a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

Universiteit Utrecht

Van brief naar e-mail

Een adviesrapport over digitale betalingsherinneringen en de transitie van brief naar e-mail.

Paul Vaneveld

ASR

Managementsamenvatting

De trend van online communicatie en zakendoen is te negeren noch te stuiten. Ook in de verzekeringsbranche is de online transitie in volle gang. Zo voert a.s.r. zelf het label Ditzo, waar verzekeringen direct online zijn af te sluiten.

De voordelen van online verzekeren zijn manifest: zowel de klant als verzekeraar besparen tijd en geld. De nadelen of risico's blijven daarentegen vaak onderbelicht. Hoe wissel je bijvoorbeeld op een veilige, betrouwbare manier persoonsgegevens uit via de e-mail? a.s.r. wil de vruchten van online verzekeren en communicatie op een prudente manier plukken. Dit onderzoek mondt daarom uit in zes adviezen over online communicatie en zakendoen. Deze adviezen zullen zich veelal richten op de overstap van brief naar e-mail.

De ineffectiviteit van betalingsbrieven

Ik richt me in dit onderzoek op betalingsherinneringen van de productlijn Schade. Deze zijn ineffectief: te weinig klanten betalen hun achterstallige premie naar aanleiding van de brieven. a.s.r. wil de betalingsbrieven binnen enkele jaren omzetten in betalingsmails. Deze overgang biedt een kans om de huidige problemen van betalingsbrieven op te lossen. Het onderzoeksdoel is dan ook: *onderzoeken hoe e-mail ingezet kan worden om de effectiviteit, oftewel de hoeveelheid mensen die op tijd betaalt, van betalingsbrieven te vergroten.* Uit de resultaten van dit specifieke onderzoek, destilleer ik vervolgens ook adviezen over de overstap van brief naar e-mail in het algemeen.

Ik onderzocht via verschillende interne gesprekken de oorzaken van de ineffectiviteit van betalingsbrieven. De taalverzorging, schrijfstijl en inhoud waren goed. Ineffectiviteit bleek vooral het gevolg van twee praktische problemen:

- Klanten ontvangen de brief niet of op een verkeerd adres;
- Klanten vergeten te betalen na ontvangst van de brief

Het onderzoek

Vervolgens onderzocht ik experimenteel hoe a.s.r. van ineffectieve betalingsbrieven effectieve betalingsmails kon maken. Ik ontwierp e-mails met een directe link naar de betalingsomgeving, zodat klanten niet langer vergaten te betalen. Ook ontwikkelde ik e-mails met een sociaal contract - een tekstkader met een privacyverklaring en veiligheidsmaatregelen - om de ervaren privacy en veiligheid van de e-mails te vergoten. E-mails waarin bedrijven via een link om geld vragen, lijken namelijk op phishing (Hong, 2012). Deze gelijkenis kan angst en argwaan aanwakkeren bij de klant, waardoor hij afziet van een betaling.

Dit leidde tot vier verschillende e-mails, waarin de directe link en het sociaal contract afwisselend terugkwamen. Ik testte de reactie van klanten op deze e-mails via een vragenlijst in de online onderzoekstool MWM^2. Klanten kregen een scenario en de e-mail te lezen en beantwoordden vervolgens schaalvragen over onder meer hun intentie om te betalen en de privacy, veiligheid en betrouwbaarheid van de e-mail. Aan het onderzoek deden 191 proefpersonen mee, verdeeld over de vier condities. De vragen baseerde ik zoveel mogelijk op wijdverspreide en gevalideerde meetinstrumenten.

Resultaten

Het onderzoek leverde verschillende interessante resultaten op:

- Proefpersonen geven aan dat ze e-mails vaker lezen en minder snel vergeten dan brieven.
- De directe link leidde niet tot een sterkere intentie om te betalen, maar zorgde ook niet voor een negatievere beoordeling van de veiligheid en privacy van persoonsgegevens.
- Het sociaal contract (een kader met een privacyverklaring en veiligheidsmaatregelen) zorgde voor een sterkere intentie om te betalen, een positievere beoordeling van veiligheid, privacy, gebruikersgemak en leidde tot meer vertrouwen in a.s.r.

Conclusies

Uit het onderzoek trok ik grofweg de volgende vier conclusies:

- De overstap op e-mail maakt betalingsbrieven effectiever, onafhankelijk van de inhoud. Mensen geven aan dat ze hun inbox vaker bekijken en e-mails minder snel vergeten, waardoor e-mails op zichzelf al effectiever zijn dan brieven.
- Een directe link leidde niet, zoals ik verwachtte, tot een negatievere perceptie van de veiligheid en privacy van persoonsgegevens. De link roept dus waarschijnlijk geen angst of argwaan op voor phishing.
- De directe link leidde evenmin tot een sterkere intentie om de achterstallige premie te betalen. Ik vermoedde dat dit effect uitbleef door beperkingen van dit onderzoek.
- Het sociaal contract kan bijdragen aan de effectiviteit van betalingsmails. Dit contract bracht namelijk verschillende positieve effecten teweeg: een sterkere intentie om te betalen en een positievere inschatting van privacy, veiligheid en vertrouwen.

Aanbevelingen voor a.s.r.

Ik destilleerde zes aanbevelingen uit de voorgaande conclusies. Deze richtten zich enerzijds specifiek op de overstap van betalingsbrieven naar betalingsmails. Anderzijds formuleerde ik drie meer algemene adviezen over de transitie van brief naar e-mail binnen a.s.r.

Aanbeveling	
Aanbevelingen voor betalingsmails	1. Stap binnen afzienbare tijd (binnen twee jaar) over op e-mail. Onafhankelijk van de inhoud van de betalingsherinnering.
	2. Voeg een sociaal contract toe aan betalingsmails.
	3. Voeg een directe link toe naar de betalingsomgeving.
Aanbevelingen voor de overstap van brief naar e-mail	4. Maak in de overgang van brief naar e-mail gebruik van de grotere symboolvariatie van e-mail.
	5. Ontwikkel een beknopte, krachtige - maximaal vijf regels - privacyverklaring.
	6. Introduceer een persoonlijke veiligheidsindicator in e-mails over betalingsverkeer.

Inhoudsopgave

Bijlage **A**: Originele betalingsbrieven

Bijlage **B**: Het onderzoeksmateriaal

Bijlage **C**: De vragenlijst

Bijlage **D**: Vragenclusters en opschoning data

1.0 Inleiding

Bijna iedereen heeft weleens online een cadeautje gekocht of in een webshop kleding besteld. Door de toenemende digitalisering hoef je voor veel aankopen niet langer de winkelstraat in: ongeveer 60 procent van de Europese bedrijven doet online zaken en dit percentage blijft toenemen (Falk & Hagsten, 2015). Zakendoen is dus in toenemende mate online mogelijk.

Veel branches gaan mee in deze trend. Allerhande producten zijn online af te nemen: van de krant tot een auto en van boodschappen tot onderwijs. De populariteit van online zakendoen is eenvoudig verklaarbaar. Er zijn namelijk voordelen aan verbonden voor zowel consumenten als bedrijven: bedrijven kunnen hun bereik en bekendheid online vergroten, terwijl ze hun overheadkosten verlagen. Consumenten kunnen overal en altijd producten bekijken en kopen.

Ook verzekeringsmaatschappijen bieden hun producten steeds vaker online aan. Zo kunnen consumenten bij ING, Allsecur, Promovendum en Bewuzt binnen enkele klikken een verzekering afsluiten. a.s.r. is zich bewust van deze ontwikkeling. Toch zet a.s.r. niet direct volledig in op online zakendoen en communicatie. Online verzekeren roept namelijk ook vragen op. Hoe wissel je bijvoorbeeld op een veilige, betrouwbare manier persoonsgegevens uit via de e-mail? En hoe maak je de inhoud van een complex verzekeringsproduct duidelijk met digitale media? De mogelijke online voordelen staan dus buiten kijf. Het is echter nog onduidelijk hoe a.s.r. digitale media, zoals e-mail, kan gebruiken om deze potentiele voordelen te realiseren.

a.s.r. ziet dus de kracht van online communicatie en zakendoen, maar wil dit pad bedachtzaam betreden. In deze scriptie ga ik daarom onderzoeken hoe a.s.r. digitale media het beste kan inzetten. Hiervoor zal ik me specifiek richten op betalingsbrieven van de productlijn Schade. Dit zijn brieven die klanten van a.s.r. ontvangen als ze hun premie niet op tijd betalen. In deze brieven verzoekt a.s.r. de klant, steeds dringender, het openstaande bedrag te betalen. De betalingsbrieven van a.s.r. zijn ineffectief. Te weinig mensen betalen hun achterstallige premie naar aanleiding van de herinneringen. Hierdoor loopt a.s.r. veel inkomstem mis en spendeert ze meer aan communicatie. De vraag rijst dus hoe a.s.r. haar betalingsbrieven effectiever kan maken.

a.s.r. verstuurt betalingsbrieven nu nog per post. De doelstelling is om dit proces binnen enkele jaren te digitaliseren: klanten krijgen betalingsherinnering in de toekomst per e-mail en kunnen hun premie ook online betalen. Betalingsbrieven zijn hiermee een geschikte testcase voor a.s.r. De voor- en nadelen van online communicatie en zakendoen zijn voor betalingsbrieven namelijk kleinschalig te onderzoeken. De ineffectiviteit van de brieven is een concreet en behapbaar probleem. Door experimenteel te onderzoeken hoe e-mail het beste ingezet kan worden om dit probleem te verhelpen, vergaart a.s.r. meer kennis over effectief zakendoen en communiceren per e-mail. In dit onderzoek worden er dus verschillende betalingsmails experimenteel vergeleken. Uit deze vergelijking volgen breder toepasbare adviezen over communicatie en zakendoen per e-mail. Het is onderzoeksdoel luidt dan ook:

Onderzoeken hoe e-mail ingezet kan worden om de effectiviteit, oftewel de hoeveelheid mensen die op tijd betaalt, van betalingsbrieven te vergroten.

Om de dit doel te bereiken, volg ik in dit onderzoek de volgende stappen: eerst leg ik de communicatieve doelen van betalingsbrieven bloot aan de hand van een functionele analyse (Lentz & Pander Maat, 2004). Zo wordt duidelijk welke effecten betalingsbrieven idealiter zouden moeten sorteren en in hoeverre ze dit daadwerkelijk doen. Vervolgens beoordeel ik in hoeverre e-mail geschikt is om deze communicatieve doelen te bereiken, aan de hand van een mediumanalyse. Deze mediumanalyse mondt uit in verschillende suggesties om betalingsbrieven digitaal vorm te geven. Deze suggesties krijgen vervolgens vorm in experimenteel onderzoek, waarin de veronderstelde effecten worden getest. Uit de resultaten van dit onderzoek volgen aanbevelingen voor a.s.r. Deze aanbevelingen zullen zich enerzijds specifiek richten op het ontwerp van betalingsbrieven en anderzijds op communiceren en zakendoen per e-mail in het algemeen.

2.0 Functionele analyse: de beoogde communicatieve effecten van betalingsbrieven

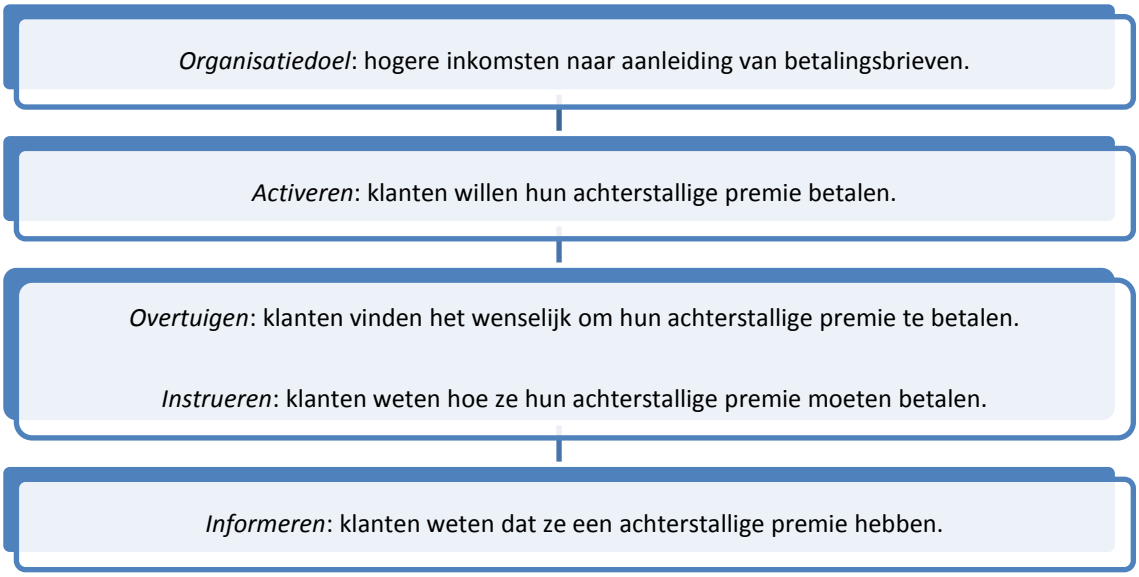
Om te onderzoeken hoe e-mail betalingsbrieven effectiever kan maken, is er kennis nodig over de functie van betalingsbrieven. Wat wil a.s.r. precies bereiken met betalingsbrieven? De specifieke communicatieve doelen van betalingsbrieven komen aan het licht door een functionele analyse. Dit is een bekende methode om communicatieve hoofddoelen en de ondergeschikte subdoelen te achterhalen (Lentz & Pander Maat, 2004).

Communicatieve doelen bestaan uit vier elementen: het gewenste communicatieve effect, het onderwerp, het publiek en het organisatiedoel. Voor betalingsbrieven zijn het onderwerp, publiek en organisatiedoel altijd gelijk.

- Het onderwerp: de betaling van achterstallige premie
- Het publiek: klanten van a.s.r. met een achterstallige premie in de productlijn Schade
- Het organisatiedoel: hogere inkomsten naar aanleiding van betalingsbrieven.

a.s.r. wil dus haar inkomsten verhogen door betalingsbrieven over achterstallige premie, gericht aan klanten van de productlijnen Schade. Welke communicatieve effecten moeten de brieven sorteren om dit organisatiedoel te behalen?

Ten eerste moeten klanten hun achterstallige premie *willen* betalen (activeren). Zonder de intentie om te betalen, gebeurt er immers niets. Klanten die willen betalen, moeten ook geloven in de oprechtheid, authenticiteit van het verzoek (overtuigen). Als zij er niet van overtuigd zijn dat ze een betalingsachterstand hebben, zullen zij niet betalen. Ten derde moeten klanten weten *hoe* ze moeten betalen (instrueren). Als laatste moeten klanten weten *dat* ze een achterstallige premie hebben (informeren). Al deze communicatieve effecten zijn hiërarchisch te ordenen, zoals is weergeven in de doelenboom (figuur 1). Als betalingsbrieven al deze communicatieve effecten realiseren, zal het organisatiedoel behaald worden.



Figuur 1: de beoogde communicatieve effecten van betalingsbrieven.

3.0 Probleemanalyse: de huidige problemen in betalingsbrieven

De functionele analyse maakte de beoogde communicatieve effecten van betalingsbrieven duidelijk. De huidige betalingsbrieven genereren te weinig inkomsten. De vraag rijst dan ook welke communicatieve effecten onvoldoende worden bereikt. Om dit vast te stellen, licht ik eerst kort de inhoud en het bedrijfsproces van betalingsbrieven toe (3.1). Vervolgens zet ik uiteen welke elementen ervoor zorgen dat de communicatieve effecten niet worden behaald (3.2).

3.1 De inhoud en het bedrijfsproces van betalingsbrieven

In totaal zijn er bij de productlijn Schade drie soorten betalingsherinneringen, die a.s.r. trapsgewijs verzendt. Eerst krijgt de klant een brief met een acceptgiro. Ten tijde van deze brief is de betalingsdeadline nog niet verstreken. In de eerste brief verzoekt a.s.r. de klant dan ook simpelweg om de premie voor de deadline te betalen. Als de klant enkele dagen voor de uiterste datum nog niet heeft betaald, volgt de tweede brief: een betalingsherinnering. Hierin herinnert a.s.r. de klant aan het openstaande bedrag en de betalingsdeadline. Ook staan de consequenties van wanbetaling beschreven: 10 euro herinneringskosten en het risico op een boete, omdat een verzekering verplicht is. Als de premie enkele dagen na de deadline nog niet is gestort, volgt er een derde brief: een aanmaning. In deze brief deelt a.s.r. de klant mee dat er 10 euro herinneringskosten in rekening worden gebracht. Ook maakt de brief duidelijk dat de klant niet langer verzekerd is, wat een strafbaar feit is. In totaal zijn er dus drie betalingsherinnering met een steeds strengere toon. Alle drie de brieven zijn te vinden in bijlage A. Het hele proces is weergegeven in de volgende tabel:

Tabel 1: het verzendproces en de inhoud van betalingsbrieven

Brief	*Tijdstip*	*Inhoud*
Acceptgiro	Twee weken voor de betalingsdeadline	-Een acceptgiro -Een betalingsherinnering
Eerste betalingsherinnering	Enkele dagen voor betalingsdeadline	-Een betalingsherinnering -De consequenties van te laat betalen: 10 euro herinneringskosten en het verzuimen van de wettelijke verzekeringsplicht
Aanmaning	Enkele dagen na de betalingsdeadline	-Een betalingsherinnering -Herinnering aan de vestreken betalingsdeadline -De consequenties van de verstreken deadline: 10 euro herinneringskosten, het verlopen van de verzekering en het verzuimen van de wettelijke verzekeringsplicht.

3.2 Problemen in betalingsbrieven: communicatieve effecten die onvoldoende worden bereikt

De beoogde communicatieve effecten, de inhoud en het bedrijfsproces van betalingsbrieven zijn nu uiteengezet. De vraag rijst nu dan ook welke communicatieve effecten onvoldoende worden bereikt en wat hier de oorzaak van is. Om deze vraag te beantwoorden, voerde ik verschillende gesprekken binnen a.s.r.:

- Fransje van der Voort: teamleider communicatie
- Lianne Peters: communicatieadviseur
- Christel van Capelleveen: copywriter

Fransje van der Voort weet als teamleider veel van de communicatieve problemen binnen a.s.r. Daarbij was zij betrokken bij eerder onderzoek naar betalingsbrieven (Brand, 2014), waardoor ze veel voorkennis heeft over het onderwerp. Lianne Peters besteedt veel tijd aan documentontwerp en tekstontwikkeling. Ze is daardoor in staat om snel problemen te herkennen in het ontwerp van betalingsbrieven. Als laatste weet Christel van Capelleveen welke klachten er onder klanten leven. Christel hielp mij dus om betalingsbrieven te bekijken vanuit het oogpunt van de klant. Vanuit verschillende expertises, schenen Fransje, Lianne en Christel hun licht op de problemen in betalingsbrieven. De problemen die zij aankaartten, bundelde ik vervolgens in de probleemanalyse.

3.2.1 Uitkomst van de gesprekken binnen a.s.r.

Ik deelde de gesprekken met Fransje, Lianne en Christel op in vier onderwerpen: stijl, taalverzorging, inhoud en klantervaringen. De eerste drie onderwerpen gaan over de kwaliteit van de brief zelf en hoe de klant deze ervaart. Het laatste onderwerp, klantervaringen, gaat over persoonlijke redenen van klanten om betaling uit te stellen: redenen die niet gerelateerd zijn aan de kwaliteit van de brief zelf. Door ook de klantervaring in de probleemanalyse op te nemen, probeer ik kokervisie te voorkomen op de kwaliteit van betalingsbrieven. De ineffectiviteit van betalingsbrieven kan immers oorzaken hebben die buiten de brieven zelf liggen.

Allereerst heb ik met Fransje en Lianne de **taalverzorging** van de brieven besproken, vanuit hun expertise als communicatieadviseur. Wij concludeerden dat de betalingsbrieven taalkundig goed zijn. De brieven bevatten geen spellings- of interpunctiefouten. De ineffectiviteit van betalingsbrieven is waarschijnlijk dus geen taalkundig probleem. De brieven zijn ontworpen door meerdere communicatieprofessionals en uitgebreid geredigeerd. Daarbij vertelde Christel dat er zelden klachten binnenkomen over de taalkundige kwaliteit van brieven. Klanten van a.s.r. vinden de taalkundige kwaliteit dus afdoende.

Ten tweede heb met Fransje de **stijl** van de brieven besproken. We bespraken onder meer de toon en schrijfstijl van de brieven. Naar de toon van betalingsbrieven is namelijk eerder onderzoek gedaan binnen a.s.r. (Brand, 2014). Fransje begeleidde dit onderzoek en kon mij dus meer vertellen over de uitkomsten. De toon is relevant vanwege het dringende betalingsverzoek in de brieven. Het betalingsverzoek bedreigt de autonomie en vrijheid van de geadresseerden en is daarmee een *face threatening act* (FTA) (Brown & Levinson, 1987). Klanten zullen het verzoek dan ook niet zonder meer uitvoeren. Zij willen namelijk hun autonomie en vrijheid, hun *negative face*, behouden (Brown & Levinson, 1987). Om klanten aan te zetten tot betaling, moet het verzoek beleefd zijn. De toon van het bericht moet dus passend zijn. Als het beta-

lingsverzoek beleefd is, verkleint het effect van FTA. Klanten zullen dan eerder overgaan tot betaling.

De toon van betalingsbrieven is dus zeer relevant. Op het eerste gezicht lijkt de toon voor verbetering vatbaar. Vooral in de eerste betalingsherinnering en aanmaning – de tweede en derde brief – verzoekt a.s.r. de klant vrij onomwonden om te betalen. Zo staan sommige zinnen in de imperatief: "Vergeet dan niet het betalingskenmerk te vermelden." In andere zinnen is alleen het woord 'alstublieft' toegevoegd om de toon vriendelijker te maken. Uit eerder onderzoek binnen a.s.r. bleek echter dat klanten een vriendelijkere toon niet hoger waardeerden. Sanne Brand (2014) onderzocht het effect van beleefdere verzoeken en mededelingen, zoals: "Wat vervelend dat de camera kapot is! Toch moeten wij u helaas laten weten dat we de schade niet vergoeden." Dergelijke beleefde zinnen bleken *meer* negatieve emoties op te roepen. Deze vorm van beleefdheid lijkt dus averechts te werken. Betalingsbrieven worden waarschijnlijk dus niet effectiever door een vriendelijkere, beleefdere toon.

Naast de toon, analyseerde ik schrijfstijl van de brieven. Hierbij lette ik bijvoorbeeld op zinnen in de lijdende, passieve vorm en tangconstructies. De stijl van de brieven is goed: zinnen zijn kort, bevatten zelden tangconstructies en zijn voornamelijk actief. Daarbij vermijdt a.s.r. technische termen, ofwel jargon. De brieven zijn hierdoor voor iedereen begrijpelijk. De ineffectiviteit van betalingsbrieven ligt dus aan de toon noch schrijfstijl.

Ten derde heb ik met Christel en Lianne de **inhoud** van de brieven besproken. Vinden klanten in betalingsbrieven alle informatie die ze nodig hebben? De inhoud van de brieven lijkt volledig. De klant weet hoeveel hij moet betalen, waarom hij moet betalen, hoe hij moet betalen en wat de consequenties zijn van wanbetaling. Christel vertelde daarbij dat er geen klachten binnenkomen over de inhoud van betalingsbrieven. Klanten stellen betaling dus niet uit door een gebrek aan kennis. Informatie toevoegen of verwijderen leidt waarschijnlijk dus niet tot effectievere betalingsbrieven.

Tabel 2: Samengevatte conclusie uit gesprekken binnen a.s.r. over betalingsbrieven

Onderwerp		*Conclusies uit gesprekken binnen a.s.r.*
Taalverzorging		• Geen spellings- en interpunctiefouten
Stijl	Toon	• Redelijk koele toon • Sporadisch gebruik imperatief • Relatief onomwonden betalingsverzoek
	Schrijfstijl	• Weinig tangconstructies • Weinig passieve vormen • Weinig jargon
Inhoud		• Voldoende informatie over de hoogte van de premie • Voldoende informatie over de aanleiding van de achterstand • Voldoende instructie om te betalen • Voldoende informatie over consequenties van wanbetaling
Klantervaring		• Klanten hebben te weinig geld • Klanten ontvangen de betalingsbrieven niet • Klanten vergeten te betalen

Als laatste heb ik met Christel gesproken over de **klantervaring**. Zij is bij Ditzo, een onderdeel van a.s.r., nauw betrokken bij de afdeling klantcontact. Met haar sprak ik over bedreigingen voor de effectiviteit buiten de betalingsbrieven zelf. Welke andere oorzaken weerhouden klanten van betaling? Ten eerste gaf Christel aan dat sommige klanten simpelweg te weinig geld hebben. Het is onduidelijk hoeveel klanten hiermee kampen. Dit probleem ligt echter buiten het bereik van a.s.r. en is voor dit onderzoek dus irrelevant.

Daarbij gaf Christel aan dat sommige brieven niet aankomen bij klanten. Zo kunnen brieven aankomen op het verkeerde postadres of per ongeluk terechtkomen bij het oud papier. Dit is een veelgehoorde klacht. Veel klanten geven aan, als er eenmaal contact is, niet eerder brieven te hebben ontvangen. Als laatste vergeten veel klanten te betalen. Klanten nemen zich vaak voor zo snel mogelijk te betalen. Voordat ze echter in de gelegenheid zijn om te betalen, zijn ze de betalingsbrief alweer vergeten. Om de achterstallige premie te betalen, moet de acceptgiro immers gepost worden. Klanten zijn vaak niet in de gelegenheid om de acceptgiro direct te verzenden, waardoor ze de betalingsbrief later vergeten. Al met al lijken praktische beperkingen de effectiviteit van betalingsbrieven in te perken: klanten ontvangen het bericht niet of vergeten te betalen.

3.2.2 Communicatieve effecten die onvoldoende worden bereikt

Uit de gesprekken binnen a.s.r. kwamen verschillende beperkingen naar voren voor de effectiviteit van betalingsbrieven. De vraag rijst hoe deze beperkingen zich verhouden tot de functionele analyse: welke communicatieve effecten staan ze in de weg?

Klanten stellen betaling veelal uit door praktische problemen. Zo vergeten ze om naar aanleiding van de brief te betalen of ontvangen ze de brief helemaal niet. Beide problemen raken het informatieve communicatieve effect: klanten weten *dat* ze een achterstallige premie hebben. Als klanten brieven niet krijgen of vergeten, weten ze immers (tijdelijk) niet meer dat er een betalingsachterstand is. Bij de overgang van betalingsbrieven naar betalingsmails, is het dus zinvol om het informatie-effect te versterken: meer klanten moeten het bericht ontvangen, terwijl minder klanten het ontvangen bericht moeten vergeten.

4.0 De overstap van brief naar e-mail

De probleemanalyse van betalingsbrieven mondde uit in een aantal verbeterpunten. In dit hoofdstuk ga ik uiteenzetten hoe e-mail kan worden ingezet om deze verbeterpunten te realiseren. Hiertoe zal ik eerst een mediumanalyse van e-mail maken, waarin kenmerkende eigenschappen worden benadrukt (4.1) Op basis van deze mediumanalyse zal ik een oplossing presenteren voor de huidige problemen in betalingsbrieven (4.2).

4.1 De eigenschappen van e-mail

Vooral praktische problemen spelen de effectiviteit van betalingsbrieven parten: klanten ontvangen de brieven niet of vergeten te betalen. Deze problemen bemoeilijken een informatief effect uit de functionele analyse: klanten weten *dat* ze een achterstallige premie hebben. Om tot een passende oplossing te komen voor dit probleem, is het nuttig om te inventariseren in hoeverre e-mail geschikt is voor informatieoverdracht. Leent e-mail zich om klanten te informeren over hun achterstallige premie?

4.1.1 Media Apropiateness

De kracht van communicatie schuilt in een sterke unie van medium en boodschap (Rice, 1993). De eigenschappen van een medium en boodschap moeten rijmen om effectief te communiceren. De Media Apropiateness Theory (Rice, 1993) is een goede eerste lakmoesproef van de match tussen een medium en de boodschap. Rice poneert in deze theorie een schaal van geschiktheid van media voor uiteenlopende taken. Deze schaal baseert hij op een uitgebreide onderzoekstraditie naar mediumgeschiktheid. Uit vele voorgaande onderzoeken is namelijk een redelijk stabiele rangschikking naar voren gekomen van media per taak. Hoewel mediavoorkeuren en -gebruik contextueel verschillen, geeft de schaal dus wel een indicatie van de geschiktheid van een medium voor een bepaalde taak (Rice, 1993). Volgens deze schaal kan e-mail het best worden ingezet voor twee activiteiten: het *uitwisselen van informatie* en *contact onderhouden*.

E-mail lijkt dus een geschikt medium om mensen te informeren over hun achterstallige premie. De ineffectiviteit van betalingsbrieven ontstaat vooral doordat klanten brieven niet ontvangen (uitwisselen van informatie) of vergeten (in contact blijven). E-mail is volgens de schaal bij uitstek een passend medium om dergelijke problemen te verhelpen. Het medium is ten eerste geschikt om informatie uit te wisselen, wat het bereik van betalingsbrieven zou kunnen vergroten. Daarbij leent het medium zich ook om in contact te blijven na het oorspronkelijke bericht, waardoor minder klanten de betalingsbrieven zouden vergeten.

De wetenschap dat e-mail een geschikt medium is om problemen in betalingsbrieven te verhelpen, is echter niet afdoende. Om tot een concrete oplossing te komen, is er meer kennis nodig over de eigenschappen van e-mail. Waarom is e-mail een geschikt medium om informatie over te brengen en in contact te blijven? Ofwel, hoe kan a.s.r. e-mail inzetten om deze doelen te bereiken?

4.1.2 Media Synchronicity

De geschiktheid van e-mail voor informatieoverdracht is te verklaren vanuit de Media Synchronicity Theory (MST) (Dennis & Valachich, 1999). Volgens deze theorie is alle communicatie op te delen in twee processen: *conveyance* en *convergence*. Conveyance is het verspreiden van benodigde en nieuwe informatie. Convergence is tot een gemeenschappelijk begrip komen van

deze informatie. Dennis en Valachich (1999) stellen dus dat alle communicatie bestaat uit informatieoverdracht en het gelijkstemmen van de interpretatie hiervan.

In tegenstelling tot de Media Apropiateness Theory (Rice, 1993), kent deze theorie gaan rangschikking van media. E-mail is volgens de MST dus niet absoluut het beste medium voor informatieoverdracht. De geschiktheid van een medium is namelijk afhankelijk van variabele factoren: de wijze van gebruik, de gebruikers en de sociale context. Een medium is geschikt als zijn eigenschappen aansluiten bij de wijze van gebruik, gebruikers en context. Zo zullen veel mensen een gebruiksaanwijzing graag per e-mail ontvangen. Als iemand de gebruiksaanwijzing daarentegen niet direct begrijpt, kan mondelinge uitleg effectiever zijn. De geschiktheid van een medium verschilt volgens de MST dus situationeel.

Hoewel er geen absolute rangschikking van mediageschiktheid mogelijk is, blijkt uit de MST wel in hoeverre mediaeigenschappen bruikbaar zijn voor *conveyance* of *convergence*. Conveyance is de overdracht van informatie, terwijl convergence een gedeeld begrip van informatie behelst. De ineffectiviteit van betalingsbrieven is een probleem van conveyance: de informatie uit betalingsbrieven is begrijpelijk (convergence), maar komt geregeld niet aan of wordt vergeten (conveyance). Om te verklaren waarom e-mail geschikt is voor informatieoverdracht, moet dus duidelijk worden welke kenmerken van e-mail conveyance faciliteren.

De volgende eigenschappen van e-mail ondersteunen de overdracht van informatie, ofwel conveyance: symboolvariatie, parallellisme, mogelijkheid tot voorbereiding en herverwerkbaarheid. Hierna zal ik kort uiteenzetten wat de eigenschappen behelzen en hoe ze bijdragen aan conveyance.

- **Symboolvariatie** refereert aan de hoeveelheid manieren waarop informatie gecommuniceerd kan worden. E-mail heeft veel verschillende symbolen, zoals plaatjes, tekst en hyperlinks. De veelheid aan symbolen ondersteunt de overdracht van informatie (Dennis & Valachich, 1999).
- **Parellelisme** refereert aan de hoeveelheid mensen die tegelijkertijd kunnen communiceren. Parellelisme is dan ook vooral belangrijk voor informatieverspreiding binnen grote groepen: het zorgt ervoor dat alle groepsleden de benodigde informatie ontvangen. Een e-mail kan meerdere geadresseerden hebben, wat de overdracht van informatie vereenvoudigt (Dennis & Valachich, 1999).
- **Mogelijkheid tot voorbereiding**: een medium waarin de zender een bericht kan voorbereiden, maakt het eenvoudiger om doordacht te communiceren. De zender kan lang stilstaan bij de inhoud van een e-mail, waardoor de informatieoverdracht effectiever wordt (Dennis & Valachich, 1999).
- **Herverwerkbaarheid** refereert aan de herhaaldelijke beschikbaarheid van een bericht. Een gesproken bericht is bijvoorbeeld vluchtig, terwijl een e-mail kan worden herlezen. Door de herverwerkbaarheid van e-mail is informatie altijd beschikbaar, wat effectieve overdracht bevordert (Dennis & Valachich, 1999).

Slim, effectief gebruik van deze eigenschappen, zou de problemen kunnen verkleinen in de informatieoverdracht van betalingsbrieven. Maar wat is slim gebruik? Hoe kan a.s.r. de kwaliteiten van e-mail concreet inzetten om de effectiviteit van betalingsbrieven op te vijzelen?

4.1.3 De verschillen tussen brief en e-mail

E-mail heeft verschillende eigenschappen die informatieoverdracht faciliteren. Hierin is e-mail echter niet uniek. Ook geschreven brieven, het huidige medium voor de betalingsherinneringen, heeft dergelijke kwaliteiten. Zo zijn zowel brieven als e-mails te herlezen (herverwerkbaarheid). Een oplossing voor de ineffectiviteit van betalingsbrieven, ligt dus waarschijnlijk in de *verschillen* tussen brief en e-mail. Welke eigenschappen voor conveyance, ofwel informatieoverdracht, van brief en e-mail komen niet overeen?

Tabel 3: Media-eigenschappen van brief en e-mail

	Symboolvariatie	*Parallellisme*	*Voorbereiding*	*herverwerkbaarheid*
e-mail	**Hoog**	Gemiddeld	Hoog	Hoog
Brief	Laag-gemiddeld	Hoog	Hoog	Hoog

Een vergelijking van e-mails en brieven toont twee verschillen: e-mail is bevorderlijker dan geschreven brieven voor symboolvariatie, maar ongeschikter voor parallelisme. E-mail heeft dus één eigenschap die zich beter leent voor conveyance, oftewel de verspreiding van informatie: een grotere symboolvariatie (Dennis & Valachich, 1999). Geschreven brieven bestaan namelijk uitsluitend uit tekst en afbeeldingen. In e-mails is de mogelijke symboolvariatie daarentegen veel groter: een e-mail kan bestaan uit tekst, afbeeldingen, geluid, animatie, links en film. In de overstap van brief naar e-mail is symboolvariatie dus waarschijnlijk de sleutel tot effectievere betalingsbrieven. De grotere symboolvariatie maakt het namelijk mogelijk om effectiever informatie over te dragen.

4.2 Een directe link naar de betalingsomgeving

De vraag rijst hoe de grotere symboolvariatie van e-mail kan worden gebruikt. Om deze vraag te beantwoorden, is er een korte terugblik nodig op het probleem. De ineffectiviteit van betalingsbrieven vloeit voort uit ontoereikende informatieoverdracht. Klanten weten niet dat ze een betalingsachterstand hebben, doordat ze:

- De betalingsbrieven niet ontvangen;
- Na ontvangst van de betalingsbrieven vergeten te betalen.

Om te achterhalen hoe e-mail deze problemen kan verhelpen, loont het om naar voorgangers te kijken. a.s.r. hoeft het wiel niet opnieuw uit te vinden. Andere bedrijven worstelde ongetwijfeld met dezelfde problematiek. Ik heb binnen de verzekeringsbranche geen voorbeelden kunnen vinden van oplossingen voor soortgelijke problemen. In de detailhandel is er wel een sprekend voorbeeld: Bol.com [Bol]. Bol is een online warenhuis. Het bedrijf verkoopt door heel Nederland allerhande goederen die thuis worden bezorgd. Bol biedt klanten de mogelijkheid om hun bestelling achteraf te betalen. Klanten hoeven producten dus pas af te rekenen nadat ze thuis zijn bezorgd. Om te voorkomen dat betalingen worden vergeten, stuurt Bol klanten een e-mail met een betalingsherinnering. Klanten vinden in deze e-mail een link naar een online betalingsomgeving. Door simpelweg op de link te klikken, kunnen klanten het product direct betalen.

Een dergelijke e-mail met link heeft twee voordelen. Ten eerste leidt het gebruik van e-mail, onafhankelijk van de inhoud, waarschijnlijk tot meer en vroegere betalingen. Een e-mail komt

namelijk meestal binnen op verschillende apparaten, zoals een computer/laptop, smartphone of tablet. Zo werd in 2014 al 53 procent van de e-mails bekeken op een smartphone of tablet (Van Rijn, 2015). Hierdoor is de kans relatief klein dat klanten het bericht niet ontvangen. Het bericht komt immers op meerdere 'plekken' binnen. Daarbij bekijken mensen hun e-mail zeer geregeld. De statistieken lopen op dit vlak uiteen, maar dat e-mail dagelijks wordt bekeken, staat buiten kijf (Cecchinato, Cox & Bird, 2014; Matt Rosoff, 2015). Brieven kunnen daarentegen verkeerd worden bezorgd of bij het oud papier belanden, zoals bleek uit de gesprekken binnen a.s.r. (3.2). Het gebruik van e-mail op zich kan betalingsbrieven dus effectiever maken. Het is immers waarschijnlijk dat de groep klanten die de betalingsherinnering niet ontvangen, slinkt bij het gebruik van e-mail. Deze bevindingen monden uit in de volgende hypothese:

H1: Betalingsmails worden door meer klanten gelezen dan betalingsbrieven.

Daarbij vergeten klanten minder snel te betalen door de directe link in de e-mail. Bol maakt slim gebruik van de *symboolvariatie* van e-mail. Door een link op te nemen, hoeven klanten betaling niet langer uit te stellen - een mogelijkheid die papieren brieven niet bieden. Hiermee ondervangt Bol een probleem waar a.s.r. nu mee kampt: klanten vergeten te betalen na ontvangst van een betalingsbrief. Al met al lijkt een e-mail met een directe link naar de betalingsomgeving dus een doeltreffende oplossing voor de ineffectiviteit van betalingsbrieven. Dit mondt uit in de volgende hypothese:

H2: Betalingsmails met een directe link naar de betalingsomgeving leiden tot minder uitstel van betaling dan betalingsmails zonder directe link.

5.0 Risico's van de overstap van brief naar e-mail

Betalingsmails lijken de problemen van de betalingsbrieven in eerste instantie te kunnen verhelpen. De overstap naar e-mail kan echter ook nieuwe problemen met zich meebrengen. Een boodschap in een volledig nieuw medium, kan ook leiden tot algeheel nieuwe problemen. In dit hoofdstuk sta ik daarom ook stil bij de risico's van de overstap en methoden om deze te ondervangen. In hoofdstuk 5.1 ga ik in op bedreigingen voor de effectiviteit van betalingsmails. In hoofdstuk 5.2 vertaal ik deze bedreigingen via een functionele analyse in communicatieve effecten. Vervolgens draag ik in 5.3 een methode aan om deze risico's te beperken.

5.1 Phishing: de ervaren veiligheid en privacy van klantgegevens in betalingsmails

Een betalingsmail (met een directe link) zou de problemen met informatieoverdracht kunnen verkleinen. Er zijn helaas ook risico's verbonden aan deze vorm van betalingsherinneringen. Een betalingsverzoek per e-mail lijkt namelijk al snel op *phishing*. Phishing is het sturen van e-mails onder een valse identiteit om geadresseerden te verleiden persoonlijke informatie te delen of geld te geven (Hong, 2012). Phishing heeft vele verschijningsvormen. De gemene deler is vaak een link: de geadresseerde komt via een link in de e-mail terecht op een neppe site, waar hij persoonsgegevens kan verliezen. Zo kan het een verzoek zijn om een online vragenlijst in te vullen voor een geldbedrag. In deze vragenlijst staan vragen over persoonlijke gegevens, die criminelen kunnen misbruiken. In andere berichten wordt lezers verteld dat hun wachtwoord aan vernieuwing toe is. Via een link komt de lezer op een neppe site, waar hij, door zijn oude wachtwoord op te geven, een nieuw wachtwoord kan aanvragen. Dit oude, nog geldige wachtwoord kan vervolgens worden misbruikt door criminelen (Hong, 2012).

Phishing is een omvangrijk probleem. Elke dag komen er zo'n 16 miljoen phishing e-mails door beveiligingsfilters heen. De helft hiervan, 8 miljoen e-mails, wordt ook daadwerkelijk geopend. In een tiende van de geopende e-mails klikken lezers ook daadwerkelijk op een link, waardoor ze een groot risico lopen op gegevensverlies (Get Cyber Save, 2015). De schattingen van de financiële schade door phishing lopen sterk uiteen: van 61 miljoen tot 3 biljoen dollar per jaar (Hong, 2012). Het staat wel vast dat phishing een grote schadepost is voor zowel bedrijven als particulieren.

De omvang van het probleem is navenant aan de bekendheid: 95% van de mensen kennen het begrip 'phishing' (Downs, Holbrook & Cranor, 2006). Deze algemene bekendheid vertaalt zich ook in argwaan, angst voor transacties per e-mail en online zakendoen in het algemeen. Zo vinden mensen e-mail een ongeschikt medium op persoonlijke informatie te delen (Rice, 1993). 95% van de mensen die online zakendoen, hebben door argwaan wel eens persoonsgegevens voor zich gehouden (Hoffman, Novak & Peralta, 1999). 75% van de mensen vinden een e-mail met link van een bank verdacht (Downs et al., 2006). Zij zullen het verzoek in dergelijke e-mails niet direct opvolgen, met het oog de veiligheid en privacy van hun gegevens (Downs et al., 2006). Een e-mail zonder persoonlijke aanhef, roept zelfs bij 85% van de mensen argwaan op. Door phishing kijken geadresseerden dus argwanend naar e-mails waarin (via een link) persoonlijke gegevens worden gevraagd. Zij zijn niet langer zeker van de veiligheid en privacy van hun persoonsgegevens.

5.1.2 De gelijkenis tussen betalingsmails en spear phishing

De omvang en consequenties van phishing zijn nu duidelijk. Maar waarom lijkt de betalingsmail van a.s.r. precies op phishing? Phishing e-mails worden meestal massaal en internationaal verzonden, waardoor ze vol spellingsfouten staan en onpersoonlijk zijn (Hong, 2012). De e-mail van a.s.r. is daarentegen persoonlijk geadresseerd en foutloos geschreven. De bekendste en zorgwekkendste kenmerken van phishing zijn in de betalingsmails dus afwezig.

Toch kunnen betalingsmails van a.s.r. bij de geadresseerden argwaan oproepen. De e-mails lijken namelijk op een relatief nieuwe vorm van phishing: *spear phishing*. Bij spear phishing gebruiken criminelen persoonlijke informatie en bekende contexten of relaties om hun slachtoffers te misleiden (Caputo et al., 2014). Zo krijgen geadresseerden valse e-mails uit naam van de bank waar zij daadwerkelijk rekeninghouder zijn. De persoonlijke en realistische informatie maakt spear phishing zeer effectief: spear phishing levert veertigmaal meer op dan oudere, onpersoonlijkere vormen van phishing (Caputo et al., 2014)

De betalingsmail van a.s.r. heeft dus karakteristieken van spear phishing. Het is een *persoonlijk* bericht van een *bekend* bedrijf, waarin (via een link) om geld wordt gevraagd. Dezelfde kenmerken die de e-mail doen lijken op spear phishing, maken het bericht echter ook geloofwaardig. Waarom zullen klanten van a.s.r. een betalingsherinnering van hun eigen verzekeraar kenmerken als verdacht? Om deze vraag te beantwoorden, is er meer informatie nodig over de risico-inschatting van e-mails. Hoe bepalen mensen of een e-mail mogelijk bedreigend is voor de privacy en/of veiligheid van hun gegevens?

De risico-inschatting van e-mails

De betalingsmail heeft drie verdachte kenmerken voor klanten van a.s.r. – 'verdacht' betekent bedreigend voor de veiligheid en privacy van persoonlijke gegevens. Ten eerste kunnen klanten het bericht verdacht vinden omdat het onconventioneel is. a.s.r. stuurt al haar betalingsherinnering per post. Een betalingsmail zal dus nieuw zijn voor alle klanten. Bekendheid is één van de belangrijkste factoren in de risico-inschatting van e-mails: als geadresseerden niet eerder een vergelijkbare e-mail van een afzender ontvingen, zullen ze het bericht eerder verwijderen (Downs et al., 2006). Er bestaat dus een kans dat klanten betalingsmails niet opvolgen, omdat ze nieuw zijn.

Daarbij is de e-mail verdacht omdat a.s.r. vraagt om bankgegevens. Klanten moeten immers inloggen op een website voor internetbankieren. Uit onderzoek blijkt dat een verzoek om bankgegevens zeer precair is. Mensen beschouwen bankgegevens als de meest privacygevoelige informatie en misbruik van deze gegevens als het onwenselijkste gevolg van phishing (Downs et al., 2006; Metzger, 2007). Het verzoek om bankgegevens weegt dus zwaar in de risico-inschatting. Enige twijfel over de authenticiteit van de e-mail kan klanten hierdoor al afhouden van betaling.

Als laatste is de betalingsmail verdacht vanwege de urgentie van het verzoek. In de betalingsherinnering wordt de klant steeds dringender verzocht om te betalen. Urgentie is een kenmerk van phishing: geadresseerden moeten *direct* hun wachtwoord vernieuwen of *nu* een 'antivirus-programma' installeren (Singleton, 2005). Een urgent verzoek, zeker een urgent verzoek om bankgegevens, kan betaling dus verhinderen.

Concluderend is het, door de drie verdachte kenmerken, waarschijnlijk dat klanten van a.s.r. betalingsmails als een bedreiging zullen ervaren voor de veiligheid en privacy van hun gegevens, ondanks authenticiteit van het bericht. Hierdoor zullen klanten eerder afzien van betaling, wat de effectiviteit van betalingsmails verkleint.

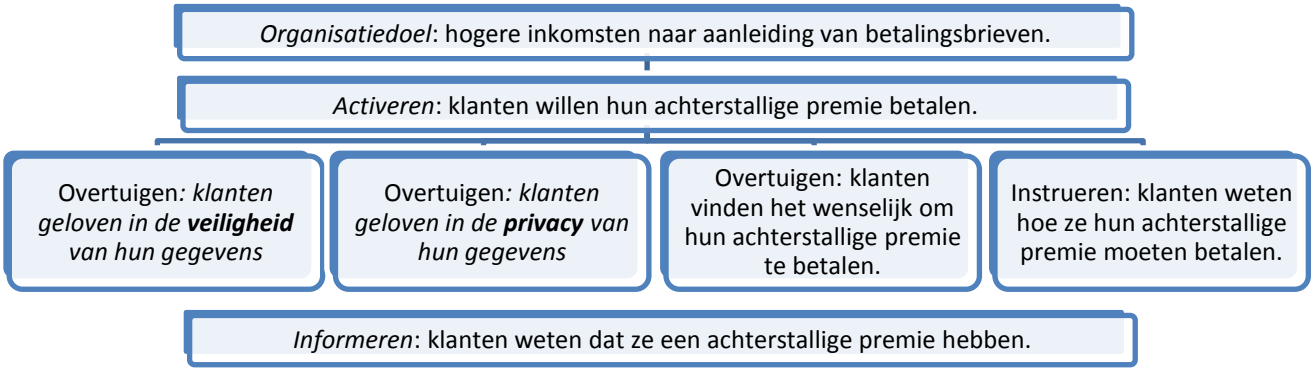
Ik verwacht daarbij dat betalingsmails met directe link naar de betalingsomgeving als een grotere bedreiging worden ervaren voor de privacy en veiligheid van gegevens. De meeste vormen van phishing werken namelijk via links (Caputo et al., 2014). Via de link kunnen klanten op een vervalste site terecht komen, waar ze persoonsgegevens verliezen. In de betalingsmail zonder link lopen klanten nog steeds risico's: ze zouden geld over kunnen maken naar een vervalst rekeningnummer of malware kunnen installeren door de mail te openen (Hong, 2012). Het risico op verlies van persoonsgegevens is echter groter in de betalingsmails met link naar de betalingsomgeving. Dit mondt uit in de volgende hypothese:

H3: Betalingsmails met een directe link naar de betalingsomgeving worden als een grotere bedreiging ervaren voor de privacy en veiligheid van persoonsgegevens dan betalingsmails zonder link naar de betalingsomgeving.

5.2 Problemen in betalingsmails: communicatieve effecten die onvoldoende worden bereikt

Klanten van a.s.r. kunnen betalingsmails dus verdacht vinden, waardoor ze afzien van betaling. Voordat er een oplossing geformuleerd kan worden voor dit probleem, is er een terugblik nodig op de functionele analyse. Als bekend is welke communicatieve effecten onvoldoende worden gerealiseerd door het phishing-probleem, kunnen er immers toegespitste maatregelen worden genomen.

De functionele analyse kan worden uitgebreid op basis van het phishing-probleem. Er moeten twee nieuwe communicatieve doelen worden gerealiseerd: klanten moeten geloven in de *privacy* en *veiligheid* van hun gegevens. Als klanten vermoeden dat de betalingsmail van a.s.r. een phishing-mail is, zijn ze immers niet meer zeker van de veiligheid en privacy van hun gegevens. Een oplossing voor het phishing-probleem moet zich rus richten op deze twee persuasieve communicatieve effecten.



Figuur 2: Functionele analyse van betalingsmails

5.3 De veiligheid en privacy van betalingsmails garanderen

De overstap van betalingsbrieven naar betalingsmails brengt dus een onverhoopt probleem met zich mee: klanten kunnen betalingsmails beoordelen als phishing en daarmee als bedreiging voor de veiligheid en privacy van hun gegevens. Om betalingsmails daadwerkelijk effectiever te maken dan betalingsbrieven, is er een oplossing van nodig voor dit probleem. In hoofdstuk 5.3.1 ga ik daarom eerst dieper in op de beoordeling phishing mails: wat noopt klanten om een verdachte, risicovolle e-mail daadwerkelijk te verwijderen? In 5.2.2 en 5.3.3 formuleer ik vervolgens een oplossing voor het phishing-probleem.

5.3.1 Keuzes over verdachte e-mails

Klanten die betalingsmails alleen verdacht vinden, doen niet af aan de effectiviteit van deze e-mails. De effectiviteit komt pas in het geding als mensen, doordat ze de e-mails verdacht vinden, afzien van betaling. Hierdoor missen betalingsbrieven immers hun doel: meer en eerdere betalingen van achterstallige premies. De vraag rijst welke afwegingen mensen maken als ze een verdachte e-mail verwijderen of behouden.

Alvorens ik hier verder op inga, zijn er heldere definities van ‘privacy’ en ‘veiligheid’ nodig. De begrippen zijn namelijk nauw verwant en worden vaak door elkaar gebruikt. In de context van online betalingen of aankopen, betekenen ze het volgende:

- **Privacy** is het vermogen om te bepalen wanneer, hoe en met wie persoonlijke informatie wordt gedeeld (Metzger, 2007).
- **Veiligheid** is de bescherming tegen het misbruik van persoonlijke gegevens.

De begrippen zijn dus nauw verweven. Veiligheid is een noodzakelijke voorwaarde voor privacy. Misbruik van gegevens is immers onvoorzien en ligt daarmee buiten de invloed van degene die de gegevens deelt. Als gegevens dus onveilig zijn, kan de eigenaar niet bepalen wanneer, hoe en met wie ze worden gedeeld. Privacy is daarentegen geen noodzakelijke voorwaarde voor veiligheid. Gegevens kunnen immers veilig zijn, oftewel niet worden misbruikt, zonder dat de gebruiker exact weet wat er met zijn gegevens gebeurt. Privacy kan dus worden gekenmerkt als de overtreffende trap van veiligheid.

De privacytheorie van Petronio (2002) gaat uitgebreid in op de spanning tussen het delen of behouden van persoonlijke informatie. Petronio stelt dat mensen een eenvoudige afweging maken bij een verzoek om persoonlijke informatie: wegen de voordelen van delen van informatie op tegen de risico’s? Deze simpele vraag gaat vooraf aan elke vrijgave of afscherming van persoonlijke gegevens. Petronio’s theorie is uitgebreid getest in de context van online aankopen en transacties. Mensen blijken online inderdaad de afweging te maken die Petronio poneert: zij wegen het gemak van online zakendoen af tegen de bijgaande privacy- en veiligheidsrisico’s (Hann et al., 2002).

Als a.s.r. betalingsmails effectief wil maken, zijn er dus twee mogelijkheden. Ten eerste kan a.s.r. de voordelen van betalingsmails benadrukken. Als de voordelen van betalen duidelijk zijn, zullen klanten de risico’s wellicht accepteren. Deze mogelijkheid biedt weinig speelruimte. De voordelen komen immers al duidelijk naar voren in het bericht zelf: als de klant betaalt, blijft hij verzekerd, worden er geen herinneringskosten in rekening gebracht en is hij niet strafbaar.

Het is dus zaak om klanten te overtuigen van de beperkte risico's. Als klanten ervan overtuigd zijn dat de betalingsmail opvolgen geen negatieve consequenties heeft, zullen zij overgaan tot betaling. Maar hoe overtuigt a.s.r. klanten van de privacy en veiligheid van hun persoonlijke gegevens?

5.3.2 Vertrouwen bij online zakendoen

Als je klanten online wil overtuigen van de veiligheid en privacy van hun persoonsgegevens, moet je hun vertrouwen winnen. Vertrouwen komt in veel literatuur terug als essentieel onderdeel in zakenrelaties. Het is een noodzakelijke voorwaarde om online zaken te doen (Midha, 2012). Zonder voldoende vertrouwen in de veiligheid en privacy van gegevens zullen klanten van a.s.r. dus niet overgaan tot betaling (Belanger, Hiller & Smith, 2002; Chen, 2010; Hoffman et al., 1999). Vertrouwen heeft dus een grote invloed op de gedragsintentie van klanten.

De term 'betrouwbaarheid' betekent, in de context van online zakendoen, het volgende: het geloof in de betrouwbaarheid en integriteit van de online aanbieder (Midha, 2012). Vertrouwen stoelt op een behoefte aan controle: mensen willen weten hoe hun gedrag anderen zal beïnvloeden, en andersom. Soms krijgt deze aandrang tot controle gestalte in regels of wetten. Controle valt dan af te dwingen. Veel andere situaties zijn daarentegen ongereguleerd. De gevolgen van gedrag zijn niet vastgelegd of simpelweg niet te overzien. Zo vertrouwen klanten van a.s.r. erop dat hun verzekeringsadviseur een passende verzekering vindt. In dergelijke gevallen substitueert vertrouwen daadwerkelijke regels: hoewel de effecten van gedrag niet volledig vastliggen, is er vertrouwen dat partijen sociaal geaccepteerd zullen handelen (Gefen & Straub, 2004).

Zoals al eerder duidelijk werd, is het vertrouwen van klanten bij online zakendoen erg laag (Belanger et al., 2002; Hoffman et al., 1999; Midha, 2012). Dit komt omdat vertrouwen interpersoonlijk is: vertrouwen bestaat tussen mensen. Online zakendoen en communiceren is daarentegen veelal onpersoonlijk (Gefen & Straub, 2004; Midha, 2012). Als klanten van a.s.r. een betalingsmail opvolgen, weten zij immers niet precies wie er over hun gegevens beschikt en hoe deze worden gebruikt. Er zijn dus geen aanwijsbare personen waarin klanten vertrouwen kunnen hebben. Daarbij zijn online transacties complex en diffuus. Het is ondoorzichtig waar gegevens precies belanden en hoe ze worden verwerkt. Door deze complexiteit hebben klanten geen controle over hun gegevens, waardoor het vertrouwen in de zakenpartner verder afneemt (Hoffman et al., 1999; Midha, 2012).

Als klanten weinig vertrouwen hebben, zijn ze terughoudender: ze nemen minder risico's. De daadwerkelijke kans op phishing is relatief klein. Als persoonsgegevens onverhoopt toch worden misbruikt, zijn de gevolgen echter groot. Persoonsgegevens kunnen online immers razendsnel worden gedeeld en op onvoorziene wijze worden ingezet (Caputo et al., 2014; Hong, 2012). Als er dus geen aanwijsbaar persoon en inzichtelijk bedrijfsproces bestaan die veiligheid en privacy van gegevens waarborgen, zullen klanten het risico op spear phishing niet altijd voor lief nemen. Klanten zullen waarschijnlijk niet altijd bereid zijn deze 'gok' te nemen.

5.3.3 Een contract over de veiligheid en privacy van gegevens

Hoewel het vertrouwen van klanten online lastiger is te winnen dan offline, is het geenszins onmogelijk. Klanten geven namelijk zelf aan wat zij nodig hebben om online aanbieders te vertrouwen: een sociaal contract (Belanger et al., 2002; Hoffman et al., 1999). Omdat online

zakendoen onpersoonlijk en diffuus is, bestaat er een sterke behoefte aan een menselijke, concrete afspraak. Zo wil 84% van de Amerikaanse bevolking dat bedrijven expliciet toestemming vragen alvorens ze persoonsgegevens gebruiken (Belanger et al., 2002). 72% van de internetgebruikers wil ook dat bedrijven uiteenzetten hoe ze persoonsgegevens gebruiken. Weinig online platforms voldoen aan deze behoefte. Klanten kunnen altijd beslissen om niet met een partij in zee te gaan (opt-out), maar worden zelden expliciet om instemming gevraagd (opt-in). Ook ontbreekt het vaak aan een alternatief. Klanten *moeten* persoonsgegevens delen als zij met een partij in zee willen gaan (Hoffman, 1999). Om het vertrouwen van klanten te winnen in de veiligheid en privacy van hun persoonsgegevens, moet a.s.r. dus een sociaal contract aangaan.

De vorm en inhoud van een sociaal contract

Om het vertrouwen daadwerkelijk te verhogen, moeten de inhoud en vorm van het contract zorgvuldig worden bepaald. Allereerst ga ik in op de inhoud. Door de gelijkenis van de betalingsmails met spear phishing, zullen klanten niet langer volledig geloven in de privacy en veiligheid van hun persoonsgegevens. Dit maakt echter niet duidelijk hoe het contract ingevuld moet worden: moet het een verklaring zijn over de privacy van gegevens, de veiligheid of beide?

Uit de literatuur blijkt dat mensen online meer waarde hechten aan de veiligheid dan aan privacy van gegevens. Zij prefereren een garantie tegen misbruik dus boven volledig inzicht en controle over het gebruik van gegevens (Belanger et al., 2002; Chen, 2015). Dit lijkt een argument te zijn om louter de veiligheid te benoemen in het contract. Het belang van veiligheid maakt privacy echter niet onbelangrijk. Zo braken 52% van de mensen weleens een online transactie af vanwege privacyoverwegingen (Midha, 2012). Hoewel de veiligheid van gegevens dus zwaarder weegt, is privacy geenszins irrelevant. In het sociale contract voor de betalingsmails van a.s.r., moeten dus zowel veiligheid als privacy terugkomen.

De thema's van het sociaal contract zijn vastgesteld. Een doordachte vormgeving van deze thema's maakt het sociaal contract pas daadwerkelijk effectief. Privacy wordt veelal beklemtoond met een keurmerk en een bijgaande privacyverklaring. Het keurmerk is bij voorkeur afkomstig van een onafhankelijke partij (Belanger et al., 2002; Kim & Kim, 2012).

Figuur 3: het privacywaarborg

Het Privacy Waarborg[1] is een bekend Nederlands voorbeeld van een keurmerk. Dit keurmerk geeft aan dat gegevensvergaring van de online aanbieder is getoetst aan de privacywetgeving. Klanten weten door het keurmerk dus in één oogopslag dat de online zakenpartner handelt binnen de kaders van de wet. De privacyverklaring heeft meestal drie kernpunten.

Ten eerste informeert de verklaring klanten. Ze worden ervan op de hoogte gesteld dat de zakenpartner privacygevoelige informatie wil gebruiken. Ten tweede geeft de verklaring klanten een keuze: zij kunnen actief instemmen met het gebruik van persoonsgegevens (opt-in).

[1] https://www.privacywaarborg.nl/

Als laatste geeft de verklaring bondig weer hoe persoonsgegevens worden gebruikt. Deze driedelige verklaring geeft klanten, in combinatie met het keurmerk, meer controle over en inzicht in de privacy van hun persoonsgegevens. Dit is bevorderlijk voor de ervaren privacy en het vertrouwen (Kim & Kim, 2012; Midha, 2012). Als a.s.r. klanten wil overtuigen van de privacy van hun gegevens, is het dus verstandig om deze elementen terug te laten komen in betalingsmails.

In het contract moet, naast de privacy van persoonsgegevens, ook de veiligheid worden benadrukt. Klanten hechten namelijk nog meer waarde aan de veiligheid van hun gegevens (Chen, 2015; Belanger et al., 2002). De beklemtoning van privacy is immers nog geen garantie voor de veiligheid: in theorie zou het sociaal contract onderdeel kunnen zijn van spear phishing. Een effectieve manier om online de veiligheid van persoonsgegevens te benadrukken, is een persoonlijke veiligheidsindicator: uit onderzoek van Lee en Bauer (2015) bleek dat 92.5% van de mensen deze indicator ziet en 72.5% de indicator vindt bijdragen aan de veiligheid van persoonsgegevens. De indicator is vaak een persoonlijke afbeelding die mensen uitzoeken aan het begin van een online zakenrelatie (Lee & Bauer, 2015; Marforio et al., 2015). Zo laten sommige banken nieuwe klanten een persoonlijke foto uploaden, bijvoorbeeld een afbeelding van een bloem. De klant en online aanbieder spreken af dat deze persoonlijke afbeelding terugkomt in alle toekomstige correspondentie. Als de afbeelding niet in de correspondentie staat, is het bericht waarschijnlijk niet authentiek.

Een persoonlijke veiligheidsindicator is een effectieve vorm van beveiliging. Het is voor phishers relatief eenvoudig om algemene logo's en keurmerken te kopiëren. Daarentegen is het aanzienlijk lastiger te achterhalen welke persoonlijke afbeelding een klant heeft gedeeld. Door de een persoonlijke veiligheidsindicator zijn de persoonsgegevens van klanten dus veiliger. Dit bevordert het vertrouwen en de ervaren veiligheid (Lee & Bauer, 2015; Marforio et al., 2015). Als a.s.r. klanten wil overtuigen van de veiligheid van hun gegevens, is het dus verstandig om een persoonlijke veiligheidsindicator terug te laten komen in betalingsmails.

Concluderend leidde de overstap op e-mail tot een nieuw probleem: de betalingsmail van a.s.r. lijkt op spear phishing, waardoor klanten niet direct overtuigd zullen zijn van de veiligheid en privacy van hun gegevens. Om klanten te overtuigen, moeten zij inzien dat de risico's op misbruik klein zijn. Klanten moeten a.s.r. en haar handelswijze vertrouwen. Ik verwacht dat een sociaal contract, waarmee klanten actief instemmen, bijdraagt aan het vertrouwen (H4). In dit contract staan een privacykeurmerk en -verklaring in combinatie met een persoonlijke veiligheidsindicator. Deze maatregelen geven klanten meer controle over en inzicht in de behandeling van hun persoonsgegevens. Hierdoor zullen ze de privacy- en veiligheidsrisico's van de betalingsmail lager inschatten (H5, H8) en eerder overgaan tot betaling (H6, H7). Deze verwachtingen zijn verwerkt in de volgende hypotheses:

H4: Betalingsmails met een sociaal contract leiden tot meer vertrouwen in de behandeling van persoonsgegevens door a.s.r. dan betalingsmails zonder sociaal contract.

H5: Betalingsmails met een sociaal contract leiden tot meer ervaren veiligheid en privacy van persoonsgegevens dan betalingsmails zonder sociaal contract.

H6: Betalingsmails met een sociaal contract leiden tot minder uitstel van betaling dan betalingsmails zonder een sociaal contract.

H7: Het effect van een directe link naar de betalingsomgeving op de intentie om direct te betalen, is groter bij betalingsmails met een sociaal contract dan bij betalingsmails zonder sociaal contract.

H8: Het effect van e-mails met een directe link naar de betalingsomgeving op de ervaren veiligheid en privacy is kleiner bij betalingsmails met een sociaal contract dan bij betalingsmails zonder sociaal contract.

6.0 Methode

Om de hypotheses te toetsen, voerde ik een experimenteel onderzoek uit. Hieronder licht ik daarom het onderzoeksontwerp, materiaal, de vragenlijst en procedure toe.

6.1 Onderzoeksontwerp

Dit experiment heeft een 2x2-tussenproefpersoonontwerp. Ik maakte dus twee soorten aanpassingen in het ontwerp van betalingsmails: (1) een directe link naar de betalingsomgeving vs. *geen* directe link naar de betalingsomgeving en (2) een sociaal contract vs. *geen* sociaal contract.

6.2 Onderzoeksmateriaal

In dit onderdeel zal ik de samenstelling verantwoorden van de onderzochte betalingsmails. Eerst zal ik in het algemeen ingaan op het ontwerp van betalingsmails. Vervolgens zal ik uiteenzetten hoe de directe link en het sociaal contract zijn ingepast.

6.2.1 Het ontwerp van betalingsmails

Zoals reeds duidelijk werd in hoofdstuk 3.2, zijn er binnen a.s.r. drie soorten betalingsmails: een acceptgiro, de eerste betalingsherinnering en een aanmaning. Deze berichten worden trapsgewijs verzonden en hebben een steeds strengere toon. In dit onderzoek vormt de aanmaning, het laatste bericht, de basis voor het onderzoeksmateriaal. In de aanmaning is het betalingsverzoek het meest direct en urgent: a.s.r. maakt klanten duidelijk dat de betalingstermijn ruimschoots overschreden is, de verzekering is komen te vervallen en er eventueel een boete volgt. De aanmaning maakt dus, meer dan haar voorgangers, de urgentie van betaling duidelijk. Deze verhoogde urgentie sluit goed aan bij het onderzoek. Een urgent verzoek om direct te betalen, is namelijk een eigenschap van phishing (Singleton, 2005). Veel phishers stimuleren geadresseerden om op de link te klikken, door te beweren dat zij *direct* moeten betalen. De aanmaning vertoont dus de meeste gelijkenis met phishing mails en leent zich daarom het best voor dit onderzoek.

Bij het samenstellen van het materiaal week ik zo min mogelijk af van de originele aanmaning van a.s.r. Een grote gelijkenis tussen de originele aanmaning en het onderzoeksmateriaal, komt de ecologische validiteit namelijk ten goede: de resultaten zijn hierdoor beter te generaliseren naar de werkelijke, alledaagse situatie. Daarbij is een minimale afwijking wenselijk vanwege de proefpersonen. Het onderzoek is uitgezet onder klanten van a.s.r. Zij hebben bepaalde verwachtingen van een e-mail van a.s.r. Als het onderzoeksmateriaal te onconventioneel is, kunnen de resultaten worden vertekend. De klanten van a.s.r. zullen het ongebruikelijke ontwerp namelijk meenemen in hun beoordeling van de betalingsmail.

De originele aanmaning [bijlage A] bestaat uit vijf alinea's met de volgende onderwerpen: een inleiding, het betalingsverzoek, het verval van dekking, de verzekeringsplicht en vragen. Alleen de laatste alinea over vragen is niet opgenomen in de uiteindelijke betalingsmails. Deze alinea is geschrapt vanwege een praktische beperking: het volledige bericht was niet te vatten in één frame. Om de laatste alinea te lezen, moesten geadresseerden naar beneden scrollen. Scrollen is in de onderzoekstool niet mogelijk, waardoor ik een alinea moest weglaten. Het stukje tekst over vragen bevatte geen inhoudelijke informatie. Door deze tekst weg te laten, bleef de kern van het bericht dus zoveel mogelijk intact.

Ik maakte verder twee inhoudelijke aanpassingen [bijlage B]. De originele aanmaning laat in het ongewisse of de klant al betaald heeft. De brief maakt dus duidelijk dat het om een administratieve fout zou kunnen gaan. Omdat dit onderzoek zich richt op de perceptie van betalingsbrieven over een daadwerkelijke betalingsachterstand, verwijderde ik ten eerste deze passage.

Ten tweede veranderde ik de alinea over het betalingsverzoek. Omdat ik onderzoek of een directe link naar de betalingsomgeving betalingsbrieven effectiever maakt, moest de mogelijkheid tot online betaling in de brief terugkomen. Ik heb dus eerst een passage toegevoegd waarin de lezer op deze mogelijkheid wordt gewezen.

Betalingsmails kunnen, zoals eerder beschreven (hoofdstuk 5), argwaan oproepen vanwege hun gelijkenis met spear phishing. Een kenmerkende eigenschap van spear phishing mails is een verzoek om persoonsgegevens (Hong, 2012). Het verzoek tot online betaling is op zichzelf al een verzoek om persoonsgegevens. Om online te betalen, moet de klant immers inloggen met zijn gebruikersnaam en/of wachtwoord. Dit verzoek is echter wat summier. Er bestaat een kans dat sommige proefpersonen eroverheen lezen. Om dit risico uit te sluiten, heb ik een extra verzoek om persoonsgegevens toegevoegd. Ik voegde in de alinea over het betalingsverzoek een passage toe over een betalingsregister. Hierin kan de klant zich met zijn naam en e-mailadres inschrijven om voortaan altijd online te betalen. Dit extra verzoek om persoonsgegevens accentueert dus de overeenkomsten tussen de betalingsmails en spear phishing mails.

De inhoud van de betalingsmails blijft dus dicht bij het origineel. Ook de opmaak is, vanuit dezelfde motivatie, grotendeels authentiek. Ik gebruikte dezelfde typografie en bladspiegel. Het logo van a.s.r. kwam ook terug in het onderzoeksmateriaal. Daarbij toonde ik de betalingsmails in een outlook-omgeving, waardoor zij er ook daadwerkelijk uitzagen als e-mails. De originele aanmaning en het onderzoeksmateriaal (de vier betalingsmails) zijn te vinden in respectievelijk bijlage A en B.

6.2.2 Directe links naar de betalingsomgeving en een sociaal contract in betalingsmails

Er zijn vier betalingsmails die verschillen in de aanwezigheid van hyperlinks naar de betalingsomgeving en een sociaal contract. Een overzicht van de condities is weergegeven in tabel 4.

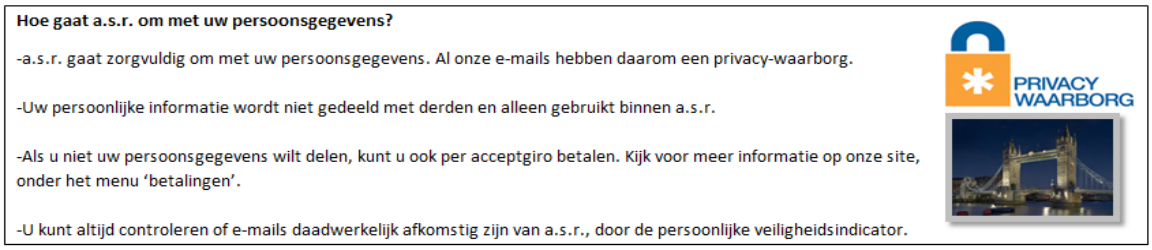
Tabel 4: *De vier verschillende betalingsmails*

Conditie	*Hyperlink*	*Sociaal contract*
1	Afwezig	Afwezig
2	Aanwezig	Afwezig
3	Afwezig	Aanwezig
4	Aanwezig	Aanwezig

In de condities met links zijn er simpelweg twee hyperlinks toegevoegd: één hyperlink naar de betalingsomgeving en één hyperlink naar het register. In de condities zonder hyperlink is er tekstueel verwezen naar het menu ‘betalingen’ op de website van a.s.r. De klant zou dan dus zelf de *url* moeten intikken, om vervolgens te betalen of zich in te schrijven in het register. De precieze teksten en plaatsing van de hyperlinks zijn te vinden in bijlage B.

In de condities met sociaal contract, voegde ik aan het einde van het bericht een kader toe (figuur 4). In dit kader staan verschillende elementen: een privacykeurmerk, een veiligheidsindicator en verschillende verklaringen over het gebruik van persoonsgegevens. Ik heb gekozen

voor zowel een privacykeurmerk als een veiligheidsindicator, omdat mensen de privacy en veiligheid van hun persoonsgegevens beide belangrijk vinden (Chen, 2015; Belanger et al., 2002; Midha, 2012). Als privacykeurmerk koos ik het wijdverspreide privacywaarborg. Nederlandse bedrijven krijgen het waarborg als zij, getoetst door een onafhankelijke partij, verschillende privacy-gedragsregels naleven. Omdat veel bedrijven dit keurmerk voeren, is het waarschijnlijker dat proefpersonen de betekenis kennen.



Figuur 4: Het sociaal contract

Als persoonlijke veiligheidsindicator koos ik een afbeelding van de Tower Bridge in London. Veiligheidsindicatoren zijn namelijk veelal persoonlijke (vakantie)foto's (Lee & Bauer, 2015; Marforio et al., 2015). In het scenario voorafgaand aan de betalingsmails met sociaal contract, beschrijf ik dat de proefpersoon een afbeelding van de Tower Bridge heeft gedeeld met a.s.r. Ook geef ik aan dat deze afbeelding in alle e-mails van a.s.r. terug zou moeten komen, als garantie van de afzenders authenticiteit. In het kader staan dus twee afbeeldingen: het privacywaarborg en een afbeelding van de Tower Bridge. Het volledige scenario en de betalingsmails met sociaal contract zijn te vinden in bijlage B.

Naast de afbeeldingen, staan er vier korte verklaringen in het kader over het gebruik van persoonsgegevens. De eerste drie verklaringen hebben betrekking op de privacy van persoonsgegevens. Uit onderzoek blijkt (Kim & Kim, 2012; Midha, 2012) dat een privacyverklaring minimaal drie elementen moet bevatten: de verklaring moet verduidelijken *dat* persoonsgegevens worden gebruikt, *hoe* dit gebeurt en geadresseerden moeten actief instemmen met het gebruik. Uit de eerste en tweede regel [tabel 5] wordt duidelijk *dat* en *hoe* persoonsgegevens worden gebruikt. In derde regel staat vervolgens een alternatieve betalingswijze: betaling per acceptgiro. Door een alternatief aan te bieden, kunnen klanten actief instemmen met gebruik van hun persoonsgegevens. Zij kunnen immers ook kiezen voor een betalingswijze die geen beroep doet op persoonsgegevens. De vergaring van persoonsgegevens is dus geen standaardprocedure. De laatste regel refereert aan de veiligheidsindicator en herinnert dus aan de betekenis van de afgebeelde Tower Bridge.

Tabel 5: *De tekst uit het sociaal contract, geordend per regel*

Regel	*Tekst*
1	-a.s.r. gaat zorgvuldig om met uw persoonsgegevens. Al onze e-mails hebben daarom een privacy-waarborg.
2	-Uw persoonlijke informatie wordt niet gedeeld met derden en alleen gebruikt binnen a.s.r.
3	-Als u niet uw persoonsgegevens wilt delen, kunt u ook per acceptgiro betalen. Kijk voor meer informatie op onze site, onder het menu 'betalingen'.
4	-U kunt altijd controleren of e-mails daadwerkelijk afkomstig zijn van a.s.r., door de persoonlijke veiligheidsindicator.

6.3 De vragenlijst

De resultaten van dit onderzoek verkreeg ik via een vragenlijst [bijlage C]. De vragen hadden de volgende onderwerpen: privacy van de betalingsmail, veiligheid van de betalingsmail, de gedragsintentie van de klant, gebruikersgemak van de betalingsmail en het vertrouwen in a.s.r.

Ik mat de ervaren **privacy** van betalingsmails met vijf 7-punts schaalvragen (helemaal mee oneens – helemaal mee eens). Ik baseerde deze vragen op de drie noodzakelijke voorwaarden voor privacy: de kennis *dat* en *hoe* persoonsgegevens worden gebruikt in combinatie met een actieve keuze voor deze toepassing (Kim & Kim, 2012; Midha, 2012). Een vraag over privacy luidde bijvoorbeeld: "Door deze e-mail weet ik waarom a.s.r. mijn persoonsgegevens nodig heeft." Bij de analyse van de resultaten wilde ik een gemiddelde score gebruiken van de vijf aparte vragen. De aparte vragen zijn alleen samen te nemen als zij individueel allemaal privacy meten. Ik testte daarom af de vragen samen voldoende betrouwbaar waren. Dit bleek het geval ($\alpha = .68$).

Veiligheid werd gemeten aan de hand van vier 7-punts schaalvragen (helemaal mee oneens – helemaal mee eens). Deze vier vragen zijn gerelateerd aan belangrijke aspecten van online veiligheid, zoals de authenticiteit van de afzender en het risico op misbruik van persoonsgegevens (Lee & Bauer, 2015; Marforio et al., 2015). Een vraag over veiligheid is bijvoorbeeld: "Door deze e-mail loop ik het risico dat mijn persoonsgegevens misbruikt worden." Ook deze vragen bleken betrouwbaar ($\alpha = .81$) en zijn dus samengenomen bij de statistische analyses.

De vier vragen over **gedragsintentie** meten of de klant (online) wil betalen. Het gaat om vier 7-punts schaalvragen (zeer onwaarschijnlijk – zeer waarschijnlijk). Een vraag over gedragsintentie is bijvoorbeeld: "Ik zou door deze e-mail mijn achterstallige premie direct betalen." De vragen waren betrouwbaar ($\alpha = .67$) en zijn daarom samengenomen.

Ik mat **gebruikersgemak** aan de hand van vier 7-punts schaalvragen (helemaal mee oneens – helemaal mee eens). De vragen stoelen op een wijdverspreid en gevalideerd meetinstrument van gebruikersgemak, The System Usability Scale (Bangor et al., 2008). Uit deze schaal selecteerde ik de meest relevante vragen over gebruikersgemak en parafraseerde deze in het Nederlands. Een voorbeeldvraag is: "Betalen via deze e-mail is eenvoudig." De vragen over gebruikersgemak waren betrouwbaar ($\alpha = .67$) en zijn dus samengenomen bij de statistische analyses.

Als laatste werd het **vertrouwen** in a.s.r. gemeten aan de hand van zes 7-punts schaalvragen (helemaal mee oneens – helemaal mee eens). Deze vragen ontspringen aan een gevalideerd en gefrequenteerd meetinstrument voor vertrouwen, de Trust Scale (Gefen & Straub, 2004). Deze schaal meet verschillende aspecten van vertrouwen, zoals welwillendheid en integriteit. Ik parafraseerde de vragen in het Nederlands, zoals bijvoorbeeld: "Ik geloof dat a.s.r. oprecht is." De vragen bleken betrouwbaar (α = .65) en zijn dus samengenomen bij de statistische analyses. Alle onderwerpen en bijbehorende vragen staan in bijlage D.

Aanvullende onderwerpen in de vragenlijst

Naast de voorgaande onderwerpen, nam ik ook enkele aanvullende onderwerpen op in de vragenlijst. Ten eerste mat ik hoe belangrijk proefpersonen **online privacy en veiligheid** vonden. Ik noemde al eerder dat online privacy en veiligheid positief kunnen bijdragen aan onder meer het vertrouwen en de gedragsintentie van klanten (Belanger et al., 2002; Chen, 2015; Midha, 2012). Deze beïnvloeding is echter voorwaardelijk. Klanten moeten online privacy en veiligheid namelijk wel belangrijk vinden. Als zij hier geen waarde aan hechten, zal de nadruk op online privacy en veiligheid in betalingsmails hen waarschijnlijk onberoerd laten. Ik mat daarom aan de hand van vijf 5-punts schaalvragen (totaal niet belangrijk – erg belangrijk) hoeveel waarde proefpersonen hechtten aan online privacy en veiligheid. Deze vragen waren betrouwbaar (α = .85) en zijn dus samengenomen bij verdere statistische analyses.

Daarnaast mat ik de **digitale geletterdheid** van de proefpersonen. Dit onderzoek richt zich namelijk op een relatief nieuwe digitale bedreiging: het verlies van persoonsgegevens door phishing. Om dit risico weloverwogen te beoordelen, is enige digitale kennis vereist. Ik mat daarom met 5-punts schaalvragen hoe bekend proefpersonen zijn met digitale begrippen als 'scam' en 'cookies'. Deze vragen waren betrouwbaar (α = .86) en zijn dus samengenomen bij verdere statistische analyses. Daarnaast vroeg ik ook direct hoe bekend de term 'phishing' was. Als laatste werden er enkele demografische gegevens gevraagd, zoals leeftijd geslacht en opleidingsniveau.

6.4 Proefpersonen

Aan dit onderzoek deden 191 proefpersonen mee[2]. Hiervan was 66.5% man en 33.5% vrouw. De proefpersonen waren gemiddeld 51 jaar. 50.3% van de proefpersonen behaalde minimaal een VWO diploma (VWO, HBO, universitaire bachelor, universitaire master). 34.5% van de proefpersonen behaalde minimaal een VBMO-t diploma (VMBO-t, MBO niveau 3 of 4, Mulo, HBS, HAVO). De overige 15.2% rondde de lagere school af, of MBO niveau 1/2.

De resultaten van dit onderzoek zijn betekenisvol als de proefpersonen in de verschillende condities vergelijkbaar zijn qua geslacht, opleidingsniveau en leeftijd. Deze gelijke verdeling sluit namelijk uit dat de uitkomsten voortkomen uit demografische variatie. Om te controleren of de respondenten niet ongelijk waren verdeeld over de condities, zijn er randomisatietests uitgevoerd voor leeftijd, geslacht en opleidingsniveau. Uit een eenwegs-variantieanalyse bleek dat leeftijd niet significant verschilde tussen de condities ($F(3, 187) = 0.75$; $p = .53$). Vervolgens bleek uit chi-kwadraattoetsen dat geslacht ($\chi^2(3) = 0.82$; $p = .83$) en opleidingsniveau ($\chi^2(39) =$

[2] Ik verwijderde sommige proefpersonen uit het bestand. Meer informatie over de opschoning van de data staat in bijlage D.

3.74; p = .79) ook niet ongelijk waren verdeeld tussen de condities. De proefpersonen in de verschillende condities waren dus vergelijkbaar qua geslacht, leeftijd en opleidingsniveau.

6.5 Afnameprocedure

Alle respondenten van dit onderzoek zijn klanten van a.s.r. Deze klanten gaven bij eerdere correspondentie met a.s.r. aan dat zij interesse hadden in onderzoek. Ik benaderde hen via een algemene mail, waarin ik het onderzoeksdoel en praktische informatie uiteenzette [bijlage B]. Proefpersonen konden vervolgens via een link het onderzoek online invullen, in de onderzoekstool MWM^2. Dit programma verdeelde de vier verschillende betalingsbrieven willekeurig onder de proefpersonen.

Het onderzoek begon met een korte inleidende pagina, waarin de duur en inhoud van het experiment stonden beschreven. Daarna volgden er enkele demografische vragen. Vervolgens lazen de proefpersonen een scenario. Zij moesten zich voorstellen dat ze een betalingsachterstand hadden van hun autoverzekering bij a.s.r. Na het scenario lazen de proefpersonen één van die vier e-mails, waarna er schaalvragen volgden over het bericht. Als laatste volgden er vragen over de bekendheid met phishing en het belang van privacy en veiligheid. Deze vragen wijzen namelijk richting het onderwerp van het onderzoek, waardoor ze proefpersonen ongewenst kunnen beïnvloeden. De volledige vragenlijst staat in bijlage C.

7.0 Resultaten

In dit onderdeel behandel ik de resultaten van het onderzoek. Ik ga eerst kort in op resultaten die niet direct in verband staan met de hypotheses (7.1). Daarna behandel ik de resultaten conform de hypotheses (7.2).

7.1 Het beste onderdeel van de betalingsmails

Bij de behandeling van de resultaten houd ik de volgorde aan van de hypotheses. Eén onderdeel van de vragenlijst valt echter niet direct onder de hypotheses, maar is wel interessant. Ik gaf proefpersonen namelijk de mogelijkheid om de beste alinea van de betalingsmail te selecteren. In de condities met een sociaal contract – het kader met informatie over privacy en veiligheid – merkte 52.5% van de proefpersonen dit aan als het beste onderdeel van de e-mail. Meer dan de helft van proefpersonen vond dus dat het sociaal contract de beste, meest relevante informatie bevatte. Daarentegen vond slechts 29.5% van de proefpersonen de alinea met een directe link het beste onderdeel. Het sociaal contract is dus populairder dan de directe link.

7.2 Resultaten van de hypotheses

In dit hoofdstuk behandel ik eerst resultaten van aanvullende onderwerpen uit de vragenlijst, zoals digitale geletterdheid (7.2.1). Vervolgens vormen de hypotheses de rode draad bij de bespreking van de onderzoeksuitkomsten (7.2.2-7.2.9).

7.2.1 Digitale geletterdheid en het belang van privacy en veiligheid

Ten eerste analyseerde ik de aanvullende onderwerpen uit de vragenlijst. Ik testte dus of er een verband was tussen digitale geletterdheid, het belang van privacy/veiligheid, de bekendheid met phishing - de aanvullende onderwerpen - en het oordeel over privacy, veiligheid, de intentie om te betalen, gebruikersgemak en vertrouwen in a.s.r. Ik vond geen verband tussen digitale geletterdheid, bekendheid met phishing en de andere onderwerpen uit de vragenlijst. De beoordeling van de betalingsmails hing dus niet samen met de bekendheid met phishing en digitale geletterdheid.

Ik vond wel een verband tussen het belang van online privacy/veiligheid en de beoordeling van privacy, veiligheid, gedragsintentie en gebruikersgemak. Dit verband was in alle gevallen negatief: hoe meer waarde proefpersonen hechtten aan privacy en veiligheid, hoe negatiever de beoordeelde privacy, veiligheid, intentie om te betalen en het gebruikersgemak van de betalingsmails [tabel 6]. Dit verband is logisch: hoge eisen aan privacy en veiligheid leiden tot een kritischere beoordeling van betalingsmails en werken terughoudendheid om te betalen in de hand.

Tabel 6: *het verband, ofwel de correlatie, en (p-waarde), tussen de persoonlijke voorkeur voor online privacy/veiligheid en de inschatting van privacy, veiligheid, gedragsintentie en het gebruikersgemak van betalingsmails*

	Privacy	Veiligheid	Gedragsintentie	Gebruikersgemak
Belang van privacy en veiligheid	-0.15 (< .05)	-0.27 (< .01)	-0.18 (< .05)	-0.20 (< .05)

Om de invloed van de persoonlijke voorkeur voor online privacy en veiligheid precies vast te stellen, verdeelde ik de proefpersonen in twee groepen: mensen die online privacy en veiligheid relatief onbelangrijk vinden en mensen die het bovengemiddeld belangrijk vinden. De scheidslijn tussen deze twee groepen is de gemiddelde score van het belang van privacy en veiligheid (G = 6.5). Vervolgens testte ik of deze groepen de privacy, veiligheid, gedragsintentie en het gebruikersgemak van de betalingsmails verschillend beoordeelden.

De groep proefpersonen die meer waarde hechtte aan online privacy en veiligheid evalueerde de privacy, veiligheid, de intentie om te betalen en het gebruikersgemak negatiever [tabel 7] dan proefpersonen die online privacy en veiligheid minder belangrijk vonden. De persoonlijke voorkeur voor online privacy en veiligheid werkt dus door in de beoordeling van de betalingsmails: een kritische houding over privacy en veiligheid leidt tot een kritischere beoordeling van de betalingsmail. Al deze verschillen zijn significant: privacy ($t(174) = 2.00$, $p < .05$), veiligheid ($t(189) = 3.19$, $p < .05$), gedragsintentie ($t(189) = 2.19$, $p < .05$) en gebruikersgemak ($t(189) = 2.67$, $p < .05$) werden significant negatiever beoordeeld als proefpersonen meer waarde hechtten aan online veiligheid en privacy.

Dit is een interessante uitkomst. Mensen vinden online privacy en veiligheid gemiddeld zeer belangrijk (G = 6.5 op een 7-punts schaal). Dit betekent dat het merendeel van de ontvangers van betalingsbrieven de privacy, veiligheid, intentie om te betalen en het gebruikersgemak relatief kritisch beoordeelt. In het hoofdstuk 'advies' zal ik handvatten aanreiken om hiermee om te gaan.

Tabel 7: *Gemiddelden en (standaarddeviaties) van privacy, veiligheid, gedragsintentie en gebruikersgemak, voor mensen die veel of weinig belang hechten aan online privacy en veiligheid (schaal 1-7; helemaal mee oneens – helemaal mee eens).*

	Online privacy/veiligheid belangrijk	Online privacy/veiligheid onbelangrijk
Privacy	3.5 (1.37)	3.8 (1.19)
Veiligheid	3.4 (1.71)	4.1 (1.32)
Gedragsintentie	3.1 (1.67)	3.6 (1.66)
Gebruikersgemak	3.7 (1.57)	4.3 (1.29)

7.2.2 Hypothese 1

De grootste beperking van de effectiviteit van betalingsbrieven is praktisch van aard: klanten van a.s.r. ontvangen betalingsbrieven niet of vergeten ze. Ik veronderstelde dat de overstap op e-mail dit probleem zou kunnen verhelpen. E-mails komen namelijk op verschillende apparaten binnen, worden vaker bekeken en kunnen direct online worden opgevolgd (Van Rijn, 2015). De eerste hypothese was dan ook:

H1: Betalingsmails worden door meer klanten gelezen dan betalingsbrieven

Ik testte deze hypothese op een bijzondere manier. Proefpersonen gaven namelijk *zelf* aan of zij hun e-mail vaker lezen dan brieven. De resultaten zijn in dit geval, in tegenstelling tot alle andere hypotheses, dus niet voortgekomen uit een vergelijking tussen de verschillende betalingsmails. Een voorbeeldvraag is: "Ik check mijn e-mail vaker dan mijn papieren post." Het ging om 7-punts schaalvragen (helemaal mee oneens – helemaal mee eens). Als de gemiddel-

de score dus hoger was dan vier, het midden van de schaal, gaven proefpersonen aan dat ze hun e-mail vaker lezen de brieven.

Proefpersonen stelden inderdaad dat ze e-mails vaker bekijken (G[3] = 5.2 SD = 1.90) en minder snel vergeten (G = 4.7 SD = 1.85) dan brieven. Als we het midden van de 7-puntschaal als ijkpunt nemen, blijken deze verschillen significant: proefpersonen kijken significant meer naar hun e-mail ($t(190) = 8.48$, $p < .05$) en vergeten e-mails significant minder vaak dan brieven ($t(190) = 5.37$, $p < .05$).

Er was echter ook een opvallend resultaat: proefpersonen verliezen brieven niet vaker dan e-mails (G = 3.5 SD = 2.01). Hoewel ze hun inbox dus vaker checken dan hun brievenbus en nieuwe e-mails bovendien minder snel vergeten, blijkt uit de resultaten niet dat brieven vaker verloren raken. Daarbij zijn de verschillen tussen brief en e-mail niet enorm groot. De scores liggen immers rond vier, het midden van schaal. De gemiddelde leeftijd van de proefpersonen (51 jaar) is een mogelijke verklaring voor de geringe verschillen. Het is denkbaar dat jongere mensen nog meer zijn gericht op e-mail. Al met al is hypothese één dus deels bevestigd. Betalingsmails zullen waarschijnlijk door meer klanten worden gelezen dan betalingsbrieven. Het verschil is echter niet groot genoeg om de effectiviteitsproblemen van betalingsbrieven volledig te verhelpen.

Tabel 6: *Gemiddelden en (standaarddeviaties) van privacy, veiligheid, betrouwbaarheid, gedragsintentie en gebruikersgemak, gesorteerd op de aan- en afwezigheid van de link en het sociaal contract (schaal 1-7; helemaal mee oneens – helemaal mee eens).*

	Directe link		Sociaal contract	
	Afwezig (N=98)	Aanwezig (N=93)	Afwezig (N=111)	Aanwezig (N=80)
Privacy	3.6 (1.34)	3.6 (1.35)	3.3 (1.21)	4.0 (1.44)
Veiligheid	3.5 (1.65)	3.7 (1.60)	3.3 (1.49)	4.1 (1.70)
Betrouwbaarheid	4.5 (0.87)	4.5 (0.92)	4.4 (0.88)	4.7 (0.90)
Gedragsintentie	3.1 (1.70)	3.4 (1.71)	3.0 (1.66)	3.6 (1.73)
Gebruikersgemak	3.8 (1.56)	4.0 (1.51)	3.7 (1.42)	4.1 (1.68)

7.2.3 Hypothese 2

Veel klanten van a.s.r. lezen de betalingsbrief wel, maar vergeten vervolgens te betalen. Een effectieve betalingsmail moet klanten dus in staat stellen om direct te betalen. Ik onderzocht daarom of een directe link richting de betalingsomgeving dit probleem kon oplossen:

H2: Betalingsmails met een directe link naar de betalingsomgeving leiden tot minder uitstel van betaling dan betalingsmails zonder een directe link.

Tabel 7: *Gemiddelden en (standaarddeviaties) voor gedragsintentie en gebruikersgemak gesorteerd op condities zonder en met link (schaal 1-7; helemaal mee oneens – helemaal mee eens).*

	Link afwezig (N=98)	Link aanwezig (N=93)
Gedragsintentie	3.1 (1.70)	3.4 (1.71)
Gebruikersgemak	3.8 (1.56)	4.0 (1.51)

[3] G staat voor gemiddelde, SD staat voor standaarddeviatie: de gemiddelde variantie rondom het gemiddelde

Uit de resultaten bleek dat betalingsmails met een directe link (G = 3.4 SD = 1.71) leiden tot een positievere gedragsintentie dan e-mails zonder een directe link (G = 3.1 SD = 1.70). Proefpersonen hebben dus, zoals verwacht, een sterkere intentie om te betalen als er een directe link in de e-mail staat. Daarbij bleken de betalingsmails met een directe link gebruiksvriendelijker (G = 4.0 SD = 1.51) dan e-mails zonder link (G = 3.8 SD = 1.56). Proefpersonen vonden de betalingsmails met link dus makkelijker in gebruik, waardoor zij waarschijnlijk sneller betalen [tabel 9].

De gevonden verschillen hebben de veronderstelde richting, maar zijn niet significant. Zowel het verschil in gedragsintentie (t(189) = 1.39, p = .17) als gebruikersgemak (t(189) = 1.14, p = .26) bereikt geen significantie. Deze verschillen zouden dus toevallig kunnen zijn. Een mogelijke verklaring is de vormgeving van het materiaal. In de betalingsmails zonder directe link staat namelijk wel precies beschreven hoe de klant online kan betalen. Het kost dus relatief weinig moeite om alsnog online te betalen als de link afwezig is. Hierdoor zouden significante verschillen kunnen uitblijven. Hypothese twee is dus niet bevestigd. Daarbij valt het op dat de scores rond het midden van de schaal liggen. Proefpersonen hebben dus een neutrale gedragsintentie na het lezen van de betalingsmail: het bericht spoort hen niet aan erg aan, maar demotiveert ook niet. Op dit vlak is er nog terrein te winnen. Een sterkere intentie om te betalen, draagt immers bij aan de effectiviteit van de betalingsmail.

7.2.4 Hypothese 3

Ik voorzag ook enkele problemen in de overstap van betalingsbrieven naar betalingsmails. Betalingsmails met een directe link vertonen namelijk erg veel gelijkenis met spear phishing e-mails (Caputo et al., 2014). Betalingsmails doen een urgent verzoek om persoonsgegevens/bankgegevens, wat verdachte eigenschappen zijn van spear phishing (Downs et al., 2006; Metzger, 2007; Singleton, 2005). Ik verwachtte daarom dat betalingsmails met een directe link als een grotere bedreiging werden ervaren voor de privacy en veiligheid van persoonsgegevens:

H3: Betalingsmails met een directe link naar de betalingsomgeving worden als een grotere bedreiging ervaren voor de privacy en veiligheid van persoonsgegevens dan betalingsmails zonder link naar de betalingsomgeving.

Tabel 8: *Gemiddelden en (standaarddeviaties) voor privacy en veiligheid gesorteerd op condities zonder met link (schaal 1-7; helemaal mee oneens – helemaal mee eens).*

	Link afwezig (N=98)	Link aanwezig (N=93)
Privacy	3.6 (1.34)	3.6 (1.35)
Veiligheid	3.5 (1.65)	3.7 (1.60)

Er is nauwelijks verschil [tabel 10] in de ervaren veiligheid van betalingsmail met (G = 3.7 SD = 1.60) en zonder (G = 3.5 SD = 1.65) directe link. Daarbij is het verschil niet significant (t(189) = 0.89, p = .38) en heeft het een onverwachte richting: betalingsmails *met* directe link, die meer gelijkenis vertonen met phishing mails, werden als veiliger beoordeeld. Hetzelfde patroon gaat op voor privacy. De scores op privacy voor betalingsmails met (G = 3.61 SD = 1.35) en zonder (G = 3.58 SD = 1.34) directe link lopen eveneens amper uiteen. Ook dit verschil is insignificant (t(189) = 0.19, p = .85) en in strijd met de hypothese: betalingsmails zonder link worden ervaren als een grotere bedreiging voor de privacy.

Ook hier zou het ontwerp van het materiaal een effect kunnen verhinderen. In de condities zonder directe link staat desalniettemin een expliciet verzoek om persoonsgegevens. Klanten kunnen namelijk handmatig naar de site gaan om daar te betalen of zich in te schrijven in het register. Als klanten dit verzoek opvolgen, zouden zij dus alsnog slachtoffer van phishing kunnen worden. De conditie zonder link is dus niet manifest veiliger en of minder privacygevoelig.

Daarbij valt het op dat de gemiddelde scores voor privacy en veiligheid rond de vier liggen. Vier is het middelpunt van de 7-puntschaal. Proefpersonen hebben dus een redelijk neutrale mening over de risico's van betalingsmails. Het zou kunnen dat de gelijkenis tussen betalingsmails en spear phishing toch minder apert is dan ik eerder voorstelde. Spear phishing ontleent zijn effectiviteit aan realisme: de e-mails zijn persoonlijk geadresseerd en afkomstig van een werkelijke relatie (Caputo et al., 2014). Hoewel de betalingsmails verschillende verdachte kenmerken bevatten – zoals een urgent verzoek om betaling en persoonsgegevens – is het mogelijk dat proefpersonen de betalingsmails toch niet dubieus vinden. Het realisme van betalingsmails kan de verdachte kenmerken overstemmen. Hypothese drie is dus niet bevestigd.

7.2.5 Hypothese 4

Naast de directe link naar de betalingsomgeving, onderzocht ik ook de invloed van het sociaal contract. Vertrouwen is bij online zakendoen erg laag, vanwege de onpersoonlijke aard en ondoorzichtigheid. Voldoende vertrouwen is voor klanten echter wel noodzakelijk om over te gaan tot een aankoop of online transactie (Belanger et al., 2002; Chen, 2010; Hoffman et al., 1999). In het geval van betalingsmails kan dit relatief lage vertrouwen nadelig uitpakken: de argwaan of angst voor phishing zou kunnen intensiveren naarmate het vertrouwen daalt. Een gebrek aan vertrouwen kan dus afdoen aan de effectiviteit van betalingsmails. Om het vertrouwen in betalingsmails te bevorderen, werd er een sociaal contract ingevoerd. Dit is een substituut voor een menselijke, persoonlijke afspraak over het gebruik van persoonsgegevens dat online vertrouwen kan stimuleren (Belanger et al., 2002; Hoffman et al., 1999). Die vierde hypothese luidde dan ook.

H4: Betalingsmails met een sociaal contract leiden tot meer vertrouwen in de behandeling van persoonsgegevens door a.s.r. dan betalingsmails zonder sociaal contract.

Tabel 9: *Gemiddelden en (standaarddeviaties) voor vertrouwen gesorteerd op condities zonder en met sociaal contract (schaal 1-7; helemaal mee oneens – helemaal mee eens).*

	Sociaal contract afwezig (N=111)	Sociaal contract aanwezig (N=80)
Vertrouwen	4.4 (0.88)	4.7 (0.90)

Het vertrouwen in a.s.r. bij betalingsmails met sociaal contract (G = 4.7 SD = 0.90) was hoger dan in de betalingsmails zonder sociaal contract (G = 4.4 SD = 0.88). Proefpersonen geloofden dus sterker in de integriteit en betrouwbaarheid van a.s.r. door het toegevoegde kader. Daarbij was dit verschil significant (t(182) = 0.67, p = <.05). Het effect is dus niet toevallig. De toename in vertrouwen is niet enorm, maar wel meetbaar [tabel 9]. Hypothese vier is dus bevestigd.

7.2.6 Hypothese 5

De inhoud van het sociaal contract richtte zich uitsluitend op de privacy en veiligheid van persoonsgegevens. Dit zijn immers de meest relevante onderwerpen bij online zakendoen, in het

bijzonder door de overeenkomsten tussen spear phishing en betalingsmails (Hoffman et al., 1999; Midha, 2012). Ik vermoedde daarom dat het sociaal contract de ervaren veiligheid en privacy zou doen toenemen:

H5: Betalingsmails met een sociaal contract leiden tot meer ervaren veiligheid en privacy van persoonsgegevens dan betalingsmails zonder sociaal contract.

Tabel 10: *Gemiddelden en (standaarddeviaties) voor privacy en veiligheid gesorteerd op condities zonder en met sociaal contract (schaal 1-7; helemaal mee oneens – helemaal mee eens).*

	Sociaal contract afwezig (N=111)	Sociaal contract aanwezig (N=80)
Privacy	3.3 (1.21)	4.0 (1.44)
Veiligheid	3.3 (1.49)	4.1 (1.70)

De ervaren privacy in de condities met sociaal contract (G = 4.0 SD = 1.44) was hoger dan in de condities zonder sociaal contract (G = 3.3 SD = 1.21). Dit verschil was significant (t(189) = 0.14, p = <.05). Hetzelfde beeld geldt voor veiligheid: de ervaren veiligheid in de condities met sociaal contract (G = 4.1 SD = 1.70) was hoger dan in de condities zonder sociaal contract (G = 3.3 SD = 1.49). Ook dit verschil was significant (t(189) = 0.36, p = <.05). Het sociaal contract zorgt dus voor een aanzienlijke toename in de gepercipieerde veiligheid en privacy [tabel 10]. Hypothese vijf is daarmee bevestigd.

7.2.7 Hypothese 6

Het sociaal contract heeft dus een positieve invloed op vertrouwen in a.s.r. en de gepercipieerde privacy en veiligheid. Uit onderzoek blijkt dat meer vertrouwen bij online zakendoen een positieve uitwerking heeft op de gedragsintentie: klanten gaan eerder over tot een aankoop of betaling als het vertrouwen hoog is (Belanger et al., 2002; Chen, 2010; Hoffman et al., 1999; Midha, 2012). Ik verwachtte daarom dat betalingsmails met een sociaal contract zouden leiden tot minder uitstel van betaling:

H6: Betalingsmails met een sociaal contract leiden tot minder uitstel van betaling dan betalingsmails zonder een sociaal contract.

Tabel 11: *Gemiddelden en (standaarddeviaties) voor gedragsintentie en gebruikersgemak gesorteerd op condities zonder en met sociaal contract (schaal 1-7; helemaal mee oneens – helemaal mee eens).*

	Sociaal contract afwezig (N=111)	Sociaal contract aanwezig (N=80)
Gedragsintentie	3.0 (1.66)	3.6 (1.73)
Gebruikersgemak	3.7 (1.42)	4.1 (1.68)

De intentie om te betalen was sterker in de condities met sociaal contract (G = 3.6 SD = 1.73) dan in de condities zonder sociaal contract (G = 3.0 SD = 1.66). Ook beoordeelden proefpersonen het gebruikersgemak positiever in de condities met sociaal contract (G = 4.1 SD = 1.68 tegenover G = 3.7 SD = 1.42). Zowel het verschil in gedragsintentie (t(167) = -2.22, p = <.05) als in gebruikersgemak (t(153) = -1.83, p = <.05) was significant. Proefpersonen zijn door het sociaal contract dus eerder geneigd hun achterstallige premie te betalen. Daarbij vinden zij de betalingsmails met sociaal contract makkelijker in gebruik. Hypothese zes is dus bevestigd. Het is wel opvallend dat gemiddelde scores niet erg hoog zijn: de scores liggen rond het middelpunt van de schaal. De toevoeging van het sociaal contract is dus geen panklare oplossing voor

het effectiviteitsprobleem van betalingsmails. In het hoofdstuk 'advies' ga ik verder in op de mogelijke toepassingen van het sociaal contract voor a.s.r.

7.2.8 Hypothese 7

Tot nog toe behandelde ik de effecten van de directe link en het sociaal contract afzonderlijk. Een samenspel is echter niet uitgesloten. Ik verwachtte dat de directe link klanten zou aanzetten om direct te betalen. Angst of argwaan voor phishing zou deze stimulans kunnen temperen. Een sociaal contract kan vertrouwen, privacy en veiligheid daarentegen verhogen. Een sociaal contract in combinatie met een directe link zou als koppel dus kunnen bijdragen aan de intentie om te betalen. Hypothese zeven luidde daarom:

H7: Het effect van een directe link naar de betalingsomgeving op de intentie om direct te betalen, is groter bij betalingsmails met een sociaal contract.

Tabel 12: *Gemiddelden en (standaarddeviaties) voor gedragsintentie en gebruikersgemak gesorteerd per betalingsmail, ofwel conditie (schaal 1-7; helemaal mee oneens – helemaal mee eens).*

	Geen link Geen sociaal contract (N=56)	Link Geen sociaal contract (N=55)	Geen link Sociaal contract (N=42)	Link Sociaal contract (N=38)
Gedragsintentie	2.9 (1.65)	3.2 (1.67)	3.4 (1.72)	3.8 (1.73)
Gebruikersgemak	3.7 (1.42)	3.8 (1.42)	3.9 (1.72)	4.4 (1.59)

De aanwezigheid van een keurmerk bij de directe link resulteerde in een sterkere gedragsintentie (G = 3.8 SD = 1.73 tegenover G = 3.2 SD = 1.67) en positiever beoordeeld gebruikersgemak (G = 4.4 SD = 1.59 tegenover G = 3.8 SD = 1.42) [tabel 14]. Het verschil in gedragsintentie ($F(3, 187) = 0.00$, $p = .96$) noch gebruikersgemak ($F(3, 187) = 0.76$, $p = .38$) was echter significant.

Om de afwezigheid van een effect te verklaren, grijp ik terug op hypothese drie. Hier stelde ik vast dat een directe link geen negatieve invloed had op de ervaren veiligheid en privacy. De vormgeving van het materiaal werd aangestipt als mogelijke oorzaak: in de condities zonder directe link stond nog steeds een verzoek om persoonsgegevens. De bedreiging van de veiligheid en privacy van persoonsgegevens was dus van dezelfde orde van grote in de condities met en zonder link.

Het sociaal contract zou de veronderstelde negatievere perceptie van veiligheid en privacy in de condities met een directe link beperken. Dit zou een positieve uitwerking hebben op de intentie om te betalen. Als de link op zichzelf echter niet leidt tot negatievere privacy en veiligheid, heeft de combinatie van link en sociaal contract geen toegevoegde waarde. Er is immers geen negatieve perceptie van veiligheid en privacy die het sociaal contract kan afzwakken. Het is dus logisch dat de combinatie van sociaal contract en link geen effect had op de gedragsintentie.

7.2.9 Hypothese 8

Ik veronderstelde dat een directe link, vanwege de gelijkenis met spear phishing, afbreuk zou doen aan de ervaren veiligheid en privacy. Het sociaal contract zou dit negatieve effect kunnen afzwakken. Een sociaal contract leidt immers tot positievere scores op privacy, veiligheid en vertrouwen. De laatste hypothese luidde daarom:

H8: Het effect van e-mails met een directe link naar de betalingsomgeving op de ervaren veiligheid en privacy is kleiner bij betalingsmails met een sociaal contract

Tabel 13: *Gemiddelden en (standaarddeviaties) voor privacy en veiligheid gesorteerd per betalingsmail, ofwel conditie (schaal 1-7; helemaal mee oneens – helemaal mee eens).*

	Geen link Geen sociaal contract (N=56)	Link Geen sociaal contract (N=55)	Geen link Sociaal contract (N=42)	Link Sociaal contract (N=38)
Privacy	3.3 (1.16)	3.4 (1.26)	3.9 (1.49)	4.0 (1.41)
Veiligheid	3.3 (1.58)	3.3 (1.41)	3.9 (1.69)	4.3 (1.69)

De aanwezigheid van een sociaal contract bij de directe link resulteerde wel in positievere veiligheidsscores (G = 4.3 SD = 1.69 tegenover G = 3.3 SD = 1.41), maar niet in positievere privacyscores (G = 3.4 SD = 1.26 tegenover G = 4.0 SD = 1.41). Zowel het verschil in veiligheid ($F(3, 187) = 0.61$, $p = .43$) als privacy ($F(3, 187) = 0.01$, $p = .91$) was niet significant. Een directe link in combinatie met een sociaal contract leidde dus niet tot een positievere perceptie van privacy en veiligheid. Hypothese acht is niet bevestigd.

De afwezigheid van een effect is hetzelfde te duiden als bij hypothese zeven: een link leidde op zichzelf niet tot negatievere scores op veiligheid en privacy. Door een sociaal contract bij te voegen, ontstaat er logischerwijs ook geen interactie-effect: als de link geen privacy- of veiligheidsbezwaren oproept, kan het sociale contract deze ook niet afzwakken.

Tabel 14: *Overzicht van de hypotheses en testuitslagen*

Hypothese		Bevestigd
1	Betalingsmails worden door meer klanten gelezen dan betalingsbrieven	Deels
2	Betalingsmails met een directe link naar de betalingsomgeving leiden tot minder uitstel van betaling dan betalingsmails zonder directe link.	Nee
3	Betalingsmails met een directe link naar de betalingsomgeving worden als een grotere bedreiging ervaren voor de privacy en veiligheid van persoonsgegevens dan betalingsmails zonder link naar de betalingsomgeving.	Nee
4	Betalingsmails met een sociaal contract leiden tot meer ervaren veiligheid en privacy van persoonsgegevens dan betalingsmails zonder sociaal contract.	Ja
5	Betalingsmails met een sociaal contract leiden tot meer ervaren veiligheid en privacy van persoonsgegevens dan betalingsmails zonder sociaal contract.	Ja
6	Betalingsmails met een sociaal contract leiden tot minder uitstel van betaling dan betalingsmails zonder een sociaal contract.	Ja
7	Het effect van een directe link naar de betalingsomgeving op de intentie om direct te betalen, is groter bij betalingsmails met een sociaal contract.	Nee
8	Het effect van e-mails met een directe link naar de betalingsomgeving op de ervaren veiligheid en privacy is kleiner bij betalingsmails met een sociaal contract.	Nee

8.0 Wetenschappelijke discussie

In dit hoofdstuk reflecteer ik eerst op de wetenschappelijke theorie (8.1). Hieruit komen direct suggesties voort voor vervolgonderzoek. Vervolgens noem ik nog enkele beperkingen van het onderzoek (8.2).

8.1 Reflectie op de wetenschappelijke theorie

Resultaten in strijd met de wetenschappelijke theorie

Dit onderzoek leverde een aantal opvallende resultaten op. Sommige uitkomsten druisten tegen de bestaande theorie in, andere waren juist een bevestiging van deze theorie. Ten eerste was het opmerkelijk dat de directe link geen effect had op ervaren veiligheid en privacy. De betalingsmails bevatten drie verdachte kenmerken van phishing: het is een nieuw soort, onconventioneel bericht, het gaat om een urgent verzoek en er wordt gevraagd om geld en persoonlijke gegevens (Downs et al., 2006; Metzger, 2007; Singleton, 2005). Ik verwachtte dat deze kenmerken in combinatie met een directe link, het bekendste kenmerk van phishing (Hong, 2012), zouden leiden tot negatievere beoordelingen van privacy en veiligheid.

Het uitblijven van de effecten is in strijd met de huidige theorie over phishing. Zo blijkt uit eerder onderzoek dat een verzoek om geld of bankgegevens bij 75% van de mensen argwaan oproept (Downs et al., 2006). Ook hebben 95% van de mensen die online zakendoen weleens persoonsgegevens voor zich gehouden uit angst voor phishing (Hoffman, Novak & Peralta, 1999). De literatuur wijst dus op een algemene angst en behoedzaamheid voor phishing mails. Toch zijn de scores op veiligheid en privacy voor de betalingsmails, die zijn doorspekt van phishing-kenmerken, neutraal: de scores liggen rond het midden van de schaal en verhogen niet significant door een directe link.

Hiervoor zijn drie mogelijke verklaringen. Ten eerste zouden proefpersonen indifferent kunnen zijn ten aanzien van veiligheids- en privacy-risico's. Deze verklaring is niet erg plausibel. Uit verschillende bronnen blijkt immers dat mensen veel belang hechten aan online privacy en veiligheid (Downs et al., 2006; Hoffman, Novak & Peralta, 1999). Ook in dit onderzoek hebben proefpersonen online privacy en veiligheid hoog in het vaandel staan (7.2.1).

Het is dus aannemelijker dat proefpersonen simpelweg niet weten hoe zij privacy- en veiligheidsrisico's van betalingsmails moeten inschatten. Blijkbaar zijn de verdachte eigenschappen niet bekend of duidelijk genoeg om argwaan, voorzichtigheid aan te wakkeren. Oudere phishing mails waren vaak onpersoonlijk of stonden vol spelfouten (Hong, 2012). De moderne spear phishing mails zijn daarentegen persoonlijk en nauwelijks te onderscheiden van echte mails. De verdachte eigenschappen uit de betalingsmails worden hierdoor waarschijnlijk niet langer beschouwd als kenmerken van phishing.

Als laatste zou de onderzoeksetting de resultaten kunnen beïnvloeden. Proefpersonen weten dat ze meedoen aan een wetenschappelijk onderzoek. Het risico op phishing is hierdoor hypothetisch. Daadwerkelijke diefstal van persoonsgegevens is immers uitgesloten in een wetenschappelijk onderzoek. Dit hypothetische, onrealistische risico zou neutrale scores in de hand kunnen werken. Een hypothetisch risico beoordelen vereist namelijk veel inlevingsvermogen.

Vervolgonderzoek naar spear phishing zou interessant zijn. Er is meer kennis nodig over de specifieke determinanten van argwaan behoedzaamheid in de context van spear phishing. De kenmerken die in oudere phishing mails aanzetten tot bedachtzaamheid, zijn in spear phishing mails immers niet meer effectief.

Resultaten in lijn met de wetenschappelijke theorie

Dit onderzoek was op andere vlakken wel in lijn met de wetenschappelijke theorie. Zo bleek het sociaal contract inderdaad een positieve uitwerking te hebben op onder meer privacy, veiligheid, vertrouwen en de intentie om te betalen. Het contract lijkt dus inderdaad te functioneren als substituut voor menselijke, interpersoonlijke afspraken (Belanger et al., 2002; Hoffman et al., 1999). Door simpelweg een kader toe te voegen met enkele afspraken en gedragsregels, kan de kwaliteit van online transacties en zakendoen dus al worden verbeterd.

Omdat het sociaal contract zo effectief bleek, zou het interessant zijn om vervolgonderzoek meer toe te spitsen. Het contract in dit onderzoek bestond uit drie verschillende elementen: een privacywaarborg, een veiligheidsindicator en uitgeschreven privacyverklaring. Door deze combinatie blijft het onduidelijk of en in hoeverre individuele elementen bijdragen aan de effecten van het contract. In de toekomst zouden deze elementen dus individueel kunnen worden onderzocht, om zo meer inzicht te krijgen in de werking van het sociaal contract.

8.2 Beperkingen van het onderzoek

Dit onderzoek heeft een aantal beperkingen. Ten eerste is het onderzoek niet volledig toepasbaar op de alledaagse praktijk (8.2.1). Daarnaast is het soms onzeker of een gemeten begrip, zoals privacy, een afspiegeling is van het daadwerkelijke begrip (8.2.2.). Als laatste valt de onderzoeksmethode te bekritiseren (8.2.3).

8.2.1 Toepasbaarheid op de alledaagse praktijk

De vraag rijst in hoeverre deze resultaten aansluiten op de alledaagse praktijk. Ofwel: in hoeverre is het onderzoek ecologisch valide. Er zijn drie duidelijke verschillen met de alledaagse praktijk. Ten eerste hebben proefpersonen geen echte betalingsachterstand. Het blijft dus onzeker of klanten die daadwerkelijke een achterstallige premie hebben, hetzelfde zouden reageren op de betalingsmails. Zo is het mogelijk dat deze klanten a.s.r. negatiever zouden beoordelen.

Ten tweede ontvingen proefpersonen slechts één betalingsherinnering: de aanmaning. De normale, trapsgewijze verzending van de drie betalingsherinnering ontbreekt dus. Het is denkbaar dat klanten de betalingsmail anders zouden beoordelen als er reeds twee berichten aan voorafgingen.

Als laatste verschilde de betalingsmail van de alledaagse praktijk vanwege de onderzoeksetting. Proefpersonen weten dat het om een wetenschappelijk onderzoek gaat. Deze kennis kan doorwerken op onder meer de perceptie van privacy en veiligheid. Privacy en veiligheidsrisico's zijn bij een wetenschappelijk onderzoek namelijk nihil. Het is uitgesloten dat de betalingsmail een echte phishing mail is. Privacy en veiligheid moeten daarom hypothetisch worden beoordeeld, wat niet overeenkomt met de werkelijkheid. Dit zou ook kunnen verklaren waarom de directe link geen effect had op de gepercipieerde privacy en veiligheid: proefpersonen zouden privacy en veiligheid irrelevant kunnen vinden in een onderzoeksetting.

Al met al wijkt dit onderzoek dus op verschillende punten af van de alledaagse praktijk. Dergelijke afwijkingen zijn gebruikelijk en misschien zelfs onvermijdelijk in wetenschappelijk onderzoek. Wel moeten deze beperkingen worden meegewogen bij de interpretatie en toepassing van de resultaten.

8.2.2 Verschillen tussen het gemeten en daadwerkelijke begrip

Naast verschillen tussen de onderzoekspraktijk en werkelijkheid, keek ik ook kritisch naar divergentie van gemeten en daadwerkelijke begrippen, ofwel constructvaliditeit. Is de perceptie van privacy bijvoorbeeld niet van meer factoren afhankelijk dan aan bod komen in de vragenlijst?

Om het daadwerkelijke begrip zo dicht mogelijk te benaderen, gebruikte ik wijdverspreide en gevalideerde vragenclusters. Ik bedacht de vragen over vrij abstracte onderwerpen als privacy en veiligheid dus niet zelf, maar trad in de voetsporen van wetenschappers. Ik denk dat er slechts bij één onderwerp een aanzienlijk hiaat bestond tussen het gemeten en werkelijke begrip: de persoonlijke voorkeur voor online privacy en veiligheid.

Dit is namelijk bij uitstek een onderwerp waar een realistische meting lastiger is. Als je proefpersonen vraagt of zij online privacy en veiligheid belangrijk vinden, zijn ze geneigd instemmend te antwoorden. Weinig mensen zijn immers tegen online privacy en veiligheid. Het is echter onwaarschijnlijk dat het toegekende belang doorwerkt in de praktijk. In de praktijk is de afweging namelijk veel complexer: er is niet altijd genoeg tijd of kennis om rekening te houden met online privacy en veiligheid. Zo kan ik onmogelijk de privacyverklaring doorlezen van elke website die ik bezoek. Een vragenlijst is dus een vrij onnauwkeurig meetinstrument voor daadwerkelijke voorkeuren voor online privacy en veiligheid. De resultaten moeten op dit vlak dus kritisch worden beoordeeld.

8.2.3 Beperkingen van de onderzoeksmethode

Als laatste valt er een kritische kanttekening te plaatsen bij de onderzoeksmethode. Ik nam dit onderzoek online af. Online afname heeft verschillende beperkingen. Zo is er een sterke variatie in de onderzoekomgeving. Sommige mensen zullen het onderzoek in een rustige ruimte invullen, andere in een drukke trein. Daarbij had ik geen zicht op het verloop van het onderzoek. Ik kon niet controleren of mensen het onderzoek volledig begrepen en geconcentreerd invulden. Online afname kan dus afdoen aan de algehele kwaliteit van de respons. Daarentegen maakte de online tool een snelle verspreiding van het onderzoek mogelijk. De voordelen wegen mijns inziens daarom op tegen de nadelen.

9.0 Conclusie

Dit onderzoek richtte zich op de betalingsbrieven van a.s.r. Schade. Deze zijn ineffectief: achterstallige premies worden niet of niet snel genoeg betaald naar aanleiding van de betalingsherinneringen. a.s.r. is van plan om betalingsherinnering - en brieven in het algemeen - binnen enkele jaren per e-mail te gaan verzenden. Ik onderzocht daarom eerst wat de huidige problemen van betalingsbrieven precies waren. Vervolgens bestudeerde ik of, en zo ja hoe, deze problemen waren op te lossen in de overgang naar betalingsmails. Hierbij was het onderzoeksdoel tweeledig. Enerzijds mondde dit onderzoek uit in kennis en advies over effectievere betalingsmails. Anderzijds konden aan de resultaten meer algemene adviezen worden ontleend voor de aanstaande, volledige overstap op e-mail.

Een praktisch probleem beperkte de effectiviteit van betalingsbrieven: veel klanten vergaten betalingsbrieven of ontvingen ze niet. Ik vermoedde dat de overstap op e-mail dit probleem deels zou verhelpen. E-mails kunnen immers op verschillende apparaten direct worden gelezen en opgevolgd. Deze veronderstelling klopte grotendeels. Mensen gaven aan dat ze hun e-mails vaker bekijken en minder snel vergeten dan papieren post.

Om de effectiviteit van de betalingsmails verder te vergroten, onderzocht ik het effect van een directe link. Ik nam aan dat deze link enerzijds zou resulteren in een sterkere gedragsintentie en meer gebruikersgemak. De link stelt klanten namelijk in staat om de betaling direct en eenvoudig te voldoen. Anderzijds verwachtte ik dat de link, vanwege de gelijkenis met phishing (Caputo et al., 2014; Hong, 2012), zou afdoen aan de ervaren privacy en veiligheid van het bericht. Beide veronderstellingen bleken onwaar. De link was geen prikkel voor betaling en riep evenmin argwaan op voor de privacy en veiligheid van persoonsgegevens.

Naast de link onderzocht ik de invloed van een sociaal contract. Het vertrouwen is bij online zakendoen en transacties, onder meer vanwege de onpersoonlijke aard, erg laag (Belanger et al., 2002; Chen, 2010; Hoffman et al., 1999). Laag vertrouwen beïnvloedt de gedragsintentie negatief. Minder vertrouwen staat dus gelijk aan minder aankopen en transacties. Uit eerder onderzoek bleek dat een sociaal contract, met regels over het gebruik van persoonsgegevens, vertrouwen kan bevorderen (Belanger et al., 2002; Hoffman et al., 1999). Ik veronderstelde daarom dat een sociaal contract een positieve uitwerking zou hebben op vertrouwen, de ervaren privacy/veiligheid en de intentie om te betalen. Al deze hypotheses werden bevestigd: het sociaal contract had een positieve uitwerkingen op alle drie de aspecten.

Concluderend was het sociaal contract op zichzelf doeltreffend. Het droeg echter niet bij aan de effectiviteit van de directe link. De combinatie van sociaal contract en directe link mondde dus niet uit in een positievere perceptie van privacy/veiligheid en een sterkere intentie om te betalen. Al met al droeg de directe link in geen enkel opzicht bij aan de effectiviteit van betalingsmails. Het sociaal contract zorgde daarentegen voor meer vertrouwen, een sterkere gedragsintentie, meer gebruikersgemak en een positievere perceptie van privacy en veiligheid. Dit onderzoek heeft verschillende beperkingen en er is veel vervolgonderzoek nodig. Desalniettemin concludeer ik dat een sociaal contract een positieve uitwerking kan hebben op de effectiviteit van betalingsmails. In het hoofdstuk ‘aanbevelingen’ smelt ik deze conclusie om tot concrete handvatten voor a.s.r.

10.0 Aanbevelingen

In dit hoofdstuk vorm ik de resultaten van het onderzoek om tot concrete aanbevelingen voor a.s.r. Eerst geef ik specifiek advies om de effectiviteit van betalingsbrieven te vergroten in de overstap naar betalingsmails (10.1). Vervolgens draag ik meer algemene aanbevelingen aan voor de overgang van brief naar e-mail.

10.1 Aanbevelingen voor effectievere betalingsmails

In dit hoofdstuk zet ik eerst nog eenmaal het probleem van betalingsbrieven helder uiteen (10.1.1). Vervolgens doe ik aanbevelingen om dit probleem te verhelpen (10.1.2-10.2.5).

10.1.1 De ineffectiviteit van betalingsbrieven

Het probleem met de huidige betalingsbrieven is concreet: ze zijn ineffectief. Klanten betalen hun achterstallige premie niet (op tijd) naar aanleiding van de betalingsherinneringen. Dit probleem is vrij urgent. Enerzijds omdat a.s.r. veel inkomsten misloopt[4] en niet doeltreffend communiceert. Anderzijds omdat klanten na de uiterste datum niet langer zijn verzekerd, wat vanzelfsprekend onwenselijk is. Dit probleem stond al enige tijd op de agenda binnen a.s.r. Tot nog toe was er echter nog niet concreet naar oplossingen gezocht. Binnen enkele jaren wil a.s.r. het proces van betalingsbrieven digitaliseren: brieven worden omgezet in e-mails. Dit is een kansrijke transitie. De overstap op e-mail is voor a.s.r. namelijk een mogelijkheid om de betalingsherinneringen te vernieuwen en verbeteren. Om de effectiviteit van betalingsmails te vergroten, raad ik a.s.r. het volgende aan:

10.1.2 Aanbeveling 1

Aanbeveling: Stap binnen afzienbare tijd (binnen twee jaar) over op e-mail. Onafhankelijk van de inhoud van de betalingsherinnering.

Het voordeel van de overstap op e-mail

Mensen stellen dat ze hun inbox vaker bekijken dan hun brievenbus en e-mails minder snel vergeten dan brieven. Dergelijke praktische zaken stonden de effectiviteit van betalingsbrieven in de weg. Ik verwacht dus dat de overstap op e-mail op zichzelf al bijdraagt aan de effectiviteit van betalingsmails. Daarbij is de verzending van e-mails goedkoper dan brieven. De overstap zal dus, zelfs als de betalingen niet toenemen, kostenbesparend zijn.

Het verwachte effect van de overstap op e-mail

Het effect van de overstap op e-mail is waarschijnlijk beperkt. Mensen geven aan nieuwe e-mails gemiddeld 16.6% vaker te checken dan nieuwe brieven en e-mails gemiddeld 10.3% minder vaak te vergeten. Overstappen op e-mail, zonder de inhoud van het bericht te veranderen, zal dus geen enorme impact hebben.

De implementatie van de overstap op e-mail

Daarbij moet er nog een praktische hindernis worden genomen: a.s.r. moet de e-mailadressen van alle klanten achterhalen. Veel e-mailadressen zijn nu nog onbekend. Ook moet a.s.r. in de

[4] Ik heb helaas niet de exacte schade kunnen achterhalen als gevolg van achterstallige premies.

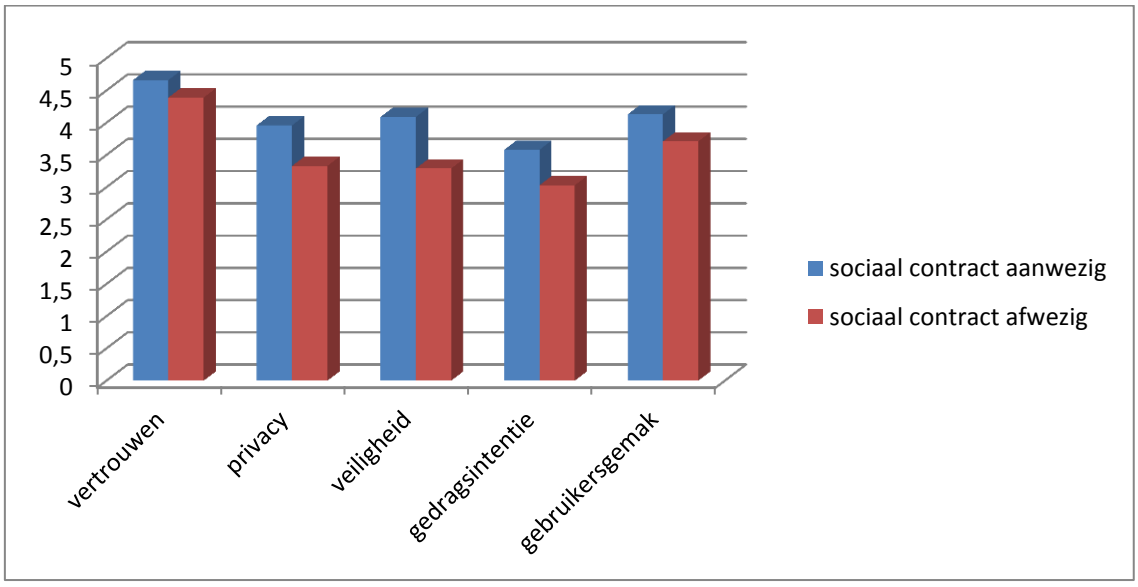
transitie rekening houden met klanten die geen e-mail willen of kunnen gebruiken. Deze groep moet worden geïdentificeerd en kunnen blijven corresponderen per post.

10.1.2 Aanbeveling 2

Aanbeveling: voeg een sociaal contract toe aan betalingsmails.

Het voordeel van een sociaal contract

In een sociaal contract staan afspraken over de veiligheid en privacy van persoonsgegevens, in de vorm van tekst en/of afbeeldingen. Digitale communicatie is vaak onpersoonlijk en niet inzichtelijk, waardoor er moeizaam vertrouwen ontstaat tussen de afzender en geadresseerde. De afspraken in het sociaal contract vormen een nieuwe basis voor dit vertrouwen. Het contract leidt daarbij tot een positievere perceptie van veiligheid en privacy. Als laatste heeft het contract een positieve uitwerking op de intentie om te betalen en het gebruikersgemak. Meer klanten zullen hun achterstallige premie dus betalen door het sociaal contract.



Figuur 5: De beoordeling van vertrouwen, privacy, veiligheid, gedragsintentie en gebruikersgemak (schaal 1-7) voor betalingsmails met en zonder sociaal contract

Het verwachte effect van het sociaal contract

Het effect van het sociaal contract is relatief groot. De verwachte verbetering zijn per deelgebied niet gigantisch, zoals te zien is in de voorgaande grafiek [figuur 5]. Alleen de toename van ervaren veiligheid (17.8%) is aanzienlijk. Hoewel het sociaal contract dus niet zorgt voor spectaculaire verbeteringen op deelgebieden, vindt er wel een algemene verbetering plaats. De kwaliteit van de betalingsmails zal dus over de hele linie enigszins vooruitgaan.

De implementatie van het sociaal contract

Het sociaal contract is, afhankelijk van de invulling, relatief eenvoudig in te voeren. Ook is het een goedkope aanpassing. Het gaat immers om een kader met tekst en afbeeldingen. De veiligheidsindicator is een technisch en organisatorisch complexer onderdeel. Hiervoor is namelijk nieuwe software nodig. Ook heeft a.s.r. een persoonlijke afbeeldingen en e-mailadres van

klanten nodig om de veiligheidsindicator te implementeren. Als a.s.r. het sociaal contract snel wil invoeren, zou ze de veiligheidsindicator dus aanvankelijk kunnen schrappen.

10.1.3 Aanbeveling 3

Aanbeveling: voeg een directe link toe naar de betalingsomgeving.

Het voordeel van een directe link

Een directe link naar de betalingsomgeving vergemakkelijkt betaling na ontvangst van de betalingsmail. Klanten kunnen met één druk op de knop hun achterstallige premie voldoen. Een link naar de betalingsomgeving is een beproefde methode, die onder meer wordt gebruikt door online warenhuis bol.com.

Het verwachte effect van de directe link

De impact van een directe link is waarschijnlijk beperkt. In dit onderzoek leidde een link tot een iets (4.9%) sterkere intentie om te betalen. Deze verhoging was niet significant. De verwachte toename van betalingen is dus gering. Dit beperkte effect is waarschijnlijk te wijden aan beperkingen van het onderzoek (7.2.2). De kracht van snel en online betalen staat echter buiten kijf: ongeveer 60 procent van de Europese bedrijven doet online zaken en dit percentage blijft toenemen (Falk & Hagsten, 2015). Ik adviseer daarom om de link in te voeren om vervolgens te zoeken naar een effectievere vormgeving.

De implementatie van de directe link

Proefpersonen ervoeren de link, ondanks de gelijkenis met phishing (5.1.2), niet als een bedreiging voor de privacy en veiligheid van persoonsgegevens. Hierdoor hoeft a.s.r. dus niet erg terughoudend te zijn bij implementatie van de link: de afwezigheid van privacy- en veiligheidsbezwaren scheppen bewegingsruimte om de link te realiseren.

De link is daarbij relatief eenvoudig te implementeren. De link verwijst namelijk naar bestaande betalingsomgeving(en), zoals IDEAL. De toevoeging gaat intern ongetwijfeld gepaard met technische en procesmatige aanpassingen. De hoofdmoot, het betalingsnetwerk zelf, bestaat echter al.

10.2 Aanbevelingen voor de toekomstige overstap op digitale communicatie

De aanbevelingen voor betalingsmails richten zich op een specifiek probleem: de ondermaatse effectiviteit van betalingsbrieven. De algemene aanbevelingen voor de overstap van brief naar e-mail zijn daarentegen meer doelgericht. In dit hoofdstuk omschrijf ik daarom eerst de doelstelling van a.s.r. (10.2.1). Vervolgens doe ik drie aanbevelingen om dit doel te realiseren (10.2.2-10.2.5).

10.2.1 Doelstelling voor de transitie richting communicatie per e-mail

a.s.r. richt haar pijlen op digitaal communiceren en zakendoen. Deze doelstelling is breed en complex: ze omvat onder meer de overgang van brief naar e-mail, een grotere rol voor online service (chat, whatsapp), kwalitatieve, interactieve websites (de nieuwe website van a.s.r.) en de mogelijkheid om online te verzekeren (Ditzo). De focus op digitaal communiceren is urgent en onvermijdelijk. Digitale communicatie groeit namelijk enorm, zowel binnen als buiten de

verzekeringsbranche. Het is simpelweg geen optie om niet digitaal te communiceren. Het klantcontact zal hierdoor op termijn verwateren, wat vanzelfsprekend schadelijk is voor a.s.r.

Ik kan geen advies geven voor alle deelgebieden van digitale communicatie. Uit dit onderzoek zijn wel enkele algemene adviezen te destilleren voor de overgang van brief naar e-mail. De volgende aanbevelingen zijn dus handvatten die de lopende transitie van brief naar e-mail moeten versoepelen.

10.2.2 Aanbeveling 4

Aanbeveling: maak in de overgang van brief naar e-mail gebruik van de grotere symboolvariatie van e-mail.

Elke brief die a.s.r. omzet in een e-mail, is een kans. De transitie is namelijk een mogelijkheid om het bericht kritisch te bekijken en eventueel te herontwerpen. Ik raad a.s.r. aan om bij de overgang op e-mail uit te gaan van symboolvariatie: de hoeveelheid manieren waarop informatie gecommuniceerd kan worden. Symboolvariatie is namelijk de enige mediaeigenschap waar e-mails zich beter voor lenen dan brieven (Dennis & Valachich, 1999). In e-mails kunnen bijvoorbeeld eenvoudig, plaatjes, video's en links worden toegevoegd. Als brieven worden omgezet in e-mails, is het dan ook verstandig om deze toegevoegde waarde te gebruiken.

Symboolvariatie is logischerwijs geen doel op zich: een optimale match tussen medium en boodschap zou leidend moeten zijn. Symboolvariatie is voornamelijk geschikt voor informatieoverdracht. De rijkheid aan symbolen vergemakkelijkt snelle en uitgebreide uitwisseling van informatie (Dennis & Valachich, 1999). Als het accent van een bericht niet op informatieoverdracht ligt, is er dus geen noodzaak om bijvoorbeeld filmpjes of links toe te voegen.[5]

10.2.3 Aanbeveling 5

Aanbevelingen: ontwikkel een beknopte, krachtige - maximaal vijf regels - privacyverklaring.

Het voordeel van een privacyverklaring

De overgang van brief naar e-mail vergroot het belang van privacy. Mensen hechten namelijk veel waarde aan controle over hun persoonsgegevens (Midha, 2012). Controle is online lastiger te waarborgen. Digitale communicatie is relatief diffuus en kwetsbaar: klanten weten niet wie persoonsgegevens hebben of gebruiken en daarbij bestaat er een kans op misbruik, door bijvoorbeeld phishing (Hoffman et al., 1999; Hong, 2012; Midha, 2012).

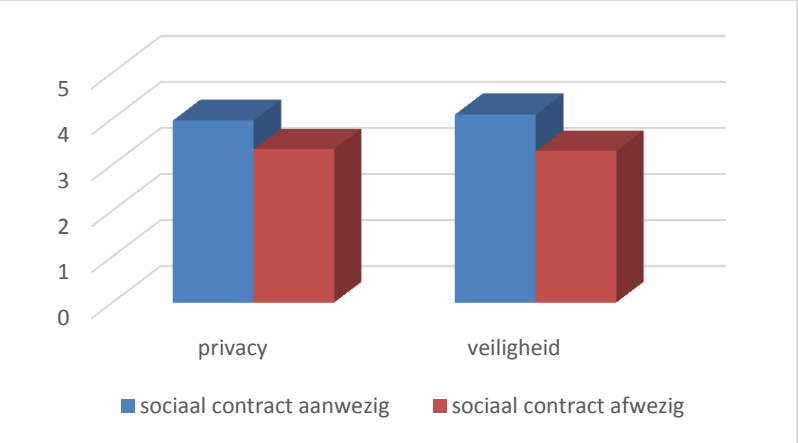
Om de perceptie van privacy te verbeteren, raad ik a.s.r. aan om een korte privacyverklaring op te stellen. Hierin moet terugkomen *dat, waarom* en *hoe* persoonsgegevens worden gebruikt. Ook moet de verklaring een minder privacygevoelig alternatief aanbieden. Als laatste kan er een onafhankelijk privacykeurmerk worden toegevoegd, zoals het privacywaarborg. Een onafhankelijk keurmerk bevordert namelijk de geloofwaardigheid van de privacyverklaring. Deze privacyverklaring kan, als ze wordt toegevoegd aan e-mails, bijdragen aan de ervaren privacy van klanten.

[5] Bij dit advies ga ik niet in op het verwachte effect en de implementatie. Daarvoor is de aanbeveling te algemeen.

Het verwachte effect van een privacyverklaring

De privacyverklaring heeft waarschijnlijk een gering effect. Het sociaal contract, dat grotendeels bestond uit een privacyverklaring, leidde tot een ietwat positievere (9%) perceptie van privacy [figuur 6]. Deze bijdrage kan, door verbeteringen in de verklaring, nog toenemen. Ik raad daarom aan om de verklaring snel in te voeren en vervolgens door te ontwikkelen.

De implementatie van een privacykeurmerk



Figuur 6: De beoordeling van privacy en veiligheid (schaal 1-7) voor betalingsmails met en zonder sociaal contract

a.s.r. kan de privacyverklaring snel en goedkoop inpassen. Er bestaat namelijk al een algemene privacyverklaring. Deze kan als uitgangspunt worden gebruikt voor de ingedikte versie. Een onafhankelijk keurmerk, zoals het privacywaarborg, heeft meer voeten in de aarde. Hiervoor moet het privacybeleid namelijk uitgebreid worden getoetst. a.s.r. zou de privacyverklaring daarom aanvankelijk kunnen invoeren zonder keurmerk.

10.2.4 Aanbeveling 6

Aanbeveling: introduceer een persoonlijke veiligheidsindicator in e-mails over betalingsverkeer.

Het voordeel van een persoonlijke veiligheidsindicator

Digitale veiligheid is een prangend probleem. Zo groeit de hoeveelheid spear phishing mails, die tot veertigmaal effectiever zijn dan traditionele vormen van phishing, spectaculair. Bij spear phishing sturen criminelen een vervalste, maar zeer realistische e-mail, om zo persoonsgegevens of geld te bemachtigen (Caputo et al., 2014). Zo zouden klanten van a.s.r. een vervalste mail uit naam van a.s.r. kunnen krijgen, waarin hen wordt verzocht om geld over te maken.

a.s.r. moet haar klanten beschermen tegen dit soort misbruik. De tevredenheid en veiligheid van klanten is immers een doel op zich en draagt ook bij aan het imago en de reputatie van a.s.r. Tijdens de transitie naar e-mail moet digitale veiligheid dan ook hoog in het vaandel staan. Ik adviseer a.s.r. daarom om een persoonlijke veiligheidsindicator te implementeren in e-mails over betalingen. Bankgegevens zijn voor klanten namelijk het meest gevoelig, precair (Downs et al., 2006; Metzger, 2007). Het is dus zaak om deze gegevens optimaal te beschermen.

Een persoonlijke veiligheidsindicator werkt eenvoudig: de klant deelt een persoonlijke afbeelding met a.s.r. Als deze afbeelding terugkomt in de correspondentie met a.s.r., is de authenticiteit van het bericht gegarandeerd. De bijdrage van de veiligheidsindicator is tweeledig: het

bericht is niet alleen daadwerkelijk, technisch veiliger, maar ook *zichtbaar*. De veiligheidsindicator kan klanten dus geruststellen.

Het verwachte effect van een persoonlijke veiligheidsindicator

Ik verwacht een vrij groot effect van een persoonlijke veiligheidsindicator. In dit onderzoek nam de ervaren veiligheid, door onder meer een persoonlijke veiligheidsindicator, fors toe (17%) [figuur 6]. Daarbij is de effectiviteit van de indicator meermaals wetenschappelijk bevestigd (bijvoorbeeld: Lee & Bauer, 2015; Marforio et al., 2015). De daadwerkelijke en ervaren veiligheid van persoonsgegevens zal dus toenemen.

De implementatie van een persoonlijke veiligheidsindicator

Een persoonlijke veiligheidsindicator is waarschijnlijk niet op korte termijn te realiseren (binnen twee jaar). Ten eerste moet a.s.r. software aanschaffen en invoeren. Binnen een relatief grote organisatie als a.s.r. is dit een tijdrovend en kostbaar proces. Daarbij moet a.s.r. klanten vragen om een persoonlijke afbeelding. Ik vermoed dat veel klanten deze niet direct zullen delen, omdat een persoonlijke veiligheidsindicator relatief onbekend is. Als laatste zijn niet alle e-mailadressen van klanten bekend. a.s.r. kan de indicator dus niet over de hele breedte invoeren.

Concluderend staan er verschillende beren op de weg. Ik opteer daarom voor een geleidelijke invoering van de veiligheidsindicator. Zo zou a.s.r. de indicator eerst als pilot kunnen opzetten. In de loop der tijd kan het project, afhankelijk van de resultaten, worden uitgerold.

Tabel 15: Aanbevelingen voor a.s.r.

Aanbeveling	
Aanbevelingen voor betalingsmails	1. Stap binnen afzienbare tijd (binnen twee jaar) over op e-mail. Onafhankelijk van de inhoud van de betalingsherinnering.
	2. Voeg een sociaal contract toe aan betalingsmails.
	3. Voeg een directe link toe naar de betalingsomgeving.
Aanbevelingen voor de overstap op digitale communicatie	4. Maak in de overgang van brief naar e-mail gebruik van de grotere symboolvariatie van e-mail.
	5. Ontwikkel een beknopte, krachtige - maximaal vijf regels - privacyverklaring.
	6. Introduceer een persoonlijke veiligheidsindicator in e-mails over betalingsverkeer.

10. Literatuurlijst

Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the system usability scale. *Intl. Journal of Human–Computer Interaction*, *24*(6), 574-594.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3), 245-270.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going Spear Phishing: Exploring Embedded Training and Awareness. *Security & Privacy, IEEE*, *12*(1), 28-38.

Cecchinato, M., Cox, A. L., & Bird, J. (2014). "I check my emails on the toilet": Email Practices and Work-Home Boundary Management. MobileHCI.

Chen, Y. H., Hsu, I. C., & Lin, C. C. (2010). Website attributes that increase consumer purchase intention: A conjoint analysis. *Journal of business research*, *63*(9), 1007-1014.

Dennis, A. R., & Valacich, J. S. (1999, January). Rethinking media richness: Towards a theory of media synchronicity. In *Systems Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on* (pp. 10-pp). IEEE.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006, July). Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security* (pp. 79-90). ACM.

Falk, M., & Hagsten, E. (2015). *E-commerce trends and impacts across Europe* (No. 220). United Nations Conference on Trade and Development.

Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services.*Omega*, *32*(6), 407-424.

Hann, I. H., Hui, K. L., Lee, T., & Png, I. (2002). Online information privacy: Measuring the cost-benefit trade-off. *ICIS 2002 Proceedings*, 1.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, *42*(4), 80-85.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*,*55*(1), 74-81.

Kim, K., & Kim, J. (2011). Third-party privacy certification as an online advertising strategy: An investigation of the factors affecting the relationship between third-party certification and initial trust. *Journal of Interactive Marketing*, *25*(3), 145-158.

Lee, J., Bauer, L., & Mazurek, M. L. (2015). The Effectiveness of Security Images in Internet Banking. *Internet Computing, IEEE*, *19*(1), 54-62.

Lentz, L., & Pander Maat, H. (2004). Functional analysis for document design.*Technical communication*, *51*(3), 387-398.

Marforio, C., Masti, R. J., Soriente, C., Kostiainen, K., & Capkun, S. (2015). Personalized Security Indicators to Detect Application Phishing Attacks in Mobile Platforms. *arXiv preprint arXiv:1502.06824*.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, *12*(2), 335-361.

Midha, V. (2012). Impact of consumer empowerment on online trust: An examination across genders. *Decision Support Systems*, *54*(1), 198-205.

NA (2015). Phishing: How many take the bait? Retrieved November 1, 2015, from http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx

Petronio, S. (2002). Boundaries of privacy. *State University of New York Press, Albany, NY*.

Rice, R. E. (1993). Media appropriateness. *Human communication research*,*19*(4), 451-484.

Rijn, J. (2015, 1 april). The ultimate mobile email statistics overview. Ingezien op 1 november 2015, from http://www.emailmonday.com/mobile-email-usage-statistics

Rosoff, M. (2015). People either check email all the time, or barely at all. Retrieved November 1, 2015, from http://uk.businessinsider.com/how-often-do-people-check-their-email-2015-8?r=US&IR=Tt

Singleton, T. (2005). Don't get “hooked” by phishing scams. *Journal of Corporate Accounting & Finance*, *16*(5), 21-28.

Bijlage A – De originele betalingsbrieven

De acceptgiro

ASR Schadeverzekering N.V.

Archimedeslaan 10
3584 BA Utrecht
Postbus 2072
3500 HB Utrecht
www.asr.nl

Datum	<datum>
Onderwerp	Acceptgiro voor uw premie
Behandeld door	Afdeling Acceptatie Schadeverzekeringen
E-mail	betalingscentrum.schade@asr.nl
Telefoon	(030) 278 03 30

Geachte <mevrouw/heer> <naam>,

Hierbij ontvangt u de acceptgiro om de premie voor uw <soort verzekering> met polisnummer <polisnummer> mee te betalen.

Wilt u ervoor zorgen dat uw premie van € <bedrag> op <vervaldatum> op ons rekeningnummer NL59ABNA0240576861 is overgemaakt?

Kosten voor een acceptgiro
Wij rekenen € 1,54 kosten voor betalen met een acceptgiro. Wilt u deze kosten liever niet? Kiest u dan voor automatische afschrijving, of voor betaling via FiNBOX. Meer informatie hierover vindt u op onze website asr.nl/betalingen.

Hebt u nog vragen?
Op asr.nl/betalingen vindt u antwoorden op veel gestelde vragen. Hebt u nog andere vragen of opmerkingen over deze brief? Bel ons dan gerust op (030) 278 03 30. Wij zijn bereikbaar van maandag tot en met vrijdag van 8.30 uur tot 17.00 uur. Wij helpen u graag!

Met vriendelijke groet,

Robert van der Schaaf
directeur Schadeverzekeringen

Bijlage A
Drie betalingsherinneringen

De eerste betalingsherinnering

Dhr. Test
Teststraat 1
1234 AB Testdorp

ASR Schadeverzekering N.V.

Archimedeslaan 10
3584 BA Utrecht
Postbus 2072
3500 HB Utrecht
Nederland
www.asr.nl

Datum	<datum>
Onderwerp	Betalingsherinnering
Behandeld door	Afdeling Acceptatie Schadeverzekeringen
E-mail	betalingscentrum.schade@asr.nl
Telefoon	(030) 278 03 30

Geachte <mevrouw/heer> <naam>,

U hebt een <soort verzekering> met polisnummer <polisnummer> bij ons. Helaas staat er voor deze verzekering nog een bedrag open. Misschien bent u dit vergeten. Het gaat om een bedrag van €<bedrag>. Wilt u dit alsnog betalen? In deze brief vindt u de betaalgegevens. Hebt u ondertussen al betaald? Dan hoeft u uiteraard niets te doen.

Uw betaalgegevens

Bedrag	€ <bedrag>
Rekeningnummer a.s.r.	<rekeningnummer a.s.r.>
Uiterste betaaldatum	<uiterste betaaldatum>
Betalingskenmerk	<betalingskenmerk>

Wat gebeurt er als u niet voor <uiterste betaaldatum> betaalt?
Betaalt u niet op tijd? Dan heeft u vanaf <ingangsdatum> geen dekking. Ook sturen wij u opnieuw een herinnering. We brengen dan € 10 herinneringskosten bij u in rekening. <als verkeer> Op dat moment laten wij ook aan de Rijksdienst voor Wegverkeer weten dat uw verzekering niet betaald is en er dus geen dekking is. Dat zijn wij wettelijk verplicht. U loopt dan het risico dat u van Justitie een boete krijgt van €400.

Hebt u nog vragen?
Op asr.nl/betalingen vindt u antwoorden op veel gestelde vragen. Hebt u nog andere vragen of opmerkingen over deze brief? Bel ons dan gerust op (030) 278 03 30. Wij zijn bereikbaar van maandag tot en met vrijdag van 8.30 uur tot 17.00 uur. Wij helpen u graag!

Bijlage A
Drie betalingsherinneringen
Met vriendelijke groet,

Robert van der Schaaf
directeur Schadeverzekeringen

Bijlage A
Drie betalingsherinneringen

De aanmaning

M.H.J. van Delst
Mgr Borretstr 43
5375 AB REEK

ASR Betalingscentrum B.V.
Debiteurenbeheer

Archimedeslaan 10
3584 BA Utrecht
Postbus 2072
3500 HB Utrecht
www.asr.nl

Datum	<datum>
Onderwerp	Betalingsherinnering
Behandeld door	Debiteurenbeheer
E-mail	debiteurenbeheer@asr.nl
Telefoon	(030) 278 00 50

Geachte <mevrouw/heer> <naam>,

U hebt een <soort verzekering> met polisnummer <polisnummer> bij ons. Wij hebben de premie voor deze verzekering nog niet van u ontvangen. Dat betekent dat eventuele schade vanaf <ingangsdatum> niet vergoed wordt. In deze brief leest u wat dat betekent en wat u kunt doen. Bij het aanmaken van deze betalingsherinnering zijn we uitgegaan van de betalingen die wij vóór <datum> hebben ontvangen. Hebt u al betaald? Dan hoeft u niets te doen.

Hebt u nog niet betaald?
Omdat u nog steeds niet hebt betaald, berekenen wij nu € 10 herinneringskosten bovenop het openstaande bedrag. Maakt u alstublieft zo snel mogelijk € <bedrag> over op rekeningnummer NL59ABNA0240576861. Betaalt u via internetbankieren? Vergeet dan niet het betalingskenmerk <betalingskenmerk> te vermelden.

Eventuele schade wordt niet vergoed
Zolang u uw premie niet betaalt, hebt u geen dekking voor schade die na <vervaldatum> is ontstaan. Dat betekent dus dat als u na die datum schade hebt, u deze zelf moet betalen. U kunt deze niet alsnog declareren na betaling van uw premie. Zodra wij uw achterstallige premie hebben ontvangen, bent u de dag daarna weer verzekerd.

<als verkeer>Realiseert u zich dat uw voertuig verzekerd moet zijn?
Wij hebben de Rijksdienst voor Wegverkeer laten weten dat uw verzekering niet betaald is en er dus geen dekking is. Dat zijn wij wettelijk verplicht. Realiseert u zich dat in de Wet Aansprakelijkheid Motorrijtuigen staat dat u verplicht bent uw voertuig te verzekeren? Omdat uw voertuig nu niet verzekerd is, loopt u het risico dat u een boete krijgt van €400.

Bijlage A
Drie betalingsherinneringen

Hebt u nog vragen?
Op asr.nl/betalingen vindt u antwoorden op veel gestelde vragen. Hebt u nog andere vragen of opmerkingen over deze brief? Bel ons dan gerust op (030) 278 00 50. Wij zijn bereikbaar van maandag tot en met vrijdag van 8.30 uur tot 17.00 uur. Wij helpen u graag!

Met vriendelijke groet,

Maarten Kerbert
directeur ASR Betalingscentrum B.V.

Bijlage B - Het Onderzoeksmateriaal

De inleidende e-mail

Wat is uw mening over online verzekeren?

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

Een kort onderzoek naar online verzekeren

Beste meneer/mevrouw,

We zijn bij a.s.r. constant bezig om onze dienstverlening te verbeteren. Dit kunnen we niet zonder *uw mening*. We vragen u daarom het volgende:

- Wilt u een kort onderzoek invullen om onze dienstverlening te verbeteren?

Meedoen is heel eenvoudig:

- Het onderzoek duurt slechts **10 minuten**.
- Het onderzoek is **anoniem**.
- Het onderzoek is **eenvoudig**: we vragen alleen om uw mening.
- U kunt het onderzoek direct invullen (klik op de link)

Heeft u vragen over dit onderzoek? Mail mij dan gerust. Alvast bedankt voor uw hulp.

Met vriendelijke groet,

Paul Vaneveld

Afdeling communicatie

paul.vaneveld@asr.nl

Bijlage B
Onderzoeksmateriaal

Scenario voor de condities zonder sociaal contract

U krijgt hierna een e-mail te lezen. Lees eerst het scenario, zodat u zich beter in de e-mail kunt inleven.

Scenario: Stelt u zich voor dat u een autoverzekering heeft bij a.s.r. U bent te laat met het betalen van uw premie. U ziet een e-mail in uw inbox, verzonden door a.s.r. In de e-mail wordt u verzocht om direct te betalen. U heeft nog nooit zo een e-mail van a.s.r. gehad en u vraagt zich daarom af of betalen via deze e-mail veilig is.

U leest eerst de e-mail, waarna u uw mening mag geven over het bericht. U moet straks dus beoordelen wat u van de e-mail vindt: is het veilig, gemakkelijk of slim om online te betalen?

Scenario voor de condities met sociaal contract

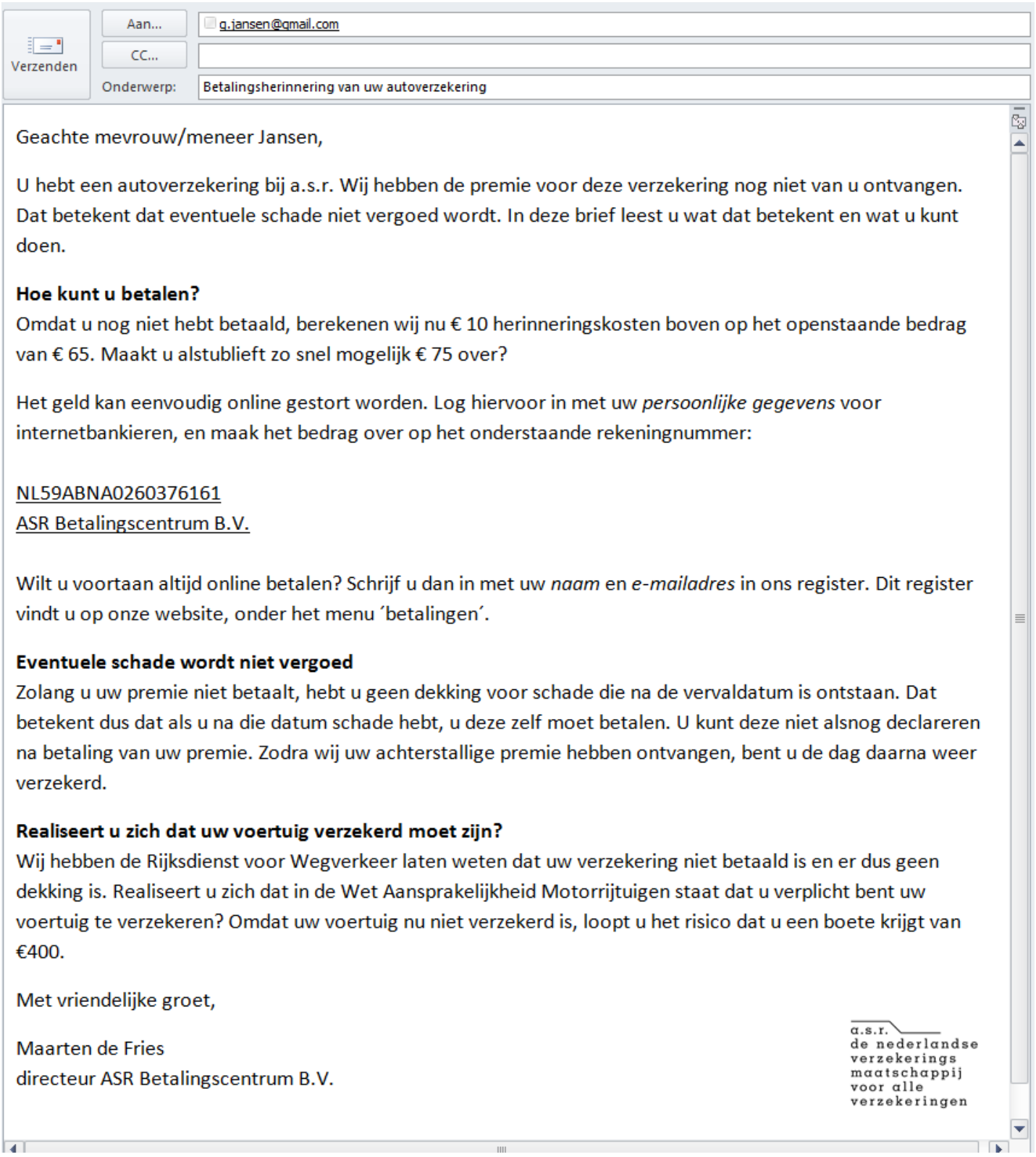
U krijgt hierna een e-mail te lezen. Lees eerst het scenario, zodat u zich beter in de e-mail kunt inleven. Scenario:Stelt u zich voor dat u een autoverzekering heeft bij a.s.r. U ziet een e-mail in uw inbox van a.s.r. In het bericht ziet u een afbeelding van de Tower Bridge in London. Dit is een veiligheidsindicator. a.s.r. vraagt klanten om een persoonlijke foto te uploaden als zij een verzekering afsluiten.

Deze foto komt terug in alle correspondentie, zodat u weet dat e-mails daadwerkelijk afkomstig zijn van a.s.r. U moet zich dus voorstellen dat de Tower Bridge uw persoonlijke afbeelding is, die u in alle correspondentie met a.s.r. hoort te zien. Hieronder staat een voorbeeld van een e-mail met veiligheidsindicator. De komende vragen gaan dus niet over de onderstaande e-mail. In de e-mail die u zo gaat lezen, staat dat u te laat bent met het betalen van uw premie. U heeft nog nooit zo'n e-mail van a.s.r. gehad. U moet daarom nu beoordelen wat u van de e-mail vindt: is het veilig, gemakkelijk of slim om online te betalen? U leest eerst de e-mail, waarna u uw mening mag geven over het bericht.

Bijlage B
Onderzoeksmateriaal

De vier betalingsmails

Zonder link/zonder sociaal contract



Verzenden

Aan... g.jansen@gmail.com

CC...

Onderwerp: Betalingsherinnering van uw autoverzekering

Geachte mevrouw/meneer Jansen,

U hebt een autoverzekering bij a.s.r. Wij hebben de premie voor deze verzekering nog niet van u ontvangen. Dat betekent dat eventuele schade niet vergoed wordt. In deze brief leest u wat dat betekent en wat u kunt doen.

Hoe kunt u betalen?
Omdat u nog niet hebt betaald, berekenen wij nu € 10 herinneringskosten boven op het openstaande bedrag van € 65. Maakt u alstublieft zo snel mogelijk € 75 over?

Het geld kan eenvoudig online gestort worden. Log hiervoor in met uw *persoonlijke gegevens* voor internetbankieren, en maak het bedrag over op het onderstaande rekeningnummer:

NL59ABNA0260376161
ASR Betalingscentrum B.V.

Wilt u voortaan altijd online betalen? Schrijf u dan in met uw *naam* en *e-mailadres* in ons register. Dit register vindt u op onze website, onder het menu ´betalingen´.

Eventuele schade wordt niet vergoed
Zolang u uw premie niet betaalt, hebt u geen dekking voor schade die na de vervaldatum is ontstaan. Dat betekent dus dat als u na die datum schade hebt, u deze zelf moet betalen. U kunt deze niet alsnog declareren na betaling van uw premie. Zodra wij uw achterstallige premie hebben ontvangen, bent u de dag daarna weer verzekerd.

Realiseert u zich dat uw voertuig verzekerd moet zijn?
Wij hebben de Rijksdienst voor Wegverkeer laten weten dat uw verzekering niet betaald is en er dus geen dekking is. Realiseert u zich dat in de Wet Aansprakelijkheid Motorrijtuigen staat dat u verplicht bent uw voertuig te verzekeren? Omdat uw voertuig nu niet verzekerd is, loopt u het risico dat u een boete krijgt van €400.

Met vriendelijke groet,

Maarten de Fries
directeur ASR Betalingscentrum B.V.

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

Bijlage B
Onderzoeksmateriaal

Zonder link/met sociaal contract

Verzenden

Aan... g.jansen@gmail.com

CC...

Onderwerp: Betalingsherinnering van uw autoverzekering

Geachte mevrouw/meneer Jansen,

U hebt een autoverzekering bij a.s.r. Wij hebben de premie voor deze verzekering nog niet van u ontvangen. Dat betekent dat eventuele schade niet vergoed wordt. In deze brief leest u wat dat betekent en wat u kunt doen.

Hoe kunt u betalen?
Omdat u nog niet hebt betaald, berekenen wij nu € 10 herinneringskosten boven op het openstaande bedrag van € 65. Maakt u alstublieft zo snel mogelijk € 75 over?

Het geld kan eenvoudig online gestort worden. Log hiervoor in met uw *persoonlijke gegevens* voor internetbankieren en maak het bedrag over op het onderstaande rekeningnummer:
NL59ABNA0260376161
ASR Betalingscentrum B.V.

Wilt u voortaan altijd online betalen? Schrijf u dan in met uw *naam* en *e-mailadres* in ons register. Dit register vindt u op onze website, onder het menu ´betalingen´.

Eventuele schade wordt niet vergoed
Zolang u uw premie niet betaalt, hebt u geen dekking voor schade die na de vervaldatum is ontstaan. Dat betekent dus dat als u na die datum schade hebt, u deze zelf moet betalen. U kunt deze niet alsnog declareren na betaling van uw premie. Zodra wij uw achterstallige premie hebben ontvangen, bent u de dag daarna weer verzekerd.

Realiseert u zich dat uw voertuig verzekerd moet zijn?
Wij hebben de Rijksdienst voor Wegverkeer laten weten dat uw verzekering niet betaald is en er dus geen dekking is. Realiseert u zich dat in de Wet Aansprakelijkheid Motorrijtuigen staat dat u verplicht bent uw voertuig te verzekeren? Omdat uw voertuig nu niet verzekerd is, loopt u het risico dat u een boete krijgt van €400.

Hoe gaat a.s.r. om met uw persoonsgegevens?

-a.s.r. gaat zorgvuldig om met uw persoonsgegevens. Al onze e-mails hebben daarom een privacy-waarborg.

-Uw persoonlijke informatie wordt niet gedeeld met derden en alleen gebruikt binnen a.s.r.

-Als u niet uw persoonsgegevens wilt delen, kunt u ook per acceptgiro betalen. Kijk voor meer informatie op onze site, onder het menu 'betalingen'.

-U kunt altijd controleren of e-mails daadwerkelijk afkomstig zijn van a.s.r., door de persoonlijke veiligheidsindicator.

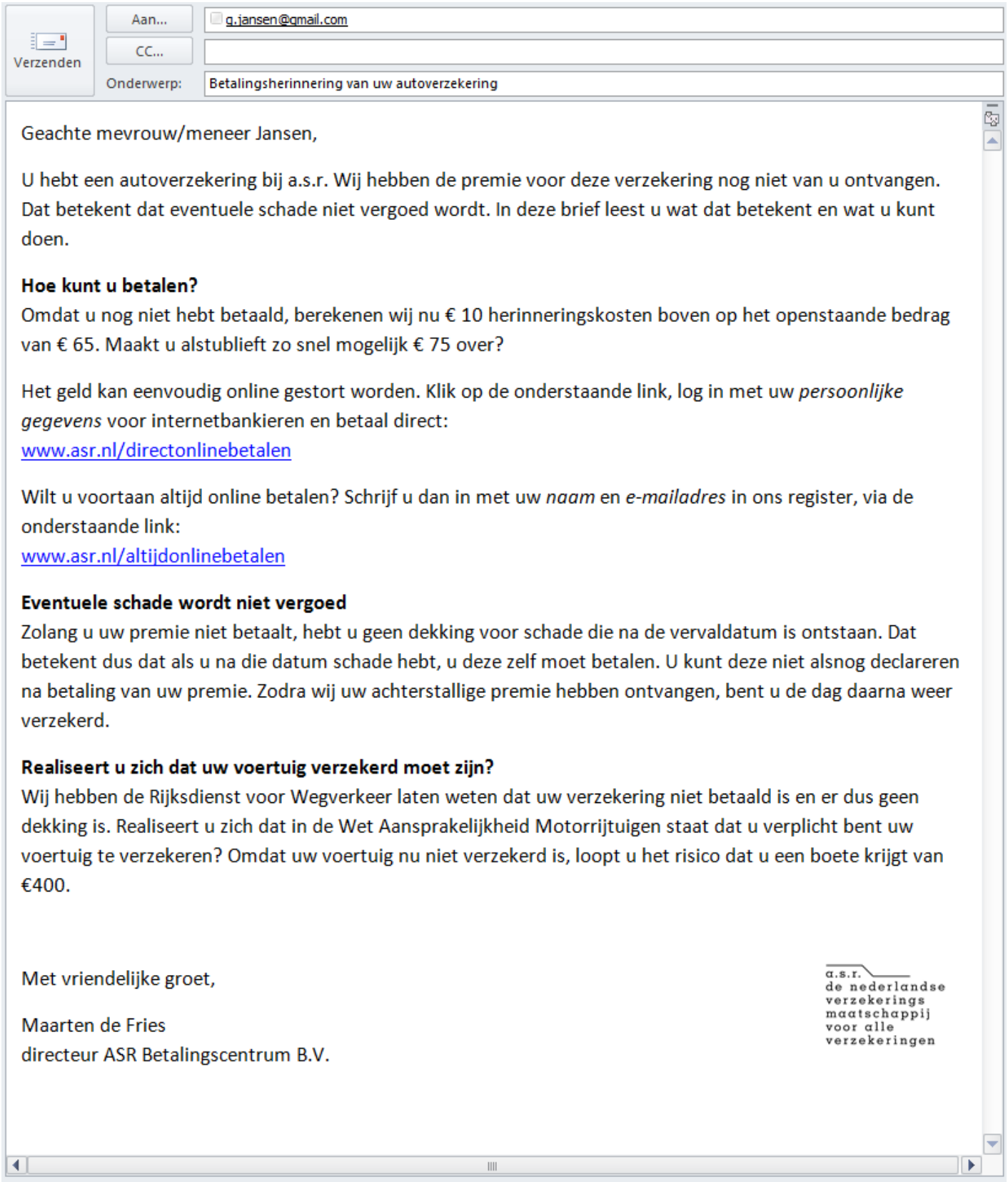
Met vriendelijke groet,

Maarten de Fries
directeur ASR Betalingscentrum B.V.

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

Bijlage B
Onderzoeksmateriaal

Met link/zonder sociaal contract



Verzenden

Aan... g.jansen@gmail.com

CC...

Onderwerp: Betalingsherinnering van uw autoverzekering

Geachte mevrouw/meneer Jansen,

U hebt een autoverzekering bij a.s.r. Wij hebben de premie voor deze verzekering nog niet van u ontvangen. Dat betekent dat eventuele schade niet vergoed wordt. In deze brief leest u wat dat betekent en wat u kunt doen.

Hoe kunt u betalen?
Omdat u nog niet hebt betaald, berekenen wij nu € 10 herinneringskosten boven op het openstaande bedrag van € 65. Maakt u alstublieft zo snel mogelijk € 75 over?

Het geld kan eenvoudig online gestort worden. Klik op de onderstaande link, log in met uw *persoonlijke gegevens* voor internetbankieren en betaal direct:
www.asr.nl/directonlinebetalen

Wilt u voortaan altijd online betalen? Schrijf u dan in met uw *naam* en *e-mailadres* in ons register, via de onderstaande link:
www.asr.nl/altijdonlinebetalen

Eventuele schade wordt niet vergoed
Zolang u uw premie niet betaalt, hebt u geen dekking voor schade die na de vervaldatum is ontstaan. Dat betekent dus dat als u na die datum schade hebt, u deze zelf moet betalen. U kunt deze niet alsnog declareren na betaling van uw premie. Zodra wij uw achterstallige premie hebben ontvangen, bent u de dag daarna weer verzekerd.

Realiseert u zich dat uw voertuig verzekerd moet zijn?
Wij hebben de Rijksdienst voor Wegverkeer laten weten dat uw verzekering niet betaald is en er dus geen dekking is. Realiseert u zich dat in de Wet Aansprakelijkheid Motorrijtuigen staat dat u verplicht bent uw voertuig te verzekeren? Omdat uw voertuig nu niet verzekerd is, loopt u het risico dat u een boete krijgt van €400.

Met vriendelijke groet,

Maarten de Fries
directeur ASR Betalingscentrum B.V.

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

Bijlage B
Onderzoeksmateriaal

Met link/met sociaal contract

Verzenden | Aan... g.jansen@gmail.com | CC... | Onderwerp: Betalingsherinnering van uw autoverzekering

Geachte mevrouw/meneer Jansen,

U hebt een autoverzekering bij a.s.r. Wij hebben de premie voor deze verzekering nog niet van u ontvangen. Dat betekent dat eventuele schade niet vergoed wordt. In deze brief leest u wat dat betekent en wat u kunt doen.

Hoe kunt u betalen?
Omdat u nog niet hebt betaald, berekenen wij nu € 10 herinneringskosten boven op het openstaande bedrag van € 65. Maakt u alstublieft zo snel mogelijk € 75 over?

Het geld kan eenvoudig online gestort worden. Klik op de onderstaande link, log in met uw *persoonlijke gegevens* voor internetbankieren en betaal direct:
www.asr.nl/directonlinebetalen

Wilt u voortaan altijd online betalen? Schrijf u dan in met uw *naam* en *e-mailadres* in ons register, via de onderstaande link:
www.asr.nl/altijdonlinebetalen

Eventuele schade wordt niet vergoed
Zolang u uw premie niet betaalt, hebt u geen dekking voor schade die na de vervaldatum is ontstaan. Dat betekent dus dat als u na die datum schade hebt, u deze zelf moet betalen. U kunt deze niet alsnog declareren na betaling van uw premie. Zodra wij uw achterstallige premie hebben ontvangen, bent u de dag daarna weer verzekerd.

Realiseert u zich dat uw voertuig verzekerd moet zijn?
Wij hebben de Rijksdienst voor Wegverkeer laten weten dat uw verzekering niet betaald is en er dus geen dekking is. Realiseert u zich dat in de Wet Aansprakelijkheid Motorrijtuigen staat dat u verplicht bent uw voertuig te verzekeren? Omdat uw voertuig nu niet verzekerd is, loopt u het risico dat u een boete krijgt van €400.

Hoe gaat a.s.r. om met uw persoonsgegevens?

-a.s.r. gaat zorgvuldig om met uw persoonsgegevens. Al onze e-mails hebben daarom een privacy-waarborg.

-Uw persoonlijke informatie wordt niet gedeeld met derden en alleen gebruikt binnen a.s.r.

-Als u niet uw persoonsgegevens wilt delen, kunt u ook per acceptgiro betalen. Kijk voor meer informatie op onze site, onder het menu 'betalingen'.

-U kunt altijd controleren of e-mails daadwerkelijk afkomstig zijn van a.s.r., door de persoonlijke veiligheidsindicator.

Met vriendelijke groet,

Maarten de Fries
directeur ASR Betalingscentrum B.V.

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

Bijlage C - De Vragenlijst

1	**Wat is uw geslacht?**	*Single-responsevraag*

- ○ Man
- ○ Vrouw

2	**Wat is uw leeftijd?**	*Open vraag (klein)*

☐ Vp

3	**Wat is uw hoogst afgeronde opleiding?**	*Single-responsevraag*

- ○ Basisschool of lagere school
- ○ LBO, LTS of Huishoudschool
- ○ MBO niveau 1
- ○ MBO niveau 2
- ○ MAVO of VMBO-T
- ○ MBO niveau 3
- ○ MBO niveau 4
- ○ MULO
- ○ HBS
- ○ HAVO
- ○ VWO
- ○ HBO
- ○ Universiteit Bachelor
- ○ Universiteit Master of Doctoraal

8	**U krijgt hierna een e-mail te lezen. Lees eerst het scenario, zodat u zich beter in de e-mail kunt inleven. Scenario:Stelt u zich voor dat u een autoverzekering heeft bij a.s.r. U ziet een e-mail in uw inbox van a.s.r. In het bericht ziet u een afbeelding van de Tower Bridge in London. Dit is een veiligheidsindicator. a.s.r. vraagt klanten om een persoonlijke foto te uploaden als zij een verzekering afsluiten.** Deze foto komt terug in alle correspondentie, zodat u weet dat e-mails daadwerkelijk afkomstig zijn van a.s.r. U moet zich dus voorstellen dat de Tower Bridge uw persoonlijke afbeelding is, die u in alle correspondentie met a.s.r. hoort te zien. Hieronder staat een voorbeeld van een e-mail met veiligheidsindicator. De komende vragen gaan dus niet over de onderstaande e-mail. In de e-mail die u zo gaat lezen, staat dat u te laat bent met	*Tussenpagina*

het betalen van uw premie. U heeft nog nooit zo'n e-mail van a.s.r. gehad. U moet daarom nu beoordelen wat u van de e-mail vindt: is het veilig, gemakkelijk of slim om online te betalen? U leest eerst de e-mail, waarna u uw mening mag geven over het bericht.

VRAAG 8 ALLEEN TONEN ALS AAN DE ONDERSTAANDE VOORWAARDEN WORDT VOLDAAN, INDIEN NIET VOLDAAN SPRING NAAR: **>> VOLGENDE VRAAG**

Minstens één van onderstaande voorwaarden is waar:
- of de onderzoeksvariabele hotspot is 1
- of de onderzoeksvariabele hotspot is 3

☐

9 **U krijgt hierna een e-mail te lezen. Lees eerst het scenario, zodat u zich beter in de e-mail kunt inleven. Scenario:Stelt u zich voor dat u een autoverzekering heeft bij a.s.r. U bent te laat met het betalen van uw premie. U ziet een e-mail in uw inbox, verzonden door a.s.r. In de e-mail wordt u verzocht om direct te betalen. U heeft nog nooit zo een e-mail van a.s.r. gehad en u vraagt zich daarom af of betalen via deze e-mail veilig is.**

Tussenpagina

U leest eerst de e-mail, waarna u uw mening mag geven over het bericht. U moet straks dus beoordelen wat u van de e-mail vindt: is het veilig, gemakkelijk of slim om online te betalen?

VRAAG 9 ALLEEN TONEN ALS AAN DE ONDERSTAANDE VOORWAARDEN WORDT VOLDAAN, INDIEN NIET VOLDAAN SPRING NAAR: **>> VOLGENDE VRAAG**

Minstens één van onderstaande voorwaarden is waar:

- of de onderzoeksvariabele hotspot is 2
- of de onderzoeksvariabele hotspot is 4

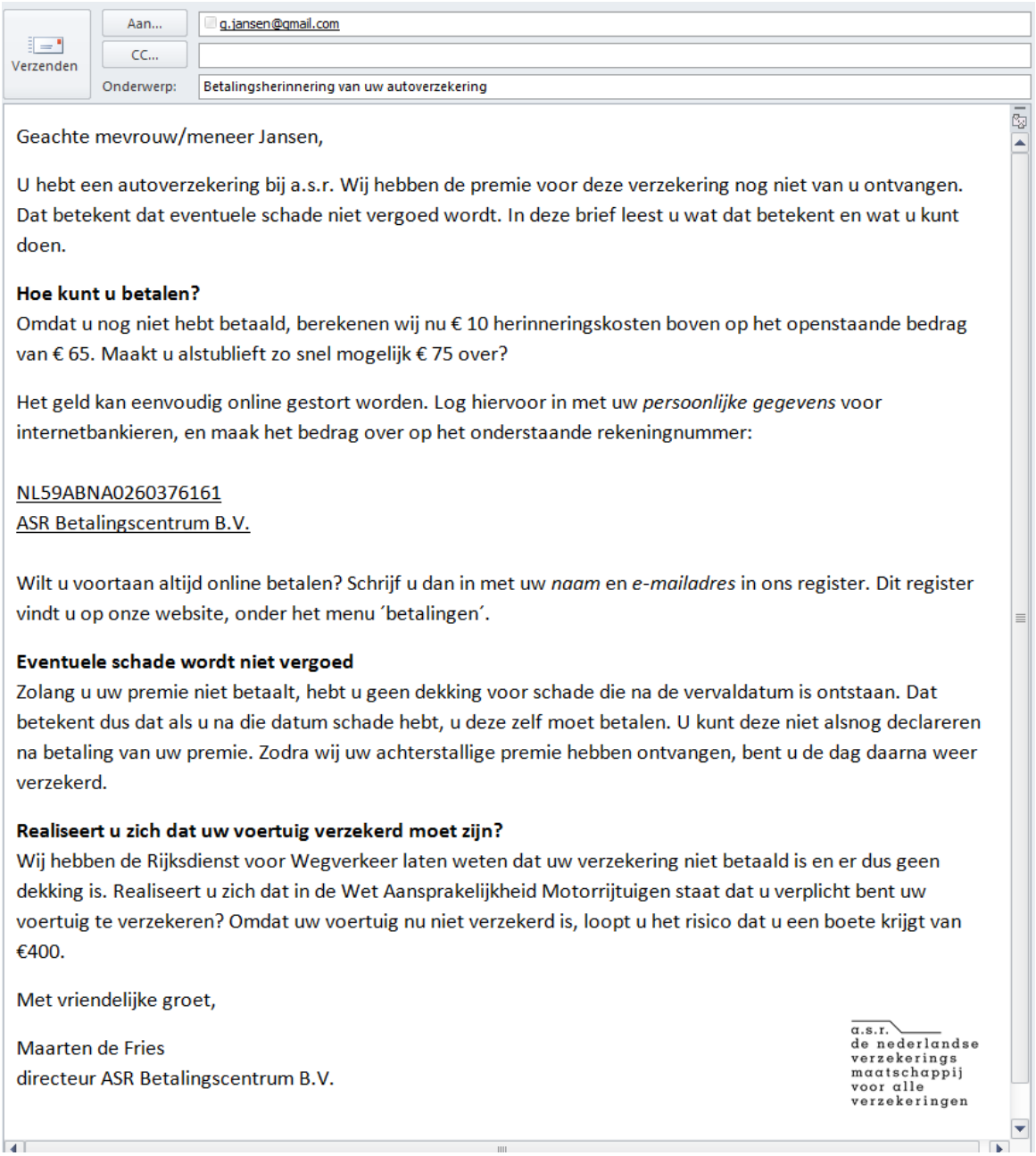
☐

10	**De komende vragen gaan over de onderstaande e-mail. Lees het bericht dan ook aandachtig en volledig door. Als u met uw muis over de afbeelding navigeert, licht elk tekstdeel groen op. U kunt aangeven welk tekstdeel u het beste vindt door erop te klikken. Daarna kunt u doorgaan met de volgende vragen.**	*Afbeeldingvraag (single response)*

VRAAG 10 ALLEEN TONEN ALS AAN DE ONDERSTAANDE VOORWAARDEN WORDT VOLDAAN, INDIEN NIET VOLDAAN SPRING NAAR: **>> VOLGENDE VRAAG**

De onderzoeksvariabele hotspot is 4

Bijlage C
De vragenlijst



Verzenden
Aan... g.jansen@gmail.com
CC...
Onderwerp: Betalingsherinnering van uw autoverzekering

Geachte mevrouw/meneer Jansen,

U hebt een autoverzekering bij a.s.r. Wij hebben de premie voor deze verzekering nog niet van u ontvangen. Dat betekent dat eventuele schade niet vergoed wordt. In deze brief leest u wat dat betekent en wat u kunt doen.

Hoe kunt u betalen?
Omdat u nog niet hebt betaald, berekenen wij nu € 10 herinneringskosten boven op het openstaande bedrag van € 65. Maakt u alstublieft zo snel mogelijk € 75 over?

Het geld kan eenvoudig online gestort worden. Log hiervoor in met uw *persoonlijke gegevens* voor internetbankieren, en maak het bedrag over op het onderstaande rekeningnummer:

NL59ABNA0260376161
ASR Betalingscentrum B.V.

Wilt u voortaan altijd online betalen? Schrijf u dan in met uw *naam* en *e-mailadres* in ons register. Dit register vindt u op onze website, onder het menu ´betalingen´.

Eventuele schade wordt niet vergoed
Zolang u uw premie niet betaalt, hebt u geen dekking voor schade die na de vervaldatum is ontstaan. Dat betekent dus dat als u na die datum schade hebt, u deze zelf moet betalen. U kunt deze niet alsnog declareren na betaling van uw premie. Zodra wij uw achterstallige premie hebben ontvangen, bent u de dag daarna weer verzekerd.

Realiseert u zich dat uw voertuig verzekerd moet zijn?
Wij hebben de Rijksdienst voor Wegverkeer laten weten dat uw verzekering niet betaald is en er dus geen dekking is. Realiseert u zich dat in de Wet Aansprakelijkheid Motorrijtuigen staat dat u verplicht bent uw voertuig te verzekeren? Omdat uw voertuig nu niet verzekerd is, loopt u het risico dat u een boete krijgt van €400.

Met vriendelijke groet,

Maarten de Fries
directeur ASR Betalingscentrum B.V.

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

- ☐ Hoe kunt u betalen
- ☐ Eventuele schade niet vergoed
- ☐ Realiseert u zich dat u verzekerd moet zijn

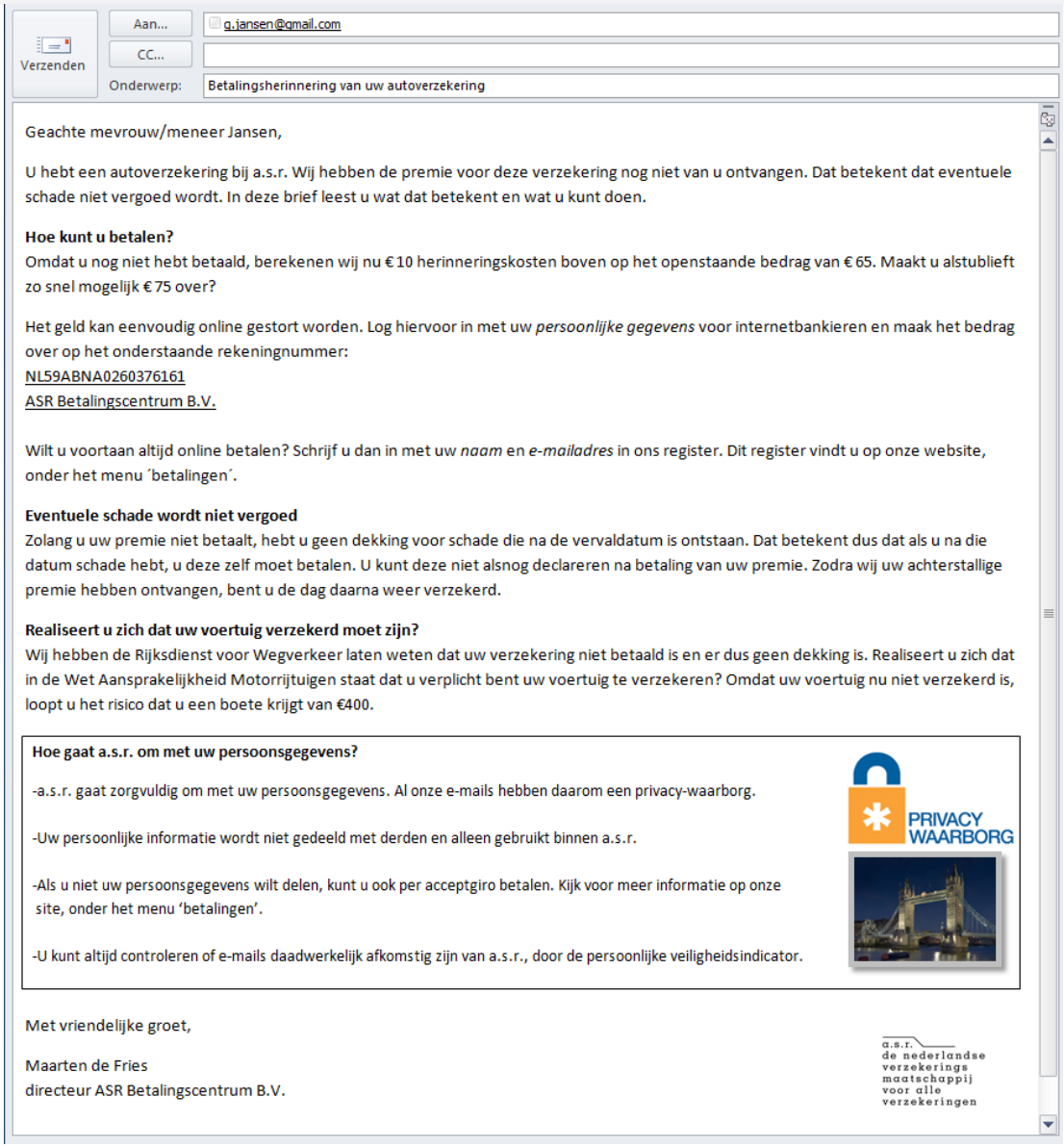
11	**De komende vragen gaan over de onderstaande e-mail. Lees het bericht dan ook aandachtig en volledig door. Als u met uw muis over de afbeelding navigeert, licht elk tekstdeel groen op. U kunt aangeven welk tekstdeel u het beste vindt door erop te klikken. Daarna kunt u doorgaan met de volgende vragen.**	*Afbeeldingvraag (single response)*

VRAAG 11 ALLEEN TONEN ALS AAN DE ONDERSTAANDE VOORWAARDEN WORDT VOLDAAN, INDIEN

Bijlage C
De vragenlijst

NIET VOLDAAN SPRING NAAR: **>> VOLGENDE VRAAG**

De onderzoeksvariabele hotspot is 3



Verzenden | Aan... g.jansen@gmail.com | CC... | Onderwerp: Betalingsherinnering van uw autoverzekering

Geachte mevrouw/meneer Jansen,

U hebt een autoverzekering bij a.s.r. Wij hebben de premie voor deze verzekering nog niet van u ontvangen. Dat betekent dat eventuele schade niet vergoed wordt. In deze brief leest u wat dat betekent en wat u kunt doen.

Hoe kunt u betalen?
Omdat u nog niet hebt betaald, berekenen wij nu € 10 herinneringskosten boven op het openstaande bedrag van € 65. Maakt u alstublieft zo snel mogelijk € 75 over?

Het geld kan eenvoudig online gestort worden. Log hiervoor in met uw *persoonlijke gegevens* voor internetbankieren en maak het bedrag over op het onderstaande rekeningnummer:
NL59ABNA0260376161
ASR Betalingscentrum B.V.

Wilt u voortaan altijd online betalen? Schrijf u dan in met uw *naam* en *e-mailadres* in ons register. Dit register vindt u op onze website, onder het menu ´betalingen´.

Eventuele schade wordt niet vergoed
Zolang u uw premie niet betaalt, hebt u geen dekking voor schade die na de vervaldatum is ontstaan. Dat betekent dus dat als u na die datum schade hebt, u deze zelf moet betalen. U kunt deze niet alsnog declareren na betaling van uw premie. Zodra wij uw achterstallige premie hebben ontvangen, bent u de dag daarna weer verzekerd.

Realiseert u zich dat uw voertuig verzekerd moet zijn?
Wij hebben de Rijksdienst voor Wegverkeer laten weten dat uw verzekering niet betaald is en er dus geen dekking is. Realiseert u zich dat in de Wet Aansprakelijkheid Motorrijtuigen staat dat u verplicht bent uw voertuig te verzekeren? Omdat uw voertuig nu niet verzekerd is, loopt u het risico dat u een boete krijgt van €400.

Hoe gaat a.s.r. om met uw persoonsgegevens?

-a.s.r. gaat zorgvuldig om met uw persoonsgegevens. Al onze e-mails hebben daarom een privacy-waarborg.

-Uw persoonlijke informatie wordt niet gedeeld met derden en alleen gebruikt binnen a.s.r.

-Als u niet uw persoonsgegevens wilt delen, kunt u ook per acceptgiro betalen. Kijk voor meer informatie op onze site, onder het menu 'betalingen'.

-U kunt altijd controleren of e-mails daadwerkelijk afkomstig zijn van a.s.r., door de persoonlijke veiligheidsindicator.

PRIVACY WAARBORG

Met vriendelijke groet,

Maarten de Fries
directeur ASR Betalingscentrum B.V.

a.s.r. de nederlandse verzekerings maatschappij voor alle verzekeringen

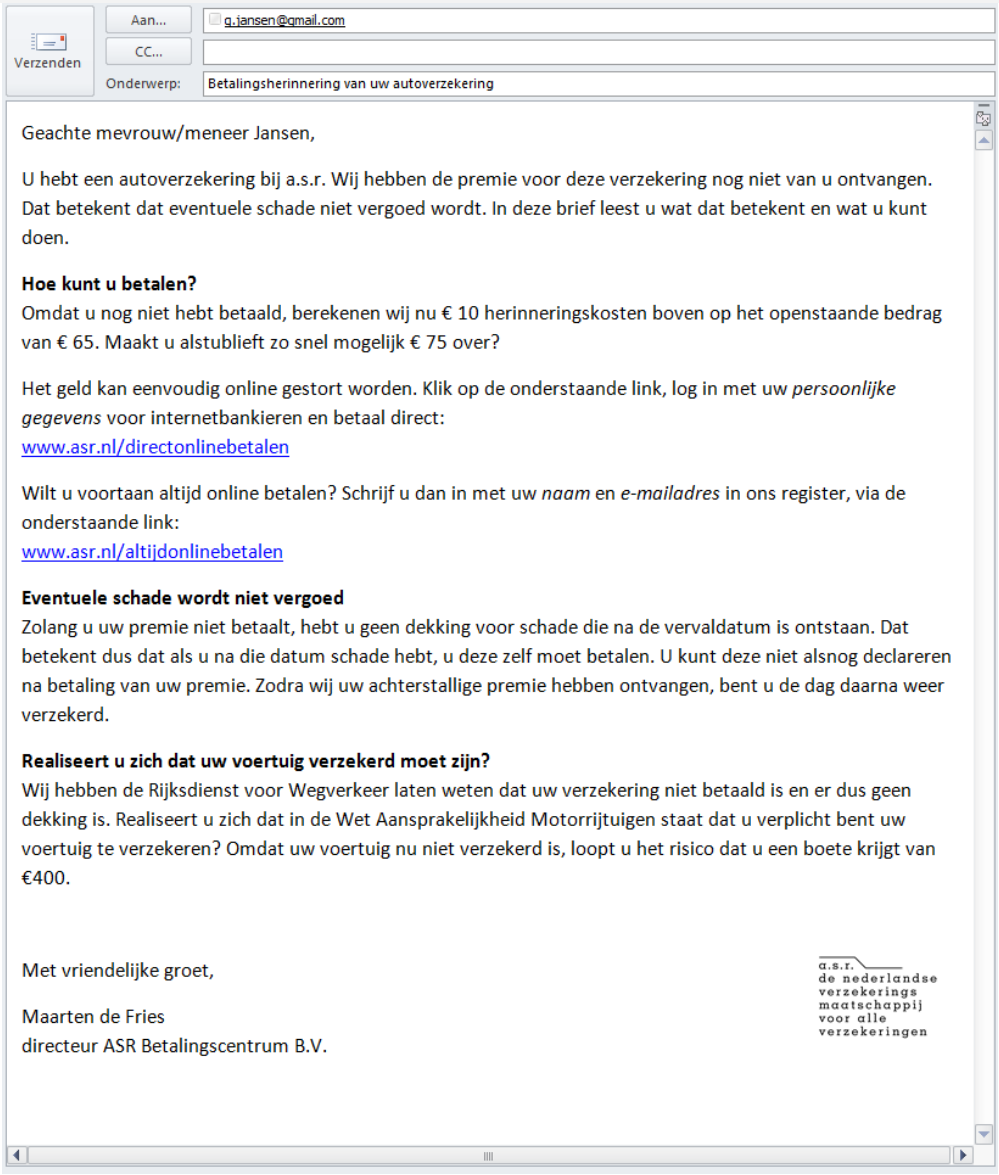
- ☐ Hoe kunt u betalen
- ☐ Eventuele schade niet vergoed
- ☐ Realiseert u zich dat u verzekerd moet zijn
- ☐ Keurmerk

12 **De komende vragen gaan over de onderstaande e-mail. Lees het bericht dan ook aandachtig en volledig door. Als u met uw muis over de afbeelding navigeert, licht elk tekstdeel groen op. U kunt aangeven welk tekstdeel u het beste vindt door erop te klikken. Daarna kunt u doorgaan met de volgende vragen.** *Afbeeldingvraag (single response)*

Bijlage C
De vragenlijst

VRAAG 12 ALLEEN TONEN ALS AAN DE ONDERSTAANDE VOORWAARDEN WORDT VOLDAAN, INDIEN NIET VOLDAAN SPRING NAAR: **>> VOLGENDE VRAAG**

De onderzoeksvariabele hotspot is 2



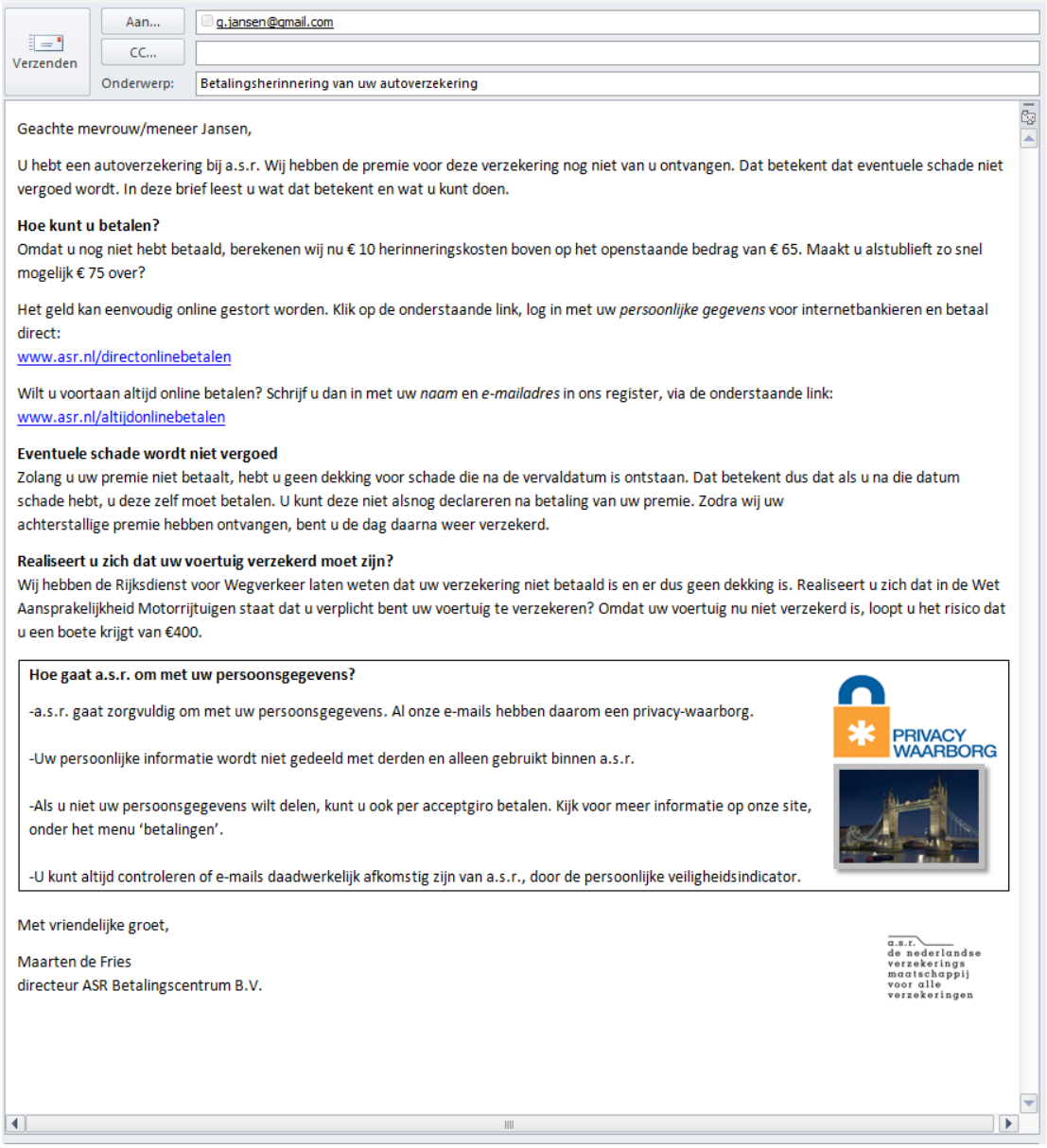
- ☐ Hoe kunt u betalen
- ☐ Eventuele schade niet vergoed
- ☐ Realiseert u zich dat u verzekerd moet zijn

13	**De komende vragen gaan over de onderstaande e-mail. Lees het bericht dan ook aandachtig en volledig door. Als u met uw muis over de afbeelding navigeert, licht elk tekstdeel groen op. U kunt aangeven welk tekstdeel u het beste vindt door erop te klikken. Daarna kunt u doorgaan met de volgende vragen.**	*Afbeeldingvraag (single response)*

Bijlage C
De vragenlijst

VRAAG 13 ALLEEN TONEN ALS AAN DE ONDERSTAANDE VOORWAARDEN WORDT VOLDAAN, INDIEN NIET VOLDAAN SPRING NAAR: **>> VOLGENDE VRAAG**

De onderzoeksvariabele hotspot is 1



Verzenden
Aan... g.jansen@gmail.com
CC...
Onderwerp: Betalingsherinnering van uw autoverzekering

Geachte mevrouw/meneer Jansen,

U hebt een autoverzekering bij a.s.r. Wij hebben de premie voor deze verzekering nog niet van u ontvangen. Dat betekent dat eventuele schade niet vergoed wordt. In deze brief leest u wat dat betekent en wat u kunt doen.

Hoe kunt u betalen?
Omdat u nog niet hebt betaald, berekenen wij nu € 10 herinneringskosten boven op het openstaande bedrag van € 65. Maakt u alstublieft zo snel mogelijk € 75 over?

Het geld kan eenvoudig online gestort worden. Klik op de onderstaande link, log in met uw *persoonlijke gegevens* voor internetbankieren en betaal direct:
www.asr.nl/directonlinebetalen

Wilt u voortaan altijd online betalen? Schrijf u dan in met uw *naam* en *e-mailadres* in ons register, via de onderstaande link:
www.asr.nl/altijdonlinebetalen

Eventuele schade wordt niet vergoed
Zolang u uw premie niet betaalt, hebt u geen dekking voor schade die na de vervaldatum is ontstaan. Dat betekent dus dat als u na die datum schade hebt, u deze zelf moet betalen. U kunt deze niet alsnog declareren na betaling van uw premie. Zodra wij uw achterstallige premie hebben ontvangen, bent u de dag daarna weer verzekerd.

Realiseert u zich dat uw voertuig verzekerd moet zijn?
Wij hebben de Rijksdienst voor Wegverkeer laten weten dat uw verzekering niet betaald is en er dus geen dekking is. Realiseert u zich dat in de Wet Aansprakelijkheid Motorrijtuigen staat dat u verplicht bent uw voertuig te verzekeren? Omdat uw voertuig nu niet verzekerd is, loopt u het risico dat u een boete krijgt van €400.

Hoe gaat a.s.r. om met uw persoonsgegevens?

-a.s.r. gaat zorgvuldig om met uw persoonsgegevens. Al onze e-mails hebben daarom een privacy-waarborg.

-Uw persoonlijke informatie wordt niet gedeeld met derden en alleen gebruikt binnen a.s.r.

-Als u niet uw persoonsgegevens wilt delen, kunt u ook per acceptgiro betalen. Kijk voor meer informatie op onze site, onder het menu 'betalingen'.

-U kunt altijd controleren of e-mails daadwerkelijk afkomstig zijn van a.s.r., door de persoonlijke veiligheidsindicator.

PRIVACY WAARBORG

Met vriendelijke groet,

Maarten de Fries
directeur ASR Betalingscentrum B.V.

a.s.r. de nederlandse verzekerings maatschappij voor alle verzekeringen

- ☐ Hoe kunt u betalen
- ☐ Eventuele schade niet vergoed
- ☐ Realiseert u zich dat u verzekerd moet zijn
- ☐ Keurmerk

14 **De volgende vragen gaan over de e-mail die u zojuist heeft gelezen. Het is belangrijk dat u zich inleeft in het scenario. Stelt u zich dus voor dat u zelf een autoverzekering heeft bij a.s.r. en deze e-mail ontvangt. Hoe beantwoordt u dan de volgende vragen?** *Tussenpagina*

Bijlage C
De vragenlijst

☐

15	**Ik kan mijn achterstallige premie op verschillende manieren betalen**	*Semantische differentiaal*

☐ helemaal mee oneens
☐
☐
☐
☐
☐
☐ helemaal mee eens

16	**Ik zou door deze e-mail mijn achterstallige premie direct betalen**	*Semantische differentiaal*

☐ zeer onwaarschijnlijk
☐
☐
☐
☐
☐
☐ zeer waarschijnlijk

17	**Ik geloof dat deze e-mail daadwerkelijk afkomstig is van a.s.r.**	*Semantische differentiaal*

☐ helemaal mee oneens
☐
☐
☐
☐
☐
☐ helemaal mee eens

18	**a.s.r. vindt winst maken belangrijker dan klanten goed helpen**	*Semantische differentiaal*

☐ helemaal mee oneens
☐
☐
☐
☐
☐
☐ helemaal mee eens

Bijlage C
De vragenlijst

19	Ik twijfel door deze mail of ik mijn achterstallige premie online zou willen betalen	*Semantische differentiaal*

- ☐ zeer onwaarschijnlijk
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ zeer waarschijnlijk

20	Ik weet wie er toegang heeft tot mijn persoonsgegevens (zoals uw naam of e-mailadres) als ik de achterstallige premie betaal	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

21	Ik vind het raar om te betalen naar aanleiding van deze e-mail	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

22	Ik verwacht dat a.s.r. afspraken nakomt	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

Bijlage C
De vragenlijst

23	**Door deze e-mail vind ik het veilig om mijn persoonsgegevens online in te vullen**	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

24	**Ik vind dat ik een aantal overbodige stappen moet doorlopen bij het betalen van de premie**	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

25	**Als ik betaal via deze e-mail en/of me inschrijf in het register, bepaal ik zelf wat er gebeurt met mijn persoonsgegevens**	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

26	**Ik geloof dat a.s.r. onoprecht is**	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

Bijlage C
De vragenlijst

27	Door deze e-mail weet ik waarom a.s.r. mijn persoonsgegevens nodig heeft	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

28	Ik zou in de toekomst altijd op deze manier willen betalen	*Semantische differentiaal*

- ☐ zeer onwaarschijnlijk
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ zeer waarschijnlijk

29	Deze e-mail maakt niet duidelijk hoe mijn persoonsgegevens gebruikt zullen worden	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

30	Door deze e-mail geloof ik dat a.s.r. goed is in verzekeren	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

31	Door deze e-mail zou ik mijn bankgegevens online invullen	*Semantische differentiaal*

- ☐ zeer onwaarschijnlijk
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ zeer waarschijnlijk

32	**Door deze e-mail geloof ik dat a.s.r. het beste met mij voor heeft**	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

33	**Door deze e-mail loop ik het risico dat mijn persoonsgegevens misbruikt worden**	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

34	**Ik heb genoeg zelfvertrouwen om online te betalen via deze e-mail**	*Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

35	**Ik vertrouw a.s.r.**	*Semantische differentiaal*

Bijlage C
De vragenlijst

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

36 **Via internetbankieren betalen na ontvangst van deze e-mail is veilig** *Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

37 **Betalen via deze e-mail is eenvoudig** *Semantische differentiaal*

- ☐ helemaal mee oneens
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐ helemaal mee eens

38 **Deze laatst vragen gaan over uw eigen digitale voorkeuren en kennis. Er zijn geen foute of goede antwoorden.** *Tussenpagina*

- ☐

39 **Hoe bekend bent u met de volgende termen?**
Een term is bekend als u de betekenis aan een ander zou kunnen uitleggen *Tabelvraag (single response)*

Willekeurige volgorde subvragen

	Volledig onbekend	Wel eens gehoord	Een beetje bekend	Redelijk bekend	Volledig bekend	
MP3	○	○	○	○	○	
JPG	○	○	○	○	○	
SPAM	○	○	○	○	○	

Bijlage C
De vragenlijst

Malware	○	○	○	○	○	
Cookie	○	○	○	○	○	
Identiteitsdiefstal	○	○	○	○	○	
Scam	○	○	○	○	○	

40 Hoe bekend bent u met de term phishing *Single-responsevraag*

- ○ Ik ken de term phishing niet
- ○ Ik heb de term phishing weleens gehoord
- ○ Ik weet ongeveer wat phishing is
- ○ Ik weet precies wat phishing is

41 Heeft uzelf, of iemand in uw omgeving, wel eens met phishing te maken gehad? *Single-responsevraag*

- ○ Ja
- ○ Nee
- ○ Weet ik niet

42 Hoe belangrijk vindt u de volgende eigenschappen bij online aankopen/betalingen? *Tabelvraag (single response)*

	Totaal niet belangrijk	Onbelangrijk	Enigszins belangrijk	Neutraal	Redelijk belangrijk	Belangrijk	Erg belangrijk	
Zelf bepalen door wie, hoe en wanneer mijn persoonsgegevens worden gebruikt	○	○	○	○	○	○	○	
Een privacykeurmerk	○	○	○	○	○	○	○	
Inzicht in het gebruik van mijn persoonsgegevens	○	○	○	○	○	○	○	
Veiligheidsmaatregelen tegen misbruik van persoonsgegevens	○	○	○	○	○	○	○	
Een veiligheidskeurmerk (zoals het beveiligde verbinding-slot in een browser)	○	○	○	○	○	○	○	

Bijlage C
De vragenlijst

43	**Geef aan in hoeverre u het eens bent met de volgende stellingen**	*Tabelvraag (single response)*

	helemaal mee oneens	mee oneens	een beetje mee oneens	niet mee oneens/eens	een beetje mee eens	mee eens	helemaal mee eens	
Ik check mijn e-mail vaker dan mijn papieren post	○	○	○	○	○	○	○	
Ik raak brieven vaker kwijt dan e-mails	○	○	○	○	○	○	○	
Ik vergeet e-mails vaker dan brieven	○	○	○	○	○	○	○	

Bijlage D – Vragenclusters en opschoning van de data

Vragenclusters en bijbehorende vragen

Tabel 1: Clusters en bijbehorende vragen

Construct	Vragen
Gedragsintentie	• Ik zou door deze e-mail mijn achterstallige premie direct betalen • Ik zou twijfelen om mijn achterstallige premie via deze e-mail online te betalen* • Ik zou in de toekomst altijd op deze manier betalen • Ik zou mijn bankgegevens online invullen via deze e-mail
privacy	• Ik kan mijn achterstallig premie op verschillende manieren betalen • Ik weet wie toegang heeft tot mijn persoonsgegevens als ik mijn achterstallige premie betaal via deze e-mail • Als ik betaal via deze e-mail en/of me inschrijf in het register, bepaal ik zelf door wie, wanneer en hoe mijn persoonsgegevens worden gebruikt • Deze e-mail maakt mij niet duidelijk hoe mijn persoonsgegevens gebruikt zullen worden* • Door deze e-mail weet ik waarom a.s.r. mijn persoonsgegevens nodig heeft
Veiligheid	• Ik geloof dat deze e-mail daadwerkelijk afkomstig is van a.s.r. • Door deze e-mail loop ik het risico dat mijn persoonsgegevens misbruikt worden* • Via internetbankieren betalen na ontvangst van deze e-mail is veilig • Ik vind het veilig om mijn persoonsgegevens in te vullen via deze e/mail
Vertrouwen (Gefen), trust scale (bron)	• Door deze e-mail vertrouw ik a.s.r. • Op basis van deze e-mail verwacht ik dat a.s.r. afspraken nakomt (integriteit) • Door deze e-mail geloof ik dat a.s.r. onoprecht is (integriteit) • Door deze e-mail geloof ik dat a.s.r. het beste mij voor heeft (welwillendheid) • A.s.r. vindt winst maken belangrijker dan klanten goed helpen (welwillendheid)* • Door deze e-mail geloof ik dat a.s.r. goed is in verzekeren (competentie)
Gebruikersgemak (verantwoording Cheng, 2015), Singleton (bron)	• Betalen via deze e-mail is eenvoudig • Ik vind het raar om op deze manier te betalen* • Ik vind bepaalde stappen bij het betalen overbodig* • Ik heb genoeg zelfvertrouwen om online te betalen via deze e-mail
Digitale geletterdheid (verantwoording	• Ik ben bekend/onbekend met de volgende termen: MP3, JPG, Spam, malware, cookie, identiteitsdiefstal, scam

Hoffman), digital litercy (bron)	
Bekendheid met phishing	• Ik weet wat precies wat phishing is • Ik heb zelf wel eens te maken gehad met phishing • Iemand in mijn omgeving heeft wel eens te maken gehad met phishing
Belang van privacy en veiligheid	Geef aan hoe belangrijk u de volgende eigenschappen vindt bij online zakendoen: • Volledige controle over mijn persoonsgegevens • Een privacykeurmerk • Inzicht in het gebruik van mijn persoonsgegevens • Veiligheidsmaatregelen tegen misbruik van persoonsgegevens • Een veiligheidskeurmerk
Demografie	• Leeftijd, geslacht, opleiding etc.

*deze vragen zijn omgepoold voor de statistische analyses

Opschoning data

Alvorens ik de data analyseerde, schoonde ik het databestand op. Hiertoe ondernam ik de volgende stappen, in chronologische volgorde.

1. Ik verwijderde één proefpersoon die één of meerdere vragen niet hadden ingevuld.

2. Ik verwijderde proefpersonen die relatief veel of weinig tijd besteedden aan het onderzoek. De ondergrens was hierbij drie minuten, de bovengrens een twintig minuten. Het minimum en maximum bepaalde ik aan de hand van mijn eigen ervaring. Ik kon het onderzoek niet binnen drie minuten afmaken, terwijl ik de vragen ken. Het is dus onwaarschijnlijk dat proefpersonen het onderzoek sneller en even geconcentreerd kunnen maken. Als proefpersonen meer dan twintig minuten deden over de vragenlijst, voltooiden zij de vragenlijst waarschijnlijk niet in één keer. Het is mogelijk om met het onderzoek te stoppen en na een pauze weer verder te werken. Omdat een pauze misschien afdoet aan de concentratie en paraatheid van informatie, verwijderde ik proefpersonen veel tijd aan de lijst spendeerden. Ik verwijderde in totaal vier proefpersonen.

3. Als laatste verwijderde ik proefpersonen met zeer afwijkende scores, zogenoemde ‘outliers’. Ik onderzocht de scores op de afhankelijk variabelen. Als de antwoorden van proefpersonen extreem afweken van het gemiddelde - bijvoorbeeld een score van 1 op privacy, terwijl het gemiddelde 5 was - verwijderde ik ze uit het databestand. Ik sloot uiteindelijk drie proefpersonen uit van het databestand.