

Hoe veilig is jouw identiteit op Facebook?

Onderzoek naar de factoren van invloed op risico-informatie zoeken en het nemen van zelfbeschermende maatregelen op Facebook

Sean-Patrick Kats - s0180564

Enschede, juni 2013

Universiteit Twente

Opleiding: Master Psychologie, Conflict, Risico en Veiligheid

Begeleiders:

Dr. Jan Gutteling

Dr. ir. Peter de Vries

Samenvatting

Facebook kan cybercriminelen de gelegenheid bieden om persoonsgegevens van een individu te misbruiken. Identiteitsdiefstal kan zeer ernstige gevolgen hebben, waardoor het belangrijk is dat mensen hun persoonsgegevens beter gaan beschermen op sociale media als Facebook. Campagnes als Alert Online beogen mensen voor dit gevaar te behoeden door ze tips te geven over hoe ze zelfbeschermende maatregelen kunnen nemen. In dit onderzoek is onderzocht welke factoren van invloed zijn op het nemen van zelfbeschermende maatregelen en het zoeken van risicorelevante informatie. Er is onderzocht door middel van een experimenteel design wat het effect is van verschillende niveaus van response efficacy en geloofwaardigheid van de zender op het zoeken van risicorelevante informatie en het nemen van zelfbeschermende maatregelen. Er is nagegaan of het effect van response efficacy en geloofwaardigheid van de zender op het nemen van zelfbeschermende maatregelen wordt gemedieerd door het informatie zoekgedrag. Tevens is nagegaan wat het effect is van de mate van beloningen die men ondervindt aan Facebook gebruik en de persoonlijke relevantie op het zoeken van risicorelevante informatie en het nemen van zelfbeschermende maatregelen. De resultaten zijn gebaseerd op de antwoorden van 132 respondenten. De manipulaties van de geloofwaardigheid van de zender en de response efficacy hadden het gewenste effect. Er blijkt een significante negatieve correlatie te zijn tussen de intentie tot het nemen van zelfbeschermende maatregelen en de variabelen hoeveel Facebookvrienden men heeft en hoe vaak men actief is op Facebook. Er is een matig tot sterke significante positieve correlatie gevonden tussen de intentie tot informatie zoeken en de intentie tot het nemen van zelfbeschermende maatregelen. Tevens bleek het dat respondenten die meer beloningen ervoeren aan het gebruik van Facebook een lagere intentie hadden tot het nemen van zelfbeschermende maatregelen. Persoonlijke relevantie van het risico heeft een positief verband met de intentie tot informatie zoeken. Implicaties voor de praktijk en aanbevelingen voor vervolgonderzoek zijn gegeven.

Abstract

Facebook may provide an opportunity for cyber criminals to exploit personal information from an individual. Identity theft can have serious consequences, so it is important that people will protect their personal information well on social media like Facebook. Public service announcements as Alert Online are designed to protect people from this danger by giving them advice on how they can take protective measures. This study examined factors that affect the adoption of self-protective measures and seeking risk relevant information. In this research an experimental design was used to measure the effects of different levels of response efficacy and source credibility on seeking risk relevant information and on taking self-protective measures. Whether the effect of response efficacy and source credibility on taking self-protective measures is mediated by information seeking behaviour is examined. Also, the effect of rewards that one takes from Facebook and personal relevance on seeking risk relevant information and on taking self-protective measures is examined. The results are based on the responses of 132 respondents. The manipulations of source credibility and response efficacy had the desired effect. A significant negative correlation was found between the intention to take self-protective measures and the variables how many Facebook friends someone has and how many times someone is active on Facebook. A moderate to strong positive correlation was found between the intention to seek information and the intention to take self-protective measures. Respondents who experienced more rewards from Facebook expressed less intention to take self-protective measures. Personal relevance of the risk had a positive relationship with the intention to seek information. Implications for practice and recommendations for future research are given.

Voorwoord

Na zes jaar studeren is de eindstreep voor mij in zicht. Ik heb veel geleerd, erg genoten van mijn studententijd en ben tevreden met het eindresultaat. Een hoge motivatie heeft even op zich laten wachten, maar sinds ik mij heb verdiept in de thema's conflict, risico en veiligheid binnen de psychologie zijn zowel mijn motivatie als mijn cijfers flink gestegen.

Voor de totstandkoming van deze masterthese wil ik graag mijn begeleiders, Jan Gutteling en Peter de Vries, bedanken voor hun inzet en adviezen. De feedbackafspraken heb ik ervaren als uitdagend, leerzaam en gezellig.

Enschede, 20 juni 2013

Sean-Patrick Kats

Inhoudsopgave

1. Inleiding.....	6
1.1 Identiteitsdiefstal	6
1.2 Alert Online	7
2. Theorie en hypothesen.....	8
2.1 Zelfbeschermende maatregelen en informatie zoeken	8
2.2 Response efficacy	8
2.3 Geloofwaardigheid van de zender	10
2.4 De beloningen van Facebook.	11
2.5 Persoonlijke relevantie	11
2.6 Hypothesen	12
3. Methoden.....	13
3.1 Design	13
3.1.1 Manipulatie van response efficacy	13
3.1.2 Manipulatie van geloofwaardigheid van de zender	14
3.1.3 Procedure	14
3.2 Metingen	15
3.2.1 Onafhankelijke variabelen	15
3.2.2 Afhankelijke variabelen	16
3.2.3 Demografische en overige variabelen	17
3.3 Pretest en manipulatiechecks	17
3.4 Respondenten	18
4. Resultaten.....	19
4.1 Algemene bevindingen	19
4.2 Het nemen van zelfbeschermende maatregelen	21
4.3 Informatie zoeken	21
4.4 Beloningen van Facebook	22
4.5 Persoonlijke relevantie	23
5. Discussie.....	24
5.1 Conclusies	24
5.1.1 Hypothese 1	24
5.1.2 Hypothese 2	25
5.1.3 Hypothese 3a, 3b, 4a & 4b	26
5.2 Kanttekeningen	27
5.3 Aanbevelingen en implicaties	28
6. Referenties.....	30
Appendix 1. Enquête Facebook	33

1. Inleiding

Tegenwoordig wordt internet bijna de hele dag door gebruikt voor zowel werk als privé. De meeste huishoudens beschikken dan ook over een computer of laptop met een internet verbinding. Tevens kunnen veel mensen momenteel ook al het internet op via hun smartphone of tablet (Van Deursen & Van Dijk, 2012).

Veel mensen maken tegenwoordig gebruik van sociale media als Facebook, Twitter en LinkedIn (Oosterveer, 2012). Sociale media vallen te definiëren als internet applicaties, waarbij de gebruikers de inhoud bepalen en maken, commentaar kunnen geven op elkaars inhoud en hun eigen inhoud met andere mensen kunnen delen (O'Reilly, 2005). Facebook is met 8,7 miljoen gebruikers het meest gebruikte type sociale media in Nederland (Oosterveer, 2012). Wereldwijd zijn er zelfs meer dan één miljard mensen actief op Facebook (Facebook, 2012). De laatste jaren is er tevens een duidelijk stijgende trend te zien in Nederland van het aantal mensen dat Facebook gebruikt (Oosterveer, 2012).

De mogelijke reden voor de sterke toenames in het aantal Facebookgebruikers is dat zij veel positieve uitkomsten ofwel beloningen ervaren aan het gebruik van Facebook (Joinson, 2008). Voor veel Facebookgebruikers is het een makkelijke manier om in contact te blijven met hun vrienden en kennissen (Joinson, 2008). Tevens is Facebook voor velen een belangrijke manier om anderen te laten weten wat zij zelf aan het doen zijn en om aan te geven welke activiteiten zij wel of niet gaan bijwonen (Joinson, 2008).

1.1 Identiteitsdiefstal

De opkomst van nieuwe sociale media als Facebook brengt nieuwe risico's met zich mee. Op een site als Facebook plaatsen veel mensen persoonlijke informatie op internet (Hoadley, Xu, Lee & Rosson, 2010; Kelly, 2008; Ransdorp & Zondervan, 2012). Het gevaar hiervan is dat door deze blootstelling van persoonlijke gegevens mensen het risico lopen dat er misbruik van wordt gemaakt door bijvoorbeeld online criminelen, stalkers, pestkopen en zelfs door vrienden of bekenden (Hoadley et al, 2010; Kelly, 2008). Vooral mensen die hun adresgegevens en telefoonnummers op Facebook zetten zijn zeer kwetsbaar voor cybercriminelen die eropuit zijn om identiteiten te stelen (Tuil, 2011). Dit blijkt wel uit een recente cybercrime zaak, waarbij 11 miljoen Facebook accounts zijn geïnfecteerd met malware die de criminelen in staat stelde om de persoonsgegevens van de gebruikers te achterhalen (Sky News, 2012).

Identiteitsfraude en diefstal kunnen grote schade aanrichten in iemands leven (Lewis, z.j.). Gebruikers van Facebook die hun volledige naam, geboortedatum, adres en relatiestatus

online plaatsen kunnen al ten prooi vallen aan cybercriminelen (Lewis, z.j.). Met deze persoonlijke gegevens kunnen de criminelen bijvoorbeeld producten bestellen op een website onder de naam van het slachtoffer, inloggen op zijn de bestaande accounts en geld van de bankrekening halen van het slachtoffer (Lewis, z.j.). Aangezien het merendeel van de Nederlanders dagelijks Facebook gebruikt (Oosterveer, 2012) kan de persoonlijke relevantie van het risico van identiteitsdiefstal op Facebook als zeer hoog worden beschouwd.

Het is wel mogelijk om via Facebook je persoonlijke gegevens te beveiligen, echter zijn er toch nog veel mensen die dit niet doen (Ransdorp & Zondervan, 2012). Facebook geeft genoeg opties om je persoonsgegevens te beschermen, maar deze zijn meestal lastig te vinden en omslachtig in gebruik (Deen, 2011). Tevens zijn de standaard privacy instellingen op Facebook niet altijd in het belang van de gebruiker. Op deze manier kan het dus voorkomen dat mensen als snel meer persoonsgegevens openbaar maken dan dat ze denken (Deen, 2011).

1.2 Alert Online

Op 12 november 2012 is de tiendaagse campagne Alert Online gestart. Tijdens deze campagne hebben verschillende partijen hun krachten gebundeld om veilig en bewust internet gebruik aan het licht te brengen (Alert Online, 2012). Op de dag dat de Alert Online campagne van start ging werd er een rapport overhandigd aan de minister van Veiligheid en Justitie door het Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Dit rapport bevatte onderzoeksresultaten die aantoonde wat het huidige cyber-awareness niveau is onder verschillende relevante doelgroepen in Nederland. Eén van de belangrijkste aanbevelingen van dit rapport was dat sociale media een belangrijk onderwerp is waarover informatie verstrekt dient te worden aan de gebruikers (Ransdorp & Zondervan, 2012). Dit omdat veel gebruikers het risico zeer groot achten dat er zich iets ongewenst zal voordoen met hun persoonlijke informatie (Ransdorp & Zondervan, 2012). Vooral jongeren zijn een kwetsbare groep, omdat zij actiever zijn op sociale media en vaak ook meer informatie prijsgeven dan andere groepen (Ransdorp & Zondervan, 2012). Een verklaring hiervoor kan zijn dat jongeren hun eigen kennis en vaardigheden om hun eigen gegevens te beschermen overschatten (Ransdorp & Zondervan, 2012). Hierdoor zijn ze mogelijk eerder geneigd om informatie over zichzelf te delen.

De Alert Online campagne is erop gericht om mensen bewust te maken van de risico's van internetgebruik en om enkele tips te geven over hoe men deze risico's kan voorkomen. Dit met het uiteindelijke doel dat mensen hun eigen persoonsgegevens op internet beter gaan beschermen. Door een gebrek aan empirische bewijzen kan men zich echter afvragen of de

zender van de gegeven tips geloofwaardig overkomt en of de tips als nuttig worden beschouwd. In dit onderzoek zal dan ook worden gekeken naar zowel de nuttigheid van de tips als de geloofwaardigheid van de zender. Daarnaast zal er nog nagegaan worden of de hoge mate van beloningen en persoonlijke relevantie van invloed zijn op het beschermen van persoonsgegevens op Facebook.

2. Theorie en hypotheses

Het is van groot belang dat de Facebook gebruiker zichzelf beter gaat beschermen tegen de gevaren van identiteitsdiefstal op Facebook. Enkele concepten die betrekking hebben op risicocommunicatie en het aanzetten tot het nemen van zelfbeschermende maatregelen en het zoeken van risico relevante informatie lijken hier goed toepasbaar op, namelijk response efficacy, geloofwaardigheid van de zender, beloningen van Facebook en persoonlijke relevantie van het risico. Deze zullen kort worden besproken.

2.1 Zelfbeschermende maatregelen en informatie zoeken

Zorgen dat burgers zelfbeschermende maatregelen nemen lijkt het doel van vele interventies en preventiecampagnes. In dit onderzoek wordt met zelfbeschermende maatregelen bedoeld dat de Facebookgebruiker zijn of haar persoonlijke informatie beschermt. Het aanzetten tot informatie zoeken is tevens een belangrijk onderwerp geworden op het gebied van risicocommunicatie (Griffin, Dunwoody & Neuwirth, 1999). Het idee hierachter is dat mensen die worden aangezet tot het zoeken van risico-informatie eerder zelfbeschermende maatregelen gaan nemen (Griffin, Dunwoody & Neuwirth, 1999; Ter Huurne & Gutteling, 2008). Dit kwam ook naar voren in een onderzoek van Kievik en Gutteling (2011) waar een duidelijk verband werd gevonden tussen informatie zoekgedrag en het nemen van zelfbeschermende maatregelen. Het is daarom dus belangrijk dat risicocommunicatie onderzoek zich niet alleen richt op de effectiviteit van risicoboodschappen, maar ook op determinanten die bijdragen tot het aanzetten van mensen tot het zoeken van informatie (Huurne, 2008). In dit onderzoek zal het zoeken naar risicorelevante informatie dan ook worden meegenomen als afhankelijke variabele naast het nemen van zelfbeschermende maatregelen.

2.2 Response efficacy

Het concept response efficacy is voor dit onderzoek ontleend uit het Extended Parallel Process Model (EPPM) van Witte (1992). Het model gaat ervan uit dat wanneer een persoon aan een risicoboodschap wordt blootgesteld de fear appeal componenten in deze boodschap

leiden tot de motivatie om deze boodschap te verwerken. Bij de fear appeal componenten kan bijvoorbeeld gedacht worden aan een tekst als 'rokers sterven jong' of een plaatje van een zwarte doorrookte long op een pakje sigaretten. Het EPPM gaat uit van twee cognitieve beoordelingsprocessen. De eerste is 'perceived threat', deze bestaat uit de ernst (severity) en de waargenomen kwetsbaarheid (susceptibility). De tweede is de waarneming van het aanbevolen gedrag, 'perceived efficacy', deze bestaat uit de verwachting van een persoon in staat te zijn het aanbevolen gedrag uit te voeren (self-efficacy) en het verwachte nut van het aanbevolen gedrag (response efficacy). Wanneer een persoon de perceived threat van de boodschap te laag waardeert zal deze niet gemotiveerd zijn om actie te ondernemen. Wordt de perceived threat als hoog gewaardeerd dan zal dit leiden tot *angst* bij een persoon. Deze angst zal de persoon dan motiveren actie te ondernemen om dit te verminderen. De perceived efficacy zal dan bepalen of dit leidt tot een *danger control process* of een *fear control process*. In het danger control process worden zowel de perceived threat als de perceived efficacy hoog gewaardeerd. Dit zal dan leiden tot *protection motivation* en dus *adaptive changes*. Bij het fear control process wordt de perceived threat wel hoog gezien, maar is de perceived efficacy laag. Dit zal op zijn beurt weer leiden tot *defensive motivation* wat leidt tot *maladaptive changes*. Ontkenning van het probleem is een voorbeeld van *maladaptive changes* (Witte, 1992).

Er zijn vele factoren die bepalen of een persoon zelfbeschermende maatregelen gaat nemen. In een groot aantal onderzoeken (o.a. Witte & Allen, 2000) is al aangetoond dat een hoge risicoperceptie en een hoge mate van self-efficacy belangrijke voorwaarden zijn voor het nemen van zelfbeschermende maatregelen. In dit onderzoek zal er dan ook voornamelijk worden gekeken naar de rol van de response efficacy in een risicoboodschap. Wanneer er wordt gekeken naar het aanzetten tot het nemen van zelfbeschermende maatregelen op Facebook via de boodschap van de Alert-online campagne kan namelijk worden afgevraagd of deze boodschap wel aan alle voorwaarden voor het nemen van zelfbeschermende maatregelen voldoet. Vooral kan worden afgevraagd of tips als 'gebruik je gezond verstand' en 'surf veilig' (Alert Online, 2012) wel worden waargenomen als nuttig in het beschermen van persoonsgegevens op Facebook. In dit onderzoek wordt dus verwacht dat tips die een hoge mate van waargenomen response efficacy hebben eerder zullen leiden tot het nemen van zelfbeschermende maatregelen dan tips die een lage mate van waargenomen response efficacy hebben.

Uit het onderzoek van Kievik en Gutteling (2011) bleek dat een hogere mate van efficacy beliefs bestaande uit de self-efficacy en response efficacy een goede voorspeller is voor het

zoeken van informatie. In dit onderzoek zal dan ook worden gekeken of de response efficacy van de risicoboodschap invloed heeft op het zoeken van risicorelevante informatie.

2.3 Geloofwaardigheid van de zender

De response efficacy gaat in op de inhoud van de risicoboodschap. In dit onderzoek zal tevens worden nagegaan of niet alleen de inhoud belangrijk is, maar ook of de geloofwaardigheid van de zender van de boodschap invloed heeft op het zoeken van informatie en het nemen van zelfbeschermende maatregelen. Een risicoboodschap zou een inhoud kunnen hebben die een hoge mate van response efficacy oproept, echter hoeft dit niet te leiden tot het uitvoeren van zelfbeschermende maatregelen als het van een zender komt die niet als geloofwaardig wordt beschouwd. Uit onderzoek van Renn en Levine (1989) bleek dat wanneer een bron die als geloofwaardig wordt beschouwd een boodschap naar buiten brengt, dat deze dan eerder tot acceptatie zal leiden in een individu. Het onderzoek van Reynolds (2011) toonde aan dat de geloofwaardigheid van de bron van de boodschap een belangrijke determinant is voor succesvolle risicocommunicatie. Tevens bleek dat de geloofwaardigheid van de bron voornamelijk wordt gebaseerd op de waargenomen competentie en eerdere ervaringen van die bron (Renn & Levine, 1989). Hiervan kan worden afgeleid dat een bron die wordt beschouwd als competent en ervaren in het gebruik van Facebook - en ook zelf laten zien dat zij het goede voorbeeld geven op Facebook - eerder als geloofwaardig wordt beschouwd en dat mensen dus eerder geneigd zijn om de adviezen van deze individu tot zich te nemen.

Vooraf bij nieuwe technologieën blijkt geloofwaardigheid van de bron een rol te spelen in hoe mensen daarmee omgaan (Purchase, 2004). In dit onderzoek wordt verondersteld dat in een situatie waarin het risico relatief nieuw is, zoals identiteitsdiefstal op Facebook, de geloofwaardigheid van de bron een belangrijkere rol gaat spelen in het aanzetten tot het nemen van zelfbeschermende maatregelen en het zoeken van risico relevante informatie. Tevens zal worden verondersteld dat zowel de waargenomen response efficacy van de gegeven tips als de geloofwaardigheid van de zender van deze tips elkaar zullen versterken. Dit houdt in dat tips die als zeer nuttig worden ervaren en van een geloofwaardige bron komen eerder zullen leiden tot het nemen van zelfbeschermende maatregelen dan wanneer het nut en/of de geloofwaardigheid laag is.

Gebaseerd op onderzoek van Kievik en Gutteling (2011) waar een mediërend effect is gevonden van informatie zoeken op de relatie tussen risicoperceptie, efficacy beliefs en het nemen van zelfbeschermende maatregelen zal in deze studie worden verwacht dat het

hierboven genoemde gezamenlijke effect van response efficacy en geloofwaardigheid op het nemen van zelfbeschermende maatregelen wordt gemedieerd door het informatie zoeken.

2.4 De beloningen van Facebook.

Facebook brengt voor een groot aantal personen veel positieve uitkomsten met zich mee. Uit een onderzoek van Joinson (2008) blijkt dat veel mensen Facebook gebruiken voor voornamelijk sociale doeleinden, zoals het kijken waar vrienden mee bezig zijn en wat hen bezig houdt. Er blijkt echter dat positieve uitkomsten ofwel beloningen die men ondervindt aan een bepaald gedrag de kans vergroten dat men geen zelfbeschermende maatregelen gaat nemen (Rogers, 1975). Een onderzoek van Midden en Huijts (2009) naar de evaluatie van nieuwe risico's toonde aan dat een hoge mate van waargenomen voordelen van een nieuw risico er toe leidde dat dit risico eerder werd geaccepteerd. Risico's worden over het algemeen als kleiner beschouwd wanneer de voordelen dat het met zich meebrengt groter zijn (Ropek & Slovic, 2003). In dit onderzoek wordt dus verondersteld dat hoe meer beloningen men ervaart aan het gebruik van Facebook, des te minder zij geneigd zijn om zelfbeschermende maatregelen te nemen en risico informatie te zoeken.

2.5 Persoonlijke relevantie

Veel interventies die zijn gericht op het bewust maken van mensen op een bepaald risico proberen de persoonlijke relevantie van dat risico voor de doelgroep te benadrukken (Rothman & Kiviniemi, 1999). Persoonlijke relevantie blijkt dan ook een belangrijke voorspeller te zijn voor het slagen van een interventie en het nemen van zelfbeschermende maatregelen (Rothman & Kiviniemi, 1999).

Daarnaast kan verondersteld worden dat de persoonlijke relevantie een belangrijke factor is voor het zoeken van risicogerelateerde informatie (Eagly & Chaiken, 1993; Huurne, 2008). Dit doordat persoonlijke relevantie mensen kan motiveren om op zoek te gaan naar informatie en deze systematischer te verwerken. Persoonlijke relevantie hangt volgens Eagly en Chaiken (1993) nauw samen met de informatie behoefte die een persoon heeft, wanneer zij het risico als persoonlijk relevanter waarnemen zullen zij dus een grote informatie behoefte hebben wat hen motiveert om op zoek te gaan naar relevante risico-informatie. Verondersteld wordt dat mensen die het risico op identiteitsdiefstal via Facebook als persoonlijk relevanter waarnemen eerder geneigd zijn zelfbeschermende maatregelen te nemen en om risico-informatie te zoeken.

2.6 Hypotheses

In de hierboven genoemde campagne Alert Online worden een aantal tips gegeven aan gebruikers om zichzelf beter te beschermen op Facebook. Het nut van deze tips is iets wat echter niet empirisch onderbouwd is. Tevens is Facebook iets wat kan worden beschouwd als nieuw communicatiemiddel en vormt dus ook een nieuw risico. Het doel van dit onderzoek is dan ook om het effect van verschillende niveaus van response efficacy en de geloofwaardigheid van de zender op het zoeken van risico-informatie en het nemen van zelfbeschermende maatregelen vast te stellen. Tevens zal er worden nagegaan wat de rol van de beloningen van Facebook en de persoonlijke relevantie van het risico hierin zijn. Op basis van bovenstaande theorie kunnen de volgende hypothesen worden opgesteld. In figuur 1 staat het conceptuele model waarin de hypothesen worden weergegeven.

Hypothese 1 zal nagaan of er een interactie effect zal optreden tussen response efficacy en de geloofwaardigheid van de zender.

H1. *Er zal een interactie-effect optreden tussen response efficacy en geloofwaardigheid van de zender, zodat een hoge mate van response efficacy en een hoge mate van de geloofwaardigheid van de zender te samen leiden tot het nemen van meer zelfbeschermende maatregelen dan wanneer één van beide of beide laag zijn.*

Hypothese 2 zal onderzoeken of het in hypothese 1 genoemde interactie effect van response efficacy en geloofwaardigheid op het nemen van zelfbeschermende maatregelen wordt beïnvloed door het zoeken van risico-informatie.

H2. *Het effect van response efficacy en geloofwaardigheid van de zender op het nemen van zelfbeschermende maatregelen wordt gemedieerd door risico-informatie zoekgedrag.*

Hypothese 3 is geformuleerd om na te gaan of de beloningen die men ondervindt aan het gebruik van Facebook effect hebben op het nemen van zelfbeschermende maatregelen en informatie zoeken.

H3a. *Een hogere mate van beloningen die men ervaart aan het gebruik van Facebook leidt tot het nemen van minder zelfbeschermende maatregelen dan een lage mate van beloningen.*

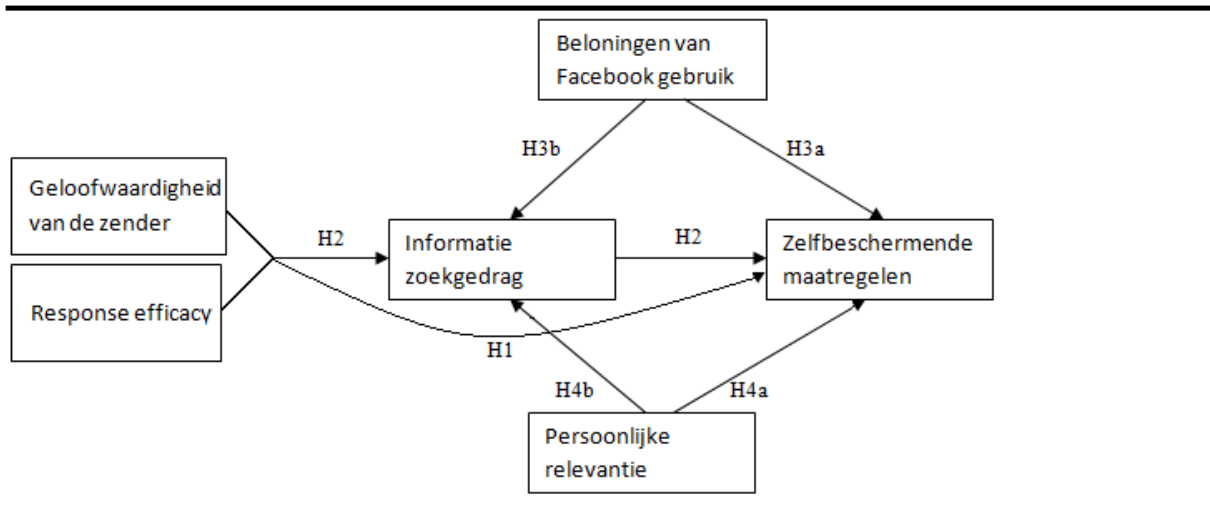
H3b. *Een hogere mate van beloningen die men ervaart aan het gebruik van Facebook leidt tot het zoeken van minder risico-informatie dan een lage mate van beloningen.*

Hypothese 4 zal nagaan of de persoonlijke relevantie van het risico invloed heeft op het nemen van zelfbeschermende maatregelen en informatie zoeken.

H4a. *Een hogere mate van persoonlijke relevantie die men ervaart aan het risico op*

identiteitsdiefstal via Facebook leidt tot het nemen van meer zelfbeschermende maatregelen dan een lage persoonlijke relevantie.

H4b. Een hogere mate van persoonlijke relevantie die men ervaart aan het risico op identiteitsdiefstal via Facebook leidt tot meer risico-informatie zoeken dan een lage persoonlijke relevantie.



Figuur 1 Conceptueel model van de hypothesen

3. Methoden

3.1 Design

De hypothesen zijn onderzocht aan de hand van een experiment met een 2 (response efficacy: hoog vs. laag) x 2 (de geloofwaardigheid van de zender: hoog vs. laag) between subject design. De afhankelijke variabelen zijn het nemen van zelfbeschermende maatregelen, de intentie tot het nemen van zelfbeschermende maatregelen, risico-informatie zoeken en de intentie tot risico-informatie zoeken. Tevens werden als onafhankelijke variabelen de 'beloningen' en 'persoonlijke relevantie' meegenomen. Hoewel Ransdorp en Zondervan (2012) stelden dat vooral jongeren een kwetsbare groep zijn op internet is in deze studie als doelgroep de gehele populatie meegenomen. De respondenten zijn random verdeeld over de verschillende condities en zijn blootgesteld aan de response efficacy en geloofwaardigheid van de zender manipulaties.

3.1.1 Manipulatie van response efficacy

Voor de manipulatie van de response efficacy zijn twee verschillende boodschappen opgesteld die tips geven over hoe je identiteitsdiefstal op Facebook kan voorkomen. De

standaard boodschap die overeenkomt met een lage mate van response efficacy is gebaseerd op de tips van de campagne Alert Online (2012). De respondenten in de lage response efficacy condities krijgen de standaardboodschap met de volgende tips te zien: *Gebruik je gezond verstand en schakel bij twijfel een expert in, bescherm je computer en houdt deze up-to-date en surf veilig*. Tevens kregen zij het bericht dat de gegeven tips door anderen als niet nuttig werden beschouwd. De verbeterde boodschap die de respondenten te zien kregen in de hoge response efficacy conditie zijn gebaseerd op tips van de website Computerworld (Deen, 2011). Dit zijn: *Plaats geen telefoonnummers of adresgegevens op Facebook, zorg dat je niet opduikt in zoekmachines en zorg dat alleen je vrienden je gegevens kunnen zien*. Vervolgens kregen de respondenten in deze conditie een bericht te lezen dat de tips door anderen als zeer nuttig werden ervaren. De volledige uitwerking van de condities is terug te vinden in Appendix 1.

3.1.2 Manipulatie van geloofwaardigheid van de zender

De geloofwaardigheid van de zender is gemanipuleerd aan de hand van de beschreven competentie en ervaring van de zender. Deze informatie is weergegeven als een Facebookpagina (zie Appendix 1). In de hoge geloofwaardigheid conditie werd respondenten verteld dat de tips die zij hebben ontvangen afkomstig zijn van een Facebookvriend die al meer dan vijf jaar dagelijks actief is op Facebook. Vervolgens kregen de respondenten in deze conditie een gedeelte van een Facebookpagina te zien die correspondeert met een hoge mate van geloofwaardigheid. De essentiële punten in deze afbeelding zijn dat de Facebookvriend 650 Facebookvrienden heeft, 80 foto's heeft en met uitzondering van zijn geslacht geen persoonlijke gegevens deelt. In de lage geloofwaardigheid van de zender conditie werd de respondenten verteld dat deze tips afkomstig zijn van een Facebookvriend die net twee maanden een Facebookaccount heeft en slechts één keer per week actief is op Facebook. Deze respondenten kregen een afbeelding te zien die een lage mate van geloofwaardigheid communiceert. Deze afbeelding verschilde alleen op de volgende punten van de hoge geloofwaardigheid afbeelding: de Facebookvriend heeft zelf 10 Facebookvrienden, heeft slecht 2 foto's en deelt meer persoonsgegevens. De volledige uitwerking van de condities is terug te vinden in Appendix 1.

3.1.3 Procedure

De enquête (Appendix 1) is via Facebook, e-mail en op papier verspreid in het privé netwerk van de onderzoeker. Eerst moesten de respondenten een aantal demografische variabelen invullen en volgden er enkele vragen over het Facebook gebruik van de respondenten. Hierna

kregen zij ongeacht de conditie de hoge risicoperceptie boodschap te zien. Dit omdat een hogere mate van waargenomen risico een voorwaarde is voor een individu om zelfbeschermende maatregelen te nemen (Witte & Allen, 2000) of informatie te zoeken (Kievik & Gutteling, 2011). De risicoboodschap is gebaseerd op een bericht van Computerworld (2011) en Mariska Media (2012), omdat dit vooraanstaande sites zijn op dit gebied. Het bericht is terug te vinden in Appendix 1. Vervolgens werden de respondenten random verdeeld over de condities en blootgesteld aan de manipulaties. Direct na de manipulaties kregen de respondenten twee controlevragen, waarna de items betreffende de afhankelijke en onafhankelijke variabelen volgden.

3.2 Metingen

3.2.1 Onafhankelijke variabelen

Om vast te stellen in hoeverre men *beloningen* ondervindt aan het gebruik van Facebook zijn vier items opgesteld op basis van de motieven voor Facebook gebruik van Joinson (2008). Deze zijn gescoord op een vijf-punts likert schaal met de waarden 1 = helemaal mee oneens tot 5 = helemaal mee eens. De gevonden Cronbach's alpha is .78.

De *persoonlijke relevantie* is gemeten aan de hand van vier items die werden gemeten met behulp van een vijf-punt likert schaal met de waarden 1 = helemaal mee oneens tot 5 = helemaal mee eens. De items hebben een Cronbach's alpha van .70.

De ernst en kwetsbaarheid vormen samen de *risicoperceptie* (Witte, 1992). Dit construct is gemeten door items uit de Risk Behavior Diagnostic Scale (RBDS) van Witte, Cameron, Mckeon en Berkowitz (1996). Samen zijn dit vijf items die werden gescoord aan de hand van een vijf-punts likert schaal met de waarden 1 = helemaal mee oneens tot 5 = helemaal mee eens. Samen hebben de constructen een Cronbach's alpha van .77. Een factoranalyse toonde echter aan dat beide constructen ieder een aparte factor zijn, daarom zijn deze verder apart behandeld.

Het construct *ernst* is gemeten aan de hand van twee items uit de RBDS en gescoord op een vijf-punts likert schaal met de waarden 1 = helemaal mee oneens tot 5 = helemaal mee eens. De gevonden Cronbach's alpha is .91.

Het construct *kwetsbaarheid* meet in hoeverre men zich kwetsbaar acht voor identiteitsdiefstal op Facebook. Het construct is gemeten aan de hand van drie items uit de RBDS en gescoord op een vijf-punts likert schaal met de waarden 1 = helemaal mee oneens tot 5 = helemaal mee eens. De gevonden Cronbach's alpha van de items is .89.

Om *self-efficacy* te meten - dus in hoeverre de respondenten zichzelf instaat achten om de

tips uit te voeren - zijn er drie items opgesteld vanuit de RBDS. Deze zijn gescoord op een vijf-punts likert schaal met de waarden 1 = helemaal mee oneens tot 5 = helemaal mee eens. De items hebben een Cronbach's alpha van .91.

Voor het construct *response-efficacy* is gemeten in hoeverre de respondenten de tips over hoe je identiteitsdiefstal op Facebook kan voorkomen als nuttig beschouwen. Deze zijn wederom gemeten door middel van drie items uit de RBDS die werden gescoord op een vijf-punts likert schaal met de waarden 1 = helemaal mee oneens tot 5 = helemaal mee eens. De gevonden Cronbach's alpha is .71.

Tenslotte is gemeten hoe *geloofwaardig* de zender van de boodschap overkomt. Dit construct werd gemeten door vier items die afkomstig zijn uit onderzoek van McCroskey (1966) en Berlo, Lemert en Mertz (1969). De items zijn gescoord aan de hand van een vijf-punts likert schaal met de waarden 1 = helemaal mee oneens tot 5 = helemaal mee eens. De items hebben een Cronbach's alpha van .84.

3.2.2 Afhankelijke variabelen

De items betreffende *risico-informatie zoekgedrag* zijn opgedeeld in twee schalen, namelijk het daadwerkelijk risico-informatie zoekgedrag en de intentie om risicorelevante informatie te zoeken. Om het *daadwerkelijke risico-informatie zoekgedrag* te berekenen kregen respondenten vier weblinks te zien en werden verzocht om hier één van te kiezen. Eén weblink verwees duidelijk naar risicorelevante informatie en de anderen duidelijk niet. Dit item is gescoord worden aan de hand van 1 = irrelevante site en 2 = relevante site. De *intentie om risicorelevante informatie* te gaan zoeken is aan de hand van één item gemeten. Deze is gescoord aan de hand van een vijf-punts likert schaal met de waarden 1 = helemaal mee oneens tot 5 = helemaal mee eens.

De items betreffende *zelfbeschermende maatregelen* zijn opgedeeld in twee schalen, namelijk daadwerkelijke zelfbeschermende maatregelen en de intentie tot het nemen van zelfbeschermende maatregelen. Voor de variabele *daadwerkelijke zelfbeschermende maatregelen* zijn vier items gebruikt. De daadwerkelijke zelfbeschermende maatregelen items meten het gedrag dat men op het moment van het invullen van de vragenlijst daadwerkelijk uitvoert. Om een schaalscore te kunnen berekenen zijn alle scores op de items aan elkaar gelijk gesteld, zodat ze worden gescoord op een schaal van 1 t/m 5. De items met als antwoordmogelijkheden 1 = iedereen, 2 = vrienden van vrienden, 3 = vrienden en 4 = alleen ik, zijn herberekend zodoende dat 2 veranderde in 2.33, 3 in 3.66, 4 in 5 en 1 is gelijk gebleven. Op deze wijze blijven de stappen tussen de scores hetzelfde. Het item dat werd

gemeten met een ja/nee antwoordmogelijkheid behandeld op de wijze dat nee overeenkomstig is met 5, aangezien nee overeenkomt met een hoge mate van het nemen van zelfbeschermende maatregelen. Ja wordt gelijk gesteld met 1, omdat dit overeenkomt met een lage mate van het nemen van zelfbeschermende maatregelen. De scores 1 en 5 worden gekozen, omdat ja en nee beide extremen zijn die als overeenkomstig kunnen worden beschouwd met de antwoorden op een Likert schaal als geheel mee eens en geheel mee oneens. De schaal heeft een Cronbach's alpha van .54.

De *intentie tot het nemen van zelfbeschermende maatregelen* is gemeten door vijf items. Deze zijn gescoord aan de hand van een vijf-punts Likert schaal met de waarden 1 = helemaal mee oneens tot 5 = helemaal mee eens. De gevonden Cronbach's alpha is .56.

3.2.3 Demografische en overige variabelen

De *demografische variabelen* die zijn meegenomen in dit onderzoek betroffen geslacht, leeftijd en opleiding.

Verder is er nog gevraagd naar *Facebookgebruik variabelen*. Dit betrof hoe lang men al actief is op Facebook, hoeveel vrienden men heeft en hoe vaak men actief is op Facebook. Er is ook nagegaan door middel van één item in hoeverre men de *default instellingen van Facebook accepteert*. Tevens is aan de hand van één item vastgesteld hoe vaak men de *privacy instellingen op Facebook verandert*. Beide items zijn gescoord aan de hand van een vijf-punts likert schaal met de waarden 1 = helemaal mee oneens tot 5 = helemaal mee eens.

Tevens is middels *controle vragen* gemeten of de respondenten de manipulaties ook daadwerkelijk hebben waargenomen. Dit gebeurde door ze twee meerkeuze vragen voor te leggen die betrekking hadden op de manipulaties.

3.3 Pretest en manipulatiechecks

Om na te gaan of de hoge risicoboodschap en manipulaties het gewenste effect hebben is er vooraf een pretest gedaan. Deze pretest is door 63 respondenten ingevuld. De hoge risicoboodschap bleek succesvol. Dit houdt in dat de respondenten ongeacht de conditie waarin zij zaten hoog scoorden op de variabele risicoperceptie ($M=3.78$; $SD=.72$). Ook de manipulaties hadden het gewenste effect. Respondenten die zijn blootgesteld aan de hoge geloofwaardigheid manipulatie scoorden significant ($F(1,61) = 38.79$, $p < .01$) hoger op de variabele geloofwaardigheid van de zender dan respondenten die zijn blootgesteld aan de lage geloofwaardigheid manipulatie. Tevens bleek dat respondenten die zijn blootgesteld aan de hoge response efficacy manipulatie significant ($F(1,61) = 4.95$, $p < .05$) hoger scoorden op de gemeten variabele response efficacy dan de respondenten in de lage response efficacy

manipulatie.

In de uiteindelijke vragenlijst die is opgesteld om de hypothesen te toetsen is tevens gecontroleerd of de manipulaties het gewenste effect hadden door het meten van waargenomen geloofwaardigheid van de zender en response efficacy van de respondent. Hier is evenals in de pretest gebleken dat de manipulaties succesvol waren. Er zijn significante hoofdeffecten in de verwachte richtingen gevonden. Zo scoorden de respondenten die werden blootgesteld aan de hoge geloofwaardigheid manipulatie significant hoger op de gemeten variabele geloofwaardigheid van de zender dan in de lage manipulatie ($F(1,130) = 6.30, p < .05$) en de respondenten die zijn blootgesteld aan de hoge response efficacy manipulatie scoorden significant hoger op de gemeten variabele response efficacy dan de lage response efficacy manipulatie ($F(1,130) = 7.29, p < .01$).

3.4 Respondenten

In totaal hebben 224 respondenten de vragenlijst ingevuld. Door 32 respondenten die wel een Facebook account hadden zijn enkel de demografische variabelen en- of de controlevragen ingevuld. Deze zijn daarom in verdere analyses niet meegenomen. Van de overgebleven 192 respondenten gaf 20.86% aan geen Facebook account te hebben. Uiteindelijk bleven er dus 152 respondenten over met een Facebook account die random over de vier condities werden verdeeld. Uit de analyse bleek dat 20 respondenten van de overgebleven 152, één of meerdere controlevragen fout had beantwoord. Aangezien de respondenten die de controlevragen niet juist hadden beantwoord de manipulatie niet hebben waargenomen zijn deze uit de steekproef verwijderd. De overige analyses gaan dus uit van 132 respondenten in plaats van 152¹. Uit verdere analyse bleek dat de respondenten die één of meerdere controlevragen fout hadden alleen significant verschilden van respondenten die ze alle twee goed hadden op één demografische variabele. Dit was de leeftijd ($F(1,150) = 13.28, p < .01$). Respondenten die één of meerdere controlevragen fout hadden beantwoord waren significant ouder dan de respondenten die beide juist hadden beantwoord.

Gemiddeld zaten er in iedere conditie $M=33$ respondenten met een minimum van 30 en een maximum van 36. De leeftijd van de respondenten varieerde van 13 tot en met 61 ($M=27.91; SD=10.36$). Van de respondenten is 67.40% man en 32.60% vrouw. In totaal had 1.5% van de respondenten als hoogst afgeronde opleiding de basisschool, 6.10% heeft MAVO, 40.90% heeft HAVO of VWO, 13.60% gaf aan een MBO opleiding te hebben

¹ Wanneer de 152 respondenten werden meegenomen in de analyses bleek dat er geen andere resultaten gevonden zijn voor de hypothesen.

afgerond, 22.00% een HBO opleiding en 15.90 % had een afgeronde universitaire opleiding.

Om na te gaan of er systematische verschillen tussen de vier condities zijn, zijn er een aantal analyses uitgevoerd. Met behulp van een ANOVA is getoetst of er significante hoofd- of interactie effecten zijn gevonden van de geloofwaardigheid en response efficacy manipulaties op de demografische en Facebookgebruik variabelen. Hieruit blijkt dat er geen significante verschillen zijn gevonden tussen condities voor leeftijd, opleiding, het aantal Facebookvrienden, hoe vaak men actief is op Facebook, hoelang men al een Facebookaccount heeft, of men de default privacyinstellingen van Facebook accepteert en of men de privacyinstellingen op Facebook vaak verandert. Met een Chi-kwadraat toets is nagegaan of er voor de variabele geslacht significante verschillen zijn gevonden tussen en binnen de manipulaties. Voor zowel het aantal mannen ($X^2(1, n = 89) = .14, ns.$) als het aantal vrouwen ($X^2(1, n = 43) = .35, ns.$) bleken er geen significante verschillen te zitten tussen de manipulaties.

4. Resultaten

4.1 Algemene bevindingen

De gemiddeldes, standaarddeviaties en correlaties tussen alle variabelen zijn berekend en staan weergegeven in tabel 1.

In tabel 1 is te zien dat er significante correlatie is gevonden tussen de intentie tot het nemen van zelfbeschermende maatregelen en de variabele hoeveel Facebookvrienden men heeft ($r = -.32$). Het lijkt er dus op dat hoe meer Facebookvrienden een persoon heeft, hoe minder deze persoon geneigd is om zelfbeschermende maatregelen te nemen.

Tevens is er een significante correlatie gevonden tussen de intentie tot het nemen van zelfbeschermende maatregelen en de variabele hoe vaak men actief is op Facebook ($r = -.27$). Mogelijk houdt dit in dat mensen die vaker actief zijn op Facebook minder snel geneigd zijn tot het nemen van zelfbeschermende maatregelen.

Daarnaast blijkt dat er enkele positieve correlaties zijn gevonden met betrekking tot het informatie zoeken. Zo correleert de intentie tot informatie zoeken significant positief met de intentie tot het nemen van zelfbeschermende maatregelen ($r = .45$) en met het daadwerkelijke informatie zoeken ($r = .22$). Het daadwerkelijke informatie zoeken correleert positief significant met de intentie tot het nemen van zelfbeschermende maatregelen ($r = .22$).

Tabel 1 *Correlaties tussen de variabelen met de bijbehorende gemiddeldes en standaarddeviaties*(n= 132)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. Aantal Facebookvrienden	-													
2. Hoe vaak actief	.35**	-												
3. Hoelang al actief	.40**	.08	-											
4. Beloningen	.22*	.57**	-.03	-										
5. Persoonlijke relevantie	.12	.09	.08	.17*	-									
6. Ernst	-.12	-.05	-.08	.02	.19*	-								
7. Kwetsbaarheid	.07	-.02	.01	.07	.42**	.17	-							
8. Self-efficacy	.10	-.13	.29**	-.27**	-.16	.04	-.17	-						
9. Response efficacy	-.10	-.06	-.13	-.05	.08	.05	-.05	.14	-					
10. Geloofwaardigheid	-.01	.05	-.05	.02	.11	.15	.06	.01	.26**	-				
11. Intentie tot informatie zoeken	-.03	-.10	-.11	.08	.33**	.29**	.19*	-.19*	.11	.02	-			
12. Daadwerkelijke informatie zoeken	-.07	.13	-.01	.07	.12	.01	.01	-.07	.05	.12	.22*	-		
13. Daadwerkelijke zelfbeschermende maatregelen	-.12	-.10	-.10	-.06	.03	.12	-.14	-.13	-.02	.10	-.11	-.05	-	
14. Intentie tot het nemen van zelfbeschermende maatregelen	-.32**	-.27**	-.19*	-.15	.12	.30**	-.01	-.15	.12	.18*	.45**	.22*	.29**	-
Gemiddelde M	2.22	3.47	2.64	3.16	2.70	4.32	3.34	4.38	3.13	2.86	2.60	1.28	3.71	3.64
Standaarddeviatie SD	.93	.83	.84	.90	.88	.81	.94	.80	.88	.94	1.34	.45	.72	.69

* p < .05. ** p < .01. (tweezijdige toetsing) Daadwerkelijk informatie zoeken: 1 = irrelevant, 2 = relevant. Overige variabelen: 1 = helemaal mee oneens tot 5 = helemaal mee eens.

Tussen de gemeten waardes van de variabelen geloofwaardigheid van de zender en de response efficacy is een zwakke doch significante positieve correlatie gevonden ($r = .26$). Dit kan erop duiden dat beide variabelen elkaar beïnvloeden en dat er mogelijk een interactie effect zal optreden. Tevens is er significante positieve correlaties gevonden tussen de gemeten waardes van geloofwaardigheid van de zender en de intentie tot het opvolgen van de gegeven tips ($r = .18$). De gemiddelde scores van zowel de gemeten variabele geloofwaardigheid ($M = 2.86$) als de gemeten variabele response efficacy ($M = 3.13$) neigen naar een score van noch mee oneens, noch mee eens.

Volgens het EPPM van Witte (1992) zijn een hoge mate van ernst, kwetsbaarheid en self-efficacy voorwaardes voor het nemen van zelfbeschermende maatregelen. In tabel 1 is af te lezen dat de gevonden gemiddeldes voor de variabelen ernst ($M = 4.32$), kwetsbaarheid ($M = 3.34$) en self-efficacy ($M = 4.38$) erop duiden dat aan deze voorwaardes is voldaan. Voor geen van de drie variabelen zijn significante verschillen gevonden in de scores tussen de condities.

4.2 Het nemen van zelfbeschermende maatregelen

Hypothese 1 is getest met behulp van een ANOVA analyse. Het hoofdeffect van de response efficacy manipulatie was niet significant ($F(1,127) = .96, ns.$), evenals het hoofdeffect van de geloofwaardigheid van de zender manipulatie ($F(1,127) = 1.67, ns.$). Wanneer er naar het interactie effect werd gekeken bleek dat deze niet significant was ($F(1,127) = 2.96, ns.$).

Met de intentie tot het nemen van zelfbeschermende maatregelen als afhankelijke variabele, bleek dat er geen significante hoofdeffecten zijn gevonden voor response efficacy ($F(1,128) = .17, ns.$) en geloofwaardigheid ($F(1,128) = .02, ns.$). Er is tevens geen interactie effect gevonden van de twee onafhankelijke variabelen ($F(1,128) = .38, ns.$). Op basis van de gevonden resultaten kan hypothese 1 niet worden bevestigd.

In tabel 1 is te zien dat de gemiddelde scores van zowel de intentie als het daadwerkelijk nemen van zelfbeschermende maatregelen allemaal tussen de drie en vier liggen wat erop duidt dat zij het er noch mee eens, noch mee oneens tot een beetje mee eens waren.

Uit verdere analyse bleek dat de scores op zowel de intentie als de daadwerkelijke zelfbeschermende maatregelen kunnen niet verklaard worden door de gevonden waardes van ernst, kwetsbaarheid of self-efficacy.

4.3 Informatie zoeken

Hypothese 2 toetst of er sprake is van een mediatie effect van zowel de intentie als het daadwerkelijke informatie zoeken op de relatie tussen de onafhankelijke variabelen geloofwaardigheid van de zender en response efficacy en zowel de intentie als het

daadwerkelijk nemen van zelfbeschermende maatregelen. Uit een ANOVA analyse bleken geen significante hoofdeffecten te zijn voor de variabele daadwerkelijk informatie zoeken. Het hoofdeffect van de response efficacy manipulatie was niet significant ($F(1,128) = .03$, *ns.*), evenals het hoofdeffect van de geloofwaardigheid van de zender manipulatie ($F(1,128) = .16$, *ns.*). Wanneer er naar het interactie effect werd gekeken bleek dat deze niet significant was ($F(1,128) = .56$, *ns.*).

Met de intentie tot het informatie zoeken als afhankelijke variabele, bleek dat er geen significant hoofdeffect is gevonden voor response efficacy ($F(1,128) = .98$, *ns.*). Wel is er een marginaal significant hoofdeffect gevonden voor geloofwaardigheid ($F(1,128) = 3.36$, $p = .07$). De gemiddelde score op de intentie tot het zoeken van informatie bleek in de lage geloofwaardigheid manipulatie $M = 2.80$ ($SD = 1.44$) en in de hoge manipulatie $M = 2.39$ ($SD = 1.20$) te zijn. Dit marginale effect kan erop duiden dat respondenten die aan de hoge geloofwaardigheid van de zender manipulatie zijn blootgesteld een lagere intentie hebben om informatie te zoeken dan die aan de lage manipulatie zijn blootgesteld. Dit effect is echter niet in de verwachte richting. Er is geen interactie effect gevonden tussen de twee onafhankelijke variabelen op de intentie tot het zoeken van informatie ($F(1,128) = .09$, *ns.*). Aangezien er geen significante interactie effecten zijn gevonden tussen de geloofwaardigheid en response efficacy manipulaties op de afhankelijke variabelen zal er dan ook niet verder worden gezocht naar een mediatie effect². Op basis van de gevonden resultaten kan hypothese 2 niet worden bevestigd.

Tabel 1 laat zien dat de gemiddelde scores op de intentie tot informatie zoeken en het daadwerkelijke informatie zoeken neigen naar een lage mate van zowel de intentie als het daadwerkelijke informatie zoekgedrag.

4.4 Beloningen van Facebook

Om hypothese 3a en 3b te toetsen zijn lineaire- en logistische regressieanalyses³ uitgevoerd. In deze analyses zijn meerdere onafhankelijke variabelen meegenomen om zo een volledig beeld te krijgen van het effect van de beloningen op de afhankelijke variabelen. De meegenomen onafhankelijke variabelen betreffen self-efficacy, ernst, kwetsbaarheid, persoonlijke relevantie, geloofwaardigheid, response efficacy en beloningen. Uit de analyses

² Voor zowel de geloofwaardigheid als de response efficacy zijn ieder aparte mediatie analyses uitgevoerd volgens de methode van Baron en Kenny (1986). De resultaten van deze analyses waren echter niet significant.

³ Voor de afhankelijke variabelen het daadwerkelijk nemen van zelfbeschermende maatregelen, de intentie tot het nemen van zelfbeschermende maatregelen en de intentie tot het zoeken van informatie zijn lineaire regressie analyses uitgevoerd. Voor de afhankelijke variabele het daadwerkelijke informatie zoeken zijn logistische regressie analyses uitgevoerd.

bleek dat de beloningen van Facebook geen significante voorspeller is voor het daadwerkelijk nemen van zelfbeschermende maatregelen ($\beta = -.08$, *ns.*). Wanneer de intentie tot het nemen van zelfbeschermende maatregelen als afhankelijke variabele werd genomen bleek de beloningen wel een significante voorspeller te zijn ($\beta = -.18$, $p < .01$). Dit toont aan dat hoe meer beloningen men ervaart aan het gebruik van Facebook hoe minder snel zij de intentie hebben om zelfbeschermende maatregelen te nemen. Hiermee is hypothese 3a dus gedeeltelijk bevestigd.

De beloningen die men ervaart aan het gebruik van Facebook bleken geen significante voorspeller te zijn voor zowel het daadwerkelijke informatie zoeken ($Wald = .49$, *ns.*) als de intentie tot informatie zoeken ($\beta = -.02$, *ns.*). Voor hypothese 3b is geen bewijs gevonden.

Uit tabel 1 blijkt dat er een significante positieve relatie bestaat tussen de beloningen die men ondervindt aan het gebruik van Facebook en het aantal Facebookvrienden dat men heeft ($r = .22$) evenals hoe vaak men actief is op Facebook ($r = .57$). Dit kan erop duiden dat hoe meer Facebookvrienden men heeft, des te meer beloningen men ervaart aan het gebruik van Facebook en hoe te vaker men actief is, des te meer beloningen men ervaart.

4.5 Persoonlijke relevantie

Om hypothese 4a en 4b te toetsen zijn wederom lineaire- en binaire regressieanalyses⁴ uitgevoerd. Tevens zijn hier de onafhankelijke variabelen self-efficacy, ernst, kwetsbaarheid, beloningen, geloofwaardigheid, response efficacy en persoonlijke relevantie meegenomen om zo een volledig beeld te krijgen van het effect van de persoonlijke relevantie op de afhankelijke variabelen. Persoonlijke relevantie bleek geen significante voorspeller te zijn voor zowel de daadwerkelijke zelfbeschermende maatregelen ($\beta = -.01$, *ns.*) als de intentie tot het nemen van zelfbeschermende maatregelen ($\beta = .08$, *ns.*). Hiermee is hypothese 4a niet bevestigd.

Persoonlijke relevantie bleek geen significante voorspeller te zijn voor het daadwerkelijke informatie zoeken ($Wald = 1.48$, *ns.*). Wel bleek dat persoonlijke relevantie een significante voorspeller is voor de intentie tot het zoeken van informatie ($\beta = .37$, $p = .01$). Dit kan erop duiden dat hoe hoger de persoonlijke relevantie van het risico is, hoe eerder men de intenties heeft om risico relevante informatie te zoeken. Hiermee is hypothese 4b dus gedeeltelijk bevestigd.

⁴ Voor de afhankelijke variabelen het daadwerkelijk nemen van zelfbeschermende maatregelen, de intentie tot het nemen van zelfbeschermende maatregelen en de intentie tot het zoeken van informatie zijn lineaire regressie analyses uitgevoerd. Voor de afhankelijke variabele het daadwerkelijke informatie zoeken zijn logistische regressie analyses uigevoerd.

5. Discussie

In dit onderzoek is onderzocht welke factoren van invloed zijn op het nemen van zelfbeschermende maatregelen en het zoeken van risicorelevante informatie. Er is onderzocht door middel van een experimenteel design wat het effect is van verschillende niveaus van response efficacy en geloofwaardigheid van de zender op het zoeken van risicorelevante informatie en het nemen van zelfbeschermende maatregelen. Tevens is nagegaan wat het effect is van de mate van beloningen die men ondervindt aan Facebook gebruik en de persoonlijke relevantie op het zoeken van risicorelevante informatie en het nemen van zelfbeschermende maatregelen.

5.1 Conclusies

Uit de resultaten bleek dat de manipulaties van de geloofwaardigheid van de zender en de response efficacy het gewenste effect hebben gehad in de verwachte richting. Echter is er wel een zwakke significante positieve correlatie gevonden tussen de beide gemeten variabelen geloofwaardigheid van de zender en response efficacy. Dit wijst er mogelijk op dat beide variabelen elkaar beïnvloeden of versterken.

Aangezien een hoge mate van risicoperceptie een voorwaarde is voor mensen om gemotiveerd te raken om informatie te zoeken en zelfbeschermende maatregelen te nemen (Kievik & Gutteling, 2011; Witte & Allen, 2000) is gepoogd om alle respondenten in een hoge mate van risicoperceptie te plaatsen. Uit de resultaten blijkt dat dit gelukt is.

5.1.1 Hypothese 1

Op basis van de literatuur werd in hypothese 1 verondersteld dat er een interactie-effect zou optreden, zodat een hogere mate van zowel geloofwaardigheid van de zender als een hoge mate van response efficacy zouden leiden tot een hogere mate van het nemen van zelfbeschermende maatregelen. In dit onderzoek is geen bewijs gevonden voor deze hypothese. Onderzoek van Witte en Allen (2000) en Kievik en Gutteling (2011) toonde aan dat een zekere mate van response efficacy nodig is voor het nemen van zelfbeschermende maatregelen. In dit onderzoek is er wel een significant verschil gevonden in scores tussen de lage en hoge response efficacy groep, echter blijkt dat de gemiddelden van beide groepen neigden naar noch mee eens, noch mee oneens. Ditzelfde geldt voor de gemiddelde scores op de variabele geloofwaardigheid van de zender. Renn en Levine (1989) toonde aan dat een hogere mate van geloofwaardigheid van een persoon leidt tot het eerder opvolgen van adviezen. Mogelijk waren de scores in de hoge geloofwaardigheid conditie en hoge response

efficacy conditie nog niet hoog genoeg om een interactie-effect tot stand te brengen om mensen aan te zetten tot het nemen van zelfbeschermende maatregelen.

De gemiddeldes van zowel de intentie tot als het daadwerkelijk nemen van zelfbeschermende maatregelen neigen allen naar een middelmatig tot hogere mate van het nemen van zelfbeschermende maatregelen ongeacht de manipulatie waaraan men is blootgesteld. Aangezien er ook geen significant verband is gevonden tussen de mate van risicoperceptie en het nemen van deze zelfbeschermende maatregelen zou dit erop kunnen duiden dat mensen vanuit zichzelf al geneigd zijn om deze zelfbeschermende maatregelen te nemen op Facebook onafhankelijk van beide manipulaties en de risicoperceptie.

5.1.2 Hypothese 2

Op basis van onderzoek van Kievik en Gutteling (2011) werd in hypothese 2 getoetst of er sprake is van een mediatie effect van informatie zoeken op de relatie tussen de onafhankelijke variabelen geloofwaardigheid van de zender en response efficacy en de afhankelijke variabelen die betrekking hebben op het nemen van zelfbeschermende maatregelen. De gevonden resultaten konden hypothese 2 niet bevestigen. Dit aangezien er geen significante interactie effecten zijn gevonden tussen de geloofwaardigheid en response efficacy manipulaties op de afhankelijke variabelen de daadwerkelijke zelfbeschermende maatregelen en het daadwerkelijke informatie zoeken.

Onderzoek (Kievik & Gutteling, 2011) toont aan dat een zekere mate van response efficacy nodig is voor het aanzetten van de individu tot het zoeken van risico relevante informatie. Zoals eerder al werd genoemd neigt de gemiddelde score van response efficacy naar 'noch mee eens, noch mee oneens'. Mogelijk is ook hier het geval dat de response efficacy in de hoge conditie groep niet hoog genoeg was om mensen te motiveren tot het zoeken van risico-informatie. Ditzelfde geldt wederom voor de gemiddelde score op de geloofwaardigheid. Dit heeft er mogelijk toe geleid dat er niet werd voldaan aan de voorwaarden voor mediatie van Baron en Kenny (1986).

Wel is er een matig tot sterke significante positieve correlatie gevonden tussen de intentie tot informatie zoeken en de intentie tot het nemen van zelfbeschermende maatregelen. Dit lijkt overeen te komen met de resultaten uit het onderzoek van Kievik en Gutteling (2011) die vonden dat respondenten die een hoge mate van risico relevante informatie zoeken vertoonden eerder de intentie hadden tot het nemen van zelfbeschermende maatregelen dan respondenten met een lage mate van risico-informatie zoekgedrag.

Tot slot is er nog een marginaal significant hoofdeffect gevonden van de

geloofwaardigheid van de zender op de intentie tot het zoeken van informatie. Dit is ook terug te zien in de gemiddelde scores van de intentie tot informatie zoeken. In de lage geloofwaardigheid manipulatie is deze hoger, dan in de hoge geloofwaardigheid manipulatie. Dit gevonden effect is echter niet in de verwachte richting. Mogelijk zou dit verklaard kunnen worden doordat alle respondenten zijn blootgesteld aan een hoge risicoperceptie boodschap. Uit het RISP model van Griffin, Dunwoody en Neuwirth (1999) blijkt dat mensen die een hoge risicoperceptie hebben een zekere informatie behoefte hebben met betrekking tot dat risico. Voor de groep in de hoge geloofwaardigheid conditie kan al aan deze informatie behoefte zijn voldaan, omdat zij al tips hebben gekregen van een geloofwaardige bron. Voor de lage geloofwaardigheid conditie geldt dit mogelijk niet, omdat de tips die zij kregen van een niet geloofwaardige bron kwam. Aangezien er een sterk positief verband is tussen de informatie behoefte en informatie zoeken (Griffin, Dunwoody & Neuwirth, 1999) kan dit verklaren waarom respondenten in de lage geloofwaardigheid conditie een hogere mate van informatie zoeken vertoonden.

Een mogelijke verklaring voor het niet vinden van significante resultaten voor hypothese 1 en 2 kan de optimistic bias zijn. De optimistic bias (Weinstein, 1980) houdt in dat mensen ervan uitgaan dat bepaalde risico's hen minder snel zullen overkomen dan anderen. Dit leidt tot onrealistisch optimisme met als gevolg dat men denkt dat het risico hen niet zal overkomen, waardoor ze niet geneigd zijn om zelfbeschermende maatregelen te nemen. Het effect treedt vooral op wanneer mensen hun eigen vermogen om met het risico om te gaan als zeer hoog inschatten of zelfs overschatten (Weinstein, 1980). Aangezien in dit onderzoek een zeer hoge mate van self-efficacy is gevonden onder de respondenten zou het mogelijk zijn dat dit tot een optimistic bias leidt met als gevolg dat men niet geneigd is om zelfbeschermende maatregelen te nemen. Dit komt overeen met de bevindingen van Ransdorp en Zondervan (2012) die luiden dat vooral jongeren de neiging hebben hun eigen vaardigheden om hun gegevens te beschermen overschatten.

5.1.3 Hypothese 3a, 3b, 4a & 4b

Hypothese 3a en 3b stellen dat een hogere mate van beloningen die men ervaart aan het gebruik van Facebook leidt tot het nemen van minder zelfbeschermende maatregelen en minder informatie zoekgedrag dan een lage mate van beloningen. Alleen voor hypothese 3a is gedeeltelijk bewijs gevonden. Het bleek dat respondenten die meer beloningen ervaren aan het gebruik van Facebook een lagere intentie hebben om zelfbeschermende maatregelen te

nemen. Deze resultaten zijn overeenkomstig met de literatuur (Rogers, 1975).

Hypothese 4a en 4b stellen dat een hogere mate van persoonlijke relevantie van het risico leidt tot het nemen van meer zelfbeschermende maatregelen en meer informatie zoekgedrag dan een lage mate van persoonlijke relevantie. Voor hypothese 4a is geen bewijs gevonden, maar hypothese 4b is wel gedeeltelijk bevestigd. Uit de resultaten blijkt dat persoonlijke relevantie een significante voorspeller is voor de variabele intentie tot informatie zoeken. Dit houdt mogelijk in dat hoe relevanter het risico is voor een individu hoe meer men de intentie heeft om risicorelevante informatie te zoeken.

De gemiddelde scores voor zowel beloningen als persoonlijke relevantie neigden allemaal naar 'noch mee eens, noch mee oneens' en verschilde niet significant tussen de manipulaties. Dit zou kunnen verklaren waarom er geen significante verbanden zijn gevonden met de afhankelijke variabelen, aangezien ook hier geldt dat een zekere mate van beloningen of persoonlijke relevantie nodig is voor het nemen van zelfbeschermende maatregelen (Rogers, 1975; Rothman & Kiviniemi, 1999) of het zoeken van informatie (Eagly & Chaiken, 1993). Mogelijk waren de gevonden effecten in dit onderzoek niet sterk genoeg om de hypothesen volledig te bevestigen.

5.2 Kanttekeningen

Bij deze studie kunnen enkele kanttekeningen worden geplaatst. Beginnend bij de steekproef kan geconcludeerd worden dat deze redelijk representatief is voor de gebruikers van Facebook. Relatief meer jongeren hebben namelijk de vragenlijst ingevuld. Opvallend was echter dat veel respondenten één of meer controlevragen fout hadden. Leeftijd was hierbij significant van invloed, zodoende dat ouderen respondenten meerdere fouten maakten dan jongere respondenten.

Desondanks dat de manipulaties het gewenste effect hebben gehad - de hoge en lage condities verschilden significant van elkaar in de voorspelde richting - bleek dat het effect van de hoge condities alsnog maar een score hadden van 'noch mee eens, noch mee oneens'. De waarden zijn dus wellicht niet hoog genoeg om mensen te motiveren informatie te zoeken en beschermende maatregelen te nemen.

Tevens zijn er in dit onderzoek hoge mate gevonden van risicoperceptie en self-efficacy. In andere onderzoeken (Kievik & Gutteling, 2011; Witte & Allen, 2000) is gebleken dat dit leidt tot het nemen van zelfbeschermende maatregelen, echter was dat in dit onderzoek niet het geval. Een reden hiervan kan zijn dat de mate van beloningen die Facebook met zich meebrengt een significante voorspeller is voor de intentie tot het niet nemen van

zelfbeschermende maatregelen. Wat er mogelijk op duidt dat de beloningen die men ondervindt aan het gebruik van Facebook zwaarder wegen dan de risico's die Facebook met zich meebrengt, waardoor men niet geneigd is zelfbeschermende maatregelen te nemen. Een andere mogelijke verklaring is het verschil in onderwerp. De studies van Kievik en Gutteling (2011) en Witte en Allen (2000) gaan in op onderwerpen met betrekking tot fysieke veiligheid, terwijl deze studie als onderwerp internetveiligheid heeft.

In dit onderzoek is ervoor gekozen de boodschap via een Facebook vriend te presenteren. Dit is vooral gedaan om ervoor te zorgen dat respondenten de boodschap serieus lezen, waar het bij een onbekende op Facebook namelijk net zo goed kan gaan om misplaatste reclame of iets dergelijks. In alle condities is de zender een Facebook vriend, zodoende dat eventuele effecten van sociale druk gelijk bleven. Twee typen reacties kwamen er echter op dit punt. Ten eerste gaven enkele respondenten in de lage geloofwaardigheid conditie aan de gekregen tips toch als geloofwaardig te beschouwen, omdat zij alleen bevriend zijn met goede vrienden op Facebook. Ten tweede waren er respondenten die opperden dat zij ook veel vage kennissen op Facebook hadden. Hier kan uit onttrokken worden dat een Facebook vriend voor iedereen dus een andere betekenis kan hebben wat invloed kan hebben gehad op de geloofwaardigheid scores.

Een beperking is dat enkele afhankelijke variabelen maar door één item worden gemeten. Dit zijn: de intentie tot het opvolgen van tips, de intentie tot het informatie zoeken en het daadwerkelijke informatie zoeken. Het gevaar is dat wanneer slechts één item gebruikt wordt dit kan leiden tot vertekende resultaten. Het daadwerkelijk informatie zoeken bestond uit het verplicht kiezen van een link waar men naartoe zou willen gaan. Aangezien de hele vragenlijst al gericht is op Facebook en de respondenten voornamelijk uit vrienden en kennissen van de onderzoeker bestonden bestaat de kans dat er sprake is geweest van sociale wenselijkheid. Het kiezen van een link is echter ook een moeiteloze en kosteloze keuze, direct na het krijgen van de informatie. Dit is wellicht niet representatief voor het informatie zoeken in hun dagelijks leven. De intentie om informatie te zoeken gaf dan ook maar een zwakke positieve significante correlatie met het daadwerkelijk informatie zoeken.

5.3 Aanbevelingen en implicaties

Betreffende implicaties voor de Alert Online campagnes kan een opmerking worden gemaakt op basis van de gevonden resultaten in dit onderzoek. Dit is dat de tips die door hen gegeven worden niet als nuttig worden beschouwd door de respondenten in het veilig gebruik van Facebook. Daar moet echter bij opgemerkt worden dat Alert Online meer op algemeen

internetgebruik waaronder Facebook is gericht, maar niet specifiek op Facebook alleen.

Ingaande op een kanttekening eerder genoemd, namelijk dat de hoge condities van de manipulaties alsnog maar een score van 'noch mee eens, noch mee oneens' hadden, kan worden aanbevolen dat in vervolg onderzoek aandacht besteed moet worden aan het maken van manipulaties die hogere mates van response efficacy en geloofwaardigheid bewerkstelligen. Wellicht door het aanpassen van de afbeelding.

Een andere kanttekening is dat enkele afhankelijke variabelen werden gemeten aan de hand van één item. Voor vervolgonderzoek kan dus aanbevolen worden om meerdere items voor deze schalen te genereren.

Uit de feedback van respondenten bleek dat velen hun persoonsgegevens op Facebook al redelijk beschermd hadden. In de vragenlijst is alleen gevraagd hoe respondenten op dat moment hun instellingen zouden invullen en er is dus geen rekening gehouden met hoe zij de instellingen hebben staan in hun werkelijke omgeving. Als dit meegenomen zou zijn dan zou dat wellicht vergelijkingen tussen huidige situatie en intentie tot het nemen van zelfbeschermende maatregelen kunnen geven.

Ten slotte dient er rekening gehouden te worden met het effect van de beloningen van Facebook die wellicht een negatief effect hebben op de intentie tot het nemen van zelfbeschermende maatregelen bij het opzetten van campagnes zoals Alert Online. Het kan voor vervolg onderzoek wellicht interessant zijn om hier verder mee te gaan.

6. Referenties

- Alert Online. (2012). Over Alert Online. Verkregen via <https://www.alertonline.nl/over-alert-online/>
- Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations. *Journal of personality and social psychology*, 51(6), 1173-1182.
- Berlo, D. K., Lemert, J. B., & Mertz, R. J. (1969). Dimensions for Evaluating the Acceptability of Message Sources. *Public Opinion Quarterly*, 33(4), 563-576.
- Computerworld. (2011). 50 Miljard redenen om Facebook te wantrouwen. Verkregen via <http://computerworld.nl/article/12556/50-miljard-redenen-om-facebook-te-wantrouwen.html>
- Deen, V. (2011). 10 Tips voor een veilig Facebook. Verkregen via <http://computerworld.nl/article/12683/10-tips-voor-een-veilig-facebook/1.html>
- Deursen, A.J.A.M. van. & Dijk, J.A.G.M. van. (2012). Trendrapport internetgebruik 2012. Een Nederlands en Europees perspectief. Enschede: Universiteit Twente.
- Eagly, A. H., & Chaiken, S. (1993). *The Psychology of Attitudes*. San Diego, Harcourt Brace.
- Facebook. (2012). Newsroom. Verkregen via <http://newsroom.fb.com/Key-Facts>
- Griffin, R.J., Dunwoody, S. & Neuwirth, K. (1999). Proposed Model of the Relationship of Risk Information Seeking and Processing to the Development of Preventive Behaviors. *Environmental Research Section*, 80, 230-245.
- Hoadley, C.M., Xu, H., Lee, J.J. & Rosson, M.B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications*, 9, 50-60.
- Huurne, E. ter. (2008). The Theoretical and Empirical Development of Fris: A Framework of Risk Information Seeking (Proefschrift). Verkregen via <http://doc.utwente.nl/59038/>
- Huurne, E. ter & Gutteling, J.M. (2008). Information needs and risk perceptions as predictors of risk information seeking. *Journal of Risk Research*, 11(7), 847-862.
- Joinson, A.N. (2008). 'Looking at', 'Looking up' or 'Keeping up with' People? Motives and Uses of Facebook. CHI '08 Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems.
- Kelly, S. (2008). Identity 'at Risk' on Facebook. Verkregen via http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm
- Kievik, M. & Gutteling, J.M. (2011). Yes we can: motivate Dutch citizens to engage in self-

- protective behavior with regard to flood risks. *Nat Hazards*, 59, 1475-1490.
- Leventhal, H. (1970). Findings and theory in the study of fear communications. In L. Berkowitz (Ed). *Advances in experimental social psychology* 119-186.
- Lewis, K. (z.j.). How Social Media Networks Facilitate Identity Theft and Fraud. Verkregen via <http://www.eonetwork.org/knowledgebase/specialfeatures/pages/social-media-networks-facilitate-identity-theft-fraud.aspx>
- Malhotra, Y. & Galletta, D. (2005). A multidimensional commitment model of volitional systems adoption and usage behavior. *Journal of Management Information Systems* 22(1), 117–151.
- Mariska Media. (2012). Identiteitsdiefstal op social media: “Ik ben gestolen!”. Verkregen via <http://www.mariskamedia.nl/wordpress/identiteitsdiefstal-op-social-media-ik-ben-gestolen/>
- McCroskey, J. C. (1966). Scales for the Measurement Of Ethos. *Speech Monographs*, 33(1), 65-72.
- Midden, C.J.H. & Huijts, N. (2009). The role of trust in the affective evaluation of novel risks: the case of CO2 storage. *Risk Analysis*, 29 (5), 743-751. DOI: 10.1111/j.1539 6924.2009.01201.x
- Oosterveer, D. (2012). Sociale media in Nederland: de cijfers. Verkregen via <http://www.marketingfacts.nl/berichten/de-laatste-social-media-cijfers-van-nederland>
- O'Reilly T. (2005) What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software. Verkregen op <http://oreilly.com/web2/archive/what-is-web-20.html>
- Purchase, I.F.H. (2004). What determines the acceptability of genetically modified food that can improve human nutrition? *Toxicology and Applied Pharmacology* 207(2), 11-15. Doi: 10.1016/j.taap.2004.12.025
- Ransdorp, Y. & Zondervan, I. (2012). Cyber Security Awareness: Een onderzoek naar kennis, bewustzijn en gedrag ten aanzien van cyber security. Amsterdam: Ministerie van Algemene Zaken/ NCTV.
- Renn, O., & Levine, D. (1989). Trust and Credibility in Risk Communication. In T. O'Riordan (Ed), *proceedings of the 1988 International Workshop on Risk Communication held at the KFA Jülich* (pp. 17-21).
- Reynolds, B.J. (2011). When the facts are just not enough: Credibly communicating about risk is riskier when emotions run high and time is short. *Toxicology and Applied Pharmacology* 254, 206–214. Doi: 10.1016/j.taap.2010.10.023

- Rogers, R.W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology*, 91(1), 93-114.
- Ropek, D., & Slovic, P. (2003). Risk Communication: A Neglected Tool in Protecting Public Health Risk, *Risk in Perspective*, 11(2).
- Rothman, A.J., & Kiviniemi, M.T. (1999). Treating People With Information: an Analysis and Review of Approaches to Communicating Health Risk Information. *Journal of the National Cancer Institute Monographs*, 25, 44-51.
- Sky News. (2012). Facebook Helps FBI Snare \$850m Cyber Gang. Verkregen via <http://news.sky.com/story/1024203/facebook-helps-fbi-snare-850m-cyber-gang>
- Sobel, M.E. (1982). Asymptotic confidence intervals for indirect effects in structural equation models. In S. Leinhardt (red.), *Sociological methodology 1982*. San Francisco: Jossey-Bass.
- Tuil, K. van. (2011). Privacy Facebook opnieuw onder vuur. Verkregen via <http://computerworld.nl/article/12557/privacy-facebook-opnieuw-onder-vuur.html>
- Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, 39, 806–820.
- Witte, K. (1992). Putting the fear back into fear appeals: The Extended Parallel Process Model. *Communication Monographs*, 59, 329-349.
- Witte, K., & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. *Health Education & Behavior*, 27(5), 591- 615. Doi: 10.1177/109019810002700506
- Witte, K., Cameron, K.A., McKeon, J.K., & Berkowitz, J.M. (1996). Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. *Journal of Health Community* 1(4), 317-342.

Appendix 1. Enquête Facebook

Beste Lezer,

Deze enquête bestaat uit een aantal vragen en stellingen. Het invullen zal ongeveer 5 tot 10 minuten duren. Deelname aan dit onderzoek is geheel vrijwillig en de resultaten uit dit onderzoek zullen geheel anoniem worden verwerkt.

U krijgt zo meteen eerst een aantal vragen en daarna krijgt u enkele berichten te lezen. Voor het slagen van dit onderzoek is het belangrijk dat u zich zo goed mogelijk probeert in te leven in de situatie en de enquête volledig invult.

Graag wil ik u verzoeken de volgende vragen in te vullen.

(Persoonsgegevens)

1. Wat is uw leeftijd?
2. Wat is uw geslacht? (man/vrouw)
3. Wat is uw hoogst afgeronde opleiding? (basisschool/mavo/havo/vwo/mbo/hbo/wo)
4. Heeft u een Facebook account? (Ja/Nee)

(Wanneer de respondent bij vraag 4 met 'nee' antwoord dan zal de enquête voor de respondent voorbij zijn. Deze krijgt dan een bericht te lezen dat dit het einde is van deze enquête en wordt dan hartelijk bedankt voor het invullen)

5. Hoe lang bent u al actief op Facebook? (minder dan 1 jaar, 1 t/m 2 jaar, 3 t/m 4 jaar, 5 jaar of meer)
6. Hoeveel Facebookvrienden heeft u? (minder dan 100, 100 t/m 250, 251 t/m 400, 401 t/m 550, 551 of meer)
7. Hoe vaak bent u actief op Facebook? (meerdere malen per dag/ gemiddeld 1 keer per dag/ gemiddeld 1 keer per wekelijks/ gemiddeld 1 keer per maand of minder)

Lees het onderstaande bericht goed door, hierna krijgt u hier enkele vragen over.

Ik ben gestolen!

De laatste jaren is er een sterke toename in het aantal gevallen van identiteitsdiefstal. Dit is te danken aan de populariteit van de sociale media als Facebook. Facebook is voor

identiteitsdieven een prachtig kanaal om persoonsgegevens te oogsten. Persoonsgegevens die op Facebook zijn geplaatst zijn meestal gemakkelijk te achterhalen. Met enkele gegevens als naam, adres, geboortedatum, woonsituatie en telefoonnummer kan een identiteitsdief al grote schade aanrichten in je leven. Dit door onder jouw naam producten te bestellen en met jouw gegevens toegang te krijgen tot jouw accounts bij websites of zelfs bij de bank. Wanneer dit eenmaal is gebeurd is het lastig om hier wat aan te doen en de gevolgen kunnen zeer ernstig zijn. De schatting is dat 1 op de 10 mensen hier slachtoffer van wordt.

(Na het lezen van dit bericht worden de respondenten random aan één van de vier condities toegekend)

Conditie 1

Na het lezen van bovenstaande bericht krijgt u enkele tips van een Facebookvriend. Deze Facebookvriend is zelf al vijf jaar lang dagelijks actief op Facebook. Hieronder vind u een afbeelding van zijn Facebook pagina. Bekijk de afbeelding goed, hierna krijgt u hier enkele vragen over.



The image shows a screenshot of a Facebook profile page for a user named Lyndon Lulof. The profile picture is a black silhouette of a person standing. The name 'Lyndon Lulof' is displayed below the profile picture. To the right of the name is a button labeled 'Vrienden'. Below the name, there are four small thumbnail images: a man's face, a person holding a sign, a yellow smiley face, and a world map. Below these thumbnails are the labels 'Vrienden 650', 'Foto's 80', 'Kaart', and 'Vind'. At the bottom of the page, there is a section for 'Activiteit Recent' with a sub-section for 'Lyndon vindt Imqur leuk.' The top of the page features the Facebook logo, a search bar with the text 'Zoek naar mensen, plaatsen en dingen', and a button labeled 'Vrienden zoeken'.

De tips die deze Facebookvriend u geeft om identiteitsdiefstal via Facebook te voorkomen worden door anderen als zeer nuttig ervaren. Hieronder staan de tips weergegeven.

- Plaats geen telefoonnummers of adresgegevens op Facebook
- Stel Facebook zo in dat je Facebook account niet opduikt in zoekmachines.
- Zorg dat alleen je Facebookvrienden je gegevens kunnen zien.

Conditie 2

Na het lezen van bovenstaande bericht krijgt u enkele tips van een Facebookvriend. Deze Facebookvriend is zelf al vijf jaar lang dagelijks actief op Facebook. Hieronder vindt u een afbeelding van zijn Facebook pagina. Bekijk de afbeelding goed, hierna krijgt u hier enkele vragen over.



The image shows a screenshot of a Facebook profile page for a user named Lyndon Lulof. The page features a blue header with the Facebook logo, a search bar, and a 'Vrienden zoeken' button. The main content area has a blue background with a world map and a silhouette of a person. Below the profile picture, the name 'Lyndon Lulof' is displayed, along with a 'Vrienden' button. The page also shows a gender indicator 'Man', a grid of photos, and a 'Vrienden 650' count. At the bottom, there is a 'Bericht' (Message) section with a text input field and a 'Foto' (Photo) section with a 'Recent' activity feed showing a post by Lyndon Lulof.

De tips die deze Facebookvriend u geeft om identiteitsdiefstal via Facebook te voorkomen worden door anderen als niet nuttig ervaren. Hieronder staan de tips weergegeven.

- Gebruik je gezond verstand en schakel bij twijfel een expert in.
- Bescherm je computer en houdt deze up-to-date
- Surf veilig.

Conditie 3

Na het lezen van bovenstaande bericht krijgt u enkele tips van een Facebookvriend. Deze Facebookvriend is nog maar twee maanden lid en is één keer per week actief is op Facebook. Hieronder vind u een afbeelding van zijn Facebook pagina. Bekijk de afbeelding goed, hierna krijgt u hier enkele vragen over.



De tips die deze Facebookvriend u geeft om identiteitsdiefstal via Facebook te voorkomen worden door anderen als zeer nuttig ervaren. Hieronder staan de tips weergegeven.

- Plaats geen telefoonnummers of adresgegevens op Facebook
- Stel Facebook zo in dat je Facebook account niet opduikt in zoekmachines.
- Zorg dat alleen je Facebookvrienden je gegevens kunnen zien.

Conditie 4

Na het lezen van bovenstaande bericht krijgt u enkele tips van een Facebookvriend. Deze Facebookvriend is nog maar twee maanden lid en is één keer per week actief is op Facebook. Hieronder vind u een afbeelding van zijn Facebook pagina. Bekijk de afbeelding goed, hierna krijgt u hier enkele vragen over.



De tips die deze Facebookvriend u geeft om identiteitsdiefstal via Facebook te voorkomen worden door anderen als niet nuttig ervaren. Hieronder staan de tips weergegeven.

- Gebruik je gezond verstand en schakel bij twijfel een expert in.

- Bescherm je computer en houdt deze up-to-date
- Surf veilig.

8. Wat werd in het voorgaande bericht niet genoemd als manier waarop een identiteitsdief via Facebook grote schade kan aanrichten in uw leven? (Door onder jouw naam producten te bestellen/ Met jouw gegevens toegang krijgen tot je accounts bij websites of bij de bank/ Een profiel aanmaken op een andere sociaalnetwerksite en zich voordoen als jou)

9. Welke persoonlijke informatie kon u terugvinden in de Facebook pagina van de Facebookvriend die u de tips gaf? (geboortedatum/Adres/Telefoonnummer/geen van bovenstaande)

(Geloofwaardigheid van de zender)

10. Geef voor ieder van de onderstaande stellingen aan in hoeverre u het hiermee eens bent.

- Ik vond de Facebookvriend van wie ik de tips kreeg geloofwaardig overkomen.
- Ik denk dat de Facebookvriend van wie ik de tips kreeg veel ervaring heeft met Facebook.
- Ik denk dat de Facebookvriend van wie ik de tips kreeg veel kennis heeft over Facebook.
- Ik denk dat de Facebookvriend van wie ik de tips kreeg zeer competent is in het gebruik van Facebook.

1 = helemaal mee oneens tot 5 = helemaal mee eens

(Beloningen van Facebook)

11. Geef aan in hoeverre u het eens bent met de volgende stellingen.

- Facebook is voor mij een belangrijke manier om in contact te blijven met mijn vrienden.
- Facebook is voor mij een belangrijke manier om mijn vrienden te laten weten wat ik doe.
- Facebook biedt veel voordelen voor mij
- Facebook is voor mij een belangrijke manier om mijn oude vrienden op te zoeken.

1 = helemaal mee oneens tot 5 = helemaal mee eens

(Persoonlijke relevantie)

12. Hoe belangrijk is het risico van identiteitsdiefstal via Facebook in uw dagelijks leven?

Geef voor ieder van de onderstaande stellingen aan in hoeverre u het hiermee eens bent.

- Het risico heeft geen invloed op mijn leven.
- Het risico is voor mij persoonlijk relevant.
- Het risico speelt een belangrijke rol in mijn dagelijkse leven, omdat ik een Facebook

account heb.

- Ik heb zelf in mijn dagelijkse leven met het risico te maken.

(Self-efficacy & Response efficacy)

13. Geef aan in hoeverre u het eens bent met de volgende stellingen over de aanbevolen tips om identiteitsdiefstal via Facebook te voorkomen

- Ik kan gemakkelijk de gegeven tips zelf uitvoeren.
- Ik ben niet in staat om de gegeven tips zelf uit te voeren.
- Ik heb de vaardigheden om de gegeven tips zelf uit te voeren.
- De gegeven tips zijn nuttig om identiteitsdiefstal via Facebook te voorkomen.
- De gegeven tips zijn effectief om identiteitsdiefstal via Facebook te voorkomen.
- Als ik de gegeven tips uitvoer, dan zal identiteitsdiefstal via Facebook mij minder snel overkomen.

1 = helemaal mee oneens tot 5 = helemaal mee eens

(Risicoperceptie)

14. Geef voor ieder van de onderstaande stellingen aan in hoeverre u het hiermee eens bent.

- Ik geloof dat identiteitsdiefstal via Facebook schadelijk kan zijn.
- Ik loop het risico dat identiteitsdiefstal via Facebook mij overkomt.
- Het is mogelijk dat ik een keer slachtoffer wordt van identiteitsdiefstal via Facebook.
- Ik geloof dat identiteitsdiefstal via Facebook ernstige gevolgen kan hebben.
- De kans is aanwezig dat identiteitsdiefstal via Facebook mij een keer overkomt.

1 = helemaal mee oneens tot 5 = helemaal mee eens

(Het nemen van zelfbeschermende maatregelen)

Nu worden er vier instellingsmogelijkheden weergegeven zoals deze ook op Facebook terug te vinden zijn. Geef bij iedere optie aan hoe u deze op dit moment zou instellen.



Privacyinstellingen en -functies

15. Wie kan berichten zien op je tijdlijn waarin jij bent getagd?

16. Wie kan zien wat anderen op je tijdlijn plaatsen?

17. Wie kan je zoeken via het e-mailadres of telefoonnummer dat je hebt opgegeven?

1 = Iedereen, 2 = vrienden van vrienden, 3 = vrienden, 4 = alleen ik

18. Wil je dat wanneer iemand zoekt op jou naam in een zoekmachines zoals Google of Bing

een link naar jouw Facebook tijdelijk wordt weergegeven?

1 = Ja, 2 = Nee

19. Geef bij onderstaande stellingen aan wat u zou doen als u nu uw persoonsgegevens opnieuw moet invoeren op Facebook.

- Ik zou mijn adresgegevens plaatsen op Facebook.
- Ik zou mijn telefoonnummer plaatsen op Facebook.
- Ik zou mijn woonsituatie plaatsen op Facebook.
- Ik zou mijn geboortedatum plaatsen op Facebook.

1 = helemaal mee oneens tot 5 = helemaal mee eens

20. Geef voor ieder van de onderstaande stellingen aan in hoeverre u het hiermee eens bent.

- Ik ga op zoek naar informatie over hoe ik mijn identiteit op Facebook beter kan beveiligen tegen identiteitsdiefstal.
- Ik ben van plan om de gegeven tips om identiteitsdiefstal op Facebook te voorkomen uit te voeren.
- Ik verander vaak mijn privacy instellingen op Facebook.
- Ik ga akkoord met de default privacy instellingen die Facebook zelf biedt.

1 = helemaal mee oneens tot 5 = helemaal mee eens

(Informatiezoekgedrag)

21. U krijgt nu vier weblinks te zien, kies de weblink van de site waar u graag naar toe zou willen.

- 1) <http://www.autoweek.nl/autonieuws/>
- 2) <http://veiligfacebook.nl/10-tips-voor-een-veilig-facebook/>
- 3) <http://www.fashionmagazine.com/fashion-news/>
- 4) <http://www.recepten.nl/nieuwe-recepten/>

Dit is het eind van de enquête.

Hartelijk bedankt voor het invullen!