Navigeren door Cyberspace: Leeftijd, Opleiding en de kans op slachtofferschap van Phishing

Masterscriptie

Ytje Poelstra

14-7-2024

Eerste corrector: Jaap Nieuwenhuis
Tweede corrector: Marijtje van Duijn

Samenvatting

In hoeverre wordt individueel slachtofferschap van phishing verklaard door leeftijd en opleiding en wordt deze relatie gemedieerd door kennis over online veiligheid?

De afgelopen decennia heeft de komst van het internet veel teweeg gebracht. Voor criminelen is er een nieuwe vorm van criminaliteit ontstaan. Een bekende vorm van online criminaliteit is phishing, waarmee criminelen via e-mail of berichten mensen naar valse websites proberen te lokken (Ministerie van Algemene Zaken, 2023). Het slachtoffer wordt verleid om op een link te klikken met het gevolg dat er persoonsgegevens of zelfs geld gestolen worden. Om gericht interventies te kunnen inzetten is het van belang te bepalen welke groep mensen het meest kwetsbaar is. Er is onderzoek gedaan naar de vraag of leeftijd en opleidingsniveau risicofactoren zijn voor het slachtoffer worden van phishing, en naar de rol die kennis over online veiligheid hierin speelt.

Voor dit onderzoek is gebruik gemaakt van data van het Planbureau Fryslân. Zij hebben een enquête uitgezet onder de Friese bevolking met daarin een experiment om de kwetsbaarheid van de respondenten te toetsen. In dit onderzoek wordt gebruik gemaakt van zowel een lineare regressieanalyse, als een logistische regressieanalyse om de statistische analyses uit te voeren om te bepalen welke invloed leeftijd, opleidingsniveau en de mediator kennis over online veiligheid hebben op de kans op slachtofferschap van phishing. Uit de resultaten blijkt dat jonge mensen vaker verkeerd hebben gehandeld in dit experiment, wat heeft geleid tot phishing. Dit is opvallend omdat uit de theorie blijkt dat oudere mensen kwetsbaarder zijn voor het slachtofferschap van phishing. Voor opleidingsniveau en de mediator kennis over online veiligheid zijn geen significante resultaten gevonden.

Voor volgonderzoek is het interessant om de frequentie van het internet gebruik te onderzoeken. Jonge mensen maken vaker gebruik van internet (Büchi, Just & Latzer, 2016) en dit zou een verklaring kunnen zijn waardoor zij vaker slachtoffer worden van phishing. Daarnaast is het interessant om een studie op te zetten waarbij de deelnemers niet van te voren weten dat zij getoetst worden op het onderwerp phishing. In het onderzoek van het Planbureau Fryslân waren de deelnemers hier zich bewust van en heeft dit mogelijk invloed gehad op de uitkomsten.

Er wordt verwacht dat de criminaliteit de komende jaren alleen maar meer online gaat plaats vinden (Radar, 2023), dus is het belangrijk om een volledig beeld te creëren over de grootste risicofactoren zodat er gericht ingezet kan worden op preventie om er voor te zorgen dat phishing in de toekomst niet een nog groter probleem wordt.

Inhoudsopgave

Inleiding

Sinds de komst van het internet is de wereld enorm veranderd. Mensen hebben niet uitsluitend meer een leven in de “echte” wereld maar ook online. Tegenwoordig gebruikt circa 97% van de Nederlandse inwoners het internet (Centraal Bureau voor de Statistiek, 2020). Hoewel deze ontwikkeling talloze voordelen met zich heeft meegebracht, heeft deze ook een keerzijde. Mensen die dagelijks actief zijn op het internet vormen een doelwit voor online criminaliteit. Op elk moment van de dag, wanneer mensen hun telefoon bij zich hebben, bestaat de mogelijkheid dat een online crimineel een poging waagt. Tegenwoordig is de telefoon niet meer uit het dagelijks beeld van de mensen te denken en hier maken criminelen gebruik van.

Een bekende vorm van online criminaliteit is phishing, waarmee criminelen via e-mails of berichten mensen naar valse websites proberen te lokken (Ministerie van Algemene Zaken, 2023). Vaak doen criminelen zich voor als legitieme organisaties zoals banken of overheidsinstellingen en vragen zij persoonlijke gegevens als wachtwoorden of financiële informatie op. De persoon wordt verleid op een link te klikken met het gevolg dat er persoonsgegevens en geld met soms enorme bedragen gestolen worden. Internet criminelen worden steeds beter in het laten lijken dat de link legitiem is, waardoor het onderscheid tussen een echte website of een nep site niet meer te herkennen valt (Radar, 2023). 84% van de Nederlanders van 12 jaar of ouder maakte bijvoorbeeld gebruik van internetbankieren in 2019. In 2015 lag dit percentage rond de 77% (Centraal Bureau voor de Statistiek, 2021). Criminelen maken vaak gebruik van een naam van de bank om mensen naar een valse website te lokken. Eén verkeerde keuze kan al grote gevolgen hebben doordat geld of persoonsgegevens gestolen worden.

Twee op de drie Nederlanders gaven aan in 2021 ten minste één keer een bericht te hebben ontvangen dat waarschijnlijk van een oplichter was (Centraal Bureau voor de Statistiek, 2022). 2% van de Nederlanders gaf aan hier te zijn

ingetrapt. Dit zorgt ervoor dat Nederlanders zich online onveiliger voelen dan op straat (Ministerie van Justitie en Veiligheid, 2022a). Er is een trend zichtbaar waarbij steeds meer criminaliteit zich verplaatst naar het internet. In 2019 werden er circa 4700 aangiftes gedaan van online criminaliteit maar in 2022 is dit aantal verdrievoudigd naar bijna 14.000 aangiftes (Radar, 2023). Daarnaast blijkt het aantal overvallen en inbraken, dus de fysieke criminaliteit, te zijn gedaald. Er is bijvoorbeeld een daling van 38% in 2022 ten opzichte van 2019 in het aantal woninginbraken in Nederland (Radar, 2023).

Veel mensen zijn tegenwoordig bekend met het nieuwe begrip phishing. Toch blijkt dat 30% van alle phising mail geopend wordt (Veneco, 2022). Ook uit onderzoek van het Planbureau Friesland blijkt dat de kennis van de Friese bevolking over beveiliging online hoog is, maar dat het gedrag online niet altijd veilig is (de Witte, Marinus & la Roi, 2023).

Om het slachtofferschap van phishing te verminderen is het belangrijk om te onderzoeken welke groep het meeste risico loopt om een phishing mail te openen. Dit onderzoek probeert aan de hand van demografische kenmerken het slachtofferschap van phishing te verklaren. Verschillende onderzoeken naar de invloed van leeftijd op het risico van slachtofferschap van phishing laten tegenstrijdige resultaten zien. In een aantal onderzoeken wordt gesteld dat jongeren vaker slachtoffer worden van online criminaliteit zoals phishing (Greitzet et al., 2021; Wilsem, 2013; Li et al., 2020). Aan de andere kant zijn er studies die concluderen dat oudere mensen vaker slachtoffer worden van online criminaliteit (Sarno et al., 2020; Gavett et al., 2017).

Het tweede persoonskenmerk waarmee het slachtofferschap van phishing probeert te verklaren in dit onderzoek, is opleidingsniveau. Een zekere mate van kritisch denken is vereist om te kunnen beoordelen of een e-mail legitiem is. Uit een onderzoek van Butler (2012) blijkt dat mensen met een hoge opleiding beter presteerden in kritisch denken dan mensen met een lage opleiding. Om deze reden is het logisch om te onderzoeken wat voor invloed het opleidingsniveau heeft op de kans op slachtofferschap zodat er gerichte preventies ingezet kunnen worden.

Kennis over online veiligheid wordt meegenomen als mediator in dit onderzoek. Dit kan bijdrage tot een beter begrip van de mechanismen die ten grond slag liggen aan het verband van deze demografische kenmerken. Door de rol van kennis over online veiligheid te onderzoeken kan het helpen bij het identificeren van beschermende factoren die de relatie tussen leeftijd en slachtofferschap van phishing kunnen beïnvloeden. Dit zou kunnen leiden tot het ontwikkelen van effectieve interventies.

Dit onderzoek beoogt een bijdrage te leveren aan de bestaande inzichten die bekend zijn over de invloed van demografische factoren op het slachtofferschap van phishing. Binnen de sociale wetenschap blijft de vraag naar verkennend onderzoek op het gebied van cyberslachtofferschap groot omdat er nog veel onduidelijkheid bestaat over welke groepen mensen het meeste risico hierop lopen (Näsi et al., 2021).

Door inzicht te krijgen op de invloed van leeftijd en opleiding op het slachtofferschap van phishing, kunnen gerichte preventie- en voorlichtingscampagnes worden ontwikkeld. Er bestaan algoritmen om verdachte websites te identificeren waardoor automatische detectiesystemen ontwikkeld kunnen worden om verdachte e-mail te verwijderen voordat zij bij de gebruiker terecht komen (Feng et al., 2020). Daarnaast kan er gerichte voorlichtingscampagnes worden ontwikkeld die aansluiten bij de specifieke behoefte van verschillende doelgroepen wanneer blijkt dat de kennis over online veiligheid van een groep erg laag is.

Phishing heeft invloed op de sociale cohesie. Sociale cohesie verwijst naar de dynamiek binnen een samenleving wat gekenmerkt wordt door attitudes en normen. Het omvat vertrouwen, een gevoel van verbondenheid en de bereidheid op hulp te bieden (Chan et al., 2006). Doordat mensen slachtoffer worden van phishing wordt het vertrouwen in de digitale wereld aangetast (Ministerie van Justitie, 2022b). Mensen kunnen minder vertrouwen hebben in de online wereld en de mensen online uit angst voor mogelijke misleiding. Er heerst, met de opkomst van phishing, een onveilig gevoel bij mensen op het internet. Twee op de drie Nederlanders heeft namelijk in 2021 tenminste één keer een verdacht bericht online ontvangen (Centraal Bureau voor de Statistiek, 2022). Als gevolg hiervan geven mensen aan dat zij zich tegenwoordig veiliger voelen op straat dan online (Ministerie van Justitie en Veiligheid, 2022a). Uit onderzoek blijkt dat meer sociale cohesie er voor zorgt dat mensen zich veiliger voelen en minder vaak slachtoffer worden van criminaliteit (Huygen & De Meerde, 2008). Het is dus van belang phishing beter te begrijpen zodat er aanbevelingen

gedaan kunnen worden voor eventuele interventies om het risico op slachtofferschap te verminderen, om zo het veiligheidsgevoel en hiermee de sociale cohesie binnen de samenleving te waarborgen. Om online slachtofferschap te voorkomen, zal online slachtofferschap eerst verklaard moeten worden.

In dit onderzoek wordt gebruik gemaakt van data van het Planbureau Friesland waarbij onderzoek is gedaan binnen de Friese bevolking. Om deze reden zal het slachtofferschap van phishing specifiek van de Friese bevolking verklaard worden aan de hand van leeftijd, opleiding en kennis. De uitkomsten van het onderzoek zullen van belang zijn om beleid gericht te kunnen inzetten zodat het gedrag online veiliger wordt. In deze scriptie staat de volgende onderzoeksvraag centraal:

In hoeverre wordt individueel slachtofferschap van phishing verklaard door leeftijd en opleiding en wordt deze relatie gemedieerd door kennis over online veiligheid?

Theoretisch kader

Dit hoofdstuk richt zich op het begrijpen van slachtofferschap van criminaliteit, met name op het begrijpen van de verklarende factoren die relevant zijn voor het slachtofferschap van phishing. In het eerste deel van het theoretisch kader wordt de gelegenheidstheorie behandeld om het mechanisme achter slachtofferschap in het algemeen te begrijpen. Vervolgens wordt deze theorie gekoppeld aan het slachtofferschap van phishing. In het tweede deel van het hoofdstuk worden verschillende theorieën besproken waaruit de hypotheses vloeien. Hierin staan de persoonskenmerken van slachtoffers centraal.

Gelegenheidstheorie

De gelegenheidstheorie is een theorie waarin niet het criminele gedrag van de daders verklaard wordt, maar waar de nadruk ligt op factoren die gelegenheid bieden voor het criminele gedrag (Ruimschotel, 1998). Deze theorie staat bekend om de uitdrukking: "gelegenheid maakt de dief." Slachtofferschap ontstaat wanneer er een gemotiveerde dader, een aantrekkelijk doelwit en afwezigheid van controle zijn (Cohen & Felson, 1997). Personen worden slachtoffer van phishing wanneer deze omstandigheden aanwezig zijn. Volgens de theorie is de aanwezigheid van gelegenheid de belangrijkste oorzaak van slachtofferschap, en de kans om slachtoffer te worden van een misdrijf is aanzienlijk kleiner wanneer deze gelegenheid ontbreekt (Felson & Clarke, 1998).

Ten eerste loopt een slachtoffer loopt risico door de aanwezigheid van gemotiveerde daders. Een gemotiveerde dader is iemand die geneigd is een misdrijf te plegen (Cohen & Felson, 1979). Met de groei van het internet hebben potentiële daders meer kennis kunnen opdoen over de technologieën die nodig zijn om phishingaanvallen uit te voeren (Hutchings & Hayes, 2009). Hierdoor kunnen ze anoniem en veilig vanuit hun eigen huis opereren waardoor slachtoffers ten alle tijden aangevallen kunnen worden.

Ten tweede kunnen mensen slachtoffer worden vanwege hun aantrekkelijkheid als doelwit. Het doelwit moet toegang hebben tot het internet en waardevolle gegevens of geld bezitten dat gestolen kan worden. Uit de inleiding blijkt dat het internetgebruik, en waaronder het internetbankieren, de afgelopen jaren enorm is gestegen waardoor het aantal geschikte doelwitten ook is toegenomen. Personen die onbeveiligde websites bezoeken of persoonlijke informatie op het internet delen, worden beschouwd als geschikte doelwitten voor potentiële daders. Uit onderzoek van Reyns en Randa (2020) blijkt dat personen die hun persoonlijke informatie online openbaar delen, een grotere kans hebben om slachtoffer te worden van

online identiteitsdiefstal, zoals phishing, dan degenen die hun informatie niet online beschikbaar stellen.

Ten derde is er weinig controle op het internet wat het een aantrekkelijk platvorm maakt voor criminelen. Op het internet heerst veel anonimiteit, ontwikkelt de technologie zich snel en heeft het een enorme omvang, waardoor criminelen onder de radar kunnen opereren. Dit resulteert in een verminderde kans op ontdekking en arrestatie. Het ontbreken van controle kan ook betrekking hebben op gebrekkige cybersecurity. Personen die hun computer niet goed beschermen, zijn makkelijkere doelwitten voor internetcriminelen. Individuen moeten proactief zorgen voor de veiligheid van hun online identiteit door bijvoorbeeld wachtwoorden regelmatig te updaten, antivirusbescherming te gebruiken en e-mails kritisch te beoordelen (Reyns & Henson, 2016). Van de drie concepten van de gelegenheidstheorie (gemotiveerde dader, aantrekkelijk doelwit en gebrek aan controle) is het gebrek aan controle de meest onderbelichte (Choi et al., 2021).

De gelegenheidstheorie legt uit waarom criminelen aangetrokken worden tot phishingaanvallen op bepaalde groepen mensen. De drie bovengenoemde redenen maken dit duidelijk. De gelegenheidstheorie biedt een raamwerk om het slachtofferschap van phishing te begrijpen door te focussen op de kenmerken en risicofactoren die een slachtoffer aantrekkelijk maken. De hypotheses die aan het einde van dit hoofdstuk zijn opgesteld, richten zich voornamelijk op het tweede punt, namelijk dat het doelwit aantrekkelijk moet zijn. De hypotheses richten zich op individuele kenmerken die de kans op slachtofferschap van phishing vergroten, wat maakt dat deze individuen aantrekkelijkere doelwitten zijn voor criminelen.

Hypotheses

Tegenwoordig heeft bijna iedereen in Nederland toegang tot het internet wat veel mensen potentieel kwetsbaar maakt. Oudere mensen in het bijzonder zijn gevoelig om niet adequaat te reageren op verdachte mails (Sarno et al., 2020). Het blijkt dat ouderen eerder geneigd zijn op verdachte links te klikken met het gevolg dat er geld of gegevens gestolen worden (Kircanski et al., 2018).

Een reden waarom ouderen kwetsbaarder zijn op het internet, kan te maken hebben met het feit dat zij een aantrekkelijk doelwit vormen voor internetcriminelen. Voorheen waren cyberaanvallen meestal willekeuring en random, echter zijn cyberaanvallen tegenwoordig geëvolueerd naar gerichte aanvallen op specifieke aangewezen doelwitten (Kim et al., 2018). Ouderen lijken vaker, in vergelijking met jongere mensen, het doelwit te zijn van online

fraude, met in het bijzonder financiële uitbuiting vanwege hun grotere potentieel voor rijkdom (Rabiner et al., 2006). Uit onderzoek van Luginbuh & Smid (2021) blijkt dat leeftijd een belangrijke factor is in de vermogensopbouw. In vergelijking met jongeren hebben ouderen over een langere periode kunnen sparen en hun hypotheek kunnen aflossen (Luginbuhl & Smid, 2021). Doordat jongeren de hypotheek nog niet afgelost hebben, hebben zij een hogere schuld. Volgens de gelegenheidstheorie zijn ouderen dus het perfecte slachtoffer omdat er meer geld te stelen valt.

De tweede reden heeft te maken met ouder worden en de cognitieve veranderingen die hiermee gepaard gaan. Gemiddeld genomen is vanaf de 60 jaar achteruitgang te zien in onder andere de verbale vaardigheid en inductief redeneren van een persoon (Schaie, 1994). Met inductief redeneren wordt het proces bedoeld waarmee iemand onvolledige informatie transformeert in een volledig weergave van kennis en overtuigingen (Kutsch, 2021). Onder verbalen vaardigheid valt bijvoorbeeld woordenkennis en dit bestaat uit het vermogen van een persoon om zich uit te drukken met behulp van woorden (Schaie, 1994). Deze twee mentale vermogens zijn cruciaal om te beslissen wanneer de inhoud van een e-mail veilig is of niet (Sarno et al., 2020). Tegenwoordig stellen criminelen e-mails of berichten erg professioneel op waardoor het lastiger wordt om de legitimiteit hiervan te beoordelen. Bij oudere mensen gaat het mentale vermogen achteruit wat hen extra kwetsbaar maakt in de kans op slachtofferschap van phishing omdat zij de legitimiteit van een e-mail niet goed kunnen oordelen.

Ten derde zijn oudere mensen positiever ingesteld dan jongere volwassenen. Ouder worden brengt ongemakken met zich mee als fysieke achteruitgang en het verlies van naasten, toch blijkt dat deze doelgroep positiever in het leven staat dan jongeren. Dit fenomeen staat bekend als het positiviteitseffect. Oudere mensen slaan positieve informatie beter op dan negatieve informatie (Reed et al., 2014). Dit zorgt ervoor dat zij de waarschuwingstekens, zoals een merkwaardig URL, van een e-mail niet zien. Zij focussen zich liever op de positieve informatie die in het bericht staat, zoals de kans op het winnen van een dure telefoon waardoor zij sneller op de verdachte URL klikken. Dit maakt dat zij sneller slachtoffer worden van phishing.

Uit de bovenstaande literatuur blijkt dat ouderen kwetsbaarder zijn en een verhoogd risico hebben op het slachtofferschap van phishing. De formulering van de eerste hypothese is als volgt;

H1: Naarmate mensen ouder worden, neemt het risico op het slachtofferschap van phishing toe.

Het risico op slachtofferschap van phishing heeft niet enkel te maken met de leeftijd maar opleiding kan hier ook een rol in spelen. Mensen met een lagere opleiding kunnen een minder ontwikkelde kritische denkvaardigheden hebben, in vergelijking met hoger opgeleiden. Er wordt veel onderzoek gedaan naar de invloed van opleiding op de kritische denkvaardigheden van een persoon. Zo blijkt dat het aantal jaren in onderwijs het kritisch denken kan voorspellen. In een onderzoek van Butler (2012) presteerden mensen met een hogere opleiding beter in kritisch denken dan mensen met een minder hoge opleiding. Bij een hogere opleiding leren studenten vaardigheden en kennis aan zodat zij een hoge mate van kritisch denken ontwikkelen (Halpern, 2014). Dit helpt de studenten kritischer naar de wereld kijken.

Om te bepalen of een bericht legitiem is of van een internetcrimineel afkomstig is, is het van belang om kritisch naar de mail te kijken. De URL is een goede aanwijzing om te bepalen of het bericht legitiem is. Criminelen maken een nieuwe website aan, met bijbehorend URL, die vaak op een echte site lijkt waar vervolgens met één klik op dit URL gegevens of geld gestolen wordt (Butavicius et al., 2022). Daarnaast kan de vorm van begroeting een hint zijn. Bedrijven waar iemand klant is zullen een mail sturen met de naam of het geslacht van de klant. Berichten met een algemene begroeting zonder de naam van de ontvanger kan een teken zijn een mail met onjuiste intenties (Canfield et al., 2016). Ten derde zijn onregelmatigheden in de grammatica, interpunctie en spelling een belangrijke indicator (Batuvicius et al., 2022). Toch worden internetcriminelen steeds beter in het schrijven en ontwerpen van een professioneel bericht wat het herkennen hiervan steeds moeilijker maakt.

Mensen met een lage opleiding hebben waarschijnlijk minder handvaten gekregen tot het aanleren van vaardigheden zoals kritisch denken, wat het risico op slachtofferschap van phishing verhoogd. Doordat zij lagere kritische denkvaardigheden hebben zijn zij mogelijk minder in staat om de legitimiteit van een e-mail te kunnen beoordelen wat hen, volgens de gelegenheidstheorie, een aantrekkelijk doelwit maakt. Om deze reden is de volgende hypothese opgesteld.

H2: Hoe hoger de opleiding, hoe grotere de kans op slachtofferschap van phishing wordt.

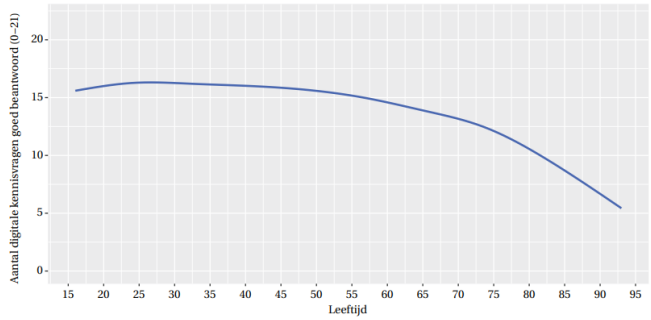
Er wordt verwacht dat kennis een bepalende factor is in het verklaren van het risico op slachtofferschap van phishing. Hypothese drie en vier stellen dat kennis een mediërend effect heeft op de relatie tussen de demografische kenmerken (leeftijd en opleiding) en het risico op slachtofferschap. Dit houdt in dat kennis verklaart waarom oudere en laagopgeleide mensen een verhoogd risico op slachtofferschap van phishing hebben. Kennis kan voorspeld worden aan de hand van leeftijd en opleiding, en verklaart vervolgens de kans op slachtofferschap van phishing. In de komende alinea's zal dit uitgelegd worden.

Hypothese 1 stelt dat ouderen meer risico hebben op het slachtoffer worden van phishing dan jongeren. Hier zijn enkele mogelijke verklaringen voor gegeven die bijgedragen hebben aan het ondersteunen van de eerste hypothese. Toch wordt verwacht dat kennis de bepalende factor is in de verklaring voor het verhoogde risico voor oudere op slachtofferschap van phishing. In de afgelopen decennia heeft het internet de wereld in een snel tempo veranderd waardoor ouderen niet opgegroeid zijn met de nieuwe technologieën. In 2020 gebruikte 49% van de 75 jaar en ouder dagelijks het internet, 78% van de ouderen tussen de 65 en 75 gebruikten dagelijks het internet tegenover 94% van de jongeren tot 25 jaar (CBS, 2021). Het blijkt dat er een kloof bestaat tussen ouderen en moderne technologie (Lee & Coughlin, 2014). Ouderen brengen minder tijd door op internet, wat er voor zorgt dat zij hier minder kennis over hebben. In vergelijking met jongeren hebben ouderen een stuk minder kennis over online veiligheid. Zo hebben zij moeite met het kritisch beoordelen van informatie en kunnen zij zich online niet goed beschermen (de Vries et al., 2022). In afbeelding 1 staat de kennis over online veiligheid met leeftijd afgebeeld. De resultaten zijn afkomstig uit een onderzoek van DIGCOM, een tweejarig onderzoeksproject dat uitgevoerd wordt door de

Universiteit van Amsterdam (de Vries et al.,2022). Circa 1500 Nederlanders van 10 tot 93 jaar hebben deelgenomen aan de studie. In afbeelding 1 is duidelijk te zien dat de kennis sterk daalt vanaf 60 jaar.

Het ontbreken van deze ervaring en kennis kan oudere volwassenen in de problemen brengen bij het identificeren van valse e-mails (Sarno et al., 2020). Hierdoor lopen zijn meer risico op het slachtoffer worden van phishing. Om deze reden is de derde hypothese opgesteld.

H3:Het verband tussen leeftijd en de kans op slachtofferschap van phishing wordt gedeeltelijk gemedieerd door de kennis over online veiligheid.

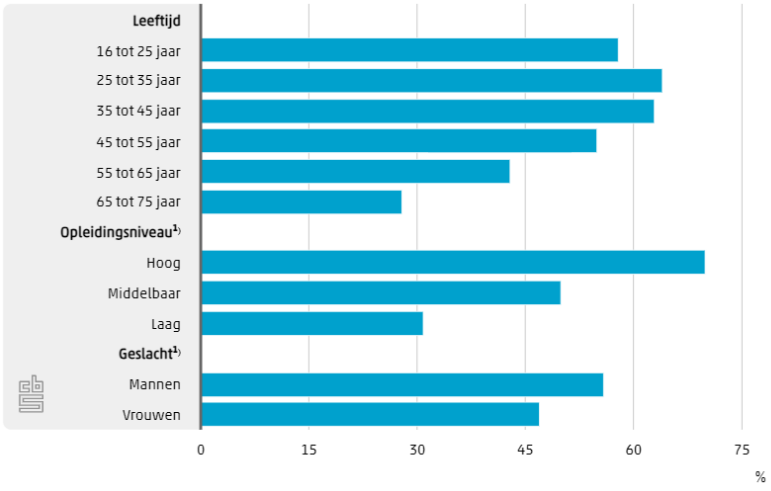


Afbeelding 1 Digitale kennis per leeftijdscategorie (de Vries et al., 2022)

Hypothese 2 stelt dat laagopgeleiden een verhoogd risico lopen op het slachtofferschap van phising. Daar is hiervoor een verklaring voor gegeven, namelijk dat laagopgeleiden minder vaardigheden hebben dan hoger opgeleiden om een valse mail te kunnen identificeren. Toch wordt wederom verwacht dat kennis de bepalende factor is in de verklaring waarom mensen met een laagopleidingsniveau een verhoogd risico lopen.

Het blijkt dat laagopgeleiden achterblijven in kennis en digitale vaardigheden op het internet. De beoordeling van de digitale basisvaardigheid is gebaseerd op de volgende gebieden; (1) informatie en digitale geletterdheid, (2) online communicatie, (3) computers en online diensten, (4)

privacybescherming en (5) softwaregebruik (CBS, 2021). Iemand heeft een digitale basisvaardigheid wanneer zij gebruik maken van één van de gebieden informatie en communicatie en één op een ander gebied. Iemand met een meer dan digitale basisvaardigheid maakt gebruik van twee of meer activiteiten uit op het gebied van informatie en communicatie en drie of meer op de andere gebieden (CBS, 2021). In afbeelding twee is te zien dat er een groot verschil zit in meer dan digitale basisvaardigheden bij de verschillende opleidingsniveaus. In 2021 had 70% van de hoogopgeleiden een goede digitale basisvaardigheid tegenover 31% van de laagopgeleiden (CBS, 2021). Ook blijkt dat laagopgeleiden minder vaak dagelijks online zijn in vergelijking met hoogopgeleiden. Zo was in 2021 96% van de hoogopgeleiden dagelijks online tegenover 76% van de laagopgeleiden (CBS, 2021).



Afbeelding 2: percentage digitale vaardigheden (CBS, 2021).

Daardoor blijkt dat laagopgeleiden zich minder veilig online gedragen. Ten eerste zijn zij minder bekend met de begrippen van internetveiligheid. Begrippen als spam, hacken, identiteitsfraude, phishing, firewall en VPN verbindingen zijn voorbeelden van begrippen die bedoeld worden. Op een schaal van 0 tot 10 die de online internet veiligheid meet, waarbij 0 het laagst en 10 het hoogst haalbare cijfer is, scoren laagopgeleiden een 6,6 en hoogopgeleiden een 8,5 (Akkermans et al., 2023). Ten tweede scoren laagopgeleiden ook het laagst op het beveiligen van hun apparaten en accounts online. Wederom met een schaal van 0

tot 10 scoren laagopgeleiden een 6,3 en hoogopgeleiden een 6,8 (Akkermans et al., 2023). Een belangrijke reden die genoemd wordt om beveiligingsmaatregelen niet te treffen is dat men niet weet hoe dit moet (Akkermans et al., 2023).

Kennis is dus een belangrijke reden waarom men hun online veiligheid vaak niet op orde hebben. Om deze reden is de laatste hypothese opgesteld.

H4: Het verband tussen opleidingsniveau en de kans op slachtofferschap van phishing wordt gedeeltelijk gemedieerd door kennis over online veiligheid.

Methoden

Beschrijving van de data en vragenlijst

De gebruikte data in dit onderzoek is secundaire data en afkomstig van het Planbureau Fryslân (PF). In dit onderzoek wordt gebruik gemaakt van gegevens die afkomstig zijn uit een studie van het Planbureau Fryslân genaamd "Bewegen inwoners van Fryslân zich veilig online?". Deze data is verzameld via het Panel Fryslân. Het panel is samengesteld uit diverse inwoners van Friesland die een representatieve mix vormen. De groep omvat zo'n 7.000 mannen, vrouwen en jongeren van de leeftijd 18 jaar en ouder met verschillende opleidingsniveaus, inkomens en achtergronden (Planbureau Fryslân, 2023). De panelleden krijgen maximaal 7 vragenlijsten per jaar toegestuurd via de mail met vragen over actuele thema's. Allereerst is er een selecte steekproef getrokken bij elke Friese gemeente op leeftijd van 18 jaar en ouder, niet wonend in een instelling. Uit deze groep is er daarna een aselecte steekproef getrokken. Vanwege een ondervertegenwoordiging van de groep 18 tot 35 jaar is er gekozen voor een oversampling van jongvolwassenen. Uit deze steekproef krijgt ieder een uitnodigingsbrief per mail toegestuurd waarin het doel en nut van het panel beschreven wordt. Twee weken later wordt er een herinneringsbrief verstuurd. Na aanmelding krijgen de respondenten een aanmeldingsvragenlijst. In deze lijst konden zij achtergrondgegevens invullen zoals leeftijd, inkomen, gezinssituatie, opleiding, afkomst etc.

Er wordt geschat dat er een aanmeldpercentage van ongeveer 8% bestaat, met een respons van 50% per vragenlijst (Planbureau Fryslân, 2021). Het percentage non-respons is aanzienlijk hoog, vooral bij het verzoek om deel te namen aan de vragenlijst. Het planbureau is zich hier bewust van, er wordt namelijk gevraagd om deel te nemen aan een online panel waarbij langdurige een bijdrage wordt verwacht (Planbureau Fryslân, 2021). Om te corrigeren voor deze non-respons is er een weging uitgevoerd om de juiste afspiegeling te krijgen van de Friese bevolking van 18 jaar en ouder. De resultaten worden gewogen op leeftijd, geslacht, opleiding en regio. Ondervertegenwoordigde groepen ontvangen een gewicht hoger dan 1, terwijl oververtegenwoordigde groepen een gewicht lager dan 1 krijgen (Planbureau Fryslân, 2021). Door deze aanpassing zorgt het ervoor dat in dit onderzoek groepen niet ondervertegenwoordigd zijn.

In 2023 is het onderzoek "Hoe Bewegen Inwoners van Friesland Zich Online" gepubliceerd. Hierin heeft het PF onderzoek gedaan naar de online veiligheid van de Friese inwoners. De panelleden hebben in 2022 een vragenlijst ontvangen met vragen over hun

digitale kennis, slachtofferschap van online criminaliteit en beschikbare informatievoorzieningen. Ook kregen de deelnemers 4 voorbeelden van mails of berichtjes waarin zij moesten aangeven welke vervolgstappen ze zouden nemen bij het ontvangen van deze mail. Voorbeelden van vervolgstappen waren; de afzender terug mailen, de mail negeren, doorsturen of verwijderen. Daarnaast moesten de leden aangeven wat de keuze van de vervolgstappen heeft beïnvloed; de afzender, de tekst of iets anders. Zo is gemeten hoe de leden een verdachte mail op veiligheid beoordelen en wat ze vervolgens met deze informatie doen. De vragenlijst is beantwoord door 2802 panelleden.

Naast de vragenlijst over online veiligheid wordt een tweede vragenlijst gebruikt om de algemene informatie over de panelleden mee te kunnen nemen in dit onderzoek. Hierin is informatie verwerkt waar zij bijvoorbeeld wonen, wat de geboortedatum is, hoe de gezinssituatie eruit ziet en wat het inkomen is. Om deze gegevens actueel te houden wordt eens in de drie jaar gevraagd of de panelleden deze gegevens kunnen bijwerken of aanpassen.

Operationalisaties

Slachtofferschap

De afhankelijke variabele in het onderzoek is het slachtofferschap van phishing. De data die gebruikt wordt komt uit de vragenlijst “Hoe Bewegen Inwoners van Friesland Zich Online”. Er zijn er vier berichten/mails voorgelegd aan de respondenten waarin zij moesten aangeven wat hun vervolgactie zou zijn na het lezen van het bericht. Twee van de vier berichten zijn neppe berichten, en dus phishing pogingen. Voor dit onderzoek is het relevant om te achterhalen welke persoonskenmerken mensen bezitten, zoals leeftijd en opleidingsniveau, die niet adequaat hebben gereageerd op de e-mail en dus onjuist hebben gehandeld. In het onderzoek van het Planbureau Fryslân is de eerste vraag een voorbeeld van een phishing mail. De vraag luidt als volgt: “Robin heeft al enige tijd een betaalrekening bij de Rabobank. Op 23 januari ontvangt Robin de onderstaande e-mail in het Postvak (zie afbeelding 3). Wat zou u met deze e-mail doen als u Robin was?” De respondent heeft keuze uit de volgende antwoordmogelijkheden:

- Ik beantwoord de e-mail
- Ik verwijder de mail
- Ik stuur de e-mail door naar iemand anders
- Ik kopieer en plak de URL uit de e-mail in een webbrowser

- ☐ Ik klik op de link in de e-mail
- ☐ Ik typ de URL over in een webbrowser
- ☐ Ik bewaar de e-mail
- ☐ Ik zoek naar meer informatie voordat ik een keuze maak
- ☐ Ik doe niets
- ☐ Iets anders, namelijk:

Van: Rabobank [mailto:bankzaken@rabobank.nl]
Verzonden: woensdag 23 januari 2019 17:58
Aan: robin@devries.nl
Onderwerp: Laatste herinnering: Uw aanvraag is nog niet verwerkt, voorkom een geblokkeerde betaalpas

Rabobank

Geachte relatie,

Uit onze administratie is gebleken dat u nog geen gebruik maakt van onze nieuwe betaalpas. De nieuwe betaalpas is beter beveiligd tegen frauduleuze praktijken en voldoet zich aan de Europese veiligheidsvoorschriften betreft bankzaken. Met de nieuwe betaalpas kunt u vertrouwd, veilig en gemakkelijk betalen en geld opnemen zoals u gewend bent en contactloos betalen in meer dan 12.000 winkels in heel Europa. Ook bent u beter beschermd tegen skimming en pinpas-fraude bij geldautomaten.

Het gebruik van uw huidige betaalpas wordt gedeactiveerd. In verband met de veiligheid van onze klanten is het verplicht uw huidige betaalpas te vervangen. Wij bieden onze klanten de mogelijkheid aan om dit kosteloos te doen. Klik hier om kosteloos uw nieuwe betaalpas aan te vragen en volg de benodigde stappen om uw aanvraag te voltooien. U ontvangt uw nieuwe betaalpas binnen **2 werkdagen** per post toegezonden.

Zolang u nog niet in bezit bent van een nieuwe betaalpas kunt u helaas nog geen gebruik maken van onze nieuwe dienstverlening.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd en van dienst te zijn geweest.

Alvast hartelijk dank voor uw medewerking.

Met vriendelijke groet,
Rabobank

Afbeelding 3: Mail die respondenten moeten beoordelen (bron: Planbureau Fryslân, 2022).

Deze mail illustreert wederom een phishing bericht. De bijbehorende vraag luidt als volgt: Een inwoner van Friesland ontvangt een appje van een onbekend nummer (zie afbeelding 4). Wat zou u met dit bericht doen als u inwoner was? De antwoordmogelijkheden zijn:

- ☐ In beantwoord het bericht
- ☐ Ik verwijder het bericht
- ☐ Ik stuur het bericht door naar iemand anders
- ☐ Als ik kinderen heb, bel ik ze op dit nieuwe nummer
- ☐ Als ik kinderen heb, bel ik hen op hun oude nummers

- ☐ Ik sla het nummer op
- ☐ Ik bewaar het bericht
- ☐ Ik zoek informatie over dergelijke berichten voordat ik iets doe
- ☐ Ik doe niets
- ☐ Ik doe iets anders, namelijk;

Afbeelding 4: Bericht die respondenten moeten beoordelen (bron: Planbureau Fryslân, 2022).

Zoals boven benoemd, is het echter enkel interessant om te kijken naar de antwoordmogelijkheden die mogelijk zouden kunnen leiden tot phishing omdat dit relevant is voor het onderzoek. Deze opties zijn; Ik kopieer en plak de URL (het www-adres) uit de e-mail in een webbrowser, Ik klik op de link in de e-mail en Ik typ de URL (het www-adres) over in een webbrowser. Bij het whatsapp bericht zijn de interessante antwoordkeuzes; Als ik kinderen heb, bel ik ze op dit nieuwe nummer en Ik sla het nummer op. Deze losse variabelen hebben een code van 0 (nee, deze optie niet gekozen) of 1 (ja, deze optie gekozen). Hier is één variabele slachtofferschap van gemaakt. Wanneer een respondent 1 geeft het aan dat zij hebben gekozen voor een optie wat leidt tot phishing. Als een respondent een 0 scoort, heeft diegene adequaat gereageerd en lopen zijn geen risico op het worden van een slachtoffer van phishing.

Opleidingsniveau

Opleidingsniveau is één van de twee onafhankelijke variabele in het onderzoek. De data van deze variabele komt uit de intakevragenlijst. In deze vragenlijst is het opleidingsniveau van de respondent vastgesteld. In de intakevragenlijst ziet de vraag met bijbehorende antwoord categorieën er als volgt uit:

Opleiding: Wat is de hoogste opleiding die u heeft afgerond?

- ☐ Basisonderwijs

- Praktijkonderwijs
- Voortgezet speciaal onderwijs (vso)
- Vmbo, havo-onderbouw, vwo-onderbouw, mbo-1 (inclusief mavo, ulo, mulo, lts, lhno, vbo)
- Havo-bovenbouw, vwo-bovenbouw (inclusief hbs, mms)
- Mbo-2, mbo-3, mbo-4
- Hbo-opleiding
- Universitaire-opleiding

In de gebruikte data is de variabele opleiding opgedeeld in drie categorieën; laag, midden, hoog. De score 1 in de dataset staat voor laag, 2 staat voor midden en 3 staat voor hoogopgeleid. Van deze variabele is een categorische variabele gemaakt. Het lage opleidingsniveau is als referentie in de analyse gezet, midden- en hoog opleidingsniveau zijn als twee dummy variabelen bewerkt. Dit betekent wanneer een respondent een score heeft van 1 op het hoge opleidingsniveau, deze automatisch op de andere twee variabelen een 0 scoort en behoort tot de groep met het hoge opleidingsniveau.

Leeftijd

De tweede onafhankelijke variabele van dit onderzoek is leeftijd. De data van de leeftijd van de respondenten komt wederom uit de intakevragenlijst. In deze vragenlijst heeft de respondent een huishoudenmatrix moeten invullen. In de matrix is gevraagd wat het geslacht is, geboortemaand en geboortejaar en wat hun positie in het huishouden is (gehuwd/ongehuwd, partner, kind of anders). In de gebruikte vragenlijst is de leeftijd omgezet in jaren en is het een continue variabele. De minimale leeftijd is 18 jaar en de maximale leeftijd is 93 jaar. Er zijn geen missende waarden gevonden en deze variabele is niet bewerkt voor dit onderzoek.

Kennis

Kennis is de mediator in het onderzoek. Om de kennis over online veiligheid te meten is in de vragenlijst de volgende vraag gesteld: “In welke mate bent u bekend met de onderstaande zaken?” De respondenten konden kiezen tussen; ik ken het, ik heb ervan gehoord maar weet niet precies wat het is en ik weet wat het is. De volgende online beveiligingsmethoden werden bevraagd: web tracking blocker, open source hardware- en software, ad-blocker, VPN-verbindingen, digitaal wachtwoordenkluis, instellingen om

cookies te blokkeren/uit te zetten, biometrische authenticatie, tweestapsverificatie, gebruik van lange wachtwoorden, het maken van back-ups, automatische updates en virusscanner. In de dataset is elke online beveiligingsmethode een aparte variabele. Om er één variabele kennis van te maken zullen deze samengevoegd worden. Voordat de variabelen gecombineerd worden, dient eerst gecontroleerd te worden of deze twee bij elkaar passen. Via Cronbach's Alpha wordt een betrouwbaarheidsanalyse uitgevoerd waarin vastgesteld wordt of verschillende items samengevoegd kunnen worden tot één variabele. Hoe dichter de Cronbach's Alpha bij de 1 ligt, hoe betrouwbaarder de schaal is. Uit de analyse is gebleken dat de losse variabelen perfect bij elkaar passen. De Cronbach's Alpha is afgerond 0,90 en dat laat zien dat er een sterke samenhang bestaat tussen alle variabelen. Er zijn geen missende waarden gevonden.

De bovenstaande variabelen worden samengevoegd tot één variabele kennis. De antwoordmogelijkheden zijn gecodeerd met een 1 (ik ken het niet), 2 (ik heb ervan gehoord maar weet niet precies wat het is) en 3 (ik ken het). Met de compute functie worden de items bij elkaar opgeteld en samengevoegd als een nieuwe variabele kennis. Hoe hoger de score op kennis, hoe hoger de kennis van de respondent over de verschillende online beveiligingsmethoden.

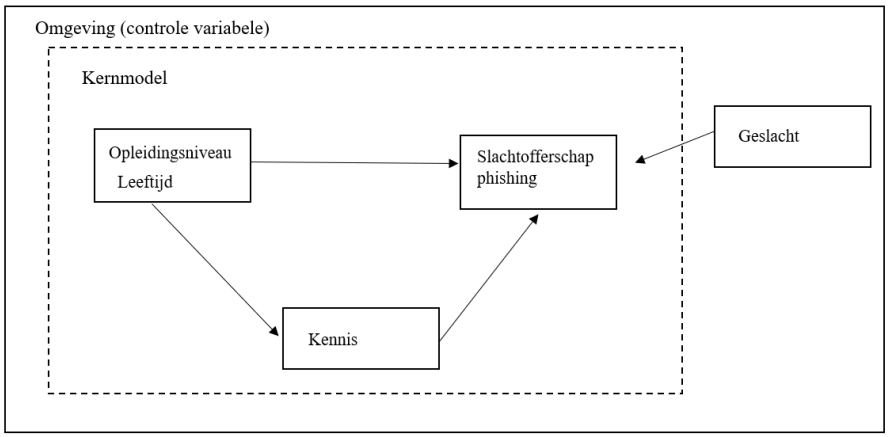
Geslacht

De controle variabele is geslacht. Deze variabele komt wederom uit de intakevragenlijst. In deze vragenlijst heeft de respondent in het huishoudenmatrix moeten invullen wat het geslacht is. Bij deze vraag staat vermeld dat de respondent het geslacht moet invullen wat op het paspoort van deze persoon staat. Er zijn drie keuze mogelijkheden; man, vrouw, X (non-binair). Uit de data van de vragenlijst die gebruikte wordt voor dit onderzoek blijkt dat niemand de optie genderneutraal heeft gekozen. Er zijn dus twee categorieën; man en vrouw. De score 1 in de dataset staat voor de man en score 2 staat voor een vrouw. Er zijn geen missende waarden gevonden en de variabele is niet bewerkt voor dit onderzoek.

Analyseopzet

Allereerst wordt er in de analyse gekeken naar de beschrijvende statistieken zoals het maximum, minimum en de standaarddeviatie. Dit draagt bij aan het vormen van een helder beeld over de variabelen en worden eventuele bijzonderheden, die invloed kunnen hebben op de analyse, benoemd. Vervolgens worden de bivariate statistieken belicht waarin er gemeten wordt hoe sterk de samenhang tussen de verschillende variabelen is.

De afhankelijke variabelen in dit onderzoek is slachtofferschap, de onafhankelijke variabelen zijn opleiding en leeftijd, de mediator is kennis en de controlevariabele is leeftijd. In afbeelding 3 staat het conceptueel model weergegeven.



Afbeelding 5: conceptueel model

In dit onderzoek wordt gebruik gemaakt van zowel een lineaire regressieanalyse, als een logistische regressieanalyse, om de onderzoeksvraag te beantwoorden. Model 1 wordt geschat aan de hand van de logistische regressieanalyse omdat de afhankelijke variabele de kans op slachtofferschap een binaire variabele is. Hier wordt getoetst wat de invloed van opleiding en leeftijd op de kans op slachtofferschap van phishing is, gecontroleerd door geslacht. Model 2 wordt getoetst door het lineaire regressiemodel. Hier wordt onderzocht wat voor invloed opleiding en leeftijd op de mediator kennis hebben gecontroleerd door de controle variabele geslacht. Het laatste model, model 3, wordt wederom geschat aan de hand van de logistische regressieanalyse omdat hier de invloed van de mediator op de kans op slachtofferschap getoetst wordt. In dit model wordt namelijk de mediator kennis toegevoegd, waardoor de invloed van de variabele zichtbaar wordt.

Resultaten

Beschrijvende statistiek

In tabel 1 staan de resultaten van de beschrijvende statistiek weergegeven. Wat opvalt is dat de gemiddelde leeftijd erg hoog ligt, namelijk rond de 63 jaar. De visualisatie van deze variabele staat weergegeven in figuur 4. De meeste respondenten zijn tussen de 60 en 80 jaar, wat maakt dat de variabele leeftijd niet mooi verdeeld is omdat de leeftijdsgroepen niet gelijk vertegenwoordigt zijn. De groep van 20 tot 50 jaar is sterk onder vertegenwoordigd en is er dus sprake van een links scheve verdeling. Aangezien leeftijd in model 2 wordt getoetst met een lineair regressiemodel, is het belangrijk om rekening te houden met de aannames. De T-toets veronderstelt dat de variabele normaal verdeeld is. Omdat de variabele scheef verdeeld is en dus niet normaal verdeeld, komt de betrouwbaarheid van de resultaten in twijfel.

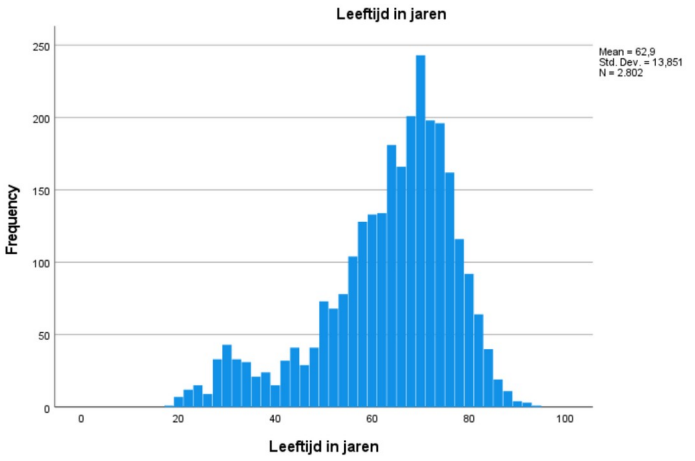
Ook blijkt uit tabel 1 dat de variabelen opleiding en geslacht niet gelijk verdeeld zijn. Ruim 63% van de ondervraagden zijn mannen terwijl de minderheid een vrouw is. Circa 52% van de respondenten heeft een hoog opleidingsniveau, terwijl iets meer dan 22% laagopgeleid is. Ook de variabele opleidingsniveau wordt meegenomen in model 2. Doordat de groepen een scheve verdeling hebben kan dit invloed hebben op de betrouwbaarheid van de resultaten.

In figuur 5 staat het histogram afgebeeld van de variabele kennis. Dit is de mediator in het onderzoek. Hierbij geldt; hoe hoger een respondent scoort op kennis, hoe hoger de algemene kennis over online veiligheid. Het gemiddelde is 31,55 op een maximale score van 39. In het figuur is duidelijk te zien dat er sprake is van een links scheve verdeling. Dit houdt in dat de meeste data rechts van het gemiddelde ligt. De meeste respondenten scoren dus hoog op algemene kennis over de online veiligheid. Er wordt verwacht dat er genoeg data beschikbaar is over de respondenten die lager scoren op kennis, maar wederom is hier sprake van een niet normale verdeling waar rekening mee gehouden moet worden.

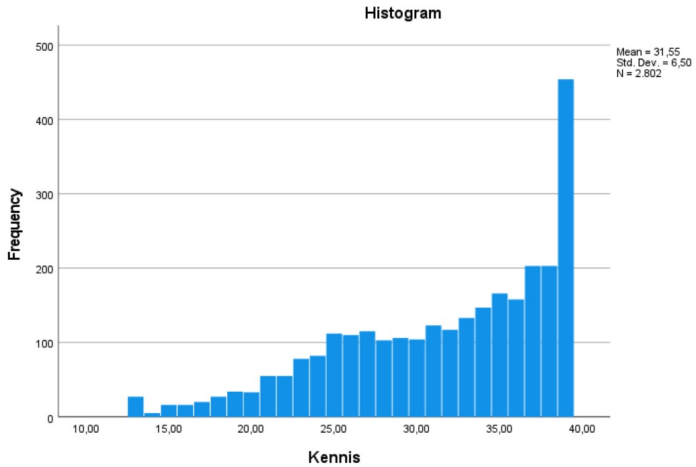
Tot slotte valt de verdeling van de kans op slachtofferschap op. Deze is zeer scheef verdeeld. 95,5% van de respondenten heeft geen kans op slachtoffer te worden van phishing omdat zij juist hebben gehandeld na het ontvangen van een verdachte mail. 5,5% van de respondenten heeft een keuze gemaakt wat leidt tot phishing. Echter, werd dit verwacht omdat het een afspiegeling is van de samenleving. Uit de inleiding bleek namelijk dat twee derde van de Nederlanders een verdachte mail hebben gekregen, waarvan 2% van deze mensen erin is getrapt.

Tabel 1: Beschrijvende statistieken n=2802

Variabele	*Gemiddelde/ Percentages (SD)*	*Min.*	*Max.*
Leeftijd	62,90 (13,85)	18,00	93,00
Opleiding		1,00	3,00
1= laag	22,30		
2= midden	26,60		
3= hoog	51,20		
Slachtofferschap		0,00	1,00
0= geen kans	94,50		
1= wel een kans	5,50		
Kennis	31,55 (6,50)	13,00	39,00
Geslacht		1,00	2,00
1=man	63,10		
2=vrouw	36,90		



Figuur 4: Verdeling leeftijd



Figuur 5: Verdeling kennis

Bivariate statistiek

In tabel 2 staan de correlaties tussen de verschillende variabelen weergegeven. Het valt op dat er twee matige correlaties bestaan. De hoogste correlatie, zoals verwacht, bestaat tussen leeftijd en kennis (r=-.328, p <.001). Dit houdt in dat oudere mensen over het algemeen een lagere score hebben wanneer de leeftijd stijgt. Daarnaast is de correlatie tussen opleidingsniveau en kennis het hoogste (r=.317, p < .001). Hier geldt; hoe hoger het opleidingsniveau hoe hoger de algemene kennis over online veiligheid. In het theoretisch kader is dit beschreven en voldoet dit aan de verwachtingen.

Wat ook opvalt is de correlatie tussen opleidingsniveau en slachtofferschap. In dit onderzoek wordt onder andere het effect van opleidingsniveau op de kans op slachtofferschap onderzocht. Uit de tweezijdige correlatietoets blijkt dat er nauwelijks een samenhang bestaat tussen de kans op slachtofferschap van phishing en opleidingsniveau (r=.008, p >.001). Zo is de correlatie tussen de kans op slachtofferschap en geslacht (r=.023, p >.001) erg laag, wat inhoudt dat tussen deze variabelen ook een zeer kleine samenhang bestaat. Daarnaast valt het op dat de correlatie tussen slachtofferschap en kennis erg laag is (r=.056, p<.001). Uit het theoretisch kader verwacht werd dat kennis invloed heeft op het slachtofferschap van phishing maar blijkt uit tabel 2 dat er een zeer kleine samenhang bestaat, wat opvallend is. Aan de hand van deze correlatie blijkt dat deze samenhang echter erg zwak is. De enige variabele die een iets grotere correlatie met de kans op slachtofferschap heeft is leeftijd, zoals verwacht wordt vanuit de theorie (r=.103, p <.001).

Tabel 2: Tweezijdige correlaties n=2802

	1	*2*	*3*	*4*	*5*
1. Leeftijd	-	-0,154*	-0,103*	-0,328*	-0,167*
2. Opleiding		-	0,008	0,317*	-0,011
3. Slachtofferschap			-	0,056*	-0,023
4. Kennis				-	-0,090*
5. Geslacht					-

*significantie niveau p<0,01

Modelschatting

In tabel 3 staan de resultaten van de analyse weergeven. Model 1 en 3 zijn door middel van het logistische regressiemodel geschat, model 2 is aan de hand van het lineaire regressiemodel geschat. Model 1 geeft de invloed van leeftijd en opleiding op de kans op slachtofferschap van phishing weer, model 2 laat de invloed van leeftijd en opleiding op kennis over online veiligheid zien en model 3 geeft het mediatie effect weer. In het theoretisch

kader zijn hypotheses opgesteld en aan de hand van deze hypotheses zullen de resultaten besproken worden.

Hypothese 1 stelt dat ouderen een verhoogd risico hebben op het worden van slachtoffer van phishing. De resultaten die van belang zijn voor deze stelling staan weergegeven in model 1. De odds-ratio van leeftijd is 0,970 (p=<0,001), deze geeft aan wanneer de leeftijd met één eenheid stijgt, de logodds op slachtofferschap daalt met 3%. Anders gezegd; de odds op slachtofferschap is voor oudere mensen, 0.970 keer zo klein als voor jongere mensen. Andersom betekent dit dat de kans op slachtofferschap voor een jongere respondent 1.03 keer groter is dan voor iemand die één jaar ouder is. Als de kans op slachtofferschap voor een jonge respondent 1.03 keer groter is voor iemand die één jaar ouder is, betekent dit dat voor mensen die 10 jaar van elkaar verschillen, het risico voor de jongere persoon ongeveer 1.344 keer groter is dan voor de oudere persoon. Wanneer respondenten 20 jaar verschillen, is het risico voor de jongere 2.208 keer groter dan de oudere. Dit resultaat is significant en kan er dus geconcludeerd worden dat er een negatief effect van leeftijd op de kans op slachtofferschap bestaat, gegeven de andere variabelen in het model. Dit is opvallend omdat uit het theoretisch kader verwacht werd dat de relatie andersom werkt.

Hypothese 2 stelt dat mensen een lagere opleiding een hogere kans hebben op slachtofferschap van phishing. Ook deze hypothese kan getoetst worden aan de hand van model 1 omdat deze het directe effect van opleiding op de kans op slachtofferschap toetst. Wat direct opvalt is dat de resultaten niet significant zijn en dit betekent dat er geen uitspraken kunnen worden gedaan over de relatie van opleidingsniveau met de kans op slachtofferschap van phishing.

Wat opvalt is dat geslacht een redelijk sterke invloed heeft op de kans op slachtofferschap. Geslacht is als controle variabele meegenomen in dit onderzoek maar in de logistische regressieanalyse blijkt dat het een sterk effect heeft op de kans op slachtofferschap. De odds-ratio voor geslacht is namelijk 0,688 (p=0,038). Dit betekent dat de kans dat een vrouw slachtoffer wordt van phishing 31,2% lager is dan die van een man. Dit bevestigt de verminderde kans op slachtofferschap voor vrouwen in vergelijking met mannen.

Tabel 3: resultaten logistische en lineaire regressie analyse

Model 1: logistische regressie, Y=slachtofferschap
Model 2: lineaire regressie, Y=kennis over online veiligheid
Model 3: logistische regressie met mediator kennis, Y=slachtofferschap

	Model 1			*Model 2*		*Model 3*		
	b (SE)	*Exp(B)*	*P**	*b (SE)*	*p*	*b (SE)*	*Exp(B)*	*P*
Constante	-0,416 (0,812)	0,660	0,425	40,808 (749)	<0,001	-1,090 (0,812)	0,336	0,179
Geslacht	-0,374 (0,180)	0,688	0,038	-3,255 (0,226)	<0,001	-0,319 (0,187)	0,727	0,088
Leeftijd	-0,030 (0,005)	0,970	<0,001	-0,154 (0,008)	<0,001	-0,028 (0,006)	0,972	<0,001
Opleiding Midden	0,055 (0,252)	1,056	0,828	2,675 (0,318)	<0,001	0,006 (0,256)	1,006	0,983
Hoog	-0,057 (0,229)	0,945	0,803	4,385 (0,278)	<0,001	-0,133 (0,239)	0,875	0,578
Kennis						0,017 (0,016)	1,017	0,277
Hosmer lemeshow test	9,082		0,335			9,850		0,276
R^2				0,237				
Partiële F				290,250	<0,001			
-2LL	1167,449					1166,237		

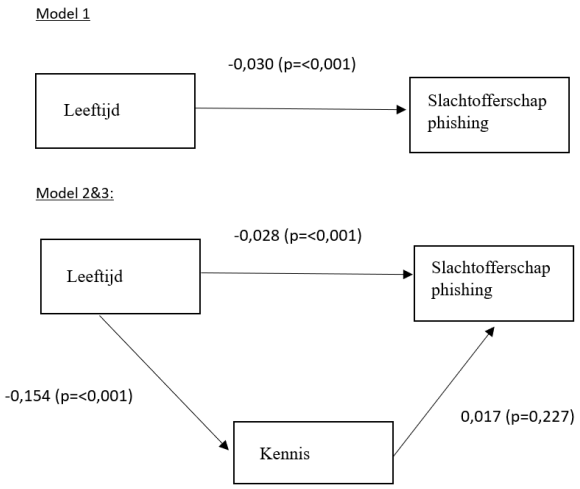
* Significantieniveau p <0,05

De derde hypothese stelt dat respondenten met een hoge leeftijd minder kennis over online veiligheid hebben waardoor zij een verhoogd risico op slachtofferschap van phishing hebben. Bij deze hypothese is van belang om te kijken wat er met de variabele leeftijd in model 3 gebeurt, ten opzichte van model 1, waar de mediator kennis is toegevoegd. Om inzichtelijk te maken wat het effect van alle variabelen in het model is, is er een model gemaakt met bijbehorende waarden in figuur 6. Omdat in het figuur alle drie modellen uit tabel 3 staan weergegeven met hun bijbehorende waarde is ervoor gekozen om de waarden van de logistische regressie (model 1 en 3) te presenteren aan de hand van de helling in plaats van de odds-ratio zoals hierboven beschreven staat.

Het totale effect van leeftijd naar de kans op slachtofferschap is -0,030, wat te zien is in model 1 in tabel 3. Wanneer kennis wordt toegevoegd in model 3, verandert het een en ander. Het directe effect van leeftijd op de kans op slachtofferschap is nu -0,028. Het indirecte effect van leeftijd via kennis kan berekend worden door de volgende berekening: totale effect-directe effect. In dit geval is het indirecte effect -0,030-0,028=-0,002. Beide hellingen van

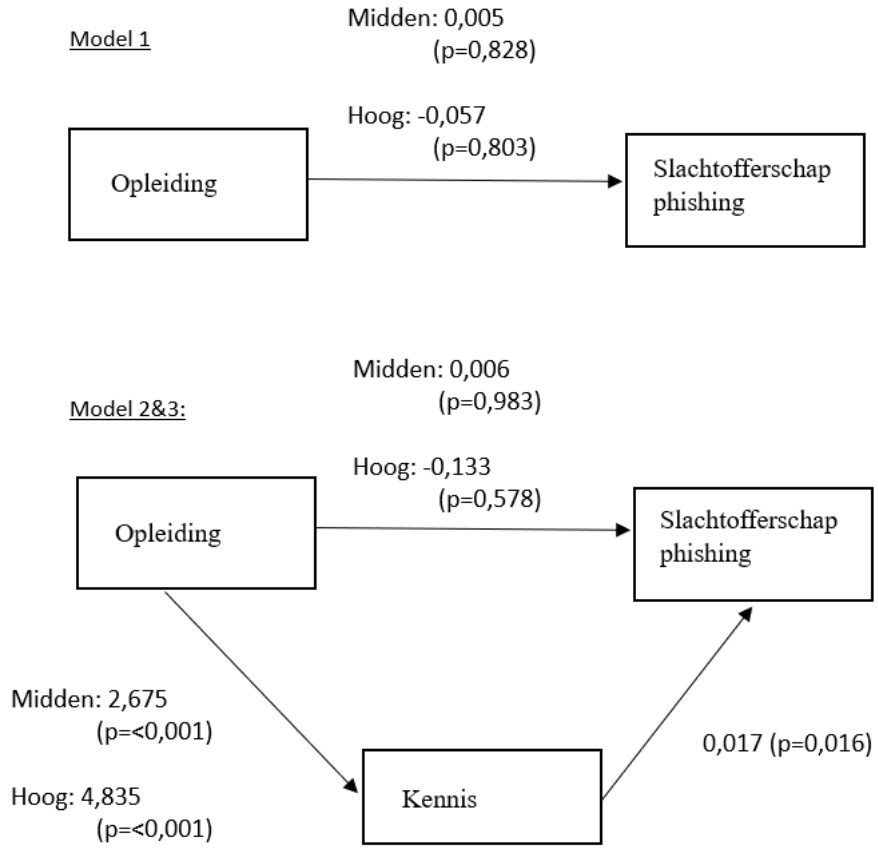
leeftijd, in model 1 en 3, zijn significant. De afname van het effect van leeftijd, het verschil tussen het effect van leeftijd op de kans op slachtofferschap in model 1 en 2&3, is zeer klein en waarschijnlijk niet significant. Daarnaast blijkt dat de relatie tussen kennis en de kans op slachtofferschap niet significant is (r=0.017, p=0,227). Er kan geconcludeerd worden dat er geen mediatie gevonden is.

Figuur 6: Resultaten mediatie, leeftijd als onafhankelijke variabele



In figuur 7 staan de resultaten van de mediatie weergeven, met opleiding als onafhankelijke variabele. Ook hier kan geconcludeerd worden dat er geen mediatie gevonden is omdat kennis geen invloed heeft op de kans op slachtofferschap van phishing, deze resultaten niet significant zijn (r=0.017, p=0,016). De enige significante resultaten in het conceptuele model is de invloed van opleidingsniveau op kennis over online veiligheid. Wanneer het opleidingsniveau stijgt, stijgt de kennis over online veiligheid. De helling van een respondent met een hoog opleidingsniveau is bijvoorbeeld 4,835 (p<0,001), wat betekent dat iemand met een hoog opleidingsniveau 4,835 punten hoger scoort op de kennis over online veiligheid dan een respondent met een laag opleidingsniveau.

Figuur 7: Resultaten mediatie, opleiding als onafhankelijke variabele



Modelinspectie

In tabel 3 staan de Hosmer-Lemeshow test en -2 Log Likelihood weergegeven. Daarnaast is de VIF-score onderzocht. Deze drie maten zijn belangrijk in het beoordelen van de modellen. De modellen zijn onderling moeilijk te vergelijken omdat twee verschillende vormen van een regressie analyse zijn gebruikt. In het komende stuk wordt de fitheid van de modellen besproken. Met fitheid wordt verwijst naar hoe goed het model de waargenomen data beschrijft.

Ten eerste zijn de VIF-scores relevant voor de lineaire regressie analyse. De VIF-scores komen uit model 2 omdat dit het enige model is die aan de hand van lineaire regressie, kennis over online veiligheid probeert te verklaren. Uit de resultaten blijkt dat er geen sprake is van multicollineariteit. Er zijn geen score gevonden van een 4 of hoger, alle scores liggen rond de 1.

De Hosmer-Lemeshow test word gebruikt om de fitheid van een logistisch regressiemodel te beoordelen. Voor model 1 is X^2=9,082 (p=0,335) en in model 3 is X^2=9,850

(p=0,276). Uit deze uitkomsten blijkt dat voor beide modellen de nulhypothese niet wordt verworpen. De nulhypothese van de Hosmer-Lemeshow test is dat er geen significant verschil bestaat tussen de modellen. Beide modellen passen goed bij de data, aangezien de p-waarden van beide modellen groter zijn dan 0,05, wat aangeeft dat er geen significant verschil is tussen de waargenomen en verwachte uitkomsten. Met andere woorden, er is geen bewijs dat de modellen slecht passen bij de data. De chi-kwadraat waarden zijn vergelijkbaar en dit betekent dat er weinig verschil is in de fit tussen de twee modellen. Door de toevoeging van de mediator kennis over online veiligheid in model 3 veranderen de waarden van de Hosmer-Lemeshow test resultaten niet, wat inhoudt dat kennis over online veiligheid niet meer toevoegt aan het model. Dit was ook verwacht omdat er geen significante gedeelte mediatie is gevonden.

Als laatste is de -2 Log Likelihood belangrijk in de vergelijking van de twee logistische modellen. Deze maat bepaalt hoeveel onverklaarde informatie er is. Een hogere waarde van de Log Likelihood betekent een slechte fit. In tabel 3 zijn de waardes weergegeven. Model 1 heeft een waarde van 1167,449 en model 3 heeft een waarde van 1166,237. Dit betekent dat model 3 een betere fit is dan model 2 omdat de waarde van de -2 Log Likelihood wat lager ligt. Dit heeft te maken met de toevoeging van de variabele kennis die een deel van de kans op slachtofferschap verklaard.

Conclusie en discussie

De hoofdvraag die centraal staat in dit onderzoek is: “In hoeverre wordt individueel slachtofferschap van phishing verklaard door leeftijd en opleiding en wordt deze relatie gemedieerd door kennis over online veiligheid?” Dit onderzoek probeert aan de hand van persoonskenmerken het slachtofferschap van phishing te verklaren. Daarnaast wordt de rol van kennis over online veiligheid onderzocht als mediator in het onderzoek.

Als eerste is er onderzocht wat de invloed van leeftijd is. Uit de literatuur blijkt dat met name ouderen kwetsbaarder zijn om slachtoffer te worden van phishing omdat zij een aantrekkelijk doelwit zijn (Luginbuh & Smid, 2021; Schaie, 1994; Reed et al., 2014). Hieruit is de eerste hypothese opgesteld: “Naarmate mensen ouder worden, neemt het risico op het slachtofferschap van phishing toe”. Deze hypothese is vervolgens getoetst hieruit blijkt dat de kans op slachtofferschap van phishing voor oudere mensen iets kleiner is dan de kans op slachtofferschap voor jongeren. Dit is opvallend omdat uit de literatuur het tegenovergestelde blijkt. Een verklaring hiervoor kan zijn dat jongeren zijn opgegroeid met het internet. Doordat zij van jongs af aan gebruik maken van internet raken zij overmoedig. Zij denken dat zij veel weten over het internet en de risico’s omdat zij hiermee opgegroeid zijn maar hierdoor kunnen jongeren naïef worden. Het feit dat jongeren vaker gebruik maken van het internet zou een tweede verklaring kunnen zijn (Büchi, Just & Latzer, 2016). Zij worden vaker blootgesteld aan de risico’s van het internet en komen dus ook vaker in aanraking met phishing mails. Om te controleren of internetfrequentie een rol speelt bij de kans op slachtofferschap van phishing is het van belang om deze variabele in vervolg onderzoek mee te nemen. Echter, was het in dit onderzoek niet mogelijk omdat het aantal internetgebruik niet gemeten is in de vragenlijst die gebruikt is.

Een andere verklaring voor de afwijkende resultaten kan gevonden worden in de verdeling van leeftijd. Uit de resultaten blijkt dat de verdeling scheef is, wat ook zichtbaar is aan het gemiddelde. De gemiddelde leeftijd is 63 jaar, wat niet representatief is voor de gehele samenleving. Het grootste deel van de respondenten is tussen de 60 en 80 jaar. Hier is het selectie effect opgetreden. Respondenten hebben zelf de keuze gehad om deel te nemen aan het onderzoek wat er voor heeft gezorgd dat de jongere mensen niet hebben gereageerd.

Daarnaast blijkt uit de theorie dat opleiding een belangrijke voorspeller kan zijn in de kans op slachtofferschap van phishing. Het is van belang om kritisch naar een verdacht

bericht te kijken om te kunnen beoordelen of deze legitiem is of niet. Mensen met een hogere opleiding zijn beter in kritisch denken dan mensen met een lagere opleiding (Butler, 2012). Mensen met een hogere opleiding hebben vaardigheden en kennis opgedaan waardoor zij een hoge mate van kritisch denken ontwikkelen wat hen helpt kritischer naar de wereld te kijken (Halpern, 2014). Aan de hand van deze theorie is de tweede hypothese opgesteld: "Hoe hoger de opleiding, hoe kleiner de kans op slachtofferschap van phishing wordt.". De gevonden resultaten zijn niet significant. Een verklaring hiervoor kan gevonden worden in de verdeling van de variabele opleiding. Deze verdeling uit de gebruikte database is namelijk scheef en niet representatief voor de samenleving. Ruim 51% van de respondenten is hoogopgeleid, terwijl in de samenleving het percentage hoogopgeleiden rond de 35% ligt (Centraal Bureau voor de Statistiek, 2022). Deze verdeling is geen goede afspiegeling van de maatschappij en zorgt in dit onderzoek voor een steekproefbias.

Uit de theorie blijkt dat de grammatica en lay-out van een e-mail belangrijk waarschuwingstekens zijn om een verdacht bericht te kunnen beoordelen (Batuvicius et al., 2022). Onregelmatigheden in het taalgebruik en de grammatica of een afwijkende lay-out zijn belangrijke aanwijzingen dat een e-mail niet legitiem is. Door de opkomst van artificiële intelligentie (AI) kunnen criminelen steeds betere nep berichten maken. AI kan teksten schrijven die niet meer te onderscheiden zijn van de echte berichten. ChatGPT begrijpt zo'n 20 talen waardoor internetcriminelen grammaticaal correcte e-mails kunnen maken in een paar seconden (Microsoft, 2023). Dit maakt het detecteren van deze berichten bijna onmogelijk voor zowel spamfilters als voor de ontvanger. Hart van Nederland (2023) heeft een onderzoek uitgevoerd onder ruim 3300 panelleden, representatief voor de Nederlandse bevolking, waar een gegenereerd AI nep bericht onder hen werd verzonden. 91% van deze leden dacht dat het bericht geschreven is door een mens en niet door de computer (Hart van Nederland, 2023). Doordat het lijkt alsof het bericht door een mens is geschreven, er geen grammatica of lay-out vormen meer te vinden zijn, is het bijna onmogelijk om via deze weg te bepalen of een bericht legitiem is of niet. Een hoge of lage opleiding en het kritisch kunnen beoordelen van een e-mail zijn niet meer van belang om een phishing bericht te kunnen opmerken.

In het literatuur hoofdstuk zijn er twee hypotheses opgesteld waarin verwacht wordt dat kennis een mediërende factor heeft op de kans op slachtofferschap. Er wordt gesteld dat

iemand met een hogere opleiding, of leeftijd, meer kennis heeft over online veiligheid waardoor zij zich online veiliger gedragen wat leidt tot een verlaagde kans op het slachtofferschap van phishing. Echter, zijn er geen significante resultaten voor gevonden dus worden de laatste twee hypotheses niet ondersteund. Hypothese drie luidt; "Het verband tussen leeftijd en de kans op slachtofferschap van phishing wordt gedeeltelijk gemedieerd door de kennis over online veiligheid" Er zijn geen significante resultaten gevonden die deze hypothese ondersteunen. De relatie tussen leeftijd en kans op slachtofferschap wordt niet verklaard door de verschillen in kennis over online veiligheid. Dit is met name interessant voor vervolgonderzoek. Wellicht zijn andere theorieën, zoals frequentie van internet gebruik of de naïviteit van jongeren, een belangrijkere reden waarom jongere mensen vaker slachtoffer worden dan oudere mensen.

De laatste hypothese veronderstelt een mediatie van kennis op de relatie tussen opleidingsniveau en de kans op slachtofferschap; "Het verband tussen opleidingsniveau en de kans op slachtofferschap van phishing wordt gedeeltelijk gemedieerd door kennis over online veiligheid". Er zijn geen significante resultaten gevonden die deze hypothese ondersteunen. Een verklaring hiervoor is erg simpel, er bestaat geen hoofdeffect tussen opleidingsniveau en de kans op slachtofferschap van phishing dus zal er ook geen mediatie effect kunnen optreden. De reden voor het ontbreken van een hoofdeffect is eerder dit hoofdstuk benoemd.

Het is van belang om te noemen dat de panelleden uit het gebruikte onderzoek op de hoogte waren van het onderwerp van dit onderzoek. Deze leden kregen een vragenlijst toegestuurd over online veiligheid. In deze vragenlijst kregen deelnemers (e-mail) berichten voor zich met de vraag of deze legitiem is of niet en wat hun actie zou zijn na het lezen van dit bericht. Doordat zij zich bewust waren van het thema van de vragenlijst en de antwoordmogelijkheden waren zij op hun hoede. Waarschijnlijk hebben zij het bericht extra goed gelezen, of zijn ze achterdochtiger geweest met het beantwoorden van de vragen. Het is niet een goede afspiegeling van hoe zij in de werkelijkheid zouden reageren. Wanneer een

respondent vluchtig de e-mail opent tijdens een pauze op het werk, en niet op hun hoede is voor phishing, kan er een andere beslissing gemaakt worden. Er is hier sprake van een reactieve responsbias. Dit treedt op wanneer deelnemers bewust zijn vanwege het feit dat zij weten dat zij deel uitmaken van een onderzoek en hierdoor hun reactie gaan aanpassen. Om daadwerkelijk te testen of de leden een phishing mail zouden herkennen, kan er een bijvoorbeeld een nep mail verstuurd kunnen worden naar de panelleden zonder dat zij weten dat zij deel uit maken van een onderzoek. Het is echter de vraag of een onderzoek met deze vorm ethisch verantwoord is.

Aanbevelingen

Op basis van de bovenstaande conclusie en bevinden, zijn er enkele aanbevelingen te formuleren die kunnen bijdragen aan vervolgonderzoek en mogelijke interventies op het gebied van phishing preventie.

Ten eerste is het van belang om een nieuw onderzoek op te zetten waarin realistische scenario's gebruik worden die beter aansluiten bij de dagelijkse omstandigheden waarin men phishing mails ontvangen. In het huidige onderzoek waren de respondenten zich bewust van het onderwerp van het onderzoek waardoor zij mogelijk hun antwoorden hebben aangepast. Het is waarschijnlijk dat de respondenten extra voorzichtigheid hebben getoond, waardoor zij meer aandacht hebben besteed aan de verdachte mails dan ze normaal gesproken zouden doen. Daarnaast kan het dan interessant zijn om maximale tijd in te stellen waarin de respondenten de vraag moeten beantwoorden. In dit onderzoek hebben zij uitgebreid de tijd gehad om het bericht te analyseren, wat niet overeenkomt met hun dagelijkse routine en hoe mensen omgaan met het lezen van e-mails. Hierdoor kan onderzocht worden hoe snel en effectief mensen phishing pogingen kunnen herkennen wanneer zij er niet op voorbereid zijn. Door de respondenten bloot te stellen aan meer realistischere omstandigheden komen de resultaten beter overeen met het daadwerkelijke gedrag.

Een opvallend resultaat van dit onderzoek is dat jongeren een grotere kans hebben op het worden van een slachtoffer van phishing dan ouderen. Het is dan van belang om bewustwordingscampagnes voor jongeren extra aandacht te geven. In 2020 is een landelijke campagne gelanceerd door de politie na aanleiding van de coronacrisis, omdat jongeren noodgedwongen vaker thuis waren en meer online waren. De campagne "Gamechangers" daagde de jongeren, aan de hand van speciale games, uit om cybercrime zoals bijvoorbeeld

phishing te herkennen (Huijsman, 2020). Het is onbekend wat de resultaten van deze campagne zijn. Op internet zijn veel meer campagnes en training te vinden over online veiligheid en de gevaren van phishing voor ouderen. Dit roep de vraag op wat het effect van deze campagnes zijn. Waaraan ligt het dat de ouderen een minder grote kans hebben op het slachtoffer worden van phishing, zijn zij over het algemeen behoedzamer op het internet of slaan de campagnes over online veiligheid aan op deze groep? Een aanbeveling vanuit dit onderzoek is om duidelijk in beeld te krijgen waarom jongeren een grotere kans hebben om slachtoffer te worden van phishing. Werken de online campagnes en sluiten deze goed bij jongeren aan en wanneer dit niet het geval is, is het van belang om te onderzoeken hoe deze groep beter bereikt kan worden om ook hen behoedzamer te laten zijn op het internet.

Als laatste is het interessant om te onderzoeken welke invloed de frequentie van internetgebruik op de kans op slachtofferschap van phishing heeft. Dit kan bijdragen aan het helpen identificeren van specifieke risicofactoren en het ontwikkelen van gerichte preventiestrategieën.

Het is van belang om beter te begrijpen wie en wanneer de meeste kans hebben op het worden van een slachtoffer van phishing omdat dit een groeiende en nog steeds opkomende criminaliteit is. Er wordt verwacht dat de criminaliteit de komende jaren alleen maar meer online gaan plaats vinden (Radar, 2023), dus is het belangrijk om een volledig beeld te creëren over de grootste risicofactoren zodat hier gericht interventies op ingezet kunnen worden.

Literatuurlijst

Akkermans, M., Arends, J., Derksen, E., & Reep, C. (2023, 10 mei). *Online Veiligheid en Criminaliteit 2022*. Centraal Bureau voor de Statistiek. Geraadpleegd op 10 juli 2023, van https://www.cbs.nl/nl-nl/longread/rapportages/2023/online-veiligheid-en-criminaliteit-2022?onepage=true

Büchi, M., Just, N., & Latzer, M. (2016). Modeling the second-level Digital Divide: a five-country study of social differences in internet use. *New Media & Society*, *18*(11), 2703–2722. https://doi.org/10.1177/1461444815604154

Butavicius, M., Taib, R., & Han, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, *123*, 102937. https://doi.org/10.1016/j.cose.2022.102937

Butler, H. A. (2012). Halpern Critical Thinking Assessment Predicts Real-World Outcomes of Critical Thinking. *Applied Cognitive Psychology*, *26*(5), 721–729. https://doi.org/10.1002/acp.2851

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human Factors*, *58*(8), 1158–1172. https://doi.org/10.1177/0018720816665025

Centraal Bureau voor de Statistiek. (2020, november 18). *Internet; toegang, gebruik en faciliteiten; 2012-2019*. https://www.cbs.nl/nl-nl/cijfers/detail/83429NED?dl=27A20

Centraal Bureau voor de Statistiek. (2021, 15 oktober). *Internetgebruik van huishoudens en personen - ICT, kennis en economie 2021*. https://longreads.cbs.nl/ict-kennis-en-economie-2021/internetgebruik-van-huishoudens-en-personen/

Centraal Bureau voor de Statistiek. (2022, 28 februari). *2,5 miljoen Nederlanders in 2021 slachtoffer van online criminaliteit*. https://www.cbs.nl/nl-nl/nieuws/2022/09/2-5-miljoen-nederlanders-in-2021-slachtoffer-van-online-criminaliteit#:~:text=Ruim%20honderdduizend%20Nederlanders%20gedupeerd%20door%20phishing&text=Van%20alle%20Nederlanders%20van%2015,waarschijnlijk)%20van%20een%20oplichter%20was.

Centraal Bureau voor de Statistiek. (2022, 17 oktober). Meer hoogopgeleiden en beroepsniveau steeg mee. *Centraal Bureau voor de Statistiek*. https://www.cbs.nl/nl-nl/nieuws/2022/42/meer-hoogopgeleiden-en-beroepsniveau-steeg-mee

Chan, J., To, H., & Chan, E. (2006). Reconsidering social cohesion: Developing a definition and analytical framework for empirical research. *Social Indicators Research*, *75*(2), 273–302. https://doi.org/10.1007/s11205-005-2118-1

Choi, J., Kruis, N. E., & Choo, K. (2021). Explaining Fear of Identity Theft Victimization Using a Routine Activity Approach. *Journal Of Contemporary Criminal Justice*, *37*(3), 406–426. https://doi.org/10.1177/10439862211001627

Cohen, L. E. & Felson. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach American Sociological Review. *American Sociological Association*, *44*(4), 588–608.

de Vries, D. A., Piotrowski, J. T., & de Vreese, C. H. (2022). Resultaten Onderzoek Digitale Competenties (DIGCOM). In *Amsterdam School of Communication Research*.

Geraadpleegd op 26 juni 2023, van https://open.overheid.nl/documenten/ronl-f74f961d2b2b84299de53ce711d44de476ab441c/pdf#:~:text=DIGCOM%20is%20een%20tweejarig%20onderzoeksproject,van%20Nederlanders%20onderzoeken%20en%20verbeteren.

Eshuis, N. (2023, 8 maart). *Vrouwen hebben wereldwijd minder vaak toegang tot internet*. De Volkskrant. Geraadpleegd op 21 juni 2023, van https://www.volkskrant.nl/nieuws-achtergrond/vrouwen-hebben-wereldwijd-minder-vaak-toegang-tot-internet~bd99bb6e/

Feng, J., MA, Zou, L., Ye, O., & Han, J. (2020). Web2Vec: Phishing Webpage Detection Method Based on Multidimensional Features Driven by Deep Learning. *IEEE Access* (8), 221214–221224. https://doi.org/10.1109/access.2020.3043188

Felson, M., & Clarke, R. V. (1998). *Opportunity Makes the Thief: Practical Theory for Crime Prevention*. Home Office.

Ferguson, L. C., Elliott, M., & Kim, S. G. (2022). Examining the Connection Between Missing Persons and Victimization: An Application of Lifestyle Exposure Theory. *Sage Journals*, *69*(3), 656–681. https://doi.org/10.1177/00111287221109768

Gavett, B. E., Zhao, R., John, S. E., Bussell, C., Roberts, J., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLOS ONE*, *12*(2), e0171620. https://doi.org/10.1371/journal.pone.0171620

Greitzer, F. L., Li, W., Laskey, K. B., Lee, J. S. H., & Purl, J. (2021). Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility. *ACM transactions on social computing*, *4*(2), 1–48. https://doi.org/10.1145/3461672

Halpern, D. F. (2014). *Thought and knowledge : an introduction to critical thinking* (5de editie). Psychology Press.

Hart van Nederland. (2023, 3 augustus). 91 procent herkent niet dat déze phishingbrief door AI is geschreven. *Hartvannederland*. https://www.hartvannederland.nl/tech/ai/91-procent-herkent-niet-dat-deze-phishingbrief-door-ai-is-geschreven

Huijsman, E. (2020, 23 juli). *Campagne moet jongeren afhouden van cybercriminaliteit*. Nederlandse Veiligheidsbranche. https://www.veiligheidsbranche.nl/kenniscentrum/campagne-moet-jongeren-afhouden-van-cybercriminaliteit/

Hutchings, A., & Hayes, H. D. (2009). Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'? *Current Issues in Criminal Justice*, *20*(3), 433–452. https://doi.org/10.1080/10345329.2009.12035821

Kim, H., Kwon, H., & Kim, K. H. (2018). Modified cyber kill chain model for multimedia service environments. *Multimedia Tools and Applications*, *78*(3), 3153–3170. https://doi.org/10.1007/s11042-018-5897-5

Kircanski K., Notthoff N., DeLiema M., Samanez-Larkin G. R., Shadel D., Mottola G.,

Gotlib, I. H. (2018). Emotional arousal may increase susceptibility to fraud in older and younger adults. *Psychology and Aging, 33*, 325–337.

Kutsch, S. (2021). *Knowledge Representation and Indicutive Reasoning Usuing Conditional Logic and Sets of Ranking Functions.* IOS Press.

Lee, C., & Coughlin, J. F. (2014). PERSPECTIVE: Older Adults' Adoption of Technology: An Integrated Approach to Identifying Determinants and Barriers. *Journal of Product Innovation Management*, *32*(5), 747–759. https://doi.org/10.1111/jpim.12176

Li, W., Lee, J. S. H., Purl, J., Greitzer, F. L., Yousefi, B., & Laskey, K. B. (2020). Experimental Investigation of Demographic Factors Related to Phishing Susceptibility. *Proceedings of the . . . Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2020.274

Luginbuhl, R., & Smid, B. (2021). De verscheidenheid van vermogens van Nederlandse huishoudens: update. In *Centraal Planbureau*.

Microsoft. (2023, 14 juli). *How AI is changing phishing scams*. Microsoft. Geraadpleegd op 4 december 2023, van https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/how-ai-changing-phishing-scams

Ministerie van Algemene Zaken. (2023, 5 april). *Wat kan ik doen tegen phishing?* Rijksoverheid.nl. https://www.rijksoverheid.nl/onderwerpen/cybercrime-en-cybersecurity/vraag-en-antwoord/phishing

Ministerie van Justitie en Veiligheid. (2022a, 7 februari). *Cybercrime*. Openbaar Ministerie. https://www.om.nl/onderwerpen/cybercrime

Ministerie van Justitie en Veiligheid. (2022b, 11 oktober). *Phishing tast het vertrouwen in de digitale wereld aan*. Nieuwsbericht | Openbaar Ministerie. https://www.om.nl/actueel/nieuws/2022/10/11/phishing-tast-het-vertrouwen-in-de-digitale-wereld-aan#:~:text=Hoe%20een%2024%2Djarige%20man,tegen%20de%2024%2Djarige%20verdachte.

Näsi, M., Danielsson, P., & Kaakinen, M. (2021). Cybercrime Victimisation and Polyvictimisation in Finland—Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*. https://doi.org/10.1007/s10610-021-09497-0

Planbureau Fryslân. (2021). Onderzoeksverantwoording. In *Planbureau Fryslân*. Geraadpleegd op 19 juli 2023, van https://www.planbureaufryslan.nl/wp-content/uploads/2022/06/FSP-2022-Panel-verantwoording-DEF.pdf

Planbureau Fryslân. (2023, maart 8). *Panel Fryslân - Planbureau Fryslân*. Geraadpleegd op 19 juli 2023, van https://www.planbureaufryslan.nl/panelfryslan/

Rabiner, D. J., O'Keeffe, J., & Brown, D. (2006). Financial Exploitation of Older Persons. *Journal of Aging & Social Policy*, *18*(2), 47–68. https://doi.org/10.1300/j031v18n02_04

Radar. (2023, 18 januari). *Criminelen stappen over naar het internet: cybercriminaliteit verdrievoudigd sinds 2019*. Radar - het consumentenprogramma van AVROTROS. https://radar.avrotros.nl/nieuws/item/criminelen-stappen-over-naar-het-internet-cybercriminaliteit-verdrievoudigd-sinds-2019/

Reed, A., Chan, L., & Mikels, J. A. (2014). Meta-analysis of the age-related positivity effect: Age differences in preferences for positive over negative information. *Psychology and Aging*, *29*(1), 1–15. https://doi.org/10.1037/a0035194

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal Of Offender Therapy And Comparative Criminology*, *60*(10), 1119–1139. Crossref. PubMed. ISI.

Reyns, B. W., & Randa, R. (2020). No honor among thieves: Personal and peer deviance as explanations of online identity fraud victimization. *Security Journal*, *33*, 228–243. Crossref.

Ruimschotel, D. (1988). Criminele gedragingen, overheid en samenleving; een drieluik. In *WRR eBooks*. WRR.

Sarno, D. M., Lewis, J. I., 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. https://doi.org/10.1177/0018720819855570

Schaie, K. W. (1994). The course of adult intellectual development. *American Psychologist*, *49*(4), 304–313. https://doi.org/10.1037/0003-066x.49.4.304

Steinberg, L. (2010). A dual systems model of adolescent risk-taking. *Developmental Psychobiology*. https://doi.org/10.1002/dev.20445

Veilig Bankieren. (2021, 23 februari). *Jongeren bankieren veel onveiliger dan ouderen | Veilig bankieren*. Geraadpleegd op 24 november 2023, van https://www.veiligbankieren.nl/actueel/jongeren-bankieren-onveiliger/

Venéco. (2022, 20 juli). *Voorkom het reële gevaar van phishing!* Geraadpleegd op 2 mei 2023, van https://www.veneco.nl/inspiratie-ontwikkelingen/voorkom-het-reele-gevaar-van-phishing#:~:text=Ruim%2090%25%20van%20alle%20succesvolle,cyberincident%20via%20phishing%20dus%20re%C3%ABel

Van Wilsem, J. (2013). "Bought it, but Never Got it" Assessing Risk Factors for Online Consumer Fraud Victimization. *European Sociological Review*, *29*(2), 168–178. https://doi.org/10.1093/esr/jcr053

De Witte, T., Marinus, J. D., & La Roi, C. (2023). Bewegen inwoners van Fryslân zich veilig online? In *Planbureau Fryslân*. Fries Sociaal Planbureau. Geraadpleegd op 2 mei 2023, van https://www.planbureaufryslan.nl/wp-content/uploads/2023/01/202301-Bewegen-Friezen-zich-veilig-online.pdf