Internetbankieren: veiligheidspercepties van gebruikers

Jurjen Jansen, Nicolien Kop & Wouter Stol

In dit onderzoek kijken we vanuit gebruikersperspectief naar de veiligheid van internetbankieren, in het bijzonder naar risicoperceptie van online bankfraude. Secundaire analyse van data op basis van vragenlijstonderzoek onder 1200 internetbankierende Nederlanders laat zien dat gebruikers van internetbankieren online bankfraude niet als groot risico zien. Hun risicoperceptie wordt voornamelijk bepaald door de ingeschatte kans om slachtoffer te worden van online bankfraude. De gepercipieerde impact van online bankfraude en de mate van vertrouwen in internetbankieren zijn in enige mate van invloed op hun risicoperceptie. (In)direct slachtofferschap heeft amper invloed op risicoperceptie. De resultaten van deze studie kunnen helpen om communicatie over risico's van internetbankieren te verbeteren.

1 Inleiding

Ruim 90% van de huishoudens in Nederland heeft toegang tot internet (Statline 2016a). Internettoegang levert mensen veel gemak op, zoals bij het onderhouden van contacten en het doen van aankopen. Een nadeel van digitalisering is dat mensen afhankelijker worden van technologie, alsook vatbaarder worden voor beveiligingsincidenten (Furnell et al. 2007). Adequate informatiebeveiliging is dus een belangrijke vereiste in onze huidige maatschappij, bijvoorbeeld om ervoor te zorgen dat gevoelige informatie niet in handen van kwaadwillenden komt.

Dit onderzoek richt zich op een specifieke online dienst, namelijk het internetbankieren. Met internetbankieren hebben gebruikers via een internetverbinding toegang tot verschillende bankdiensten, zoals het bekijken van saldi en het betalen van rekeningen. In Nederland wordt hier volop gebruik van gemaakt. 85% van de Nederlanders van zestien jaar en ouder maakt hiervan gebruik (Eurostat 2016). Internetbankieren biedt gebruikers gemak en flexibiliteit bij het doen van financiële transacties (Davinson en Sillence 2014).

Internetbankieren kent echter een keerzijde. Waar vroeger banken werden overvallen, gebruiken criminelen nu *phishing* of *banking malware* om aan inloggegevens en beveiligingscodes te komen van gebruikers, waarmee vervolgens geld van de bijbehorende bankrekening kan worden gestolen. Phishing is een poging tot oplichting (art. 326 Wetboek van Strafrecht): de dader probeert langs digitale weg en op bedrieglijke wijze (vaak per e-mail) iemand ertoe te bewegen gegevens te verstrekken om daarmee wederrechtelijk voordeel te behalen. Malware is een samentrekking van *malicious software* en een containerbegrip voor schadelijke software zoals virussen, wormen, trojaanse paarden en spyware. Phishing en mal-

doi: 10.5553/TvV/187279482017016001003

ware zijn de meest voorkomende dreigingen voor gebruikers van internetbankieren in Nederland. Deze twee dreigingen staan centraal in dit onderzoek.
Het onderzoek gaat specifiek in op de denkbeelden van gebruikers over deze dreigingen. Volgens Johnson en Tversky (1983) en Slovic (1987) is het, wanneer het gaat om veiligheid, van belang om percepties van mensen in kaart te brengen en te begrijpen. Percepties over gevaar en risico zijn namelijk van invloed op het nemen van beslissingen en dus op het gedrag van mensen (Johnston en Warkentin 2010). Dit geldt ook voor internetbankieren (Cunningham et al. 2005; Jansen en Van Schaik 2016; Yousafzai et al. 2003). Dus om te begrijpen hoe mensen reageren op aanvallen op internetbankieren, dienen we te onderzoeken hoe zij hun online veiligheid en aanvallen daarop waarderen. Daarom kijken we in dit onderzoek specifiek naar risicoperceptie. Daarnaast faciliteert onderzoek naar risicoperceptie het ontwerpen van risicocommunicatie en mitigatietechnologieën (Garg en Camp 2012).
Risicoperceptie in geval van internetbankieren kan worden gezien als het gepercipieerde mogelijke verlies bij het gebruik van die dienst (Yousafzai et al. 2003). We spreken van percepties, omdat mensen veelal vertrouwen op een intuïtief oordeel over risico (Slovic 1987). Risico's zijn in die zin sociaal geconstrueerd; mensen baseren risico's op emotioneel beladen waardeoordelen, evenals op cognitieve claims (Garland 2003) die niet overeen hoeven te komen met de werkelijkheid.
Het doel van dit artikel is om inzicht te krijgen in de risicoperceptie van gebruikers over online bankfraude en zicht te krijgen op welke factoren van invloed zijn op die risicoperceptie. De centrale vraag luidt dan ook: wat is de aard van de risicoperceptie van gebruikers van internetbankieren ten aanzien van online bankfraude en waardoor wordt deze perceptie gevormd? Onderzoek naar risicoperceptie in het online domein is schaars (Garg et al. 2012). Dit onderzoek probeert die leemte op te vullen. Daarnaast is over de invloed van cybercrimeslachtofferschap op de vorming van risicoperceptie eveneens nog weinig bekend (Henson et al. 2013; Jackson et al. 2005). Dit artikel levert een bijdrage aan de kennis omtrent risicoperceptie in het online domein door slachtofferschap van online bankfraude te includeren als mogelijke verklarende variabele voor risicoperceptie.

2 Theorie

Risicoperceptie kan worden bestudeerd vanuit verschillende benaderingen. Twee belangrijke zijn de *revealed preferences*-benadering van Starr (1969) en de *expressed preferences*-benadering van Fischhoff et al. (1978). Slovic en Peters (2006) vertalen deze twee benaderingen in *risk as analysis* en *risk as feelings*, waarbij de eerste benadering uitgaat van logica, redenering en wetenschappelijke beraadslaging en de tweede benadering van instinctieve en intuïtieve oordelen. Dit betekent bijvoorbeeld dat risico een andere betekenis heeft voor wetenschappers dan voor leken (Slovic 1987).
Omdat we in ons onderzoek kijken naar percepties van gebruikers, nemen we de *expressed preferences*-benadering als uitgangspunt. Deze benadering neemt in ogenschouw dat gebruikers niet over volledige informatie beschikken en dat ze de

informatie die ze hebben niet optimaal kunnen gebruiken. Bovendien speelt deze subjectieve variant in verschillende theoretische modellen een fundamentele rol (o.a. Rogers 1975), bijvoorbeeld om gedrag in relatie tot informatiebeveiliging beter te begrijpen (Johnston en Warkentin 2010; Liang en Xue 2010).

2.1 Voorspellers van risicoperceptie

In het dagelijks gebruik wordt risico omschreven als de mogelijkheid van verlies, schade, nadeel of vernietiging (Garland 2003). In meer theoretische zin kan risico worden gezien als een maat voor blootstelling aan gevaar, uitgedrukt in waarschijnlijkheid (kans) en de mate van verlies (impact) (Garland 2003; Jackson et al. 2005; Liang en Xue 2010).

Onderzoekers op het gebied van risicoperceptie, waaronder Griffin et al. (2004), Slovic (1987) en Vlaev et al. (2009), hebben laten zien dat risicoperceptie een multidimensionaal karakter heeft. Griffin et al. noemen, naast kans en impact, ook persoonlijke controle en institutioneel vertrouwen als voorspellers van risicoperceptie. Persoonlijke controle is een zelfevaluatie van de mate van controle over de vatbaarheid voor schade als het risico werkelijkheid wordt (Griffin et al. 2004). Institutioneel vertrouwen heeft volgens hen betrekking op in hoeverre een individu andere partijen bekwaam acht om ervoor te zorgen dat hij of zij geen nadeel ervaart van een betreffende dreiging. Een grote mate van gepercipieerde controle over de eigen veiligheid en een grote mate van institutioneel vertrouwen leiden tot verlaagde risicoperceptie (Griffin et al. 2004).

Uit de meer algemene *fear of crime*-literatuur leren we dat er een verband is tussen risicoperceptie en angst. Derhalve putten we uit deze literatuur om meer te weten te komen over de mogelijke invloed van slachtofferschap op risicoperceptie. Henson et al. (2013) stellen bijvoorbeeld dat individuen die slachtoffer zijn geweest van een bepaald delict (persoonlijke ervaring) hogere niveaus van angst kennen ten aanzien van dat delict dan niet-slachtoffers. Hun perceptie is kennelijk veranderd door het slachtofferschap. Naast persoonlijke ervaring kunnen zowel de sociale omgeving als de media een voorspellende werking hebben op risicoperceptie en angst (Hale 1996; Henson et al. 2013; Jackson et al. 2005; Johnson en Tversky 1983), ook wel aangeduid als indirect slachtofferschap of plaatsvervangende ervaring.

Voor de volledigheid wordt in dit onderzoek ook gekeken naar de invloed van demografische variabelen. In eerder onderzoek is aangetoond dat de demografische variabelen geslacht, leeftijd, opleidingsniveau en werkstatus een voorspellende werking hebben op risicoperceptie (Bronfman et al. 2008; Savage 1993). Ook in de *fear of crime*-literatuur spelen deze variabelen een voorspellende rol. Zo rapporteren vrouwen, ouderen, laagopgeleiden en mensen met een laag inkomen over het algemeen hogere niveaus van angst voor criminaliteit dan hun tegenhangers (Hale 1996), hoewel deze groepen objectief gezien de minste kans maken om slachtoffer te worden van criminaliteit (Pleysier 2011). Wat betreft leeftijd is in een aantal studies echter een omgekeerd effect gevonden, namelijk dat jongere mensen meer angst hebben voor (bepaalde vormen van) criminaliteit (Henson et al. 2013; Jackson 2009).

doi: 10.5553/TvV/187279482017016001003

In de literatuur zijn nog andere factoren benoemd die van invloed lijken op risicoperceptie. Fischhoff et al. (1978) beschrijven in het psychometrisch paradigma negen dimensies van risico. Naast de dimensies controle over het risico en de ernst van de gevolgen die reeds aan bod zijn gekomen, identificeren zij: vrijwilligheid van het risico, tijdigheid van het effect, kennis van experts over het risico, kennis van ervaringsdeskundige leken over het risico, hoe nieuw het risico is, of het één mens/systeem of meerdere mensen/systemen aantast en of het een risico is waarmee men heeft leren leven of een waar men angstig voor is. Ook culturele aspecten, attitudes, risicogevoeligheid en specifieke angsten kunnen van invloed zijn op hoe mensen risico's waarnemen (Sjöberg 2000). Vanwege de beperkingen van het gebruikte databestand waar wij onze secundaire analyse op hebben verricht, konden deze factoren niet in onze analyses worden opgenomen. Wij komen hier in de discussie van onze resultaten op terug.

2.2 Consequenties van risicoperceptie

Een belangrijke ontdekking in de psychologie, door Tversky en Kahneman in 1974, was dat mensen heuristieken (vuistregels) gebruiken om betekenis te geven aan onzekerheden (Thaler en Sunstein 2009). Hoewel deze vuistregels in sommige gevallen opgaan, leiden ze in andere gevallen tot hardnekkige vooroordelen die consequenties kunnen hebben voor risico-inschatting.

Onderzoek naar objectieve en subjectieve oordelen over dreigingen heeft inzichtelijk gemaakt dat er vooroordelen zijn in het menselijk denken (Slovic et al. 1982). Zo wordt de frequentie van niet-frequente gebeurtenissen vaak overschat en die van frequente onderschat. Verder vindt overschatting vooral plaats bij dramatische of sensationele gebeurtenissen, terwijl niet-spectaculaire gebeurtenissen vooral worden onderschat. Huang et al. (2011) stellen dat kennis een sleutelfactor is in de kloof tussen gepercipieerde veiligheid en de daadwerkelijke veiligheid van een systeem. Een gebrek aan kennis is vaak de oorzaak in het onder- of overschatten van het beveiligingsniveau van een systeem.

Indien het gepercipieerde risico hoger of lager is dan het daadwerkelijke risico, kan dat nadelige gevolgen hebben. Overschatting van risico's kan ervoor zorgen dat men bepaalde producten of diensten ten onrechte niet gebruikt. 'Niet gebruiken' is in de Nederlandse context voor internetbankieren bijna niet denkbaar, omdat er weinig alternatieven voorhanden zijn, maar men kan wel minder internetbankieren (bijvoorbeeld geen online aankopen doen). Indien het risico wordt onderschat, kan dat mensen aanmoedigen om onveilig gedrag te vertonen (Huang et al. 2011).

3 Methode

Onderhavig onderzoek betreft een secundaire analyse van een dataset die heeft gediend voor onderzoek naar motivaties voor veilig online gedrag door gebruikers van internetbankieren (Jansen en Van Schaik 2016). Medio 2015 is hiervoor een online vragenlijst afgenomen. De vragenlijst is gebaseerd op literatuuronderzoek en is zowel kwalitatief als kwantitatief gepretest. Voor onderhavig onderzoek is

aanvullend literatuuronderzoek verricht om het theoretisch kader verder aan te scherpen.
In dit onderzoek staat de afhankelijke variabele 'risicoperceptie' centraal. We hebben geanalyseerd in hoeverre de afhankelijke variabele wordt beïnvloed door de volgende onafhankelijke variabelen: gepercipieerde kans, gepercipieerde impact, *locus of control*, vertrouwen in internetbankieren en (in)directe ervaring met slachtofferschap (persoonlijk, omgeving en media). De demografische kenmerken geslacht, leeftijd, opleidingsniveau en werkstatus zijn meegenomen als controlevariabelen.
Locus of control kan intern of extern zijn. Interne locus of control betekent dat mensen geloven zelf de controle te hebben over bepaalde uitkomsten, terwijl bij externe locus of control mensen dit toedichten aan het lot of het in handen van anderen leggen (Rotter 1966; Workman et al. 2008), zoals een bank. Vertrouwen in internetbankieren wordt gezien als een psychologische toestand die leidt tot de bereidheid van de klant om banktransacties uit te voeren op het internet in de verwachting dat de bank aan haar verplichtingen zal voldoen, ongeacht het vermogen van de klant om de acties van de bank te monitoren of controleren (Yousafzai et al. 2003). Studies naar de adoptie van internetbankieren hebben laten zien dat risicoperceptie afneemt, naarmate het niveau van vertrouwen in internetbankieren toeneemt (Davinson en Sillence 2014; Yousafzai et al. 2009). Locus of control en vertrouwen in internetbankieren liggen nauw aan tegen de constructen persoonlijke controle en institutioneel vertrouwen (zie par. 2.1).
De variabelen zijn gebaseerd op bestaande schalen en zijn gemeten met drie stellingen die respondenten konden beantwoorden aan de hand van een vijfpunts Likertschaal van 1) 'helemaal mee oneens' tot 5) 'helemaal mee eens'. De vragen over risicoperceptie zijn gebaseerd op Grabner-Kräuter en Faullant (2008), de vragen over gepercipieerde kans en impact zijn overgenomen van Witte (1996), de locus of control-vragen zijn gebaseerd op Workman et al. (2008) en de vragen over vertrouwen zijn overgenomen van Yousafzai et al. (2009). Om slachtofferschap te meten kregen respondenten na een beschrijving van phishing en malware de vraag in hoeverre ze van slachtofferschap van deze dreigingen hebben gehoord (eigen omgeving en media). Daarna is aan de respondenten gevraagd of zij in de afgelopen vijf jaar zelf slachtoffer waren. Tot slot hebben de respondenten hun demografische gegevens ingevuld.

3.1 Respondenten

Het aanschrijven en werven van respondenten werd gedaan door een extern online panelbureau. In totaal bezochten 1850 mensen de vragenlijst. 614 mensen hebben de vragenlijst bezocht, maar niet of gedeeltelijk ingevuld. Wij hebben geen aanvullende informatie kunnen bemachtigen over de achtergrondkenmerken van deze mensen. Bij de eerste (selectie)vraag zijn 36 mensen van verdere deelname uitgesloten, omdat zij niet tot de doelgroep behoorden: 14 hiervan lieten hun internetbankieren door iemand anders beheren en de overige 22 maakten geen gebruik van internetbankieren.
In totaal vulden 1200 respondenten de vragenlijst volledig in. 54,8% van de respondenten is vrouw en 45,2% is man. De gemiddelde leeftijd van de responden-

Tijdschrift voor Veiligheid 2017 (16) 1
doi: 10.5553/TvV/187279482017016001003

ten is 49 jaar (SD = 14,5) en de opleidingsniveaus zijn gecategoriseerd als hoog (52,5%), midden (32,3%) en laag (15,2%). Wat betreft werkstatus zijn de respondenten in loondienst (53,9%), ondernemer/zelfstandige (6,9%), gepensioneerd (18,8%) of hadden een andere status (20,3%), zoals student of werkzoekend. In totaal kan 56,9% worden gerekend tot de werkzame beroepsbevolking. Deze groep bestaat uit ondernemers/zelfstandigen en mensen die twaalf uren per week of meer in loondienst werken.

Omdat we geen cijfers tot onze beschikking hadden van de totale Nederlandse populatie die gebruikmaakt van internetbankieren, hebben we de achtergrondkenmerken van de respondenten vergeleken met die van de totale Nederlandse bevolking. In hoeverre de respondenten op demografische kenmerken representatief zijn voor alle internetbankierende Nederlanders is niet exact vast te stellen. De gepresenteerde cijfers betreffen dus een indicatie. Vrouwen zijn iets oververtegenwoordigd in de dataset en mannen iets ondervertegenwoordigd ($p < 0{,}01$). De verdeling van de Nederlandse bevolking is 50,5% vrouw en 49,5% man (Statline 2015).[1] In vergelijking tot de Nederlandse bevolking is de leeftijdscategorie tot 30 jaar in ons databestand ondervertegenwoordigd ($p < 0{,}001$) (Statline 2016b).[2] Hoogopgeleide respondenten zijn oververtegenwoordigd en laagopgeleiden ondervertegenwoordigd in onze dataset ($p < 0{,}001$). De verdeling van opleidingsniveaus was volgens Statline (2013) in 2012 hoog (28,6%), midden (40,7%) en laag (30,7%).[3] Over heel Nederland gezien was het percentage dat behoort tot de werkzame beroepsbevolking 64,8% (CBS 2015a).[4] Dit percentage is significant hoger dan het percentage in ons databestand ($p < 0{,}001$).

3.2 Data-analyse

Voor de beschrijvende analyses is gebruikgemaakt van SPSS (versie 23). Om te bepalen in welke mate de voorspellende variabelen van invloed zijn op risicoperceptie gebruikten we padanalyse (*partial-least-squares path-modelling* (PLS)). Deze analysemethode is geschikt voor verkennend onderzoek en is gericht op het maximaliseren van de hoeveelheid verklaarde variantie (Hair et al. 2014). De verklarende analyse is uitgevoerd met behulp van het statistische softwareprogramma SmartPLS 2.0 (Ringle et al. 2005). We hebben een standaard PLS *bootstrapping*-procedure toegepast (N = 5000), zoals aangeraden door Henseler et al. (2009), om de significantie van de parameters uit het structurele model te toetsen. Het structurele model vertegenwoordigt de relaties tussen de afhankelijke en onafhankelijke variabelen.

Naast het structurele model levert PLS een meetmodel op dat we allereerst evalueerden. Hiermee kregen we inzicht in hoeverre de data aan de voorwaarden voldeden voor de toegepaste analysemethode. De *component loadings* van de individuele items laden voldoende hoog (≥ 0,70) op het corresponderende construct en aanzienlijk lager op de overige constructen, wat bewijs levert voor de unidimensiona-

1 Berekening aan de hand van peildatum 2015, totale Nederlandse bevolking.
2 Berekening aan de hand van peildatum 2016, Nederlandse bevolking 20-80 jaar.
3 Berekening aan de hand van peildatum 2012, Nederlandse bevolking 15-65 jaar.
4 Berekening aan de hand van peildatum 2015 (kwartaal 1), Nederlandse bevolking 15-65 jaar.

liteit van de items (Henseler et al. 2009), zie tabel 1. De betrouwbaarheid van de constructen werd beoordeeld aan de hand van het samengestelde betrouwbaarheidscoëfficiënt (*composite reliability*). Alle constructen waren voldoende betrouwbaar (≥ 0,70): risicoperceptie (0,88), gepercipieerde kans (0,88), gepercipieerde impact (0,90), locus of control (0,84) en vertrouwen in internetbankieren (0,89).

Tabel 1 Component loadings

	PR	PV	PS	LoC	TR
PR1	**0,85**	0,60	0,32	-0,22	-0,38
PR2	**0,81**	0,67	0,22	-0,28	-0,37
PR3	**0,87**	0,61	0,31	-0,29	-0,41
PV1	0,63	**0,88**	0,18	-0,26	-0,33
PV2	0,69	**0,90**	0,23	-0,28	-0,35
PV3	0,55	**0,73**	0,21	-0,19	-0,24
PS1	0,27	0,22	**0,87**	0,08	-0,08
PS2	0,20	0,13	**0,83**	0,10	-0,03
PS3	0,37	0,26	**0,91**	0,04	-0,13
LoC1	-0,27	-0,26	0,13	**0,83**	0,40
LoC2	-0,28	-0,27	0,03	**0,81**	0,39
LoC3	-0,20	-0,17	0,02	**0,77**	0,34
TR1	-0,45	-0,35	-0,12	0,41	**0,91**
TR2	-0,29	-0,26	-0,02	0,45	**0,79**
TR3	-0,41	-0,33	-0,11	0,35	**0,85**

Noot: PR: risicoperceptie. PV: gepercipieerde kans. PS: gepercipieerde impact. LoC: locus of control. TR: vertrouwen in internetbankieren.

Convergente validiteit – de mate van samenhang tussen de items van hetzelfde construct (Hair et al. 2014) – werd beoordeeld aan de hand van de *average variance extracted* (AVE). De AVE was voor alle constructen, met uitzondering van locus of control, hoger dan de grenswaarde van 0,70: risicoperceptie (0,72), gepercipieerde kans (0,71), gepercipieerde impact (0,76), locus of control (0,64) en vertrouwen in internetbankieren (0,71). We hebben locus of control behouden in de analyses, omdat variantie in de items van locus of control meer wel dan niet werd verklaard (waarde ≥ 0,50). Discriminante validiteit – de mate waarin een construct verschilt van de andere constructen (Hair et al. 2014) – werd bepaald door een analyse van de wortel van de AVE. De betreffende uitkomstwaarde moet groter zijn dan de correlaties met de andere constructen (Fornell-Larcker-criterium). Alle waarden voldeden hieraan, zie tabel 2. Aanvullende SPSS-analyses toonden geen multicollineariteit-problemen. Dit betekent dat de voorspellende variabelen niet te sterk met elkaar correleren.

De onafhankelijke variabelen die betrekking hebben op slachtofferschap van phishing en malware zijn samengevoegd en gedichotomiseerd (0 = nee, 1 = ja). De correlaties tussen deze variabelen en 'risicoperceptie' zijn: zelf meegemaakt slachtofferschap (0,08), slachtofferschap omgeving (-0,02) en slachtofferschap

doi: 10.5553/TvV/187279482017016001003

Tabel 2 Coëfficiënten discriminante validiteit

	01	02	03	04	05
01 Risicoperceptie	**0,85**				
02 Gepercipieerde kans	0,75	**0,84**			
03 Gepercipieerde impact	0,34	0,25	**0,87**		
04 Locus of control	-0,31	-0,29	0,08	**0,80**	
05 Vertrouwen in internetbankieren	-0,46	-0,37	-0,10	0,47	**0,85**

Noot: Vetgedrukte waarden betreffen de wortel van de AVE. De overige waarden betreffen correlaties.

media (-0,13). De demografische kenmerken zijn als volgt gecodeerd: geslacht (0 = vrouw, 1 = man), leeftijd (in jaren), opleidingsniveau (1 = laag, 2 = gemiddeld, 3 = hoog) en werkstatus (0 = niet-werkzame beroepsbevolking, 1 = werkzame beroepsbevolking). De correlaties tussen de demografische variabelen en 'risicoperceptie' zijn als volgt: geslacht (-0,09), leeftijd (-0,02), opleidingsniveau (-0,14) en werkstatus (-0,05). Gezien het verkennende karakter van deze studie hebben we bovengenoemde variabelen, ondanks de lage correlatie met de afhankelijke variabele, toch meegenomen in de analyse.

4 Resultaten

Voordat we stilstaan bij de uitkomsten van de padanalyse, bespreken we eerst hoe gebruikers denken over de risico's en veiligheid van internetbankieren en in hoeverre zij te maken hebben gehad met slachtofferschap van phishing en malware.

4.1 Percepties van risico en veiligheid

De antwoorden die respondenten gaven op stellingen over risicoperceptie en de voorspellers van risicoperceptie staan in tabel 3. We zien dat een gering percentage respondenten internetbankieren risicovol acht en het plausibel acht slachtoffer te worden van online bankfraude. Ter vergelijking is een aanvullende stelling opgenomen waarin werd gesteld dat anderen een grote kans hebben om hiervan slachtoffer worden. Hier is 37,6% het (helemaal) mee eens en 16,2% (helemaal) mee oneens. Respondenten zijn het grotendeels (helemaal) eens met de stellingen dat online bankfraude een grote impact kan hebben. Respondenten zijn het over het algemeen (helemaal) eens dat ze zelf controle kunnen uitoefenen op de veiligheid van hun internetbankieren (een hoge score op de locus of control-schaal duidt op interne locus of control). Tot slot tonen respondenten overwegend vertrouwen in het systeem van internetbankieren. Meer dan de helft van de respondenten is het namelijk met de desbetreffende stellingen eens.

Tabel 3 *Item-scores (in procenten), gemiddelden en standaarddeviaties voor risicoperceptie en voorspellers (N = 1200)*

Construct	Items	1	2	3	4	5
Risico-perceptie (M = 2,6, SD = 0,79)	Ik ben bang om slachtoffer te worden van fraude met internetbankieren	11,1	35,7	36,3	13,9	3,0
	Ik denk dat criminelen vrij gemakkelijk geld kunnen stelen tijdens het internetbankieren	11,9	43,9	34,0	8,3	1,9
	Ik ben bang dat anderen ongewenst toegang kunnen krijgen tot mijn internetbankieren	8,0	36,7	33,4	18,8	3,2
Kans (M = 2,7, SD = 0,71)	Het is waarschijnlijk dat ik slachtoffer word van fraude met internetbankieren	9,4	43,2	41,2	5,3	1,0
	Ik denk dat ik een grote kans heb om slachtoffer te worden van fraude met internetbankieren	11,8	40,6	39,2	7,0	1,4
	Het is mogelijk dat ik slachtoffer word van fraude met internetbankieren	3,8	24,3	39,8	28,0	4,1
Impact (M = 4,0, SD = 0,76)	Ik denk dat fraude met internetbankieren een ernstig probleem is	1,3	3,7	20,8	41,6	32,8
	Ik denk dat fraude met internetbankieren een serieus probleem is	0,5	4,0	17,4	47,3	30,8
	Ik vind fraude met internetbankieren een aanzienlijk probleem	0,5	7,8	24,2	43,0	24,6
Locus of control (M = 4,0, SD = 0,72)	Ik kan zelf invloed uitoefenen op de veiligheid van mijn internetbankieren	0,9	1,6	13,5	47,6	36,4
	Het ligt binnen mijn macht om mezelf adequaat te beschermen tegen fraude met internetbankieren	1,3	4,2	17,4	44,6	32,6
	De primaire verantwoordelijkheid om mij te beschermen tegen fraude met internetbankieren ligt bij mijzelf	2,3	6,9	22,3	37,2	31,3
Vertrouwen (M = 3,7, SD = 0,70)	Ik vertrouw internetbankieren	2,1	4,7	28,7	54,0	10,5
	Ik vertrouw mijn bank	1,9	4,5	22,7	51,1	19,8
	Ik vertrouw het internet voor het doen van bankzaken	2,1	6,3	32,4	51,4	7,8

Noot: 1–5, helemaal mee oneens – helemaal mee eens; M, gemiddelde; SD, standaarddeviatie.

Tijdschrift voor Veiligheid 2017 (16) 1
doi: 10.5553/TvV/187279482017016001003

4.2 Slachtofferschap

Van de respondenten kent 16,3% iemand uit de eigen omgeving, zoals gezinsleden, familieleden, vrienden of collega's, die slachtoffer is geworden van phishing. Voor malware ligt dit percentage op 21,5%. In totaal kent 29,6% (N = 355) van de respondenten iemand in zijn of haar omgeving die slachtoffer is geworden van een of beide vormen van online bankfraude. Meer dan de helft van de respondenten (69,1% voor phishing en 52,1% voor malware) geeft aan geen slachtoffers te kennen uit de eigen omgeving, maar er wel via de media over gehoord te hebben. In totaal zegt driekwart van de respondenten hierover gehoord te hebben in de media (75,6%, N = 907). Respectievelijk 8,8% en 15,1% geven aan niemand te kennen alsook nooit in de media iets gelezen of gehoord te hebben over slachtofferschap van online bankfraude. De overige respondenten, respectievelijk 5,8% en 11,3%, geven aan niet te weten of ze iemand kennen of hiervan gehoord te hebben.

We definiëren direct slachtofferschap als respondenten die in de afgelopen vijf jaar gegevens hebben afgestaan naar aanleiding van een phishing-aanval en/of in deze periode een malware-infectie hebben gehad die was gericht op internetbankieren. In beide gevallen hoeft het slachtoffer dus nog geen geld kwijt te zijn. In artikel 51a Wetboek van Strafvordering wordt gesproken van slachtofferschap in geval van vermogensschade (er is geld weg) of ander nadeel (er zijn gegevens afgetroggeld c.q. de malware-infectie is gelukt) als dat een rechtstreeks gevolg is van een strafbaar feit.

Op de vraag of men zelf te maken heeft gehad met phishing, antwoordt 46,8% negatief. 4,1% weet het niet zeker. 49,1% (N = 589) heeft dus wel eens met phishing te maken gehad. Veruit de meesten hiervan hebben wel eens phishing e-mails ontvangen (N = 569). Sommigen zijn door iemand gebeld om gegevens af te staan (N = 82) of zijn wel eens ongewild terecht gekomen op een phishing website (N = 27). Van die 49,1% geeft 71,0% (N = 418) aan dat minstens een van de ervaringen met phishing te maken had met internetbankieren. In totaal gaf 2,4% aan in de afgelopen vijf jaar naar aanleiding van een phishingaanval gegevens te hebben afgestaan (N = 10). Deze tien zijn in dit onderzoek slachtoffers. Hiervan gaven zes personen aan dat het in de afgelopen twaalf maanden plaatsvond en drie van de tien dat er geld van hun bankrekening was gehaald.

Op de vraag of men in de afgelopen vijf jaar zelf te maken heeft gehad met malware antwoordt 57,8% negatief. 24,8% weet het niet zeker. 17,4% (N = 209) heeft wel eens te maken gehad met een malware-infectie op het apparaat dat men gebruikt voor internetbankieren. Van de gerapporteerde malware-infecties was 9,6% gericht op internetbankieren (N = 20). Deze twintig zijn in dit onderzoek slachtoffers. Tien respondenten meldden dat de infectie de afgelopen twaalf maanden plaatsvond en zeven van de twintig dat er geld van hun bankrekening was gehaald.

Hoewel een aanzienlijk deel van de respondenten te maken heeft gehad met dreigingen gericht op internetbankieren, hebben we slechts tien phishing- en twintig malware-slachtoffers kunnen identificeren. Drie van hen waren slachtoffer van beide vormen en zo hebben we in totaal 27 unieke slachtoffers (2,3%). Slachtof-

ferschap komt voor onder zowel mannen als vrouwen, onder alle opleidingsniveaus en onder alle leeftijdscategorieën.

4.3 Verklaringen voor risicoperceptie

We hebben gebruikgemaakt van padanalyse om te evalueren in hoeverre de onafhankelijke variabelen de afhankelijke variabele 'risicoperceptie' voorspellen. De resultaten hiervan zijn weergegeven in het structurele model, zie tabel 4.

Tabel 4 Testresultaten van het structurele model

Afhankelijke variabele	R^2	Voorspellende variabelen	Beta	Standard error	t[a]
Risicoperceptie	0,64	Gepercipieerde kans	0,61	0,02	**26,62**
		Gepercipieerde impact	0,17	0,02	**8,49**
		Locus of control	-0,05	0,02	**2,41**
		Vertrouwen in internetbankieren	-0,18	0,03	**7,40**
		Slachtofferschap (zelf)	0,03	0,02	1,87
		Slachtofferschap (omgeving)	-0,04	0,02	**2,25**
		Slachtofferschap (media)	-0,04	0,02	**2,09**
		Geslacht	-0,05	0,02	**2,44**
		Leeftijd	-0,06	0,02	**2,89**
		Opleidingsniveau	-0,07	0,02	**3,90**
		Werkstatus	-0,02	0,02	1,18

Noot: Vetgedrukte waarden zijn significant ($t \geq 1{,}96$ [$\alpha = 0{,}05$], $t \geq 2{,}57$ [$\alpha = 0{,}01$]).
[a]Bootstrap, N = 5000.

In het structurele model zien we dat 64% van de variantie is verklaard voor risicoperceptie ($R^2 = 0{,}64$). De sterkste voorspeller voor risicoperceptie is de gepercipieerde kans op online bankfraude. We interpreteren de effectgrootte zoals voorgesteld door Cohen (1988): klein (0,02), middelmatig (0,15) en groot (0,35). Twee voorspellers die middelmatig bijdragen zijn de gepercipieerde impact van online bankfraude en de mate van vertrouwen in internetbankieren, waarbij de laatste een negatieve relatie met risicoperceptie weergeeft. Interne locus of control kenmerkt zich eveneens door een negatieve relatie, maar is een minder sterke verklarende variabele. Voor slachtofferschap zijn twee marginaal significante (negatieve) verbanden gevonden. De toegevoegde waarde van demografische variabelen voor verklarende variantie is klein, maar geslacht, leeftijd en opleidingsniveau zijn wel statistisch significant.

Tijdschrift voor Veiligheid 2017 (16) 1
doi: 10.5553/TvV/187279482017016001003

5 Beperkingen, conclusie en discussie

Uit ons onderzoek blijkt dat gebruikers van internetbankieren online bankfraude niet als groot risico zien. Dit geldt eveneens voor de kans om hiervan slachtoffer te worden. Gebruikers schatten de kans dat zij slachtoffer worden lager in dan de kans dat anderen slachtoffer worden. Dat mensen eigen risico's onderschatten en dat van anderen overschatten, komt overeen met wat in de literatuur bekend is (Workman et al. 2008). De *impact* van online bankfraude wordt daarentegen wel hoog ingeschat.

Respondenten hebben redelijk veel vertrouwen in internetbankieren en zien weinig risico's in relatie tot online bankfraude. Dit lijkt mooi, maar brengt potentieel gevaar met zich mee. Vanuit de literatuur die *risk as feelings* als uitgangspunt neemt, is bekend dat er een correlatie bestaat tussen risicoperceptie en het communiceren van voordelen van een (risicovolle) activiteit (Finucane et al. 2000). Hoe meer voordeel, hoe lager de perceptie van risico en vice versa. Het is voor banken dus van belang om een goede balans te vinden tussen het gebruiksgemak van hun diensten en de veiligheid ervan, niet alleen wat het gebruik betreft, maar ook in de communicatie hierover. Risico-onderschatting kan immers aanmoedigen om onveilig gedrag te vertonen, en dat vergroot dus uiteindelijk het risico. Hale (1996) stelt bijvoorbeeld dat het goed is dat mensen enige mate van bezorgdheid hebben in relatie tot criminaliteit, zodat zij zich ertegen wapenen.

Respondenten hebben weinig te maken met direct slachtofferschap van online bankfraude. Het gaat om tien phishing- en twintig malware-slachtoffers; in totaal 27 unieke slachtoffers, ofwel 2,3% van de respondenten. Dergelijke percentages zijn niet vreemd als we deze vergelijken met cijfers van het CBS (2015b): ongeveer 6% van de Nederlandse bevolking heeft te maken gehad met malware waarbij men gegevens heeft verloren en ongeveer 3% met online fraude. Verschil met ons onderzoek is dat CBS-cijfers gericht zijn op algemene online problematiek, terwijl onze cijfers uitsluitend betrekking hebben op internetbankieren.

Een belangrijke noot bij de vragen over slachtofferschap is dat respondenten phishing en malwareaanvallen mogelijk niet hebben opgemerkt. Het kan namelijk zijn dat malware zich heeft genesteld in de systemen van een eindgebruiker zonder dat hij of zij dat door heeft gehad, bijvoorbeeld omdat de virusscanner het niet heeft opgemerkt. Ook kan het zijn dat respondenten bepaalde voorvallen zijn vergeten, aangezien de vraagstelling betrekking heeft op de afgelopen vijf jaar. Het is dus mogelijk dat het percentage slachtoffers van phishing en malware in werkelijkheid hoger is.

Het structurele model laat zien dat de voorspellende variabelen uit de literatuur significant zijn en in de voorspelde richting. Dit betekent dat als gebruikers de kans (groot effect) en de impact (middelmatig effect) evalueren als groot, hun risicoperceptie groter is. Het betekent eveneens dat als gebruikers veel vertrouwen hebben in internetbankieren (middelmatig effect) en denken zelf controle te hebben over de veiligheid van internetbankieren (klein effect) hun risicoperceptie lager is.

De slachtoffervariabelen zijn amper van invloed op de verklaarde variantie van risicoperceptie. Direct slachtofferschap heeft geen significante voorspellende wer-

king. Dit is contra-intuïtief. Dat we geen significant verband vinden, heeft vermoedelijk te maken met de variabele 'gepercipieerde kans'. Deze variabele correleert sterk met risicoperceptie, hoewel het correlatieniveau aanvaardbaar is volgens het Fornell-Larcker-criterium. Wanneer we deze voorspeller in het structurele model buiten beschouwing laten, dan zien we dat zelf meegemaakt slachtofferschap wel een positief significante invloed heeft op risicoperceptie. Het effect van zelf meegemaakt slachtofferschap lijkt dus weg te worden verklaard door gepercipieerde kans. Dit verandert echter niet de conclusie van het onderzoek, want de invloed van slachtofferschap op de verklaarde variantie van risicoperceptie blijft ook in dat geval zeer gering.

Indirect slachtofferschap heeft een marginaal effect, maar in een andere richting dan verwacht. Dat ervaring met slachtofferschap in de persoonlijke omgeving de risicoperceptie doet afnemen, kan mogelijk worden verklaard doordat respondenten verhalen horen van slachtoffers waarvan de schade volledig is vergoed. Een andere mogelijkheid is dat zij uitleg hebben gekregen over hoe de aanval heeft plaatsgevonden en dat respondenten daardoor beter zijn voorbereid en derhalve het risico lager inschatten. Henson et al. (2013) vonden in hun studie ook een significant negatieve relatie tussen indirect slachtofferschap en angst. Zij geven als mogelijke verklaring dat slachtoffers hun ervaring bagatelliseren of niet serieus nemen, wat van invloed kan zijn op de percepties van de respondenten. De negatieve relatie tussen mediaberichtgeving en risicoperceptie kan zijn veroorzaakt door reclamecampagnes waarin gebruikers een handelingsperspectief wordt geboden dat bijdraagt aan de veiligheid van internetbankieren, waardoor men denkt minder risico te lopen. Een andere mogelijkheid is dat mensen het risico laag inschatten doordat de schadebedragen die worden gecommuniceerd relatief klein zijn. Verdiepend onderzoek is nodig om te achterhalen of de hierboven gepresenteerde assumpties juist zijn.

Overeenkomstig de literatuur dragen demografische variabelen op zichzelf niet veel bij aan de verklaarde variantie van risicoperceptie, maar zijn ze wel statistisch significant (Bronfman et al. 2008). Uitzondering hierop is werkstatus. Vrouwen, jongeren en lager opgeleiden hebben hogere niveaus van risicoperceptie voor online bankfraude dan mannen, ouderen en hoger opgeleiden. Dat vrouwen en lager opgeleiden hierop hoger scoren, correspondeert met wat bekend is uit de literatuur. In dit onderzoek lijken jongeren een hoger risico te ervaren van online bankfraude dan ouderen, terwijl in algemene termen ouderen vaker hogere niveaus van risicoperceptie rapporteren. Henson et al. (2013) concluderen echter dat leeftijd geen consistente voorspeller is voor risicoperceptie. Mogelijk is de variabele 'gepercipieerde kans' van invloed op de voorspellende werking van leeftijd. Wanneer we deze variabele verwijderen, blijkt leeftijd er namelijk niet meer toe te doen als voorspeller.

Hoewel 64% van de variantie in risicoperceptie is verklaard, is aanvullend onderzoek nodig om te achterhalen welke variabelen nog meer van invloed zijn op risicoperceptie. Een mogelijkheid is om de dimensies uit het psychometrisch paradigma (Fischhoff et al. 1978) als uitgangspunt te nemen (zie par. 2.1). Een basis hiervoor ligt in het werk van Garg en Camp (2012) die het psychometrisch paradigma al eerder toepasten op online risico's. Mogelijk dragen de aanvullende

Tijdschrift voor Veiligheid 2017 (16) 1
doi: 10.5553/TvV/187279482017016001003

dimensies bij aan de verklaarde variantie van risicoperceptie. Ook variabelen die meer op de mens zelf gericht zijn, kunnen hieraan bijdragen, denk bijvoorbeeld aan risicogevoeligheid en risicobereidheid. Dergelijke variabelen hebben we niet kunnen meewegen in onderhavig onderzoek als gevolg van de beperkingen in het databestand waarop de secundaire analyse is verricht.
Omdat het risico van online bankfraude niet is uit te sluiten, is het van belang om te blijven investeren in de weerbaarheid van gebruikers van internetbankieren, bijvoorbeeld door te communiceren over risico's en mogelijkheden om deze risico's tegen te gaan. Op basis van onze resultaten lijkt het zinvol om in dergelijke communicatie rekening te houden met de variabele 'gepercipieerde kans', omdat deze het meest van invloed is op risicoperceptie. Dit betekent dat het doel van de communicatie niet moet zijn dat iedereen denkt dat internetbankieren 100% veilig is. Dat zou in de hand kunnen werken dat men zich onveilig(er) gaat gedragen. Het gaat erom dat gebruikers voldoende bewust worden gemaakt van risico's, zodat zij alert zijn en de juiste maatregelen treffen voor een veilige internetbankierervaring.

6 Financiering en dankwoord

Deze studie is onderdeel van het Kennisprogramma Veiligheid Digitaal Betalingsverkeer. Dit programma is gefinancierd door de bancaire sector (vertegenwoordigd door de Nederlandse Vereniging van Banken), de Politieacademie en de Nationale Politie. De auteurs willen de referenten bedanken voor hun waardevolle commentaar en verbetersuggesties.

Literatuur

Bronfman, N.C., L.A. Cifuentes en V.V. Gutiérrez (2008) Participant-focused analysis: Explanatory power of the classic psychometric paradigm in risk perception. *Journal of Risk Research*, 11(6), 735-753.

CBS (2015a) *Bevolking 15 tot 75 jaar-oud*. Verkregen via www.cbs.nl/nl-nl/achtergrond/2015/20/bevolking-15-tot-75-jaar-oud.

CBS (2015b) *Voorzichtig op internet door bezorgdheid over veiligheid*. Verkregen via www.cbs.nl/nl-NL/menu/themas/vrije-tijd-cultuur/publicaties/artikelen/archief/2015/voorzichtig-op-internet-door-bezorgdheid-over-veiligheid-2015.htm.

Cohen, J. (1988) *Statistical power analysis for the behavioural sciences*. Lawrence Erlbaum.

Cunningham, L.F., J. Gerlach en M.D. Harper (2005) Perceived risk and e-banking services: An analysis from the perspective of the customer. *Journal of Financial Services Marketing*, 10(2), 165-178.

Davinson, N. en E. Sillence (2014) Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies*, 72(2), 154-168.

Eurostat (2016) Individuals using the internet for internet banking. Verkregen via: http://ec.europa.eu/eurostat/tgm/refreshTableAction.do;?pcode=tin00099&language=en.

Finucane, M.L., A. Alhakami, P. Slovic en S.M. Johnson (2000) The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making*, 13(1), 1-17.

Fischhoff, B., P. Slovic, S. Lichtenstein, S. Read en B. Combs (1978) How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, 9(2), 127-152.

Furnell, S.M., P. Bryant en A.D. Phippen (2007) Assessing the security perceptions of personal Internet users. *Computers & Security*, 26(5), 410-417.

Garg, V. en J. Camp (2012) End user perception of online risk under uncertainty. *Proceedings of the 45th Hawaii International Conference on System Sciences*, 3278-3287.

Garg, V., L. Huber, L.J. Camp en K. Connelly (2012) Risk communication design for older adults. *Gerontechnology*, 11(2), 166-173.

Garland, D. (2003) The rise of risk. In R.V. Ericson en A. Doyle (Ed.), *Risk and morality*. University of Toronto Press, 48-86.

Grabner-Kräuter, S. en R. Faullant (2008) Consumer acceptance of internet banking: The influence of internet trust. *International Journal of Bank Marketing*, 26(7), 483-504.

Griffin, R.J., K. Neuwirth, S. Dunwoody en J. Giese (2004) Information sufficiency and risk communication. *Media Psychology*, 6(1), 23-61.

Hair, J.F., G.T.M. Hult, C.M. Ringle en M. Sarstedt (2014) *A primer on partial least squares structural equation modeling (PLS-SEM)*. Los Angeles: SAGE Publications.

Hale, C. (1996) Fear of crime: A review of the literature. *International Review of Victimology*, 4(2), 79-150.

Henseler, J., C.M. Ringle en R.R. Sinkovics (2009) The use of partial least squares path modelling in international marketing. In R.R. Sinkovics (Ed.), *Advances in international marketing*. Emerald.

Henson, B., B.W. Reyns en B.S. Fisher (2013) Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice*, 29(4), 475-497.

Huang, D.-L., P.-L. Rau, G. Salvendy, F. Gao en J. Zhou (2011) Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, 69(12), 870-883.

Jackson, J. (2009) A psychological perspective on vulnerability in the fear of crime. *Psychology, Crime & Law*, 15(4), 365-390.

Jackson, J., N. Allum en G. Gaskell (2005) Perceptions of risk in cyber space. In R. Mansell en B.S. Collins (Ed.), *Trust and crime in information societies*. Northampton: Edward Elgar.

Jansen, J. en P. van Schaik (2016) Understanding precautionary online behavioural intentions: A comparison of three models. *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance*, 1-11.

Johnson, E.J. en A. Tversky (1983) Affect, generalization, and the perception of risk. *Journal of Personality and Social Psychology*, 45(1), 20-31.

Johnston, A.C. en M. Warkentin (2010) Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.

Liang, H. en Y. Xue (2010) Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.

Pleysier, S. (2011) Over objectieve en subjectieve onveiligheid: En de (on)zin van het rationaliteitdebat. *Tijdschrift voor Veiligheid*, 10(4), 24-40.

Ringle, C.M., S. Wende en A. Will (2005) SmartPLS 2.0.M3. Hamburg: SmartPLS. Verkregen via: www.smartpls.com.

Rogers, R.W. (1975) A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93-114.

Rotter, J.B. (1966) Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied*, 80(1), 1-28.
Savage, I. (1993) Demographic influences on risk perceptions. *Risk Analysis*, 13(4), 413-420.
Sjöberg, L. (2000) Factors in risk perception. *Risk Analysis*, 20(1), 1-11.
Slovic, P. (1987) Perception of risk. *Science*, 236(4799), 280-285.
Slovic, P., B. Fischhoff en S. Lichtenstein (1982) Why study risk perception?. *Risk Analysis*, 2(2), 83-93.
Slovic, P. en E. Peters (2006) Risk perception and affect. *Current Directions in Psychological Science*, 15(6), 322-325.
Starr, C. (1969). Social benefit versus technological risk. *Science*, 165, 1232-1238.
Statline (2013) *Beroepsbevolking: Behaalde onderwijs naar persoonskenmerken 2001-2012*. Verkregen via: http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=71822NED&D1=0&D2=a&D3=a&D4=0-1,4&D5=a&D6=0&D7=2,l&HD=130926-1540&HDR=T,G3,G5,G6,G1&STB=G2,G4.
Statline (2015) *Beroepsbevolking: Kerncijfers*. Verkregen via: http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=37296ned&D1=a&D2=0,10,20,30,40,50,60,(l-1),l&HD=130605-0924&HDR=G1&STB=T.
Statline (2016a) *Internet faciliteiten; particuliere huishoudens*. Verkregen via: http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=83291NED&D1=a&D2=0-5&D3=0&D4=a&VW=T.
Statline (2016b) *Bevolking; geslacht, leeftijd en burgerlijke staat, 1 januari*. Verkregen via: http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=7461BEV&D1=0&D2=0&D3=0-100,122-129&D4=0,10,20,30,40,50,l&HDR=T,G3&STB=G1,G2&VW=T.
Thaler, R.H. en C.R. Sunstein (2009) *Nudge: Improving decisions about health, wealth and happiness*. London: Penguin Group.
Vlaev, I., N. Chater en N. Stewart (2009) Dimensionality of risk perception: Factors affecting consumer understanding and evaluation of financial risk. *Journal of Behavioral Finance*, 10(3), 158-181.
Witte, K. (1996) Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, 1, 317-341.
Workman, M., W.H. Bommer en D. Straub (2008) Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799-2816.
Yousafzai, S., J. Pallister en G. Foxall (2009) Multi-dimensional role of trust in Internet banking adoption. *The Service Industries Journal*, 29(5), 591-605.
Yousafzai, S.Y., J.G. Pallister en G.R. Foxall (2003) A proposed model of e-trust for electronic banking. *Technovation*, 23(11), 847-860.