Social engineering: digitale fraude en misleiding

Een meta-analyse van studies naar de effectiviteit van interventies

Jan-Willem Bullée en Marianne Junger*

Onderzoek toont aan dat online criminaliteit in de afgelopen jaren een grote bedreiging is gaan vormen voor zowel individuen (Henson e.a. 2016; Internet Crime Complaint Center 2018; Marinos & Sfakianakis 2012; Reep-van den Bergh & Junger 2018) als organisaties (Klahr e.a. 2017). Veel online gepleegde delicten bevatten een element van fraude en misleiding, ofwel '*social engineering*' (Blakeborough & Correia 2017; Verizon Risk Team 2018). Aanvallers gebruiken misleiding, bedrog en andere overtuigingstechnieken als aanvalstactiek om slachtoffers gevoelige informatie te laten delen of kwaadwillige acties uit te laten voeren (Gupta e.a. 2011). Door slimme trucs proberen zij iets van je te verkrijgen, zoals persoonlijke informatie en logininformatie, maar uiteindelijk komt het meestal neer op: geld.

Social engineering wordt beschouwd als een van de grootste cybergevaren, omdat mensen erg bevattelijk blijken te zijn voor misleiding. Social-engineeringaanvallen lijken op het eerste gezicht legitiem en ongevaarlijke berichten of verzoeken te betreffen. De computergebruiker heeft vaak niet door dat hij slachtoffer is van een dergelijke aanval (Hadnagy & Wilson 2010). Daarom wordt vaak gesteld dat de mens de zwakste schakel is in informatiebeveiliging (Happ e.a. 2016; Schneier 2000).

Er zijn eindeloos veel mogelijkheden voor social engineers. De enige beperking is de verbeelding van de aanvallers. Het succes van social engineering hangt vooral af van de 'kwaliteit' en de wijze waarop zij

* Dr. J.-W. Bullée is werkzaam bij Awareways, Computer & Network Security. Hij promoveerde in 2017 op het proefschrift *Experimental social engineering* aan de Universiteit Twente. Prof. dr. M. Junger is hoogleraar Cyber Security en Business Continuity aan de Universiteit Twente.

doi: 10.5553/JV/016758502020046002009

wordt uitgevoerd. De resultaten kunnen dan ook erg variëren. In de context van e-mailphishing loopt het slagingspercentage uiteen van bijna 0% tot meer dan 80% (Sokol e.a. 2017; Vishwanath 2015; Wright e.a. 2014; Yang e.a. 2017). In persoonlijke verhalen vertellen professionele *penetration testers*[1] vaak dat de kans dat zij ergens binnenkomen nagenoeg 100% is.

Vandaar dat het beperken van de kans op succes zo belangrijk is. Echter: mensen leren weerstand te bieden is niet eenvoudig. Daarnaast is er nog niet veel ervaring met de effectiviteit van interventies opgedaan. Sommige auteurs zijn negatief over het mogelijk succes: Bada en collega's (2015) gaven hun onderzoek de titel mee 'Cyber security awareness campaigns: Why do they fail to change behaviour?' Een gefundeerd oordeel over de effectiviteit van interventies die social engineering moeten bestrijden, is er niet. Om hierop een antwoord te vinden hebben wij een overzicht van de literatuur gemaakt en een meta-analyse verricht. Onze onderzoeksvraag luidt: welke vormen van interventies en specifieke elementen hierin, om social engineering tegen te gaan, zijn het meest succesvol?

Hieronder geven wij een overzicht van de relevante literatuur en beschrijven wij beknopt de methode en de resultaten van de meta-analyse uitgevoerd op deze literatuur. Voor meer gegevens over de literatuur en meta-analyse verwijzen wij naar Bullée en Junger (2020a; 2020b).

Methodiek van de meta-analyse

Om relevante studies op te sporen is de Scopus-database geraadpleegd. Vervolgens is voor alle zoekresultaten gekeken of deze bruikbaar waren. De zoekopdracht leverde 418 resultaten op. Na het controleren op geschiktheid, bleven er 19 studies over voor de analyse. Een studie kan een of meerdere interventies testen. In totaal zijn er 37 interventies gevonden, en voor iedere interventie is de effectgrootte berekend. Deze maat geeft het verschil aan in kwetsbaarheid tussen proefpersonen in de controle en die in de interventiegroep. Specifiek is Cohen's *d* (van 'difference') gebruikt; deze maat is het verschil

1 Penetration testers zijn ethische hackers die een geautoriseerde gesimuleerde cyberaanval ('pentest') op een computersysteem uitvoeren om de beveiliging van het systeem te evalueren.

doi: 10.5553/JV/016758502020046002009

Tabel 1 Beoordeling van effectomvang volgens Cohen (2013)

Categorisering	Effectgrootte
Klein	0,2 en lager
Middelgroot	0,5
Groot	0,8 en groter

tussen de twee gemiddelden gedeeld door de standaardafwijking (Cohen 2013). Voor een indeling naar de omvang van het effect, zie Tabel 1.

De studies zijn beschreven aan de hand van een aantal kenmerken:
1. de context van de studies;
2. de karakteristieken van de interventie;
3. de kenmerken voor de evaluatiestudie.

Effectiviteit van interventies

In totaal zijn 19 studies in de analyse betrokken, met gezamenlijk N=23.146 proefpersonen en 37 observaties (d.w.z. effectgrootten). De gemiddelde effectgrootte van een interventie om social engineering tegen te gaan, is 0,54 (95% CI=[0,359, 0,719], I^2=89,31%, 37 studies). Dit wordt beschouwd als een middelgroot effect (Cohen 2013). De I^2-statistiek is een maat voor heterogeniteit, de variantie in een meta-analyse (Higgins e.a. 2003). Voor een overzicht van de effectgrootte per studie wordt verwezen naar Bullée en Junger (2020b).

Type social engineering

De geselecteerde studies maakten gebruik van verschillende typen schijnaanvallen om de vaardigheid van hun deelnemers te testen. Een relatief groot deel van de interventies was gericht op phishing en daarom gebruikten deze studies e-mail als 'schijnaanval'. Daarnaast is gebruik gemaakt van persoonlijk contact (face to face), de telefoon, sms of een phishingwebsite. De wijze waarop interventies werden getest, heeft impact op de effectiviteit (F(4, 32)=5,53, p=,002). Interventies die via sms of een website werden getest, gingen gepaard

doi: 10.5553/JV/016758502020046002009

met relatief grote effecten op slachtofferschap (respectievelijk EG=1,37 en 1,25).[2] Interventies die werden getest via e-mail, face to face of de telefoon werden geassocieerd met kleinere effecten (respectievelijk EG=0,35, 0,30 en 0,27).

Preslachtofferschap

Interventies en trainingsmateriaal hebben tot doel het bewustzijn te vergroten en gedrag te veranderen met betrekking tot een bepaald onderwerp. Het ingrijpen bij iemand die het gewenste gedrag al uitvoert, is echter verspilling van tijd en middelen. In plaats daarvan is het efficiënter om de interventie alleen te verstrekken aan degenen die deze nodig hebben. Daartoe dient '*pre-victimisation*': alleen gebruikers die 'vallen' voor de aanval wordt een interventie aangeboden. Daarnaast dient preslachtofferschap bij een schijnaanval om een gebruiker te motiveren: als ze voor de social-engineeringaanval zijn gevallen, zullen ze worden gemotiveerd om te leren hoe ze dit in de toekomst kunnen voorkomen. Daarom gebruiken securityonderzoekers vaak een tweefasebenadering. Die bestaat eruit dat alle proefpersonen bijvoorbeeld een nepphishingmail ontvangen. Vervolgens worden degenen die het gewenste gedrag hebben uitgevoerd (bijvoorbeeld niet op de link klikken) 'met rust gelaten'. Degenen die slachtoffer zijn geworden (bijvoorbeeld op de link hebben geklikt), worden doorverwezen of uitgenodigd om deel te nemen aan een bewustmakingscursus over social engineering (Kumaraguru e.a. 2007a).
De combinatie van preslachtofferschap met een interventie wordt een 'embedded' training of interventie genoemd. Verschillende onderzoeken toonden aan dat deze previctimisatie een relevant aspect was van interventies in zowel laboratoriumonderzoeken (Kumaraguru e.a. 2009; Mayhorn & Nyeste 2012; Sheng e.a. 2007) als reallife (Kumaraguru e.a. 2008). In tegenstelling tot de verwachting was het effect van ingebedde interventies kleiner dan het effect van niet-ingebedde interventies ($Q(1)=9{,}38$, $p=,002$). De gemiddelde effectgrootte van ingebedde interventies was 0,18 en van de niet-ingebedde interventies 0,70.

2 Wanneer wordt gesproken over effecten, zijn het effecten in de verwachte richting, namelijk dat de interventie leidt tot minder slachtofferschap. Zo niet, dan wordt dit expliciet vermeld.

doi: 10.5553/JV/016758502020046002009

Modaliteit van de interventie

Interventies werden aangeboden op verschillende wijzen: soms werd een gebruiker getraind tijdens een gesprek, of er werd een fysiek document verstrekt om kennis of online waarschuwingen over te dragen om te informeren over potentieel gevaar. Soms is de training interactief, bijvoorbeeld wanneer gebruikers in een klaslokaal communiceren met een trainer (Mayhorn & Nyeste 2012; Lastdrager e.a. 2017). Er is gesuggereerd dat het gebruik van interactieve antiphishingtraining een effectievere manier is om gebruikers in staat te stellen phishing-URL's te identificeren dan het gebruik van passieve zelfstudies over phishing (Arachchilage e.a. 2016; Davinson & Sillence 2010; Kumaraguru e.a. 2010; Mayhorn & Nyeste 2012; Sheng e.a. 2007). Andere 'trainingsmodaliteiten' bestonden uit het verzenden van nepphishingmails naar gebruikers: de eerste antiphishingstudies bevatten geen opleidingsonderdeel (Dodge e.a. 2007). In plaats daarvan testten deze onderzoeken het effect van een 'ik heb je'-moment. Wanneer een gebruiker slachtoffer werd van een nepphishingmail, ontving deze de melding dat hij 'slachtoffer' was geworden. Het idee is dat medewerkers beseffen hoe kwetsbaar ze zijn en daarom in de toekomst voorzichtiger handelen. Door het herhaaldelijk verzenden van nepphishingmails kan het aantal slachtoffers geleidelijk worden verminderd (Dodge e.a. 2007; Aburrous e.a. 2010).
De modaliteit maakt uit voor de effectiviteit ($F(2, 34)=3{,}57$, $p={,}039$). Interventies die mondeling werden gepresenteerd of gebruik maakten van een interactieve inhoud hadden een relatief groot effect (EG=1,00 en 0,94). Degenen die alleen tekst gebruikten, hadden een kleiner effect (EG=0,36).

Priming op gevaar

Mensen reageren vaak sneller op bepaalde tekens, woorden of gewaarwordingen als zij deze eerder hebben waargenomen (Dolan e.a. 2010; Kenrick e.a. 2005). In de fysieke wereld steunt veel onderzoek op het bestaan van zogeheten *priming*-effecten (Cameron e.a. 2012). Online hebben verschillende interventies ook gebruik gemaakt van vormen van priming (Acquisti e.a. 2012; Grazioli 2004; Parsons e.a. 2015). Zo informeerden Stockhardt en collega's (2016) en Parsons en collega's (2015) van tevoren dat de interventie over phishing ging. Acquisti en

doi: 10.5553/JV/016758502020046002009

collega's (2012; niet in de meta-analyse) 'primeden' respondenten door een verschil in lay-out van de website, 'slordig/deviant' versus 'netjes/professioneel'. Maar de resultaten laten niet altijd positieve effecten zien (Sundar e.a. 2013; Grazioli & Wang 2001). Over het algemeen lijken de resultaten niet overtuigend over de impact van priming in een online context. In onze meta-analysestudie bleek dat interventies die gebruik maakten van priming effectiever waren (EG=1,01) dan interventies die geen gebruik maakten van priming (EG=0,38; Q(1)=10,42, p=,001).

Waarschuwing voor gevaar (warning)

Waarschuwingen zijn een directere manier om een boodschap over te brengen dan priming. Traditionele offline waarschuwingen zijn succesvol geweest in het beïnvloeden van gedrag (Argo & Main 2004; Wogalter e.a. 2012). Richtlijnen voor adequate offline waarschuwingen zijn samengevat door Wogalter en collega's (2012). Waarschuwingen kunnen gebruikers in beginsel ook helpen zich online veiliger te gedragen; maar veel gebruikers pasten hun gedrag echter niet aan wanneer geldbeloningen in het geding waren (Barth e.a. 2019; Kirlappos & Sasse 2012; Christin e.a. 2011). In de huidige studie vinden wij dat waarschuwingen, alleen of in combinatie met een training, geen invloed hadden op het effect van een interventie (EG (F(2, 34)=0,17, p=,848).

Focus van de inhoud op de interventie

De focus van interventies varieert sterk. Phishingmails bevatten vaak links naar kwaadaardige websites. De meeste gebruikers zijn echter niet op de hoogte van de structuur van URL's en domeinnamen (Herzberg & Jbara 2008). Het gevolg is dat oplichters er vaak in slagen om gebruikers ertoe te verleiden op deze links te klikken. Dienovereenkomstig richten veel antiphishingspellen zich op het herkennen van phishing-URL's. Andere antiphishinginterventies leggen gebruikers enkele meer algemene kenmerken van phishingmails uit. Deze worden bijvoorbeeld beschreven als:

1. Phishingmails vragen vaak om persoonlijke informatie.
2. Phishingmails bevatten vaak een gevoel van urgentie.

doi: 10.5553/JV/016758502020046002009

3. Bij phishingmails komen vaak het e-mailadres van de afzender in het veld 'Van' en de bedrijfsnaam niet overeen.
4. Phishingmails bevatten vaak een bedreiging om een reactie te stimuleren.
5. Phishingmails bevatten vaak verkeerd gespelde woorden, vreemde spaties of slordige grammatica.
6. Phishingmails bevatten vaak links naar phishingwebsites.
7. Door met de muis over een link in een e-mail te bewegen wordt de gekoppelde URL onthuld (Downs e.a. 2006).

Een probleem bij het toepassen van deze kenmerken is dat phishingmails veranderen: ze worden steeds geavanceerder en gepersonaliseerde *spearphishing* maakt het ook moeilijker om ze te herkennen (Bullée e.a. 2017).

De focus van de interventie hangt significant samen met de effectgrootte ($F(5, 31)=3{,}84$, $p={,}008$). Interventies die gericht waren op de URL werden geassocieerd met een groot effect (EG=1,19), interventies gericht op cybercriminaliteit in het algemeen hadden een middelgroot effect (EG=0,60). Interventies gericht op social engineering en interventies gericht op de inhoud van een e-mail hadden een klein tot middelgroot effect (EG=0,34 en 0,34). Interventies die gericht waren op zowel de URL als de e-mail hadden een klein effect (EG=0,28). Tot slot werden de overige interventies geassocieerd met een middelgroot effect (EG=0,52).

Technische aspecten van een interventie

De meeste interventies waren gericht op mensen, omdat mensen informatie kunnen onthullen en kwetsbaar zijn voor aanvallen. Sommige interventies bouwen echter technische tegenmaatregelen in als extra beveiliging. Gebruikers kunnen deze niet omzeilen, ook niet als ze dat willen. Omdat slechts één interventie een dergelijke technische component had, namelijk Margulies en Herzberg (2013), kunnen we hierover geen uitspraken doen.

Formaat van de interventies

Interventies zijn ontwikkeld in veel verschillende formaten. Zo werden antiphishinginterventies aangeboden door gebruikers een sms-bericht

doi: 10.5553/JV/016758502020046002009

te sturen, of een stripverhaal, een combinatie van een stripverhaal en tekst of een spel te geven. Een strip lijkt bijvoorbeeld effectiever dan een tekst met grafische elementen (Kumaraguru e.a. 2007b).
Twee grootschalige reallife-antiphishingstudies onderzochten het effect van ingebedde trainingen (Kumaraguru e.a. 2008; Caputo e.a. 2014). De ene studie gebruikte een cartoon (Kumaraguru e.a. 2008), de andere studie een tekst (Caputo e.a. 2014). De inhoud van de boodschap was vergelijkbaar. De cartoon (met weinig woorden) verbeterde het gebruikersgedrag binnen het bedrijf (Kumaraguru e.a. 2008). De tekst (met veel woorden) verhinderde echter niet dat werknemers het slachtoffer werden van phishing (Caputo e.a. 2014). Er zijn ook spellen ontwikkeld, meestal als een meer uitgebreide vorm van antiphishingtraining. Gaming vergroot de motivatie van gebruikers om te leren (Sheng e.a. 2007). Het positieve effect van leren door gamen wordt bevestigd in de leerwetenschap (Clark & Mayer 2016). Het meest geteste antiphishingspel is Anti-Phishing Phil (Arachchilage e.a. 2016; Davinson & Sillence 2010; Kumaraguru e.a. 2010; Mayhorn & Nyeste 2012; Sheng e.a. 2007). Deze game leert gebruikers onderscheid te maken tussen legitieme URL's en phishing-URL's. De belangrijkste boodschap van het spel is om aandacht te besteden aan URL's; aangezien dit goede indicatoren zijn voor phishing. Phil, het hoofdpersonage in het spel, krijgt punten wanneer hij legitieme wormen eet (d.w.z. URL's), terwijl punten worden afgetrokken wanneer Phil slechte wormen eet. Het spel bestaat uit vier ronden en elke ronde begint met een korte uitleg met antiphishingadvies. Daarnaast bevat de training voorbeelden en oefenvragen (Sheng e.a. 2007). De Anti-Phishing Phil-game is in verschillende onderzoeken getest (Arachchilage e.a. 2016; Davinson & Sillence 2010; Kumaraguru e.a. 2010; Mayhorn & Nyeste 2012; Sheng e.a. 2007). Meer recentelijk is er een game ontwikkeld voor smartphones (Arachchilage & Cole 2011). De meeste antiphishingexperimenten met games lieten positieve resultaten zien bij het leren van gebruikers om phishingaanvallen te identificeren. Het is echter moeilijk om het exacte effect van antiphishingspellen te bepalen in vergelijking met trainingsinterventies omdat veel van de antiphishingspellen zijn getest in kleinschalige pilotstudies (bijv. Sheng e.a. 2007; Yang e.a. 2012).
In onze meta-analyse vonden wij echter geen statistisch significant effect van het interventieformaat op een afname van slachtofferschap ($F(4,32)=2,57$, $p=,057$).

doi: 10.5553/JV/016758502020046002009

Gebruik van tips

Verschillende interventies gaven tips of een specifieke aanbeveling aan gebruikers. Gebruikers kregen onder meer de volgende tips (Kumaraguru e.a. 2007b, p. 75):
– Klik nooit op links in e-mails.
– Typ het websiteadres in de webbrowser.
– Zoek en bel zelf de klantenservice.
– Geef nooit persoonlijke informatie.

In de meta-analyse bleek het geven van tips geen effect te hebben (F(2, 34)=0,18, p=,837).

Intensiteit van de interventie

Sommige interventies waren vrij eenvoudig en sommige waren relatief uitgebreid. Het lijkt plausibel dat intensievere interventies leiden tot sterkere effecten en meer impact op de lange termijn; maar vermoedelijk zijn deze ook meer tijdrovend, moeilijker te implementeren en duurder. Daarom verdient een eenvoudige maar effectieve interventie in het algemeen de voorkeur in termen van kosteneffectiviteit. Intensiteit bleek inderdaad van belang voor de effectgrootte (F(2, 34)=3,60, p=,038). Interventies met een hoge intensiteit hadden een groot tot zeer groot effect (EG=0,97), terwijl interventies met een lage of gemiddelde intensiteit een klein tot middelgroot effect hadden (EG=0,41 en 0,34).

Kenmerken van de evaluatiestudie onderzoeksmethode

In de vorige paragraaf zijn de kenmerken besproken van interventies die potentiële slachtoffers moeten helpen social engineering te weerstaan. Maar de wijze waarop het onderzoek is uitgevoerd, kan ook impact hebben op onderzoeksresultaten.

Langetermijneffecten van de interventie

Ongeacht het onderzoeksdesign en de inhoud of de kwaliteit van de training, blijkt dat het behouden van opgedane kennis moeilijk is voor

doi: 10.5553/JV/016758502020046002009

gebruikers. Sommige studies testten het bewaren van kennis na zestien dagen (Alnajim & Munro 2009), vier weken (Lastdrager e.a. 2017) of een paar maanden (Canova e.a. 2015; Caputo e.a. 2014). De meta-analyse laat zien dat de tijd tussen het verstrekken van de interventie en het testen van de kwetsbaarheid voor social engineering leidt tot een kleine maar significante vermindering van het aantal slachtoffers (p=,047). De effectomvang neemt af (EG=-,0005) voor elk extra uur na het uitvoeren van de interventie.

Omgeving: reallife of lab

In experimenten kan het gedrag van de proefpersonen in een gecontroleerde omgeving worden geobserveerd (Siedler & Sonnenberg 2010). In het lab zijn mensen zich bewust van het feit dat ze meedoen aan onderzoek en zijn zij soms ook ingelicht over het doel van het experiment. Hierdoor kunnen zij vooringenomen zijn in hun gedrag. Het is niet bij voorbaat zeker dat ze buiten het experiment hetzelfde gedrag zouden vertonen en vergelijkbare vermoedens van bijvoorbeeld social engineering hebben. Daarom wordt verwacht dat de effecten van interventies die worden getest in een laboratoriumomgeving groter zijn dan die van interventies die in een veldexperiment worden onderzocht. Dit komt overeen met onze eigen analyses (Q(1)=7,19; p=,007): EG=0,81 in laboratoriumstudies en EG=0,33 in veldexperimenten.
Zich bewust zijn van deelname als onderzoeksonderwerp heeft betrekking op het waarnemereffect. Mensen hebben de neiging om aspecten van hun gedrag te veranderen wanneer ze zich ervan bewust zijn dat ze worden geobserveerd en mogelijk de onderzoeksresultaten kunnen beïnvloeden (Monahan & Fisher 2010). Bij sommige labstudies wisten deelnemers niet precies waar het onderzoek, bijvoorbeeld phishing, over ging, terwijl dit bij andere veldexperimenten wel duidelijk was. Het zich bewust zijn van het onderwerp van het onderzoek en de interventie valt dus niet samen met laboratorium versus veldexperiment en is daarom apart bekeken. Zoals verwacht is het waarnemereffect ook gevonden in onze meta-analyse (F(2,34)=5,06, p=,012). Naarmate de deelnemers zich minder bewust waren van het feit dat zij deelnamen aan onderzoek of van het onderwerp van het onderzoek nam de effectgrootte af (respectievelijk (EG=0,87, EG=0,40 en EG=0,23).

doi: 10.5553/JV/016758502020046002009

Randomisatie

Sterkere onderzoeksdesigns hebben zowel een maximale interne als een maximale externe validiteit (Campbell & Stanley 1963). Het gebruik van gerandomiseerde experimenten is de beste onderzoeksmethode om het effect van interventies te bestuderen (Feder e.a. 2000). Twee studies (Weisburd e.a. 2001; Welsh e.a. 2011) hebben aangetoond, in een overzicht van criminologisch onderzoek, dat betere onderzoekdesigns vaak geringere effecten rapporteerden en minder goede onderzoekdesigns vaak sterkere effecten. Dat pleit ervoor om de sterkste onderzoeksdesigns te gebruiken: het heeft geen nut interventies te implementeren die in feite – indien goed onderzocht – geen effect hebben. Voor online interventies vinden wij echter geen invloed van randomisatie op de effectgrootte ($F(2, 34)=0,09$, $p=,913$). Mogelijk komt dat omdat de zwakkere onderzoekdesigns in onze eigen meta-analyse niet zijn geïncludeerd.

Slotbeschouwing

Het goede nieuws is dat er interventies zijn die helpen om de effecten van social-engineeringaanvallen te beperken.
De ideale interventie, op basis van onze meta-analyse, is een interventie waarin de volgende elementen zitten:
- De interventie is interactief (bijv. een spel).
- Er is contact met gebruikers (bijv. een les).
- De interventie heeft een specifieke focus en behandelt een of twee concrete onderwerpen (bijv. over URL's en phishingmails).
- De interventie is relatief intensief.

Een effectieve interventie is niet het enige dat een organisatie moet doen om veilig te zijn. Een aantal aanvullende tips:
- Voer schijnaanvallen uit, dan weet je hoe je organisatie erbij staat.
- Blijf alert en houd op regelmatige momenten trainingen of vergelijkbare oefeningen.
- Evalueer je beleid regelmatig, dan weet je of je vorderingen maakt.

Tot slot is het anoniem delen van een databank met informatie over beveiliging, over (schijn)aanvallen en over effecten van interventies erg nuttig.

doi: 10.5553/JV/016758502020046002009

Onze studie heeft een aantal beperkingen. De reikwijdte van onze conclusies over de effectiviteit wordt beperkt door een aantal zaken. Er zijn nog niet zoveel experimentele studies die interventies tegen social engineering hebben getest. Dat beperkt de mogelijkheden voor analyses: een multivariate analyse is niet goed mogelijk. Daarnaast is lastig dat er nog niet veel systematiek is in dit veld, zowel bij het ontwikkelen van interventies als bij de wijze waarop ze het best kunnen worden getest. Meer overeenstemming over de eisen die aan het ontwikkelen van interventies kunnen worden gesteld en het adequaat testen ervan zouden winst opleveren voor de groei van de kennis op dit terrein.

Verder zagen wij dat interventies die alleen gericht waren op het uitleggen van de URL zeer effectief waren. Deze uitkomst kan gedeeltelijk het gevolg zijn van het feit dat bij het onderzoek naar de effectiviteit van deze interventies in bijna alle gevallen de respondenten werden ingelicht over het doel van de interventie; terwijl studies die 'blind' testten en dus feitelijk zuiverder onderzoek verrichtten hierdoor minder grote effecten vonden. Omdat wij geen multivariate analyse konden uitvoeren vanwege het grote aantal variabelen ten opzichte van het aantal effectgroottes is het mogelijk dat dit gegeven de uitkomsten heeft beïnvloed.

Daarnaast is er niet evenveel aandacht geweest voor elk type social engineering. Er is – terecht – veel onderzoek gedaan naar phishing en het herkennen van foute URL's. Maar er is jammer genoeg veel minder aandacht geweest voor andere typen social engineering, zoals via de telefoon. Daarnaast blijkt dat sommige tips, bijvoorbeeld over phishing, kunnen verouderen omdat de aanvallers slimmer worden. Zo is de tip dat de aanhef van een e-mail niet specifiek is ('beste klant') als indicatie voor phishing niet meer heel adequaat: met spearphishing lukt het de aanvallers om de e-mailontvanger bij naam te noemen. Terwijl de offline criminaliteit flink afneemt in dit coronatijdperk, lijkt de online criminaliteit alleen maar toe te nemen (Flemming 2020; Banken.nl 2020). Omdat het probleem van social engineering daarmee alleen maar belangrijker lijkt te worden, pleiten wij ervoor dat er meer wordt gedaan aan het systematisch ontwikkelen van interventies en het adequaat testen ervan.

doi: 10.5553/JV/016758502020046002009

Literatuur

Aburrous e.a. 2010
M. Aburrous, M.A. Hossain, K. Dahal & F. Thabtah, 'Experimental case studies for investigating e-banking phishing techniques and attack strategies', *Cognitive Computation* (2) 2010, afl. 3, p. 242-253.

Acquisti e.a. 2012
A. Acquisti, L.K. John & G. Loewenstein, 'The impact of relative standards on the propensity to disclose', *Journal of Marketing Research* (49) 2012, afl. 2, p. 160-174.

Alnajim & Munro 2009
A. Alnajim & M. Munro, 'An anti-phishing approach that uses training intervention for phishing websites detection', *ITIG 2009 – 6th International Conference on Information Technology: New generations*, 2009, p. 405-410.

Arachchilage & Cole 2011
N.A.G. Arachchilage & M. Cole, 'Design a mobile game for home computer users to prevent from "phishing attacks"', *Information Society (i-Society)* 2011, p. 485-489.

Arachchilage e.a. 2016
N.A.G. Arachchilage, S. Love & K. Beznosov, 'Phishing threat avoidance behaviour: An empirical investigation', *Computers in Human Behavior* (60) 2016, p. 185-197.

Argo & Main 2004
J.J. Argo & K.J. Main, 'Meta-analyses of the effectiveness of warning labels', *Journal of Public Policy and Marketing* (23) 2004, afl. 2, p. 193-208.

Bada e.a. 2015
M. Bada, A.M. Sasse & J.R.C. Nurse, *Cyber security awareness campaigns: Why do they fail to change behaviour?*, 2015, www.cs.ox.ac.uk/files/7194/csss2015_bada_et_al.pdf.

Banken.nl 2020
Banken.nl, 'Scherpe toename phishing vanwege corona', 2020, www.banken.nl/nieuws/22291/scherpe-toename-phishing-vanwege-corona.

Barth e.a. 2019
S. Barth, M.D.T. de Jong, M. Junger, P.H. Hartel e.a. 'Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources', *Telematics and Informatics* (41) 2019, p. 55-69.

Blakeborough & Correia 2017
L. Blakeborough & S. Correia, *The scale and nature of fraud: A review of the evidence*, 2017, www.gov.uk/government/publications/the-scale-and-nature-of-fraud-a-review-of-the-evidence.

doi: 10.5553/JV/016758502020046002009

Borenstein e.a. 2010
M. Borenstein, L.V. Hedges, J.P.T. Higgins & H.R. Rothstein, 'A basic introduction to fixed-effect and random-effects models for meta-analysis', *Research Synthesis Methods* (1) 2010, afl. 2, p. 97-111.

Bullée & Junger 2020a
J.H. Bullée & M. Junger, 'Social engineering', in: T.J. Holt & A.M. Bossler (red.), *Palgrave international handbook of cybercrime and cyberdeviance*, Cham, Zwitserland: Palgrave Macmillan 2020, p. 1-28.

Bullée & Junger 2020b
J.H. Bullée & M. Junger, 'Are interventions against social engineering effective, not effective or do they have adverse effects? A meta-analysis', nog niet gepubliceerd.

Bullée e.a. 2017
J.H. Bullée, L. Montoya, M. Junger & P. Hartel, 'Spear phishing in organisations explained', *Information and Computer Security* (25) 2017, afl. 5, p. 593-613.

Cameron e.a. 2012
C.D. Cameron, J.L. Brown-Iannuzzi & B.K. Payne, 'Sequential priming measures of implicit social cognition: A meta-analysis of associations with behavior and explicit attitudes', *Personality and Social Psychology Review* (16) 2012, afl. 4, p. 330-350.

Campbell & Stanley 1963
D.T. Campbell & J.C. Stanley, *Experimental and quasi-experimental designs for research*, Boston, MA: Houghton, Mifflin Company 1963.

Canova e.a. 2015
G. Canova, M. Volkamer, C. Bergmann & B. Reinheimer, *NoPhish app evaluation: Lab and retention study* (NDSS workshop on usable security 2015), 2015.

Caputo e.a. 2014
D.D. Caputo, S.L. Pfleeger, J.D. Freeman & M.E. Johnson, 'Going spear phishing: Exploring embedded training and awareness', *IEEE Security and Privacy* (12) 2014, afl. 1, p. 28-38.

Christin e.a. 2011
N. Christin, S. Egelman, T. Vidas & J. Grossklags, 'It's all about the benjamins: An empirical study on incentivizing users to ignore security advice', *International Conference on Financial Cryptography and Data Security*, 2011, p. 16-30.

Clark & Mayer 2016
R.C. Clark & R.E. Mayer, *E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning*, Hoboken, NJ: John Wiley & Sons 2016.

Cohen 2013
J. Cohen, *Statistical power analysis for the behavioral sciences*, New York, NY: Routledge 2013.

doi: 10.5553/JV/016758502020046002009

Davinson & Sillence 2010
N. Davinson & E. Sillence, 'It won't happen to me: Promoting secure behaviour among internet users', *Computers in Human Behavior* (26) 2010, afl. 6, p. 1739-1747.

Dodge e.a. 2007
R.C. Dodge, C. Carver & A.J. Ferguson, 'Phishing for user security awareness', *Computers & Security* (26) 2007, afl. 1, p. 73-80.

Dolan e.a. 2010
P. Dolan, M. Hallsworth, D. Halpern, D. King e.a., *MINDSPACE: Influencing behaviour for public policy*, 2010, www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf.

Downs e.a. 2006
J.S. Downs, M.B. Holbrook & L.F. Cranor, 'Decision strategies and susceptibility to phishing', *Proceedings of the Second Symposium on Usable Privacy and Security*, 2006, p. 79-90.

Feder e.a. 2000
L. Feder, A. Jolin & W. Feyerherm, 'Lessons from two randomized experiments in criminal justice settings', *Crime & Delinquency* (46) 2000, afl. 3, p. 380-400.

Flemming 2020
S. Flemming, 'Threat spotlight: Coronavirus-related phishing', 2020, https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/.

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

Gupta e.a. 2011
M. Gupta, S. Agrawal & N. Garg, 'A survey on social engineering and the art of deception', *International Journal of Innovations in Engineering and Technology* (1) 2011, afl. 1, p. 31-35.

Hadnagy & Wilson 2010
C. Hadnagy & P. Wilson, *Social engineering: The art of human hacking*, New York, NY: Wiley 2010.

Happ e.a. 2016
C. Happ, A. Melzer & G. Steffgen, 'Trick with treat – Reciprocity increases the willingness to communicate personal data', *Computers in Human Behavior* (61) 2016, p. 372-377.

doi: 10.5553/JV/016758502020046002009

Henson e.a. 2016
B. Henson, B.W. Reyns & B.S. Fisher, 'Cybercrime victimization', in: *The Wiley handbook on the psychology of violence*, Chichester: John Wiley & Sons 2016, p. 553-570.

Herzberg & Jbara 2008
A. Herzberg & A. Jbara, 'Security and identification indicators for browsers against spoofing and phishing attacks', *ACM Transactions on Internet Technology* (8) 2008, afl. 4, p. 1-36.

Higgins e.a. 2003
J.P.T. Higgins, S.G. Thompson, J.J. Deeks & D.G. Altman, 'Measuring inconsistency in meta-analyses', *British Medical Journal* (327) 2003, afl. 7414, p. 557-560.

Internet Crime Complaint Center 2018
Internet Crime Complaint Center, *2017 internet crime report*, 2018, https://pdf.ic3.gov/2017_IC3Report.pdf.

Kenrick e.a. 2005
D.T. Kenrick, S.L. Neuberg & R.B. Cialdini, *Social psychology: Unraveling the mystery*, Boston, MA: Allyn & Bacon 2005.

Kirlappos & Sasse 2012
I. Kirlappos & M.A. Sasse, 'Security education against phishing: A modest proposal for a major rethink', *IEEE Security Privacy* (10) 2012, afl. 2, p. 24-32.

Klahr e.a. 2017
R. Klahr, J. Shah, P. Sheriffs, T. Rossington e.a., *Cyber security breaches survey 2017: A survey detailing business action or cyber security and the costs and impacts of cyber breaches and attacks*, 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf.

Kumaraguru e.a. 2007a
P. Kumaraguru, Y. Rhee, A. Acquisti, L.F. Cranor e.a., 'Protecting people from phishing: The design and evaluation of an embedded training email system', *Conference on Human Factors in Computing Systems – Proceedings*, 2007, p. 905-914.

Kumaraguru e.a. 2007b
P. Kumaraguru, Y. Rhee, S. Sheng, S. Hasan e.a., 'Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer', *ACM International Conference Proceeding Series. Vol. 269*, 2007, p. 70-81.

Kumaraguru e.a. 2008
P. Kumaraguru, S. Sheng, A. Acquisti, L.F. Cranor e.a., 'Lessons from a real world evaluation of anti-phishing training', *eCrime Researchers Summit*, 2008, p. 1-12.

doi: 10.5553/JV/016758502020046002009

Kumaraguru e.a. 2009
P. Kumaraguru, J. Cranshaw, A. Acquisti, L.F. Cranor e.a., 'School of phish: A real-world evaluation of anti-phishing training', *SOUPS 2009 – Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009, p. 1-12.

Kumaraguru e.a. 2010
P. Kumaraguru, S. Sheng, A. Acquisti, L.F. Cranor e.a., 'Teaching Johnny not to fall for phish', *ACM Transactions on Internet Technology* (10) 2010, afl. 2, p. 1-31.

Lastdrager e.a. 2017
E.E. Lastdrager, I. Carvajal Gallardo, P.H. Hartel & M. Junger, 'How effective is anti-phishing training for children?', *SOUPS 2017 – Proceedings of the 13th Symposium on Usable Privacy and Security*, 2017, p. 229-239.

Marinos & Sfakianakis 2012
L. Marinos & A. Sfakianakis, *ENISA threat landscape 2012*, 2012, www.enisa.europa.eu/publications/ENISA_Threat_Landscape/at_download/fullReport.

Margulies & Herzberg 2013
R. Margulies & A. Herzberg, *Conducting ethical yet realistic usable security studies*, www.researchgate.net/publication/253954682_Conducting_Ethical_yet_Realistic_Usable_Security_Studies.

Mayhorn & Nyeste 2012
C.B. Mayhorn & P.G. Nyeste, 'Training users to counteract phishing', *Work* (41) 2012, p. 3549-3552.

Monahan & Fisher 2010
T. Monahan & J.A. Fisher, 'Benefits of "observer effects": Lessons from the field', *Qualitative Research* (10) 2010, afl. 3, p. 357-376.

Parsons e.a. 2015
K. Parsons, A. McCormac, M. Pattinson, M. Butavicius e.a. 'The design of phishing studies: Challenges for researchers', *Computers and Security* (52) 2015, p. 194-206.

Reep-van den Bergh & Junger 2018
C.M.M. Reep-van den Bergh & M. Junger, 'Victims of cybercrime in Europe: A review of victim surveys', *Crime Science* (7) 2018, afl. 1, p. 1555-1570.

Schneier 2000
B. Schneier, 'Crypto-gram, October 15, 2000', 2000, www.schneier.com/crypto-gram/archives/2000/1015.html.

doi: 10.5553/JV/016758502020046002009

Sheng e.a. 2007
S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti e.a., 'Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish', *SOUPS 2007 – Proceedings of the 3rd Symposium on Usable Privacy and Security*, 2007, p. 88-99.

Siedler & Sonnenberg 2010
T. Siedler & B. Sonnenberg, 'Experiments, surveys and the use of representative samples as reference data', *German Council for Social and Economic Data (RatSWD)*, 2010.

Sokol e.a. 2017
P. Sokol, M. Glova, T. Mézešová & R. Hučková, 'Lessons learned from phishing test', *25th interdisciplinary information management talks – Digitalization in management, society and economy* 2017, p. 297-304.

Stockhardt e.a. 2016
S. Stockhardt, B. Reinheimer, M. Volkamer, P. Mayer, e.a., Teaching phishing-security: Which way is best?, 31st IFIP International Information Security and Privacy Conference (SEC), May 2016, Ghent, Belgium. p. 135-149. https://hal.inria.fr/hal-01369549/document.

Sundar e.a. 2013
S.S. Sundar, H. Kang, M. Wu, E. Go e.a., 'Unlocking the privacy paradox: Do cognitive heuristics hold the key?', *CHI'13 extended abstracts on human factors in computing systems*, 2013, p. 811-816.

Verizon Risk Team 2018
Verizon Risk Team, *2018 Annual report*, 2018, www.verizon.com/about/sites/default/files/2018-Verizon-Annual-Report.pdf.

Vishwanath 2015
A. Vishwanath, 'Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack', *Journal of Computer-Mediated Communication* (20) 2015, afl. 5, p. 570-584.

Weisburd e.a. 2001
D. Weisburd, C.M. Lum & A. Petrosino, 'Does research design affect study outcomes in criminal justice?', *The ANNALS of the American Academy of Political and Social Science* (578) 2001, afl. 1, p. u50-70.

Welsh e.a. 2011
B.C. Welsh, M.E. Peel, D.P. Farrington, H. Elffers e.a., 'Research design influence on study outcomes in crime and justice: A partial replication with public area surveillance', *Journal of Experimental Criminology* (7) 2011, afl. 2, p. 183-198.

doi: 10.5553/JV/016758502020046002009

Wogalter e.a. 2012
M.S. Wogalter, K.R. Laughery Sr & C.B. Mayhorn, 'Warnings and hazard communications', in: G. Salvendy (red.), *Handbook of human factors and ergonomics*, Hoboken, NJ: Wiley 2012, p. 868-894.

Wright e.a. 2014
R. Wright, M. Jensen, J. Thatcher, M. Dinger e.a., 'Influence techniques in phishing attacks: An examination of vulnerability and resistance', *Information Systems Research* (25) 2014, afl. 2, p. 385-400.

Yang e.a. 2012
C.C. Yang, S.S. Tseng, T.J. Lee, J.F. Weng e.a., 'Building an anti-phishing game to enhance network security literacy learning', *2012 IEEE 12th International Conference on Advanced Learning Technologies*, 2012, p. 121-123.

Yang e.a. 2017
W. Yang, A. Xiong, J. Chen, R. Proctor e.a., 'Use of phishing training to improve security warning compliance: Evidence from a field experiment', *Proceedings of the hot topics in science of security: Symposium and bootcamp*, 2017, p. 52-61.

doi: 10.5553/JV/016758502020046002009