Bacheloropdracht

Welke criteria nemen personen in overweging bij het beoordelen van een phishing e-mail?

Door Lars Mol
S0150894
23-9-2014

1. Inhoudsopgave

2. Voorwoord

Dit rapport omvat een onderzoek naar de criteria die personen in overweging nemen bij het beoordelen van e-mail, meer in het specifiek, phishing e-mail.
Deze opdracht is uitgevoerd ter afsluiting van mijn bachelor European Public Administration aan de Universiteit Twente.
Ik wil Hans Heerkens, Marianne Junger en Elmer Lastdrager bedanken voor de begeleiding geboden in het proces wat heeft geleid tot het tot stand komen van dit rapport.
Het rapport zoals dat hier voor u ligt is het resultaat van analyses gedaan in de zomer van 2013, en is opgeleverd in de staat waarin het nu verkeerd in september 2014.

3. Samenvatting

In dit onderzoek wordt de volgende onderzoeksvraag behandeld: Welke criteria nemen personen in overweging bij het beoordelen van een phishingmail? Voor het beantwoorden van deze vraag is een hardop denk onderzoek uitgevoerd met 24 werknemers van de Universiteit Twente, werkzaam binnen verschillende afdelingen.

Vanuit de theorie blijkt dat vertrouwen een grote rol speelt bij het al dan niet overgaan tot online transacties en het overhandigen van financiële gegevens. Het vertrouwensmodel van Mayer leert ons dat welwillendheid, bekwaamheid en integriteit belangrijke factoren zijn van vertrouwen. Tevens spelen uiterlijk design en informatiedesign en structuur een grote rol voor online betrouwbaarheid.

Op basis van deze achtergrondtheorie, zijn inhoudelijke, estetische, organisatorische en veiligheidscodes opgesteld, en is er door middel van het coderen en analyseren van hardopdenkprotocollen gekeken welk van deze criteria door de respondenten werden meegenomen bij het beoordelen van een vanuit de naam van de ING bank verstuurde phishing e-mail.

Voor elk van de opgestelde inhoudelijke, estetische, organisatorische en veiligheidscodes, is geconcludeerd dat respondenten deze kenmerken in overweging namen bij het beoordelen van phishingmail. Naast deze bevindingen gaat het onderzoek nog een stuk verder en kijkt of variatie in de mate van dwang van de e-mail zorgt voor verschillen in de kenmerken die respondenten in overweging nemen. Hieruit is naar voren gekomen dat bij meer dwang, efficiëntie, veiligheid en identiteit meer in overweging worden genomen, tevens bleek dat respondenten bij een hogere mate van dwang meer gedachten uitspraken en eerder geneigd waren om een keuze te maken.

Tot slot is het verschil tussen 3 groepen respondenten onderzocht, namelijk de respondenten die expliciet de keuze maken niet op de e-mail in te gaan, respondenten die geen explicitiete keuze maken, en respondenten die besluiten wel op de e-mail in te gaan. Hier is duidelijk geworden dat respondenten die geen keuze maken en besluiten wel op de e-mail in te gaan, veiligheidsaspecten niet in overweging nemen bij het beoordelen van de e-mail. Het lijkt er dus op dat deze respondenten geen veiligheidsproblemen waarnemen.

4. Introductie

Nieuwe technologieën zoals het internet hebben de manieren waarop onze samenleving communiceert, deelneemt in recreatie en waarop bedrijven werken radicaal verandert (Nhan et al.,2009). De snelheid en het gemak dat internet ons biedt heeft ervoor gezorgd dat internet een belangrijk medium is geworden waar wij met zijn allen gebruik van maken.
Nieuwe technologieën zoals het internet openen tevens nieuwe deuren voor criminelen.
Er zijn vele manieren waarop misbruik gemaakt wordt van het internet. Enkele veelgebruikte vormen van ongewenst gedrag en criminaliteit die voorkomen op het internet zijn (Nhan et al., 2009):

1) Spamming: Het versturen van ongewenste e-mails naar miljoenen e-mail adressen.
2) Het aannemen van een valse identiteit door het vervalsen van websites, e-mailadressen, of ip adressen, hierdoor worden internetgebruikers misleid, dit heet ook wel phishing.
3) Het met virussen infecteren van computers om informatie te stelen
4) Ontduiking van spamfilter technologie om toch spam te kunnen verzenden

Alle criminele activiteiten op het internet gezamenlijk, vallen onder het kopje cybercrime.
Of deze vormen van ongewenst gedrag en criminaliteit nu social engineering, bedrog, vertrouwentrucs, cognitieve vertekening of oplichting worden genoemd, het concept van het uitbuiten van naïviteit en vertrouwen van personen is vandaag de dag net zo gangbaar als een lange tijd geleden (McAfee, 2008). Sterker nog, internet vergemakkelijkt om verscheidene redenen de mogelijkheid om anderen te bedriegen (Grazioli & Wang, 2001):

1) Internet maakt het gemakkelijker om de identiteit van producten, individuen en organisaties te vervalsen.
2) De kosten om een, goed, betrouwbaar uitziend bedrijf op te zetten zijn door internet afgenomen.
3) Internet zorgt ervoor dat bedriegers een groter bereik hebben en dus toegang hebben tot meer potentiële slachtoffers.
4) Internet heeft het begaan van criminaliteit gemakkelijker gemaakt, niet alleen in termen van anonimiteit, maar ook door de verschillen in jurisdictie tussen landen, die vervolging van daders vaak bemoeilijken.

Waar internet de mogelijkheden tot bedrog vergroot, probeert antivirus software de gebruikers van internet bescherming te bieden, echter zolang mensen van nature vertrouwend zijn, en gezien het feit antivirus software vaak volgt op de criminele activiteiten om deze in te perken, zal er ruimte zijn voor ongewenst gedrag en criminaliteit op het internet. Het moge duidelijk zijn dat internetcriminaliteit door de jaren heen groter is geworden en dat er veel vormen van internet criminaliteit zijn. Het is onmogelijk om in één scriptie alle vormen van internet criminaliteit goed uit te leggen, laat staan naar allemaal onderzoek te doen. Dit onderzoek zal zich zodoende beperken tot slechts één van de vormen van cybercrime, namelijk phishing. De naam phishing komt van fishing, het uitwerpen van een lokaas, in de hoop dat enkelen zullen toehappen. Phishing is een vorm van internetfraude die bestaat uit het oplichten van mensen, door ze te lokken naar een valse website die een kopie is van de echte website (Tsow & Jakobsson 2007), om ze daar, nietsvermoedend, te laten inloggen met hun inlognaam en wachtwoord, of andere gegevens. Hierdoor verkrijgt de fraudeur deze gegevens met alle gevolgen van dien.
Phishing is een groeiend probleem, waar in heel 2010 de schade door phishing in Nederland 9,8 miljoen bedroeg, is dit gestegen tot 11,2 miljoen in enkel het eerste half jaar van 2011 (NOS, 2011)
Phishing e-mails vragen vaak om het ondernemen van een actie, bijvoorbeeld inloggen op een nagemaakte website, maar kunnen zelfs al schadelijk zijn wanneer een lezer enkel op een link klikt. Soms is het kwaad dan al geschied en is er al een virus geïnstalleerd.

Er zijn verscheidene onderzoeken gedaan naar waarom phishing werkt, bijvoorbeeld de studie van Nhan, Kinkade & Burns getiteld "*finding a Pot of gold at the End of an Internet Rainbow"* en de studie "*Why phishing works"* van Dhamija, Tygar & Hearst in 2006.
De reeds aanwezige studies betreffende phishing, focussen zich voornamelijk op websites en niet op e-mails, tevens ligt de focus vaak op de uitkomst, vallen mensen wel of niet voor phishing.
Er zijn studies die ons vertellen dat anti-phishing tekens en waarschuwingen vaak niet werken(nhan et al., 2009).
De manier waarop het phishing probleem aangepakt wordt is op dit moment nog niet optimaal, natuurlijk zijn er op elk e-mailsysteem spamfilters en is er de don't get phished reclamecampagne van de Nederlandse vereniging van banken.
Door middel van dit onderzoek is getracht de stap voorafgaand aan de activiteit op de phishing websites te onderzoeken. Het doel van de huidige studie is om te onderzoeken hoe mensen phishing e-mails lezen, wat ze er bij denken en wat hen opvalt. De focus ligt zodoende meer op het proces voorafgaand aan de uitkomst dan de uitkomst zelf. Door dit proces duidelijker in beeld te brengen kan er gewerkt worden naar een gerichtere bestrijding van phishing door middel van nieuwe interventies en betere voorlichting.
De onderzoeksvraag in dit rapport luidt dan ook als volgt: *Welke criteria nemen personen in overweging bij het beoordelen van een phishing e-mail?* Om deze vraag te beantwoorden, is er data verzameld. Werknemers van de Universiteit Twente hebben deelgenomen in hardop denk sessies waarin zij in een zo natuurlijk mogelijke setting een phishing e-mail hebben gelezen en daarop al hun gedachten hardop uit hebben gesproken.
In de hoofdstukken die volgen zal allereerst de theorie dat gebruikt is binnen dit onderzoek worden doorgenomen en zullen de onderzoeksvragen om tot een beantwoording van de hoofdvraag te komen, worden uiteengezet, om vervolgens de onderzoeksopzet uiteen te zetten en tot slot de resultaten en conclusies te presenteren.

5. Theorie

Dit hoofdstuk stelt zich ten doel de bruikbare theorie omtrent phishing uiteen te zetten, om zodoende op basis van deze theorie een codeerschema op te zetten aan de hand waarvan de vraag *"Welke criteria nemen personen in overweging bij het beoordelen van een phishing e-mail?"* beantwoord kan worden.
Zoals eerder al gezegd is phishing een vorm van oplichting. Oplichting zal alleen succesvol zijn indien de oplichter het vertrouwen krijgt van de opgelichte, zodoende zal een groot deel van de theorie gaan over vertrouwen. Allereerst wordt uitgelegd wat vertrouwen nou eigenlijk is, om vervolgens elementen en kenmerken die zorgen dat mensen vertrouwen hebben uit te leggen. Om te kunnen begrijpen waarom mensen vallen voor phishing e-mails moet allereerst begrepen worden waarom vertrouwen belangrijk is. Een gebrek aan vertrouwen is herhaaldelijk geïdentificeerd als een van de grootste obstakels voor mensen om niet mee te gaan in e-commerce en online transacties, en overhandiging van financiële of persoonlijke data (Wang & Emurian, 2005).

5.1 Wat is vertrouwen

Vertrouwen wordt in het Oxford Engelse woordenboek (1971) gedefinieerd als "*confidence in or reliance on some quality or attribute of a person or thing, or the truth of a statement".* Vertrouwen kan worden omschreven als een complexe relatie tussen verschillende actoren, of partijen, immers, in elke vertrouwende relatie bestaan er twee specifieke partijen, namelijk de partij die het vertrouwen geeft (de vertrouwer), en een partij die het vertrouwen krijgt (de vertrouwde), deze twee partijen kunnen bijvoorbeeld personen en organisaties omvatten. Vertrouwen is geen gegeven. Het is niet te allen tijde zomaar aanwezig, het ontwikkelen van vertrouwen is gebaseerd op het vermogen van de vertrouwde om in het belang van de vertrouwende te werken. Het omvat kwetsbaarheid, daar het alleen nodig is in een omgeving die onveilig en risicovol is, de vertrouwende partij moet zich kwetsbaar willen opstellen en neemt bij het vertrouwen het risico om iets te verliezen dat belangrijk voor hem is. Om dit daadwerkelijk te doen, is het van essentieel belang dat de vertrouwende erop moeten vertrouwen dat de vertrouwde deze kwetsbaarheid niet uitbuit (Wang & Emurian, 2005). Zodoende leidt vertrouwen tot acties, welke actie is volkomen afhankelijk van de situatie. Iemand leent bijvoorbeeld zijn geld aan een vriend, omdat hij erop vertrouwt dat deze dit later terug zal betalen. Vertrouwen is een subjectieve aangelegenheid, het wordt direct beïnvloed door individuele verschillen en situationele factoren. Verschillende scenario's zorgen allemaal voor een verschillend niveau van vertrouwen (Wang & Emurian, 2005). Een actor is niet per definitie betrouwbaar of onbetrouwbaar, vertrouwen is een continuüm (Mayer et al. 1995).
Online vertrouwen komt in veel overeen met vertrouwen in het algemeen, echter zijn er een paar verschillen, bij online vertrouwen gaat het niet alleen om vertrouwen in de persoon, maar ook om vertrouwen in de technologie (Wang & Emurian, 2005). Het internet is complex en biedt anonimiteit. Dit maakt het mogelijk dat mensen zich onvoorspelbaar kunnen gedragen. Online kunnen een ieders acties, soms, door middel van het installeren van bijvoorbeeld een trojan horse, zelfs zonder zelf iets in te vullen, verzameld worden om later gebruikt te worden. Consumenten zijn op internet vooral kwetsbaar voor het verlies van geld en het verlies van privacy (Wang & Emurian, 2005).

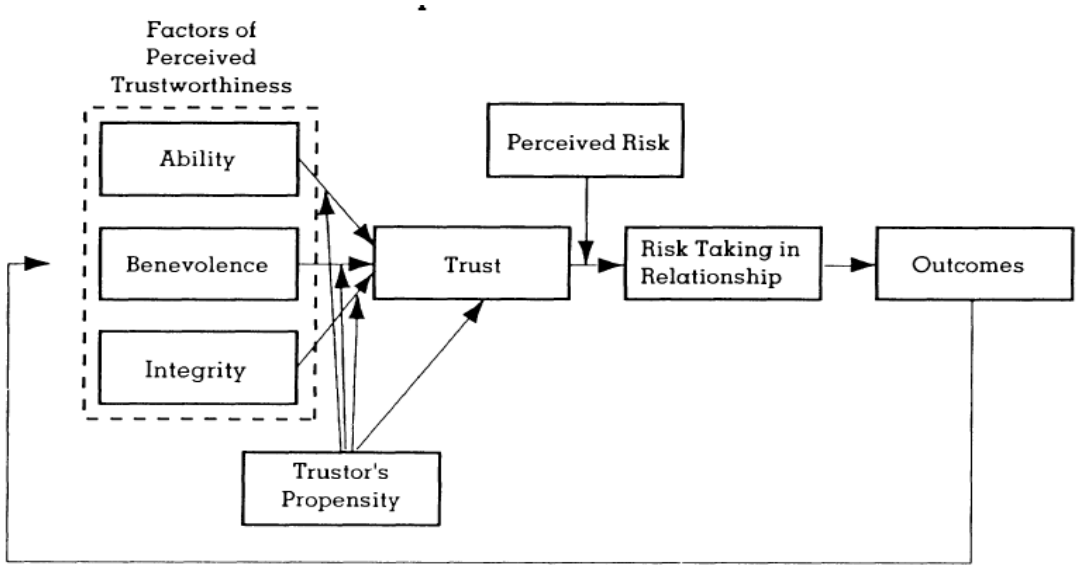
5.2 Vertrouwen en marketing

Nu duidelijk is dat vertrouwen een complexe relatie tussen twee partijen is, is het van belang om te weten wat voor factoren er voor zorgen dat de vertrouwende de vertrouwde al dan niet betrouwbaar vindt. Om deze factoren te kunnen onderscheiden is gekeken naar marketingtheorieën, marketingtheorieën proberen te begrijpen hoe consumenten kunnen worden overtuigd tot het ondernemen van een actie, bijvoorbeeld tot het kopen van een product, of een lidmaatschap van een organisatie.
Theorie vanuit de marketing stelt dat wederkerigheid, consistentie, sociale validatie, het iemand al dan niet wenselijk of leuk vinden, autoriteit en schaarste een grote rol spelen bij marketing (Cialdini, 2001).
Voor het verkrijgen van vertrouwen om zodoende iemand te overtuigen wordt vaak ingespeeld op deze basiskenmerken van menselijk gedrag (Cialdini, 2001).
Wederkerigheid kan hierin omschreven worden als, wanneer jij wat voor mij doet, doe ik wat voor jou. Consistentie heeft betrekking op het gelijk blijven van een verhaal, wanneer iemand elke keer een ander verhaal vertelt met betrekking op dezelfde gebeurtenis, zal dit het vertrouwen niet ten goede komen.
Personen zijn tevens gevoelig voor sociale validatie, wanneer er gezegd wordt dat veel anderen iemand al voor gingen, zal dit leiden tot het sneller volgen van nieuwe individuen.
Ook het iemand wenselijk of leuk vinden speelt een rol, wanneer de vertrouwende de vertrouwde leuk of wenselijk vind, zal hij de vertrouwde meer vertrouwen dan wanneer dit niet het geval is.
Mensen zijn tevens erg gevoelig voor autoriteit, indien een persoon autoriteit uitstraalt, zal het voor hem/haar makkelijker worden om andere personen te overtuigen, dit omwille van het legitieme aura van autoriteit (Cialdini, 2001).
Ook schaarste speelt een belangrijke rol in marketing en overtuigen, indien mogelijkheden en producten minder beschikbaar worden, verlangt de mens er steeds meer naar (Cialdini, 2001).
De theorie van Cialdini heeft in dit onderzoek geholpen met het selecteren van een zo goed mogelijke phishingmail, verstuurd vanuit een organisatie met autoriteit.

5.3 Een model van vertrouwen, organisatorische kenmerken van vertrouwen

De eerder genoemde voorbeelden vanuit de marketing zijn niet de enige factoren die vertrouwen kunnen beïnvloeden, in 1995 is door Mayer et al. een model van vertrouwen opgesteld, wat de meer persoonlijke factoren omtrent vertrouwen benadrukt, dit model is te zien in figuur 1.

Figuur 1: Model van vertrouwen (Mayer et al., 1995)



Volgens dit model bepalen drie factoren de gepercipieerde betrouwbaarheid, namelijk: bekwaamheid, welwillendheid en integriteit. Bekwaamheid is van belang bij vertrouwen in die zin dat een persoon op een bepaald technisch gebied zeer bekwaam kan zijn, maar op een ander gebied niet. Dit maakt vertrouwen domeinspecifiek (Mayer et al., 1995). Welwillendheid is de mate waarin de vertrouwde goed wil doen aan degene die hem vertrouwt, zonder dat er een egocentrisch motief is.
Welwillendheid suggereert dat de vertrouwde een specifieke verbintenis heeft met de vertrouwende (Mayer et al., 1995). De relatie tussen integriteit en vertrouwen omvat het feit dat de vertrouwende het beeld heeft dat de vertrouwde een set principes aanhangt die de vertrouwende acceptabel vindt (Mayer et al., 1995). Deze kenmerken zijn niet voor iedereen gelijk, of iemand vertrouwen heeft, is afhankelijk van aangeboren neiging, de ene persoon is van nature eerder geneigd iemand te geloven en vertrouwen dan de ander.
Aangeboren neiging heeft tevens invloed op in welke mate een persoon iemand bekwaam, welwillend en integer acht en heeft zo een invloed op vertrouwen. De factoren bekwaamheid, welwillendheid, integriteit en de invloed van de aangeboren neiging zorgen voor een bepaald niveau van vertrouwen, door het bespeurde risico af te wegen tegen de mate van vertrouwen zal een individu overgaan tot het ondernemen van een actie en daarmee het nemen van een risico, of niet (Mayer et al., 1995)
De uitkomsten die hieruit voortkomen worden meegenomen in een volgende afweging die een persoon maakt. Bijvoorbeeld indien een persoon al een keer voor een bepaalde vorm van phishing of ander bedrog is gevallen, zal dit zorgen voor een hogere mate van alertheid bij een volgende afweging. Indien een persoon juist altijd goede ervaringen heeft, misschien juist voor minder alertheid bij een volgende afweging. De hiergenoemde determinanten geven kenmerken van een organisatie weer waarop individuen deze organisatie kunnen beoordelen. Omwille van deze reden, zulle deze determinanten van vertrouwen meegenomen worden in het onderzoek als variabelen.

5.4 Ander onderzoek betreffende Phishing, de esthetische kenmerken

Nu duidelijk is wat voor marketing factoren en meer persoonlijke factoren invloed kunnen hebben op het vertrouwen, is het belangrijk om te kijken wat voor belangrijke aspecten waar individuen op lijken te letten bij het lezen van phishing gerelateerde zaken zijn voortgekomen uit eerder onderzoek. Zodat deze eveneens als determinanten kunnen worden meegenomen in ons codeerschema in dit onderzoek.

Zoals eerder al gezegd, is er tot op heden geen onderzoek gedaan naar de wijze waarop mensen phishing e-mails lezen, onderzoek wat hier het dichtste bijkomt, is het onderzoek van Dhamija, Tygar & Hearst, betreffende de manier waarop mensen (phishing) websites beoordelen op betrouwbaarheid (Dhamija, Tygar & Hearst, 2006) een andere interessante studie is de studie van Egelman, Cranor & Hong, betreffende web browser phishing waarschuwingen (Egelman, Cranor & Hong, 2008).

Zo blijkt uit de studie van Nhan, Kinkade & Burns (2009) dat men zich in fraudulente e-mail vaak voor doet als een persoon met autoriteit, denk aan een arts, advocaat of bankier, tevens worden fraudulente e-mails vaak verstuurd uit naam van banken, politieke organisaties, of andere organen met een hoge legitimiteit (Nhan, Kinkade & Burns, 2009). Hieruit blijkt dat de marketingtechniek omtrent het voordoen als een orgaan met autoriteit dus ook binnen internet criminaliteit gebruikt wordt.

Het onderzoek van Dhamija, Tygar & Hearst maakt ons duidelijk dat phishing wel degelijk een groot probleem is: sommige phishing aanvallen hebben tot 5% van hun ontvangers zo ver gekregen om gevoelige informatie in te vullen op foute websites. Ongeveer 2 miljoen gebruikers hebben informatie aan phishing websites doorgegeven wat resulteerde in $1.2 miljard verlies voor Amerikaanse banken en creditcard bedrijven in 2003 (Dhamija, Tygar & Hearst, 2006).

Betreffende phishing websites is er een gebrek aan kennis over veiligheid en veiligheids indicatoren. Er wordt veel gebruik gemaakt van visuele misleiding, door middel van plaatjes van werkelijke hyperlinks te gebruiken om iemand naar een verkeerde site te leiden, of door een perfecte kopie te maken van de werkelijke website.
Op websites lijken de belangrijkste seintjes voor een bezoeker de manier van spreken, spelfouten en andere tekenen van onprofessioneel design (Dhamija, Tygar & Hearst, 2006).
Ander onderzoek wijst uit dat de grootste factor online voor de mate van betrouwbaarheid uiterlijk design is, gevolgd door informatie design/structuur (Tsow & Jakobsson 2007).

5.5 Besliskunde

Naast deze theorie over vertrouwen speelt de besliskunde een rol in dit onderzoek.
Een beslissing is het maken van een keuze uit verschillende alternatieven.
In het geval van phishing en dit onderzoek kunnen op vele momenten beslissingen worden genomen:

1) Open ik de e-mail?
2) Lees ik de e-mail door?
3) Klik ik op de gegeven link?
4) Vul ik mijn gegevens in op de site?
5) Klik ik op bevestigen en verstuur ik mijn gegevens?

Door gebruik te maken van de hardop denk methode, verder uitgelegd in hoofdstuk 5, onderzoeksopzet & dataverzameling, beperkt het onderzoek zich tot de derde, vierde en vijfde beslissing, dit omdat de eerste en tweede beslissing vast liggen in het experiment, de opdracht voor elke deelnemer is immers om de mail hardop door te lezen. Bij elk van deze beslissingen kunnen

mensen kiezen tussen de alternatieven: doe ik het wel, of doe ik het niet. Welk van deze alternatieven gekozen wordt, wordt bepaald door een aantal kenmerken (ofwel attributen) (Heerkens, 2003), deze attributen zullen verderop in het onderzoek vastgesteld worden en spelen uiteindelijk de hoofdrol in het analyseren van de e-mails, de respondenten die de e-mail te lezen krijgen, zullen immers een beslissing nemen afgaande op in hoeverre ze deze attributen als positief ofwel negatief ervaren.
Zullen er grotendeels negatieve gevoelens bij de e-mail zijn, zal een respondent waarschijnlijk sneller geneigd zijn niet op de e-mail in te gaan dan wanneer de gevoelens overwegend positief zijn.
Tevens is het van belang dat voor een respondent het ene attribuut zwaarder kan wegen dan een ander attribuut. Bijvoorbeeld: de ene respondent, Respondent I hecht veel waarde aan spelling, de spelling in de e-mail is goed, dus respondent I besluit op de e-mail in te gaan, waar een andere respondent, respondent II waarde hecht aan bekwaamheid van het handelen van een organisatie, deze blijkt door de respondent als slecht te worden ervaren en dus besluit respondent II niet op de e-mail in te gaan.
Door het afwegen van de attributen komt de lezer van de phishing e-mail tot een besluit: wel ingaan op de phishing e-mail, of niet ingaan op de phishing e-mail.

5.6 Hypothesen

In deze paragraaf zijn op basis van de eerder gegeven theoretische concepteneen aantal hypothesen opgesteld worden die bevestigt ofwel ontkracht zullen worden gedurende de analyse.
De theorie heeft uitgewezen dat vertrouwensaspecten (Mayer et al., 1995), de manier van spreken, spelling en andere vormen van uiterlijk en inhoudelijk design(Dhamija, Tygar & Hearst, 2006; Tsow & Jakobsson, 2007) van belang zijn bij het beoordelen van fraudulente websites. Dit onderzoek gaat er vanuit dat dit voor phishing e-mails eveneens het geval is.
Op basis van de verzamelde informatie zullen de opgestelde hypothesen getoetst worden op een beschrijvend niveau, in vervolg onderzoek is het eventueel mogelijk om meer verklarend te werk te gaan.

Hypothese 1: Respondenten besteden tijd aan het lezen van de afzender en aanhef van de mail en spreken hier gedachten bij uit.

Hypothese 2: Respondenten nemen esthetische kenmerken in overweging bij het beoordelen van e-mails.

Hypothese 3: Respondenten nemen organisatorische kenmerken in overweging bij het beoordelen van e-mails.

Hypothese 4: Respondenten nemen veiligheidskenmerken in overweging bij het beoordelen van e-mails.

Hypothese 5: Respondenten nemen de inhoudelijke geloofwaardigheid in overweging bij het beoordelen van e-mails.

Hypothese 6: Er zijn verschillen in de respondent zijn of haar beoordelingen over de e-mail naargelang de dwingendheid van de e-mail; Een hogere mate van dwang, zorgt voor andere beoordelingen dan een lagere mate van dwang.

Hypothese 7: Er zijn verschillen waar te nemen in de manier van lezen en interpretatie van de e-mail tussen personen die wel voor de e-mail vallen en personen die niet voor de e-mail vallen.

6. Onderzoeksopzet & dataverzameling.

Voor het uitvoeren van dit onderzoek is gekozen voor de hardopdenkmethode. Wat deze methode precies inhoudt en waarom dit een goede manier van dataverzameling is voor dit onderzoek, zal in deze paragraaf worden uiteengezet.
Zowel de kracht als de beperkingen zullen aan bod komen.

6.1 De hardop denk methode

Een voor de hand liggende manier om kennis te verzamelen is door aan mensen te vragen hoe zij een taak uitvoeren en welke kennis ze hiervoor gebruiken.
Echter is gebleken dat mensen vaak niet kunnen vertellen hoe ze een taak uitvoeren. Erger zelfs, er is bewijs dat mensen vaak foute informatie geven (Van Someren et al, 1994).
De hardop denk methode is een goede manier om deze foutieve informatie uit te bannen en direct informatie te verzamelen over het oplossingsproces wat plaatsvindt wanneer iemand een probleem probeert op te lossen (Van Someren et al, 1994).
Bij het gebruiken van de hardop denk methode is het zeer belangrijk om rekening te houden met het feit dat het probleem niet te moeilijk mag zijn, omdat verbale processen dan vaak de cognitieve processen niet bij zullen kunnen houden. Dit houdt in dat een proefpersoon niet alles wat hij denkt zal zeggen en zal zorgen voor gaten in het protocol (Van Someren et al. 1994).

De hardop denk methode wordt voornamelijk gebruikt in studies betreffende duidelijke beslissingsproblemen, waarbij het van belang is dat de problemen niet te makkelijk zijn, omdat er voor de respondenten wel een zeker dilemma moet zijn (Van Someren et al. 1994). Om het probleem niet te makkelijk te maken moest de phishing e-mail dan ook enigszins betrouwbaar zijn. Er is dan ook voor gekozen om een e-mail zonder spellingsfouten, van een orgaan met autoriteit te gebruiken. Aangezien phishing e-mails mensen ook willen overtuigen tot het nemen van een beslissing - zo werd in dit onderzoek gebruikte phishing e-mail aan het einde gevraagd in te loggen op een bepaalde link, wat een duidelijk keuzemoment is – en aangezien het probleem niet te moeilijk is, is de hardop denk methode dan ook tevens geschikt voor dit onderzoek.
Het kan zo zijn dat respondenten het keuzemoment niet herkennen, om dit probleem tegen te gaan is een iets aangepaste tweede versie van de e-mail gemaakt, waarin de noodzaak tot het maken van een keuze explicieter wordt gesteld, hierin wordt aangegeven dat de respondent anders niet meer kan internetbankieren. Zoals al eerder vermeld, stelt dit onderzoek zich ten doel te analyseren op wat voor manier mensen phishing e-mails lezen. Om dit te kunnen opsporen, is het belangrijk om vlak op het leesproces van respondenten te zitten. Zodoende moet direct, tijdens het lezen, de gedachten van de respondent vastgelegd worden. De hardop denk methode is vanwege het feit dat het direct informatie verzamelen mogelijk maakt, een goede methode om dit onderzoek uit te voeren.
Het uitvoeren van een hardop denk onderzoek klinkt misschien simpel, maar het brengt veel voorbereiding met zich mee.
Alvorens te beginnen aan het uitvoeren van de hardop denk sessies, moesten eerst een aantal stappen worden doorlopen.

6.2 De phishing e-mail

Allereerst moest er een document worden geproduceerd waarmee respondenten gebrieft konden worden. Het document wat hiervoor opgesteld is op een eerder document van Heerkens uit 1999. Dit document omvat de taken van de proefleider, een briefing voor de respondent waarin het doel van het onderzoek uiteen wordt gezet en enkele oefenopgaven voor de respondent om samen met de proefleider te oefenen en zo in het hardopdenken te komen (zie bijlage 10.1 &10.2).

Hieropvolgend is een e-mail uitgekozen, dit na een analyse van meerdere, op het internet gevonden en via mijn begeleider, mevrouw Junger verkregen, door een werknemer van de ABN Amro aangeleverde phishing e-mails. Voor het kiezen van een e-mail zijn enkele selectiecriteria opgesteld, zo diende de e-mail goede spelling en goed taalgebruik te hebben, daar phishing e-mails heden ten dage steeds beter worden en het er anders te dik bovenop lag dat het hier om een fraudulente e-mail ging. Tevens moest de e-mail voldoende lengte hebben, om zodoende de respondent voldoende de mogelijkheid te geven om goed hardop na te denken. Ook was een huisstijl gewenst, daar het gebruik van een huisstijl steeds gangbaarder wordt binnen phishing e-mails. Tot slot moest er een duidelijk keuze moment binnen de e-mail zijn, zodat de respondent uiteindelijk daadwerkelijk een beslissing diende te nemen. Het bleek erg moeilijk een e-mail te vinden die voldeed aan alle criteria, maar uiteindelijk is gekozen voor een e-mail door criminelen verzonden uit naam van de ING (zie bijlage 10.3 & 10.4) deze e-mail heeft goede spelling en goed taalgebruik, is circa 350 woorden lang en bevat een duidelijk, gevraagd, keuzemoment. Een huisstijl ontbreekt helaas, maar aangezien de e-mail zeer sterk was op alle andere kenmerken en geen enkele e-mail aan alle kenmerken voldeed, bleek dit de beste keuze.
De e-mail is binnen het onderzoek gebruikt zoals deze daadwerkelijk door criminelen verzonden is, de A-versie, en in een iets aangepaste variant, de B-versie, die meer dwingt tot het ondernemen van actie.
Op basis van de gekozen e-mail, dienden er kopieën van de ING website gemaakt te worden, waarop de respondent uit zou komen indien deze zou klikken op de in de e-mail gegeven link. In samenwerking met mijn begeleider, Lastdrager, is een exacte kopie van de ING login pagina gemaakt.
Tot slot dienden er interviewvragen voor na het onderzoek opgesteld te worden. Dit om een back-up aan bruikbare informatie te hebben indien het hardopdenken niet goed zou gaan en als aanvulling op de hardopdenkprotocollen, tevens gaven de interviewvragen een evaluatie van wat elke respondent van het hardopdenken vond. Hiervoor is gebruik gemaakt van een aantal standaard vragen binnen het hardopdenken en zijn een aantal nieuwe, onderzoeksgerelateerde vragen bedacht (zie bijlage 10.5).
Vervolgens is een pilot uitgevoerd, waarin zowel voor de A-versie als de B-versie van de e-mail een proef hardopdenksessie met een respondent is gehouden, de proefsessies zijn opgenomen met een voicerecorder, uitgetypt en oppervlakkig geanalyseerd. Zodoende werd na overleg met Heerkens en Lastdrager duidelijk dat respondenten genoeg gedachten bij de e-mail uitspraken om een dergelijk onderzoek mogelijk te maken.
Na het doorlopen van al deze stappen is het echte onderzoek uitgevoerd.

6.3 Procedure

De data gebruikt in dit onderzoek is verzameld op de Universiteit Twente alwaar verschillende medewerkers van verschillende afdelingen per e-mail benaderd en gevraagd zijn om deel te nemen aan dit onderzoek.
Aangezien iedereen met een e-mail adres slachtoffer kan worden van phishing, was het niet nodig een specifieke doelgroep te kiezen.
Werknemers zijn verkozen boven studenten, om zo een heterogenere groep respondenten te krijgen, wanneer gekeken wordt naar opleidingsniveau en leeftijd.
De steekproef van het totale onderzoek bestaat uit 24 personen, bestaande uit 12 mannen en 12 vrouwen, met verschillende opleidingsniveaus en verschillende achtergronden.
Zo hebben er personen met een financiële achtergrond, marketing achtergrond en secretariële achtergrond meegewerkt.
Meer specificaties kunnen worden gevonden in tabel 1 en 2.

Tabel 1: Specificatie van de steekproef

Versie	Man	Vrouw	Gemiddelde leeftijd	Totaal
A	5	7	47,08	12
B	9	3	48,00	12

Tabel 2: Specificatie hoogst genoten opleiding Respondenten mail versie A

Hoogst genoten opleiding	Frequentie	Percentage
Middelbaar beroepsonderwijs	4	33,3%
Hoger beroepsonderwijs en wetenschappelijk onderwijs Bachelor	7	58,3%
Wetenschappelijk onderwijs, doctoraal of master	1	8,3%
Totaal	12	100%

Tabel 3: Specificatie hoogst genoten opleiding Respondenten mail versie B

Hoogst genoten opleiding	Frequentie	Percentage
Middelbaar algemene voortgezet onderwijs	1	8,3%
Middelbaar beroepsonderwijs	3	25%
Hoger beroepsonderwijs en wetenschappelijk onderwijs Bachelor	4	33,3%
Wetenschappelijk onderwijs, doctoraal of master	4	33,3%
Totaal	12	100%

Met elk van de 24 respondenten is een hardop denk sessie gehouden. Tijdens een hardop denk sessie is het de bedoeling dat de respondent gedurende de hele sessie hardop praat en alle gedachten die tijdens de sessie naar boven komen hardop uitspreekt.
Om dit gewenste resultaat te bereiken zijn alle respondenten voorafgaande aan het onderzoek eerst gebrieft.
In de briefing werd aan de respondenten verteld dat het gaat om een onderzoek naar marketing en communicatie van verscheidene bedrijven in hun e-mails.
Dit om de deelnemers het onderzoek in te laten gaan zonder dat het idee phishing of internet criminaliteit al werd gesuggereerd.
Ook stelde de briefing zich ten doel uit te leggen wat er van de respondent verwacht werd, zo werd er in de briefing herhaaldelijk verteld dat er hardop nagedacht moest worden.
Na de briefing werd begonnen met enkele oefenopgaven.
Één van de oefenopgaven bestond uit het hardop voorlezen van en hardop nadenken over een korte e-mail. Oefenopgaven als deze stelden ten doel dat respondenten konden wennen aan het hardop denk principe en zich bij aanvang van het echte experiment al zoveel mogelijk op hun gemak voelden. De oefenopgaven maakten het eveneens mogelijk voor de observant om te zien of de respondent begrepen heeft wat er met hardop denken bedoel wordt en dus, wat er van hem verwacht wordt. Dit is van belang aangezien de observant zich tijdens het hardop denk proces afzijdig dient te houden. De respondent heeft zodoende dus, zonder enige hulp, het probleem moeten oplossen. De e-mail gebruikt voor de oefenopgave en ook de ING e-mail zijn gelezen op een laptop in het programma Microsoft Outlook 2010, om zodoende zo goed als mogelijk de werkelijke situatie van het doorlezen van e-mail te benaderen. Elke respondent kreeg één versie van de mail te lezen, ofwel de A-versie, zoals deze daadwerkelijk door criminelen verzonden is, ofwel de iets dwingendere B-versie. De A-versie en B-versie zijn hieronder weergegeven, tevens zijn beide versies van de mail terug te vinden in bijlage 10.3 en 10.4
De verschillen tussen de A en B versie van de e-mail zijn als volgt:
De A versie heeft als onderwerp *"Storing Mijn ING verholpen"* waar de B versie het onderwerp *"Storing Mijn ING"* voert, dit geeft een verschil in noodzaak aan, wanneer de storing al verholpen is,

kan het zijn dat personen eerder geneigd zijn om te denken *"alles is toch alweer opgelost, waarom krijg ik hier nog bericht over?"*
Het tweede verschil tussen de A en B versie van de e-mail is te vinden in de eerste alinea.
De A versie van de e-mail begint als volgt:
Gisteren, woensdag 3 april, zijn er problemen geweest met de weergave van de af- en bijschrijvingen en daarmee het saldo van onze klanten in onze systemen. Op dit moment draait alles weer correct en zijn alle problemen opgelost.
Aldus deze versie van de e-mail, is alles in principe al weer goed, in de B versie is dit zodoende aangepast, de B versie begint met *"Gisteren, woensdag 3 april, zijn er problemen geweest met de weergave van de af- en bijschrijvingen en daarmee het saldo van onze klanten in onze systemen. Op dit moment draait bijna alles weer correct en zijn de meeste problemen opgelost."* en geeft zodoende meer de noodzaak van de e-mail neer, er blijkt immers nog een probleem te zijn.
De e-mails zijn vervolgens identiek, tot de laatste alinea, die zich ten doel stelt de respondent actie te laten ondernemen.
Versie A gebruikt hiervoor de volgende tekst *"Om vervelende omstandigheden te voorkomen, willen wij u vragen om uw rekening bij te werken via onderstaande link Inloggen Internet Bankieren*"
E-mail a stelt dus dat er vervelende omstandigheden kunnen optreden, maar probeert verder niet te triggeren tot het bijwerken van gegevens. Versie B sluit daarom dwingender af, er is al een probleem, en de respondent kan dit door actie te ondernemen oplossen. De slotalinea van e-mail B luidt als volgt: *Om vervelende omstandigheden te voorkomen is uw account voor het internetbankieren in een beveiligde omgeving geplaatst, wat betekent dat u op dit moment niet meer kunt internetbankieren. U dient deze blokkering op te heffen door in te loggen op onderstaande link en vervolgens het formulier dat verschijnt in te vullen Inloggen Internet Bankieren*. Versie B, is zodoende dwingender dan versie A.

Afsluitend aan de hardopdenksessie zijn 23 vragen gesteld, te beginnen met enkele algemene, tot meer specifieke met afsluitend een paar vragen over het verloop van het onderzoek.
Hiervoor genoemde vragen zijn gesteld om eventuele tekortkomingen in de hardop denk sessies te kunnen opvangen.
Wanneer bleek dat de hardop denk methode toch niet goed werkte voor het lezen van een e-mail, er nog relevante en bruikbare informatie was door het gebruik van de vragenlijst.
Gelukkig werkte de hardop denk methode wel degelijk en bleken de hieruit verkregen gegevens zeer bruikbaar.

De hardop denk sessies zijn opgenomen met een voicerecorder.
Hoewel direct coderen vanaf de voicerecorder aantrekkelijk lijkt in termen van efficiency is dit een niet aan te raden methode, het maakt het namelijk erg lastig om te controleren of de codering wel correct is uitgevoerd (Someren et al. 1994). Vandaar dat de hardop denk sessies alvorens te worden gecodeerd eerst volledig op de computer zijn uitgewerkt.
Na het uitwerken van de hardop denk sessies op de computer is het codeerschema opgesteld, het tot stand komen van het codeerschema zal worden besproken in hoofdstuk 6.
Vervolgens zijn de hardopdenksessies gecodeerd en vervolgens nagelopen door meerdere personen. Het coderen gebeurde door de hardopdenksessies op te delen in segmenten, segmenten zijn de kleinst mogelijke zinsdelen met een eigen betekenis, en hier vervolgens, waar mogelijk een code aan te hangen. Tot slot zijn de gecodeerde gegevens ingevoerd in Excel en op verschillende manieren vergeleken. Ook zijn de gestelde interviewvragen geanalyseerd, om zodoende relevante extra informatie, of discrepantie tussen het hardop denken en het interview te kunnen beschrijven.
Al met al duurde het hele onderzoek, dus de briefing, oefenopgaven, de hardop denk sessie en het stellen van de interviewvragen, ongeveer 40 minuten per persoon.

7. Codeerschema & Variabelen.

Dit hoofdstuk zal achtereenvolgens het tot stand komen van het codeerschema voor dit onderzoek, de afhankelijke en onafhankelijke variabelen, en de hypothesen bespreken.

7.1 Codeerschema

Voor het analyseren van de hardop denk sessies is het van belang om een aantal codes op te stellen, dit om de protocollen te operationaliseren en zodoende kennis uit de protocollen te kunnen verwerven en dus protocollen te kunnen analyseren (Van Someren et al, 1994).
Het codeerschema moet alle belangrijke kenmerken voortgekomen uit de theorie zo goed mogelijk dekken en moet ook voor buitenstaanders te begrijpen en toepasbaar zijn (Van Someren et al, 1994). Dit zodat het opnieuw coderen voor een ieder mogelijk is en een ieder uiteindelijk op dezelfde coderingen uit zal komen.

Om tot een goed codeerschema te komen voor dit onderzoek, is het van belang om in ogenschouw te nemen welke aspecten vanuit de theorie als belangrijk naar voren komen.
Voor het maken van een codeerschema zal er dus een korte terugkoppeling nodig zijn naar de theorie. Zoals in hoofdstuk 4 beschreven zijn er veel factoren die invloed hebben op vertrouwen. Zo kwamen in paragraaf 4.2 enkele marketing kenmerken naar voren, zo zorgt autoriteit ervoor dat personen makkelijker vertrouwen vergaren en maakt schaarste het hebben van iets voor mensen interessanter. Voor het opstellen van codes zijn deze marketing kenmerken van minder belang, echter helpen ze ons wel begrijpen op wat voor een manier phishers proberen in te spelen op het gevoel en vertrouwen van mogelijke slachtoffers. Paragraaf 4.3 gaf een schema met daarin het model van Mayer, met meer persoonlijke kenmerken, waargenomen risico en integriteit, welwillendheid en bekwaamheid naar voren. Paragraaf 4.4 gaf een overzicht van enkele reeds uitgevoerde studies en de punten die volgens deze studies belangrijk waren. Hierdoor werd duidelijk dat esthetische kenmerken als taalgebruik, lay-out en spelling ook wel degelijk een rol spelen bij het al dan niet vertrouwen van een website of e-mail. Om de uiteengezette theorie toepasbaar te maken op het lezen van e-mails, is het belangrijk om te kunnen indenken op wat voor manier mensen naar e-mails kijken. Na de pilot is dan ook een eerste analyse gedaan, waarbij op basis van de theorie een aantal codes zijn opgesteld. Hierbij is in ogenschouw genomen dat het codeerschema zo compleet mogelijk moest zijn, maar dat er ook niet teveel verschillende categoriseringen moeten zijn, daar dit het model te complex zou maken. De conclusie na een eerste analyse van de pilot bestanden was dat er door lezers gekeken wordt naar esthetische kenmerken, inhoudelijke kenmerken, organisatorische kenmerken en veiligheidskenmerken.

- *Esthetische kenmerken* zijn de kenmerken die betrekking hebben op dingen als spelling, opmaak, taalgebruik, lay-out en dergelijke. Bij het analyseren van de pilotmails, kwamen er echter ook op en aanmerkingen betreffende langdradigheid en bondigheid, dus de efficiëntie van de e-mail, ook dit wordt onder esthetiek geschaard, aangezien het een op of aanmerking is op het uiterlijk, meer specifiek, de lengte van de mail.
- *De inhoudelijke kenmerken* zijn opmerkingen betreffende de inhoud van de e-mail, of juist kanttekeningen bij deze inhoud, ze hebben zodoende betrekking op de geloofwaardigheid van de inhoud van de e-mail. Wordt er in de mail de waarheid verteld? Of vertelt men juist onzin?
- *Onder organisatorische kenmerken* worden opmerkingen verstaan die betrekking hebben op de organisatie of het handelen van de organisatie die de e-mail verstuurt. Het schema van Mayer speelt hierin een belangrijke rol, aangezien respondenten waarde leken te hechten aan de welwillendheid en de bekwaamheid van de organisatie, ook gedachten over de identiteit van de organisatie vallen onder organisatorische kenmerken.

- Tot slot de *veiligheidskenmerken*, dit zijn opmerkingen waaruit blijkt dat de respondent acties veilig dan wel onveilig lijkt te vinden, indien een respondent enig risico bespeurt zal hij dit wellicht afwegen tegen de mogelijke baten.

Op basis van de theorie en een analyse van de eerste protocollen zijn de volgende codes opgesteld:

Figuur 2: Een overzicht van de codes

Inhoudelijke codes	**Esthetische codes**	**Organisatorische codes**	**Veiligheid codes**	**Overige codes**
1) Geloofwaardigheid van de inhoud	1) Spelling	1) Welwillendheid	1) Veiligheid	1) Keuze
	2) Opmaak	2) Bekwaamheid		2) Overig
	3) Taalgebruik	3) Identiteit		
	4) Efficiëntie			

Elk van deze 12 kenmerken kent drie scores, te weten positief, neutraal en negatief. Hierin betekend positief dat de respondent een segment positief beoordeeld op het gegeven kenmerk, het gevoel van de respondent wordt hierdoor, denken we, dan ook positief beïnvloed, de respondent zal bij een positief gevoel, waarschijnlijk eerder geneigd zijn de mail te vertrouwen. In het geval dat de gradatie van een code neutraal is, geeft de respondent een neutraal oordeel over een bepaald segment, wat tevens inhoudt dat zijn of haar gevoel niet of nauwelijks beïnvloedt wordt. In h et geval dat een segment negatief gecodeerd is, betekend dit dat de respondent een negatief of slechter gevoel heeft bij het gegeven segment.

Nu er een overzicht is van welke codes in dit onderzoek gebruikt zijn en wat voor gradaties er voor elk van de codes is, is het van belang om te weten wat elke code inhoudt. Zodoende zal hieronder een omschrijving gegeven worden van elke code.

Inhoudelijke codes

Geloofwaardigheid van de inhoud.

Op het internet wordt geloofwaardigheid gedefinieerd als de waargenomen deskundigheid en betrouwbaarheid van een website (Zhiping, 2007). In dit onderzoek is de code geloofwaardigheid van de inhoud gegeven wanneer respondenten opmerkingen of uitlatingen deden over het waarheidsgehalte van de inhoud van de e-mail. Deze opmerkingen konden betrekking hebben op zowel twijfel aan de inhoud van de e-mail, of vertrouwen in de inhoud van de e-mail.

Esthetische codes

Spelling.

De code spelling is aan segmenten gegeven indien respondenten opmerkingen maakten, of uitlatingen deden omtrent de spelling van woorden. Verwacht werd dat deze code in het geval van dit onderzoek niet veel terug zou komen, daar de e-mail geen spelfouten bevat.

Opmaak.

De code opmaak is gegeven aan segmenten indien respondenten opmerkingen maakten, of uitlatingen deden omtrent alinea indeling, tussenkopjes en huisstijl van de e-mail.

Taalgebruik.

De code taalgebruik is gegeven aan segmenten wanneer respondenten op of aanmerkingen hadden betreffende juistheid of apartheid van de aanhef van de mail, de groet van de mail, of betreffende formeel en informeel taalgebruik.

Efficiëntie.
De code efficiëntie heeft betrekking op de langdradigheid of bondigheid van de e-mail. Segmenten waarin de respondent aangaf verstrekte informatie interessant ofwel langdradig te vinden, zijn gecodeerd met de code efficiëntie.

Organisatorische codes

Welwillendheid.
Segmenten zijn gecodeerd met welwillendheid wanneer respondenten opmerkingen maakten over het al dan niet tonen van goede wil door de organisatie die de e-mail verzonden heeft.

Identiteit.
Segmenten zijn gecodeerd met de code identiteit wanneer respondenten het hadden over de afzender van de e-mail en het vertrouwen daarin. Het gaat er in deze om dat respondenten gedachten uitspreken waarin ze uitspreken dat ze denken dat de e-mail al dan niet daadwerkelijk afkomstig is van de vermelde organisatie.

Bekwaamheid.
Segmenten zijn gecodeerd met de code bekwaamheid indien respondenten spraken over feiten betreffende het al dan niet naar behoren of verwachting handelen van de organisatie.

Veiligheidcodes

Veiligheid.
Segmenten zijn gecodeerd met de code veiligheid wanneer duidelijk blijkt dat een respondent denkt over de veiligheid van de e-mail en daarbij al dan geen risico's waarneemt.

Overige codes

Keuze.
Segmenten zijn gecodeerd als keuze wanneer de respondent duidelijk een keuze maakt om iets wel, of juist niet te doen. Indien er wel een keuze gemaakt is, wordt hierna vaak een actie ondernomen.

Overig.
Segmenten waarin respondenten opmerkingen maakten als Ahh uhh of mededelingen deden over het scrollen naar een volgende alinea, zijn gecodeerd als overig. Ook alle segmenten die geen betrekking hebben op inhoudelijke, organisatorische, esthetische en veiligheidskenmerken zijn gecodeerd als overig.

Vanuit de theorie leken autoriteit, schaarste en integriteit ook van belang (Cialdini, 2001) (Mayer et al., 1995).
Autoriteit wordt door de e-mail, doordat men zich voordoet als de ING bank, geclaimd.
De lezers kunnen aanmerkingen op deze autoriteit maken door op het aspect Identiteit in te gaan, autoriteit wordt zodoende niet apart gemeten.
Integriteit en schaarste komen in de gedachten van respondenten in deze e-mails echter niet terug en zijn daarom dan ook niet opgenomen in het codebestand.
Schaarste is echter wel meegenomen als criterium bij het ontwerpen van de tweede phishing e-mail, dit door te zeggen dat de respondent zijn gegevens moet bijwerken, omdat hij anders niet meer kan internetbankieren.

7.2 Variabelen

Om de in paragraaf 4.5 gegeven hypothesen te kunnen beantwoorden, zullen de variabelen die hiervoor van belang zijn geïdentificeerd moeten worden. Welke criteria zijn van belang?

Afhankelijke variabele

Onze afhankelijke variabele is het al dan niet in gaan op een phishing e-mail.

Onafhankelijke variabelen

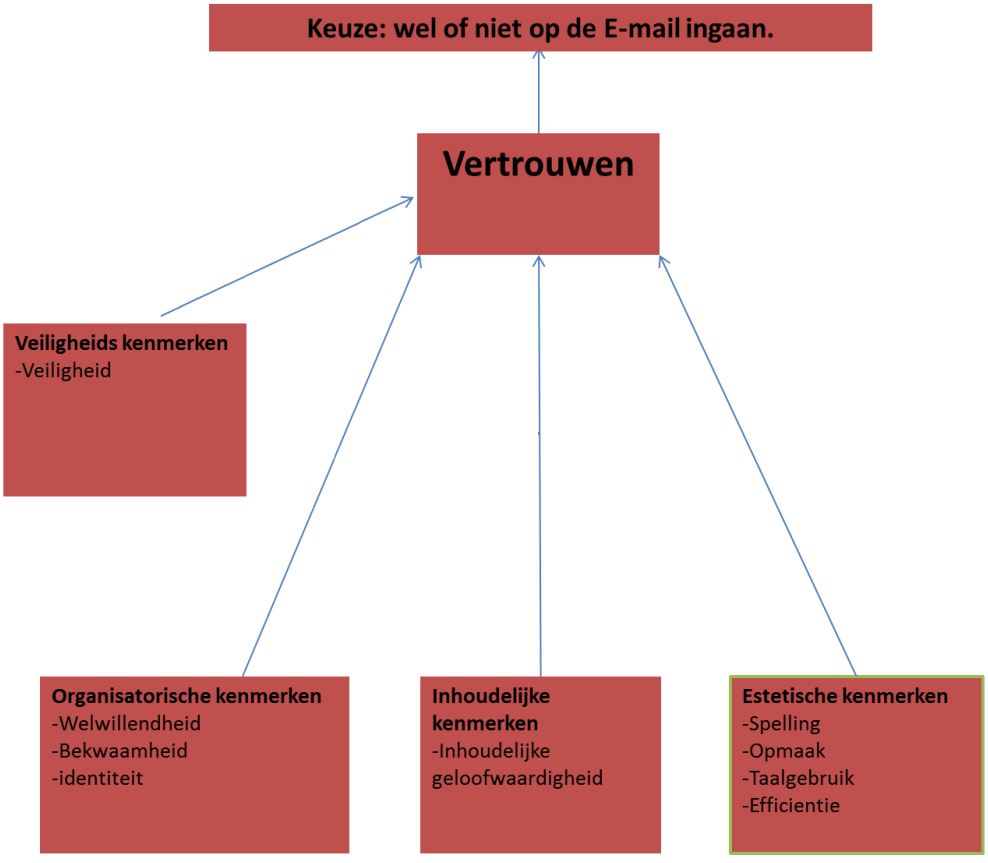
De onafhankelijke variabelen vloeien voort uit de opgestelde codes in het codeerschema en zijn als volgt:

- De geloofwaardigheid van de inhoud van de e-mail (Inhoudelijk)
- De waargenomen professionaliteit van de organisatie in de e-mail (Organisatorisch)
- Gedachten van de respondent over de esthetiek van de e-mail (Esthetiek)
- Gedachten over de veiligheid van de gevraagde actie (Veiligheid)

Des te positiever de gedachten van respondenten over deze variabelen, des te hoger het vertrouwen in de e-mail zal zijn.
Gedachten over de veiligheid van de gevraagde actie, zullen waarschijnlijk pas komen nadat er gedachten over de inhoud, organisatie en esthetiek zijn uitgesproken. Elk van deze variabelen is een determinant voor vertrouwen.

Op basis van het schema van Mayer in paragraaf 4.3, en de codes opgesteld in paragraaf 6.1, kunnen de codes als volgt schematisch worden weergegeven.

Figuur 3: Criteria die mogelijkerwijs een rol spelen bij het overwegen en besluiten al dan niet in te gaan op een phishing e-mail



Met dit schema wordt gesteld dat organisatorische, inhoudelijke en esthetische kenmerken zorgen voor vertrouwen of wantrouwen. Op basis van de mate van vertrouwen worden de risico's die de respondent bespeurd, afgewogen tegen het vertrouwen, dus: zijn de risico's die ik waarneem acceptabel genoeg gegeven het vertrouwen wat ik in de e-mail heb. Op basis hiervan zal een respondent besluiten wel, of niet op de e-mail in te gaan.

8. Resultaten

Dit hoofdstuk bestaat uit de beantwoording van de in hoofdstuk 6.3 opgestelde hypothesen.
Dit zal gebeuren op basis van kwantitatieve evenals kwalitatieve gegevens, voortgekomen uit de hardop denk protocollen en de bijbehorende afsluitende interviews.

8.1 Hypothese 1; afzender en aanhef

De eerste hypothese die getoetst zal worden is de hypothese:
Respondenten besteden tijd aan het lezen van de afzender en aanhef van de mail en spreken hier gedachten bij uit.
Deze hypothese is tot stand gekomen op basis van de aanhef van de in dit onderzoek gebruikte e-mail, de aanhef van de e-mail is: *"Beste klant"* wat een vrij ongebruikelijke en informele aanhef is voor een organisatie als de ING bank.
Bovendien stuurt de ING bank nooit e-mail waarin zij vraagt om gegevens. *"Mijn ING is strikt persoonlijk, geef nooit uw gebruikersnaam en wachtwoord aan iemand anders. De ING vraagt nooit naar persoonsgebonden gegevens als gebruikersnaam, wachtwoord of TAN-codes. Niet in een e-mail en niet per telefoon Ga altijd vertrouwelijk om met deze gegevens, net als de pincode van uw betaalpas."* (ING, 2014).
Dit geldt overigens voor elke bank en zou mogelijkerwijs kunnen leiden tot twijfel over de identiteit van de afzender bij de respondent.

Het eerste wat opvalt wanneer de protocollen verkregen uit het hardop denken geanalyseerd worden, is dat respondenten op verschillende plekken beginnen met lezen.
Zo beginnen 9 respondenten het lezen bij de afzender en het onderwerp van de e-mail, de andere 15 slaan dit stuk over en beginnen met de aanhef van de e-mail.
2 personen sloegen in eerste instantie het onderwerp over, maar lezen deze na het lezen van de aanhef "*Beste klant"* alsnog.

Er zijn voorbeelden van respondenten die beginnen met het lezen van de aanhef dan wel afzender van de e-mail en gelijk wantrouwend zijn:

Zo is er een respondent die twijfelt aan de identiteit van de afzender op basis van de aanhef "beste".

> *"Beste klant, nou eh ik vind, van de ING uit vind ik dat het geachte klant moet zijn, omdat beste heel informeel is" (*Respondent 3-A, r.1-4)

Een andere respondent leest aandachtig het onderwerp, en kijkt vervolgens gelijk wie de e-mail ondertekent, heeft, wanneer dit de directievoorzitter lijkt te zijn zorgt dit voor enige twijfel aan het feit of de identiteit van de afzender wel klopt, dit wordt duidelijk gemaakt door de woorden "toe maar. Ik krijg een mail van de directievoorzitter ING Nederland".

> "*Goed, ik heb map B geopend, en de mail heet, het subject, storing mijn ING, en de mail is van ING, nou ga ik eerst eens even kijken, naar beneden scrollen, wie die mail dan precies ondertekent: Dick Jue, directievoorzitter ING Nederland, toe maar. Ik krijg een mail van de directievoorzitter ING Nederland, nou scroll ik weer naar boven en ga ik even lezen."*
> (Respondent 5-B, r.1-12)

Weer een andere respondent geeft gelijk aan te twijfelen aan de identiteit van de afzender. Ook gebruikt hij de woorden 'vervelend mailtje' die duiden op gedachten over spam mail, of phishingmail, en dus zorgen voor een negatief gevoel betreffende veiligheid van de mail.

> *"Ok, storing ING, even oppassen dat dit niet zo'n vervelend mailtje is, wat niet bij de ING vandaan komt, maar echt van de ING bank is" (*Respondent 3-B, r.1-4)

Ook de volgende respondent heeft twijfel bij de identiteit van de afzender van de e-mail en de veiligheid van de e-mail.

> "*Storing Mijn ING, ok, nou ik ben klant van de ING, uhm, ik ben altijd een beetje een eh huiverig bij dit soort dingetjes. Omdat ik weet dat de bank nooit, of zelden informatie stuurt*" (Respondent 10-B, r.2-7)

Er zijn ook respondenten die een positieve eerste indruk van de e-mail krijgen, dat wil zeggen dat ze na het lezen van de aanhef en/of afzender, het gevoel hebben dat de e-mail daadwerkelijk van de ING bank afkomstig is.

> *"Storing mijn ING. Hè gadverdamme, het, het is altijd wel wat met de ING. Dat is echt inderdaad zo"* (Respondent 2-B, r.2-5)

Ondanks het feit dat de respondent niet blij is met de reden van de e-mail, begint de respondent met een positief gevoel te lezen, de respondent denkt dat er weer wat bij de ING aan de hand is geweest en lijkt het voor de hand liggend te vinden dat daarvoor een e-mail gestuurd is.

> "*Storing mijn ING verholpen. Er zal waarschijnlijk iets met internetbankieren aan de hand geweest zijn"* (Respondent 8-A, r.1-2)

Ook deze respondent begint het lezen in de veronderstelling dat er iets met internetbankieren aan de hand is geweest en vindt het niet raar dat daarvoor een e-mail is gestuurd, de respondent begint zodoende te lezen met een positief gevoel betreffende de geloofwaardigheid van de inhoud.

Naast een positief en negatief gevoel kan er een neutraal gevoel aanwezig zijn, respondenten lezen de aanhef en/of afzender en hechten hier geen verdere gevoelswaarde aan.

> *"Hij komt van, Ok, storing ING"* (Respondent 12-A, r.1-2)

De respondent neemt aan dat de e-mail van ING afkomstig is, maar besteed hier verder geen aandacht aan.

Tot slot doen 13 respondenten (55%) geen uitspraken betreffende de aanhef of afzender tijdens het hardop denken, in sommige gevallen wordt de afzender wel gelezen, maar in veel van deze gevallen wordt begonnen met lezen bij de aanhef.
Deze respondenten lijken geen gedachten te hebben bij het begin van de e-mail, uitgaande van de uitspraak van Cialdini dat mensen van nature vertrouwen hebben in de medemens, kan er vanuit worden gegaan dat deze personen dus positief aan de e-mail zullen beginnen, dat wil zeggen dat ze beginnen met lezen vol vertrouwen.

Ook opvallend zijn de gegevens die naar voren komen uit de volgende 2 interviewvragen:

- *Weet u nog wat de aanhef van de e-mail was?*
- *Vond u dit een gebruikelijke of ongebruikelijke aanhef voor een e-mail van dit type organisatie?*

De antwoorden op deze vragen konden grofweg gecategoriseerd worden in 4 categorieën.
De eerste categorie omvat de respondenten die de aanhef van de e-mail niet meer zegt te weten.
De tweede categorie omvat de respondenten die de daadwerkelijke aanhef van de e-mail als antwoord gaf, namelijk beste klant
De derde categorie omvat de respondenten die dachten, of zeker wisten te weten dat de aanhef van de e-mail Geachte klant was.

De vierde categorie omvat de respondenten die het onderwerp van de e-mail definieerden als de aanhef.

Tabel 4: Uitkomsten Interviewvraag 5: Weet u nog wat de aanhef van de e-mail was?

Antwoord	**Aantal**	**Percentage**
Respondent weet de aanhef van de e-mail niet meer	7	29,2%
Respondent geeft als antwoord Beste klant	7	29,2%
Respondent geeft als antwoord Geachte klant	6	25,0%
Respondent geeft als antwoord Storing ING	4	16,7%
Totaal	24	100%

De uitkomsten van deze tabel zijn opvallend, slechts 29,2% van de respondenten wist na de hardop denk sessie de juiste aanhef van de e-mail nog, dit waren voornamelijk de respondenten die bij het lezen van deze aanhef en de afzender al een negatief gevoel bij de e-mail hadden. 25% gaf aan dat hij of zij dacht dat de e-mail begon met de aanhef “geachte klant”, sommige van deze respondenten waren hier echter niet helemaal zeker over. Een mogelijke reden waarom ze dan toch dit antwoord gaven is het feit dat ‘geachte’ een formelere en daarmee gebruikelijkere aanhef zou zijn voor een e-mail van een organisatie.

Opvolgend op deze vraag is de vraag “*Vond u dit een gebruikelijke of ongebruikelijke aanhef voor een e-mail van dit type organisatie?”*
Bij het analyseren van de antwoorden op deze vraag zijn de antwoorden van respondenten die in de voorgaande vraag binnen de categorie “respondent antwoord Storing ING” vielen, weggelaten.
De antwoorden die door deze respondenten gegeven zijn, gaan immers feitelijk gezien niet over de aanhef, maar over het onderwerp van de e-mail.
In onderstaande tabel staan de uitkomsten van deze vraag.

Tabel 5: Uitkomsten Interviewvraag 6: Vond u dit een gebruikelijke of ongebruikelijke aanhef voor een e-mail van dit type organisatie?

Gebruikelijk	**Aantal**	**Percentage**
Ja	8	33,3%
Nee	6	25,0%
Weet Niet	6	25,0%
Totaal	20	83,3%

Nu duidelijk is wat respondenten dachten dat de aanhef van de e-mail was, en of ze deze gebruikelijk of ongebruikelijk vonden, is het interessant om de antwoorden op beide vragen te vergelijken.
Dit is gedaan door middel van onderstaande kruistabel. In deze kruistabel zijn wegens de bovengenoemde reden, eveneens de respondenten die bij interviewvraag 5 in de categorie “respondent antwoord Storing ING” vielen, weggelaten.

Tabel 6: Aanhef in combinatie met de gebruikelijkheid daarvan volgens de respondent.

Weet u nog wat de aanhef van de mail was? * Vond u dit een gebruikelijke of ongebruikelijke aanhef voor een mail van dit type organisatie? Crosstabulation

			Vond u dit een gebruikelijke of ongebruikelijke aanhef voor een mail van dit type organisatie?			
			Ja	Nee	Weet niet	Total
Weet u nog wat de aanhef van de mail was?	Respondent weet de aanhef van de email niet meer	Count	1	1	5	7
		% of Total	5,0%	5,0%	25,0%	35,0%
	Respondent antwoord Beste klant	Count	2	4	1	7
		% of Total	10,0%	20,0%	5,0%	35,0%
	Respondent antwoord Geachte klant	Count	5	1	0	6
		% of Total	25,0%	5,0%	0,0%	30,0%
Total		Count	8	6	6	20
		% of Total	40,0%	30,0%	30,0%	100,0%

Zeven respondenten gaven aan de aanhef van de e-mail niet meer te weten. Één van deze respondenten gaf echter aan de aanhef wel gebruikelijk gevonden te hebben een ander vond de aanhef juist ongebruikelijk. Vijf van deze zeven personen wisten niet of de aanhef gebruikelijk of ongebruikelijk was.
Van de zeven respondenten die als aanhef beste klant antwoorden gaven er twee aan dit een gebruikelijke aanhef te vinden, vier gaven aan dit niet te vinden en één persoon wist het niet.
Van de zes respondenten die geachte klant antwoorden als aanhef van de e-mail vonden er vijf de aanhef gebruikelijk en één respondent vond dit niet gebruikelijk.
De respondent die geachte klant niet als gebruikelijk ervoer gaf hiervoor de volgende uitleg

> *"Ik had wel verwacht dat, dat een persoonlijke mail zou zijn met mijn naam bijvoorbeeld erboven, of geachte mevrouw ….., of beste …."* (Respondent 9-A, interviewvraag 6).

Geachte klant lijkt als een gebruikelijkere aanhef te worden gezien dan beste klant, maar ook beste klant vormt voor sommige respondenten geen probleem.

De eerste hypothese kan kortweg als volgt beantwoord worden.
De eerste indruk die respondenten krijgen wanneer zij beginnen met het lezen van de e-mail is over het algemeen gezien niet negatief.
Er zijn 11 respondenten die aandacht besteden aan de aanhef en afzender, en hier opmerkingen overmaken en 13 respondenten die hieromtrent geen uitspraken doen. Het is dus lang niet altijd het geval dat respondenten gedachten hebben over de afzender of aanhef van de e-mail.
Betreffende de aanhef wordt dit door het interview achteraf bevestigd, slechts 7 personen wisten de juiste aanhef van de e-mail en slechts 6 respondenten gaven aan de aanhef ongebruikelijk te vinden.
Lang niet alle respondenten besteden dus uitgebreid aandacht aan de aanhef en afzender van de e-mail. Slechts voor weinig respondenten wordt het vertrouwen in eerste instantie beïnvloed door de aanhef en de afzender van de e-mail.

8.2 Hypothese 2: Esthetische kenmerken

Deze paragraaf richt zich op het beantwoorden van de hypothese: *Respondenten nemen esthetische kenmerken in overweging bij het beoordelen van e-mails.*

Volgens de theorie zijn op websites de manier van spreken, spelfouten en andere tekenen van onprofessioneel design, redenen waardoor mensen zich bewust worden van misleiding of bedrog (Dhamija, Tygar & Hearst, 2006).
Eerder in dit rapport hebben wij getracht dit om te zetten naar criteria binnen e-mails.

Zodoende zijn wij uitgekomen op een framework van esthetische criteria, dit framework omvat de criteria spelling, opmaak, taalgebruik en efficiëntie, die in de hardopdenk protocollen elk hun eigen code hebben gekregen.
Wanneer mensen een positief gevoel over de esthetische criteria binnen een e-mail hebben, zal dit wellicht leiden tot vertrouwen, en wanneer personen een negatief gevoel hebben bij deze esthetische criteria, zal dit wellicht leiden tot wantrouwen.
De vraag die deze hypothese tracht te beantwoorden is of mensen ook daadwerkelijk op de esthetische criteria letten.
Achtereenvolgens zullen de criteria spelling, opmaak, taalgebruik en efficiëntie aan bod komen.

Spelling
Phishing e-mails zitten vaak vol spelfouten, maar de goede phishing e-mails, die boven de andere phishing e-mails uitsteken, zijn die mails waar geen spelfouten inzitten.
In dit onderzoek is dan ook gekozen voor een goede phishingmail waar geen spelfouten in terugkomen.
Toch zijn er enkele respondenten geweest die op en aanmerkingen maakten betreffende spelling.
Gezien over alle protocollen zijn er 4 opmerkingen over spelling.
Zo gaf één respondent aan verkeerd hoofdlettergebruik te zien.

> *"Werken met een hoofdletter, ok?"* (Respondent 12A, r.67).

Een andere respondent gaf aan het woord mij te zien staan waar mijn hoort te staan.

> "*Huh, mij? Da's nie sterk, dat ie daar mij zegt"* (Respondent 1B, r.10).

Opmerkelijk is dat deze fouten in beide e-mails niet aanwezig waren, mogelijkerwijs hebben respondenten door snel lezen een fout gezien die er niet was.
Andere respondenten maakten positieve opmerkingen betreffende de spelling.

> *"Ehh, ik zie nogsteeds geen taalfouten. Dus dat zou maar zo eens geen spam mail kunnen zijn"* (Respondent 7B, r.19-29)
>
> "*Gelukkig geen spelfouten"* (Respondent 10B, r.78).

Deze opmerkingen duiden op het feit dat deze respondenten hebben gelet op de spelling in de e-mail om te bepalen of ze deze konden vertrouwen. Dit maakt spelling dan ook een criterium waar daadwerkelijk op gelet wordt bij het bepalen van de legitimiteit van een e-mail.
Of een e-mail met één of enkele spelfouten minder effectief zal zijn kan op basis van dit onderzoek niet wordengezegd en zal dus verder onderzocht dienen te worden.
Het enige wat geconcludeerd kan worden, is dat sommige respondenten spelling als attribuut in overweging nemen, wanneer zij een e-mail doorlezen.

Opmaak
De opmaak van de in dit onderzoek gebruikte e-mail is vrij simpel, er is gebruik gemaakt van alinea's en tussenkopjes maar een huisstijl van de organisatie die de e-mail stuurt ontbreekt.
De huisstijl van een bedrijf is een consistente presentatie naar buiten toe en zorgt voor een eenduidige uitstraling. Grote bedrijven zullen in hun communicatie dan ook gebruik maken van een huisstijl.
Voorafgaande aan het onderzoek was de verwachting dan ook dat veel respondenten op of aanmerkingen zouden hebben op het ontbreken van een huisstijl.
Uiteindelijk bleek het aantal opmerkingen hieromtrent tegen te vallen, in het totaal zijn er tijdens het hardop denken slechts 6 opmerkingen gemaakt met betrekking op de opmaak van de e-mail, elk van deze opmerkingen was negatief.
Deze opmerkingen waren veelal van algemene aard.

> "*Oh, die mail is niet zo heel netjes opgesteld"* (Respondent 2-A, r.24), "*Ik vind trouwens die opmaak zegmaar, dat stoort mij dan, dat het niet netjes is."* (Respondent 9-A, r.15-17).

Ook maakte één persoon een opmerking over het ontbreken van een logo en ging daarin wat meer richting huisstijl.

> *"zie ik ook geen logo derbij staan"* (Respondent 12-B, r.157)

Opvallend is dat alle respondenten die opmerkingen maakten betreffende de opmaak een communicatie achtergrond hebben. En zodoende kennis hebben over het feit hoe er professioneel gecommuniceerd dient te worden.

Slechts 2 respondenten komen in het interview achteraf terug op de opmaak.
Aan één respondent werd de vraag gesteld of de bank op een andere manier beter had kunnen communiceren, en wat voor aanbevelingen de respondent kon geven na het lezen van de e-mail.
De respondent antwoordde met

> "*Hmm, in ieder geval eh iets te doen aan om het in de huisstijl te doen"* (Respondent 9-A, interviewvraag 17)

Een andere respondent zei

> *"De hele opmaak is vrij saai, terwijl ik juist van een professioneel bedrijf verwacht, dat ze ook in de aanhef gewoon hun eigen huisstijl zichtbaar hebben en ook onderin."* (Respondent 3-B, interviewvraag 10).

<u>Taalgebruik</u>
Wanneer taalgebruik binnen phishing e-mails bekeken wordt, is te zien dat dit vaak slecht is, in dit onderzoek is gekozen voor een e-mail waarin het taalgebruik wel goed was. Toch zijn op en aanmerkingen op het taalgebruik terug te vinden in enkele van de protocollen.
Zo geeft één van de respondenten aan dat er eerst in de wij vorm geschreven wordt en daarna in de ik vorm.

> *"Eerst spreken ze in de wij vorm, daarna in de ik vorm, uhm"* (Respondent 2-A, r.49).

Een andere respondent spreekt over het raar plaatsen van leestekens

> *"Wat is er gisteren precies gebeurd? Ik vind het ook raar om daar dan een vraagteken in te zetten"* (Respondent 9-A, r.22-23)
>
> *"De verstoring? Ik zou storing gezegd hebben"* (Respondent 9-b, r.15-16)

De meeste negatieve opmerkingen betreffende taalgebruik zijn wederom afkomstig van respondenten uit de communicatie sector.

Naast deze negatieve opmerkingen was er ook sprake van positieve opmerkingen omtrent taalgebruik, zo gaf een respondent aan dat de e-mail wel heel erg banktaal was

> *"Ja, het is wel heel erg bank uhhh taal"* (Respondent 4-B, r.69)

Daar deze e-mail ook pretendeert van een bank afkomstig te zijn, is dit positief, gezien het doel van dit onderzoek.

<u>Efficiëntie</u>
De variabele efficiëntie is gedurende het onderzoek ontstaan, 14 respondenten kwamen met opmerkingen betreffende langdradigheid, of juist het nuttig zijn van informatie.
Voorafgaande aan het onderzoek lag niet in de verwachting dat respondenten opmerkingen zouden maken in deze trend.
Enkele interessante uitspraken betreffende efficiëntie zullen nu besproken worden.
De in het onderzoek gebruikte e-mail begint met een excuus, vervolgens wordt het volgende gezegd "*U mag van ons verwachten dat u gemakkelijk en foutloos uw bankzaken dagelijks bij ons kunt regelen, hier zijn wij gisteren helaas niet in geslaagd. Wat is er gisteren precies gebeurd?*"
Er is hier onderscheid te maken tussen respondenten die het interessant vinden om te weten wat er gisteren precies gebeurd is en respondenten die dit allemaal maar overbodig vinden.
Zo zegt de ene respondent *"Ja, daar ben ik benieuwd naar"* (Respondent 12-A, r.22) *"ben benieuwd"* (Respondent 1-A, r.20), wat een positieve opmerking is betreffende efficiëntie. Waar anderen juist negatief zijn en zeggen: *"Is voor mij eigenlijk minder interessant, wat er nou gebeurd is want"* (Respondent 10-B, r.24-25).
Er zijn zelfs respondenten die dreigen af te haken door langdradigheid van de e-mail.

"Het is allemaal veel te veel detail, wat en op welke manier heeft mij dit geraakt. Ik heb helemaal geen zin meer om dit verder door te lezen. En was dit niet een opdracht die ik af heb te maken, dan ging ik nu de email sluiten" (Respondent 2-B, r.41-46).
"Ja, ik vind het een beetje een lege email, met weinig informatie eigenlijk, maar heel veel tekst" (Respondent 9-A, r.67-69).

Het lijkt er dus op dat een te langdradige e-mail in bepaalde gevallen niet eens afgelezen zal worden.

Cijfermatige gegevens esthetische kenmerken

Voor het beantwoorden van deze hypothese is het belangrijk om te weten hoeveel van de respondenten daadwerkelijk naar esthetische kenmerken kijken. In dit onderzoek stellen we, dat indien 15% van de respondenten één of meerdere opmerkingen maakt betreffende een bepaald kenmerk, het waarschijnlijk is dat dit kenmerk daadwerkelijk een rol speelt bij het beoordelen van de E-mail. Onderstaande tabel laat zien in hoeveel procent van de gevallen respondenten opmerkingen over elk van de esthetische kenmerken had.

Tabel 7: Bij hoeveel respondenten komt elke esthetische code voor?

Totale steekproef	**Absoluut**	***Procentueel***
Spelling	4	17%
Efficiëntie	15	63%
Opmaak	4	17%
Taalgebruik	5	21%
Aantal respondenten totaal	24	

Beantwoording hypothese

Respondenten kijken bij het doorlezen van hun e-mail wel degelijk naar esthetische kenmerken, efficiëntie komt in de in dit onderzoek gekozen e-mail het meeste terug. Dit waarschijnlijk omdat het een vrij lange e-mail is.
Enkele respondenten vinden het ontvangen van veel informatie fijn, maar bij de meeste lijkt het enkel te leiden tot irritatie, of zelfs stoppen met lezen van de e-mail.
Taalgebruik en spelling worden tevens aangedragen door respondenten, vijf respondenten maken opmerkingen betreffende het taalgebruik en vier betreffende de spelling, ondanks het feit dat het taalgebruik in de e-mail goed is en de e-mail geen spelfouten bevat. Het lijkt erop dat taalgebruik en spelling een gedegen rol spelen bij het beoordelen van e-mails, om hieromtrent meer zekerheid te verkrijgen moet in vervolgonderzoek een e-mail met één of enkele spelfouten en meer apart taalgebruik gebruikt worden.
Wat betreffende de opmaak zijn er enkele respondenten die het ontbreken van een huisstijl aankaarten, in totaal maakten er vier respondenten opmerkingen betreffende de opmaak van de e-mail. Ondanks dat een huisstijl gebruikelijk is, lijkt het ontbreken ervan voor respondenten over het algemeen niet storend. Vier van de 24 is 17% en het lijkt er zodoende sterk op dat alle esthetische kenmerken in overweging genomen worden bij het beoordelen van een e-mail.
Het is niet zo dat door alle respondenten over alle esthetische criteria nagedacht wordt, maar 19 van de 24 respondenten neemt in ieder geval 1 of enkele esthetische kenmerken mee in hun overweging, dit is te zien in onderstaande tabel overgenomen uit SPSS.

Tabel 8: Neemt de respondent esthetische kenmerken mee bij het beoordelen van de e-mail

Esthetische kenmerken	**Aantal**	**Percentage**
Respondent neemt esthetische kenmerken wel in overweging	19	79,2%
Respondent neemt esthetische kenmerken niet in overweging	5	20,8%
Totaal	24	100%

Desondanks het feit dat niet alle respondenten Esthetische kenmerken herkennen, of meenemen in het beoordelen van een mail, is 19 van de 24 wel een substantieel grote groep. Er kan dus worden gesteld dat Esthetische kenmerken wel in overweging genomen worden bij het beoordelen van de e-mail.

8.3 Hypothese 3: Organisatorische kenmerken

De hypothese die in deze paragraaf getest zal worden is:
*Respondenten nemen organisatorische kenmerken in overweging bij het beoordelen van e-mails***.**
Deze organisatorische kenmerken zijn de kenmerken die voortgekomen zijn uit het model van Mayer et. al, uitgelegd in paragraaf 2.3.
De organisatorische kenmerken geoperationaliseerd in dit onderzoek zijn bekwaamheid, welwillendheid en identiteit.
Achtereenvolgens zal nu het belang van bekwaamheid en welwillendheid besproken worden, het belang van identiteit is besproken in paragraaf 5.1, hier is duidelijk gemaakt dat identiteit een rol speelt bij het beoordelen van e-mails. Identiteit wordt zodoende minder uitgebreid meegenomen binnen deze paragraaf.

<u>Bekwaamheid</u>
Bekwaamheid lijkt een belangrijk criterium te zijn bij het lezen van e-mails in dit onderzoek, 22 van de 24 respondenten heeft uitspraken gedaan die op enigerlei wijze over de bekwaamheid van de organisatie gaan.
Respondenten waardeerden de bekwaamheid van de bank zowel positief als wel negatief.
Maar in grotere mate negatief, wat te verwachten was naargelang de inhoud van de e-mail.
De e-mail spreekt namelijk van *"een probleem met de weergave van de af en bijschrijvingen en daarmee het saldo van klanten in onze systemen".*
Verscheidene reacties van respondenten op deze zin zijn als volgt:

> "*Alweer"* (Respondent 12-A, r.6) *"Da's nie best"* (Respondent 1-A, r.6),
> *"Ok, dus ze geven wel aan dat er een probleem is geweest. Ik vind het te laat. Het was gisteren. Ze hadden het gisteren meteen moeten versturen"* (Respondent 3-A, r.9-12)

Hierboven gelezen reacties wijzen op een negatief gevoel bij de bekwaamheid van het handelen van de organisatie, daar de organisatie niet heeft gedaan wat zij hoort te doen.
Een andere reactie op deze zin was: *"Hebben we gelezen"* (Respondent 3-B, r.16), deze respondent beoordeeld zodoende de bekwaamheid van de organisatie nog niet op basis van het probleem.
Een andere respondent kwam zelfs met een positieve opmerking betreffende bekwaamheid op basis van deze zin *"Dus opzich is dit denk ik eh goed dat ING me nu eens een keer informeert"* (Respondent 10-A, r.14), deze respondent lijkt te vinden dat het probleem wat hier optreedt, een keer kan optreden en hecht juist waarde aan het feit dat de organisatie informatie verschaft.

Verderop in de e-mail wordt gesproken van onterechte roodstand, er zijn respondenten die hier geen uitspraken over doen, maar ook respondenten die uitspraken doen omtrent negatieve bekwaamheid van de bank. Vervolgens geeft de bank het volgende aan *"We hebben direct maatregelen getroffen om te zorgen dat alle klanten met hun ING betaalpas ongeacht het rekeningsaldo tot 250 euro geld konden opnemen en konden betalen bij alle pinautomaten"*
Hierop kwamen zowel positieve als negatieve reacties.

> *"Vandaar dat ik kon pinnen, en wat een goede service"* (Respondent 4-A, r.38-39).
> *"Maargoed, dat kan veel te weinig zijn, 250 euro het is maar net eh, als je in het buitenland bent en waar je het voor nodig hebt, als je op dat moment je hotel moet betalen, kom je er niet met 250 euro"* (Respondent 3-A, r.85-88)

Het lijkt erop dat de bekwaamheid wordt beoordeeld op het verwachtingspatroon van de respondent betreffende de service die een organisatie zou moeten leveren.

Waar de organisatie de verwachtingen van respondenten nakomt, zullen ze tevreden zijn, en waar de verwachtingen niet stroken met de werkelijkheid, zal dit niet het geval zijn.
Lastig is echter dat verwachtingen van personen verschillen, de ene persoon lijkt te vinden dat een foutje op zijn tijd kan gebeuren en vindt het goed dat er een e-mail is gestuurd en dus de organisatie, ondanks een fout, bekwaam.
Waar anderen de organisatie afstraft op de fout, aangezien een fout als deze, volgens hen, bij een professionele organisatie als een bank niet mag voorkomen.

Welwillendheid

Ook welwillendheid komt in de protocollen terug.
Zo is er een respondent die het feit dat de ING uitlegt wat er is gebeurt getuigd van welwillendheid.

> *"Uiteraard wil ik u in meer detail uitleggen wat er is gebeurd. Dat is wel netjes, dat ze dit doen"* (Respondent 2-A, r.8-10)

Een ander vindt het aanbieden van een excuus een teken van welwillendheid.

> *"Nou, ze beginnen in ieder geval al netjes met het aanbieden van een excuus, dat helpt altijd als er iets verkeerd is gegaan" (*Respondent 8-A, r.15-16)

Weer een ander vindt een excuus juist niet genoeg en waardeert de welwillendheid zodoende negatief.

> *"Nou, bos bloemen dan maar"* (Respondent 4-B, r.12)

Wat getuigd van welwillendheid lijkt per persoon te verschillen en is zodoende, evenals bekwaamheid subjectief. Men lijkt welwillendheid te beoordelen op basis van wat men sociaal wenselijk, of acceptabel acht.

Identiteit

11 (45%) respondenten doen uitspraken betreffende de identiteit van de afzender van de e-mail, deze zijn overwegend negatief, namelijk in 19 van de 31 segmenten gecodeerd als identiteit is de gedachte over identiteit Negatief. Bij het behandelen van hypothese 1: "*Respondenten besteden tijd aan het lezen van de afzender en aanhef van de mail en spreken hier gedachten bij uit",* zijn reeds voorbeelden betreffende vertrouwen of wantrouwen in de identiteit op basis van het lezen van de aanhef naar voren gekomen. Twee van deze voorbeelden zijn in deze paragraaf herhaald, meer voorbeelden zijn te vinden in paragraaf 7.1.

> *" Storing ING, storing mijn ING, hè gadverdamme, het, het is altijd wel wat met de ING, dat is echt inderdaad zo"* (Respondent 2-B r.1-5)

Wijst op een positieve uitspraak betreffende identiteit, de respondent gelooft immers dat de e-mail daadwerkelijk van de ING bank afkomstig is.

> *"Ok, storing ING, even oppassen dat dit niet zo'n vervelend mailtje is, wat niet bij de ING vandaan komt, maar echt van de ING bank is" (*Respondent 3-B, r.1-4)

Wijst op een negatieve uitspraak betreffende identiteit, de respondent gelooft immers niet dat de e-mail daadwerkelijk afkomstig is van de ING bank.

Cijfermatige gegevens Organisatorische kenmerken

Evenals voor de esthetische kenmerken is voor de organisatorische kenmerken een tabel opgesteld waarin af te lezen is bij hoeveel van de respondenten elk organisatorische kenmerk voorkwam. Ook hier wordt gesteld dat 15% een voldoende hoog percentage is, om te verwachten dat deze organisatorische kenmerken daadwerkelijk een rol spelen bij het beoordelen van een e-mail.

Tabel 9: Bij hoeveel respondenten komt elke organisatorische code voor?

Totale steekproef	**Absoluut**	***Procentueel***
Welwillendheid	9	38%
Identiteit	11	46%
Bekwaamheid	22	92%
Aantal respondenten totaal	24	

Beantwoording hypothese

Zowel bekwaamheid, identiteit als welwillendheid zijn codes die terugkomen in de protocollen, een groot deel van de respondenten lijkt wel degelijk te beoordelen of de organisatie handelt zoals ze wenselijk en gebruikelijk achten voor een organisatie van dit type en nemen zodoende organisatorische kenmerken mee bij het beoordelen van e-mails.
Bekwaamheid wordt door het overgrote deel van de respondenten beoordeeld, welwillendheid in mindere mate, het is dus niet zo dat alle respondenten zowel bekwaamheid als welwillendheid meenemen in het beoordelen van hun e-mails.
Onderstaande tabel, opgesteld op basis van de codering binnen de protocollen, geeft dit cijfermatig weer.

Organisatorische kenmerken	**Aantal**	**Percentage**
Respondent neemt organisatorische kenmerken wel in overweging	22	91,7%
Respondent neemt organisatorische kenmerken niet in overweging	2	8,3%
Totaal	24	100%

Tabel 8: Neemt de respondent organisatorische kenmerken mee tijdens het beoordelen van de e-mail

Organisatorische kenmerken worden dus wel degelijk in overweging genomen bij het beoordelen van de e-mail.

8.4 Hypothese 4: Veiligheidskenmerken

De 4e gestelde hypothese is als volgt: *Respondenten nemen veiligheidskenmerken in overweging bij het beoordelen van e-mails.*

In de in dit onderzoek gebruikte e-mails wordt aan het einde gevraagd om op een gegeven link in te loggen, voorafgaande aan de hardopdenksessies was de verwachting dat elk van de respondenten hier een afweging zou maken betreffende de veiligheid van het klikken. En zodoende dus een beoordeling zou maken op basis van het feit of het risico wat ze waargenomen hebben, accepteerbaar, of te groot is. Uit onderstaande tabel blijkt dat dit echter niet waar is.

Tabel 9: Neemt de respondent veiligheidskenmerken mee tijdens het beoordelen van de e-mail

Veiligheids kenmerken	**Aantal**	**Percentage**
Respondent neemt veiligheids kenmerken wel in overweging	14	58,3%
Respondent neemt veiligheids kenmerken niet in overweging	10	41,7%
Totaal	24	100%

Op basis van de vooronderstelling dat alle respondenten veiligheid mee zouden nemen in hun beoordeling is dit een vreemde uitkomst, slechts 14 van de 24 respondenten lijken veiligheidskenmerken in overweging te nemen bij het lezen van de e-mail.

Wanneer elk van de 14 respondenten risico waarneemt, verschilt van respondent tot respondent. De ene respondent neemt al vroeg in de e-mail risico waar.

> "*maar ik weet ook, dat er wel heel vaak, bij bankenmails, wel phishing of zoiets is, dus ik ben wel een beetje alert nu."* (Respondent 5-B r.31-34).

Voor de meeste respondenten gebeurt dit echter pas aan het einde van de e-mail, wanneer er gevraagd wordt om actie te ondernemen en zij moeten besluiten al dan niet te klikken op een gegeven link.
Zo zijn er 4 respondenten die, na de veiligheidswaarschuwing gegeven na het klikken op de link, geen gevaar waarnamen en besloten door te klikken.
Deze respondenten hadden een positief gevoel bij de veiligheid van de e-mail, ze namen geen risico's waar. Een voorbeeld hiervan is als volgt:

> *"Nou eens even kijken naar dat inloggen, hoe dat gaat.(de respondent klikt op de link) Eh, doesn't find it… ok, continue, yes"* (Respondent 1-B, r.71-75)

Een andere respondent had wel twijfel bij de link, maar kwam na een afweging tot de conclusie dat klikken tot op zekere hoogte wel veilig was, uiteindelijk besloot deze respondent ook te stoppen.

> *"Ja dan, als ik op de link ga staan, word ik wel naar iets van de ING toegestuurd, maar of dat dan de officiële ING site is of niet, dat zal moeten blijken. Opzich kan het geen kwaad om er op te linken"* (Respondent 3-B, r.110-114). *"Er staat wel bij in de melding uhm. Om de eigen computer te beschermen, alleen op links te klikken die we echt vertrouwen hmm. Vertrouwen, vertrouwen we deze, vertrouwen we deze, naja, ING heeft wel wat problemen gehad, dus we drukken gewoon even op yes"* (Respondent 3-B, r.131-136)

Andere respondenten komen bij het overwegen van de veiligheid van de link tot een andere beoordeling, ze besluiten wel te klikken, maar stoppen bij de veiligheidswaarschuwing, aangezien deze hen doet inzien dat de e-mail wel eens onveilig kan zijn.

> *"This location may be unsafe, verrek, haha, ja ik denk dat ik dit, dus even niet ga, do you want to continue, no"* (Respondent 5-A, r.69) *"Ja, ik ga niet met een ongeldige"* (Respondent 5-A, r.69)

Weer andere respondenten besluiten niet te klikken.

> *"Nou, dat ga ik dus zeker niet doen, als ze mij dat via de e-mail vragen dan eh, zal ik daar zeker niet intrappen, want dit kan net zo goed een spam zijn"* (Respondent 3-A, r.127-130)

Weer een andere respondent zegt het volgende.

> *"Ja, ik heb, moet ik dit nu aanklikken? Nou, proberen. We gaan eens even kijken waar ie heengaat trouwens, deze link. Hmm hè uhhs, hyperlink, copy hyperlink, eens even kijken waar we dan terecht komen. Je weet maar nooit, he? En of dat inderdaad een vertrouwt adres is"* (Respondent 9-B, r.92-100) *"Nou hier zou ik dus niet op klikken, C, users, dat nee, dat lijkt me niet wat"* (Respondent 9-B, r.104-105)

<u>Beantwoording hypothese</u>
Het lijkt er dus op dat verschillende respondenten veiligheid van acties dus op verschillende manieren proberen vast te stellen en beoordelen.
14 van de 24 respondenten beoordelen de veiligheid van hun acties tijdens het lezen van de e-mail en nemen zodoende veiligheidskenmerken mee in het beoordelen van de e-mail.
Veiligheidskenmerken lijken dus nog lang niet door iedereen herkent te worden, maar worden door een meerderheid van de respondenten wel in overweging genomen.

8.5 Hypothese 5: inhoudelijke geloofwaardigheid

De hypothese die behandeld zal worden in deze paragraaf luidt als volgt**:** *Respondenten nemen de inhoudelijke geloofwaardigheid in overweging bij het beoordelen van e-mails.*

Bij het analyseren van de hardop denk protocollen blijkt dat 23 respondenten de geloofwaardigheid van de inhoud van de e-mail beoordelen, in deze beoordeling geven de respondenten aan of ze de inhoud van de mail wel, al dan niet geloven. In totaal zijn 235 uitspraken gedaan betreffende de inhoudelijke geloofwaardigheid van de mail, waarvan er 45 positief, 84 neutraal en 106 negatief zijn. Enkele voorbeelden van opmerkingen betreffende inhoudelijke geloofwaardigheid zullen hieronder gegeven worden.
Een neutrale opmerking betreffende inhoudelijke geloofwaardigheid is bijvoorbeeld:

> *"Vanwege het lange paasweekend, ja, waren er veel betaaltransacties en duurde deze verwerking langer, ok"* (Respondent 3-B, r.70-r.74)

De respondent maakt hier door het gebruik van de woorden *"ja"* en "*ok"* wel opmerkingen met betrekking tot de geloofwaardigheid van de inhoud, maar is in zijn uitspraken neutraal.
Positieve opmerkingen betreffende inhoudelijke geloofwaardigheid zijn bijvoorbeeld:

> "*Ik ben me bewust van de impact die dit incident op u als klant had en de ongerustheid en onduidelijkheid die het teweeg heeft gebracht. Ja, ongerust word je er wel van, want als dit kan gebeuren, dan, wanneer is dan de volgende keer, en ze vertellen niet of dit een incident is geweest, of dat dit vaker kan gebeuren"* (Respondent 3-A, r.156-r.168)"

Uit de opmerking, *"ja, ongerust word je er wel van"* is immers op te maken dat de respondent de inhoud van de voorgaande zinnen betreffende de impact van het incident op de klant, als geloofwaardig beschouwt.
Een negatieve opmerking betreffende inhoudelijke geloofwaardigheid is als volgt:

> *"Klanten die hiervoor te maken hebben gekregen met een roodstand hoeven zelf geen actie te ondernemen, hiervoor worden geen kosten in rekening gebracht, ja, ik vind het een raar bericht van de, om zo te verschijnen"* (Respondent 12-B, r.220-224).

De respondent geeft hier duidelijk een negatieve opmerking betreffende inhoudelijke geloofwaardigheid, hij vindt het door de bank verstrekte bericht immers raar.

<u>Beantwoording hypothese</u>
23 van de 24 respondenten doet uitlatingen betreffende de inhoudelijke geloofwaardigheid, en of hij of zij deze positief, neutraal, dan wel negatief ervaart. De respondenten nemen inhoudelijke geloofwaardigheid dus zeker in overweging bij het beoordelen van de e-mail, en de uitspraken betreffende inhoudelijke geloofwaardigheid blijken overwegend negatief.

8.6 Hypothese 6: Dwang

Deze paragraaf stelt zich tot doel de vijfde hypothese binnen dit onderzoek te beantwoorden. Deze hypothese luidt: *Er zijn verschillen in de respondent zijn of haar beoordelingen over de e-mail naargelang de dwingendheid van de e-mail; Een hogere mate van dwang, zorgt voor andere beoordelingen dan een lagere mate van dwang.*

De 12 protocollen van de A versie van de e-mail omvatten, zoals af te lezen in tabel 10, gezamenlijk 997 segmenten, voor de B versie zijn dit er 1291. In het geval van de A versie zijn 236 (23,67%) van deze segmenten gecodeerd als één van de bruikbare codes voor analyse die eerder opgesteld zijn, dat wil zeggen dat deze segmenten de code welwillendheid, identiteit, bekwaamheid, veiligheid, geloofwaardigheid, spelling, efficiëntie, of taalgebruik hebben gekregen. Voor de B versie zijn dit 317 (24,55%) segmenten.

Tabel 10: Segmenten per versie en het percentage bruikbaar gecodeerde segmenten

Versie	Aantal segmenten	Aantal bruikbaar gecodeerde segmenten
A	997 (100%)	236 (23,67%)
B	1291 (100%)	317 (24,55%)

Tabel 11 laat ons zien dat in het geval van versie A 39 uitspraken gecodeerd als positief, 40 als neutraal en 157 als negatief. Voor versie B zijn dit respectievelijk 46, 95 en 176 uitspraken zijn. Het percentage positief gecodeerde uitspraken ligt voor beide versies dicht bij elkaar. Echter is binnen versie A slechts in 16,95% van de gevallen een uitspraak gedaan die duidt op een neutraal gevoel. In versie B is dit 29,97%. De respondenten die de A versie van de e-mail voorgelegd kregen waren op hun beurt in meer procent van de gevallen negatief, namelijk 66,53% van de gecodeerde segmenten geven een negatief gevoel weer, waar dit voor respondenten die de B versie van de e-mail voorgelegd kregen 55,52% is. Absoluut gezien echter, maakten respondenten die de A versie van de e-mail voorgelegd kregen minder negatieve opmerkingen dan respondenten die de B versie van de e-mail voorgelegd kregen.

Tabel 11: Absolute en Procentuele aantallen positief, neutraal en negatief gecodeerde segmenten per versie.

Versie	Positief	Neutraal	Negatief	Totaal
A	39(16,53%)	40 (16,95%)	157 (66,53%)	236 (100%)
B	46 (14,51%)	95 (29,97%)	176 (55,52%)	317 (100%)

Tabel 12 laat ons zien dat Respondenten die de A versie van de mail voorgelegd kregen, gemiddeld gezien minder opmerkingen maakten betreffende inhoudelijke, esthetische of veiligheidskenmerken, dan de respondenten die versie B van de e-mail voorgelegd kregen. Gemiddeld gezien was het aantal gecodeerde opmerkingen binnen de A versie 19,66 en binnen de B versie 26,42. Hierbij moet gezegd worden dat binnen zowel versie A, als versie B een uitschieter naar boven zit, respondent 3-A staat garant voor 74 van de gecodeerde segmenten binnen versie A, waar als respondent 3-B garant staat voor 89 gecodeerde segmenten binnen versie B. Procentueel gezien, was in de A versie 23,67% van het totaal segmenten codeerbaar, voor de B versie ligt dit percentage op 24,55%.

Tabel 12: Het gemiddeld aantal segmenten en gecodeerde segmenten per respondent.

Versie	Gemiddeld aantal segmenten per respondent	Gemiddeld aantal segmenten gecodeerd als opmerking betreffende inhoudelijke, esthetische, organisatorische of veiligheidskenmerken
A	83,08	19,66
B	107,58	26,42

Op basis van deze resultaten lijkt het erop dat een hogere mate van dwang zorgt voor meer opmerkingen, en voor een lager percentage negatieve opmerkingen. Aangezien de steekproef van dit onderzoek slechts 24 personen omvat, en elke e-mail dus slechts door 12 personen gelezen is, kunnen deze conclusies echter ook op toeval berusten.
Bovenstaande gegevens geven een korte, zeer oppervlakkige vergelijking weer, voor een betere vergelijking is het van belang om niet alleen naar het aantal positief, neutraal en negatief gecodeerde opmerkingen te kijken binnen beide versies, maar om te kijken op welke codes respondenten positief, neutraal en negatief waren binnen beide versies. Er zal nu dan ook een vergelijkende analyse van de A en B groep volgen op elk van de in de vorige paragrafen besproken, inhoudelijke, esthetische, organisatorische en veiligheidscodes.

Vergelijkende analyse inhoudelijke codes versie A en versie B

Tabel 13: Hoeveel procent van de inhoudelijke codes is positief, neutraal en negatief gecodeerd, naargelang versie.

	Positief		**Neutraal**		**Negatief**		**Totaal**	
Code	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B
geloofwaardigheid	19 (18,63%)	26 (19,55%)	22 (21,57%)	62 (46,62%)	61 (59,80%)	45 (33,83%)	102 (100%)	133 (100%)

Allereerst zijn de twee versies van de e-mail vergeleken op de inhoudelijke code, geloofwaardigheid. Uit tabel 13 blijkt dat voor zowel versie A als versie B ongeveer 19% van de opmerkingen gecodeerd als geloofwaardigheid, positief waren. De opmerkingen betreffende geloofwaardigheid waren in het geval van de B versie procentueel gezien vaker neutraal, dan binnen de A versie, respectievelijk 46,62% en 21,57%. Binnen de A versie waren de opmerkingen met betrekking tot geloofwaardigheid overwegend negatief, 59,8% van de opmerkingen omtrent geloofwaardigheid was voor deze versie negatief, waar dit voor de B versie slechts 33,83% was. Binnen de A versie van de e-mail waren in totaal 102 opmerkingen die gecodeerd zijn als zijnde geloofwaardigheid, waar dit in versie B 133 opmerkingen zijn.

Tabel 14: Hoeveel procent van het totaal aan gecodeerde segmenten valt onder de waarden positief, neutraal en negatief van de inhoudelijke code, naargelang versie.

	Positief		**Neutraal**		**Negatief**		**Totaal**	
Code	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B
Geloofwaardigheid	19 (8,05%)	26 (8,20%)	22 (9,32%)	62 (19,56%)	61 (25,85%)	45 (14,20%)	102 (43,22%)	133 (41,96%)
Alle codes gezamenlijk							236 (100%)	317 (100%)

Wanneer, zoals in tabel 14, de gecodeerde opmerkingen betreffende inhoudelijke geloofwaardigheid af worden gezet tegen het totaal aantal gecodeerde opmerkingen binnen beide versies, blijkt dat binnen versie A 43,22% van de gecodeerde opmerkingen de code geloofwaardigheid te hebben, binnen versie B is dit 41,96%. Dit percentage ligt zo dicht bij elkaar dat het er niet op lijkt dat de mate van dwang zorgt voor een verschil in de hoeveelheid gedachten betreffende inhoudelijke geloofwaardigheid. Wel is het geval dat bij de e-mail met een hogere mate van dwang een veel hoger percentage aan neutraal gecodeerde geloofwaardigheids opmerkingen aanwezig is, waar bij een lagere mate van dwang het grootste gedeelte van de geloofwaardigheids opmerkingen negatief gecodeerd is. Het lijkt er zodoende op dat bij een hogere mate van dwang de inhoud van de e-mail minder in twijfel wordt getrokken dan bij een lagere mate van dwang.

Tabel 15: Bij hoeveel respondenten komt de code geloofwaardigheid voor binnen versie A en binnen versie B

Code	Versie A	Versie B
Geloofwaardigheid	11 (91,67%)	12 (100%)

Zowel binnen versie A als versie B worden opmerkingen betreffende geloofwaardigheid door veel respondenten uitgesproken. In versie A maken 11 van de 12 respondenten opmerkingen gecodeerd als geloofwaardigheid, in versie B zijn dit 12 van de 12 respondenten.

Wanneer, zoals in tabel 14, de gecodeerde opmerkingen betreffende inhoudelijke geloofwaardigheid af worden gezet tegen het totaal aantal gecodeerde opmerkingen binnen beide versies, blijkt dat

binnen versie A 43,22% van de gecodeerde opmerkingen de code geloofwaardigheid te hebben, binnen versie B is dit 41,96%. Dit percentage ligt zo dicht bij elkaar dat het er niet op lijkt dat de mate van dwang zorgt voor een verschil in de hoeveelheid gedachten betreffende inhoudelijke geloofwaardigheid. Wel is het geval dat bij de e-mail met een hogere mate van dwang een veel hoger percentage aan neutraal gecodeerde geloofwaardigheids opmerkingen aanwezig is, waar bij een lagere mate van dwang het grootste gedeelte van de geloofwaardigheid opmerkingen negatief gecodeerd is. Een verklaring hiervoor valt op basis van dit onderzoek echter niet te geven.

Vergelijkende analyse Esthetische codes versie A en versie B

Zoals al eerder uitgelegd zijn de esthetische codes in dit onderzoek spelling, efficiëntie, opmaak en taalgebruik. Eerder is al uitgelegd dat de lage aantallen opmerkingen betreffende esthetische kenmerken waarschijnlijk ten grondslag ligt aan een goede spelling, goed taalgebruik en een nette opmaak binnen de phishing e-mail, desondanks zullen de waar te nemen verschillen tussen beide versies, aan de hand van tabel 16,17 en 18 worden tentoon gespreid.

Tabel 16: Hoeveel procent van elk van de esthetische codes is positief, neutraal en negatief gecodeerd, naargelang versie.

	Positief		**Neutraal**		**Negatief**		**Totaal**	
Code	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B
Spelling	0 (0%)	2 (66,67%)	0 (0%)	0 (0%)	1 (100%)	1 (33,33%)	1 (100%)	3 (100%)
Efficiëntie	2 (12,5%)	2 (4,35%)	0 (0%)	2 (4,35%)	14 (87,5%)	42 (91,30%)	16 (100%)	46 (100%)
Opmaak	0 (0%)	0 (0%)	0 (0%)	0 (0%)	4 (100%)	2 (100%)	4 (100%)	2 (100%)
Taalgebruik	0 (0%)	1 (25%)	0 (0%)	1 (25%)	3 (100%)	2 (50%)	3 (100%)	4 (100%)
Esthetische kenmerken gezamenlijk	2 (8,33%)	5 (9,09%)	0 (0%)	3 (5,45%)	22 (91,67%)	47 (85,45%)	24 (100%)	55 (100%)

Tabel 17: Hoeveel procent van het totaal aan gecodeerde segmenten valt onder de waarden positief, neutraal en negatief van elk van de esthetische codes, naargelang versie.

	Positief		**Neutraal**		**Negatief**		**Totaal**	
Code	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B
Spelling	0 (0%)	2 (0,63%)	0 (0%)	0 (0%)	1 (0,42%)	1 (0,32%)	1 (0,42%)	3 (0,95%)
Efficiëntie	2 (0,85%)	2 (0,63%)	0 (0%)	2 (0,63%)	14 (5,93%)	42 (13,25%)	16 (6,78%)	46 (14,51%)
Opmaak	0 (0%)	0 (0%)	0 (0%)	0 (0%)	4 (1,69%)	2 (0,63%)	4 (1,69%)	2 (0,63%)
Taalgebruik	0 (0%)	1 (0,32%)	0 (0%)	1 (0,32%)	3 (1,27%)	2 (0,63%)	3 (1,27%)	4 (1,27%)
Esthetische kenmerken gezamenlijk	2 (0,85%)	5 (1,58%)	0 (0%)	3 (0,95%)	22 (9,32%)	47 (14,83%)	24 (10,17%)	55 (17,35%)
Alle codes gezamenlijk							236 (100%)	317 (100%)

Tabel 18: Bij hoeveel respondenten komen de esthetische codes voor binnen versie A en binnen versie B

Code	Versie A	Versie B
Spelling	1 (8,33%)	3 (25%)
Efficiëntie	6 (50%)	9 (75%)
Opmaak	2 (16,67%)	2 (16,67%)
Taalgebruik	2 (16,67%)	3 (25%)

Spelling

Spelling lijkt in zowel de A als de B-versie van de e-mail geen grote rol te spelen, er is slechts één opmerking betreffende spelling gemaakt binnen versie A, binnen de B versie zijn dit er drie. Voor de A versie gaat het hier om een negatieve opmerking. Binnen de B versie zijn twee (66,67%) van deze opmerkingen positief en één (33,33%) van negatieve aard. Tabel 17 laat zien dat deze ene opmerking binnen versie A, 0,42% van alle codes binnen mail A vertegenwoordigt, de drie als spelling gecodeerde opmerkingen binnen mail B omvatten gezamenlijk 0,95% van alle codes binnen de B versie. Het feit dat weinig gecodeerde opmerkingen de code spelling hebben gekregen kan worden verklaard door het feit dat de e-mail geen spelfouten bevat.

Efficiëntie

Binnen versie A van de e-mail zijn in totaal 16 opmerkingen gemaakt betreffende efficiëntie, voor versie B zijn dit 46 opmerkingen. Binnen zowel de A als de B versie zijn gemaakte opmerkingen betreffend efficiëntie overwegend negatief, in versie A zijn 14 (87,5%) opmerkingen negatief, en in versie B zijn 42 (91,3%) van de opmerkingen van negatieve aard. Al hoewel binnen beide versies de opmerkingen gemaakt betreffende Efficiëntie overwegend negatief zijn, ligt het aantal opmerkingen betreffende efficiëntie, gemaakt in de B versie bijna drie keer zo hoog als in de A versie. In tabel 16 is af te lezen dat voor versie A 6,78% van de gecodeerde opmerkingen gecodeerd is als efficiëntie, binnen versie B heeft 14,51% van de gecodeerde segmenten de code efficiëntie gekregen. Tabel 18 laat zien dat er binnen versie B (9) meer respondenten opmerkingen betreffende efficiëntie maken dan in de A versie (6). Het lijkt er dus sterk op dat een hogere mate van dwang zorgt voor een hoger aantal opmerkingen betreffende efficiëntie, meer specifiek een negatieve beleving van efficiëntie van de e-mail. Tevens lijkt een hogere mate van dwang ervoor te zorgen dat meer verschillende personen opmerkingen maken betreffende efficiëntie.

Opmaak

Opmaak speelt in versie A evenals B geen erg grote rol, in versie A van de e-mail zijn in totaal vier opmerkingen gemaakt betreffende de opmaak, voor de B versie zijn dit twee opmerkingen. Zoals in tabel 17 af te lezen is dit respectievelijk 1,69% van de gecodeerde opmerkingen voor versie A en 0,63% van de gecodeerde opmerkingen voor versie B. Voor zowel versie A als versie B, zijn alle gemaakte opmerkingen betreffende de opmaak van de e-mail negatief. Waarschijnlijk zijn er weinig opmerkingen gemaakt betreffende de opmaak omdat de e-mail, op het ontbreken van een huisstijl na een nette opmaak had. Indien de opmaak erg slordig is zou het goed kunnen zijn dat er meer opmerkingen betreffende de opmaak gemaakt worden.

Taalgebruik

Binnen versie A hebben drie opmerkingen de code taalgebruik gekregen, voor versie B zijn dit er vier. Voor versie A zijn elk van de drie opmerkingen omtrent taalgebruik van negatieve aard. Voor versie B is één neutraal van de opmerkingen positief (25%), één neutraal (25%) en zijn er twee negatief (50%). Voor zowel versie A als versie B van de e-mail zijn 1,27% van het totaal aantal gecodeerde

opmerkingen, opmerkingen betreffende taalgebruik, dit lage percentage kan verklaard worden door het feit dat het taalgebruik in de e-mail goed was.

Esthetische kenmerken gezamenlijk

De analyse wijst uit dat er betreffende esthetische kenmerken tussen de A en B versie enkel op het gebied van efficiëntie grote verschillen zijn. Hoewel binnen beide versies de meeste opmerkingen gemaakt betreffende efficiëntie overwegend negatief is, hebben binnen versie B 14,51% van het totaal aan gecodeerde segmenten de code efficiëntie, waar dit voor versie A maar 6,78% is. Er zijn zodoende in versie B meer opmerkingen gemaakt die wijzen op het in overweging nemen van efficiëntie, meer specifiek, opmerkingen die wijzen op een negatieve ervaring van de efficiëntie van de e-mail. Elk van de overige esthetische kenmerken omvat voor zowel versie A als versie B van de e-mail minder dan 2% van de gecodeerde opmerkingen. Het gaat voor deze kenmerken tevens om erg lage aantallen, zodoende kunnen de verschillen op deze esthetische kenmerken evengoed op toeval berusten.

Vergelijkende analyse Organisatorische codes versie A en versie B

Tabel 19: Hoeveel procent van elk van de organisatorische codes is positief, neutraal en negatief gecodeerd, naargelang versie.

	Positief		**Neutraal**		**Negatief**		**Totaal**	
Code	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B
Welwillendheid	10 (66,67%)	1 (25%)	3 (20%)	1 (25%)	2 (13,33%)	2 (50%)	15 (100%)	4 (100%)
Identiteit	0 (0%)	4 (15,38%)	3 (60%)	5 (19,23%)	2 (40%)	17 (65,38%)	5 100%)	26 (100%)
Bekwaamheid	8 (10,67%)	8 (19,05%)	11 (14,67%)	11 (26,19%)	56 (74,67%)	23 (54,76%)	75 (100%)	42 (100%)
Organisatorische kenmerken gezamenlijk	18 (18,95%)	13 (18,06%)	17 (17,89%)	17 (23,61%)	60 (63,16%)	42 (58,33%)	95 (100%)	72 (100%)

Tabel 20: Hoeveel procent van het totaal aan gecodeerde segmenten valt onder de waarden positief, neutraal en negatief van elk van de organisatorische codes, naargelang versie.

	Positief		**Neutraal**		**Negatief**		**Totaal**	
Code	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B
Welwillendheid	10 (4,24%)	1 (0,32%)	3 (1,27%)	1 (0,32%)	2 (0,85%)	2 (0,63%)	15 (6,35%)	4 (1,27%)
Identiteit	0 (0%)	4 (1,26%)	3 (1,27%)	5 (1,58%)	2 (0,85%)	17 (5,36%)	5 (2,12%)	26 (8,20%)
Bekwaamheid	8 (3,39%)	8 (2,52%)	11 (4,66%)	11 (3,47%)	56 (23,73%)	23 (7,26%)	75 (31,77%)	42 (13,24%)
Organisatorische kenmerken gezamenlijk	18 (7,63%)	13 (4,10%)	17 (7,20%)	17 (5,36%)	60 (25,42%)	42 (13,25%)	95 (40,25%)	72 (22,71%)
Alle codes gezamenlijk							236 (100%)	317 (100%)

Tabel 19 geeft een overzicht van de gemaakte opmerkingen betreffende de organisatorische codes. Aan de hand van deze tabel en tabel 20 en 21, zullen versie A en versie B van de e-mail vergeleken worden op deze organisatorische codes.

Tabel 21: Bij hoeveel respondenten komen de organisatorische codes voor binnen versie A en binnen versie B

Code	Versie A	Versie B
Welwillendheid	7 (58,33%)	2 (16,66%)
Identiteit	4 (33,33%)	7 (58,33%)
Bekwaamheid	11 (91,67%)	11 (91,67%)

Welwillendheid

Wanneer er gekeken wordt naar welwillendheid in tabel 19, blijkt dat voor versie A van de e-mail er in totaal 15 opmerkingen gemaakt zijn betreffende deze welwillendheid, 10 (66,67%) hiervan waren positief. Voor de B versie van de e-mail echter, zijn slechts vier opmerkingen gemaakt betreffende welwillendheid, waarvan er slechts één van positieve aard was. Uit tabel 20 blijkt dat voor versie A 6,35% van de gecodeerde opmerkingen welwillendheid betrof, voor versie B is dit slechts 1,27%. Het lijkt er zodoende op, dat respondenten bij een hogere mate van dwang, minder opmerkingen maken betreffende welwillendheid van de organisatie. Tabel 21 laat zien dat er bij een hoge mate van dwang ook slechts 2 respondenten zijn die opmerkingen maken betreffende deze welwillendheid, waar dit bij een lage mate van dwang 7 respondenten zijn. Welwillendheid is overigens de enige code in het onderzoek die in het merendeel van de gevallen positief gescoord is.

Identiteit

Binnen de A versie van de e-mail zijn in totaal vijf opmerkingen gemaakt betreffende identiteit, waar dit in de B versie 26 opmerkingen betreft. Binnen de A versie van de e-mail, zijn zoals te lezen in tabel 19, drie (60%) opmerkingen betreffende identiteit neutraal, voor de B versie zijn dit er vijf (19,23%). Binnen de B versie van de e-mail zijn opmerkingen betreffende Identiteit overwegend negatief, 17 (65,38%) van de opmerkingen betreffende identiteit hebben hier een negatieve strekking.
Tabel 20 laat ons zien dat van alle gecodeerde opmerkingen in versie A 2,12% de code identiteit heeft gekregen, voor versie B is dit 8,20%. Het lijkt erop, dat naarmate er meer dwingend om een actie gevraagd wordt, respondenten meer aandacht besteden en dus meer opmerkingen maken, betreffende de juistheid van de identiteit van de afzender van de e-mail. Ook lijken meer respondenten überhaupt het attribuut welwillendheid te scoren, 7 respondenten spreken immers over identiteit bij een hogere mate van dwang, waar dit in de e-mail met een lagere mate van dwang slechts 4 respondenten waren.
Op basis van de in tabel 19 en 20 gepresenteerde gegevens, lijkt het, het geval dat identiteit negatiever wordt beoordeeld bij een hogere mate van dwang. Door het lage aantal gecodeerde opmerkingen betreffende identiteit in versie A, kunnen we dit echter niet met zekerheid zeggen.

Bekwaamheid

Bekwaamheid komt binnen beide versies van de e-mail het meeste voor van de organisatorische kenmerken. Versie A kent 75 opmerkingen gecodeerd als bekwaamheid, voor versie B bedraagt dit aantal 42. Voor beide versies zijn 8 van deze opmerkingen positief, dit beslaat respectievelijk 10,67% van de opmerkingen gecodeerd als bekwaamheid voor versie A, en 19,05% van de opmerkingen gecodeerd als bekwaamheid voor versie B. Binnen beide versies is het aantal neutrale opmerkingen betreffende bekwaamheid 11, dit is respectievelijk 17,89% en 23,61%. Het aantal negatieve opmerkingen omtrent bekwaamheid ligt in versie A op 56 (74,67%) en in versie B op 23 (54,76%). Wanneer gekeken wordt naar tabel 18 zien we dat binnen versie A 31,77% van de gecodeerde opmerkingen bekwaamheid betreft, voor versie B is dit slechts 13,24%. Binnen zowel versie A als versie B maken 11 respondenten opmerkingen betreffende de bekwaamheid van de organisatie, wat er wederom op wijst dat respondenten bekwaamheid een belangrijk attribuut vinden.

Organisatorische kenmerken gezamenlijk

De opmerkingen betreffende organisatorische kenmerken zijn zowel binnen versie A als versie B voornamelijk negatief van aard, voor versie A zijn 60 van de 95 opmerkingen negatief van aard, dit is 63,16%, voor versie B van de e-mail zijn 42 van de 72 opmerkingen van negatieve aard, wat gelijk staat aan 58,33% van de als organisatorisch gecodeerde kenmerken. Binnen zowel versie A als versie B is circa 18% van de opmerkingen positief van aard.

Binnen versie A, de versie van de e-mail met een lagere dwang zijn veel meer opmerkingen gemaakt betreffende bekwaamheid en welwillendheid, Het feit dat het aantal opmerkingen betreffende bekwaamheid en welwillendheid in versie A hoger ligt dan in versie B, zou veroorzaakt kunnen zijn door het feit dat binnen versie A van de e-mail meer respondenten vertrouwden op de identiteit van de afzender, en zodoende eerder geneigd zijn uitspraken te doen over de bekwaamheid en welwillendheid van deze afzender en organisatie, dit kan op basis van dit onderzoek echter niet met zekerheid gezegd worden.

Respondenten die versie B van de e-mail voorgelegd kregen, maakten veel meer opmerkingen betreffende identiteit. Ook waren er onder de respondenten die versie B van de e-mail voorgelegd kregen meer verschillende respondenten die identiteit beoordeelden, binnen versie A waren dit er immers slechts 4 en in versie B 7. Het lijkt er zodoende op dat de hogere mate van dwang zorgt voor meer gedachten over de identiteit van de afzender.

Organisatorische kenmerken lijken binnen versie A een grotere rol te spelen dan in versie B, binnen versie A zijn immers 40,25% van de gecodeerde opmerkingen gecodeerd als één van de organisatorische kenmerken, waar dit binnen versie B slechts 22,71% is.

Binnen versie A komen opmerkingen gecodeerd als welwillendheid overwegend positief terug en het grootste deel van de opmerkingen betreffende identiteit is neutraal, bekwaamheid wordt overwegend negatief beoordeeld. Voor versie B zijn opmerkingen overwegend negatief voor zowel welwillendheid, identiteit en bekwaamheid.

Vergelijkende analyse veiligheidscodes versie A en versie B

Tabel 22: Hoeveel procent van de code veiligheid is positief, neutraal en negatief gecodeerd, naargelang versie.

	Positief		**Neutraal**		**Negatief**		**Totaal**	
Code	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B
Veiligheid	0 (0%)	2 (3,51%)	1 (6,67%)	13 (22,81%)	14 (93,33%)	42 (73,68%)	15 (100%)	57 (100%)

Tabel 23: Hoeveel procent van het totaal aan gecodeerde segmenten valt onder de waarden positief, neutraal en negatief van de code veiligheid, naargelang versie.

	Positief		**Neutraal**		**Negatief**		**Totaal**	
Code	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B	Versie A	Versie B
Veiligheid	0 (0%)	2 (0,63%)	1 (0,42%)	13 (4,10%)	14 (5,93%)	42 (13,25%)	15 (6,36%)	57 (17,98%)
Alle codes gezamenlijk							236 (100%)	317 (100%)

Tabel 24: Bij hoeveel respondenten komt de code veiligheid voor binnen versie A en binnen versie B

Code	Versie A	Versie B
Veiligheid	5 (41,66%)	9 (75,0%)

Tabel 22, 23 en 24 maken een vergelijking van verschillen binnen de veiligheidscodes tussen versie A en versie B mogelijk. Hieruit blijkt dat in de versie met minder dwang, versie A, veel minder

opmerkingen gemaakt zijn betreffende veiligheid (15), dan binnen versie B, waar meer dwingend om een actie wordt gevraagd. Hier zijn dit er bijna vier keer zoveel, namelijk 57.
Binnen de A versie van de e-mail zijn geen positieve opmerkingen gemaakt betreffende veiligheid, binnen versie B zijn dit er 2 (3,51%). Voor zowel versie A als versie B zijn opmerkingen betreffende veiligheid overwegend negatief, versie A kent 14 (93,33%)negatieve opmerkingen betreffende de code veiligheid voor versie B zijn dit er 42 (73,68%). Tabel 23 onderbouwt het verschil tussen de opmerkingen betreffende veiligheid nogmaals, in versie A is slechts 6,36% van de gecodeerde segmenten gecodeerd als veiligheid, waar dit in versie B 17,98% van de gecodeerde segmenten is.
In tabel 24 is af te lezen dat onder de respondenten die de A versie van de e-mail voorgelegd kregen, slechts 5 (41,66%) respondenten opmerkingen hadden betreffende veiligheid, waar dit in de meer dwingende versie, versie B, 9 (75%) van de respondenten waren. Een hogere mate van dwang lijkt er zodoende voor te zorgen dat meer respondenten getriggerd worden op de code veiligheid en uitspraken doen betreffende de veiligheid. Dit betekent niet noodzakelijk dat deze respondenten een negatiever gevoel uitten betreffende veiligheid, dan bij een mindere mate van dwang.

De code keuze
Ook de code keuze speelt een rol, in versie A, de minder dwingende variant van de e-mail, maken respondenten slechts 20 keuzes, waar dit in de B versie 42 is. Het lijkt er zodoende op dat een hogere mate van dwang er voor zorgt dat respondenten eerder geneigd zijn om ook daadwerkelijk een keuze te maken om wel al dan geen actie te ondernemen.

Beantwoording hypothese
Op basis van bovenstaande analyses kunnen we de hypothese "*Er zijn verschillen in de respondents beoordelingen over de e-mail naargelang de dwingendheid van de e-mail; Een hogere mate van dwang, zorgt voor andere beoordelingen dan een lagere mate van dwang."* als volgt beantwoorden:
Zowel bij een hogere als wel lagere mate van dwang zijn de geuitte gevoelens van respondenten overwegend negatief. Op het attribuut geloofwaardigheid lijken respondenten bij een hogere mate van dwang vaker neutrale opmerkingen te maken over de inhoudelijke geloofwaardigheid, waar deze bij een lagere mate van dwang juist overwegend negatief zijn.
Op het gebied van de esthetische kenmerken, spelling, taalgebruik en opmaak zijn weinig verschillen waar te nemen, dit kan verklaard worden door het feit dat de opmaak in beide versies hetzelfde was en het taalgebruik en de spelling binnen beide versies even goed waren. Een hogere mate van dwang lijkt echter wel te zorgen voor meer perceptie betreffende het attribuut efficiëntie.
Ook maken respondenten bij een hogere mate van dwang meer opmerkingen betreffende veiligheid en identiteit. Ook het aantal opmerkingen betreffende deze veiligheid schiet door een hogere mate van dwang een flink stuk omhoog. In versie A is immers slechts 6,36% van de opmerkingen gecodeerd als veiligheid, waar dit in versie B 17,98% van de opmerkingen betreft.
Tot slot lijken respondenten, wanneer er meer dwingend om een actie gevraagd wordt, ook daadwerkelijk vaker keuzes te maken, respectievelijk 20 keuzes in de A versie van de e-mail, tegenover 42 in de B versie.

8.7 Hypothese 7: manier van lezen en interpretatie

In deze paragraaf zal de laatste hypothese van dit onderzoek beantwoord worden, deze hypothese luidt: *Er zijn verschillen waar te nemen in de manier van lezen en interpretatie van de e-mail tussen personen die wel voor de e-mail vallen en personen die niet voor de e-mail vallen.*

Om te kijken of er verschillen waar te nemen zijn tussen personen die wel en die niet voor de e-mail vallen, is de steekproef opgedeeld in drie groepen:

- Groep 1: Respondenten die expliciet kiezen niet op de e-mail in te gaan.
- Groep 2: Respondenten die geen expliciete keuze tot actie maken.

- Groep 3: Respondenten die kiezen om wel op de e-mail in te gaan.

In de eerste groep vallen de respondenten die duidelijk aangeven de gevraagde actie niet uit te gaan voeren. De tweede groep zijn de respondenten die hier geen uitlating over doen en zodoende geen keuze maken en de derde groep bestaat uit de respondenten die zegt, dit nu, of later, wel te gaan doen.
De distributie van de steekproef over deze groepen is te zien in onderstaande tabel.

Tabel 25: Distributie van steekproef over groepen

	Groep	**Absoluut**	**Procentueel**
	1	17	70,83%
	2	4	16,67%
	3	3	12,50%
			100%
Totaal respondenten			
24			

Groep 2 bestaat uit respondent 2-A, 10-A en 12-A en 4-B, en groep 3 bestaat uit respondent 7-A, 9-A en 6-B. Het is opmerkelijk dat voornamelijk onder de respondenten die de A-versie van de e-mail voorgelegd kregen, respondenten zijn die uiteindelijk geen keuze maken, dit bevestigt wederom wat al in hypothese 6 gesteld is, namelijk dat minder dwang leidt tot het minder maken van een uiteindelijke keuze.
Op basis van de indeling in groepen zijn onderstaande tabellen gemaakt, deze maken het analyseren van verschillen en overeenkomsten tussen de 3 groepen mogelijk.

Tabel 26: Hoeveel procent van elke code is positief, neutraal en negatief gecodeerd, naargelang groep.

	Positief			**Neutraal**			**Negatief**		
Inhoudelijke Code	Gr.1	Gr.2	Gr.3	Gr.1	Gr.2	Gr.3	Gr.1	Gr.2	Gr.3
Geloof - waardigheid	14,72%	29,41%	52,38%	35,03%	58,82%	23,81%	50,25%	11,76%	23,81%
	Positief			**Neutraal**			**Negatief**		
Esthetische Code	Gr.1	Gr.2	Gr.3	Gr.1	Gr.2	Gr.3	Gr.1	Gr.2	Gr.3
Spelling	66,67%	0%	0%	0%	0%	0%	33,33%	100%	0%
Efficiëntie	4,35%	33,33%	0%	4,35%	0%	0%	91,30%	66,67%	100%
Opmaak	0%	0%	0%	0%	0%	0%	100%	100%	100%
Taalgebruik	50%	33,33%	0%	50%	33,33%	0%	50%	33,33%	100%
	Positief			**Neutraal**			**Negatief**		
Organisatorische Code	Gr.1	Gr.2	Gr.3	Gr.1	Gr.2	Gr.3	Gr.1	Gr.2	Gr.3
Welwillend-heid	77,78%	40%	0%	22,22%	20%	0%	0%	40%	0%
Identiteit	14%	0%	0%	17,86%	100%	100%	67,86%	0%	0%
Bekwaam-heid	10,11%	15%	50%	14,61%	40%	12,5%	75,28%	45%	37,5%
	Positief			**Neutraal**			**Negatief**		

Veiligheidscode	Gr.1	Gr.2	Gr.3	Gr.1	Gr.2	Gr.3	Gr.1	Gr.2	Gr.3
Veiligheid	2,78%	0%	0%	19,44%	0%	0%	77,78%	0%	0%

Tabel 26 laat zien dat enkel groep 1 van de respondenten, de respondenten die besluiten niet op de e-mail in te gaan, overwegend negatief zijn op organisatorische, inhoudelijke en veiligheidscodes, op esthetiek zijn alle drie de groepen overwegend negatief, maar zoals al eerder uitgelegd, komt behalve efficiëntie geen van de esthetische kenmerken vaak genoeg voor om hier een goede vergelijking tussen groepen mee te maken. Tevens is er te zien dat respondenten uit groep 2 en groep 3, respectievelijk de groep respondenten die geen keuze maken en de groep respondenten die kiezen op de e-mail in te gaan, geen opmerkingen maken betreffende veiligheid.

Tabel 27: Hoeveel procent van de gecodeerde items valt onder elke code naargelang groep.

Inhoudelijke Code	Gr.1	Gr.2	Gr.3
Geloof - waardigheid	197 (43,02%)	17 (30,35%)	21 (53,85%)
Esthetische Code	Gr.1	Gr.2	Gr.3
Spelling	3 (0,66%)	1 (1,78%)	0 (0%)
Efficiëntie	56 (12,24%)	3 (5,26%)	3 (7,69%)
Opmaak	2 (0,44%)	1 (1,78%)	3 (7,69%)
Taalgebruik	2 (0,44%)	3 (5,26%)	2 (5,13%)
Organisatorische Code	Gr.1	Gr.2	Gr.3
Welwillend-heid	9 (1,97%)	10 (17,54%)	0 (0%)
Identiteit	28 (6,11%)	1 (1,78%)	2 (5,13%)
Bekwaam-heid	89 (19,44%)	20 (35,08%)	8 (20,51%)
Veiligheidscode	Gr.1	Gr.2	Gr.3
Veiligheid	72 (15,73%)	0 (0%)	0 (0%)
Alle codes gezamenlijk	Gr.1	Gr.2	Gr.3
Totaal	**458 (100%)**	**56 (100%)**	**39 (100%)**

Uit tabel 27 is af te lezen dat respondenten die besloten niet op de e-mail in te gaan, een hoger percentage en hoger aantal gedachten hebben betreffende efficiëntie, identiteit en veiligheid dan respondenten die geen keuze maken, of besluiten op de e-mail in te gaan.

Tabel 28: Hoeveel procent van het totaal aantal gecodeerde segmenten is positief, neutraal en negatief naargelang groep.

Totaal	Gr.1	Gr.2	Gr.3
Positief	56 (12,23%)	14 (25%)	15 (38,46%)
Neutraal	105 (22,93%)	22 (39,29%)	8 (20,51%)
Negatief	297 (64,85%)	20 (35,71%)	16 (41,03%)
Totaal	458 (100%)	56 (100%)	39 (100%)

Tabel 28 leert ons dat respondenten die besluiten niet op de mail in te gaan in hun opmerkingen negatiever zijn dan respondenten die geen keuze maken, of besluiten op de e-mail in te gaan.

Beantwoording hypothese 7
Er zijn zeer zeker verschillen waar te nemen tussen respondenten die niet en respondenten die wel voor de e-mail vallen. Het eerste wat opvalt wanneer we bovenstaande tabellen voor elke groep respondenten analyseren is dat de groep respondenten die niet besluit op de e-mail in te gaan, de enige groep is waar daadwerkelijk door de respondent aan veiligheid wordt gedacht, respondenten die geen expliciete keuze maken, of besluiten op de e-mail in te gaan, lijken dus het aspect veiligheid in de e-mail niet tegen te komen, ze nemen geen risico's waar. Tevens zijn de respondenten die geen keuze maken, of voor de e-mail vallen, positiever in hun oordelen over de e-mail dan respondenten die ervoor kiezen niet op de e-mail in te gaan. Zoals te zien in tabel 28, is in de groep respondenten die voor de e-mail valt 38,46% van de gecodeerde opmerkingen positief en 41,03% negatief, waar dit voor respondenten die besluiten niet op de e-mail in te gaan 12,23% positief en 64,85% negatief is. die besluiten op de e-mail in te gaan, dan voor respondenten die besluiten niet op de e-mail in te gaan, het aantal gecodeerde opmerkingen voor respondenten die besluiten op de e-mail in te gaan, is gemiddeld 13, respondenten die geen expliciete keuze maakten, maakten gemiddeld 14 gecodeerde opmerkingen. Waar dit voor respondenten die besluiten niet op de e-mail in te gaan 26,9 is.

9. Conclusies, aanbevelingen voor vervolgonderzoek en beperkingen.

Dit hoofdstuk stelt zich ten doel de conclusies van dit onderzoek uiteen te zetten, vervolgens zullen aanbevelingen gedaan worden voor vervolgonderzoek en tot slot zullen de beperkingen van dit onderzoek aan bod komen.

9.1 Conclusies

Deze paragraaf stelt zich ten doel de hoofdvraag van dit onderzoek te beantwoorden.
De hoofdvraag luidde als volgt:
Welke criteria nemen personen in overweging bij het beoordelen van een phishing e-mail?
Deze vraag zal worden beantwoord door gebruik te maken van de vergaarde informatie door het beantwoorden van de in hoofdstuk 7 gestelde hypothesen.

Duidelijk is geworden dat respondenten veel criteria in overweging nemen bij het beoordelen van een phishing e-mail. In dit onderzoek is gesteld dat dit in ieder geval esthetische kenmerken, inhoudelijke kenmerken, organisatorische kenmerken en veiligheids kenmerken zijn.

Onder de esthetische kenmerken werden hier de codes spelling, efficiëntie, opmaak en taalgebruik geschaard.
Het inhoudelijke element betreft de code geloofwaardigheid van de inhoud, de organisatorische kenmerken zijn welwillendheid, bekwaamheid en identiteit. Het veiligheidselement werd weergegeven door de code veiligheid.
Door het analyseren en uiteenzetten van verschillende quotes uit de interviewprotocollen is duidelijk geworden dat verschillende respondenten bij het lezen van hetzelfde stuk, over dezelfde dingen erg uiteenlopende gedachten kunnen hebben.

In dit onderzoek besteedden 11 van de 24 respondenten uitgebreid aandacht aan de afzender en aanhef van de e-mail. Het feit echter dat slechts zeven respondenten na afloop van de hardopdenksessie de aanhef van de e-mail nog wisten, geeft aan dat dit voor de meeste respondenten geen grote indruk heeft gemaakt, ondanks dat de aanhef beste klant, vanuit een bank gezien een vrij ongebruikelijke aanhef is. Het lijkt er dus op dat sommige respondenten bij het beoordelen van een phishingmail wel kijken naar aanhef en afzender, maar dat lang niet iedereen hier uitgebreid aandacht aan besteed.

In dit onderzoek wordt gesteld dat, wanneer 15% van de respondenten een bepaald kenmerk meeneemt in zijn overwegingen, er gezegd kan worden dat dit kenmerk daadwerkelijk een rol speelt bij het beoordelen van phishing e-mail.
Lettend op de esthetische kenmerken van de e-mail, bleek dat 19 van de 24 respondenten in ieder geval één van de esthetische kenmerken in overweging namen bij het beoordelen van de e-mail. In totaal waren er 4 (17%) respondenten met opmerkingen omtrent de spelling, daar de e-mail geen spelfouten omvatte, is dit nogsteeds opmerkelijk, het blijkt dat er door respondenten gedachten waren over de spelling en in gevallen zelfs spelfouten werden waargenomen die er niet waren.
Betreffende de efficiëntie van de e-mail hadden 15 (63%) respondenten op of aanmerkingen. Interessant hier is, dat wat sommige respondenten als langdradig en irritant ervoeren, door andere respondenten juist ervaren werd als handig of interessant.
Slechts in 4(17%) van de protocollen kwam de code opmaak terug, wat opmerkelijk is gezien het ontbreken van een huisstijl. Het lijkt er dus op dat de gemiddelde lezer niet noodzakelijk van een bank verwacht dat er een huisstijl gebruikt wordt in het e-mailcontact. Betreffende taalgebruik maakten 5 (21%) respondenten opmerkingen, de één vond het taalgebruik slecht voor een bank, waar een ander aangaf dat de mail juist veel banktaal gebruikte.
Organisatorische kenmerken werden door 22 van de 24 respondenten in overweging genomen.
9 (38%) respondenten maakten opmerkingen betreffende de welwillendheid, 11 (46%) betreffende de identiteit en 22 (92%) betreffende de bekwaamheid van de organisatie. Ook hier was het weer het geval, dat wat door de ene lezer als positief ervaren werd, door de andere als negatief ervaren kon worden.
Kijkend naar het veiligheidsaspect van de e-mail, is gebleken dat 14 van de 24 respondenten veiligheid in overweging nam bij het beoordelen van de e-mail. Verschillende respondenten lijken een heel verschillend idee te hebben bij veiligheid, waar de ene respondent die risico waarnam, besloot om niet te klikken omdat dit wel eens gevaarlijk kon zijn, besloot de andere juist dat klikken nog niet zo gevaarlijk kon zijn en dat het gevaar pas zou komen wanneer hij of zij gegevens in zou gaan voeren. Weer andere respondenten besloten juist dat actie ondernemen hen wel veilig leek.
Ook inhoudelijke geloofwaardigheid van de e-mail speelt een grote rol in het beoordelen van phishing e-mail. 23 van de 24 respondenten had opmerkingen betreffende de inhoudelijke geloofwaardigheid, deze opmerkingen bleken in de meeste gevallen negatief.
Naast het identificeren van de kenmerken die respondenten in overweging nemen bij het beoordelen van een phishing e-mail, heeft dit onderzoek ook een begin gemaakt in de analyse betreffende verschillen in beoordeling die gevonden worden bij verschillende maten van dwang en verschillen tussen respondenten die expliciet besluiten niet op de e-mail in te gaan, die geen keuze maken en die besluiten wel op de e-mail in te gaan. Door het lage aantal respondenten en het feit dat het

onderzoek nog geen SPSS analyses op significantie uitvoert, zijn de hier gevonden uitkomsten slechts verwachtingen van bepaalde trends.
Zo lijkt het er sterk op dat bij een hogere mate van dwang, respondenten meer gedachten hebben en zodoende meer opmerkingen maken. In de B versie van de mail is het scenario voor de respondent enigszins negatiever dan in de A versie, daar hij in de B versie al niet meer kan internetbankieren, en in de A versie gezegd wordt dat de respondent moet voorkomen dat hij niet meer kan internetbankieren, dit zou een invloed kunnen hebben op het verschil in aantal opmerkingen. Binnen de A versie van de e-mail zijn 5 (41%) respondenten die opmerkingen maken betreffende de veiligheid waar dit voor de B versie 9 (75%) van de respondenten is. Het aantal opmerkingen betreffende veiligheid betreft in de A versie 15 (6,96%) opmerkingen en in de B versie 52 (17,98%) opmerkingen. Binnen de A versie was 93,33% van de opmerkingen betreffende veiligheid negatief, waar dit binnen de B versie slechts 73,68% was. Meer specifiek zorgt een hogere mate van dwang binnen de e-mail voor meer gedachtes over veiligheid, meer dwang lijkt er voor te zorgen dat respondenten eerder geneigd zijn hun veiligheid te overdenken, echter betekend dit niet noodzakelijk dat ze ook eerder een veiligheidsprobleem herkennen. Meer dwang bleek ook voor het eerder maken van een keuze te zorgen, binnen de A versie van de mail werd 20 keer een keuze gemaakt, waar dit binnen de B versie 42 keer was, het lijkt erop dat het heel expliciet stellen van een keuze er ook daadwerkelijk voor zorgt dat mensen eerder besluiten een keuze te maken.
Verder lijkt een hogere mate van dwang er voor te zorgen dat er minder opmerkingen worden gemaakt betreffende welwillendheid en bekwaamheid, dit zou gedeeltelijk verklaard kunnen worden door het feit dat respondenten juist meer negatieve opmerkingen maken over de identiteit en omwille van een negatief gevoel bij de identiteit, niet overgaan tot het maken van opmerkingen over de bekwaamheid van de organisatie en de welwillendheid van de organisatie, daar ze de identiteit van de e-mail in twijfel trekken. Tot slot worden er bij een hogere mate van dwang meer , opmerkingen gemaakt met betrekking tot de efficiëntie van de e-mail, de opmerkingen betreffende efficiëntie zijn zowel bij een lage als hoge mate van dwang negatief. Over de overige esthetische kenmerken en inhoudelijke geloofwaardigheid zijn geen relevante uitspraken te doen op basis van dit onderzoek.
De verschillen tussen respondenten die expliciet kiezen niet op de e-mail in te gaan, respondenten die geen keuze maken en respondenten die kiezen om wel op de e-mail in te gaan, maakten duidelijk dat respondenten die geen keuze maakten en respondenten die besloten wel op de mail in te gaan, totaal niet getriggerd werden op het aspect veiligheid, in totaal maakten deze respondenten 0 opmerkingen die gecodeerd konden worden als veiligheid.
Respondenten die besloten niet op de mail in te gaan maakten gemiddeld 26,94 opmerkingen per persoon, voor respondenten die geen keuze maakten was dit 14 per persoon en voor respondenten die besloten op de e-mail in te gaan, was dit 13 per persoon. Hieruit blijkt dat respondenten die uitgebreider en meer nadenken, eerder geneigd zijn de e-mail niet te vertrouwen dan de respondenten die weinig gedachten bij de e-mail uitspreken. Weinig gedachten lijkt dus te wijzen op weinig negatieve triggers en het eerder geloven van de e-mail. Dit wordt nog eens bevestigd wanneer de groepen respondenten procentueel gezien vergeleken worden. Binnen de groep respondenten die voor de e-mail valt is 38,46% van de gedachten positief en 41,03% negatief, waar dit voor respondenten die besluiten niet op de e-mail in te gaan 12,23% positief en 64,85% negatief is.
Concluderend kan gezegd worden dat respondenten zowel esthetische, organisatorische, inhoudelijke geloofwaardigheid en veiligheidskenmerken meenemen in het beoordelen van e-mails, echter niet alle respondenten herkennen dezelfde dingen en wat de ene persoon als positief ziet, kan door een ander als negatief gezien worden. Iedereen leest zijn mail dus op verschillende wijze, de ene persoon heeft wel 60 gedachten bij een e-mail, waar een ander er maar 10 heeft. Wel lijkt het erop dat een hogere mate van dwang er voor zorgt dat respondenten meer veiligheidsaspecten herkennen, en respondenten die uiteindelijk voor een phishing e-mail vallen of besluiten er niet op in te gaan, lijken deze aspecten totaal niet tegen te komen. Het lijkt er dus op dat voornamelijk het nadenken over de veiligheid er voor zorgt dat een respondent wel of niet op een e-mail ingaat.

9.2 Aanbevelingen voor vervolgonderzoek

De gegevens verkregen in dit onderzoek bieden de mogelijkheid tot veel vervolgonderzoek en verdere analyses en indien het gegevensbestand uitgebreid wordt, kunnen op basis van het nu gedane onderzoek veel vervolgonderzoeken gedaan worden.

Het belang van elk criterium

Dit onderzoek heeft zich enkel ten doel gesteld de criteria die een rol spelen bij het lezen van e-mail te identificeren, het lijkt erop dat veiligheid een grote rol speelt en dat het percentage positieve en negatieve gedachten ook belangrijk is in het al dan niet klikken. Een grotere mate van dwang lijkt er voor te zorgen dat respondenten eerder veiligheidskenmerken herkennen. In vervolgonderzoek kan duidelijk gemaakt worden wat het belangrijkste criterium is en hoeveel elk van de criteria meewegen in de overwegingen van respondenten.

Het doel van de e-mail

In het interview dat volgde op de hardop denk sessies werd de vraag gesteld "*Wat denkt u dat het actiedoel van de e-mail was?".* Ondanks dat geen van de respondenten uiteindelijk voor de phishing e-mail gevallen is, geven veel respondenten aan dat het actiedoel informeren en overtuigen is.
Veel respondenten lijken, ondanks dat ze de juiste keuze maken en niet op de e-mail ingaan, niet te beseffen dat het actiedoel van de e-mail is om achter inloggegevens te komen.
Wanneer respondenten zich beter bewust zijn van de criteria die terugkomen in een phishing e-mail zullen zij dit actiedoel misschien wel kunnen identificeren.
Een uitgebreid onderzoek wat zich ten doel stelt om de standaard misleidingstechnieken gebruikt in phishing e-mails te identificeren kan leiden tot meer kennis en er zodoende voor zorgen , door gerichtere campagnes, dat ontvangers van phishing e-mail een e-mail wel zelf kunnen bestempelen als phishing.

Mate van dwang

Tussen de A en B versie van deze e-mail is een verschillende mate van dwang gecreëerd, waar de A versie van de e-mail vraagt om gegevens bij te werken. Wordt in de B versie een daadwerkelijke beperking opgelegd wanneer dit niet wordt gedaan, namelijk, men kan dan niet meer internetbankieren.
In vervolgonderzoek is het interessant om op extensievere wijze te onderzoeken hoe de mate van dwang invloed heeft op hoe mensen phishing e-mails beoordelen.

Uitbreiden van de dataset en eventuele statistische analyses

Wanneer de dataset uitgebreid wordt is het mogelijk om statistische analyses te doen, om zodoende de veronderstellingen met betrekking tot de verschillen geïdentificeerd bij verschillende maten van dwang en de verschillen tussen respondenten die wel en niet op de e-mail in te gaan, statistisch te toetsen op significantie.

9.3 Beperkingen

Ondanks dat dit onderzoek ons kennis verschaft in de criteria die in overweging worden genomen bij het beoordelen van e-mail, zijn er ook enkele beperkingen aan het onderzoek.

Dit onderzoek is uitgevoerd met twee varianten van slechts 1 phishing e-mail.
De codes opgesteld op basis van de variabelen organisatie, inhoud, esthetiek en veiligheid komen in de protocollen allemaal terug, maar er blijft een kleine kans dat bij analyse van een andere e-mail blijkt dat nog meer factoren een rol spelen in de beoordeling van e-mail.
We kunnen op basis van dit onderzoek alleen zeggen, dat de hier gedefinieerde attributen in ieder geval een rol spelen bij het beoordelen van e-mails.

De steekproef in het onderzoek is met 24 personen tevens vrij klein, het uitvoeren van hardop denk sessies met meer personen kan eveneens leiden tot de conclusie dat meer factoren een rol spelen in de beoordeling van e-mail, tevens kan een onderzoek met meer respondenten SPSS analyses betreffende significantie mogelijk maken, om zodoende relaties te testen.

10.Literatuurlijst

Cialdini, R. B. (2001). The science of persuasion. *SCIENTIFIC AMERICAN-AMERICAN EDITION-*, *284*(2), 62-67.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590). ACM.

Egelman, S., Cranor, L. F., & Hong, J. (2008, April). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1065-1074). ACM.

Grazioli, S., & Wang, A. (2001, December). Looking without seeing: understanding unsophisticated consumers' success and failure to detect Internet deception. In *Proceedings of the 22nd International Conference on Information Systems. New Orleans*.

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the Internet. *Group Decision and Negotiation*, *13*(2), 149-172.

Heerkens, J.M.G. (1999). *Instructie voor proefleiders bij het onderzoek 'het afwegen van kenmerken van kapitaalgoederen.* Universiteit Twente

Heerkens, J.M.G., *Het interview na afloop van de hardop denksessie*. Universiteit Twente

Heerkens, J.M.G., *Codeerschema voor het onderzoek: Afwegingen bij inkoopprocessen*. Universiteit Twente

Herley, C. (2012). Why do Nigerian Scammers Say They are from Nigeria?. In *Proceedings of the Workshop on the Economics of Information Security*.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y. K. (2007). What instills trust? a qualitative study of phishing. *Financial Cryptography and Data Security*, 356-361.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709-734.

Nhan, J., Kinkade, P., & Burns, R. (2009). Finding a Pot of Gold at the End of an Internet Rainbow: Further Examination of Fraudulent Email Solicitation.*International Journal of Cyber Criminology*, *3*(1).

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in human behavior*, *21*(1), 105-125.

Norton(2014). Online fraud: Phishing, *us.norton.com.* Ontvangen op 20-1-2014, via: http://us.norton.com/cybercrime-phishing

NOS (2011). Schade door phishing verdubbeld, *Nos.nl*. ontvangen op: 9-9-2013, via: http://nos.nl/artikel/313214-schade-door-phishing-verdubbeld.html

Someren, M. W. V., Y. F. Barnard, et al. (1994). *The think aloud method*. London, Academic Press.

Walter, Z. (2007, September). Web credibility and stickiness of content Web sites. In *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on* (pp. 3820-3823). IEEE.

11. Appendices

11.1 Introductie van de opdracht

2. Instructies voor de proefleider

De taken van de proefleider

De proefleider heeft de volgende taken:

1: De opdracht toelichten.
2: Ervoor zorgen dat de proefpersoon hardop blijft denken.
3: De proefpersoon helpen bij vragen of problemen.
4: Ervoor zorgen dat de gedachten en handelingen van de proefpersoon worden vastgelegd.
5: Ervoor zorgen dat alle verzamelde informatie aan het einde van de hardop-denk-sessie wordt verzameld.

1 De opdracht toelichten

Stel jezelf voor als de proefpersoon binnenkomt (indien nodig).
Hallo, ik ben Lars Mol, student aan de UT, ik zit in de afsluitende fase van mijn bachelor Bestuurskunde en hoop door deze interviews meer informatie te verzamelen voor mijn onderzoek naar marketing in e-mails.
Wilt u een kopje koffie, thee of een glaasje water?
U kunt gedurende het experiment op elk moment koffie, thee of water pakken, dit hoeft u niet aan mij te vragen.

Wat is uw naam?
Wat is uw baan/ studierichting?
Mag ik u vragen wat uw hoogst genoten schoolopleiding is die u met een diploma heeft afgerond?
En uw leeftijd?
Hoeveel uur zit u per week achter de computer (hoeveel is daarvan privé en hoeveel werk)? Hoe vaak bekijkt u daarbij uw e-mail?

Vertel dat je een aantal zaken letterlijk zult voorlezen omdat iedere proefpersoon precies hetzelfde te horen moet krijgen. Het komt misschien ietwat geforceerd over, maar het is de beste manier om het onderzoek uit te voeren.
Ik zal een aantal zaken letterlijk voorlezen, omdat elke proefpersoon precies hetzelfde te horen moet krijgen, het kan dus zijn dat ik wat geforceerd overkom, maar het is de beste manier om dit onderzoek uit te voeren.

Begin daarna met het letterlijk oplezen van de volgende tekst:

Zo meteen krijgt u van mij een e-mail. Bij dit experiment wil ik graag weten wat u denkt bij het lezen van de e-mail. Om dit te bereiken vraag ik u hardop te denken tijdens het lezen van de e-mail. Met 'hardop denken' bedoel ik dat u alles wat u denkt hardop zegt, vanaf het moment dat u begint met het lezen van de e-mail, tot op het moment dat u de gehele e-mail door hebt gelezen.
Blijf voortdurend hardop zeggen wat u denkt. U kunt uw gedachten allemaal uitspreken en hoeft deze niet van tevoren te ordenen, ook hoeft u niet uit te leggen waarom u denkt wat u denkt.

U mag denken en handelen alsof u alleen in deze kamer bent en u hardop tegen uzelf praat. Het is erg belangrijk dat u blijft praten. Als u langere tijd niets zegt zal ik u vragen hardop te denken.
Datgene wat u zegt wordt opgenomen met een voicerecorder, zodat ik naderhand het interview uit kan werken en het kan vergelijken met andere interviews op overeenkomsten, verschillen en opvallendheden. Deze informatie wordt vertrouwelijk behandeld. Dat wil zeggen dat uw anonimiteit gewaarborgd blijft en uit het onderzoeksrapport niet kan worden afgeleid van welke proefpersoon bepaalde informatie afkomstig is.
Voordat ik u de opdracht geef krijgt u eerst enige informatie over het doel van dit experiment en over de wijze waarop de opdracht moet worden uitgevoerd. Daarna zullen we samen enkele kleine proefopgaven doen om u te laten oefenen in het hardop denken.
Als we dit gedaan hebben, ontvangt u de eigenlijke opdracht.
Ik wil u nu vragen om de achtergrondinformatie door te lezen. Als er iets onduidelijk is, kunt u mij om uitleg vragen. U hoeft nu nog niet hardop te denken.

Reik de achtergrondinformatie uit ('Het experiment en uw rol daarin') en geef de proefpersoon 10 minuten de tijd om de achtergrondinformatie door te lezen. Overigens heeft de proefpersoon waarschijnlijk niet zoveel tijd nodig.

Begrijpt u wat er van u wordt verwacht?

Beantwoord eventuele vragen. Vestig daarna, voor zover dat nog niet is gebeurd tijdens het beantwoorden van de vragen, de aandacht op de volgende punten. Kijk na elk punt de proefpersoon even aan om te zien of het duidelijk is

Nog even samenvatten:
1: U kunt het best uw eigen logica gebruiken, zonder rekening te houden met wat u denkt dat anderen in de organisatie (of ik als proefleider) al dan niet juist of acceptabel vinden. Voor het maken van een afweging is geen standaardmethode beschikbaar, dus u moet afgaan op uw eigen inzicht.
2: U moet alle gedachten onmiddellijk uitspreken, hoe onbelangrijk, 'gek' of onrijp ze voor u ook mogen lijken, ook spreekt u de handelingen die u op de computer onderneemt hardop uit;
3: Ik als proefleider ben aanwezig om vast te leggen wat u zegt en doet. Het is de bedoeling dat u hardop nadenkt.
Het is dus niet de bedoeling dat u tegen mij praat, tenzij u bijvoorbeeld behoefte hebt aan schrijfpapier en dergelijke;
4: Inhoudelijke vragen over de opdracht kunnen niet door mij worden beantwoord. Ik kan u dus niet helpen met het uitvoeren van de opdracht;
5: Het maakt niet uit wat voor een besluit u na het lezen van de e-mail neemt, er zijn immers geen goede en geen foute antwoorden, zolang u maar al uw gedachten en gevoelens hardop uitspreekt.
Schrik niet indien ik aan het schrijven ben, dit doe ik enkel om bij het interview achteraf een geheugensteun te hebben.
6: Maak indien u dat zinnig vindt aantekeningen. De aantekeningen zou ik graag na afloop van het experiment van u willen hebben, om ze eventueel voor mijn onderzoek te kunnen gebruiken.

NB: Laat je niet in met de interpretatie van de opdracht door de proefpersoon, tenzij je van mening bent dat bijvoorbeeld het taalgebruik in de opdracht misverstanden oproept.

Is duidelijk wat er van u wordt verwacht?

Beantwoord eventuele vragen.

Mooi zo. We beginnen met vier kleine oefenproblemen. Ze hebben inhoudelijk niets met de opdracht te maken maar ze geven u de gelegenheid te oefenen in het hardop denken. Allereerst vraag ik u twee getallen te vermenigvuldigen en mij te vertellen wat u denkt terwijl u het antwoord berekent.
Indien alles duidelijk is zet ik nu de voicerecorder aan.

Zet de voicerecorder aan.

Hoeveel is 24 maal 36?

Geef de proefpersoon een minuut de gelegenheid de opdracht uit te voeren. Het antwoord is overigens 864, maar het gaat er niet om of de proefpersoon het juiste antwoord vindt, alleen of hij/zij hardop denkt.

Goed. Nu geef ik u nog twee oefenproblemen voordat we beginnen aan het eigenlijke experiment. De opdracht is voor beide oefenproblemen gelijk: hardop uw gedachten weergeven terwijl u de opdracht uitvoert. Hier is het tweede oefenprobleem:
In deze opdracht is het de bedoeling dat u een opsomming geeft. U hoeft het aantal opgesomde items niet bij te houden; dat doe ik voor u.

Noem twintig diersoorten.

Geef de proefpersoon een minuut de gelegenheid de opdracht uit te voeren.

Als de proefpersoon tussen het noemen van de diersoorten lang nadenkt, wijs hem/haar daar dan op. Deze oefening is juist bedoeld om de proefpersoon te leren om bijvoorbeeld ook gedachten over de te gebruiken systematiek (bijvoorbeeld eerst huisdieren, dan dieren uit de dierentuin etc.) weer te geven.

Prima. Voor het laatste oefenprobleem wil ik u vragen achter de computer plaats te nemen.
Open outlook en daarin "MAP 1".

Lees nu de e-mail hardop voor en denk hardop na tijdens de opdracht, dus bij alles wat u leest, vergeet niet al uw gedachtes uit te spreken.

Geef de proefpersoon onderstaande e-mail.

-----Original Message-----
From: Minahermans@gmail.com
Sent: Tuesday, may 21, 2013 12:34 PM
Subject: Buurt BBQ vanavond

Beste Peter,

Vandaag hebben wij Whiskey helaas moeten laten inslapen, hij had al een tijdje last van vocht in de buik en de dierenarts raadde ons sterk aan om Whiskey te laten inslapen aangezien hij veel pijn had en toch niet lang meer had.
Frans en ik zijn er stuk van en zullen daarom vanavond helaas toch niet op de buurt barbecue aanwezig zijn.

Groetjes,

Evelien

Goed zo. Dit waren de oefenopgaven. Nu kunnen we beginnen aan het eigenlijke experiment.
U zult een e-mail te lezen krijgen die u dient door te nemen alsof u hem zelf ontvangen heeft, denk u in dat u achter uw eigen computer zit en de e-mail doorleest.
Indien geen klant bent bij de gegeven organisatie, denk u dan in dat dit wel het geval is.
Spreek al uw gedachten bij de opdracht van deze e-mail uit
Het is van groot belang dat u hardop blijft denken, u kunt niks raars of fouts zeggen.
Heeft u voorafgaande aan de opdracht nog vragen?

Reik de Opdracht uit.

Beantwoord eventuele vragen.

Zet de recorder aan.

Dan wil ik u nu vragen om de e-mail die staat in "MAP A" te openen en aan de opdracht te beginnen.
U heeft voor de opdracht een half uur de tijd. Veel succes. Denk vanaf nu hardop.
Dit houdt in dat u ook wat u leest uitspreekt.
-Noteer de tijd-

5 Debriefing

Voorafgaande aan het onderzoek heb ik u verteld dat het een onderzoek betreft waarmee we meer inzicht willen creëren in de manier waarop mensen marketing e-mails lezen. Tevens zei ik dat wij wilden onderzoeken hoe goed mensen de kwaliteit van de communicatie van bedrijf richting consument achtten.

Op dit moment kan ik u nog geen resultaten geven van het onderzoek, aangezien ik er nog volop mee bezig ben, indien u het interessant vindt om de uitkomsten van mijn onderzoek te ontvangen, wil ik u vragen uw e-mail adres achter te laten, zodat ik u de uitkomsten later toe kan sturen.

Tot slot wil ik u heel erg bedanken voor uw deelname aan het onderzoek, als dank heb ik nog een klein presentje voor u.

Overhandig USB stick.

11.2 Achtergrond informatie

1.Het experiment en uw rol daarin

Inleiding

Het doel van dit onderzoek is om te weten te komen wat mensen vinden van de manier van marketing en communicatie van verschillende bedrijven in hun e-mails.
In meerdere mate gaat het erom te weten te komen wat voor een gevoel u bij de e-mails krijgt, en of en zo ja hoe, dat gevoel gedurende het lezen verandert.
Een fictief voorbeeld: De Albert Heijn heeft als vervanging van de bonuskaart een pasje waarop u AH-Miles kunt sparen en legt via de e-mail uit hoe dit werkt en biedt gelijk de mogelijkheid om het pasje online aan te vragen. Wij zijn geïnteresseerd in uw gedachtegangen bij deze e-mail, vindt u de uitleg die Albert Heijn geeft goed en duidelijk en zou u het AH-Miles pasje gelijk bestellen?

Als u besluiten neemt voor uzelf is er in de regel geen reden om uw afweging zo expliciet te maken als hier gebeurt. Maar als u een besluit neemt als werknemer voor een bedrijf zult u uw beslissing grondig moeten kunnen motiveren. Dat kan onder meer gebeuren door aan te geven hoeveel belang u hecht aan bepaalde kenmerken.
Bij dit onderzoek wordt u gevraagd om **tijdens de opdracht** al uw afwegingen en gedachtes betreffende de e-mails uit te spreken.

Hieronder vindt u informatie met betrekking tot het doel van de opdracht en de wijze waarop deze moet worden uitgevoerd. Verder worden enkele aanwijzingen gegeven die u kunnen helpen bij het hardop uitspreken van uw gedachten en wordt de rol van de proefleider toegelicht. Lees de informatie zorgvuldig door. Daarna zal de proefleider u vragen of alles duidelijk is. Zo ja, dan krijgt u enkele korte opgaven om te oefenen in het hardop denken
Vervolgens ontvangt u de opdracht. Denk hardop vanaf het moment dat u de opdracht krijgt.

Het doel van de opdracht

Het doel van de opdracht die u gaat uitvoeren is: meer inzicht creëren in de manier waarop mensen marketing e-mails lezen en uitvinden hoe goed mensen de kwaliteit van de communicatie van bedrijven richting consument achten.
Uw taak is om de u voorgelegde e-mail zo zorgvuldig mogelijk door te lezen.
Het is de bedoeling dat u datgene wat u denkt gedurende de hele tijd hardop uitspreekt.

Belangrijk: Het maakt niet uit wat voor een besluit u na het lezen van de e-mail neemt, er zijn immers geen foute antwoorden, zolang u maar al uw gedachten en gevoelens hardop uitspreekt.

De resultaten van dit onderzoek zullen worden gebruikt om in een latere fase meer inzicht te krijgen welke marketing strategieën en manieren van informatie verschaffing nou wel en niet werken en wat hier nou de redenen van zijn.

De uitvoering van de opdracht

Van u wordt een zo nauwkeurig mogelijke afweging verwacht. U bent niet gebonden aan wat u denkt dat in het algemeen logisch of correct wordt gevonden maar mag uw eigen persoonlijke logica hanteren. Er is bij deze opdracht geen juiste wijze van afwegen. Vele wijzen van afwegen kunnen

juist zijn. De onderzoeker heeft zich dan ook vooral geen beeld gevormd van de afwegingen die mogelijk zijn.
Alle afwegingen die voor u relevant zijn, zijn voor ons dan ook interessant.

De beschikbare middelen

U heeft een half uur beschikbaar voor deze opdracht. Afsluitend volgt een interview.
U kunt gebruik maken van potlood en papier.
Behalve de e-mail ontvangt u geen informatie, de e-mail is alles wat u nodig heeft.

De rol van de proefleider

De proefleider is slechts aanwezig om uw gedachten en handelingen vast te leggen. Hij of zij geeft u geen extra informatie. Als u vergeet om uw gedachten hardop uit te spreken zal de proefleider u hierop wijzen. Gedurende het experiment zal de proefleider soms aan het schrijven zijn, schrik hier niet van, dit gebeurt enkel om eventuele onderwerpen te noteren voor het interview achteraf.

Hardop denken

Lees tijdens het experiment de e-mail hardop. Spreek tevens elke gedachte die bij u opkomt onmiddellijk uit, ook als hij volgens u niets met de opdracht heeft te maken of als u er niet zeker van bent dat de gedachte juist is. Bij het beoordelen van de wijze waarop u de opdracht uitvoert wordt niet zozeer gekeken naar de 'juistheid' van uw gedachten maar vooral naar de compleetheid van de weergave ervan.
Probeer niet om gedachten toe te lichten of samen te vatten voor de proefleider. Dit kan de uitvoering van de opdracht verstoren.

<u>De opdracht</u>

U zult straks plaats nemen achter een computer om een e-mail door te lezen.
Stelt u zich voor dat dit uw computer is en dat het een e-mail is die u daadwerkelijk heeft gekregen.
U leest de e-mail door en bij dit doorlezen leest u hardop en spreekt u alles wat u denkt hardop uit. U bent volkomen vrij in de wijze waarop u eventuele besluiten neemt.
Nogmaals, wees u er terdege van bewust dat er geen foute en goede antwoorden zijn, tevens is geen enkele gedachte raar. Zolang u maar de afwegingen maakt en besluiten neemt die u juist acht.

11.3 E-mail versie A

-----Original Message-----
From: Storing ING
Sent: Saturday, April 06, 2013 12:34 PM
Subject: Storing Mijn ING verholpen

Beste klant,

Gisteren, woensdag 3 april, zijn er problemen geweest met de weergave van de af- en bijschrijvingen en daarmee het saldo van onze klanten in onze systemen. Op dit moment draait alles weer correct en zijn alle problemen opgelost.

Uiteraard wil ik u in meer detail uitleggen wat er is gebeurd, maar allereerst wil ik u mijn welgemeende excuses aanbieden. U heeft door de verstoring hinder ondervonden. U mag van ons verwachten dat u gemakkelijk en foutloos uw bankzaken dagelijks bij ons kunt regelen. Hier zijn wij gisteren helaas niet in geslaagd.

Wat is er gisteren precies gebeurd?

In de nacht van dinsdag 2 april op woensdag 3 april is het boekingsproces van ING door een technisch probleem vastgelopen. Hierdoor moest de gehele verwerking gisteren opnieuw plaatsvinden. Vanwege het lange paasweekend waren er veel betaaltransacties en duurde deze verwerking langer. Hierin is een vertraging ontstaan waardoor bepaalde betaalopdrachten tijdelijk dubbel zijn uitgevoerd. Dit had tot gevolg dat sommige klanten een verkeerd saldo zagen. Een aantal klanten heeft hierdoor onterecht rood gestaan, waardoor ze niet konden pinnen. We hebben direct maatregelen getroffen om te zorgen dat alle klanten met hun ING betaalpas ongeacht het rekeningsaldo tot 250 euro geld konden opnemen en konden betalen bij alle pinautomaten. Klanten die hierdoor te maken hebben gekregen met een roodstand hoeven zelf geen actie te ondernemen. Hiervoor worden geen kosten in rekening gebracht.

Evaluatie en verbetering

We zijn gisteren direct begonnen met de verschillende evaluaties, van zowel de technische aspecten van de storing tot het klantcontact en de communicatie. Alle bevindingen die daaruit voortkomen waarmee we onze dienstverlening aan u verder kunnen verbeteren worden natuurlijk doorgevoerd. Ik ben me bewust van de impact die dit incident op u als klant had en de ongerustheid en onduidelijkheid die het teweeg heeft gebracht. Het gaat om de kern van onze dienstverlening en wij zullen er alles aan doen om u de dienstverlening te bieden die u van ons mag verwachten.

Om vervelende omstandigheden te voorkomen, willen wij u vragen om uw rekening bij te werken via onderstaande link Inloggen Internet Bankieren

Vriendelijke groet,
Nick Jue

11.4 E-mail versie B

-----Original Message-----
From: Storing ING
Sent: Saturday, April 06, 2013 12:34 PM
Subject: Storing Mijn ING

Beste klant,

Gisteren, woensdag 3 april, zijn er problemen geweest met de weergave van de af- en bijschrijvingen en daarmee het saldo van onze klanten in onze systemen. Op dit moment draait bijna alles weer correct en zijn de meeste problemen opgelost.

Uiteraard wil ik u in meer detail uitleggen wat er is gebeurd, maar allereerst wil ik u mijn welgemeende excuses aanbieden. U heeft door de verstoring hinder ondervonden. U mag van ons verwachten dat u gemakkelijk en foutloos uw bankzaken dagelijks bij ons kunt regelen. Hier zijn wij gisteren helaas niet in geslaagd.

Wat is er gisteren precies gebeurd?

In de nacht van dinsdag 2 april op woensdag 3 april is het boekingsproces van ING door een technisch probleem vastgelopen. Hierdoor moest de gehele verwerking gisteren opnieuw plaatsvinden. Vanwege het lange paasweekend waren er veel betaaltransacties en duurde deze verwerking langer. Hierin is een vertraging ontstaan waardoor bepaalde betaalopdrachten tijdelijk dubbel zijn uitgevoerd. Dit had tot gevolg dat sommige klanten een verkeerd saldo zagen. Een aantal klanten heeft hierdoor onterecht rood gestaan, waardoor ze niet konden pinnen. We hebben direct maatregelen getroffen om te zorgen dat alle klanten met hun ING betaalpas ongeacht het rekeningsaldo tot 250 euro geld konden opnemen en konden betalen bij alle pinautomaten. Klanten die hierdoor te maken hebben gekregen met een roodstand hoeven zelf geen actie te ondernemen. Hiervoor worden geen kosten in rekening gebracht.

Evaluatie en verbetering

We zijn gisteren direct begonnen met de verschillende evaluaties, van zowel de technische aspecten van de storing tot het klantcontact en de communicatie. Alle bevindingen die daaruit voortkomen waarmee we onze dienstverlening aan u verder kunnen verbeteren worden natuurlijk doorgevoerd. Ik ben me bewust van de impact die dit incident op u als klant had en de ongerustheid en onduidelijkheid die het teweeg heeft gebracht. Het gaat om de kern van onze dienstverlening en wij zullen er alles aan doen om u de dienstverlening te bieden die u van ons mag verwachten.

Om vervelende omstandigheden te voorkomen is uw account voor het internetbankieren in een beveiligde omgeving geplaatst, wat betekent dat u op dit moment niet meer kunt internetbankieren. U dient deze blokkering op te heffen door in te loggen op onderstaande link en vervolgens het formulier dat verschijnt in te vullen Inloggen Internet Bankieren

Vriendelijke groet,
Nick Jue
Directievoorzitter ING Nederland

11.5 Interviewvragen

4 Het interview achteraf

De opdracht is nu voltooid. We zijn nu toe aan het laatste deel van dit experiment. Ik wil u enkele vragen stellen over de wijze waarop u de opdracht heeft uitgevoerd. De antwoorden dienen als aanvulling op hetgeen u heeft gezegd tijdens het uitvoeren van de opdracht. Eerst zal ik enkele meer algemene vragen stellen. Daarna kunnen we dieper ingaan op punten die voor dit onderzoek van bijzonder belang zijn. Als op enig moment iets niet duidelijk is of u wilt zelf iets ter sprake brengen, doe dat dan gerust.

Vraag 1: Zijn er gedachten die u tijdens het hardopdenken niet kwijt kon, maar die u nu toch nog graag wilt uitspreken?

Vraag 2: Kunt u formuleren wat volgens u de centrale boodschap van de e-mail was?
Vraag 3: Wat denkt u dat het actiedoel van de e-mail was? (Informeren, overtuigen)
Vraag 4: Kunt u aangeven of u op momenten moeite had met de opdracht?
Vraag 5: Weet u nog wat de aanhef van de e-mail was?
Vraag 6: Vond u dit een gebruikelijke of ongebruikelijke aanhef voor een e-mail van dit type organisatie?
Vraag 7: Weet u nog wat de groet aan het einde van de e-mail was?
Vraag 8: Vond u dit een gebruikelijke of ongebruikelijke afsluiting voor een e-mail van dit type organisatie?
Vraag 9: Weet u nog wie de afzender van de e-mail was?
Vraag 10: In welke mate acht u de afzender betrouwbaar?
Vraag 11: In de e-mail wordt bepaalde informatie verstrekt, in welke mate acht u de verstrekte informatie betrouwbaar?
Vraag 12: Aan het einde van de e-mail wordt u gevraagd om een actie te ondernemen, weet u nog wat dit was?
Vraag 13: Zou u deze actie uitgevoerd hebben?
Vraag 14: Kunt u aangeven op welke momenten u volgens u een keuze moest maken?
Vraag 15: Welke keuze heeft u toen gemaakt?
Vraag 16: Wat heeft u doen besluiten om deze keuze te maken?
Vraag 17: Wat was/waren volgens u de alternatieve keuze mogelijkheden? Gemaakt?

Dit waren de inhoudelijke vragen, dan wil ik tot slot een paar vragen over het verloop van het onderzoek stellen.
Vraag 18: Was er voldoende tijd beschikbaar voor het uitvoeren van de opdracht?
Vraag 19: Vond u het moeilijk of vervelend om hardop te denken?
Vraag 20: Denkt u dat het uitvoeren van de opdracht gemakkelijker of moeilijker zou zijn gegaan als ik geen voicerecorder zou hebben gebruikt?
Vraag 21: Denkt u dat het uitvoeren van de opdracht gemakkelijker zou zijn geweest zonder mijn aanwezigheid?
Vraag 22: Denkt u dat u voldoende tot uitdrukking hebt kunnen brengen wat u dacht en deed?
Vraag 23: Wilt u hier nog iets aan toevoegen?

11.6 Reflectieverslag

Inleiding

Door middel van dit reflectieverslag blik ik terug op het professioneel functioneren tijdens het uitvoeren van mijn bacheloropdracht, uitgevoerd ter afsluiting van de opleiding European Public Administration aan de Universiteit Twente. In mijn opdracht heb ik een onderzoek gedaan naar wat voor kenmerken mensen in overweging nemen bij het lezen van phishingmails. Hierbij ben ik begeleid door Dhr. J.M.G. Heerkens, Mw. M.Junger en Dhr. E.E.H. Lastdrager. Achtereenvolgend zal ik nu mijn leerpunten bespreken en een kritische blik werpen op punten waarop ik kan verbeteren.

Wat heb ik geleerd?

Tijdens het uitvoeren van deze opdracht heb ik voor het eerst een empirisch onderzoek van begin tot eind zelf uitgevoerd. Het allereerste leerpunt voor mij was gelijk aan het begin van mijn bacheloropdracht. Waar een onderzoeksvraag gedefinieerd moet worden. In eerste instantie wilde ik veel te grote dingen onderzoeken, Dhr. Van der Kolk heeft mij gestuurd in het opstellen van een kleinere, beter handelbare onderzoeksvraag. Ik heb zodoende geleerd dat het belangrijk is om het tijdsbestek dat je beschikbaar hebt voor het beantwoorden van een onderzoeksvraag goed in overweging te nemen bij het kiezen van deze onderzoeksvraag.
Voor het uitvoeren van mijn onderzoek heb ik veel theorie moeten lezen om zodoende een theoretisch kader te kunnen schrijven, waarin de theorie belangrijk voor mijn onderzoek terugkwam, maar irrelevante informatie niet meegenomen werd
Na het opstellen van mijn theoretisch kader ben ik bezig gegaan met mijn daadwerkelijke onderzoeksopzet, ik heb hier geleerd dat een goed onderzoek opzetten heel wat tijd vergt en dat er veel verschillende manieren zijn van een onderzoek doen. In het geval van mijn onderzoek moesten interviewvragen, protocollen en e-mails opgesteld worden die ik aan respondenten zou laten lezen, ik heb in ogenschouw leren nemen hoe ik een protocol en interviewvragen op moet stellen wat voor een breed scala aan mensen goed begrijpbaar is.
Na het maken van mijn onderzoeksopzet ben ik begonnen met de dataverzameling, allereerst is een pilot uitgevoerd, om te kijken of de opzet goed was, waarna ik echt met proefpersonen contact heb opgenomen. Ik ben daarna hardopdenksessies gaan afnemen, ik heb zodoende geleerd hoe hardopdenksessies werken. Er is mij duidelijk geworden dat het lastig is om proefpersonen te werven, ik denk dat ik zelf na het uitvoeren van dit onderzoek dan ook vaker zelf aan onderzoeken van andere studenten zal meewerken. Tevens werd mij duidelijk dat verschillende personen met erg verschillende insteken een onderzoek ingaan
Na mijn dataverzameling ben ik begonnen met het invoeren van mijn data, het invoeren van mijn data bestond uit het uittypen van protocollen en deze coderen, ik verwachtte dat dit werk wel mee zou vallen, maar voor alle codes goed waren heb ik deze toch een keer of drie moeten aanpassen. Ik heb zodoende geleerd dat goed coderen een secuur en lastig werk is.
Tot slot ben ik de gegevens gaan analyseren om zodoende tot een antwoord op mijn onderzoeksvraag te komen. Ik heb geleerd dat ik een enkele set aan gegevens op heel veel verschillende manieren cijfermatig kan analyseren en dat je daarnaast ook door middel van het presenteren van tekst uit de protocollen statements soms goed kan onderbouwen. Tot slot heb ik gemerkt dat ik goed ben in het werken met Excel en dat ik het analyseren van cijfertjes leuk vind.

Wat kan ik verbeteren?
Ik ben ruim een jaar bezig geweest met het uitvoeren van deze opdracht, dit komt gedeeltelijk door veel ziekte, maar anderzijds door een slechte planning. Ik moet sneller afspraken met begeleiders plannen wanneer ik ergens vastloop en dingen minder op zijn beloop laten.

Tevens heb ik gemerkt dat ik niet sterk ben in het schrijven van een coherent verhaal, hierin kan ik door het vaker schrijven van essays en verslagen beter worden. Ook heeft Dhr. Lastdrager mij, voor het schrijven van een coherent verhaal, de tip gegeven om bij elke paragraaf in één zin aan te geven wat ik in deze paragraaf nou vertel en wat ik er zou moeten vertellen, ook deze strategie kan mij in andere onderzoeken helpen om gemakkelijker een coherent verhaal te schrijven. Tot slot moet ik leren dat het niet noodzakelijk betekend dat iets goed te begrijpen is wanneer ik het zelf begrijp. In het geval van mijn Excel tabellen waren deze voor mij gelijk al duidelijk, maar mijn begeleiders gaven aan dat deze niet makkelijk te interpreteren waren. Om dit in één keer goed te doen, kan ik volgende keer mijn tabellen aan derden laten lezen en vragen of zij ze begrijpen.

Conclusie

Door dit onderzoek heb ik geleerd hoe ik een echt empirisch onderzoek opzet en heb ik geleerd dat mijn interesse binnen een onderzoek ligt op de analyse van gegevens en dan voornamelijk in het cijfermatige gedeelte. Ik ben erachter gekomen dat ik niet heel sterk ben in het schrijven van een samenhangend verhaal en dat ik hierin nog zal moeten verbeteren. Ook heb ik wederom gezien dat planning niet mijn sterkste kant is. Al met al denk ik dat het uitvoeren van deze bacheloropdracht een leerzame ervaring is geweest en ben ik tevreden met wat ik uiteindelijk op papier heb gezet!