# Haastige Spoed is Zelden Goed. Ook Online.

De invloed van een verhoogde systematische verwerking op de effectiviteit van phishing berichten bij senioren

Mart Geurts (4368118)
In opdracht van: de Veiligheidsregio Limburg-Noord
Interne Begeleider: Doeschka Anschutz
Tweede lezer: Daniela Becker
Externe begeleiders: Nick Boersma, Danique Willemsen
Faculteit Sociale Wetenschappen
Radboud Universiteit Nijmegen
Datum: 31 Augustus 2020
Woordenaantal: 5432

## Samenvatting

Een variant van internetcriminaliteit: phishing, is een wereldwijd probleem. Phishing houdt in dat criminelen door middel van misleiding persoonlijke gegevens proberen te achterhalen, dit zorgt voor economische en psychologische schade. Een groep internetgebruikers waarbij de gevolgen van phishing disproportioneel grote schade kunnen aanrichten zijn de senioren. Dit onderzoek is gedaan bij senioren, gedefinieerd als; mensen van 50 jaar of ouder die lid zijn van een seniorenvereniging. Volgens het Heuristisch-Systematisch Model (HSM) zou een verhoogde mate van systematische verwerking ervoor kunnen zorgen dat de effectiviteit van een phishing bericht wordt verlaagd. De vraagstelling die in dit onderzoek centraal staat is: Wat is de invloed van een toename in de mate van systematische verwerking op phishing aanvallen bij senioren? Om deze vraag te beantwoorden is een animatievideo ontwikkelt en getoond aan inwoners van de regio Limburg-Noord. Dit onderzoek (N = 213) heeft aangetoond dat het bekijken van de ontworpen animatievideo het aantal ingevulde persoonsgegevens verlaagd bij senioren. Omdat dit het eerste onderzoek is, voor zover bij de auteur bekend, dat het gedrag op deze manier meet, draagt dit onderzoek op een wetenschappelijke manier bij aan de literatuur over phishing. Limitaties en suggesties voor vervolgonderzoek worden besproken.


## Introductie

In de laatste jaren is er een toename in het aantal meldingen van een vorm van online criminaliteit genaamd *phishing*, waarbij de wereldwijde, financiële schade aan individuen en bedrijven elk jaar tot enkele miljarden kunnen oplopen (Federal Bureau of Investigation, 2020; Jain & Gupta, 2017). Een definitie van phishing welke geformuleerd is door Zhang en collega's (2012) en welke in dit onderzoek gebruikt zal worden, luidt; "Phishing houdt in dat criminelen door middel van misleiding persoonlijke gegevens proberen te achterhalen. Vaak wordt er gebruikt gemaakt van een legitiem uitziende e-mail of SMS." Naast e-mail of sms (ook wel *smishing* genoemd), rapporteren internet security bedrijven zoals Malwarebytes (2018) en Symantec (2019) dat de aanvallen steeds geavanceerder worden. Zo worden nu ook kanalen als social media gebruikt en wordt er steeds vaker een variant van phishing genaamd *spear phishing* toegepast, waarbij de aanval specifiek gericht is op een individu, een type internetgebruiker of een bepaald bedrijf. Een recent voorbeeld hiervan uit Nederland is dat criminelen de corona crisis misbruiken om in te spelen op de angst van mensen rondom het virus; zo waarschuwden een Brits internet security bedrijf dat er phishing berichten verstuurd werden van zogenaamd het RIVM (zie bijlage 1) met de bedoeling persoonlijke gegevens te

achterhalen (Algemeen Dagblad, 2020). Dit onderzoek richt zich op het voorkomen van phishing aanvallen die specifiek gericht zijn op een type internetgebruiker.

Een groep internetgebruikers waarbij de gevolgen van phishing disproportioneel grote schade kunnen aanrichten zijn de senioren (Gavett et al., 2017). Deze groep krijgt, in vergelijking tot jonge mensen, vaker te maken met socio-psychologische schade na slachtoffer te zijn geweest van internetcriminaliteit (Gustafson, 2020). In een vragenlijst van *The Guardian* (2015) zijn vaak genoemde voorbeelden hiervan sociale exclusie, vaak gedreven door angst of schaamte en lang aanhoudende gevoelens van stress. Dit onderzoek is uitgevoerd bij senioren, gedefinieerd als; mensen van 50 jaar of ouder die lid zijn van een seniorenvereniging.

Hoewel de gevolgen van phishing uitgebreid gerapporteerd en bestudeerd zijn in de bestaande literatuur, blijft onderzoek naar de beslissingen die mensen maken wanneer zij in aanraking komen met phishing onderbelicht. Het onderstaande deel beschrijft de psychologische processen die hieraan ten grondslag liggen**.**

***Theoretische achtergrond***

Internetcriminelen ontwerpen phishing berichten met het doel om menselijke emoties te beïnvloeden (zoals angst of hebzucht) en hiermee de ervaren druk te vergroten, waarbij zij zich vaak richten op specifieke groepen, zoals senioren (Goel, Williams, & Dincelli, 2017). Onderzoek uit de cognitieve neurowetenschap leert ons dat emoties een invloedrijke rol spelen bij het maken van beslissingen (Damasio, 1994). Er zijn meerdere voorbeelden van phishing berichten die inspelen op emoties om de ervaren druk te verhogen. Een van die voorbeelden is angst, wat werkt als een waarschuwingssignaal voor schade wanneer iemand de perceptie heeft dat zijn welzijn bedreigd wordt (Ledoux, 2003). Dit zorgt ervoor dat iemand zo snel mogelijk voorzorgsmaatregelen neemt om zichzelf te beschermen (Leventhal, 1970). Een bekend voorbeeld hiervan is een internetcrimineel die deze angstreactie gebruikt door zich voor te doen als een medewerker van een bank waarin de crimineel aangeeft dat het account van het slachtoffer geblokkeerd wordt tenzij diegene op een weblink klikt en zijn of haar persoonsgegevens invult (waardoor deze in de handen van de crimineel terecht komen). De angst om iets waardevols te verliezen vergroot de kans dat mensen hun persoonsgegevens aan de internetcrimineel overhandigen (Kim & Kim, 2013). Andere voorbeelden van dit soort overtuigingstechnieken om de ervaren druk te vergroten zijn: autoriteit en schaarsheid (Cialdini, 2007). Deze worden regelmatig door internetcriminelen toegepast in phishing aanvallen (Butavicius, Parsons, Pattinson, & McCormac, 2016). Schaarsheid is gebaseerd op het idee dat mensen ergens meer waarde aan hechten wanneer iets weinig of enkel voor een

bepaalde tijd beschikbaar is, zoals een prijs die je kan winnen via een e-mail. Het principe achter autoriteit leent zich aan het feit dat iemand sneller iets zou doen voor een figuur met autoriteit. Door zich voor te doen als de CEO van een bank heeft de crimineel een grotere kans van slagen (Butavicius, et al., 2016). Door de ervaren druk op mogelijke slachtoffers van phishing te vergroten proberen criminelen dus persoonsgegevens te achterhalen.

Internetcriminelen verhogen de ervaren druk door gebruik te maken van overtuigingstechnieken. Deze verhoogde ervaren druk spoort de menselijke gewoonte aan om snel en intuïtief te oordelen wanneer zij voor een beslissing komen te staan, ook al staat er valse informatie in een phishing bericht dat ontdekt kan worden wanneer hier de tijd voor wordt genomen. Slachtoffers worden op deze manier geduwd richting het accepteren van, of het reageren op phishing berichten (Watters, 2009).

De manier waarop de beslissing van mensen rondom phishing berichten mogelijk verklaard kan worden is volgens het informatieverwerking model van Chaiken (1999), genaamd het Heuristisch-Systematisch Model (HSM). HSM stelt dat mensen eerst de validiteit van een bericht evalueren voordat zij een oordeel vellen. Een belangrijk aspect van het HSM is dat mensen gebruik maken van een combinatie van heuristische en systematische processen om de validiteit van een bericht of situatie te beoordelen voordat zij wel of niet worden overtuigd (Luo, Zhang, Burd, & Seazzu, 2013). Een beoordeling die gevormd wordt door heuristische verwerking maakt gebruik van vuistregels en kijkt naar factoren in en rondom de bron zoals het formaat, onderwerp en afzender. Deze vuistregels of “heuristieken” die gebruikt worden kosten doorgaans weinig tijd en dit proces eist daarnaast weinig cognitief vermogen relatief aan een systematische manier van verwerken. Wanneer een oordeel gevormd wordt door een systematische verwerking, wordt de inhoud van de informatie zorgvuldig onderzocht. Hierdoor eist de beoordeling vergeleken met een heuristische verwerking veel cognitief vermogen (Chen, Duckworth, & Chaiken, 1999).

Wanneer mensen gebruik maken van heuristische processen om phishing berichten te verwerken wordt er in mindere mate gelet op signalen die kunnen wijzen op bedrog of misleiding (Luo, et al., 2013). Phishing berichten lokken deze heuristische manier van verwerken uit en onderdrukken de systematische manier van verwerking (Watters, 2009). Hierdoor wordt het cognitieve vermogen wat mensen gebruiken wanneer zij phishing berichten verwerken laag gehouden. In een onderzoek van Vishwanath, Harrison en Ng (2018) werd aangetoond dat mensen die de informatie in phishing e-mails op een systematische manier verwerkte, minder snel phishing e-mails opende en op de link hierin klikte. Een verhoogde mate van systematische verwerking verlaagt de kans dat phishing

aanvallen slagen (Luo, Zhang, Burd, & Seazzu, 2013). Dit onderzoek tracht de mate van systematisch verwerking te vergroten door de onderliggende factoren te beïnvloeden.

Systematische verwerking wordt beïnvloed door twee factoren. Ten eerste speelt het cognitieve vermogen een belangrijke rol (Vishwanath et al., 2011). In de context van dit onderzoek, wordt het cognitieve vermogen gebruikt om het bericht inhoudelijk te analyseren. Hoe hoger de ervaren druk, des te lager het cognitieve vermogen wat beschikbaar wordt gesteld tijdens het maken van een beslissing, wat zorgt voor een lage mate van systematische verwerking (Williams, Hinds, & Joinson, 2018). Ten tweede speelt de cognitieve bekwaamheid een rol. Dit houdt in dat mensen de bedreiging van een phishing bericht kunnen herkennen en weten hoe ze daar mee om moeten gaan. Bekwaamheid wordt in dit stuk beschreven aan de hand van de Protection Motivation Theory (PMT) (Rogers, 1975) dat doorgaans wordt gebruikt bij onderzoek naar online veiligheidsgedrag (bv. Tsai, et al., 2016; Liang, Xue, 2010; Workman, Bommer, Straub, 2008). PMT stelt dat online veiligheidsgedrag, met het doel om jezelf te beschermen, voorspelt wordt door je bekwaamheid om dit gedrag uit te voeren. Deze bekwaamheid wordt opgesplitst in twee factoren: Een combinatie van de threat appraisal en de coping appraisal (Shillair, et al., 2015). Threat appraisal bestaat uit een evaluatie van de bedreiging waarbij de perceptie van de gebruiker, de ernst van de bedreiging en hoe vatbaar diegene denkt te zijn voor de bedreiging, centraal staan (Rohm & Milne, 2004). Daarnaast bestaat de coping appraisal uit een evaluatie van de aanbevolen actie om de bedreiging tegen te gaan en het waargenomen vermogen om deze actie uit te voeren (Floyd et al., 2000). In de context van dit onderzoek wordt dit toegepast op het herkennen van signalen die wijzen op een phishing aanval en het weten hoe je moet reageren op mogelijke phishing aanvallen. Voorbeelden van deze signalen kunnen bestaan uit verdachte spelfouten, hyperlinks of algemene aanheffen boven een bericht. Zo heeft het onderzoek van Dhamija, Tygar en Hearst (2006) aangetoond dat een aanzienlijk deel van de mensen niet op factoren als de adresbalk of HTML van een e-mail letten, terwijl dit van wezenlijk belang kan zijn voor het herkennen van phishing aanvallen. Wanneer mensen berichten kunnen herkennen als phishing (threat appraisal) en weten hoe ze daar mee om moeten gaan (coping appraisal) zorgt dit voor een vermindering van de negatieve gevolgen hiervan (Dhamija, Tygar, Hearst, 2006; Zhang, Luo, Burd, & Seazzu, 2012). Voldoende cognitief vermogen om het bericht te verwerken in combinatie met de cognitieve bekwaamheid zorgen voor een verhoging in de mate van systematisch verwerking.

***Huidig onderzoek***

Voor dit onderzoek is een animatievideo ontwikkelt met het doel de mate van systematische verwerking van een phishing berichten te vergroten om zo de negatieve gevolgen van phishing te voorkomen. In de korte animatievideo van circa twee minuten worden senioren aan de hand van voorbeelden ingelicht waar criminelen op inspelen, de mogelijke gevolgen van phishing en wordt er duidelijk gemaakt hoe de deelnemers met phishing kunnen omgaan. In de methodesectie van dit stuk wordt verder toegelicht waarom hiervoor is gekozen en hoe de animatievideo is ontwikkeld.

Dit onderzoek toetst de invloed van het zien van de Animatievideo op het aantal ingevulde persoonsgegevens (gedragsmaat) en de intentie van een individu om zichzelf te weren tegen phishing. De persoonsgegevens die worden gevraagd aan de participanten zijn voornaam, achternaam, straatnaam, postcode, e-mailadres en telefoonnummer. De gegevens die de participanten invullen worden omwille van de privacy niet opgeslagen maar gecodeerd tot 1 (wel ingevuld) en 0 (niet ingevuld). Voorafgaand aan het onderzoek is stilgestaan bij de ethische verantwoording van de gedragsmaat. De reden dat bijzonder gevoelige persoonsgegevens, zoals wachtwoorden of creditcardgegevens, niet gevraagd zijn is dat dit mogelijk angst of andere negatieve emoties zou kunnen opwekken bij de participanten. Onderzoek naar phishing waarbij levensechte scenario's worden gesimuleerd, zoals in dit onderzoek, kunnen kennis opleveren voor het ontwikkelen van preventieve maatregelen. Om deze reden stellen Resnik en Finn (2018) dat onderzoek naar phishing ethisch verantwoord is wanneer de onderzoeker zich aan een viertal regels houdt, namelijk: De risico's moeten minimaal zijn, de privacy van de participanten moet beschermd worden, de participanten moeten zich op elk moment kunnen terugtrekken en de participanten moeten een debriefing ontvangen over het daadwerkelijke doel van het onderzoek. In dit onderzoek wordt aan deze eisen voldaan.

De persoonsgegevens die gevraagd worden in dit onderzoek komen overeen met de persoonsgegevens die door internetcriminelen worden gezocht om te gebruiken voor bijvoorbeeld spear phishing (Parmar, 2012). Recente voorbeelden van phishing gericht op een individu zijn "uw bankrekening staat in quarantaine, log hier in om deze eruit te halen" of "Belangrijk: de laatste update over het nieuwe covid-19 virus. Klik snel! Dit kunt u niet missen!" die verstuurd worden via whatsapp, SMS of e-mail (NU.nl, 2020). De voor- en achternaam in combinatie met thuisadres en postcode worden toegevoegd aan het bericht om zo een gevoel van echtheid te creëren waardoor het mogelijke slachtoffer sneller zijn of haar persoonsgegevens invult.

Naast persoonsgegevens wordt ook de intentie van de participanten om zichzelf tegen phishing te weren gemeten. Voorgaand onderzoek naar phishing is het oneens of de intentie om online veiligheidsgedrag uit te voeren wel een goede voorspeller is van het daadwerkelijke gedrag (yang, Xiong, Chen, Proctor, 2017; Egelman, Cranor, & Hong, 2008) of juist niet (Spiekerman; Grossklags, & Berendt, 2001; Boss, Galleta, Lowry, Moody, & Polak, 2015). Deze mogelijke discrepantie tussen intentie en gedrag is een bekend fenomeen binnen de sociaal psychologische literatuur, namelijk de *intention-behaviour gap* (Sheeran, & Webb, 2016). Het merendeel van de onderzoeken naar phishing meet de intentie in plaats van daadwerkelijk gedrag. Dit onderzoek meet, voor zover bekend bij de auteur, als eerste het gedrag rondom phishing op deze manier. Door zowel het gedrag als de intentie om dit gedrag uit te voeren te meten, kan dit onderzoek bijdragen aan een verklaring voor deze discrepantie op het gebied van onderzoek naar phishing

In dit onderzoek wordt de vraag gesteld: Wat is de invloed van een toename in de mate van systematische verwerking op phishing aanvallen bij senioren? Op basis van de bovenstaande literatuur wordt verwacht dat het zien van de animatievideo het aantal ingevulde persoonsgegevens verlaagt. De hypothesen die hieruit volgen zijn, 1a: het zien van de animatievideo verlaagt het aantal ingevulde persoonsgegevens, 1b: de leeftijd van de deelnemers heeft invloed op het aantal ingevulde persoonsgegevens. Hiernaast wordt verwacht dat het zien van de animatievideo de intentie om jezelf te beschermen tegen phishing wordt verhoogd. De hypothesen die hieruit volgen zijn, 2a: Het zien van de animatievideo verhoogt de score op de intentie vragenlijst, 2b: de leeftijd van de deelnemers heeft invloed op de score van intentie op de vragenlijst. Om dit te onderzoeken is een quasi-experiment uitgevoerd in de regio Noord-Limburg waarbij een groep senioren is verdeeld over twee groepen waarbij de helft de animatievideo te zien kreeg en de andere helft niet. Hierna werden zij gevraagd bepaalde persoonsgegevens in te vullen gevolgd door een vragenlijst.

## Methode

### *Deelnemers*

Er zijn naar schatting 1750 mogelijke deelnemers uit de regio Limburg-Noord benaderd via e-mail. Hiervan hebben 338 mensen de link in de e-mail geopend en zijn er 238 akkoord gegaan met de voorwaarden van het onderzoek. Hiervan zijn 213 meegenomen in de Data-Analyse. Senioren worden in dit stuk gedefinieerd als 50-plussers die lid zijn van een seniorenvereniging. De reden voor het verwijderen van deze 25 participanten was het niet, of

niet volledig, bekijken van de animatievideo of het niet, of niet volledig, invullen van de vragenlijsten. De uiteindelijke participanten bestonden uit 133 mannen en 80 vrouwen tussen de 57 en 88 jaar ($M$ = 74.66, $SD$ = 5.80).

***Procedure***

De deelnemers voor dit onderzoek zijn actief benaderd met behulp van de Katholieke Bond voor Ouderen (KBO), dit is een seniorenorganisatie in o.a. Noord-Limburg. De KBO heeft meerdere afdelingen van verschillende grootten. In overleg met de consulent van de KBO is besloten welke afdelingen benaderd werden. Hier werd onder andere gekeken naar het aantal leden van de afdelingen om te zorgen voor een gelijke verdeling van het aantal participanten over de twee groepen. De demografisch vergelijkbare afdelingen zijn willekeurig verdeeld over de twee condities (wel animatievideo/ geen animatievideo). Hierna is een e-mail verstuurd met daarin een weblink (bijlage 2). De e-mails zijn via de secretaris van de desbetreffende afdeling verstuurd naar haar leden om de privacy van de leden te waarborgen. De onderzoeker heeft nooit persoonsgegevens van de participanten kunnen inzien. De vragenlijst is met Qualtrics ontwikkelt en begon met het vragen of de participant akkoord gaat met de voorwaarden van het onderzoek. Hierna volgde, voor de experimentele groep, de animatievideo die via Youtube in de vragenlijst was opgenomen. De participanten werden gevraagd om de gehele animatie video af te kijken. Dit is echter niet altijd gebeurd waardoor meerdere participanten niet konden worden meegenomen in dit onderzoek. Hierna werden de participanten gevraagd hun voornaam, achternaam, straatnaam, postcode, e-mailadres en telefoonnummer in te vullen. Dit is uiteindelijk bij elkaar opgeteld om zo een score voor de gedragsmaat te berekenen waarbij nul het minimale aantal persoonsgegevens is en 6 het maximale aantal persoonsgegevens. Ook leeftijd en geslacht werden gevraagd, deze worden niet gezien persoonsgegevens en dus ook niet meegenomen in de berekening van de gedragsmaat (zie bijlage 3 voor een overzicht hiervan). Hierop volgde een vragenlijst voor intentie en werden de deelnemers in de experimentele groep gevraagd naar hun mening over de animatievideo. Hierna kregen de deelnemers de ruimte om opmerkingen te plaatsen en volgde een korte debriefing.

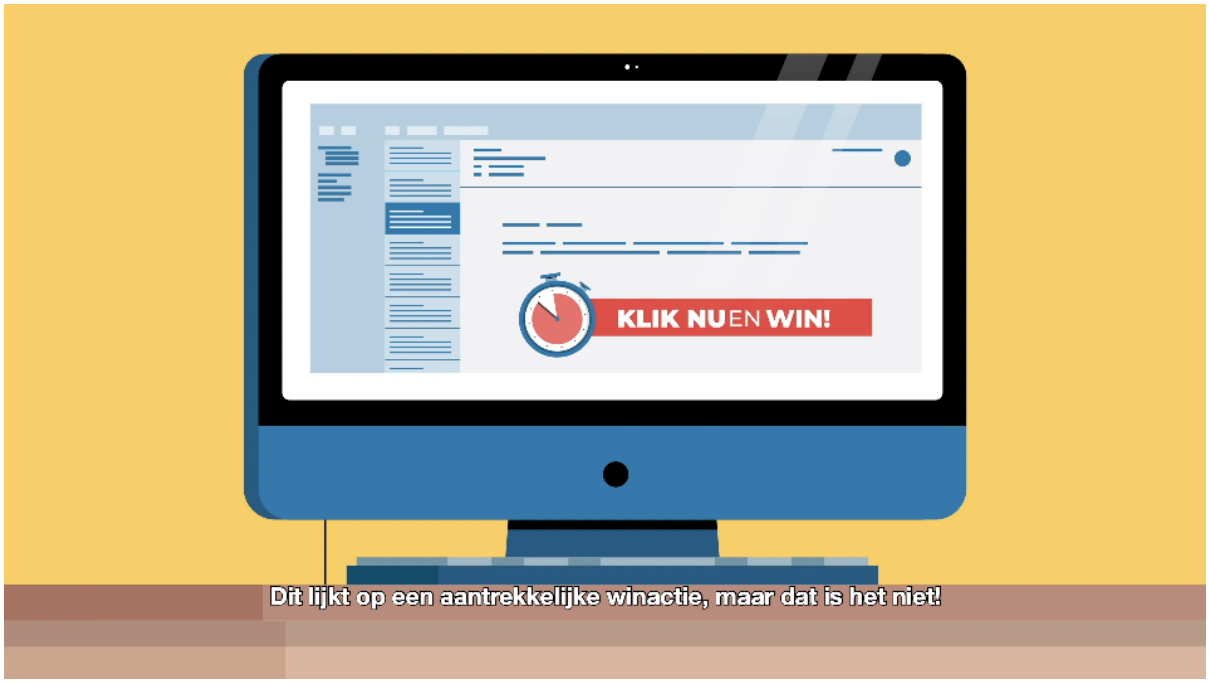
## Materialen

***Animatievideo***

Uit voorgaand onderzoek blijkt dat video's gebaseerd op een *dual process theory*, zoals het HSM (Chaiken & Trope, 1999), eerder effectief zijn geweest als interventie bij onderzoek gericht op het bevorderen van veiligheidsgedrag (Brown, et al., 1997; Roberto, Meyer, Johnson, & Atkin, 2000) en online veiligheidsgedrag (Turel, Mouttapa, & Donato, 2015).

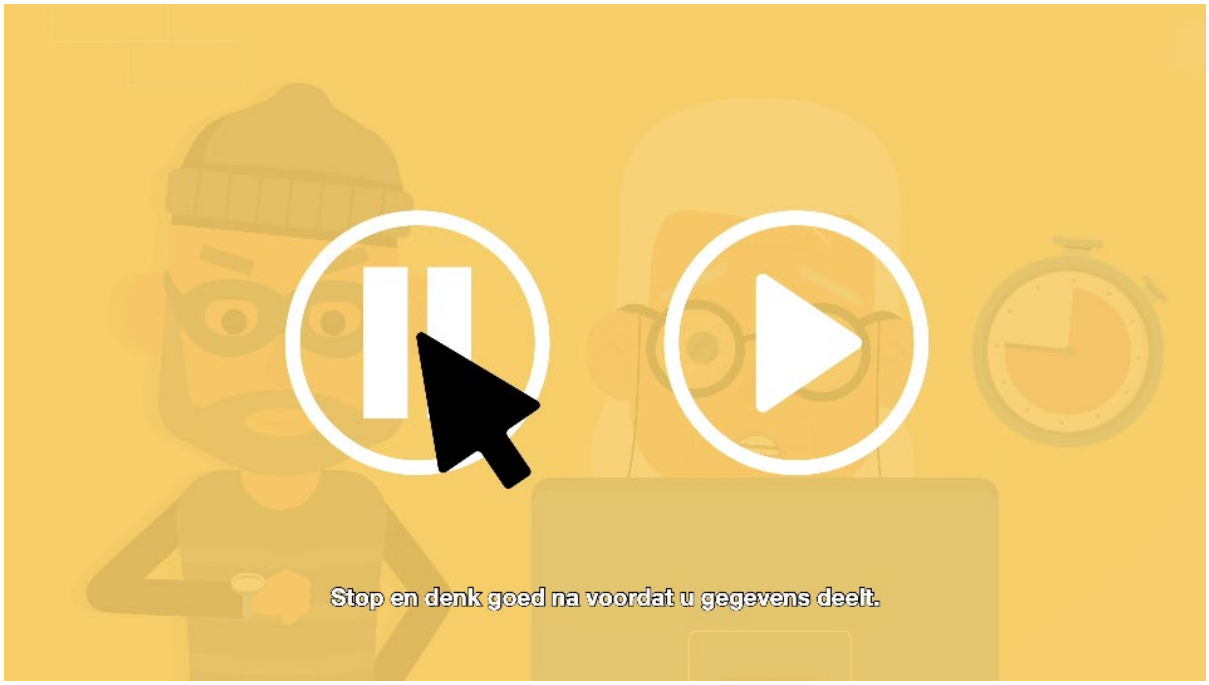
Voortbordurend op deze studies heeft dit onderzoek een animatievideo ontwikkelt met het doel de mate van systematische manier van verwerking van een phishing bericht te vergroten. Mocht de video hierin slagen, dan vertaalt zich dit in een lager aantal ingevulde persoonsgegevens bij senioren. Bij de animatievideo staan twee doelen centraal.

Ten eerste tracht de animatievideo het cognitieve vermogen te bevorderen door de ervaren druk van een phishing bericht te verlagen. De video gebruikt recente en veelgebruikte voorbeelden om uit te leggen hoe criminelen dit doen, zoals hieronder in figuur 1.




*Figuur 1: Poging van een crimineel om de ervaren druk te vergroten.*

De animatievideo laat zien hoe criminelen te werk gaan en geeft aan dat mensen nooit direct op een verzoek dat om gegevens vraagt hoeven te reageren en altijd kunnen stoppen om na te denken voordat ze gegevens delen, ook al wordt dit gevoel sterk opgewekt, ze kunnen altijd op “pauze” drukken (figuur 2). Vervolgens sluit de video af met de boodschap “Haastige spoed is zelden goed. Ook online” om af te sluiten met de boodschap dat je nooit meteen hoeft te reageren. Op deze manieren probeert de video de druk die een phishing bericht oproept te voorkomen. Door deze ervaren druk te verlagen wordt de mate van systematische verwerking verhoogt (Williams, Hinds, & Joinson, 2018).




*Figuur 2: Je kan altijd op "pauze" drukken voordat je gegevens deelt.*

Ten tweede tracht de animatievideo de cognitieve bekwaamheid te bevorderen. Zo zorgt onder andere het voorbeeld in *figuur 1* ervoor dat mensen phishing berichten beter kunnen herkennen. Belangrijk hierbij is dat het herkennen van de phishing bericht (threat appraisal) gekoppeld gaat met weten hoe je me phishing berichten om moet gaan (coping appraisal) (Maddux, & Rogers, 1983). Onderzoek leert ons namelijk dat wanneer de threat appraisal dusdanig benadrukt wordt dit averechtse effecten kan hebben (Wang & Rao, 2017). Een verhoging in de threat appraisal kan een hoge angstreactie veroorzaken op alle binnenkomende berichten, waardoor mensen ook normale berichten als phishing kunnen gaan zien (Liang, & Xue, 2009). Om deze reden bevat de intro van de animatievideo onder andere de boodschap: "*Online diensten zijn handig en zorgen voor vermaak"* en ligt de focus niet op de negatieve gevolgen van phishing maar de manier waarop deze gevolgen voorkomen kunnen worden.

Hiernaast is bij de vormgeving van de animatievideo *narrative persuasion* toegepast door de hoofdpersoon en de crimineel steeds terug te laten komen in een doorlopend verhaal. Het gebruiken van een verhaal kan een boodschap meer kracht geven wanneer het mensen probeert te overtuigen (Bilandzic & Busselle, 2013). Dit wordt gedaan om de aandacht van de kijker bij de animatievideo te houden en de boodschap te versterken.

De animatievideo moet ervoor zorgen dat mensen de manier waarop internetcriminelen te werk gaan leren herkennen en begrijpen waardoor de ervaren druk

hiervan vermindert, dit moet op zijn beurt zorgen voor een verhoging in de mate van systematische verwerking. Voor een link naar de complete animatievideo zie bijlage 4.

De vragenlijst voor intentie bestond uit drie vragen is vertaald en aangepast uit Anderson en Agarwal (2010) met als voorbeeld de vraag: "In de toekomst ga ik mijzelf weren tegen phishing", voor de vragenlijst is een betrouwbare cronbachs alpha gevonden ($\alpha$ = .718). De vragen zijn gemeten op een likert schaal van één (zeer mee oneens) tot vijf (zeer mee eens). De score op de drie vragen werd bij elkaar opgeteld waardoor er een minimale score van nul en een maximale score van vijftien bestond. Hiernaast zijn er voor de experimentele groep twee vragen toegevoegd over wat ze van de animatievideo vonden, namelijk: "ik vond de animatievideo leerzaam" en "ik vond de animatie leuk". Ook deze vragen werden op likert schaal van één (zeer mee oneens) tot vijf (zeer mee eens) gemeten.

***Data-Analyse***

Indien aan de assumpties voldaan werd, zouden de hypotheses getoetst worden met een variantieanalyse corrigerend voor eventuele covariantie (ANCOVA). De onafhankelijke variabele is de groep van de participant (Groep 1 = Animatievideo, Groep 2 = controle). De afhankelijke variabelen zijn: het aantal ingevulde persoonsgegevens (kwantitatief) en de score op de vragenlijst met betrekking tot de intentie om zichzelf te weren tegen phishing (kwantitatief).

## Resultaten

***Beschrijvende statistieken***

Aan de hand van de afhankelijke variabele *groep* zijn de deelnemers ($N$ = 213) verdeeld over het wel zien van de animatievideo (experimentele groep, $N$ = 79) en het niet zien van de animatievideo (controlegroep, $N$ = 134). Het gemiddelde aantal ingevulde persoonsgegevens (afhankelijke variabele) voor de experimentele groep is 3.39 ($SD$ = 2.70), voor de controlegroep is het gemiddelde aantal ingevulde persoonsgegevens 5.04 ($SD$ = 2.03). Hiernaast is de gemiddelde score op de intentie vragenlijst (afhankelijke variabele) voor de experimentele groep 13.31 ($SD$ = 1.68), voor de controlegroep is gemiddelde score op de intentie vragenlijst 12.61 ($SD$ = 2.07). Hiernaast antwoorde de deelnemers op de vraag in hoeverre ze de animatievideo leerzaam vonden overwegend positief, slechts drie participanten reageerden negatief op deze vraag. De vraag in hoeverre deelnemers de animatievideo leuk vonden leverde slechts één iemand negatief antwoord op.

***Analyses***

Ten eerste is er gekeken naar de invloed van de onafhankelijke variabele *groep* (experimentele groep/ controlegroep) op de afhankelijke variabele *aantal persoonsgegevens* (minimaal = 0, maximaal = 6) met als covariaat *leeftijd* (*M* = 74.66, *SD* = 5.80). Om de assumpties voor een ANCOVA te toetsen wordt er gekeken naar de gelijke scores van de covariaat op de groep en de homogeniteit van de regressiehellingen (Field, 2013). Voor de onafhankelijkheid van de covariaat op de groep is een t-test gedaan die laat zien dat de experimentele groep (*M* = 74.76, *SD* = 5.28) niet significant verschilt van de controlegroep (*M* = 74.60, *SD* = 6.09) op leeftijd, *t*(211) = .195, *p* = .845, dit betekent dat deze assumptie niet geschonden is. Hierna is de homogeniteit van de regressiehellingen getoetst en die blijkt niet significant (*p* = .157) te zijn, dit beteken dat deze assumptie niet geschonden is.
Uit de ANCOVA bleek dat de experimentele groep (*M* = 3.39, *SD* = 2.70) significant minder persoonsgegevens invulde dan de controlegroep (*M* = 5.04, *SD* = 2.03) wanneer er gecorrigeerd werd voor leeftijd, *F*(1,210) = 26.26, *p* < .001, *eta2* = .111. Dit betekent dat de groep die de animatievideo te zien kregen minder persoonsgegevens invulde. Hiernaast bleek dat de leeftijd significant het aantal ingevulde persoonsgegevens voorspelt, *F*(1,210), *p* = .018, *eta2* = .026. Leeftijd heeft dus invloed op het aantal ingevulde persoonsgegevens.

Om de invloed van leeftijd bij beide groepen verder te onderzoeken werd een exploratieve analyse gedaan waarbij leeftijd werd opgesplitst, hierbij werden de participanten verdeeld over een groep tot en met 74 jaar (*N* = 108) en een groep van 75 jaar of ouder (*N* =115). Uit de variantieanalyse bleek dat, in de experimentele groep, deelnemers tot en met 74 jaar (*M* = 2.77, *SD* = 2.70) in vergelijking met deelnemers van 75 jaar of ouder (*M* = 4.14, *SD* = 2.55) significant minder persoonsgegevens invulde, *F*(1,77) = 5.32, *p* = .024, *eta2* = .065. Dit betekent dat mensen tot en met 74 jaar minder persoonsgegevens invulden in de experimentele groep. In de controlegroep werd geen significant verschil gevonden op het aantal ingevulde persoonsgegevens tussen deelnemers tot en met 74 jaar en deelnemers van 75 jaar of ouder, *F*(1, 132) = 1.52, *p* = .220, *eta2* = .011. Dit betekent dat het verschil tussen de twee leeftijdscategorieën enkel in de experimentele groep gevonden is.

Ten tweede is er gekeken naar de invloed van de onafhankelijke variabele *groep* op de *intentie* (score op de intentie vragenlijst, minimaal = 0, maximaal = 15) met als covariaat *leeftijd* (*M* = 74.66, *SD* = 5.80). De homogeniteit van de regressiehellingen werd getoetst en die blijkt niet significant (*p* = .593) te zijn, dit beteken dat deze assumptie niet geschonden is. Uit de ANCOVA bleek dat de experimentele groep (*M* = 13.31, *SD* = 1.68) significant hoger scoorden op de intentie vragenlijst dan de controlegroep (*M* = 12.62, *SD* = 2.07) wanneer er gecorrigeerd werd voor leeftijd, *F*(1,210) = 23.16, *p* = .014, *eta2* = .031. Dit betekent dat de

groep die de animatievideo te zien kregen hoger scoren op de intentie om zichzelf te weren tegen phishing. Hiernaast bleek dat leeftijd geen significante invloed heeft op intentie $F(1,210) = 6.21$, $p = .162$, $eta2 = .010$. Leeftijd heeft geen invloed op de score van de intentie vragenlijst.

## Conclusie

De vraagstelling die in dit onderzoek centraal staat is: Wat is de invloed van een toename in de mate van systematische verwerking op phishing aanvallen bij senioren? Om deze vraag te beantwoorden is een animatievideo ontwikkeld en getoond aan inwoners van de regio Limburg-Noord. Hierop volgend is het aantal ingevulde persoonsgegevens gemeten. De deelnemers aan dit onderzoek zijn over twee groepen verdeeld. De experimentele groep die de animatievideo te zien kregen en de controlegroep die deze niet te zien kregen.

De eerste hypothese van dit onderzoek stelt dat de experimentele groep minder persoonsgegevens in zouden vullen dan de controlegroep terwijl er voor leeftijd werd gecorrigeerd. De resultaten lieten zien dat de mensen die de animatievideo te zien kregen significant minder persoonsgegevens invullen in dan de controlegroep terwijl er voor leeftijd gecorrigeerd is. Deze hypothese kan dus worden bevestigd. Dit suggereert dat het zien van de animatievideo de mate van systematische verwerking van een phishing bericht verhoogt, hetgeen in lijn is met voorgaand onderzoek (Luo et al., 2013; Vishwanath et al., 2018). Verder is gevonden dat, in de experimentele groep, leeftijd een significante invloed heeft op het aantal ingevulde persoonsgegevens. In de experimentele groep vulde deelnemers onder de 75 jaar significant minder persoonsgegevens in dan mensen 75 jaar of ouder. In de controlegroep is er geen significant verschil gevonden tussen de twee leeftijdscategorieën.

De tweede hypothese van dit onderzoek stelt dat de groep die de animatievideo te zien kregen hoger zouden scoren op de vragenlijst voor intentie. De resultaten lieten zien dat de mensen die de animatievideo te zien kregen significant hoger scoorden op de vragenlijst voor intentie dan de mensen in de controlegroep terwijl er voor leeftijd gecorrigeerd is. Deze hypothese wordt dus ook bevestigd. Dit suggereert dat de intentie van een individu om zichzelf te weren tegen phishing het daadwerkelijke gedrag, het wel of niet invullen van persoonsgegevens, voorspelt, dit is in lijn met voorgaand onderzoek (Yang et al., 2017; Egelman et al., 2008). Verder is gevonden dat leeftijd geen significante invloed heeft op de score van de intentie vragenlijst.

## Discussie

Dit onderzoek laat gedragsverandering zien aan de hand van een significante vermindering op het aantal ingevulde persoonsgegevens door de participanten. Dit resultaat is gekoppeld aan een sterke geobserveerde power. De gevonden power suggereert dat de kans op een type twee fout, het vinden van een onterecht significant resultaat, erg klein is. Vervolgens laten de resultaten van dit onderzoek zien dat mensen in de controlegroep onder de 75 niet verschillen in het aantal ingevulde persoonsgegevens ten opzichte van mensen van 75 jaar of ouder, dit is in lijn met voorgaand onderzoek dat stelt dat leeftijdscategorieën niet verschillen op de mate van vatbaarheid voor phishing berichten (Sarno, et al., 2020; Bullee et al., 2017). Hier tegenover vullen mensen in de experimentele groep onder de 75 jaar significant minder persoonsgegevens in vergelijking met mensen 75 jaar of ouder. Dit suggereert dat de interventie een groter effect heeft op mensen onder de 75 jaar.

Ook al zijn de resultaten veelbelovend zijn er enkele limitaties aan dit onderzoek waarbij stilgestaan moet worden ten behoeve van de generaliseerbaarheid. Ten eerste moesten deelnemers aan dit onderzoek een e-mail openen en vervolgens op een weblink klikken om aan het onderzoek te beginnen. Voorgaand onderzoek laat zien dat mensen die sneller geneigd zijn een weblink te openen, ook sneller slachtoffer worden van phishing (Downs, Holbrook, & Cranor, 2007; Caputo et al., 2013). Het zou kunnen dat de mensen die mee hebben gedaan met dit onderzoek sneller persoonsgegevens in zouden vullen in vergelijking met mensen die niet mee hebben gedaan, aangezien de participanten zelf op de link in de e-mail hebben geklikt. Hierdoor bestaat de mogelijkheid dat de participanten in dit onderzoek niet representatief zijn voor de algemene populatie. Ten tweede zijn omwille van de privacy van de participanten geen daadwerkelijke persoonsgegevens opgeslagen, maar is slechts geregistreerd of participanten *wel* of *niet* iets hebben ingevuld. Zou iemand bijvoorbeeld een niet bestaand e-mailadres of telefoonnummer hebben ingevuld dan werd dit gezien als *wel* ingevuld. Het is naast privacyoverwegingen ook praktisch niet haalbaar om betrouwbaar te controleren of ingevulde persoonsgegevens daadwerkelijk correcte gegevens zijn. Om deze reden zou het kunnen dat het daadwerkelijke aantal *correct* ingevulde persoonsgegevens lager ligt dan het aantal ingevulde persoonsgegevens gemeten in dit onderzoek.

Naar aanleiding van de behaalde resultaten is er geconcludeerd dat het zien van de animatievideo ervoor kan zorgen dat senioren minder persoonsgegevens invullen. Hierdoor worden mogelijk minder mensen het slachtoffer van phishing wat de eerdergenoemde negatieve gevolgen beperkt. Dit biedt interessante aanknopingspunten voor overheidsinstanties over de manier waarop informatie rondom phishing gecommuniceerd kan

worden. Dit onderzoek maakt gebruik van recente voorbeelden van phishing om de systematische manier van verwerking bij het maken van een beslissing te verhogen, wat eerder een positieve invloed had bij onderzoek naar online veiligheidsgedrag (Turel, Mouttapa, & Donato, 2015). Beleidsmakers zouden kunnen overwegen om soortgelijke initiatieven op te zetten, aangezien de kosten relatief laag zijn in vergelijking met de mogelijke schade die phishing aan kan richten.

Hiernaast is de informatie in de animatievideo relevant voor een brede doelgroep en is deze relatief goedkoop en makkelijk te verspreiden. Zo kan de animatievideo voor een breder publiek worden ingezet. De meest voor de hand liggende doelgroep zijn de rest van de afdelingen van de KBO, waaronder de afdelingen die de animatievideo niet te zien kregen in dit onderzoek. Hiernaast zijn niet enkel senioren vatbaar voor phishing en zijn campagnes omtrent bewustwording van dit fenomeen voor alle demografische groepen van belang (Norris, Brooks, & Dowell, 2019). Het implementeren van de animatievideo biedt kansen om de negatieve gevolgen van phishing om grotere schaal te verminderen.

Dit onderzoek draagt bij aan de bestaande literatuur. Ten eerste draagt het bij aan het inzetten van het HSM bij het ontwikkelen van een interventie, dit model is breed inzetbaar (Chaiken & Trope, 1999), en dit onderzoek heeft laten zien dat het gebruikt kan worden om de gevolgen van phishing te voorkomen bij senioren. Ten tweede draagt het bij aan de literatuur rondom de *intention-behaviour gap*, het lijkt erop dat de intentie om zichzelf te weren tegen phishing op zijn minst het gedrag zoals gemeten in dit onderzoek kan voorspellen.

Deze resultaten dragen bij aan het voorkomen van phishing, ook heeft het nieuwe inzichten geleverd voor vervolgonderzoek. Waar het huidige onderzoek het gedrag rondom phishing aan de hand van het aantal ingevulde persoonsgegevens meet, zou vervolgonderzoek dit kunnen complimenteren door naar andere typen gegevens te vragen, zoals bankgegevens of wachtwoorden. Wanneer er minder te verliezen valt, bijvoorbeeld wanneer de crimineel vraagt om een e-mailadres, wordt minder snel de mate van systematische verwerking verhoogd dan wanneer de mate van risico hoog is, bijvoorbeeld wanneer de crimineel vraagt om bankgegevens (Luo et al., 2012). Voorgaand onderzoek laat zien dat de mate van waargenomen risico een voorspeller is van online veiligheidsgedrag (Dinev, & Hart, 2006). Dit wil zeggen dat wanneer mensen een hoge mate van risico waarnemen, zij persoonlijke informatie eerder zouden bewaken (Malhotra et al., 2004). Hier tegenover staat dat wanneer mensen het idee hebben dat er weinig te verliezen valt, zij sneller persoonlijke informatie zouden verstrekken (li et al., 2011). Ervanuit gaande dat de gedragsmaat in dit onderzoek een

lage risico perceptie op bij mensen opwekt, zou het dus kunnen dat het effect van de animatievideo verschilt wanneer gevraagd wordt naar gegevens die een hoge mate van risico perceptie opwekken. Vervolgonderzoek zou de invloed van de interventie op verschillende gedragsmaten kunnen toetsen en daarbij de ervaren mate van risico te meten om hiervoor te controleren. Hiernaast zou vervolgonderzoek kunnen kijken naar de duurzaamheid van de gemeten gedragsverandering. Een follow-up meting kan uitwijzen of mensen het gewenste gedrag blijven tonen.

Dit onderzoek heeft aangetoond dat het bekijken van een ontworpen animatievideo het aantal ingevulde persoonsgegevens verlaagd bij senioren. Omdat dit het eerste onderzoek is, voor zover bij de auteur bekend, dat het gedrag op deze manier meet, draagt dit onderzoek op een wetenschappelijke manier bij aan de literatuur over phishing. Ook is er met dit onderzoek bijgedragen aan het gebruik van het HSM (Chaiken, 1999) in de context van het onderzoek naar phishing. Ten slotte draagt dit onderzoek bij om de grote maatschappelijke, economische en psychologische gevolgen van phishing te verminderen. Zo zouden beleidsmedewerkers de ontworpen animatievideo in kunnen zetten of de gehanteerde methode kunnen gebruiken voor het ontwikkelen van vergelijkbare campagnes.

**Referenties**


Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS quarterly*, *34*(3), 613-643. doi: 10.2307/25750694

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly (MISQ)*, *39*(4), 837-864. doi: 10.25300/misq/2015/39.4.5

Bilandzic, H., & Busselle, R. (2013). Narrative persuasion. *The Sage handbook of persuasion: Developments in theory and practice*, *2*, 200-219. doi: 10.4135/9781452218410.n10

Brinton Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems*, *25*(4), 364-390. doi: 10.1057/ejis.2015.21

Brown, S. J., D. A. Lieberman, B. A. Gemeny, Y. C. Fan, D.M. Wilson, and D.J Pasta, (1997). "Educational Video Game for Juvenile Diabetes: Results of a Controlled Trial." *Medical Informatics 22*(1), 77–89. doi: 10.3109/14639239709089835

Bullee, J. W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information & Computer Security*. doi: 10.1108/ics-03-2017-0009

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *Paper presented at; the 26th Australasian Conference of Information Systems (ACIS), Adelaide (2015).* doi: 10.1002/9780470086100.ch6

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, *12*(1), 28-38. doi: 10.1109/msp.2013.106

Cialdini, R. B., (2007). *Influence: The psychology of persuasion* (Vol. 55, p. 339). New York: Collins. doi: 10.1038/scientificamerican0201-76

Chaiken, S. (1999). The heuristic-systematic. *Dual-process theories in social psychology*, *73*. doi: 10.4135/9781446249215.n13

Chaiken, S., & Trope, Y. (Eds.). (1999). *Dual-process theories in social psychology*. Guilford Press. doi: 10.4135/9781412956253.n164

Chen, S., Duckworth, K., & Chaiken, S. (1999). Motivated heuristic and systematic processing. *Psychological Inquiry*, *10*(1), 44-49. doi: 10.1207/s15327965pli1001_6

Damasio, A. R. (1994). Descartes' error: Emotion, rationality and the human brain.

Dhamija, R., & Tygar, J. D. (2005, July). The battle against phishing: Dynamic security skins. In *Proceedings of the 2005 symposium on Usable privacy and security* (pp. 77-88). doi: 10.1145/1073001.1073009

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). doi: 10.1145/1124772.1124861

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80. doi: 10.1287/isre.1060.0080

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007, October). Behavioral response to phishing risk. In Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit (pp. 37-44). doi: 10.1145/1299015.1299019

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). doi: 10.1145/1357054.1357219

Federal Bureau of Investigation. (2020). *2019 Internet Crime Report.*

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. sage. doi: 10.1024/1012-5302/a000397

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *Plos one*, *12*(2). doi: 10.1371/journal.pone.0171620

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1), 2. doi: 10.17705/1jais.00447

Gustafsson, H. (2020). Fraud targeting the elderly-A prize of our open society?

Het Algemeen Dagblad. (2020, 12 maart). *Let op: nepmails van het RIVM in omloop om persoonlijke gegevens te ontfutselen.* Geraadpleegd op: https://www.ad.nl/tech/let-op-nepmails-van-het-rivm-in-omloop-om-persoonlijke-gegevens-te-ontfutselen

Jain, A. K., & Gupta, B. B. (2017). Phishing detection: Analysis of visual similarity based approaches. *Security and Communication Networks*, *2017*. doi: 10.1155/2017/5421046

Kim, D., & Kim, J. H. (2013). Understanding persuasive elements in phishing e-mails: A categorical content and semantic network analysis. *Online Information Review, 37*(6), 835-850. doi: 10.1108/oir-03-2012-0037

LeDoux, J. (2003). The emotional brain, fear, and the amygdala. *Cellular and Molecular Neurobiology, 23*(4- 5), 727-738. doi: 10.1023/A:1025048802629

Leventhal, H. (1970). Findings and theory in the study of fear communications. In *Advances in experimental social psychology* (vol. 5, pp. 119-187). New York: Academic Press. doi: 10.1016/s0065-2601(08)60091-x

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434-445. doi: 10.1016/j.dss.2011.01.017

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, 71-90. doi: 10.2307/20650279

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, *11*(7), 1. doi: 10.17705/1jais.00232

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28-38. doi: 10.1016/j.cose.2012.12.003

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology, 19*(5), 469-479. doi: 10.1016/0022-1031(83)90023-9

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355. doi: 10.1287/isre.1040.0032

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*(3), 231-245. doi: 10.1007/s11896-019-09334-5

NU.nl (10 Juni, 2020). *Ouderen vaker online tijdens coronacrisis, makkelijke prooi voor oplichters.* Geraadpleegd op https://www.nu.nl/tech/6056997/ouderen-vaker-online-tijdens-coronacrisis-makkelijke-prooi-voor-oplichters.html

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*, *2012*(1), 8-11. doi: 10.1016/s1361-3723(12)70007-6

Qualtrics, I. (2013). Qualtrics. *Provo, UT, USA*.

Resnik, D. B., & Finn, P. R. (2018). Ethics and phishing experiments. *Science and engineering ethics*, *24*(4), 1241-1252. doi: 10.1007/s11948-017-9952-9

Roberto, A. J., Meyer, G., Johnson, A. J., & Atkin, C. K. (2000). Using the parallel process model to prevent firearm injury and death: Field experiment results of a video-based intervention. *Journal of Communication*, *50*(4), 157-175. doi: 10.1111/j.1460-2466.2000.tb02867.x

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The journal of psychology*, *91*(1), 93-114. doi: 10.1016/0022-1031(83)90023-9

Sarno, D. M., Lewis, J. E., Bohil, C. J., & Neider, M. B. (2020). Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. *Human factors*, *62*(5), 704-717. doi: 10.1177/0018720819855570

Sheeran, P. (2002). Intention—behavior relations: a conceptual and empirical review. *European review of social psychology*, *12*(1), 1-36. doi: 10.1002/0470013478.ch1

Sheeran, P., & Webb, T. L. (2016). The intention–behavior gap. *Social and personality psychology compass*, *10*(9), 503-518. doi: 10.1111/spc3.12265

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199-207. doi: 10.1016/j.chb.2015.01.046

Spiekermann, S., Grossklags, J., & Berendt, B. (2001, October). E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce* (pp. 38-47). doi: 10.1145/501158.501163

Sniehotta, F. F., Scholz, U., & Schwarzer, R. (2005). Bridging the intention–behaviour gap: Planning, self-efficacy, and action control in the adoption and maintenance of physical exercise. *Psychology & health*, *20*(2), 143-160. doi: 10.1080/08870440512331317670

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information systems research*, *6*(2), 144-176. doi: 10.1287/isre.6.2.144

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. doi: 10.1016/j.cose.2016.02.009

Turel, O., Mouttapa, M., & Donato, E. (2015). Preventing problematic Internet use through video-based interventions: A theoretical model and empirical test. *Behaviour & Information Technology*, *34*(4), 349-362. doi: 10.1080/0144929x.2014.936041

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *45*(8), 1146-1166. doi: 10.1177/0093650215627483

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576-586. doi: 10.1016/j.dss.2011.03.002

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: an investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378-396. doi: 10.1287/isre.2016.0680

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1-13. doi: 10.1016/j.ijhcs.2018.06.004

Watters, P. A. (2009). Why do users trust the wrong messages? A behavioural model of phishing. In *2009 eCrime Researchers Summit* (pp. 1-7). IEEE. doi: 10.1109/ecrime.2009.5342611

Wirth, W., Böcking, T., Karnowski, V., & Von Pape, T. (2007). Heuristic and systematic use of search engines. *Journal of Computer-Mediated Communication*, *12*(3), 778-800. doi: 10.1111/j.1083-6101.2007.00350.x

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior*, *24*(6), 2799-2816. doi: 10.1016/j.chb.2008.04.005

Yang, W., Xiong, A., Chen, J., Proctor, R. W., & Li, N. (2017, April). Use of phishing training to improve security warning compliance: evidence from a field experiment. In *Proceedings of the hot topics in science of security: symposium and bootcamp* (pp. 52-61). doi: 10.1145/3055305.3055310

Zhang, W., Luo, X., Burd, S. D., & Seazzu, A. F. (2012, January). How could I fall for that? Exploring phishing victimization with the heuristic-systematic model. In *2012 45th Hawaii International Conference on System Sciences* (pp. 2374-2380). IEEE. doi: 10.1109/hicss.2012.302

Bijlage 1: Sms-bericht waarbij de internetcrimineel zich voordoet als het RIVM

Bijlage 2: e-mail verstuurd richting de participanten.

Beste KBOer,

In samenwerking met de Radboud Universiteit Nijmegen doen wij onderzoek naar het gedrag rondom internetveiligheid. Om dit gedrag beter in beeld te brengen vragen wij of u aan dit onderzoek wilt meewerken door een korte vragenlijst in te vullen. Het duurt ongeveer 5 minuten!

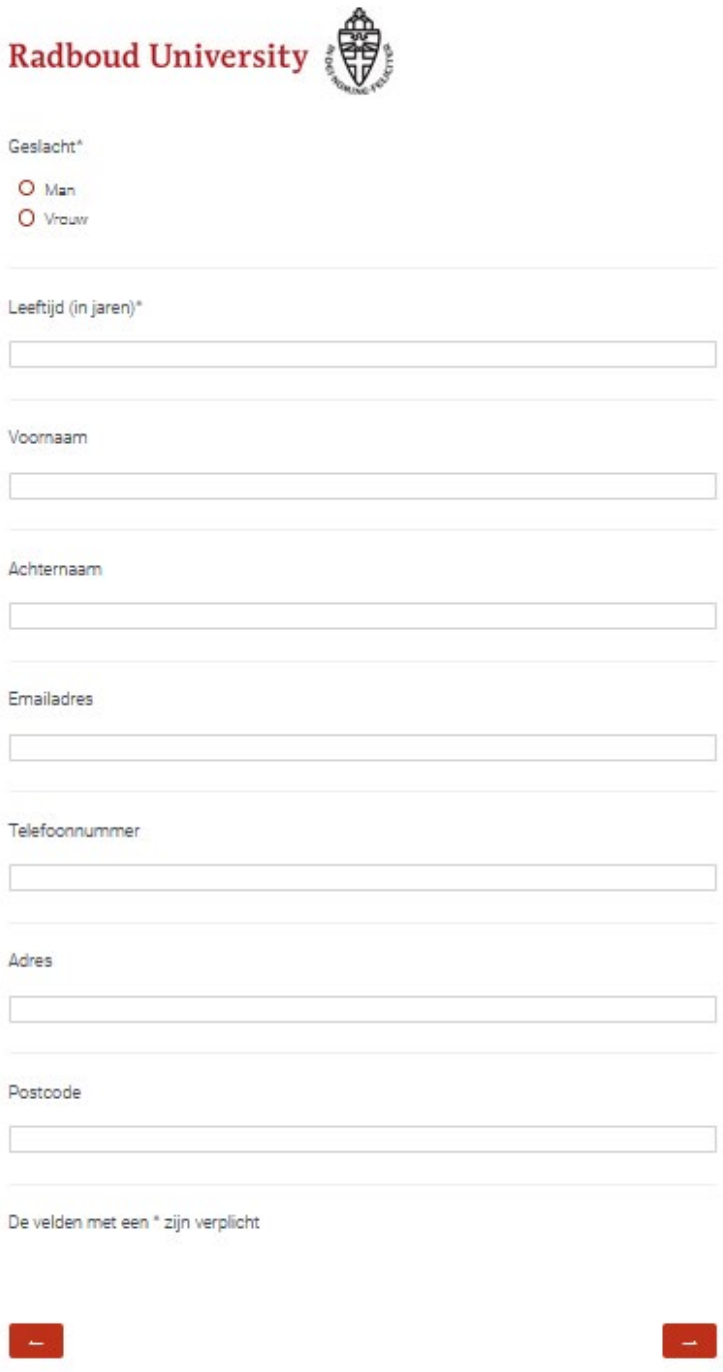
Wilt u een belangrijke bijdrage leveren aan het voorkomen van internetcriminaliteit? Klik op de onderstaande link om mee te doen aan het onderzoek.

Onderzoek Internetveiligheid

Heeft u vooraf vragen? Neem dan gerust contact op met de onderzoeker: Mart Geurts (telefoon: 0633812060; e-mail: mart.geurts@student.ru.nl).

Met vriendelijke groet

Bijlage 3: Opmaak in Qualtrics waar de deelnemers werden gevraagd persoonsgegevens in te vullen.



Bijlage 4: Youtube link naar de Animatievideo.

https://youtu.be/oj_ucFJDzU0