% veilig internet dan ook erg belangrijk. Toch zegt bijna 20% zich er eigenlijk niet zo over te willen bekommeren. De helft van de internetgebruikers wil dit nadrukkelijk wel. Er is dus nog een grote groep over die daar neutraal tegenover staat.

Figuur 4.14 Geef aan in hoeverre u het eens bent met de volgende stellingen



Bron: Synovate
Basis: Nederlanders 15+ (n=288)

Twee derde van de internetgebruikers acht zichzelf goed op de hoogte van de gevaren van het internet. Echter 22% vindt dat de gevaren overschat worden, terwijl 38% van menig is dat de gevaren helemaal niet worden overschat. Bijna 30% geeft aan zich echt

zorgen te maken over onveilige aspecten. Uit recent onderzoek van Unisys blijkt dat Nederlanders zich zeer onbezorgd opstellen tegenover veiligheid in ICT. Nederland komt zelfs uit de bus als het meest onbezorgde land van de wereld. Op een schaal van 0-300 scoort Nederland 89 punten en daarmee maken we ons weinig zorgen over internetveiligheid.[25]

4.2 Ouders

In deze paragraaf bespreken we de resultaten van het onderzoeksgedeelte dat zich richtte op ouders. De meeste vragen richtten zich op het internetgedrag van de kinderen en de eventuele zorgen die ouders hebben bij dit gedrag.

Eerst worden de zorgen die ouders hebben over hun internettende kind besproken. Vervolgens komen nog aan bod; het internetgebruik van de kinderen, controle door ouders, kennis en informatievergaring en de voorlichting van kinderen. In de laatste paragraaf vergelijken we hoe de gemiddelde ouder zich verhoudt tot het externe panel van ouders die actief zijn op de website van Ouders Online.

4.2.1 Ouders en hun zorgen

Van alle ouders zegt gemiddeld 45% zich wel eens zorgen te maken als een kind op internet is. Het verschil tussen ouders met jonge kinderen en ouders met jongeren is slechts twee procent. Ouders van jongeren maken zich iets meer zorgen. Aan de bezorgde ouders is gevraagd of ze hun zorgen kort toe wilden lichten. Grofweg zijn er een aantal hoofdzorgen te onderscheiden. De ouders van de jongere kinderen maken zich vooral veel zorgen om onwenselijke *content* die te makkelijk voor handen is. *"Het is vrij eenvoudig om de gekste dingen op het scherm te krijgen", "..1x klikken en het kan mis zijn"*. Een andere grote zorg van deze ouders is de confrontatie van hun kind met individuen die *"…niet zijn wie ze zeggen te zijn"*.

Diezelfde zorg wordt ook veel genoemd in het panel met ouders met oudere kinderen. *"Er zijn genoeg gekken die contact kunnen zoeken met een kind of puber. Zeker via allerlei chatprogramma's! Nu weet ik wel dat kinderen die persoon zelf moeten toevoegen aan hun MSN om maar iets te noemen, maar toch, vaak gaat dat makkelijk, die persoon kan al een vriend of vriendin kennen van je kind en dan den kt je kind dat het vertrouwd is, wat dus helemaal niet zo hoeft te zijn."*

Ook zijn er zorgen geuit over de bescherming van persoonlijke informatie. *"Ze zet in mijn ogen teveel informatie op het internet, op bijvoorbeeld een site als Hyves. Gaat dan om achternaam en de naam en locatie van de school waar ze op zit"* Deze zorg werd regelmatig uitgesproken. Minder, maar ook genoemd is cyberpesten, schadelijke downloads en zorgen als verslavingen en gebrek aan beweging.

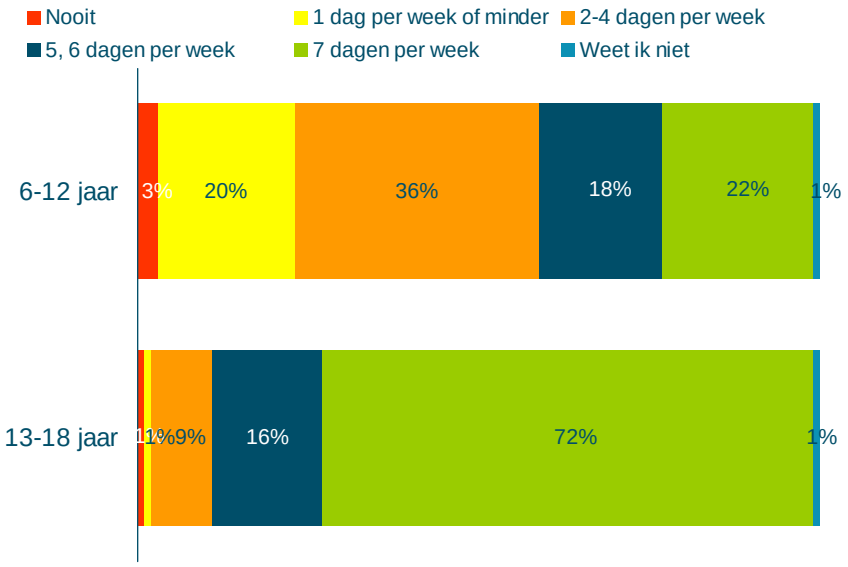
4.2.2 Internet gebruik van de kinderen

Bij een derde van de ouders met kinderen tussen 6 en twaalf jaar heeft het kind de beschikking over een eigen pc of laptop met internettoegang. Bij ouders van kinderen

[25] http://www.unisyssecurityindex.com/netherlands/

tussen 13 en 18 jaar ligt dit aandeel op driekwart. Aan de ouders is gevraagd hoeveel uur per week de kinderen zich op internet begeven (Figuur 4.15).

Figuur 4.15 Op hoeveel dagen van de week maakt uw kind van [leeftijd] thuis of ergens anders gewoonlijk gebruik van internet?



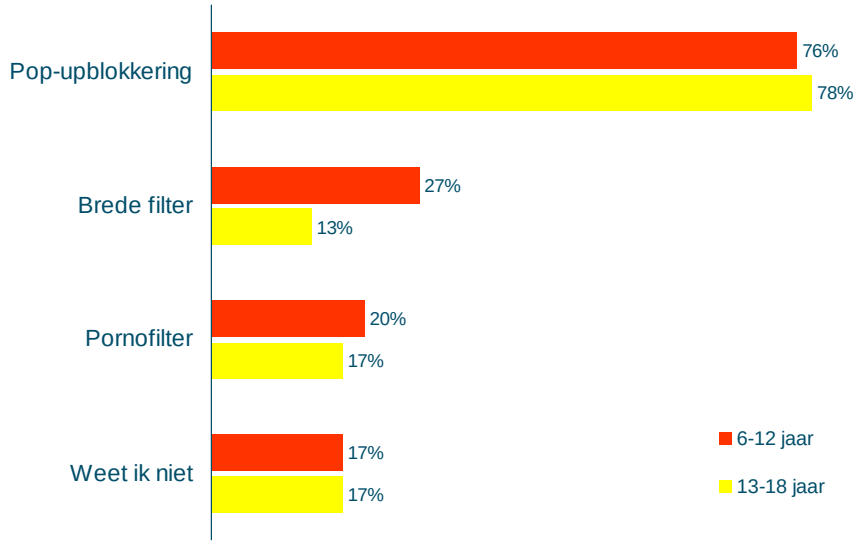
Bron: Synovate:
Basis: ouders van kinderen tussen 6 en 12 jaar (n=310); ouders van kinderen tussen 13 en 18 jaar (n=302).

Van de kinderen tussen 13 en 18 jaar internet 72% elke dag en nog eens zestien procent is vijf à zes dagen online te vinden. Van de jongere kinderen is 22% dagelijks online en ongeveer een kwart 1 dag per week of minder.

4.2.3 Gebruik van filters en controle

Aan de ouders is gevraagd of zij van technische middelen gebruik maken om hun kinderen te beschermen tegen ongewenste informatie (Figuur 4.16).

Figuur 4.16 Maakt u gebruik van een filter met onderstaande functionaliteiten?



Bron: Synovate
Basis: ouders van kinderen tussen 6 en 12 jaar (n=310); ouders van kinderen tussen 13 en 18 jaar (n=302).

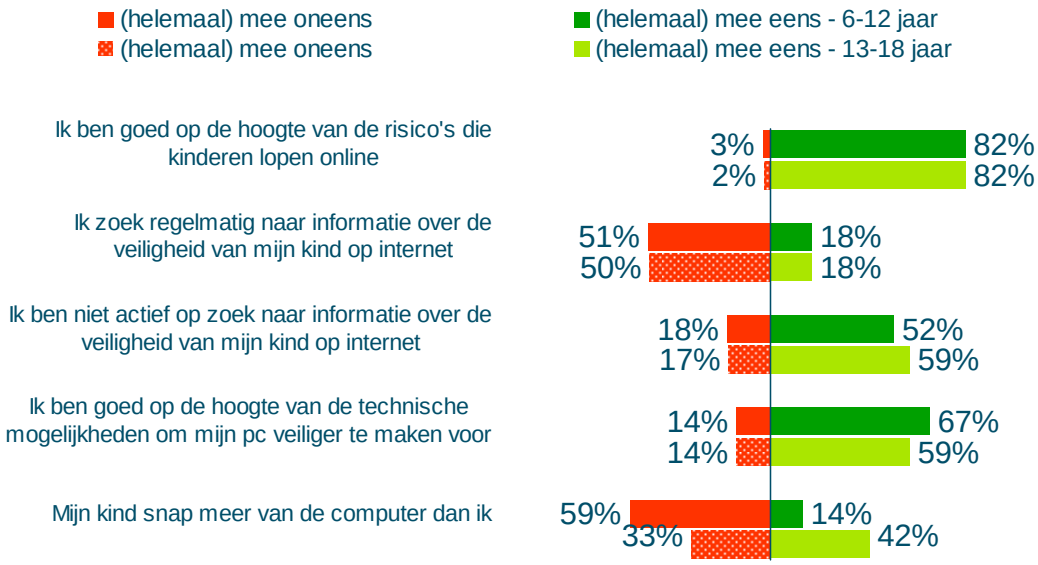
Pop-ups worden op grote schaal geweerd, deze functionaliteit zit ingebouwd in de meeste browsers. Ruim drie kwart van de ouders geeft aan pop-ups te blokkeren. Voor de jongere kinderen wordt meer gefilterd dan voor de oudere kinderen. Een kwart van de ouders van jonge kinderen geeft aan een filter te gebruiken die hun kinderen bijvoorbeeld ook beschermd tegen betaal- en goksites. Dit percentage ligt duidelijk lager bij de ouders met pubers. Ongeveer een vijfde van alle ouders gebruikt een pornofilter. Bijna hetzelfde aantal ouders weet niet precies welke filters ze gebruiken of gebruikt er geen. Van de ouders met jongere kinderen vindt 34% het expliciet niet nodig om gebruik te maken van een filter.

4.2.4 Eigen kennis en informatievergaring

Bijna de helft van alle ouders (45%) maakt zich wel eens zorgen als hun kind op internet is. Dit geldt zowel voor de ouders van pubers als van jongere kinderen. Het merendeel van de ouders maakt zich echter geen zorgen. In deze paragraaf gaan we dieper in op de kennis die ouders hebben van mogelijke risico’s online en de manier waarop zij aankijken tegen de voorlichting over deze risico’s.

Door middel van de volgende stellingen is gevraagd hoe ouders zelf aankijken tegen hun eigen kennis over veiligheidsissues op internet.

Figuur 4.17 Geef aan in hoeverre u het eens bent met de volgende stellingen

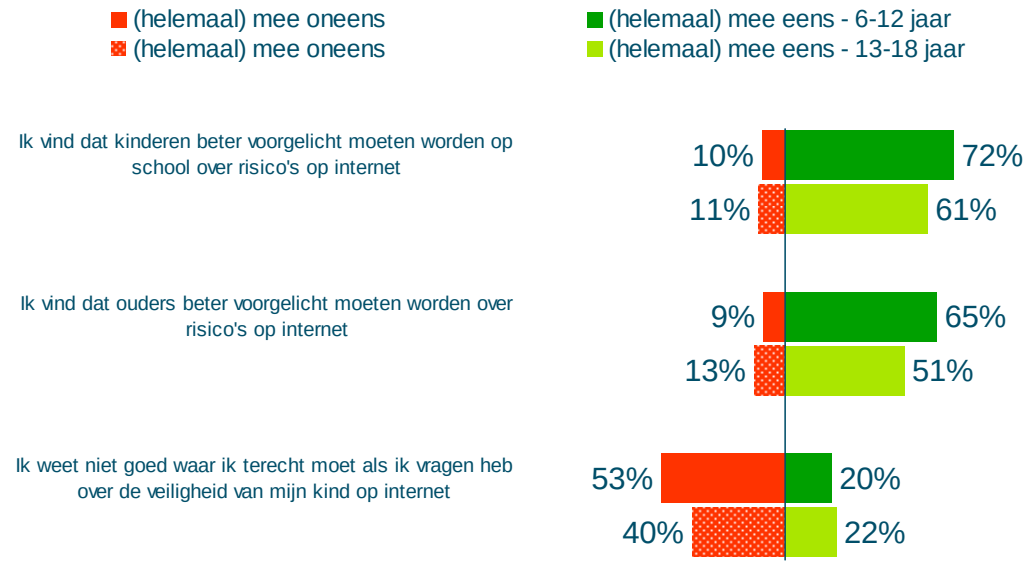


Bron: Synovate
Basis: ouders van kinderen tussen 6 en 12 jaar (n=310); ouders van kinderen tussen 13 en 18 jaar (n=302).

Ruim 80% van de ouders acht zich goed op de hoogte van de risico's die kinderen lopen online. Minder zeker is men over de eigen kennis om de computer technisch beter te beveiligen. Van de ouders schat 14% de kennis op dit vlak zelfs onvoldoende. Toch maakt ook een ruime meerderheid zich hier geen zorgen over. Meer dan de helft van de ouders is niet zelf actief op zoek naar extra informatie om zich beter te laten informeren. Bijna twintig procent doet dit wel. 40% Van de ouders met een puber thuis schat dat hun kind meer van de computer af weet dan zij zelf. Ouders met jongere kinderen bestrijden dit met een ruime meerderheid (59%), 14% ondersteunt de stelling.

Aan de ouders is ook gevraagd of zij extra voorlichting, voor zowel ouders als kinderen, nodig achten.

Figuur 4.18 Geef aan in hoeverre u het eens bent met de volgende stellingen

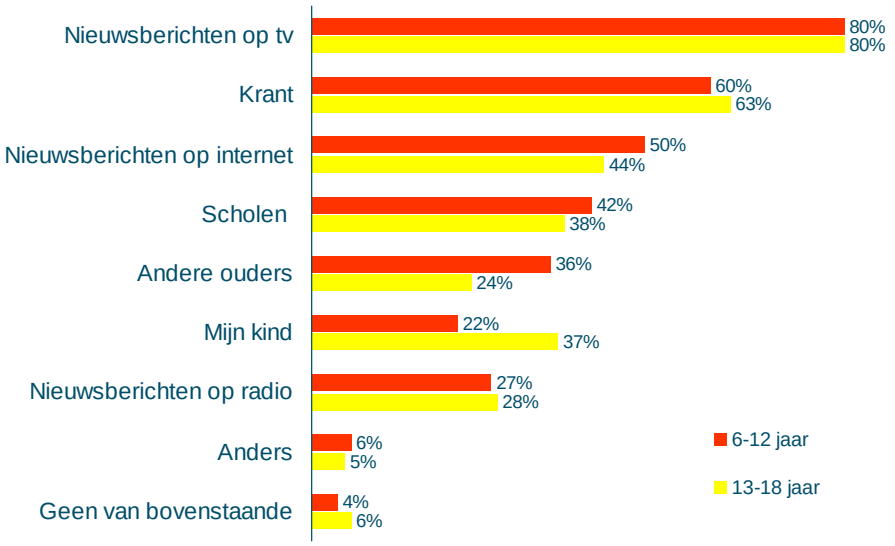


Bron: Synovate
Basis: ouders van kinderen tussen 6 en 12 jaar (n=310); ouders van kinderen tussen 13 en 18 jaar (n=302).

Van de ouders acht 80% zichzelf goed geïnformeerd. Toch vindt ook een meerderheid van beide groepen ouders dat ouders beter voorgelicht moeten worden. Ongeveer een vijfde van beide groepen geeft aan dat zij niet goed weten waar ze met vragen terecht moeten. 53% Van de ouders met jonge kinderen weet dat wel, voor de ouders met pubers is dit percentage iets lager, namelijk 40%.
Een ruime meerderheid van beide groepen ouders vindt dat ook de school meer initiatief kan nemen tot voorlichting op dit onderwerp. Slechts een op de tien ouders is het hier nadrukkelijk niet mee eens.

In de volgende figuur is weergegeven via welke kanalen ouders hun huidige kennis hebben opgedaan.

Figuur 4.19 Via welke informatiekanalen hoort u wel eens over de risico's die kinderen online lopen?

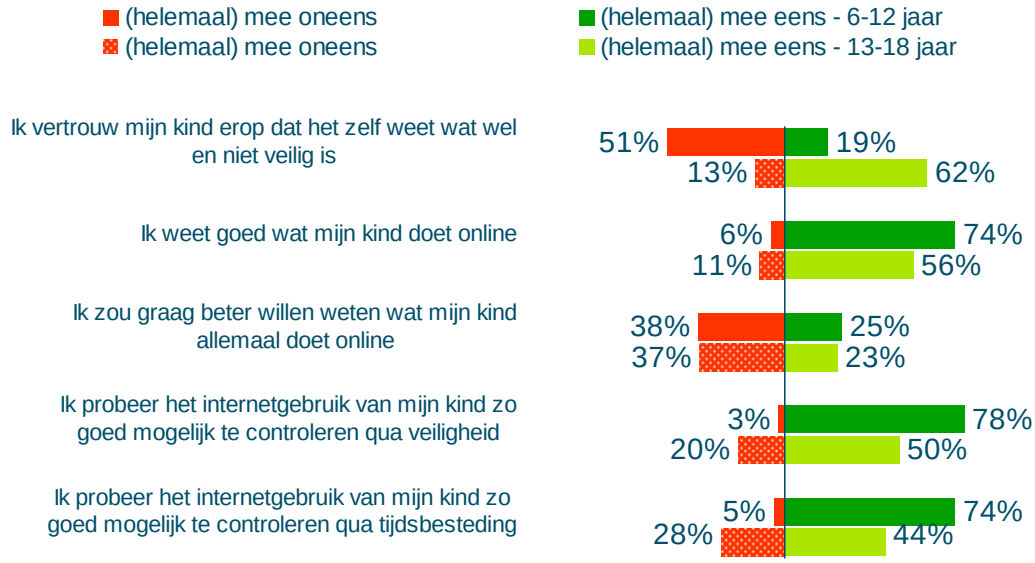


Bron: Synovate
Basis: ouders van kinderen tussen 6 en 12 jaar (n=310); ouders van kinderen tussen 13 en 18 jaar (n=302).

De massamedia hebben een groot aandeel in de informatievoorziening rond veiliginternet. Nieuws op televisie speelt hierbij een grote rol. Dit medium bereikt 80% van de ondervraagden als het gaat om informatie over internetveiligheid. Ook de krant en het internet hebben een groot aandeel. Ongeveer 40% van beide doelgroepen zegt ook informatie te ontvangen via de scholen. Ouders met jongere kinderen praten vaker onderling over de risico's dan ouders van pubers. Deze ouders krijgen echter vaker informatie van het kind zelf.

Eerder werd al ingegaan op de mogelijkheden om via technische middelen de kinderen te beschermen tegen ongewenste surfeffecten. In de volgende stellingen is aan de ouders gevraagd in hoeverre ze zelf controle uitoefenen op het surfgedrag.

Figuur 4.20 Geef aan in hoeverre u het eens bent met de volgende stellingen



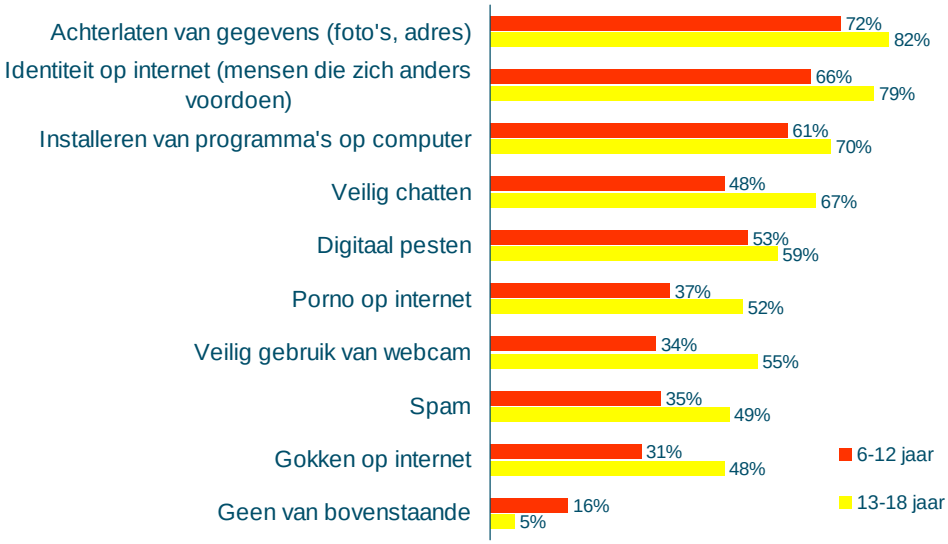
Bron: Synovate
Basis: ouders van kinderen tussen 6 en 12 jaar (n=310); ouders van kinderen tussen 13 en 18 jaar (n=302).

Het merendeel van de ouders met kinderen in de leeftijd 13-18 vertrouwt erop dat hun kinderen zelf al over voldoende kennis beschikken om de afweging te maken tussen wat wel en niet veilig is. Van deze groep ouders controleert 44% hoeveel tijd hun kind online besteedt en 50% probeert te controleren of hun kind verantwoord gebruik maakt van het internet. Ouders met jongere kinderen doen dit in meer gevallen. De tijdsbesteding van de kinderen wordt in 74% van de gevallen gecontrolleerd en de veiligheid van het gedrag in 78% van de gevallen. Bijna een kwart van alle ouders zou beter willen weten wat de kinderen doen online. Bijna 40% bestrijdt deze stelling echter en acht zich al voldoende op de hoogte. Van de ouders met jongere kinderen zegt 74% al goed te weten wat hun kind online doet. Dit percentage ligt bij ouders met de oudere kinderen op 56%.

4.2.5 Praten met kinderen

Hoewel het merendeel van de ouders zich niet direct zorgen maakt, vindt een nog grotere meerderheid het onderwerp wel van belang. Door middel van diverse stellingen is aan ouders gevraagd hoe zij zelf het onderwerp met hun kinderen behandelen.

Figuur 4.21 Over welk van de volgende onderwerpen praat u met uw kind?

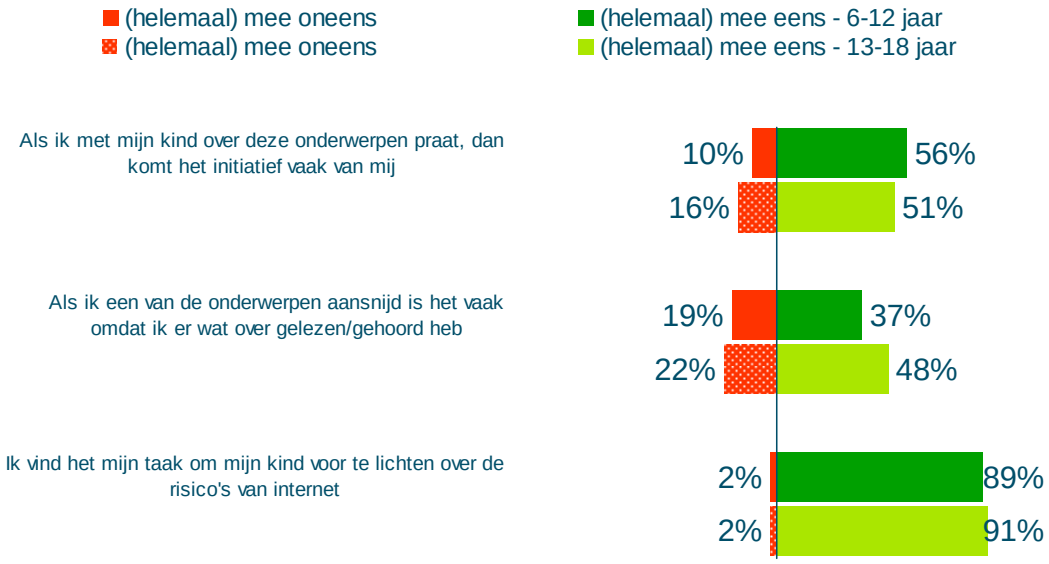


Basis: ouders van kinderen tussen 6 en 12 jaar (n=310); ouders van kinderen tussen 13 en 18 jaar (n=302).

Over alle genoemde onderwerpen wordt met jongeren vaker gesproken dan met de jongste kinderen. De verschillen zijn het grootst bij de onderwerpen veilig chatten, gebruik van webcams en gokken op internet. Bij digitaal pesten is het verschil het kleinst.

Eerder zagen we al dat veel ouders meenden dat scholen hun kinderen beter zouden moeten voorlichten. In onderstaande stellingen is gevraagd naar de eigen verantwoordelijkheden.

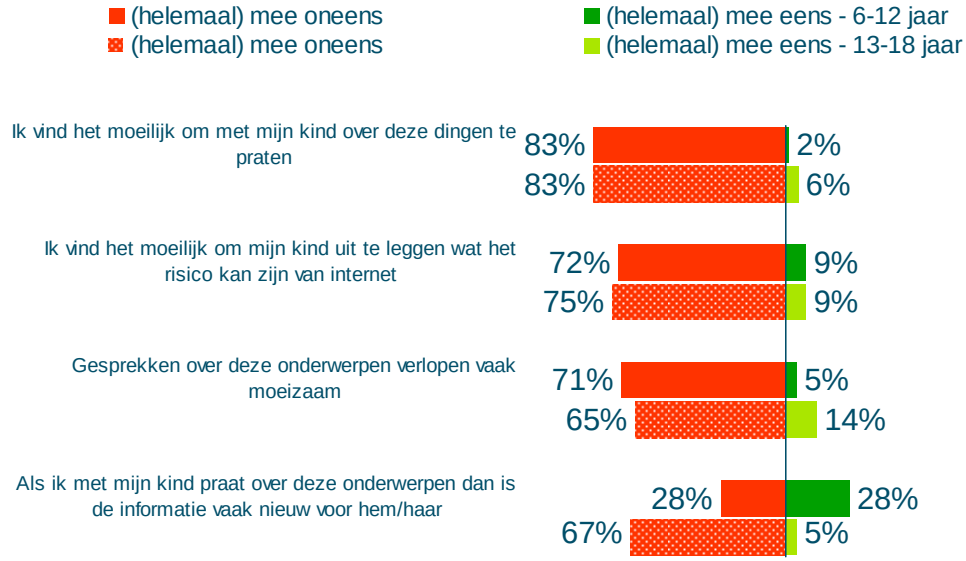
Figuur 4.22 Geef aan in hoeverre u het eens bent met de volgende stellingen



Bron: Synovate
Basis: ouders van kinderen tussen 6 en 12 jaar (n=310); ouders van kinderen tussen 13 en 18 jaar (n=302).

Bijna alle ouders zien het als hun taak om met hun kinderen over de gevaren van internetgebruik te praten. Voor de helft van de ouders geldt dat zij het initiatief tot een gesprek over de risico's van internet nemen. In een minderheid van de gevallen gaat het initiatief niet van de ouder uit. Bijna de helft van de ouders van jongeren praat vaak met het kind naar aanleiding van een bericht in de actualiteit. Bij ouders van jongere kinderen ligt dit percentage lager (37%).

Figuur 4.23 Geef aan in hoeverre u het eens bent met de volgende stellingen

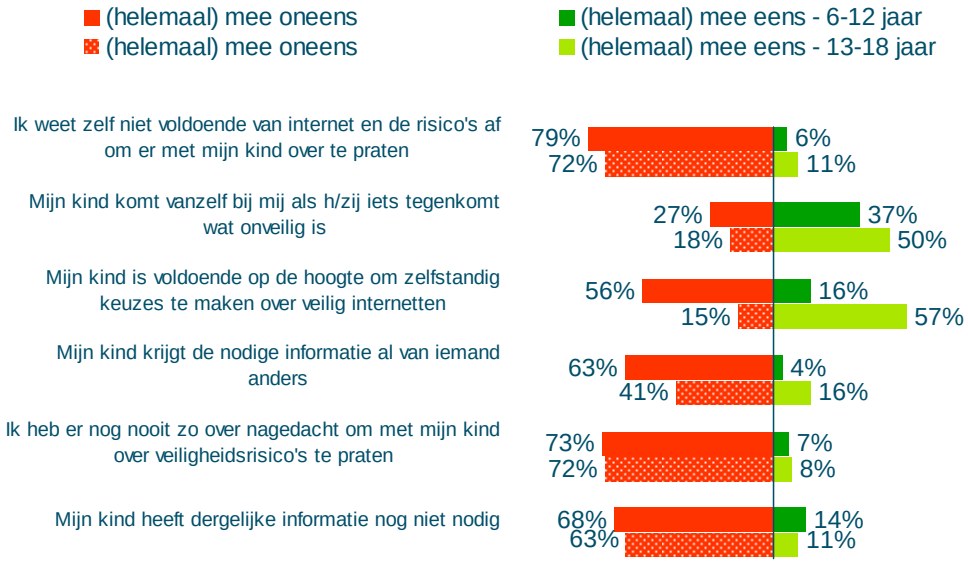


Bron: Synovate

Basis: ouders van kinderen tussen 6 en 12 jaar (n=310); ouders van kinderen tussen 13 en 18 jaar (n=302).

Ouders vinden het over het algemeen niet moeilijk om met hun kind over veiligheid en internet te praten (Figuur 4.23)Ook het duidelijk maken van de risico's aan hun kind vinden zij in de meeste gevallen niet moeilijk. De gesprekken verlopen over het algemeen niet moeizaam. Ouders van pubers geven wat vaker aan dan ouders van jonge kinderen dat gesprekken over veiligheid moeizaam gaan. Niet geheel verrassend is, dat de informatie die ouders in dergelijke gesprekken geven voor pubers meestal niet nieuw is en voor jonge kinderen relatief vaak juist wel nieuw is.

Figuur 4.24 Geef aan in hoeverre u het eens bent met de volgende stellingen



Bron: Synovate
Basis: ouders van kinderen tussen 6 en 12 jaar (n=310); ouders van kinderen tussen 13 en 18 jaar (n=302).

Het merendeel van de ouders (79%, 72%) acht zich voldoende geïnformeerd om het gesprek met het kind aan te gaan. Een ongeveer even grote groep bestrijdt dan ook de stelling dat ze er nooit zo aan gedacht hebben om dit onderwerp met hun kind te bespreken. Van de ouders met jongeren vindt 57% dat het kind zelf al voldoende op de hoogte is. Van deze ouders verwacht 50% dan ook dat het kind zelf initiatief neemt tot een gesprek als hij met dreigingen te maken krijgt. Bij de ouders met jongere kinderen ligt dit percentage op 37%.

4.2.6 Panel van Ouders online

Naast de representatieve groep ouders met kinderen in de leeftijdscategorieën 6-12 jaar en 13-16 jaar, heeft er ook een extern panel deelgenomen aan dit onderzoek. 228 Respondenten die regelmatig de site Ouders Online bezoeken zijn vergeleken met de overige ouders. Reden van deze vergelijking is om te kijken of er een verschil zit in de perceptie van beide groepen, met in het achterhoofd dat de ouders van Ouders Online via die *community* toegang hebben tot informatie en adviezen over de veiligheid van kinderen online. In deze paragraaf lichten we kort toe waar er significante verschillen gevonden zijn.

- Achtergrond

Over de achtergrond van dit panel kan worden gezegd dat deze ouders jonger zijn, hoger opgeleid, vaker vrouw, een meer links politieke voorkeur hebben en jongere kinderen hebben dan de ouders in het algemene panel.

- Filters
  Ouders van Ouders Online maken vaker gebruik van brede filters en vinden het ook vaker nodig om filters in te zetten om hun (veelal jongere kinderen) te beschermen.
- Kennis

Ouders van Ouders Online zoeken vaker actief naar informatie over de veiligheid van hun kinderen online. Ze zeggen die informatie ook gemakkelijker te kunnen vinden. Ze halen de informatie vaker van internet dan andere ouders.

- Voorlichting
  De ouders van Ouders Online praten minder met hun kinderen over de genoemde onderwerpen. Dit hangt mogelijk samen met het gegeven dat de kinderen van deze ouders relatief jong zijn. Deze ouders vinden ook dat ouders zelf beter voorgelicht moeten worden.
- Controle
  De ouders van ouders online hebben minder vertrouwen in het eigen inschattingsvermogen rondom risico's van het kind (ook hier zit mogelijk een verklaring door het leeftijdsverschil) en zijn naar eigen inschatting beter op de hoogte van de activiteiten van hun kinderen online. Ook proberen ze het internetgedrag van de kinderen actiever in de gaten te houden, zowel qua veiligheid als qua tijdsbesteding.

4.3 Senioren

In oktober 2007 kwam het Sociaal Cultureel Planbureau met een rapport dat onder andere ingaat op het internet gebruik van senioren. Deze groep is steeds vaker online, maar voor vele was desinteresse en gebrek aan kennis een van de hoofdredenen om zich niet op het internet te wagen[26].

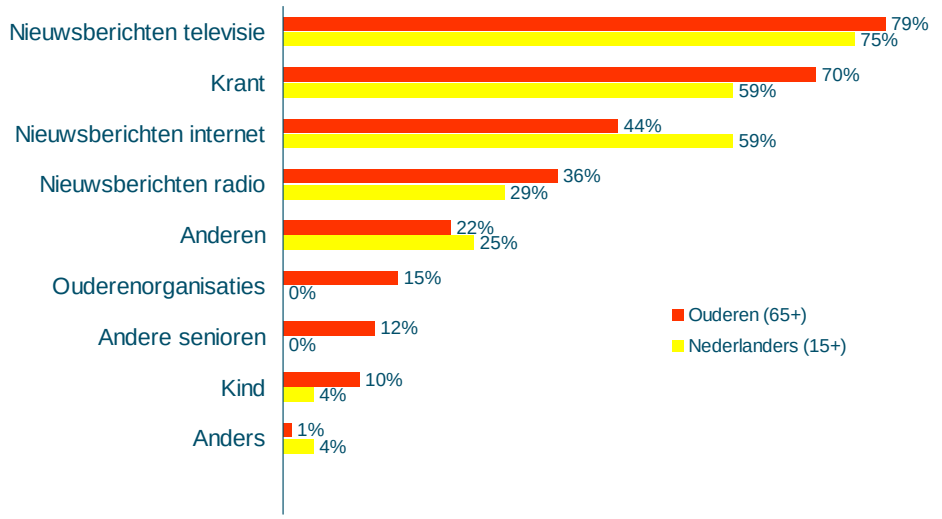
In dit hoofdstuk bekijken we hoe ouderen van 65 jaar en ouder aan informatie komen over veiligheid op internet, hoeveel kennis zij erover denken te hebben en hoe veilig zij zich op internet voelen. De resultaten worden steeds afgezet tegenover Nederlanders van 15 jaar en ouder.

4.3.1 Informatievergaring

In Figuur 4.25 is weergegeven via welke kanalen ouderen zich informeren over risico's op internet.

[26] Sociaal Cultureel Planbureau, *Achterstand en afstand. Digitale vaardigheden van lager opgeleiden, ouderen, allochtonen en inactieven.* Den Haag, oktober 2007.

Figuur 4.25 Op welke wijze hoort u wel eens over de risico's op internet?



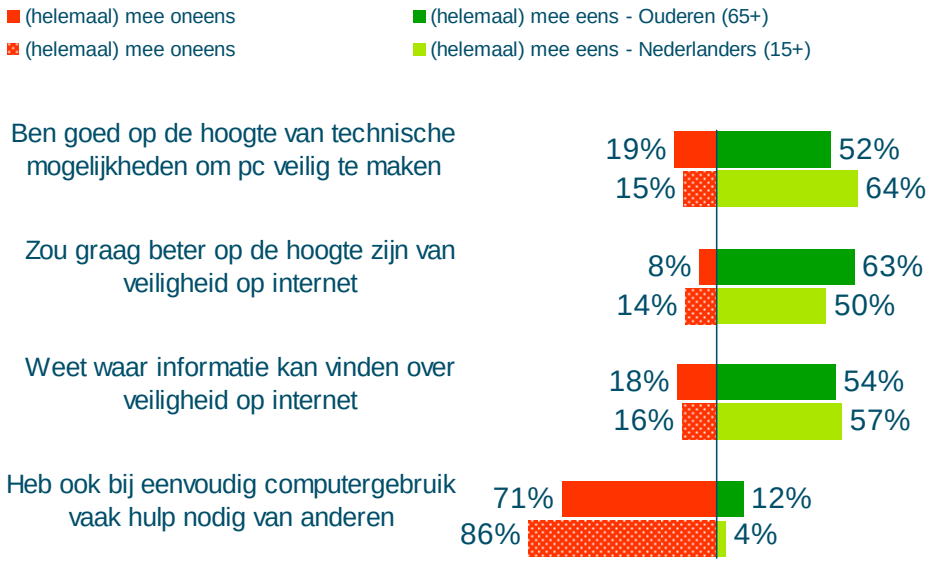
Bron:Synovate
Basis: groep ouderen 65+ (n=349); groep Nederlanders 15+ (n=288)

Grofweg lijkt de wijze waarop ouderen en de Nederlander aan informatie over risico's van internetgebruik komen op elkaar. Ouderen vergaren vaker informatie via de televisie, krant en radio en in mindere mate van het internet. Een op de tien ouderen ontvangt informatie via hun kinderen. Van de ouderen wordt 15% geïnformeerd via ouderenorganisaties en 12% geeft aan ook met andere senioren te praten over veilig internet.

4.3.2 Eigen kennis

Zoals ook eerder bij andere doelgroepen is gedaan, is aan de senioren gevraagd om zelf in te schatten hoe goed zij op de hoogte zijn van veiligheidszaken (Figuur 4.26). De resultaten zijn afgezet tegen de antwoorden van de gemiddelde Nederlander.

Figuur 4.26 Geef aan in hoeverre u het eens bent met de volgende stellingen



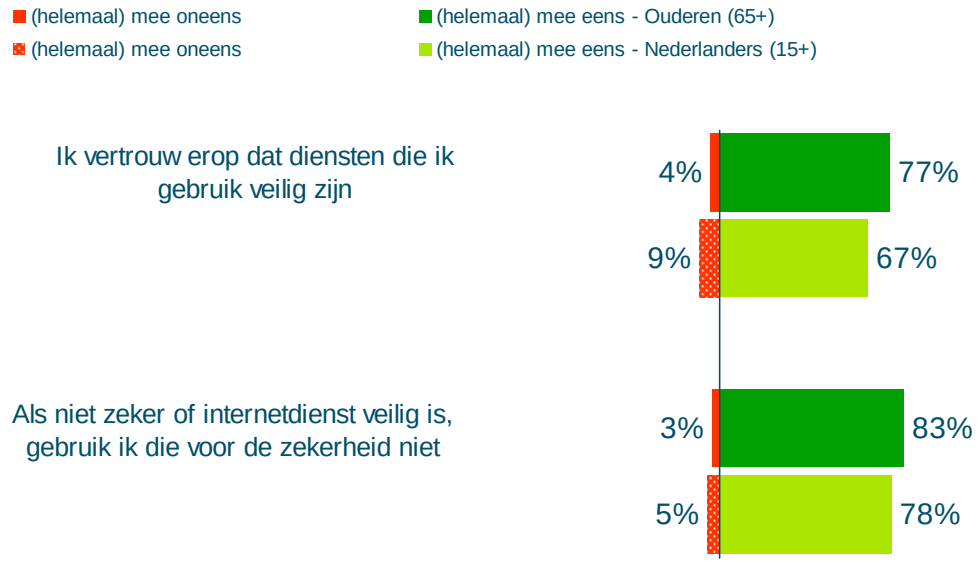
Bron: Synovate
Basis: groep ouderen 65+ (n=349); groep Nederlanders 15+ (n=288)

De helft van de ouderen acht zich goed op de hoogte van de technische mogelijkheden om de computer te beveiligen. Hiermee scoren ze 12% lager dan de gemiddelde Nederlander. Ook geeft 19% van de senioren aan nadrukkelijk niet goed op de hoogte te zijn, hier wijken zij 4% af van de gemiddelde Nederlander. Zowel de groep Nederlanders als de groep senioren geeft aan graag beter op de hoogte te willen zijn. Ook hier scoren de senioren hoger dan gemiddeld (63% vs. 50%). Van de senioren zegt 54% wel te weten waar ze informatie kunnen vinden, mochten ze daar behoefte aan hebben. Hier ontlopen ze de gemiddelde Nederlander niet veel, deze scoort 57%.
Bij eenvoudig computergebruik lijken ouderen zich best goed te kunnen redden. Slechts een op de tien geeft aan nog hulp van anderen nodig te hebben en bijna drie kwart van de groep bestrijdt dat. Toch liggen de percentages nog iets hoger dan bij de gemiddelde Nederlander.

4.3.3 Algemene veiligheidsbeleving

Door nog twee stellingen is aan ouderen gevraagd in hoeverre zij vertrouwen hebben in de diensten die zij online gebruiken (Figuur 4.27).

Figuur 4.27 Geef aan in hoeverre u het eens bent met de volgende stellingen



Bron: Synovate
Basis: groep ouderen 65+ (n=349); groep Nederlanders 15+ (n=288)

Ouderen blijken iets beter van vertrouwen dan de Nederlandse bevolking in zijn geheel. Terwijl 77% van de ouderen erop vertrouwt dat de gebruikte internetdiensten veilig zijn, geldt dat voor tweederde van de Nederlanders. Het vertrouwen in online diensten is daarmee redelijk groot.

De meeste ouderen nemen het zekere voor het onzekere: ruim 80% gebruikt diensten in geval van twijfel niet. Hierbij wijken ouderen nauwelijks af van Nederlanders in het algemeen.

4.4 Kernbevindingen

- Meer dan 90% van de Nederlanders gebruikt een virusscanner. 75% installeerde in de week voorafgaand aan het onderzoek beveiligingsupdates van deze software.
- Veel gebruikers hebben ervaringen met dreigingen. Spam is daarbij het meest genoemd.
- Filters om schadelijke content te weren worden door een minderheid van de ouders gebruikt. Veel ouders vinden dit niet nodig.
- Er wordt vooral veel gebruik gemaakt van internet bankieren en marktplaatsen. Gebruikers hebben veel vertrouwen in deze diensten, maar maken zich meer zorgen over de beveiliging van persoonlijke gegevens.
- Bijna de helft van de ouders maakt zich wel eens zorgen over de veiligheid van hun kind online. Deze zorgen hebben vooral betrekking op de confrontatie met ongewenste informatie en het gegeven dat kinderen benaderd kunnen worden door onbekenden met slechte bedoelingen.
- Van deze ouders vindt 80% dat ze zelf goed op de hoogte zijn en 95% van de ouders met kinderen in de leeftijd 13-18 jaar praat de kinderen over diverse onderwerpen. Wat niet uit dit onderzoek blijkt is of kinderen goed op de hoogte zijn met de risico’s en hoe ze omgaan met de kennis die zij hebben over het onderwerp.

- Er is weinig behoefte aan extra informatie over veiligheid op internet. Huidige kennis wordt vooral opgedaan via de massamedia.
- Ouderen maken zich minder zorgen over de veiligheid van internetdiensten en de impact van malware en beschermen zich minder goed tegen dreigingen. Toch wijkt de groep niet erg veel af van de groep Nederlanders.

5 Conclusies

Het programma Digivaardig & Digibewust stimuleert het bewust en veilig gebruik van digitale middelen. In dit onderzoek is de vraag gesteld wat we eigenlijk weten over veilig internetgebruik en hoe verschillende doelgroepen hun eigen veiligheid ervaren. Een eventuele kloof tussen deze twee aspecten kan enerzijds leiden tot verminderd diensten gebruik omdat gebruikers hun veiligheid niet gewaarborgd achten, maar anderzijds ook tot onveilig dienstengebruik omdat gebruikers zich geen zorgen maken over diensten waarbij dat wel het geval zou moeten zijn. Om veilig gebruik te maken van het internet, is het voor gebruikers daarom noodzakelijk om te kunnen beoordelen wat veilig is en wat niet.

Deze vraag (wat is veilig online en wat niet) blijkt niet eenvoudig te beantwoorden. Uit dit onderzoek bleek dat er door verschillende partijen, verschillende informatie verzameld wordt over de veiligheid van het internet, maar dat deze vooral ingaan op de hoeveelheid dreigingen die op het internet bestaan. Slechts zeer beperkt is bekend (en openbaar) in welke mate gebruikers met deze risico’s geconfronteerd worden en welke schade zij dan oplopen. Hierdoor ontbreekt het bij alle betrokken partijen aan een compleet dreigingsbeeld.

Desalniettemin maken Nederlanders veel gebruik van het internet. De laatste jaren zijn er steeds meer diensten online beschikbaar gekomen. Een deel van de diensten die we veel gebruiken bestond al ‘offline’ en krijgen een online variant zoals het geval bij internet bankieren, of marktplaatsen, maar soms wordt offline dienstverlening volledig vervangen door een digitale dienst zoals het geval bij de belastingaangifte. Maar er komen ook steeds meer nieuwe diensten bij. Zo worden meningen over het actuele ontwikkelingen geventileerd via blogs, zijn er veel games online te spelen en krijgen diverse sociale netwerken steeds meer aanhang. Vooral jongere doelgroepen maken veel gebruik van deze zogenaamde web 2.0-toepassingen.

Het zijn nieuwe ontwikkelingen die gebruikers steeds meer mogelijkheden bieden, maar waar in sommige gevallen ook nieuwe risico’s mee verbonden zijn. Uit verschillende bronnen bleek dat recente dreigingen zich vaker richten op online diensten en sociale netwerken. Dit omdat deze diensten ook in gebruik steeds populairder worden en vaak door goed vertrouwen van een gebruiker schade kan worden toegedaan aan het volledige netwerk. Hier gaat vaak een actie van een gebruiker, een klik op een link, aan vooraf. Bewustzijn is hierbij dus erg belangrijk. Dreigingen als spam en virussen worden in negen van de tien gevallen opgevangen door een virusscanner. Omdat gebruikers zich steeds vaker bewust zijn dat zij deze moeten inschakelen en up to date moeten houden, lopen zij hier minder risico’s.

Hoewel er wel signalen zijn hoe en waar dreigingen zich ontwikkelen, kunnen er door het gebrek aan data over de impact geen uitspraken worden gedaan over de risico’s die privégebruikers lopen bij het gebruik van bepaalde diensten of het internet in het algemeen. Men zou kunnen zeggen dat gebruikers op hun hoede moeten zijn, al valt niet precies te zeggen waarvoor. Daardoor is het ook moeilijk in te schatten of vertrouwen in bepaalde diensten terecht is of onterecht.

Uit het gebruikersonderzoek bleek bijvoorbeeld dat internetbankieren erg populair is bij de verschillende doelgroepen en dat deze dienst een hoog vertrouwen geniet. Of dit vertrouwen terecht is, kan beter beoordeeld worden door de bank dan door de gebruiker zelf. Zonder nu te concluderen dat het vertrouwen in internet bankieren onterecht is, is het wel belangrijk om te constateren dat de gebruiker zich nu wellicht als vanzelfsprekend veilig acht, omdat hij informatie mist. Omdat de afweging over de veiligheid van een dienst nu niet te bepalen is, is het ook niet duidelijk waar de gebruiker zijn afwegingen op baseert. Alleen een goed geinformeerder gebruiker kan bewust een veilige keuze maken.

Gebruikers moeten alert blijven, zo ook voor de dreigingen die niet direct een technische oorzaak hebben, zoals confrontatie met onbekenden op chatsites en het prijsgeven van privégegevens op sociale netwerksites. Ongeveer de helft van de ondervraagde ouders uitten hier zorgen over. Hoewel een gewaarschuwd mens voor twee telt, is het ook in deze gevallen niet duidelijk hoe groot het risico is dat gebruikers daadwerkelijk lopen.

Op welke manieren kan het programma *Digivaardig & Digibewust* bijdragen aan een veiliger internet en een meer verantwoord gebruik van haar doelgroepen?

- Er ligt een grote uitdaging om een completer beeld te krijgen van de hoeveelheid dreigingen, de risico's en de impact voor gebruikers. Het programma zou initiatieven om dit beeld aan te vullen, met name op het gebied van impactmeting, kunnen ondersteunen of initiëren. Hierdoor kunnen de doelgroepen hun afwegingen maken op basis van feitelijke risico's en impact. Nu is de perceptie nog te veel incidentgedreven. Waar nodig kan het programma met de kennis van de feitelijke risico's voor gebruikers de doelgroepen extra voorlichten.
  Ook biedt een realistisch dreigingsbeeld mogelijkheden om urgente risico's (gezamenlijk) te bestrijden en beter te voorkomen in de toekomst.

- Uit het gebruikersonderzoek bleek dat veel ouders met hun kinderen praten over de dreigingen die online bestaan, vaak incident gedreven naar aanleiding van een bericht in de media. Uit dit onderzoek blijkt niet wat het effect is van deze voorlichting en hoe het gesteld is met het kennisniveau van de kinderen. Ook zeggen de ouders zelf niet veel meer behoefte te hebben aan voorlichting. Er is in de laatste jaren ook al voorlichting geweest voor ouders. Interessant zou zijn om te kijken welke invloed de voorlichting van de ouders heeft op het gedrag van de kinderen. Het hoeft helemaal niet vanzelfsprekend te zijn dat een goed voorgelichte ouder de kinderen ook heeft kunnen overtuigen van het belang van bewust internetgebruik. Mogelijk schatten kinderen de risico's anders in en verkiezen zij het nut of plezier van een dienst boven eventuele veiligheidsrisico's. Om hier uitspraken over te doen is meer onderzoek nodig.

- De senioren die in dit onderzoek ondervraagd zijn, zijn veelal actieve internetgebruikers. Over het algemeen blijken ouderen minder goed op de hoogte van veiligheidsrisico's en lopen ze iets achter in het gebruik van beveiligingen. Deze groep ondervindt ook minder last van risico's, waardoor het gevoel van urgentie mogelijk niet zo hoog is als bij de andere groepen. Ze vinden het ook moeilijker om de juiste informatiekanalen te vinden dan de andere doelgroepen.

Hoewel er geen sprake is van een grote kloof tussen ouderen en de Nederlandse bevolking, zou het programma ouderen kunnen ondersteunen bij het vinden van de juiste informatiekanalen, of nieuwe kanalen inrichten.