2014

De online scholier: Hét slachtoffer van phishing?

Een onderzoek naar de relaties tussen internetgedrag en het slachtofferschap van phishing onder scholieren uit Nederland en Duitsland

Job Leemreize – S1112139
Bachelor Bestuurskunde
Faculteit Management & Bestuur
Universiteit Twente

Eerste begeleider: Prof. Dr. M. Junger
Tweede meelezer: Prof. Dr. P. Hartel

UNIVERSITEIT TWENTE.

7-1-2014

Voorwoord

In dit onderzoek wordt er aandacht besteed aan de relatie tussen internetgedrag van scholieren en het slachtofferschap van phishing. Mijn interesse voor dit onderwerp is gewekt na het volgen van de minor Crime Science & Risk Governance in het derde jaar van de opleiding bestuurskunde aan de Universiteit Twente. Cybercrime spreekt mij aan vanwege de plek waarop het zich afspeelt: Het internet.

Ik wil hierbij ook mijn dank uitspreken aan Prof. Dr. Marianne Junger voor haar kritische blik op het gehele onderzoek en haar goede begeleiding tijdens het gehele proces van dit bacheloronderzoek. Ook wil ik Prof. Dr. Pieter Hartel bedanken voor zijn taken als tweede meelezer. Daarnaast wil ik mijn dank uitspreken aan mijn medestudenten Sabine Tankink en Keith Davelaar voor de goede en leuke samenwerking ten aanzien van de dataverzameling en het gehele onderzoeksproces. Ook wil ik Sebastian Wachs van de Universiteit Bremen bedanken voor de mogelijkheid om aan te sluiten bij zijn datacollectie en de werkzaamheden voor het afronden van het meetinstrument. Daarnaast wil ik de medewerkers van het Bataafs Lyceum, Het Maranium College en SG de Waerdenborgh bedanken voor de medewerking bij het verzamelen van de data voor dit onderzoek. Verder wil ik mijn dank uitspreken aan alle andere studenten en docenten die mij hebben geadviseerd en hebben geholpen bij het neerzetten van deze bachelorscriptie.

Ondergetekende,

Job Leemreize

Samenvatting

Ter afronding van mijn bachelor Bestuurskunde te Universiteit Twente schrijf ik dit onderzoek.

In dit bacheloronderzoek zal er gekeken worden naar de relatie tussen het internetgedrag van middelbare scholieren en het slachtofferschap van phishing onder deze scholieren. Phishing is een techniek binnen de cybercrime waarbij wordt geprobeerd gevoelige informatie los te weken van een slachtoffer, door zich voor te doen als een betrouwbare derde partij (Jagatic, Johnson, Jakobsson, & Menczer, 2007). Vrijwel iedereen gebruikt tegenwoordig internet, hierdoor is het potentieel slachtofferschap van phishing groot.

Echter, gebruikt niet iedereen internet op dezelfde wijze, maar verschillen mensen van internetgedrag. Internetgedrag kan gezien worden als de manier waarop en waarvoor men het internet gebruikt. Door internetgedrag te koppelen aan slachtofferschap bij phishing ontstaat er een interessante onderzoeksvraag om te onderzoeken:

Wat is de relatie tussen het internetgedrag van middelbare scholieren en het slachtofferschap van phishing onder scholieren?

Deze verklarende vraag zal worden beantwoord aan de hand van een empirisch onderzoek, waarbij online vragenlijsten zullen worden afgenomen onder middelbare scholieren in zowel Duitsland als Nederland. Om een theoretisch kader vast te stellen en een achtergrond te geven over wat phishing precies inhoudt, wordt er gebruik gemaakt van de wetenschappelijke literatuur. Ook de bestaande algemene modellen vanuit de Crime Science, zoals de Routine Activities Theory, zullen terug te vinden zijn in mijn onderzoek.

Ook zullen in dit onderzoek de verwachtingen wat betreft de relaties tussen het internetgedrag van scholieren en het slachtofferschap bij phishing evenals andere algemene relaties rondom het slachtofferschap bij phishing getoetst worden door middel van statistische analyses in SPSS. Deze analyses worden gemaakt op basis van de data, die in de afgelopen maanden zijn verzameld.

De relevantie van deze studie is relatief groot, omdat er relatief weinig informatie over het slachtofferschap van phishing bekend is. Naast dat er gezocht zal worden naar de prevalentie van het slachtofferschap van phishing onder scholieren, wordt ook de relatie tussen het internetgedrag en slachtofferschap getest. Hiermee kan duidelijk worden welke invloed het internetgedrag van scholieren uitoefent op de kans dat zij slachtoffer worden van phishing. Aan de hand van de resultaten van dit onderzoek kunnen scholen, ouders en de overheid mogelijk betere preventiemiddelen inzetten tegen het slachtoffer worden van phishing. Des te meer duidelijkheid over het probleem, des te preciezer preventiemiddelen ingezet kunnen worden voor deze vorm van cybercrime te voorkomen.

Inhoudsopgave

Inleiding onderzoek

Rond 1995 kwam phishing op in de hackerswereld. Phishing, afkomstig van het woord ‘’Fishing’’, is een term gebruikt voor het ‘’vissen’’ naar informatie op het internet. Phishing is een frauduleuze cybercrimetechniek waarbij de ‘’Phisher’’, de uitvoerder van phishing, probeert gevoelige informatie te verkrijgen door zich op te stellen als een betrouwbare derde partij (Jagatic et al., 2007)**.** De vervanging van de ‘’f’’ door een ‘’ph’’ is een veelvoorkomende verandering die gemaakt wordt in de hackers scene, ooit geïntroduceerd bij het ‘’Phreaking’’, de originele beginvorm van het hacken . Hierbij werd het telefoonnetwerk gemanipuleerd door het uitzenden van specifieke radiofrequenties. (APWG, 2013a)

Nu steeds meer mensen het internet gebruiken zien meer cybercriminelen hun kans schoon om daar financieel gewin uit te behalen. Als gevolg hiervan groeit het aantal phishing aanvallen fors, al zijn de aantallen wel steeds fluctuerend (Jaishankar, 2008).

In een populatie van 57 miljoen Amerikanen zijn er 1,4 miljoen mensen slachtoffer geworden van identiteitsdiefstal, dit resulteert in een oplopende kostenpost voor banken en creditcardmaatschappijen van 1,2 miljard dollar in 2003 (Litan, 2004) .

Ook op het gaming platform is het resultaat van phishing zorgbarend (Barosso et al., 2008). In de gaming wereld is er steeds meer echt geld in omgang om bijvoorbeeld virtueel speeltegoed te kopen. Hierdoor wordt het voor phishers aantrekkelijker om zich ook in deze virtuele werelden te gaan manifesteren. Niet alleen gaming, maar ook andere vormen van internetgebruik zijn typerend voor het internetgebruik van scholieren, zoals het volop gebruiken van sociale netwerken (zoals Facebook en Hyves) en het steeds meer gebruiken van online bankieren op steeds jongere leeftijd. Daarnaast bezitten steeds meer scholieren een telefoon waarop gebankierd kan worden, iets wat omtrent phishing risicovol kan zijn. Deze vormen van internetgebruik hebben allen mogelijk een vergroot risico wat betreft het slachtoffer worden van phishing.

Door middel van dit onderzoek wil ik, na het geven van een indicatie van de prevalentie van phishing, onderzoeken in hoeverre verschillende aspecten van internetgedrag, samengevat onder de dimensie ‘’internetgedrag’’, samenhangen met slachtofferschap van phishing. Het doel is te weten te komen welke activiteiten op het internet ertoe leiden dat scholieren slachtoffer worden. Ook wordt er gekeken naar welke demografische factoren verband houden met het slachtofferschap van phishing.

Middels dit onderzoek wordt getracht beter inzicht te krijgen in het slachtofferschap bij phishing. Hierdoor kan effectiever gezocht worden naar preventiemiddelen tegen phishing voor zowel scholieren als de rest van de bevolking.

Probleemstelling en onderzoeksvragen

Het aantal internetgebruikers stijgt met de dag, zo had in 2012 94% van de mensen in Nederland een internetverbinding (Eurostat, 2012). Echter heeft het gebruik van internet ook zijn keerzijde, namelijk de aanwezigheid van cybercrime. Net als in de fysieke wereld is misdaad ook aanwezig in de digitale wereld. Omdat het niet reëel is om het internet niet te gebruiken, is het daarom van belang om oplossingen te zoeken voor deze problemen. Hiervoor is het belangrijk beter te begrijpen waarom sommige gebruikers slachtoffer worden van phishing en anderen niet. In dit onderzoek wordt onderzocht of internetgedrag de bepalende factor van dit probleem van slachtofferschap van phishing kan zijn.

De hoofdvraag van het onderzoek is:

Wat is de relatie tussen het internetgedrag en de demografische karakteristieken van middelbare scholieren en de kans op slachtofferschap van phishing?

Deze hoofdvraag wordt onderzocht aan de hand van de volgende deelvragen:

1. *In welke mate komt slachtofferschap van phishing bij scholieren voor?*
2. *In welke mate zijn scholieren betrokken bij de verschillende soorten van internetgebruik die relevant zijn voor phishing?*
3. *Welke factoren van internetgedrag hangen samen met slachtofferschap van phishing?*
4. *Welke demografische en socio-economische factoren hangen samen met het slachtofferschap van phishing onder scholieren?*

Korte beschrijving onderzoek

In dit kwantitatieve onderzoek met een cross-sectioneel research design zal er aan de hand van de data van een digitale vragenlijst (afgenomen onder scholieren op scholen in Nederland en Duitsland) een antwoord gegeven worden op de eerder opgestelde onderzoeksvragen. Hierbij wordt er eerst een theoretisch kader geschetst waarna de onderzoeksvragen aan de hand van de resultaten getoetst zullen worden.

Leeswijzer

Dit rapport is als volgt opgesteld: In het komende hoofdstuk zal eerst de definitie van phishing gegeven worden, waarna de verschillende soorten behandeld zullen worden. Hierna zal er door een literatuuronderzoek een blik geworpen worden op de huidige inzichten wat betreft het slachtofferschap van phishing. In het derde hoofdstuk zal het methodologische aspect van het onderzoek aan bod komen. Hierin worden achtereenvolgens de datacollectie, instrumenten en analyseprocedures uiteengezet. In hoofdstuk vier zullen de resultaten getoond worden op basis van de verzamelde data. Op basis van de resultaten die in dit hoofdstuk besproken worden, zullen in het laatste hoofdstuk conclusies getrokken worden wat betreft de belangrijkste bevindingen in relatie tot beantwoording van de eerder opgestelde onderzoeksvragen. Er zal afgesloten worden met een discussie en de beperkingen van dit onderzoek. Ook zal er een voorstel worden gedaan voor verdergaand onderzoek op basis van het huidige onderzoek.

Literatuuronderzoek

In deze paragraaf zal de definiëring van phishing behandeld worden alsmede de verschillende soorten phishing om hiermee een beter beeld te geven wat phishing precies is.

Definiëring van phishing

Er zijn, net als de meeste andere concepten, meerdere definities te vinden over wat phishing nou precies is. De definitie van Jagatic et al. luidt als volgt: ‘*’Phishing is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party*’’(Jagatic et al., 2007, p. 1). In deze definitie zijn drie kernelementen van phishing te vinden. Ten eerste *‘’a form of social engineering’’.* Social engineering is een concept dat wordt gebruikt in de computer security sector. Dit concept kan beschreven worden als ‘*’een niet technische manier van inbraak, die zwaar afhankelijk is op menselijke interactie, waarin vaak gemanipuleerd wordt om het normale beveiligingspatroon van mensen te doorbreken*’’. Dit element van de definitie van Jagatic et al. geeft dus aan dat er sprake is van (digitale) inbraak en manipulatie. Het tweede te onderscheiden element in de definitie van Jagatic et al. is ‘’sensitive information’’. Hierbij geeft hij aan dat het verkrijgen van gevoelige informatie eigenlijk het doel is van de phisher. Middels deze gevoelige informatie kan de phisher dan ook zijn financiele winst behalen. Het derde belangrijke element in de definitie van Jagatic et al. is ‘’Impersonating a trustworthy third party’’, hiermee wil hij duidelijk maken dat de phisher zich voor doet als een betrouwbare derde partij. Dit kunnen personen zijn, maar ook bedrijven of autoriteiten. Zo blijkt ook dat phishers zich vaak voordoen als een autoriteit, omdat zij via deze manier sneller de betrouwbaarheid wekken bij het slachtoffer (Charoen, 2011). Ook definitie van Jakobsson & Meyers en de definitie van de Australian Institute of Criminology bevat dezelfde drie kernelementen. Omdat meerdere definities dezelfde drie kernelementen bevatten, wordt er in dit onderzoek daarom gebruik gemaakt van de definitie van Jagatic et al. Deze definitie bevat de drie gestelde elementen het duidelijkst.

Een indicatie van de prevalentie en kosten van phishing

In deze paragraaf wordt een schets gegeven van het huidige probleem van slachtofferschap, om de ernst van het probleem te kunnen tonen.

Phishing wordt een steeds groter probleem, het aantal phishing aanvallen stijgt met de dag (Jaishankar, 2008). Phishing leidt in Nederland dan ook tot een steeds grotere slachtofferpost. In de eerste helft van 2011 werden in Nederland 2418 bankklanten het slachtoffer van fraude met internetbankieren tegenover 1383 klanten in 2010, waar dit aantal in 2009 nog 154 lager was. Een ander onderzoek toont aan dat phishing een zeer laag *slagingspercentage heeft (namelijk 0.000564) maar dat door de grote aantallen* aanvallen die worden uitgevoerd het opgetelde aantal slachtoffers significant is (Trusteer, 2009). De onderzoekers concluderen dat elk jaar circa 0,47% van alle klanten van een bank slachtoffer worden van phishing (Trusteer, 2009). De Anti-Phishing Work Group indiceert dat op zijn minst 5 procent van de gebruikers reageert op phishing scams, en dat er ongeveer 2 miljoen

mensen hun informatie weggegeven hebben aan gespoofde (nagebootste) websites. Daarbij is onder 1,47 miljoen volwassen internetgebruikers, aangetoond dat van alle internetgebruikers die zich herinneren ooit gevoelige informatie te hebben gegeven aan een phisher, hiervan 55% daadwerkelijk slachtoffer zijn geworden van identiteitsfraude (Litan, 2004).

De gemiddelde schade voor de slachtoffers in Nederland was wel lager in 2011 dan in 2010, waar in 2010 de gemiddelde schade voor het slachtoffer nog 7068 euro was, was dat in 2011 ongeveer 4632 euro. De totale schade is echter toegenomen, van 9,8 miljoen in 2010 naar al 11,2 miljoen in slechts de eerste helft van 2011 (Biesterbos, 2011)**.** In Amerika zou er, op basis van het jaar 2003, in totaal voor 1,2 miljard dollar aan schade zijn geleden door banken en creditcardmaatschappijen in dat jaar (Dhamija, Tygar, & Hearst, 2006; Litan, 2004).

In het resultatendeel van dit onderzoek zal een tabel met de slachtofferpercentages van huidige onderzoek worden gegeven om de prevalentie van phishing daarmee aan te tonen.

Vormen van phishing & modus operandi

Uit paragraaf ‘’Definiëring van phishing’’ kan er geconcludeerd worden dat er bij phishing drie kernelementen spelen: Manipulatie, gevoelige informatie en het kweken van betrouwbaarheid. Echter zijn de manieren waarop dit gedaan wordt, de manieren waarop gephisht wordt, niet altijd hetzelfde. Binnen deze cybercrime zijn verschillende vormen van phishing te onderscheiden met allen een verschillende modus operandi. Het is belangrijk deze vormen van phishing te onderscheiden om een beter zicht te krijgen op wanneer men nou wel of geen slachtoffer is van phishing. Zo is het nodig om te onderscheiden welke vormen van phishing er zijn om te kunnen onderzoeken welke vormen van internetgedrag samenhangen met het slachtofferschap van de verschillende soorten phishing.

Spear Phishing

Bij deze vorm van phishing is er sprake van een specifiek doelwit en niet van een grote groep doelwitten (Rajalingam, Alomari, & Sumari, 2012). Waar andere vormen van phishing vaak één dezelfde e-mail naar een grote groep mensen sturen, wordt er bij deze vorm van phishing met één persoon per keer gewerkt en krijgt elke persoon een unieke en op maat gemaakte phishing mail (Ledford, 2012). Vaak worden specifieke organisaties doelwit van spear phishing, om op deze manier toegang te krijgen tot bepaalde vertrouwelijke informatie van de organisatie. Beveiligingsspecialisten zeggen dan ook dat deze vorm van phishing veel moeilijker te detecteren is. Ze zijn lastiger te detecteren omdat het vaak lijkt alsof dit soort berichten via een legitiem lijkende wijze verstuurd zijn, waarbij de mails direct naar een doelwit wordt gestuurd waarvan de phishers weten dat hij of zij een relatie heeft met de organisatie als wie de phisher zich voordoet (Brody, Mulig, & Kimball, 2007).

Whaling

Deze vorm van phishing sluit deels aan op het ‘’spear-phishing’’ wat hiervoor besproken is. Ook bij deze vorm van phishing wordt er eerder per persoon gewerkt, dan in grote groepen mensen. Hét kenmerkende voor whaling is echter dat ze phishers hier slechts de ‘’Big Fish’’ van de organisatie als doelwit voor ogen hebben. Deze vorm van phishing is dan ook de meest op bedrijven gefocuste vorm van phishing waarbij aanvallen worden gedaan op de

hoge managers binnen een enkel bedrijf, of op de topmensen, zoals de CFO's of CEO's (Chief Financial Officers & Chief Executive Officers) (Ollmann, 2007)**.** Het doel van deze aanvallen is, net als bij spear phishing, het verkrijgen van ongeautoriseerde toegang tot vertrouwelijke informatie. Toegang verschaffen tot de vertrouwelijke informatie wordt bij voorkeur gedaan door middel van het installeren van zogenaamde malicious software, ook wel ''Malware'' genoemd, op de computers van de topmensen. Malicious software is software waarvan de intentie is om kwaad te doen, of waarvan de effecten kwaadaardig zijn (Aycock, 2009). Malware kan gedefinieerd worden als ''A piece of software developed either for the purpose of harming a computing device or for deriving benets from it to the detriment of its user'' (Jakobsson & Myers, 2007, p. 105).

Clone Phishing

Bij deze vorm van phishing wordt een bestaande, door de slachtoffer eerder ontvangen, e-mail gekloond door de phisher. Hij doet dit door de e-mailadressen en namen van slachtoffers te verkrijgen, waarna hij in de gekloonde mail de originele links vervangt met gephishte kwaadaardige links. Op deze manier lijkt het slachtoffer dus nogmaals de originele mail te ontvangen van de phisher, maar zijn de de links in de e-mail vervangen door de phisher. Vaak wordt er bij deze manier van phishing ook gebruik gemaakt van het zogenaamde ''Adress Spoofing''. Door adress spoofing kan de phisher het laten lijken dat de e-mail ook daadwerkelijk verstuurd is door de instantie, in plaats van de phisher zelf (Shi & Saleem, 2012).

Een andere techniek die hier vaak gebruik wordt is ''IP Spoofing'', waarbij de het ip-adres van waar de e-mail verzonden is vervalst wordt en daarmee dus ook de locatie en afkomst van het bericht zo vervalst kan worden dat het lijkt alsof hij vanaf de juiste plek afkomstig is. Daarnaast voorkomt de phisher zo dat hij ontmaskert waar hij zit (Duan, Yuan, & Chandrashekar, 2006)**.** Over het ''spoofen'' wordt in de volgende paragraaf verder uiteengezet.

Spoofing

Spoofing kan worden gezien als een situatie waarbij een persoon zich, door data te vervalsen, succesvol weet voor te doen als een ander en zich daarmee een onrechtmatig voordeel doet (Rhee, 2013). Dit is een phishing techniek waarbij veelal gebruik wordt gemaakt van nagemaakte e-mailadressen, ip-adressen of zelfs hele websites. De vier meest voorkomende technieken binnen spoofing zijn: Website Spoofing, URL-spoofing, E-mail Spoofing en Internet Protocol Spoofing, ook wel IP-Spoofing genoemd.

Website Spoofing

Bij website spoofing wordt een hele bestaande website nagemaakt, met als doel informatie te vergaren van de internetgebruiker die per ongeluk op een dergelijke site komt. Deze websites worden ook wel ''Hoax Websites'' genoemd. Mensen komen vaak per ongeluk op deze websites, omdat er vaak gebruik gemaakt wordt van URL-Spoofing.

URL- Spoofing

Deze vorm van spoofing wordt vaak gebruik in combinatie met andere vormen van spoofing om bijvoorbeeld de URL's in een nagemaakte e-mail te vervangen waarbij een vervalste

URL zich laat lijken als de echte legitieme URL van een website. Zo kan bijvoorbeeld een website zoals GamingInsider.co.uk (GAMINGINSIDER.CO.UK) veranderd zijn in GamingInsider.co.uk, (GAMINGLNSIDER.CO.UK), waar de hoofdletter ‘’I’’ veranderd wordt in een kleine letter van ‘’L’’. Wanneer deze website in de zoekresultaten zou staan van Google, zou men er redelijkerwijs van kunnen uitgaan dat dit de echte website is waar ze naar op zoek zijn.

E-Mail Spoofing

Bij e-mail spoofing worden er e-mails, inclusief de volledige opmaak van de e-mail, nagemaakt om deze vervolgens de verspreiden onder willekeurige personen. Een bekend voorbeeld van e-mail spoofing zijn de nagemaakte e-mails van banken. Hierin wordt bijvoorbeeld medegedeeld dat er een beveiligingsupdate is uitgevoerd door de bank en dat om de update te voltooien ingelogd moet worden

Internet Protocol Spoofing

Internet Protocol Spoofing ook wel IP Spoofing genoemd, is een laatste vorm van spoofing. Bij IP Spoofing wordt het IP-adres van de spoofer gemaskerd of vervalst. Op deze manier lijkt het dus alsof een bepaald bericht afkomstig is van een vertrouwde computer of persoon (Tanase, 2003).

Ook wordt IP Spoofing vaak gebruikt bij de zogenaamde DDoS aanvallen (Distributed Denial of Service), hierbij wordt een grote hoeveelheid aanvragen gedaan op de server van een bepaalde website om deze onbereikbaar te maken. IP-Spoofing wordt hierbij gebruikt voor het versturen van de packetgegevens naar de servers, terwijl daar een valse IP achter zit (Abliz, 2011).

Tabnabbing

Tabnabbing is een van de meest recente vormen van phishing die in opkomst is. Deze vorm van phishing maakt geen gebruik van misleiding via mails, sms’jes of dergelijken. Het enige waarvan de phisher met deze techniek gebruik maakt, is een mogelijk groot aantal tabbladen dat openstaat in de browser van het slachtoffer. Deze phishing techniek maakt geen gebruik van deceptie via valse URL’s of andere content zoals nagemaakte websites, maar gebruikt de tekortkomingen van ons geheugen (Unlu & Bicakci, 2010). Hiermee bedoelen Unlu & Bicacki dat phishers gebruik maken van het feit dat mensen tijdens een internetsessie niet precies onthouden welke websites zij geopend hebben of open hebben staan in al hun tabbladen.

Een voorwaarde voor het kunnen uitvoeren van dit soort aanvallen door een phisher, is dat er zogenaamde ‘’JavaScripts’’ aanwezig zijn, die deze aanval kunnen uitvoeren. Bij dit soort aanvallen heeft het slachtoffer verschillende tabbladen in zijn browser geopend. Ons menselijk geheugen weet niet precies meer welke sites er in deze tabbladen open staan. Het kwaadaardige JavaScript checkt of er op een van de tabbladen een tijd geen activiteit is geweest. Wanneer het slachtoffer een bepaalde website in een tabblad een tijd niet actief is geweest veranderd het JavaScript de website, die in eerste instantie open stond in dat tabblad, naar echt lijkende website die veel bezocht wordt, zoals bijvoorbeeld Gmail.com. Ook het icoontje bovenin het tabblad, de zogenaamde ‘’Favicon’’, en de tabbladtitel worden veranderd door het JavaScript (Unlu & Bicakci, 2010). Op deze manier is dus, zonder dat de

gebruiker het weet, de hele oorspronkelijke site achter het tabblad vervalst tot een phishingwebsite. Wanneer de gebruiker weer op het tabblad klikt, ziet deze een dergelijk bericht als ‘’u bent te lang inactief geweest op uw Gmail, log alstublieft nogmaals in’’. Ons geheugen laat ons hierbij een in de steek, en geeft geen seintje dat we in het begin van de browsersessie helemaal geen Gmail bezocht hebben. Echter, is Gmail een veelbezochte website en staat hier dus bij veel mensen wel een tabblad van open. Hierdoor denken veel mensen dat het slechts hun uitgelogde Gmail account is. Ze loggen na de melding die verschijnt door het JavaScript weer ‘’opnieuw’’ in op hun Gmail, niet wetende dat dit een gephiste website is. Op het moment dat de inloggegevens ingevuld zijn, worden deze direct opgevangen op de server van de phisher. De phisher kan velvolgens doen met de gegevens wat hij wenst.

Specifiek onderzoek naar slachtofferschap

Vele onderzoeken zijn in het verleden al gedaan naar algemeen slachtofferschap van phishing**,** zoals het onderzoek van Sheng et al. en Jagatic et al.**,** Echter, dit onderzoek heeft een andere aanpak. Misdaad niet alleen persoonsgebonden maar ook situatiegebonden is, om die reden wordt slachtofferschap van phishing het huidige onderzoek per specifieke situatie gemeten. Er is daarom gekozen om aan de hand van drie specifieke situaties bij internetgebruik het slachtofferschap van phishing te onderzoeken.

De drie gekozen vormen van internetgebruik onder scholieren die in het huidige onderzoek centraal staan zijn: Online Gaming, het gebruik van Social Networking Sites en Online Bankieren. Deze drie vormen van internetgebruik vormen, samen met enkele algeme factoren van exposure, de representatie voor de afhankelijke variabele ‘’internetgedrag’’ in de onderzoeksvraag. Er wordt onderzocht hoe slachtofferschap van phising via deze specifieke vormen van internetgebruik verklaard kan worden.

In een eerder uitgevoerde studie is al eens de relatie tussen online lifestyle en het slachtoffer worden van computer crimes onderzocht. Er werd geprobeerd online lifestyle te meten aan de hand van drie variabelen: (a) Beroep- en vrijetijdsactiviteiten op het Internet (b) Risicovolle online vrijetijdsactiviteiten en (c) risicovolle online beroeps activiteiten. Er werd aangetoond dat de online lifestyle van een internetgebruiker een substantiële factor is in het verkleinen van slachtofferschap van computer-crimes (Choi, 2008).Daarnaast tonen de resultaten dat risicovolle vrijetijdsactiviteiten op het internet de grootste contributie geven aan het worden een slachtoffer van een computer misdaad (Choi, 2008). Het betrokken zijn bij online riskant gedrag en riskante activiteiten, zoals het downloaden van gratis games en muziek op onbekende websites, het openen van onbekende bijlagen in e-mails en het klikken op pop-up berichten, de kans op worden van een online slachtoffer significant vergroten(Choi, 2008). Op basis van deze resultaten is er gekozen om drie specifieke vrijetijdsactiviteiten te meten ten aanzien van internetgedrag.

In de volgende paragraven zal verklaard worden hoe scholieren op de drie getoetste platformen van internetgebruik (Social Networking Sites,Online Gaming, Online Bankieren) slachtoffer kunnen worden van phishing. Dit doen we eerst aan hand van de Routine Activities Theory van Cohen & Felson (1979) waarna slachtofferschap verklaard zal worden aan de hand van enkele algemene verklaringen.

De analyses in dit onderzoek zullen dan ook gedaan worden op de drie specifiek gekozen platformen van internetgebruik, namelijk: Social Networking Sites, Online Gaming en Online Bankieren. Zowel het internetgedrag van de scholieren als diverse demografische factoren zullen worden getoetst ten aanzien van slachtofferschap op de drie gekozen platformen van internetgebruik. De resultaten van deze analyses worden besproken in het resultatendeel.

De Routine Activities Theory

Voorwaarden voor het plaatsvinden van een misdrijf

Binnen de Routine Activities Theory (RAT) zijn 3 hoofd-elementen die met elkaar verbonden zijn. De RAT zegt daarbij dat voor elke misdaad die plaatsvindt, er sprake moet zijn van een ‘’likely offender’’ een ”suitable target’’ en ‘’the absence of a capable guardian’’ wil misdaad zich kunnen manifesteren. Slechts wanneer al deze drie elementen aanwezig zijn doet zich misdaad voor. In de initiële vorm van de Routine Activities Theory, waren slechts deze drie elementen aanwezig. John Eck ging echter dieper in op deze theorie. John Eck was van mening dat het complexer lag en kwam met zijn zogenaamde ‘’Crime Triangle’’ (Zie figuur)

Figuur 1: De crime triangle (Popcenter.org, 2013b)

Anders dan Cohen & Felson, vond Eck dat er naast de binnenste driehoek, die van de Routine Activities Theorie, er een tweede driehoek om het bestaande RAT moest zijn. In deze driehoek bevinden zich drie supervisors: de Guardians, die als een controlefactor op de targets/victims fungeren. De Handler, die de offender in de gaten houdt. En als derde de Manager, die overzicht houdt op de plaatsen waar mogelijk misdaden zouden kunnen gebeuren. Het aanwezig zijn van de drie elementen van de RAT veroorzaakt volgens Eck dan ook nog geen misdaad. Volgens Eck ontstaat er misdaad wanneer de misdadiger zijn ‘’handler’’ kan ontvluchten, een target vindt vrij van een guardian, op een goede plek die niet in de gaten wordt gehouden door een manager (Wortley & Mazerolle, 2008).

De Routine Activities Theory als verklaring van slachtofferschap per specifieke vorm van internetgedrag.

In deze paragraaf zal de Routine Activities Theory specifiek op slachtofferschap bij phishing toegepast worden. Zoals er eerder al beschreven werd, geeft de RAT drie elementen die de aanwezigheid van misdaad verklaren. We kijken in deze paragraaf hoe deze elementen zich doorvertalen naar slachtofferschap bij phishing binnen de drie specifieke vormen van internetgebruik namelijk: Gamen, het gebruik van social media en online bankieren.

Omdat de Routine Activities Theory initieel opgesteld is om misdaad te verklaren in de fysieke wereld, moet er in ogenschouw genomen worden dat phishing eigenlijk niet in de fysieke wereld, maar de digitale wereld plaats vindt. De Routine Activities Theory zal in dit onderzoek dan ook naar de digitale wereld geïnterpreteerd worden.

De aanwezigheid van een ‘’Likely offender” & de afwezigheid van Handlers

Aanwezigheid van likely offenders

Het eerste element van de Routine Activity Theory (RAT) is gebaseerd op een mogelijke overtreder, die de intentie heeft om een bepaalde misdaad te voltooien. Naarmate het aantal internetgebruikers toeneemd, groeit waarschijnlijk ook het aantal likely offenders (Hutchings & Hayes, 2009). Niet alleen het aantal internetgebruikers neemt toe, maar ook het aantal phishingaanvallen dat uitgevoerd wordt groeit en het aantal phishingactiviteit is gestegen (APWG, 2013a; Jaishankar, 2008). Hieruit is dus af te leiden dat ofwel een zelfde aantal likely offenders meer aanvallen uitvoeren, ofwel dat er een groter aantal likely offenders is die aanvallen uitvoeren. Het mogelijk stijgen van het aantal likely offenders heeft zijn invloed op het slachtofferschap bij phishing op alle drie de vormen van internetgebruik. Zowel in de gamingwereld als op social media als bij online bankieren zorgt een groter aantal phishingaanvallen mogelijk voor een groter slachtofferschap. Of het vergrote aantal phishingaanvallen een gelijke invloed heeft op elk van de drie speficieke vormen van internetgedrag moet nog blijken.

Afwezigheid van handlers

De afwezigheid van handlers is het element dat de crime triangle van Eck toevoegt aan het originele element ‘’Likely offenders’’ van de routine activities theory. Hierbij is het zo dat volgens Eck, de offender zijn misdaad niet kan doen wanneer er een handler aanwezig is die hem in de gaten houdt. Wanneer deze handler er niet is heeft de offender vrij spel en kan de offender dus toeslaan, mocht de kans zich voortdoen. De afwezigheid van handler bepaald dus of een offender een misdaad kan plegen, en kan dus verklaren waarom misdaad plaats kan vinden.

Maar, waar er in de fysieke wereld een handler aanwezig is om de offenders in bewang te houden, hebben offenders op het internet vrij spel. Ze kunnen in hun eentje vanaf hun computers de phishing aanvallen uitvoeren zonder dat iemand ze daar in bedwingt. Wat wel

gedaan kan worden zijn zogenaamde ‘’Takedowns’’. Wanneer een website gerapporteerd wordt als phishing kunnen er juridische acties genomen worden, om deze website ‘’Down’’ te halen, zodat deze geen slachtoffers meer kunnen maken (Hegt, 2008). Echter, worden hiermee niet de offenders zelf in bedwang gehouden maar de middelen waarmee de offender zijn misdaad pleegt.

Minimale pakkans

Het voordeel voor de phishers is dat zij anoniem zijn op het internet en er geen geografische beperkingen zijn. Omdat zij anoniem zijn op het internet kunnen ze moeilijk gepakt worden en is het makkelijk voor phishers om juridische aanklachten te ontwijken (AusCERT, 2005). Deze anoniemiteit op het internet en de lage kans om gepakt te worden, zorgt er mogelijk voordat het aantal likely offenders toeneemt.

Weinig efforts, Lage risico’s, hoge beloningen als verklaring voor slachtofferschap.

Een goed aansluitend inzicht, naast de Routine Activities theory, zijn de Twenty five techniques of situational prevention. De situationele misdaadpreventie oppert voor specifieke preventie in plaats van algemene preventie. Bij de situationele misdaadpreventie gaat het er om dat er binnen een specifieke vorm van misdaad preventietechnieken ingezet worden om enkel die specifieke vorm van misdaad te bestreden. Een set van elementen binnen de situationele misdaad preventie maakt duidelijk in welke vijf hoofdstromen situaties kunnen worden veranderd ten aanzien van misdaadpreventie:

- Increasing the effort the offender must make to carry out the crime.
- Increasing the risks the offender must face in completing the crime.
- Reducing the rewards or benefits the offender expects to obtain from the crime.
- Removing excuses that offenders may use to “rationalize” or justify their actions.
- Reducing or avoiding provocations that may tempt or incite offenders into criminal acts.

(Popcenter.org, 2013a)

Deze vijf principes bieden de hoofdstromen voor situationele misdaadpreventie. Een opmerking wat betreft punt 1 en 2: Des te hoger de moeite en risico is, des te lager de kans dat de misdadiger zijn slag zal slaan. Ook het verkleinen van de beloning van de misdaad kan een goede optie zijn om de aantrekkelijkheid van misdaad te verkleinen. Wanneer een bepaalde misdaad minder opbrengt, is het mogelijk dat de misdadiger besluit om af te stappen van deze misdaad, omdat deze niet genoeg beloning brengt voor de moeite, de tijd en het risico dat de misdadiger er in steekt. Naast de meer materiële zijde van preventie, bestaan er ook technieken voor preventie in meer psychologische zin. Door excuses voor misdaad weg te halen belet je de misdadiger om zijn misdaad te rechtvaardigen. Daarnaast is het belangrijk om mogelijke incentives die misdaad oproepen zoveel mogelijk te minimaliseren, zodat een misdadiger niet uitgelokt wordt om misdaad te begaan.

Weinig effort

Volgens de 25 techniques of situational prevention is een van de manieren waarom misdaad kan worden teruggedrongen de moeite die de misdadiger moet begaan te vergroten.

Wanneer we kijken naar phishing dan kan dit gedaan worden door middel van virusscanners, firewalls en andere software die internetgebruikers beschermen tegen phishing. Dit is bijvoorbeeld mogelijk door ‘’Gateway anti- virus scanning. Dit soort software zorgt voor een extra laag van bescherming die bijvoorbeeld phishing mails er uit filtert en blokkeert (Tally, Thomas, & Van Vleck, 2004) . Door de verschillende soorten beschermende software moet de phisher meer moeite doen, omdat hij eerst deze ‘’blokkades’’ moet omzeilen voor hij daadwerkelijk zijn phishingaanval kan laten slagen.

Dit inzicht biedt echter ook een verklaring voor waarom phishingaanvallen wel kunnen slagen. Zo zijn zogenaamde ‘’phishing-kits’’ online makkelijk te verkrijgen en vereisen deze slechts een laag niveau van expertise om deze te kunnen gebruiken (AIC, 2006). De moeite die de phisher moet doen om zijn instrumenten voor phishing te kunnen krijgen en gebruiken is dus laag. Omdat het zo weinig moeite kost om deze instrumenten te , lokt dit mogelijk ook nieuwkomers. Dit zou een verklaring zijn voor het slachtofferschap van phishing en het toenemende aantal phishingaanvallen.

De aanwezigheid van een “Suitable Target’’ & de afwezigheid van guardian

De aanwezigheid van een ‘’Suitable Target’’

De targets van phishing zijn niet altijd hetzelfde. Sommige gefocuste phishingtechnieken gebruiken slechts een kleine poel van targets, waar andere phishingtechnieken een zeer brede groep proberen te phishen. Ook zit er een verschil in het type mensen dat mogelijk een doelwit van phishing wordt. Zo zijn bij”whale phishing’’ het welvarende en machtige deel van de maatschappij mogelijke ‘’Suitable targets’’. Door het toenemende aantal mensen en organisaties dat gebruik maakt van het internet, is het aantal doelwitten vergroot voor de phisher. De kans dat hiertussen een ‘’Suitable Target’’ zit, is dus ook groter dan jaren geleden. Wanneer we kijken naar welke sectoren vooral het target worden van phishing, dan zijn het de financiële sector en de betalingssector waarop de phishers het gemunt hebben, gevolgd door de veiling-, de gaming- en de social networking sector (Charoen, 2011; Rajalingam et al., 2012). De drie specifieke vormen van internetgedrag bevinden zich dus allen in sectoren die vaak target worden van phishing.

In de gaming sector specifiek was er een 12% stijging in reports van phishing in online games (APWG, 2013b). Hierbij werden vooral inloggegevens gestolen en de voorwerpen die de spelers in het spel hadden verkregen werden verkocht op de zwarte markt voor echt geld. Daarnaast geven ze aan dat gamers niet alleen financieel schade lijden, maar ook de identiteiten van de gamers beschadiging op kunnen lopen als gevolg van identiteitsdiefstal na phishing (APWG, 2013b). Identiteitsdiefstal na phishing komt namelijk vaak voor. In een onderzoek onder 1,78 miljoen volwassen internetgebruikers die zich herinneren ooit gevoelige informatie te hebben gegeven aan een phisher, gaf maar liefst 55% aan ook daadwerkelijk het slachtoffer geworden van identiteitsfraude (Litan, 2004).

In dit onderzoek zal phishing bij online gaming nader bekeken worden. Zo zal er ook gekeken worden of de mate waarin een scholier online games speelt invloed heeft op het slachtofferschap bij phishing. Hierover meer in het resultatendeel.

De afwezigheid van een ‘’Capable Guardian’’

Het derde element van de RAT, is de afwezigheid van de ‘’Capable Guardian’’. In het geval van phishing hoeft dit niet per se een persoon te zijn. Virusscanners en spamfilters zijn namelijk een veelvoorkomende bescherming tegen phishing. Omdat de phishing mails meestal direct naar een persoon gestuurd worden en er meestal geen andere mensen zicht op krijgen, is het eigenlijk de technologie die het werk moet doen. Een voorbeeld van zo een anti phishing tool is bijvoorbeeld WebRep van Avast!. Deze tools kunnen gemakkelijk als een plug-in bij de browser geïnstalleerd kan worden en daarmee betere bescherming tegen phishing sites bieden. Echter, het Security Intelligence Report van Microsoft toont aan dat nog steeds gemiddeld 24 procent van de computers onbeschermd is.Dit houdt in dat er dus geen beschermende software op de computer eïnstalleerd is (Microsoft, 2012).

Waar er wel winst valt te behalen is het vergroten van de security awareness van de internetgebruiker, dit kan bijvoorbeeld via Anti-Phishing educatie. Het onderzoek van Sheng et al. toont dan ook in een experiment aan, dat na verschillende methoden van anti-phishing educatie, er een reductie van 28% plaats vond in het aantal mensen dat viel voor phishing (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). In een ander onderzoek wordt aangegeven dat ‘’User security education and training’’ een van de belangrijkste aspecten is voor het beveiligingsbeleid van een organisatie (Dodge Jr, Carver, & Ferguson, 2007**)**. Het kernprincipe in de preventie tegen digitale misdaad, is volgens Grabosky & Smith dan ook: De benodigdheid van het creëren van awareness over de risico’s die mogelijke toekomstige slachtoffers lopen (Grabosky & Smith, 2001).

Ook zijn er diverse organisaties die awareness proberen te creëren rondom phishing en die bescherming proberen te bieden aan internetgebruikers tegen phishing. Zo is er bijvoorbeeld PhishTank, een samenwerkend coördinatiecentrum voor data en informatie tegen phishing op het internet. PhishTank geeft middels een ingewikkeld ‘’voting-systeem’’ internetgebruikers de kans om te stemmen of bepaalde websites ‘’Phishing’’ of ‘’Niet-Phishing’’ zijn, waarmee PhishTank probeert het aantal ‘’false-positives’’ te verminderen en de hoeveelheid data omtrent phishing te vergroten (Shi & Saleem, 2012). Ook is er de Anti-Phishing Working Group, opgericht in 2003. Deze groep is een internationaal consortium waar bedrijven die getroffen worden door phishing aanvallen bijeengebracht worden met beveiligingsbedrijven, beveiligingssoftware, wetshandhavinginstanties en andere overheidsorganisaties. Deze organisaties kunnen worden gezien als een ‘’Guardian’’ voor de plaats waar phishing gebeurd, het internet. Hoewel ze niet een directe weerstand kunnen bieden voor de internetgebruiker, zorgen ze wel voor het vergroten van de awareness rond phishing, zodat de internetgebruiker en de bedrijven die beïnvloedt worden door phishing zichzelf tegen phishing kunnen beschermen.

Plaats & het ontbreken van een manager

De derde dimensie van de Routine Activities Theory (RAT) in combinatie met de aanvulling van Eck, namelijk Place & Manager, is in de digitale wereld problematisch. In de inleiding van dit hoofdstuk werd al verteld dat de RAT initieel uitgaat van een fysieke wereld. Omdat het internetnet niet een geografisch gebonden ‘’plaats’’ is, maar het slechts een oneindige stroom van data is, is het ook lastig om deze te managen. Er is dan ook niet een ‘’manager’’ van het hele internet. Internetproviders zijn echter wel in staat deze rol te vervullen. Zij leveren namelijk het internet aan de internetgebruiker, en hebben ook de mogelijkheid om dit

te monitoren en/of mensen uit te sluiten van het internet. Internetproviders zouden dus mogelijk toezicht moeten houden op mogelijke phishing activiteiten binnen de digitale wereld waarin hun internetgebruikers zich bevinden. Het probleem hiervan is wel dat elke internetgebruiker het internet voor een verschillend doeleinde gebruikt en dat al deze digitale websites waarop de internetgebruikers zich bevinden zich onderling verschillen van elkaar. Het zou voor internetproviders of andere mogelijke toezichthouders op het internet handig zijn om te weten in welke ‘’gebieden’’ van het internet er veel phishing activiteit is om het zo beter tegen te kunnen gaan. In dit onderzoek zullen we dus ook toetsen welke gebieden of specifieke vormen van internetgebruik samenhangen met slachtofferschap.

Algemene verklaringen voor slachtofferschap van phishing

Naast dat de Routine Activities Theory een verkaring biedt voor het slachtoffer worden van phishing aan de hand van verschillende vormen van internetgebruik, bekijken we in dit onderzoek ook welke andere algemene verklaringen er kunnen zijn voor het slachtofferschap. In deze paragraaf zullen enkele algemene factoren die invloed hebben op het slachtoffer worden van phishing gepresenteerd alsmede enkele factoren die invloed hebben op de manier waarop iemand het internet gebruikt. Deze paragraaf biedt een theoretische onderbouwing voor de samenhang tussen demografische en socio-economische factoren en internetgedrag. Daarnaast worden aanvullende inzichten voor de te toetsen relaties tussen internetgedrag en slachtofferschap bij phishing getoond.

De transitie van offline naar online handelingen als verklaring

Verschuiving van offline handelingen naar digitale handelingen

Een algemeen inzicht voor een vergrote kans van slachtofferschap, is dat slachtofferschap bij phishing komt doordat steeds meer handelingen gedigitaliseerd zijn. Handelingen die eerder nog ‘’offline’’ werden gedaan, worden nu veelvuldig online gedaan. Er is dus veel meer informatie online beschikbaar gekomen door deze verschuiving. Omdat het bankieren en het kopen van spullen nu ook veelvuldig online gebeurd, neemt de hoeveelheid gevoelige informatie die online staat toe. Deze toename van gevoelige informatie leidt tot een groter aantal kansen voor de phisher om toe te slaan en dus meer slachtofferschap (Rajalingam et al., 2012).Wanneer men op het internet dus geen of minder gebruik maken van diensten waarbij betalingsgegevens van pas komen, zoals het online shoppen of online bankieren, is er dus ook geen of minder informatie bekend over hun bankgegevens en zijn deze mensen dus waarschijnlijk minder vaak slachtoffer van phishing. Mijn verwachting is dan ook dat de data van mijn onderzoek uit zal wijzen dat mensen die vaker online bankieren en/of online shoppen, vaker slachtoffer zijn (geweest) van phishing.

Of deze verwachting klopt zal worden besproken in het resultatendeel van dit onderzoek, waar zal worden getoetst of de frequentie van online bankieren en het gebruik van de mobiele telefoon voor mobiel bankieren factoren zijn die in relatie staan met slachtofferschap bij phishing en dan met name phishing bij online bankieren.

Het onderhouden van sociale contacten

Een inzicht wat betreft de te toetsen relatie, is dat het actief zijn op sociale netwerken de kans op slachtofferschap vergroot (Chhabra, Aggarwal, Benevenuto, & Kumaraguru, 2011; Jagatic et al., 2007). Deze relatie tussen het actief zijn op sociale netwerken en het slachtoffer worden van phishing is vooral te verklaren door het digitaal aanbieden van informatie (vaak ook gevoelige informatie) door de internetgebruiker. Waar we ‘’vroeger’’ gewoon onze gesprekken face to face hielden en de informatie dus ook onder de twee personen bleef, zijn er nu veel derde partijen die de informatie, die verschaft wordt in een online gesprek met een ander, kunnen gebruiken of misbruiken.

Op sociale netwerken plaatsen internetgebruikers al snel gevoelige informatie die bruikbaar is voor een phisher, zonder dat ze het door hebben. Daarbij is de aanwezigheid van deze informatie van belang voor de phisher, maar vooral hoe hij/zij deze informatie kan gebruiken om als een betrouwbare derde partij over te komen bij het slachtoffer. Zo kan de phisher door middel van de aanwezige informatie op Facebook zich voor gaan doen als een willekeurige Facebookgebruiker door de informatie die de Facebookgebruiker heeft verschaft op de sociale netwerk site te gebruiken. De phisher maakt vaak gebruik van de informatie op SNS’s (Social Networking Sites) om hiermee zich voor te kunnen doen als een vriend van een slachtoffer. De slachtoffers geven namelijk sneller hun gevoelige informatie aan deze ‘’vriend’’, dan een volkomen vreemde (Boyd & Ellison, 2008). Het blijkt zeer gemakkelijk en zeer effectief voor phishers om betrouwbaar over te komen bij slachtoffers wanneer gebruik wordt gemaakt van de aanwezige informatie op de social networking sites (Jagatic et al., 2007).

Het is nog niet bekend of de grootte van de vriendengroep die gebruikers op sociale netwerken hebben, uitmaakt voor het slachtofferschap op deze specifieke vorm van internetgedrag. Deze relatie zal onderzocht worden in dit onderzoek. Ook zal onderzocht worden of de mate van het gebruik van Social Networking Sites (SNS) en het aantal vrienden dat men op deze sites heeft invloed heeft op het slachtofferschap van phishing.

Geslacht & Leeftijd als verklaring

Het algemene inzicht is dat vrouwen vaker slachtoffer worden van phishing dan mannen (Sheng et al., 2010). Vrouwen klikken vaker op phishing links dan mannen en vullen ook vaker hun informatie in wanneer ze op een phishing site zitten.

Tevens komt naar voren dat mannen significant meer gebruik maken van het internet en hier ook significant langer achter zitten wanneer ze het gebruiken (Teo & Lim, 2000). Mannen zijn dan ook dominant op het internet, wat komt door de traditionele gedachte dat mannen technologischer ingesteld zijn dan vrouwen en mannen meer vertrouwen hebben in computers, met als gevolgd dat mannen vaker van het internet gebruik maken (Krendl, Broihier, & Fleetwood, 1989). Waarschijnlijk zijn mannen minder vaak slachtoffer dan vrouwen, omdat hier de tussenliggende factor van technical knowledge speelt, waarbij mannen vaak een hogere technical knowledge hebben en daarmee minder vaak slachtoffer zijn (Sheng et al., 2010).

Een inzicht wat betreft leeftijd is dat jongere mensen vaker slachtoffer worden van phishing dan oudere mensen. Hierbij toont Sheng et al. (2010) aan dat de groep van 18-25 jaren vatbaarder is voor slachtofferschap van phishing.

In het resultatendeel van dit onderzoek zal dan ook getoetst worden of geslacht en leeftijd een verklarende factor zijn voor het slachtofferschap van phishing op basis van de drie specifieke vormen van internetgebruik. Ook zal getoetst worden of de nationaliteit (Nederlands of Duits) uitmaakt voor het slachtofferschap van phishing.

Mate van internetgebruik als verklaring

Mannen zitten vaker en langer op het internet en hebben hierdoor mogelijk een grotere kans om slachtoffer te worden van phishing (Hoffman, Kalsbeek, & Novak, 1996). Daarbij blijkt dat mensen die een hoger opleidingsniveau hebbenvaker een hoge mate van internetgebruik hebben, dan zij die een lager opleidingsniveau hebben. Mensen met een lager opleidingniveau gebruiken nog steeds wel internet, maar in een mindere mate dan hoger opgeleiden dat doen (Hoffman et al., 1996). Ook is het belangrijk om te kijken naar het aantal e-mailadressen dat een persoon bezit. Wanneer phishingaanvallen veelvuldig via de mail gedaan worden, zou het kunnen zijn dat mensen die meer e-mailadressen hebben dus meer phishing e-mails ontvangen. Het grotere aantal ontvangen phishingmails kan de kans vergroten op slachtofferschap.

In het resultatendeel van dit onderzoek wordt getoetst of internetgebruik (in aantal uren per dag) een verklarende factor is voor slachtofferschap van phishing op basis van de vergaarde data. Ook zal er worden gekeken of het aantal e-mailadressen dat een scholier bezit invloed heeft op het slachtofferschap van phishing.

Niveau van technical knowledge

Een recent onderzoek toont aan dat slachtofferschap bij phishing ook samenhangt met de technical knowledge van een internetgebruiker (Sheng et al., 2010)**.** Technical knowledge kan gezien worden als het algemene niveau van technische kennis dat iemand heeft. De aanwezige relatie is zo dat mensen met een hogere algemeen niveau van technische kennis minder vaak voor phishing vallen. Mensen die zichzelf een hogere inschatting van hun technische kennis hebben gegeven, werden minder vaak slachtoffer werden van phishing (Sheng et al., 2010). Hierbij bestaat wel het methodologische issue dat het zo zou kunnen zijn dat mensen zich anders ingeschat hebben dan reëel is.

Onderzoeksmethode & Research Design

In dit hoofdstuk komen vooral de methodieken van het onderzoek naar voren. Zo wordt besproken wat het onderzoeksdesign is, wat de onderzoekssample is voor het onderzoek en hoe de datacollectie wordt gedaan. Ook de procedures voor de analyse van de data worden in dit hoofdstuk besproken, afsluitend met de analyse van de data zelf.

Onderzoeksmethode

In dit onderzoek, waar er een antwoord wordt gegeven op wat de relatie is tussen internetgedrag en slachtofferschap van phishing onder scholieren, wordt gebruik gemaakt van een cross-sectioneel onderzoeksdesign. Met name omdat er in een tijdspad van 8 weken gewerkt moet worden, was het slechts mogelijk om één meting te doen, wat kenmerkend is voor het cross-sectionele onderzoeksdesign. Daarnaast is dit onderzoek niet gerandomiseerd noch wordt er gebruik gemaakt van een controlegroep. Daarnaast gebruik ik kwantitieve data om de onderzoeksvraag te beantwoorden. Hiervoor is gekozen omdat op deze wijze de verklarende onderzoeksvraag goed via SPSS te toetsen is. Hoe ik mijn onderzoeksvraag ga toetsen zal later in dit hoofdstuk aan bod komen.

Steekproef

Omdat dit onderzoek gespecificeerd is op scholieren, is het van belang dat scholieren ook de units of observation zijn, om de vraag goed te kunnen beantwoorden. De units of analysis zijn daarbij middelbare scholen.

De scholen waar de data verzameld werden waren: SG Marianum te Groenlo, het Bataafs Lyceum te Hengelo en SG de Waerdenborgh te Holten en Goor. Daarnaast is er data verzameld in Duitsland op drie scholen in de omgeving Bremen. Er was geen voorgeselecteerde selectie van scholieren die de vragenlijst in zouden vullen, het doel was om ter plekke zo veel mogelijk scholieren binnen deze scholen bereid te vinden om de vragenlijst in te vullen.

Meetinstrument

Het gekozen instrument voor de dataverzameling is een digitale vragenlijst. Het voordeel van het collecteren van data via een digitale vragenlijst is namelijk dat de interactie tussen respondent en vragenlijst dynamischer is bij online vragenlijsten dan bij papieren vragenlijsten (Babbie, 2010). Daarnaast is het bij een online vragenlijst veel gemakkelijk om in een keer alle data van alle vragenlijsten in een dataset te krijgen. Hierdoor is het niet nodig om alles handmatig in te vullen, wat voorkomt dat er fouten worden gemaakt bij het overtypen van de data.

De vragen die toegevoegd zijn ten behoeve van het huidige onderzoek, namelijk voor het onderzoeken van het internetgedrag en het slachtofferschap van phishing, zijn verdeeld in drie typen vragen: Ten eerste vragen die uitwijzen wat de frequentie is van een bepaald type internetgebruik onder scholieren zoals gamen, shoppen of internet bankieren. Ten tweede een aantal scenarioschetsen van phishing per vorm van internetgebruik, waarmee gevraagd werd of de scholieren in het laatste jaar wel eens slachtoffer waren geworden van phishing.

De laatste categorie vragen waren vragen die vooral risicovolle factoren meten. Hierbij werd er onder anderen gevraag hoeveel e-mail adressen men bezat, hoeveel uur men achter de computer zit en of men bijvoorbeeld wel eens mobiel bankiert.

Concepten

Slachtofferschap van phishing

Het slachtofferschap van phishing wordt in deze studie op basis van een 6 vragen/variabelen gedaan. Omdat het hier een onderzoek naar specifiek slachtofferschap betreft, zijn deze vragen toegespitst op 3 vormen van internetgebruik: *Gaming, Social Networking en Online Bankieren.*

Deze drie vormen van internetgedrag zijn gekozen aan de hand van een theorie van Choi welk zegt dat risicovolle vrijetijdsactiviteiten op het internet de grootste contributie geven aan het slachtoffer worden van een computer misdaad (Choi, 2008). Deze theorie, in combinatie met een inzicht in de sectoren die het meest doelwit waren van phishing, aan de hand van de theorie van Charoen (2011) en Rajalingam (2012), maakt dat er voor deze drie specifieke vormen van internetgebruik is gekozen.

Een eerste set van 3 vragen representeert de eerste drie variabelen*: ''Phishing online gaming'' ''Phishing SNS'' & ''Phishing Online Banking''*. Door middel van scenarioschetsen wordt hiermee aan de scholieren via een Ja/Nee vraag gevraagd of het desbetreffende hen wel eens overkomen was in de afgelopen 12 maanden.

Er is voor het meten van slachtofferschap specifiek gekozen voor scenariovragen, om hiermee de slachtoffervraag (ben ik slachtoffer van phishing?) weg te halen bij de scholier. Door ze te bevragen door middel van een scenarioschets van phishing, is het voor de scholieren makkelijker te beantwoorden of ze slachtoffer zijn geweest van phishing of niet. Wanneer er rechtstreeks gevraagd wordt ''Ben je wel eens slachtoffer van phishing geweest?'' bestaat namelijk de kans dat de scholieren de inhoud van phishing niet goed begrijpen, of dat men gerelateerd slachtofferschap (zoals slachtofferschap van fraude) onder phishing schaart en hiermee een valse perceptie van het slachtofferschap teweeg brengt.

De tweede set vragen meten via de overige drie variabelen de frequentie van het slachtofferschap van phishing in de afgelopen 12 maand: "*Amount Phishing Online Gaming", Amount Phishing SNS & Amount Phishing Online Banking*. Er wordt hier gevraagd hoe vaak de in de eerdere vragen gestelde scenario's voorgekomen zijn bij hen. Deze vragen zijn in de vragenlijst zo gefilterd dat deze slechts beantwoord hoeft te worden bij een positief antwoord op de voorgaande set vragen. De antwoordcategorieën van deze vragen zijn: Een keer, Twee keer, Meer dan twee keer

Internetgedrag

In dit onderzoek wordt ''internetgedrag'' door een 8-tal variabelen vertegenwoordigd, gemeten door met een 8-tal vragen.

Aantal uren internetgebruik. Aan de hand van deze variabele proberen we inzicht te krijgen in de mate van internetgebruik van de scholier. We proberen hiermee te verklaren of het

aantal uren dat men het internet gebruikt bepalend is voor het worden van een slachtoffer van phishing. Het meten van deze variabele wordt gedaan aan de hand van een meerkeuze vraag met opties variërend van ‘’Ik gebruik het internet niet dagelijks’’ tot ‘’meer dan 6 uur per dag’’.

Aantal e-mailadressen. Er is gevraagd naar het aantal e-mailadressen is dat scholier bezit. We vragen hierbij aan de scholier om het aantal e-mailadressen dat hij/zij bezit in een cijfer op te geven, zodat dit resulteert in een ratio schaal.

Frequentie van online gaming. Deze variabele kan gezien worden als een specifiekere vorm van variabele 1. Aan de hand van deze variabele valt specifieker te meten welke vorm van internetgebruik een bepalende factor kan zijn voor het worden van een phishing slachtoffer. Deze vraag is gemeten aan de hand van een ordinale schaal, met 5 antwoordcategorieën: Nooit, een paar keer per jaar, een paar keer per maand, een paar keer per week & dagelijks.

Het bezitten van een eigen profiel op Social Networking Sites. Deze variabele meet of men in het bezit is van een eigen social networking profiel. Dit is gemeten aan de hand van een ja/nee vraag.

Frequentie van het gebruik van Social Networking Sites (SNS). Ook deze variabele geldt als een specificatie van variabele 1. Deze variabele wordt gemeten aan de hand van een vraag met 3 antwoordcategorieën: Nooit, zelden of regelmatig.

Het aantal vrienden op social networking sites. Deze variabele is getoetst via een multiple choise vraag met antwoordcategorieën variërend van 0-50 tot meer dan 400 vrienden.

Frequentie van Online bankieren. Deze variabele heeft dezelfde opbouw als variabele 3, en maakt gebruik van dezelfde antwoordcategorieën.

Het gebruik van Mobiel Bankieren. Er wordt hier gevraagd of men ook zijn mobiele telefoon gebruik om mee te online bankieren. Deze variabele wordt gemeten aan de hand van een Ja / Nee vraag.

Demografische gegevens

In het onderzoek bevinden zich ook een 3-tal demografische variabelen, om op eventuele verbanden tussen demografie en slachtofferschap van phishing te kunnen toetsen.

Leeftijd. De leeftijd wordt gemeten aan de hand van een open vraag. Hierbij is gevraagd de leeftijd in jaren in te vullen.

Geslacht. Het geslacht van de scholier is gevraagd aan de hand 2-keuze vraag met de antwoordcategorieën Man en Vrouw.

Nationaliteit. Omdat dit onderzoek in twee landen afgenomen wordt, is het ook belangrijk om de nationaliteit te vragen. Hiervoor is ook een 2-keuze vraag ingesteld.

Datacollectie

De datacollectie is gedaan aan de hand van een digitale, vooral kwantitatieve, vragenlijst, met daarin enkele vragen voor kwalitatieve data. Deze vragenlijst maakt onder anderen gebruik van reeds bestaande en gevalideerde schalen en vragen.

De vragenlijst is beschikbaar gesteld in drie talen: Nederlands, Engels en Duits, waarbij de Engelse versie vooral fungeerde als optie voor mogelijk verder internationaal onderzoek en als communicatiemiddel tussen het Nederlandse en Duitse research Team. De vertalingen van de vragenlijsten zijn gedaan middels de internationaal vastgestelde vertaalrichtlijnen. Deze richtlijnen behoeven dat de vragenlijst dubbel vertaald wordt van Engels naar Nederlands naar Engels, om zo de vertaling te kunnen valideren. De terugvertaling van het Nederlands naar het Engels is gedaan door externe personen die niets te maken hebben gehad met het onderzoek, een van de voorwaardes van de vertaalrichtlijnen.

De datacollectie is op alle scholen gedaan in de weken 23 en 24, waarbij er op verschillende en deels overlappende tijden data is verzameld. Daarbij is geprobeerd zo veel mogelijk bij alle datacollectie aanwezig te zijn om alles in goede banen te leiden. Bij het zoeken naar respondenten en het verkrijgen van data hebben we ook hulp gehad van mensen binnen de scholen zelf, zoals van mediatheek supervisors en docenten. Om de opkomst en de welwillendheid van de scholieren te vergroten is er bij de dataverzameling gebruik gemaakt van een loterij, waarbij scholieren na het invullen van de vragenlijst hun e-mailadres konden afgeven om zo kans te maken op een van de zes prijzen.

Data Cleaning

Om respondenten die de vraag willekeurig en onjuist hebben ingevuld er uit te filteren, is de data opgeschoond. Dit is gedaan door de mensen die binnen 500 seconden de vragenlijst hebben ingevuld er uit te filteren, ware het dat het invullen vragenlijst gemiddeld 20 minuten tijd beslaat. Daarnaast hebben we in de open vragen gekeken naar antwoorden die geen verband hadden met het onderzoek noch de gestelde vraag. Bij cases waar vreemde antwoorden ingevuld waren in de open vragen, is extra goed gekeken of het patroon van antwoorden naar inschatting wel reëel en naar waarheid is ingevuld.

Data analyse

Om de verschillende relaties te kunnen toetsen betreffende phishing, wordt er in dit onderzoek gebruik gemaakt van SPSS. Dit is een programma waarmee statistische analyses kunnen worden gedaan, op basis van een vergaarde dataset. Met behulp van dit programma hebben wij de datasets van zowel de Duitse respondenten als de Nederlandse respondenten kunnen combineren tot één dataset met alle cases, gescheiden door een samplecode ‘’1’’voor Nederlandse cases en ‘’2’’ voor Duitse cases. Dit maakt het analyseren van verschillen tussen de twee landen mogelijk.

Chi-Square Analyse (Chi-Kwadraattoets)

Een chi-square analyse is een parametervrije toets waarbij getoetst wordt op significante verschillen tussen populaties. Deze toets doet dit op basis van een vergelijking tussen de waargenomen aantallen en de verwachte aantallen.

De formule van de Chi-Kwadraattoets is als volgt:

$$\chi^2 = \sum \frac{(f-e)^2}{e},$$

Hierbij staat e voor de verwachte waarde en f voor de waargenomen waarde. De Som (Σ) van het verschil tussen de waargenomen waarde minus de verwachte waarde, gedeeld door de verwachte waarde levert de chi-square op. Omdat het huidige onderzoek een groot aantal cases bevat, is de chi-square via SPSS berekend, in plaats van handmatig.

Odds Ratio

De Odds Ratio (OR) maakt een belangrijk onderdeel uit van de Logistische Regressie. De OR vertelt ons iets over het verband tussen een variabele A en een variabele B. Met de OR kan bepaald worden wat de ‘’mate’’ waarin men variabele A bezit uit maakt voor de kans op het hebben of worden van B. In het geval van het huidig onderzoek kan met de Odds Ratio bijvoorbeeld bekeken worden wat het gebruik van mobiel bankieren (Variabele A) uit maakt voor de kans op het worden van slachtofferschap van phishing bij online bankieren (Variabele B). Wanneer de Odds Ratio groter is dan 1, kunnen we concluderen dat het gebruik van mobiel bankieren dat kans op het worden van slachtoffer van phishing bij online bankieren vergroot. Is dit getal kleiner dan 1, dan is het omgekeerd en draagt het niet bij aan de kans op phishing. Er moet hierbij wel onderscheid gemaakt worden in de meetniveaus van de variabelen. Bij een variabele die dichotoom is (bijv: Man/Vrouw) kan men niet spreken van een grotere of kleinere mate, maar enkel van het zijn van een man of vrouw.

Logistische Multivariate Regressie Analyse

De regressie analyse wordt gebruik om relaties tussen 2 variabelen vast te stellen. Zo kan er op deze manier bepaald worden of variabele x correleert met variabele y. Ook kan de richting en sterkte van een verband hiermee bepaald worden door de zogenaamde regressiecoëfficiënt ofwel de ‘’Slope’’ (B) te berekenen. Een negatieve waarde van dit coëfficiënt indiceert een negatief verband tussen de twee variabelen (meer x leidt tot minder y), een positieve waarde indiceert daarbij een positieve relatie (meer x leidt tot meer y)

De standaardformule voor regressie is als volgt: $y = a + bX$

Hierbij vertelt de ‘’a’’ door welk punt de lijn de y as snijdt (de y-intercept) en de ‘’b’’ de richting en de stijlheid van de lijn, met de sterkte X. Door middel van SPSS is direct de B te berekenen voor de gehele dataset. Ook verteld SPSS direct of het verband significant is. Dit doet het door een P-waarde te geven bij de regressieanalyse. Daarbij wordt bij dit onderzoek gehanteerd dat er sprake is van significantie wanneer $p < 0,05$.

Bij multivariate wordt de relatie tussen een groep afhankelijke variabelen en een onafhankelijke variabelen getoetst. Waarbij de bivariate regressie analyse een relatie tussen één afhankelijke en één onafhankelijke variabele toetst, toets de multivariate regressie een groep afhankelijke variabelen met de onafhankelijke variabelen. De formule voor deze vorm van regressie wijkt dan ook af in de zin dat hier voor meerdere factoren getoetst worden, en er dus meerdere ‘’B’’s aanwezig zijn in de formule. De formule van een multivariateregressie ziet er uit als volgt:

Y = b1x + b2x + b3x + …..

Waarbij b1, b2 en b3 elk een aparte afhankelijke variabele vertegenwoordigen.

In het huidige onderzoek wordt een specifieke vorm van regressieanalyse gebruikt, namelijk de logistische regressieanalyse. Deze vorm van regressieanalyse wordt gebruikt wanneer een groot deel van de variabelen een nominaal of ordinaal meetniveau hebben. Aangezien in dit onderzoek een groot deel van de variabelen van deze niveaus zijn, is er gekozen om logistische regressieanalyse te gebruiken voor de toetsing van de relatie van de hoofdvraag.

Onderzoeksresultaten

Karakteristieken van de onderzoekspopulatie

In de studie is er data verzameld onder 1.276 scholieren uit zowel Duitsland en Nederland. Hiervan waren 31,3% (400) leerlingen Nederlands en 68,7% (876) Duits. De gemiddelde leeftijd van de sample was 14,24 jaar (SD = 1,364). Hierbij was 32.4% (414) van de scholieren 11-13 jaar oud, 62.3% (795) was 14-16 jaar oud en 4,9% (40) 17-19 jaar oud. Onder de respondenten 51,7% mannelijk en 48,2% vrouwelijk. Onder de Nederlandse respondenten is ook het opleidingsniveau gemeten, hieruit volgde dat 40,3% (161) van de scholieren op het VMBO/MAVO zat, 21,3% (85) op het HAVO en 38,5% (154) op het VWO.

Betrokkenheid bij algemeen en specifieke vormen van internet gebruik

In deze studie is ook het internetgedrag van de scholieren onderzocht. Zo is er gevraagd hoeveel men gebruik maakt van het internet en hoeveel e-mailadressen men heeft. Ook is gevraagd of de scholieren gebruik maken van de bepaalde specifieke vormen van internetgebruik (Online gaming, Online bankieren en Gebruik van Social Networking Sites) en zo ja, hoe vaak ze dit doen.

Frequentie van algemeen internetgebruik

Onder de totale sample geeft 18.5% van de scholieren aan het internet gemiddeld meer dan zes uur per dag te gebruiken, 5.1% gemiddeld 6 uur per dag, 7.6% gemiddeld 5 uur per dag, 12.9% gemiddeld 4 uur per dag, 19.1% gemiddeld 3 uur per dag, 21.6% gemiddeld 2 uur per dag, 11.2% gemiddeld 1 uur per dag te gebruiken . Daarnaast gebruikt 11.2% van de scholieren het internet niet dagelijks. De onderlinge verschillen per land en geslacht zijn hierbij te vinden in de descriptives tabel (Tabel I). De resultaten tonen ook aan dat Nederlandse scholieren gemiddeld meer uren gebruik maken van het internet per dag (Mean= 4.11) dan Duitse scholieren (Mean = 3.32).

Aantal e-mailadressen

De resultaten van het onderzoek tonen aan dat op basis van de gehele sample men gemiddeld 2,49 e-mail adressen bezit. Hier bezitten scholieren in Nederland gemiddeld 2,71 (SD=2.348 N = 400) e-mailadressen, tegenover 2,40 (SD=2.398 N=876) e-mailadressen onder Duitse scholieren. Nederlandse scholieren lijken dus meer e-mailadressen te bezitten dan Duitse scholieren.

Betrokkenheid bij Online Gaming

De resultaten in de tabel (tabel I) tonen aan dat op basis van de totale sample 69.1% (882) van de scholieren online games speelt en 30.4% (388) geen games speelt. Daarvan spelen onder de Nederlandse scholieren 90,5% van de mannen online games tegenover 62.1% onder de vrouwen, met daarbij een gemiddeld percentage van 77.3% onder alle

Nederlandse scholieren. In Duitsland zijn deze percentages respectievelijk 77.3% en 53.9% met een gemiddelde van 65.4% onder alle Duitse scholieren. Daarbij speelt een groot deel (21,7%) van het totale aantal scholieren iedere dag games.

Ook zijn er verschillen waar te nemen per land ten aanzien van de frequentie waarin men online games speelt. Zo speelt in Nederland 30,0% (120) van de scholieren iedere dag games tegenover 18.0% (278) onder de Duitse scholieren. De resultaten wijzen uit dat mannen vaker online games spelen dan vrouwen en dat zowel Nederlandse mannelijke als vrouwelijke scholieren vaker games spelen dan Duitse de Duitse scholieren.

Betrokkenheid bij Online Bankieren

Op basis van de totale onderzochte populatie is te zien dat 61,0% van de scholieren wel eens gebruik maakt van online bankieren. Onder de Nederlandse scholieren gebruikt 58.3% van de mannen en 56.9% van de vrouwen wel eens online bankieren, met een gemiddelde van 56.5% onder alle Nederlandse scholieren . Onder de Duitse scholieren zijn deze percentages respectievelijk 67.2% en 59.8%, met een gemiddelde van 63.0%. Duitse scholieren gebruiken dus vaker online bankieren dan Nederlandse scholieren.

Op basis van de totale sample blijkt dat 2.4% van de scholieren elke dag online bankiert. 7.3% doet dit een paar keer per week, 22.2% een paar keer per maand en 29.1% een paar keer per jaar. De percentages per land en geslacht zijn hierbij terug te vinden in de descriptives tabel.

Ook is er gevraagd of de scholieren wel eens gebruik maakten van online bankieren via de mobiele telefoon: Mobiel bankieren. Wanneer we kijken naar de betrokkenheid per land, dan zien we dat in Nederland onder de mannen 14.3% en onder de vrouwen 17.2% gebruik maakt van online bankieren via de mobiele telefoon. In Duitsland zijn deze percentages respectievelijk 37,3% en 29,9%. Niet alleen het online bankieren in het algemeen ligt dus hoger in Duitsland, maar ook het percentage scholieren dat dit doet via de mobiele telefoon is hoger.

Betrokkenheid bij Gebruik Social Networking Sites

De studie laat zien dat 86.6% van alle scholieren gebruik maakt van Social Networking Sites. In Nederland geeft 90,3% van de scholieren aan wel eens Social Networking Sites te gebruiken. In Duitsland is dit percentage 85.3%. Hierbij gebruikt in Nederland 86.9% van de mannen en 94.4% van de vrouwen Social Networking sites. In Duitsland is dit respectievelijk 83.4% en 87.4%. Nederlandse scholieren zijn daarmee vaker op social networking sites actief van Duitse scholieren. Onder deze scholieren gebruikt 66.9% van de totale sample deze vorm van internetgebruik ‘’Regelmatig’’.

In de studie is ook gevraagd naar het aantal vrienden dat men heeft op Social Networking sites. Hierbij geeft onder de Nederlandse scholieren 12,3% aan meer dan 400 vrienden te hebben op SNS en 14.3% tussen de 0 en 50 vrienden te hebben op SNS. De tussenliggende waarden per land en geslacht zijn hierbij te vinden in de descriptives tabel.

Tabel I: Descriptives tabel onderzoekspopulatie (N=1276)	**Nederland *(N= 400)***				**Duitsland *(N= 876)***				**Totaal Gecombineerd *(N= 1276)***	
Variables		**Mannen**	**Vrouwen**	**Totaal**		**Mannen**	**Vrouwen**	**Totaal**		
	N	**%**	**%**	**%**	**N**	**%**	**%**	**%**	**N**	**%**
Leeftijd (Jaren)										
11-13	122	33.9	26.4	30.5	292	33.7	33.3	33.3	414	**32.4**
14-16	237	56.1	63.5	59.3	558	63.1	64.9	63.7	795	**62.3**
17-19	40	10.0	10.1	10.0	22	3.2	1.8	2.5	62	**4.9**
Missing	1	-	-	0.2	4	-	-	0.5	5	**0.4**
Opleidingsniveau										
VMBO	161	35.7	45.8	40.3	-	-	-	-	161	**40.3**
HAVO	85	24.4	17.3	21.3	-	-	-	-	85	**21.3**
VWO	154	39.9	36.9	38.4	-	-	-	-	154	**38.4**
Speelt online games										
Nee	88	9.5	37.9	22.0	300	22.7	46.1	34.2	388	**30.4**
Ja	309	90.5	62.1	77.3	573	77.3	53.9	65.4	882	**69.1**
Missing	3	-	-	0.7	3	-	-	0.3	6	**0.5**
Frequentie online gaming										
Nooit	88	9.5	37.9	22.0	300	22.7	46.1	34.2	388	**26.5**
Een paar keer per jaar	58	8.6	22.0	14.5	169	10.7	28.0	19.3	227	**17.8**
Een paar keer per maand	55	12.3	15.9	13.8	125	14.4	14.2	14.3	180	**14.1**
Een paar keer per week	76	23.2	14.1	19.0	121	21.1	6.7	13.9	197	**15.4**
Iedere dag	120	46.4	10.1	30.0	158	31.1	5.0	18.0	278	**21.7**
Missing	3	-	-	0.7	3	-	-	0.3	6	**0.5**
Slachtoffer phishing: online gaming										
Ja	16	6.1	3.6	4.0	81	19.1	6.8	9.2	97	**7.6**
Nee	292	93.9	96.4	73.0	493	80.9	93.2	56.3	785	**61.5**
Missing	92	-	-	23.0	302	-	-	34.5	394	**30.9**
Gebruik online bankieren										
Nee	166	41.7	43.1	41.5	318	32.8	40.2	36.3	484	**37.9**
Ja	226	58.3	56.9	56.5	552	67.2	59.8	63.0	778	**61.0**
Missing	8	-	-	2.0	6	-	-	0.7	14	**1.1**
Gebruik mobiel bankieren										
Nee	190	85.7	83.8	47.5	366	62.7	70.1	41.8	559	**43.8**
Ja	35	14.3	17.2	8.8	187	37.3	29.9	21.3	226	**17.7**
Missing	175	-	-	43.7	323	-	-	36.9	491	**38.5**
Frequentie online bankieren										
Nooit	166	41.7	43.1	41.5	318	32.8	40.2	36.3	484	**37.9**

Een paar keer per jaar	152	37.2	40.8	38.0	219	23.4	26.9	25.0	371	**29.1**
Een paar keer per maand	63	18.7	12.6	15.7	220	28.4	22.1	25.1	283	**22.2**
Een paar keer per week	8	1.0	3.5	2.0	85	11.5	8.0	9.7	93	**7.3**
Iedere dag	3	1.4	0.0	0.8	28	3.7	2.7	3.2	31	**2.4**
Missing	8	-	-	2.0	6	-	-	0.7	14	**1.1**
Slachtoffer phishing: online bankieren										
Ja	9	4.7	3.0	2.3	31	6.8	4.1	3.5	40	**3.1**
Nee	216	95.3	97.0	54.0	527	93.2	95.9	60.2	743	**58.3**
Missing	175	-	-	43.7	318	-	-	36.3	493	**38.6**
Gebruik SNS										
Ja	361	86.9	94.4	90.3	747	83.4	87.4	85.3	1108	**86.8**
Nee	39	13.1	5.6	9.7	128	16.6	12.6	14.6	167	**13.1**
Missing	-	-	-	-	1	-	-	0.1	1	**0.1**
Frequentie gebruik SNS										
Nooit	51	18.8	5.6	12.8	148	18.7	16.5	16.9	199	**15.6**
Zelden	73	21.1	15.2	18.2	111	16.5	9.9	12.7	184	**14.4**
Regelmatig	272	60.1	79.2	68.0	582	64.8	73.6	66.4	854	**66.9**
Missing	4	-	-	1.0	35	-	-	4.0	39	**3.1**
Totaal aantal vrienden op SNS										
0-50	57	20.2	10.7	14.3	70	12.0	6.8	8.0	127	**10.0**
51-100	51	16.1	11.8	12.8	75	9.3	10.8	8.6	126	**9.9**
101-150	45	13.0	11.8	11.3	79	12.8	8.4	9.0	124	**9.7**
151-200	41	11.9	10.7	10.3	78	11.2	9.7	8.9	119	**9.3**
201-250	40	11.4	10.7	10.0	72	8.2	11.0	8.2	112	**8.8**
251-300	28	5.2	10.7	7.0	69	8.2	10.2	7.9	97	**7.6**
301-350	35	7.8	11.8	8.8	47	6.3	6.3	5.4	82	**6.4**
351-400	16	2.6	6.5	4.0	62	7.4	9.2	7.1	78	**6.1**
Meer dan 400	49	11.9	15.4	12.3	195	24.6	27.6	22.3	244	**19.1**
Missing	38	-	-	9.5	129	-	-	14.7	167	**13.1**
Slachtoffer phishing: SNS										
Ja	6	1.6	1.8	1.5	66	6.9	10.8	7.5	72	**5.6**
Nee	355	98.4	98.2	88.8	678	93.1	89.2	77.4	1033	**81.0**
Missing	39	-	-	9.7	132	-	-	15.1	171	**13.4**
Uren internetgebruik (Per dag)										
Ik gebruik het internet niet dagelijks	6	1.4	1.4	1.5	78	9.3	8.5	8.9	84	**6.6**
1 uur	35	10.4	6.7	8.8	98	13.2	9.2	11.2	133	**10.4**
2 uur	65	17.6	14.5	16.3	189	18.0	25.3	21.6	254	**19.9**
3 uur	74	22.6	13.4	18.5	167	19.6	18.6	19.1	241	**18.9**
4 uur	58	12.7	16.8	14.5	107	13.0	11.5	12.2	165	**12.9**
5 uur	41	9.0	11.7	10.3	56	5.7	7.1	6.4	97	**7.6**
6 uur	26	6.3	6.7	6.5	39	4.8	4.1	4.5	65	**5.1**

Meer dan 6 uur	95	20.0	28.5	23.8	141	16.4	15.8	16.1	236	**18.5**
Missing	-	-	-	-	1	-	-	0.1	1	**0.0**
Aantal e-mail adressen in bezit										
Heeft geen e-mail	0	0.0	0.0	0	19	3.4	1.0	2.2	19	**1.5**
1-3 e-mail adressen	323	76.5	86.5	80.8	717	75.4	89.8	81.8	1040	**81.5**
4-6 e-mail adressen	61	17.6	12.4	15.3	104	15.2	8.8	11.9	165	**12.9**
Meer dan 6 e-mail adressen	15	5.9	1.1	3.8	28	6.0	0.4	3.2	43	**3.4**
Missing	1	-	-	0.3	8	-	-	0.1	9	**0.7**

Tabel II: Slachtofferschap bij Phishing Online Gaming, Phishing SNS & Phishing Online Banking - Gecategoriseerd voor Leeftijd, Nationaliteit, Geslacht, Opleidingniveau, Aantal e-mailadressen, Aantal uren internetgebruik, Frequentie Online Gaming, Frequentie Online Bankieren, Gebruik Mobiel Bankieren, Frequentie Gebruik SNS & Aantal vrienden op SNS.

Variables	Slachtoffer Phishing Online Gaming (%)					Slachtoffer Phishing SNS (%)					Slachtoffer Phishing Online Banking (%)				
	N	Ja	Nee	χ^2	Df	N	Ja	Nee	χ^2	Df	N	Ja	Nee	χ^2	Df
Leeftijd (Jaren)															
11-13	300	10.0	90.0	3.060	2	316	7.9	92.1	2.096	2	229	3.1	5.4	4.837	2
14-16	543	10.5	89.5			729	6.2	93.8			521	5.4	94.6		
17-19	36	19.4	80.6			59	3.4	96.6			36	11.1	88.9		
Nationaliteit															
Nederlands	308	5.2	94.8	16.282**	1	361	1.7	98.3	20.653**	1	226	4.0	96.0	.787	1
Duits	574	14.1	85.9			746	8.8	92.1			562	5.5	94.5		
Geslacht															
Jongen	538	14.3	85.7	15.482**	1	557	5.0	95.0	4.023*	1	420	6.2	93.8	2.318	1
Meisje	344	5.8	94.2			550	8.0	92.0			368	3.8	96.2		
Opleidingsniveau															
VMBO/MAVO	121	5.8	94.2	.176	2	150	1.3	98.7	.434	2	90	3.3	96.7	.880	2
HAVO	68	4.4	95.6			77	1.3	98.7			43	2.3	97.7		
VWO	119	5.0	95.0			134	2.2	97.8			93	5.4	94.6		
Aantal e-mailadressen in bezit															
Heeft geen e-mail	9	11.1	88.9	30.201**	3	9	0.0	100.0	1.182	3	5	20.0	80.0	3.570	3
1-3 E-mail Adressen	704	8.7	91.3			894	6.3	93.7			629	4.6	95.4		
4-6 E-mail Adressen	124	15.3	84.7			158	7.6	92.4			119	6.7	93.3		
Meer dan 6 E-mail adressen	40	35.0	65.0			41	4.9	95.1			32	3.1	96.9		
Aantal Uren Internetgebruik															
Geen dagelijks gebruik	47	8.5	91.5	31.921**	7	41	4.9	95.1	13.736	7	28	10.7	89.3	16.824*	7
1 Uur	87	9.2	90.8			100	5.0	95.0			55	1.8	98.2		
2 Uur	165	4.2	85.8			216	4.6	95.4			140	1.4	98.6		
3 Uur	174	8.0	92.0			216	5.6	94.4			158	2.5	97.5		
4 Uur	123	9.8	90.2			158	8.2	91.8			110	4.5	95.5		
5 Uur	66	15.2	84.8			90	6.7	93.3			73	8.2	91.8		
6 Uur	45	8.9	91.1			62	0.0	100.0			50	6.0	94.0		
Meer dan 6 Uren	175	21.7	78.3			224	10.7	89.3			174	9.2	90.8		
Frequentie Online Gaming															
Nooit	5	0.0	100.0	38.316**	4	327	3.7	96.3	8.918	4	216	5.6	94.4	1.709	4
Een paar keer per jaar	226	4.0	96.0			200	7.5	92.5			136	4.4	95.6		
Een paar keer per maand	178	8.4	91.6			154	8.4	91.6			108	4.6	95.4		
Een paar keer per week	196	8.7	91.3			171	5.3	94.7			121	3.3	96.7		
Iedere dag	277	20.2	79.8			251	9.2	90.8			206	6.3	93.7		
Frequentie Online Bankieren															

Nooit	311	8.0	92.0	12.319*	4	393	5.9	94.1	3.252	4	16	0.0	100.0	5.707	4
Een paar keer per jaar	264	9.5	239			331	6.3	93.7			369	5.4	94.6		
Een paar keer per maand	208	13.9	86.1			258	6.2	93.8			281	3.9	96.1		
Een paar keer per week	75	14.7	72.7			86	8.1	91.9			91	5.5	94.5		
Iedere dag	22	27.3	72.7			29	13.8	86.2			31	12.9	87.1		
Gebruik Mobiel Bankieren															
Nee	398	9.8	90.2	7.237**	1	439	5.5	94.5	5.138*	1	549	4.9	95.1	.283	1
Ja	161	18.0	82.0			205	10.2	89.8			222	5.9	94.1		
Frequentie Gebruik SNS															
Nooit	129	10.9	89.1	.662	2	58	6.9	93.1	3.603	2	92	4.3	95.7	.164	2
Zelden	136	8.8	91.2			168	3.0	97.0			109	5.5	94.5		
Regelmatig	588	11.2	88.8			850	6.8	93.2			568	5.3	94.7		
Aantal Vrienden op SNS															
0-50	103	11.7	88.3	16.584*	8	126	5.6	94.4	14.366	8	73	6.8	93.2	11.391	8
51-100	102	4.9	95.1			126	4.8	95.2			64	4.7	95.3		
101-150	87	8.0	82.0			123	3.3	96.7			74	4.1	95.9		
151-200	76	9.2	90.8			119	3.4	96.6			76	2.6	97.4		
201-250	84	3.6	96.4			112	3.6	96.4			73	0.0	100.0		
251-300	63	12.7	87.3			97	11.3	88.7			61	3.3	96.7		
301-350	62	11.3	88.7			82	8.5	91.5			54	3.7	96.3		
351-400	46	15.2	84.8			78	7.7	92.3			54	7.4	92.6		
Meer dan 400	154	16.9	83.1			224	9.4	90.6			185	8.6	91.4		

Prevalentie slachtofferschap van phishing

De resultaten van de studie in de descriptives- en slachtofferschaptabel (Tabel I & II) tonen een groot aantal percentages wat betreft het slachtofferschap van phishing. Wederom zijn deze weergegeven op basis van de drie specifieke vormen van internetgebruik waarmee het slachtofferschap gemeten werd.

Phishing bij Online Gaming

Het grootste slachtofferpercentage werd gevonden bij online gaming. Op basis van de totale sample gaf 7.6% van de scholieren aan wel eens gephisht te zijn bij het online gamen. Per land zijn er verschillen te ontdekken in de percentages van het slachtofferschap. Zo is in Nederland 4,0% van de scholieren wel eens gephisht bij het online gamen, terwijl dit percentage in Duitsland een stuk hoger ligt, namelijk 9.2% (Tabel I). Ook aan de hand van geslacht zijn in beide landen verschillen te vinden, en wel zo dat in beide gevallen mannelijke scholieren vaker slachtoffer zijn geworden dan vrouwelijke slachtoffers. Het meest schokkende resultaat is gevonden onder Duitse mannelijke scholieren. Onder deze groep werd een slachtofferpercentage van maarliefst 19.1% gevonden. Dit is verassend aangezien er in Duitsland minder scholieren aangaven te gamen (65.4%) dan Nederlandse scholieren (77.3%) terwijl het slachtofferschap in Duitsland toch hoger ligt. Wanneer we kijken naar de slachtofferschapstabel (tabel 2). Dan is daar te zien dat het relatief aantal slachtoffers van phishing bij online gaming het grootst is onder die mensen die aangaven dagelijks meer dan 6 uur het internet te gebruiken. Van alle respondenten die aangaven dat ze meer dan 6 uur per dag het internet gebruikten, heeft 21.7% in een opvolgende slachtoffervraag aangegeven dat hij of zij ook wel eens gephisht is bij het online gamen. Ook wanneer er gekeken wordt naar de frequentie van het gamen dan valt te zien dat in de groep die aangaf dagelijks te gamen een relatief hoger slachtofferpercentage te vinden is. Onder de scholieren die aangaven dagelijks te gamen, gaf 20.2% in de opvolgende slachtofferschapsvraag aan wel eens slachtoffer te zijn geweest van phishing in de laatste 12 maanden.

Bij de variabele ‘’aantal e-mailadressen in bezit’’ zien we een zelfde verschijnsel. Zij die aangaven meer dan 6 e-mailadressen te bezitten, zijn relatief ook een stuk vaker slachtoffer van phishing bij online gaming, met een percentage van 35.0% (zie tabel II). Ter vergelijking met het slachtofferschap bij de andere vormen van phishing is er wel op te merken dat het aantal e-mailadressen wat men bezit vooral invloed heeft op het slachtofferschap bij gaming, maar niet zo zeer bij de andere twee vormen van slachtofferschap. Zo liggen de percentages van slachtofferschap van de mensen die aangaven 6 of meer e-mailadressen te bezitten daar op de 4.9% en 3.1% en zijn dan ook niet hoger dan mensen die minder e-mailadressen bezitten (Zie tabel II).

Phishing bij Social Networking Sites

Ook is slachtofferschap van phishing gemeten aan de hand van het gebruik van Social Networking Sites. Hoewel zowel in Duitsland als Nederland het overgrote deel een profiel heeft op een social networking site (NL: 90,3%, DE: 85.3%), vallen via deze weg niet de meeste slachtoffers. Op basis van de gehele sample (N=1276) werd er een slachtofferpercentage van 5.6% gevonden. Wanneer we kijken naar de

slachtofferpercentages per land, dan vinden we in Nederland een percentage van 1.5% (6) en in Duitsland een percentage van 7.5% (66). Waar in Nederland het slachtofferschap bij beide geslachten ongeveer gelijk is (namelijk 1,6% onder de mannen en 1.8% onder de vrouwen) is er een groter verschil op te merken in Duitsland. Onder de Duitse scholieren werd een percentage van 6.9% slachtofferschap onder mannelijke scholieren gevonden, tegenover een percentage van 10.8 onder vrouwelijke scholieren. Wederom is bij deze vorm van slachtofferschap van phishing, net als het slachtofferschap bij online gaming, het percentage slachtoffers hoger in Duitsland dan in Nederland. Middels de slachtofferschaptabel is te bevestigen dat vrouwen vaker slachtoffer zijn van phishing bij SNS (8.0%) dan mannen (6.0%), op basis van de totale sample, exclusief missing cases.

Wanneer we kijken naar de slachtofferschaptabel (tabel II). Dan valt er niet direct op te merken dat de frequentie van het gebruik in SNS en het aantal vrienden dat men bezit op SNS uit maken voor het slachtofferschap. Zo zijn bijvoorbeeld de mensen die aangaven meer dan 400 vrienden te hebben op SNS niet vaker slachtoffer van phishing bij SNS dan de mensen die aangaven minder vrienden te hebben, zoals te zien in de slachtofferschaptabel.

Phishing bij Online Bankieren

De resultaten van de laatste getoetste vorm, slachtofferschap van phishing bij online bankieren, leveren het laagste slachtofferpercentage op. Er werd hier een percentage van 3.1% slachtofferschap gevonden op basis van de totale sample (1276). Hierbij lag het percentage in Nederland ietwat lager met een slachtofferschap van 2.3% dan in Duitsland: 3.5%. Zowel in Nederland als Duitsland werden mannelijke scholieren vaker slachtoffer via deze manier van phishing dan vrouwelijke scholieren. Zo zijn de percentages in Nederland onder mannen en vrouwen 4.7% en 3.0% en in Duitsland respectievelijk 6.8% en 4.1%.

In de slachtofferschaptabel (Tabel II) valt wel te zien dat bij phishing bij online bankieren een hogere frequentie van online bankieren, het gebruik van mobiel bankieren en het aantal uren dat men per dag het internet gebruikt een relatief hogere slachtofferschapschappercentages van phishing bij online bankieren geven. Deze oplopende cijfers kunnen mogelijk de verklaring geven of deze variabelen verklarende factoren zijn bij het slachtoffer worden van phishing bij online bankieren.

Om goed te kunnen concluderen welke variabelen weldegelijk het slachtofferschap van phishing bij de verschillende vormen van internetgebruik kunnen verklaren, is er een logistische regressieanalyse benodigd. In deze analyse kan getoetst worden of er een significante relatie bestaat tussen de diverse variabelen van internetgedrag en demografie, en de slachtofferschapvariabelen. Deze logistische regressieanalyse is dan ook uitgevoerd. De resultaten hiervan worden uitgewerkt in de volgende alinea.

Logistische regressieanalyse: Demografische relaties bij het slachtofferschap van phishing

Deze studie wil ook relaties onderzoeken wat betreft de demografische en socio-economische karakteristieken van de scholieren en het slachtofferschap van phishing. Onderstaand zijn de resultaten te lezen van de logistische regressie ten aanzien van het slachtofferschap van phishing bij de drie specifieke vormen van internetgebruik.

Leeftijd & het slachtofferschap van phishing

De verschillen in leeftijd onder de scholieren lijken in geen geval uit te maken op het slachtofferschap van phishing. In alle gevallen werd er geen significant verband gevonden tussen leeftijd en de kans op het worden van slachtoffer van phishing. Leeftijd, onder scholieren, blijkt dus niet uit te maken. Dat wil zeggen, in de leeftijdsgroep van 12-19, maakt het niet uit wat je leeftijd is ten aanzien van de kans op het worden van slachtoffer van phishing.

Nationaliteit & het slachtofferschap van phishing

Bij zowel phishing bij online gaming als phishing bij SNS is een significante relatie gevonden tussen nationaliteit en het worden van slachtoffer van phishing bij online gaming (OR 3.30 p .00) en phishing bij SNS (OR 6.41 p .00). Ten aanzien van het slachtofferschap bij online bankieren werd geen significante relatie gevonden met nationaliteit. De data suggereert hierbij dat het wonen in Duitsland een hogere kans op slachtofferschap bij phishing in het geval van online gaming en SNS oplevert.

Geslacht & het slachtofferschap van phishing

In de theorie van dit onderzoek behandelden we hoe geslacht mogelijk een factor voor slachtofferschap van phishing kan zijn. De regressieresultaten tonen dat er bij geslacht inderdaad significante relatie werd gevonden ten aanzien van het slachtofferschap bij phishing. In alle gevallen van slachtofferschap bij phishing is er een significante relatie gevonden met geslacht. De richtingen van deze verbanden zijn niet allemaal hetzelfde. De OR's ten aanzien van online gaming en online bankieren, respectievelijk 2.10 en 2.62, tonen dat slachtoffers van phishing bij online gaming en online bankieren vaker mannelijk zijn. Mannen zouden dus een verhoogde kans hebben op het worden van slachtoffer van phishing bij online gaming en online bankieren. Bij de relatie tussen geslacht en het slachtofferschap van phishing bij SNS gebruikers ligt dit anders. Bij deze relatie werd een OR van 0.29 gevonden, zoals te zien in tabel V. Dit betekend dat slachtoffers van phishing die tevens SNS gebruiken vaker vrouwelijk zijn. In dit geval zouden vrouwen die SNS gebruiken dus een hogere kans hebben op het worden van slachtoffer van phishing in vergelijking met mannen die SNS gebruiken. Deze relaties zijn goed te onderbouwen met de cijfers uit de slachtofferschaptabel (Tabel II).

Logistische regressieanalyse: Van internetgedrag naar slachtofferschap van phishing

Middels logistische regressie is er getoetst op mogelijke relaties tussen de verschillende variabelen van internetgedrag en het slachtofferschap van phishing op basis van de drie specifieke vormen.

Tabel III: Logistische Regressie slachtofferschap Phishing Online Banking & internetgebruik + demografische factoren. (N=788)

	Phishing Online Banking		
	OR	**95%-CI**	**p**
Leeftijd	1.05	0.80 – 1.38	.72
Nationaliteit	1.21	0.51 – 2.89	.67
Geslacht	2.62	1.15 – 5.98	.02*
Aantal e-mail adressen in bezit	0.97	0.86 – 1.10	.64
Internetgebruik (Aantal uren)	1.23	1.02 – 1.48	.03*
Frequentie Online Gaming	0.80	0.54 – 1.19	.28
Frequentie Online Bankieren	0.93	0.60 – 1.43	.74
Gebruik mobiel bankieren	0.89	0.41 – 1.97	.78
Bezit van een SNS profiel	0.87	0.15 – 5.12	.87
Frequentie SNS	0.94	0.45 – 1.94	.87
Aantal vrienden op SNS	1.00	0.87 – 1.16	.97
Slachtofferschap Phishing Online Gaming	3.50	1.32 – 9.30	.01**
Slachtofferschap Phishing SNS	2.51	0.89 – 7.14	.08

*= Significant op het 0.05 niveau *= Significant op het 0.01 niveau.

Tabel IV: Logistische Regressie slachtofferschap Phishing Online Gaming & internetgebruik + demografische factoren. (N=882)

	Phishing Online Gaming		
	OR	**95%-CI**	**p**
Leeftijd	1.08	0.87 – 1.33	.50
Nationaliteit	3.30	1.72 – 6.35	.00**
Geslacht	2.10	1.08 – 4.09	.03*
Aantal e-mail adressen in bezit	1.13	1.05 – 1.21	.00**
Internetgebruik (Aantal uren)	1.20	1.04 – 1.37	.01**
Frequentie Online Gaming	1.49	1.14 – 1.94	.00**
Frequentie Online Bankieren	1.09	0.77 – 1.53	.63
Gebruik mobiel bankieren	1.27	0.66 – 2.45	.47
Bezit van een SNS profiel	5.79	1.81 – 18.52	.00**
Frequentie SNS	1.50	0.87 – 2.59	.14
Aantal vrienden op SNS	1.00	0.90 – 1.12	.96
Slachtofferschap Phishing Online Bankieren	3.23	1.18 – 8.89	.02*
Slachtofferschap Phishing SNS	5.05	2.39 -10.68	.00**

*= Significant op het 0.05 niveau *= Significant op het 0.01 niveau.

Tabel V: Logistische Regressie slachtofferschap Phishing Social Networking Sites & internetgebruik + demografische factoren (N=1107).

		Phishing SNS	
	OR	**95%-CI**	**p**
Leeftijd	0.98	0.78 – 1.23	.86
Nationaliteit	6.41	2.43 – 16.89	.00**
Geslacht	0.29	0.15 – 0.59	.00**
Aantal e-mail adressen in bezit	0.96	0.85 – 1.07	.45
Internetgebruik (Aantal uren)	1.07	0.92 – 1.24	.41
Frequentie Online Gaming	1.21	0.90 – 1.62	.20
Frequentie Online Bankieren	0.90	0.61 – 1.34	.61
Gebruik mobiel bankieren	1.52	0.74 – 3.10	.25
Frequentie SNS	0.94	0.54 – 1.62	.82
Aantal vrienden op SNS	1.08	0.96 – 1.20	.19
Slachtofferschap Phishing Online Bankieren	3.20	1.09 – 9.40	.03*
Slachtofferschap Phishing Online Gaming	5.60	2.66 – 11.78	.00**

*= Significant op het 0.05 niveau *= Significant op het 0.01 niveau.

Het aantal e-mailadressen in bezit & het slachtofferschap van phishing

Ten aanzien van de variabele “aantal e-mailadressen’’ werden er significante verbanden gevonden met het slachtofferschap van phishing bij online gaming (OR: 1.13, p .00, zie tabel IV). Met de andere twee vormen van slachtofferschap werd er geen significant verband gevonden. Het aantal e-mailadressen dat een scholier bezit lijkt dus alleen verband te hebben met phishing bij online gaming. Het in bezit zijn van een groter aantal e-mailadressen zou dus in het geval van phishing bij online gaming leiden tot een grotere kans op het worden van een slachtoffer van phishing bij online gaming.

De relatie tussen het aantal uren internetgebruik per dag & het slachtofferschap van phishing

De resultaten van de regressieanalyse tonen (zie tabel III, IV & V) dat er bij twee van de drie gevallen van phishing er een significante relatie met het aantal uren internetgebruik, namelijk bij phishing bij online gaming (Significant op het 0.01 niveau) en phishing bij online bankieren (Significant op het 0.05 niveau). Het aantal uren dat men per dag op het internetgedrag blijk dus in 2 van de 3 gevallen uit te maken voor het slachtofferschap van phishing en wel zo dat, Met gevonden Odds Ratios (OR) van boven de 1, mensen met een hoger aantal uren internetgebruik per dag meer kans hebben om slachtoffer te worden van phishing bij online gaming en phishing bij online bankieren.

Frequentie van gebruik internetvormen & het slachtofferschap van phishing

Ook is er gekeken naar een verband tussen de frequentie van het spelen van games, het actief zijn op social networking sites het online bankieren en het slachtofferschap van

phishing. Wederom werd er hier enkel ten aanzien van het online gamen een significant verband gevonden (OR 1.49, p .00, zie tabel IV). Voor slachtofferschap van phishing bij online gaming heeft dus, zoals redelijkerwijs verwacht kan worden, men meer kans om slachtoffer te worden van phishing bij online gaming naarmate men in een hogere frequentie online games speelt. Bij de andere twee vormen kan een dergelijke relatie niet aangetoond worden.

Mobiel bankieren & het slachtofferschap van phishing (Bij online bankieren)

In het theoriedeel van dit onderzoek werd er verwacht dat er mogelijk een relatie zou kunnen bestaan tussen het slachtofferschap van phishing, in het specifiek slachtofferschap bij online bankieren, en het gebruik van de mobiele telefoon voor internetbankieren. De resultaten van de logistische regressie tonen dat dit niet het geval is. Er werd geen significante relatie gevonden tussen het gebruik van de mobiel bankieren en het slachtoffer worden van phishing bij online bankieren alsmede slachtofferschap bij online gaming en SNS. Het mobiel bankieren verhoogt dus niet te kans om slachtoffer te worden van phishing.

Het hebben van een eigen profiel op social media & het slachtofferschap bij phishing

Buiten dat het hebben van een eigen profiel op social networking sites een voorwaarde is om slachtoffer te kunnen worden van phishing via social networking, hebben wij dit ook getoetst op de andere vormen van phishing. Daarbij blijk het dat het hebben van een eigen social networking profiel bijdraagt aan het slachtofferschap van phishing bij online gaming. In de logistische regressie werd er een significant verband gevonden tussen het bezitten van een eigen SNS profiel en het slachtofferschap van phishing bij gaming. Het hebben van een eigen profiel op SNS verhoogd dus de kans op het worden van slachtoffer van phishing bij online gaming. Ten aanzien van het online bankieren werd geen verband gevonden.

Het aantal vrienden op SNS & het slachtofferschap van phishing (Bij social networking sites)

Het aantal vrienden dat men heeft op Social Networking Sites (SNS) zou, zoals in de theorie vermeld, verband kunnen hebben met het slachtofferschap bij phishing, in het specifiek voor phishing bij SNS. Uit de resultaten van de logistische regressie (Tabel III, IV en V) blijkt echter dat er geen significant verband bestaat tussen het aantal vrienden dat men heeft op SNS en de kans op slachtofferschap van phishing bij SNS. Ook ten aanzien van de andere vormen van slachtofferschap is er geen verband gevonden. Het aantal vrienden dat men heeft op SNS blijkt dus in geen geval verband te hebben met het worden van slachtoffer van phishing.

Onderlinge relaties tussen het slachtofferschap van phishing.

Niet alleen tussen de variabelen van internetgedrag en het slachtofferschap van phishing zijn significante relaties gevonden, ook tussen de verschillende vormen van slachtofferschap bij phishing. Zo tonen bijvoorbeeld de resultaten van de logistische regressie aan dat ten aanzien van SNS het zijn van slachtoffer van phishing bij online bankieren en online gaming bijdraagt aan het worden van slachtoffer van phishing bij SNS. Bij het slachtofferschap van phishing bij online gaming vonden we een zelfde fenomeen. Ten aanzien van het slachtofferschap bij online gaming vonden we een relatie met het slachtofferschap bij

phishing SNS & slachtofferschap bij online bankieren. Ten aanzien van phishing bij online bankieren werd er alleen een significante relatie gevonden met online gaming. De onderlinge relaties tussen de slachtofferschapsvormen laten zien dat het goed mogelijk is dat een aantal dezelfde mensen op meerdere platformen slachtoffer worden. Er is dus mogelijk een soort universele factor bij deze mensen die verklaard dat ze in het algemeen slachtoffer worden van phishing, ongeacht de vorm van internetgebruik. Om te weten te komen wat deze mogelijke universele factor zou kunnen zijn kan niet worden aangetoond met dit onderzoek en zal dus verdergaand onderzoek nodig zijn.

Conclusie, Discussie & Beperkingen

In dit laatste hoofdstuk zullen de deelvragen beantwoord worden. Er wordt per deelvraag bekeken wat er geconcludeerd kan worden. Daarna wordt er afgesloten met een discussie over de onderzoeksresultaten en uitkomsten en de beperkingen van het huidige onderzoek.

Conclusie

Ten aanzien van de betrokkenheid van scholieren bij het algemeen internet gebruik kunnen we concluderen dat Nederlandse scholieren vaker en langer gebruik maken van het internet vergeleken met Duitse scholieren. Ook zien we dat Nederlandse studenten gemiddeld meer e-mailadressen bezitten dan Duitse scholieren.

Binnen de drie vormen van internetgebruik zijn de scholieren het meest betrokken met Social Networking, 86.6% van de totale sample gaf aan hiervan gebruik te maken. Daarnaast zijn de scholieren betrokken bij het online gamen en online bankieren, maar in mindere mate dan dat zij betrokken zijn met Social Networking (Zie tabel I). De betrokkenheid bij de verschillende specifieke vormen van internetgebruik zijn verschillend bij een vergelijking tussen de verschillende geslachten. Zo is op basis van de data bijvoorbeeld te concluderen dat er grote verschillen bestaan tussen mannelijke en vrouwelijke scholieren bij de betrokkenheid bij gaming, mannelijke scholieren zijn significant meer en vaker betrokken zijn bij het spelen van online games dan vrouwelijke scholieren. Bij de betrokkenheid ten aanzien van Social Networking Sites en het Online bankieren blijkt geslacht minder van invloed te zijn.

Uit de resultaten rondom het slachtofferschap zijn ook een aantal conclusies te trekken. Zo is te concluderen dat het grootste aantal slachtoffers, op basis van de drie specifieke vormen van internetgebruik, via het online gamen gemaakt worden. Dit wordt op de voet gevolgd door Social Networking en vervolgens door Online Bankieren. Hierbij zorgen de Duitse mannelijke scholieren (met een slachtofferpercentage van 19,1%) voor een groot deel van het totale aantal slachtoffers van phishing via het online gamen en bestaat er een groot verschil tussen de mannen en vrouwen qua slachtofferschap. Bij de twee andere vormen van internetgebruik zijn er kleinere verschillen aanwezig in slachtofferschap tussen mannen en vrouwen (Zie tabel I).

Wat betreft de slachtofferpercentages zijn er ook verschillen ten aanzien van nationaliteit. Hoewel Duitse scholieren minder betrokken zijn met online gaming, zijn zij wel vaker slachtoffer van phishing via online gaming dan Nederlandse scholieren. Ook ten aanzien van phishing bij Social Networking en Online bankieren vielen er relatief meer slachtoffers in Duitsland dan in Nederland op basis van de onderzochte populatie. Een verklaring hiervoor werd niet gevonden in het huidige onderzoek, en zal onderzocht moeten worden in verdergaand onderzoek.

Ten aanzien van de relaties tussen het internetgedrag en het slachtofferschap van phishing zijn een aantal belangrijke relaties gevonden. De verwachting op basis van de theorie was dat een hogere mate van internet leidt tot een grotere kans op slachtofferschap. De resultaten van de regressieanalyse tonen aan dat het aantal uren internetgebruik per dag inderdaad in relatie staat met het slachtofferschap van phishing bij online gaming en online

banking, waarbij mensen die meer op het internet zitten meer kans hebben om slachtoffer te worden van phishing bij deze twee specifieke vormen van internetgebruik. Deze uitkomst strookt dus met de verwachtingen op basis van de theorie.

In de theorie werd ten aanzien van de frequentie waarin men een specifieke vorm van internetgebruik uitoefent een verwachting gemaakt dat mensen die vaker gamen, online bankieren of social networken meer kans op slachtofferschap van phishing zouden hebben. Zo zeiden Chhabra et al. (2011) dat het actief zijn op sociale netwerken de kans op slachtofferschap van phishing vergroot. Ten aanzien van deze vormen van slachtofferschap van phishing via gaming kan er op basis van de resultaten van de logistische regressie geconcludeerd worden dat de mate of frequentie waarin men games speelt relatie staat met het slachtofferschap van phishing via die specifieke vorm van internetgebruik. Bij de andere twee vormen van internetgebruik werden geen significante relaties gevonden. Hierbij valt te concluderen dat scholieren die vaker gamen een grotere kans lopen om daarbij slachtoffer te worden van phishing. Dit resultaat sluit aan bij de verwachtingen die werden gemaakt in de theorie ten aanzien van de frequentie van gaming. Gelijke verwachtingen ten aanzien van de frequentie waarin met social networked en online bankieren waren niet juist, er werder geen relaties werden gevonden ten aanzien van de andere twee vormen van internetgebruik, daar waar het wel verwacht werd.

Ook is er een significante relatie gevonden tussen het aantal e-mailadressen dat men bezit en het slachtofferschap van phishing via het spelen van online games. De verwachting was dat het bezitten van een groter aantal e-mail adressen leidt tot een hogere kans op slachtofferschap van phishing, zoals in de theorie werd beschreven. De significante relatie tussen het aantal e-mailadressen dat men bezit en het slachtofferschap van phishing via gaming toont daarbij aan dat het hebben van een groter aantal e-mailadressen de kans op het worden van slachtoffer van phishing via gaming vergroot. In de literatuur is een dergelijke relatie nog niet onderzocht, maar het past op basis van de theorie goed in het huidige kader rondom het slachtofferschap van phishing.

De verwachting in de theorie ten aanzien van het gebruik van de mobiele telefoon voor online bankieren en het aantal vrienden, of ‘’connecties’’, dat scholieren hebben invloed zou hebben op de kans op slachtofferschap van phishing. Hiervoor is geen significante relatie gevonden ten aanzien van het slachtofferschap van phishing. Er kan dus geconcludeerd worden dat deze factoren geen invloed hebben op het slachtofferschap bij phishing. Mijn verwachtingen ten aanzien van het gebruik van de mobiele telefoon en het aantal vrienden dat men heeft op social networks en dat het een grotere kans van slachtofferschap zou opleveren waren dus niet juist. Hoewel Rajalingam et al. (2012) zeggen dat deze extra gecreëerde gevoelige informatie op het internet kan leiden een groter slachtofferschap van phishing, kan dat in dit onderzoek niet bevestigd worden.

Een belangrijk resultaat in dit onderzoek is echter dat er tussen de drie verschillende variabelen van het slachtofferschap van phishing onderling ook significantie relaties bestaan. Hierover zijn in de theorie geen verwachtingen gemaakt, maar is het via de resultaten van het onderzoek aan het licht gekomen. Zo is, zoals in de resultaten (tabel III, IV, V) te zien is, het slachtofferschap van phishing bij online games onderling verbonden met het slachtofferschap via online bankieren en social networking. Daaropvolgend zien we bij het slachtofferschap van phishing via social networking en het slachtofferschap via online bankieren vergelijkbare onderlinge relaties. Uit deze onderlinge verbondenheid bij het

slachtofferschap van phishing valt te concluderen dat mensen die via de ene vorm van internetgebruik slachtoffer worden van phishing, ook een grotere kans hebben om slachtoffer van phishing te worden via de andere vorm van internetgebruik. Het is dus goed mogelijk dat een significant deel van de slachtoffers, binnen de drie specifieke vormen van internetgebruik, vertegenwoordigd wordt door een groep met dezelfde scholieren en daarmee dus via verschillende vormen van internetgebruik meerdere keren slachtoffer zijn geworden van phishing.

Ook zijn er demografische factoren die onder scholieren in relatie staan met het slachtofferschap van phishing. Tussen nationaliteit en het slachtofferschap van phishing werd hierbij dan ook een significante relaties gevonden. Ten aanzien van phishing bij online gaming en phishing bij SNS zijn er een aantal significante relaties gevonden met Nationaliteit. Hierbij tonen de resultaten aan dat de groep van slachtoffers van phishing bij deze vormen van internetgebruik in grotere mate door Duitse scholieren vertegenwoordigd wordt. Duitse scholieren lijken een grotere kans te hebben op het worden van slachtoffer van phishing bij online gaming en het gebruik van Social Networking Sites (SNS). Een mogelijke verklaring hiervoor werd niet gevonden in het huidige onderzoek, er zal dus vervolgonderzoek nodig zijn om een verklaring hiervoor te achterhalen.

Op basis van de gevonden significante relaties in de logistische regressieanalyse is ook te concluderen dat geslacht significant relateert aan het slachtofferschap van phishing. Bij alle drie de specifieke vormen van internetgebruik ten aanzien van het slachtofferschap van phishing werd een significante relatie gevonden met geslacht. Echter, zijn de richtingen van deze relaties wel verschillend. Waar bij online gaming en online bankieren de mannelijke scholieren meer kans hebben om slachtoffer te worden van phishing, hebben bij het slachtofferschap van phishing via social networking sites de vrouwelijke scholieren meer kans om daarbij slachtoffer te worden van phishing. Ten aanzien van het gebruik van social networking gaat de verwachting op dat vrouwen vaker slachtoffer schijnen te worden van phishing dan mannen, zoals Sheng et al. (2010) beweren. Echter kunnen we dit niet zeggen van de andere twee vormen van internetgebruik, waar het omgekeerd blijkt te zijn.

Wat betreft leeftijd werd er op basis van de theorie van Sheng et al. (2010) en het theoretisch kader van het huidige onderzoek verwacht dat jongere mensen vaker slachtoffer zouden zijn van phishing en dus dat leeftijd in relatie zou staan met het slachtofferschap van phishing. Echter kan op basis van de resultaten geconcludeerd worden dat, onder scholieren, hierbij in geen geval een significant verband bestaat met het slachtofferschap van phishing. De verwachtingen die eerder gemaakt zijn blijken niet correct te zijn op basis van een steekproef onder scholieren.

Samenvattend kan er dus geconcludeerd dat, onder scholieren, het aantal uren internetgebruik per dag, de frequentie waarin scholieren games spelen en actief zijn op SNS, het aantal e-mailadressen dat scholieren bezitten, de nationaliteit van een scholier en het geslacht van een scholier bepalende en bijdragende factoren zijn voor het slachtofferschap van phishing. Daarbij bestaat er een onderling verband tussen de verschillende vormen van slachtofferschap. Hierbij hebben mensen die slachtoffer zijn geworden van phishing via bijvoorbeeld online gaming, ook een grotere kans hebben om slachtoffer te worden van phishing bij de twee andere specifieke vormen van internetgebruik.

Discussie & Beperkingen

Een eerste punt voor discussie komt voort uit enkele opvallende resultaten. Ten eerste is er in de resultaten te zien dat slachtofferschap van phishing bij elke internetvorm hoger ligt in Duitsland dan in Nederland. Daarbij is er binnen de variabele die gemeten zijn, geen directe verklaring te vinden. Het zou kunnen zijn dat de awareness rondom phishing in Duitsland lager is, en de Duitse scholieren daarom, onbewust, risicovoller handelen. Een andere mogelijkheid is dat Duitse studenten minder bekwaam of ervaren zijn met het internet in het algemeen en daarom vaker slachtoffer worden. Zowel de ervaring op het internet als de awareness van phishing is niet gemeten dit onderzoek. Dit zou een verbetering kunnen zijn bij opvolgend onderzoek.

Naast dat de uitkomsten per land een discussiepunt zou kunnen zijn, zijn er ook wat merkwaardige resultaten gevonden bij de regressieanalyse. Zo zijn er verbanden gevonden tussen variabelen waarbij dat niet verwacht werd en anderzijds geen verbanden gevonden waar dat soms wel verwacht werd. Een voorbeeld hiervan de frequentie waarin met online bankiert. Men zou verwachten dat deze variabele, al dan niet positief of negatief, in relatie zou staan met het slachtofferschap van phishing via online gaming. Toch tonen de resultaten van de regressieanalyse dat er geen verband is gevonden ten aanzien van het slachtofferschap bij online bankieren.

Ook zijn er enkele resultaten gevonden die anders zijn dan de huidige literatuur beweerd. Zo tonen de resultaten van dit onderzoek bijvoorbeeld dat leeftijd geen verklaring kan bieden voor het slachtofferschap van phishing. Andere literatuur, besproken in het theoriedeel van dit onderzoek,toont wel een significante verband gevonden werden ten aanzien van het slachtofferschap van phishing. Daarnaast liggen de percentages van slachtofferschap hoger dan dat strookt procentuele schattingen die zijn gemaakt in de literatuur.

Een belangrijke beperking in dit onderzoek is dat de enquête enkel onder scholieren is afgenomen. Dit hebben we gedaan omdat wij ook enkel geïnteresseerd waren in deze bevolkingsgroep. Echter betekent dat wel dat de resultaten die gevonden zijn in dit onderzoek mogelijk niet representeerbaar zijn voor de gehele bevolking. Waar leeftijd onder scholieren volgens de resultaten niet uitmaakt voor het slachtofferschap, kan dit op basis van de gehele bevolking wel zo zijn. De leeftijdsverschillen zijn in de sample van dit onderzoek immers maximaal 8 jaar (11 t/m 19). Het zou dus mogelijk zijn dat bij een onderzoek over de gehele bevolking, leeftijd en opleidingniveau wel significant samenhangen met het slachtofferschap van phishing.

Het specifieke aan dit onderzoek onder scholieren is dan ook meteen een zwaktepunt. Omdat er specifiek naar één groep uit de gehele samenleving gekeken wordt, is het lastig om deze resultaten te generaliseren over de hele samenleving. De resultaten die gevonden zijn in dit onderzoek gelden dus mogelijk alleen onder scholieren. Een dergelijk onderzoek met een representatie van de gehele Duitse en Nederlandse bevolking zou mogelijke verschillen en overeenkomsten aan kunnen tonen met een huidig onderzoek. Dit zou dan ook een mogelijk onderwerp kunnen zijn voor vervolgend onderzoek in deze richting.

Daarnaast zijn scholieren een lastige doelgroep om te meten. Een mate van self-selection zou plaats gevonden kunnen hebben bij de afnamen van de data. Zo was er bij de datacollectie goed te zien dat bepaalde studenten interesse hadden in het onderzoek. Echter

was een andere groep scholieren waarbij veel minder, of min of meer met tegenzin, aan het onderzoek deel genomen werd. Sommige scholieren zouden bijvoorbeeld geïnteresseerder kunnen zijn doordat zij al eens slachtoffer zijn geweest van phishing en dat graag willen rapporteren. Daarbij bestaat dus een risico dat vooral zij die al eens slachtoffer zijn geweest van phishing sneller meedoen aan het onderzoek en dus, ten aanzien van de gehele populatie, oververtegenwoordigd zouden zijn in de data. Een ander discussiepunt is de ‘’vervuiling’’ in de data. Sommige scholieren zullen wellicht het onderzoek moedwillig gesaboteerd hebben door niet kloppende data in te voeren. Hierdoor kan het zijn dat de gemeten waarden mogelijk afwijken van de werkelijke waarden. De oplossing voor het self-selection probleem zou een gerandomiseerd onderzoek zijn. Echter, wegens geld- en tijdgebrek was dit niet mogelijk voor het huidig onderzoek. De oplossing voor het probleem van de vervuiling van de data is data cleaning, welk wij op zo een goed mogelijke manier hebben geprobeerd uit te voeren.

Ook is het mogelijk dat de data cleaning de resultaten enigszins kan hebben beïnvloedt. Omdat we de dataset zo goed mogelijk hebben proberen schoon te maken, kan het ook zijn dat er cases verloren zijn gegaan die eigenlijk niet hadden moeten worden verwijderd. De scheidingslijn tussen een ‘’vervuilde’’ case en normale cases is dan ook niet te concretiseren omdat elke case anders is.

Advies voor vervolgonderzoek

Mijn advies voor vervolgonderzoek is de verbreding van de slachtoffercategorieën binnen phishing. Waar in dit onderzoek alleen gekeken is naar specifiek slachtofferschap binnen Gaming, Social Networking en Online Bankieren, zijn er ook nog vele andere sectoren waar phishing plaats vindt en welke dus onderzoek vereisen. Ook het aantal afhankelijke variabelen zou vergroot kunnen worden, aangezien er nog veel meer variabelen van internetgedrag het slachtofferschap zouden kunnen verklaren. Enkele voorbeelden hierbij zouden bijvoorbeeld zijn: Het aantal jaren ervaring met het internet, de technische kennis van de respondent en in welke mate men op de hoogte is van phishing. Daarnaast zou phishing bekeken kunnen worden aan de kant van de dader. Het is aan te raden vervolgonderzoek te doen naar de vragen: “Welke factoren leiden tot het phishen?” ,“Wat is de drijfveer voor de cybercriminelen die phishen en hoe zouden deze mogelijk verkleind kunnen worden? “Door het tijdsbestek waarin gewerkt moest worden, kon geen onderzoek naar de vragen gedaan worden. Tevens zouden deze antwoorden een extra aanvulling zullen zijn op de wetenschappelijke literatuur.

Een ander interessant onderzoeksaspect om te onderzoeken zijn de verschillen in slachtofferpercentages tussen de verschillende landen. Uit de data van het huidige onderzoek blijkt dat scholieren in Duitsland relatief vaker slachtoffer zijn geworden dan scholieren in Nederland. Waar dit precies door komt, is niet duidelijk geworden uit dit onderzoek. Dit komt mogelijk door het ontbreken van niet-getoetste verklarende zoals bijvoorbeeld het aantal jaren ervaring met het internet of de aandacht die er is besteed op school aan onderwerpen zoals phishing. Echter zijn deze variabelen slechts vermoedens over wat invloed zou kunnen hebben op de verschillen tussen Nederland en Duitsland.

Het design van het onderzoek is ook nog te verbeteren, zo zouden achteraf gezien mondelinge interviews wellicht betere data opgeleverd hebben. Echter, omdat er in dit

onderzoek gewerkt moest worden met een strikte tijdslimitiet en een groot aantal respondenten, was dit geen optie. Mondelinge interviews zijn namelijk veel tijdrovender dan een online enquête. Ook is het probleem van self-selection op te lossen door bijvoorbeeld alle scholieren, na overleg, verplicht mee te laten doen aan het onderzoek. Deze verbeteringen kosten echter wel veel extra tijd en geld, iets waartoe de mogelijkheid er wellicht niet altijd is.

Referentielijst

Abliz, M. (2011). Internet Denial of Service Attacks and Defense Mechanisms. *University of Pittsburgh Technical Report*.

AIC. (2006). Acquiring high tech crime tools' High Tech Crime Brief. *Australian Institute of Criminology 13*, 1-2.

APWG. (2013a). Origins of the word "Phishing" Retrieved May 8th, 2013, from http://www.antiphishing.org/word_phish.html.12

APWG. (2013b). Phishing Activity Trends Report 4th Quarter of 2012: Unifying the Global Response To Cybercrime. *Anti Phishing Working Group*.

AusCERT. (2005). Australian 2005 Computer Crime and Security Survey.

Aycock, J. (2009). *Computer Viruses and Malware*: Springer.

Babbie, E. (2010). *The Practice of Social Research* (12th edition ed.): Wadsworth.

Barosso, D., Bartle, R., Chazeran, C., de Zwart, M., Doumen, J. M., Gorniak, S., . . . Thumann, M. (2008). ENISA Position Paper: Virtual Worlds, Real Money Security and Privacy in Massively-Multiplayer Online Games and Social and Corporate Virtual Worlds. *ENISA Position Paper 1 ENISA*.

Biesterbos, P. (2011). Fraude met internetbankieren neemt sterk toe, from http://www.elsevier.nl/Economie/nieuws/2011/11/Fraude-met-internetbankieren-neemt-sterk-toe-ELSEVIER322254W/

Boyd, D. M., & Ellison, N. B. (2008). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication, 13*, 210–230.

Brody, R., Mulig, E., & Kimball, V. (2007). Phishing, Pharming and Identity Theft. *Academy of Accounting and Financial Studies Journal, 11*(3).

Charoen, D. (2011). Phishing: a Field Experiment. *International Journal of Computer Science and Security (IJCSS), 5*(2).

Chhabra, S., Aggarwal, A., Benevenuto, F., & Kumaraguru, P. (2011). Phi.sh/$oCiaL: The Phishing Landscape through Short URLs. *CEAS'11*.

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology, 2*(1), 308–333.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. *CHI 2006 Proceedings*.

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*, 73-80.

Duan, Z., Yuan, X., & Chandrashekar, J. (2006). Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates. *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*. Eurostat. (2012). Internet access and use in 2012 More than half of internet users post messages to social media……and over 60% read news online Retrieved July 5th, 2013, from http://europa.eu/rapid/press-release_STAT-12-185_en.htm

Grabosky, P., & Smith, R. G. (2001). Telecommunication fraud in the digital age' in Wall DS *Crime and the internet*.

Hegt, S. (2008). Analysis of Current and Future Phishing Attacks on Internet Banking Services. *Technische Universiteit Eindhoven*.

Hoffman, D. L., Kalsbeek, W. D., & Novak, T. P. (1996). Internet and Web Use in the United States: Baseline for Commercial Development. *Communications of the ACM*.

Hutchings, A., & Hayes, H. (2009). Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'? *Current Issues in Criminal Justice*.

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social Phishing. *Communications of the ACM, 50*(10), 94-100.

Jaishankar, K. (2008). Identity related crime in the cyberspace: Examining phishing and its impact. *International Journal Of Cyber Criminology, 2*(1), 10-15.

Jakobsson, M., & Myers, S. (2007). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*.

Krendl, K., Broihier, M., & Fleetwood, C. (1989). Children and computers: Do sex -related differences persist? *Journal of Communications, 39*, 85-93.

Ledford, J. (2012). Spear Phishing: Identity Theft's New Black, from http://idtheft.about.com/od/theftmethods/a/Spear_Phishing.htm

Litan, A. (2004). Phishing Victims Likely Will Suffer Identity Theft Fraud. *Gartner, Inc*.
Microsoft. (2012). An in-depth perspective on software vulnerabilities and exploits, malware, potentially unwanted software, and malicious websites. *Microsoft Security Intelligence Report, 14*.

Ollmann, G. (2007). The Phishing Guide. Understanding & Preventing Phishing Attacks. *IBM Internet Security Systems*.

Popcenter.org. (2013a). Situational Crime Prevention from http://www.popcenter.org/about/?p=situational

Popcenter.org. (2013b). Use the problem analysis triangle, from http://www.popcenter.org/learning/60steps/index.cfm?stepnum=8

Rajalingam, M., Alomari, S. A., & Sumari, P. (2012). Prevention of Phishing Attacks Based on Discriminative Key

Point Features of WebPages. *International Journal of Computer Science and Security (IJCSS), 6*(1).

Rhee, M. J. (2013). *Wireless Internet Mobile Security*: Wiley.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *CHI 2010*.

Shi, J., & Saleem, S. (2012). Phishing. *University of Arizona*.

Tally, G., Thomas, R., & Van Vleck, T. (2004). Anti-Phishing: Best practices for institutions and consumers. *McAfee Research Technical Report*.

Tanase, M. (2003). IP Spoofing: An Introduction, from http://www.symantec.com/connect/articles/ip-spoofing-introduction

Teo, T. S. H., & Lim, V. K. G. (2000). Gender differences in internet usage and task preferences. *Behaviour & Internet Technology, 19*(4), 283-295.

Trusteer. (2009). Measuring Effectiveness of Wild Phishing Attacks. Retrieved from http://www.opensourceintelligence.eu/ric/doc/Phishing-Statistics-Dec-2009-FIN.pdf

Unlu, S. A., & Bicakci, K. (2010). NoTabNab: Protection Against The "Tabnabbing Attack". *TOBB University of Economics and Technology Ankara, Turkey*.

Wortley, R., & Mazerolle, L. G. (2008). *Environmental Criminology and Crime Analysis*: Willan Publishing.

Appendix: Research Tool Victimization of Phishing (Leemreize, J.P.)

G.1 Victimization of phishing (16 items)					
Definition	*Definition of phishing: ''a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party'' (Jagatic, Johnson, Jakobsson, & Menzer, 2005)*	***Definitie van phishing: "een techniek binnen de cybercrime waar een persoon op frauduleuze wijze gevoelige informatie probeert los te weken van een slachtoffer, door zich voor te doen als een betrouwbare derde partij." (Jagatic, Johnson, Jakobsson, & Menzer, 2005)***			
	**Sensitive information is for example: your loginname, your passwords, your bankaccounts, your name, where you live, your e-mail, your phonenumber etc.*				
				Answer Categories	Antwoordopties
	When people play online games such as World of Warcraft, Battlefield, Runescape or Habbohotel, sometimes other people or websites try to get your information of your gaming account.	*Wanneer mensen online games spelen zoals World of Warcraft, Battlefield, Runescape of Habbohotel, gebeurd het wel eens dat mensen je proberen te misleiden om gevoelige informatie, zoals je inlognaam en wachtwoord, van je gaming account ze te geven.*			

G.1.1	How often do you play online games?	Hoe vaak speel je online games?		Never / a few times a year / a few times a month / a few times a week / every day	Nooit / een paar keer per jaar / een paar keer per maand / een paar keer per week / elke dag
G 1.2	Has, in the past 12 months, someone ever tricked you into giving your login information or other sensitive information of your gaming account?	Heeft, in de laatste 12 maanden, een vreemde je wel eens misleid zodat je je login, wachtwoord of andere gevoelige informatie van je gaming account gaf?		Yes/No	Ja/Nee
G 1.3	How often did this happen?	Hoe vaak is dit gebeurd?		Never / Once / Twice / More than twice	Nooit / Een keer / Twee keer / Meer dan twee keer
G.1.4	If yes, what happened? (I.E Did you loose money?)	Als dit je overkomen is, hoe is dat gebeurd? (En ben je bijvoorbeeld spullen kwijtgeraakt?)		Open Question	Open Vraag
	When people use social networking sites such as Facebook, Hyves, Google+ or MySpace, there are sometimes people that try to get your login information or other sensitive information from you.	*Wanneer mensen gebruik maken van sociale netwerk sites zoals Facebook, Hyves, Google+ of MySpace, gebeurd het wel eens dat mensen je via die sites proberen te misleiden om gevoelige informatie aan ze te geven.*			
G.1.5	How often do you use social networking sites (Such as Facebook, Hyves, MySpace etc.?)	Hoe vaak gebruik je sociale netwerk sites? (Zoals Facebook, Hyves, Myspace etc)		Never / a few times a year / a few times a month / a few times a week / every day	Nooit / een paar keer per jaar / een paar keer per maand / een paar keer per week / elke dag
G.1.6	Has someone ever tricked you into giving your account-, login- or any other sensitive information via social networking sites such as Facebook, Hyves, Google+ or MySpace?	Ben je, in de laatste 12 maanden, wel eens op bijvoorbeeld Facebook, Hyves of MySpace door iemand misleid zodat je account-login- of andere gevoelige informatie aan hem/haar gaf?		Yes/No	Ja/Nee

G.1.7	How often did this happen?	Hoe vaak is dit gebeurd?		Never / Once / Twice / More than twice	Nooit / Een keer / Twee keer / Meer dan twee keer
G.1.8	If yes, what happened?	Als dit je overkomen is, hoe is dat gebeurd?		Open Question	Open Vraag
	When people use online banking, like iDeal, Paypal or other ways of doing online transactions, they sometimes get fake e-mails from people who try to get your banking details, login, passwords or other sensitive information.	*Wanneer mensen gebruik maken van online bankieren, zoals iDeal, Internetbankieren of PayPal, krijgen mensen wel eens nep e-mails van mensen of websites, waar geprobeerd wordt om je bankinformatie, login informatie of andere informatie van je los te krijgen.*			
G.1.9	How often do you use online banking?	Hoe vaak gebruik jij online bankieren?		Never / a few times a year / a few times a month / a few times a week / every day	Nooit / een paar keer per jaar / een paar keer per maand / een paar keer per week / elke dag
G.1.10	Has someone ever tricked you, by for example a fake e-mail, into giving your banking details such as your login and/or password for online banking?	Heeft, in de laatste 12 maanden, iemand je wel eens misleid, bijvoorbeeld met een valse e-mail, om je login en/of paswoord of andere gevoelige informatie over je online bank account te vertellen?		Yes/No	Ja/Nee
G.1.11	How often did this happen?	Hoe vaak is dit gebeurd?		Never / Once / Twice / More than twice	Nooit / Een keer / Twee keer / Meer dan twee keer
G.1.12	If yes, what happened?	Als dit je overkomen is, hoe is dat gebeurd?		Open Question	Open Vraag

	When people shop online, sometimes people or websites try to trick you into giving them personal- and banking details, logins and passwords and other sensitive information.	*Wanneer mensen online winkelen gebeurd het wel eens dat mensen of websites je proberen te misleiden om aan hun jouw gevoelige informatie te geven, zoals je persoonlijke en bankgegevens.*			
G.1.13	How often do you shop online?	Hoe vaak winkel jij online?		Never / a few times a year / a few times a month / a few times a week / every day	Nooit / een paar keer per jaar / een paar keer per maand / een paar keer per week / elke dag
G.1.14	Has someone ever tricked you into giving personal or banking details, or login information when you were shopping online?	Heeft iemand of iets je, tijdens het online winkelen, wel eens misleid om je persoonlijke informatie en/of login informatie prijs te geven?		Yes/No	Ja/Nee
G.1.15	How often did this happen?	Hoe vaak is dit gebeurd?		Never / Once / Twice / More than twice	Nooit / Een keer / Twee keer / Meer dan twee keer
G.1.16	If yes, what happened?	Als dit je overkomen is, hoe is dat gebeurd?		Open Question	Open vraag
G.2 Risky online behaviour (3 items)					
G.2.1	Do you use your mobile phone for online banking?	Gebruik je wel eens je mobiel om online mee te betalen?		Yes/No	Ja/Nee
G.2.2	What is an estimate number of online transactions you do in a month? (This include iDeal payments, online purchases, mobile banking etc.)	Wat is een schatting van het aantal online transacties die je maakt per maand? (Hier vallen ook iDeal betalingen, online aankopen, en overboekingen via de mobiel onder)		x times a month	x keer per maand
G.2.3	How many e-mail accounts do you have?	Hoeveel e-mailadressen heb je?		x e-mail accounts	x e-mail adressen