# Het succes van social engineering

Bullée, Jan Willem; Montoya, Lorena; Junger, Marianne; Hartel, Pieter

**DOI**
10.5553/TvV/187279482018017102004

**Publication date**
2018

**Document Version**
Final published version

**Published in**
Tijdschrift voor Veiligheid

# Het succes van social engineering

*Jan-Willem Bullée, Lorena Montoya, Marianne Junger & Pieter Hartel*

*Social engineering is een aanvalstechniek waarin misleiding en bedrog worden gebruikt om doelwitten actief te laten meewerken aan hun eigen slachtofferschap. In dit artikel wordt aan de hand van een praktisch voorbeeld en bijbehorende theorieën inzicht gegeven in social engineering-praktijken. Daarnaast zal er ook worden ingegaan op een drietal experimenten (i.e. face-to-face, telefoon en e-mail) waarin systematisch onderzoek naar dit gevaar centraal staat. De resultaten geven inzicht in hoe kwetsbaar een organisatie is voor social engineering en welke medewerkers het meeste baat hebben bij een bewustwordingscampagne.*

## 1 Introductie

De mens is vaak de zwakste schakel in informatiebeveiliging (Happ, Melzer & Steffgen, 2016; Schneier, 2000). Aanvallers gebruiken misleiding, bedrog en overtuigingstechnieken als aanvalstactiek om hun doelwit gevoelige informatie te laten delen of kwaadwillige acties uit te laten voeren (Gupta, Agrawal & Garg, 2011). Dit noemen we social engineering en wordt beschouwd als een van de grootste cybergevaren. Het gevaar van social engineering-aanvallen is dat het op het eerste oog legitiem en ongevaarlijk lijkt, zodat het doelwit zich er niet van bewust is slachtoffer te zijn (Hadnagy & Wilson, 2010). Dit artikel is een samenvatting van het proefschrift *Experimental Social Engineering* van Bullée (2017). Er zal een uitleg van social engineering worden gegeven aan de hand van theorieën uit de criminologie en psychologie, daarnaast worden drie onderzoeken waarin social engineering systematisch is onderzocht kort samengevat. Bij die drie onderzoeken zal verder ingegaan worden op welke groepen het meeste baat hebben bij een interventie en wat het effect hiervan is.

Social engineering wordt al eeuwen gebruikt als aanvalstactiek. Mogelijk een van de oudste verhalen is afkomstig van het oude Griekse leger, ten tijde van de Trojaanse Oorlog. Na tien jaar in oorlog te zijn met de Trojanen leek het erop dat het Griekse leger zich terugtrok van het strijdtoneel en liet het leger het houten standbeeld van een paard achter. De Trojanen verwelkomden het geschenk en vierden de overwinning. Die nacht verschenen Griekse soldaten vanuit het paard en veroverden de stad (Graves, 1992). Een mythe of niet, dit voorbeeld geeft aan hoe het menselijke element wordt misbruikt om een doel te bereiken wanneer dit anders niet mogelijk was.

Hoe vaak komt social engineering nu eigenlijk voor? Tijdens de 2015-editie van de goed bezochte Black Hat-conferentie zijn 494 bezoekers (voornamelijk IT-beveiligingsexperts) gevraagd wat populaire aanvalsmethoden zijn. Meer dan 80% antwoordde dat hun favoriete methode social engineering is (Chmielewski, 2015). Hoewel het lastig is om te onderzoeken welke aanvalstactieken een aanvaller alle-


Tijdschrift voor Veiligheid 2018 (17) 1-2
doi: 10.5553/TvV/187279482018017102004

maal gebruikt, kunnen we wel iets zeggen over de aanvallen die zijn opgemerkt. Uit de data van de ISACA en RSA Conference-vragenlijst blijkt dat 46,45% (*N* = 327) van de organisaties succesvol is aangevallen middels social engineering en 68,32% (*N* = 481) middels phishing (ISACA and RSA Conference 2015). Uit het rapport *Internet Security Threat Report* blijkt dat social engineering op nummer 4 (15,8%) staat in de lijst van meest voorkomende oorzaken van datalekken in 2016. Tevens is het de op een na grootste oorzaak (6,4%) van identiteitsfraude (Symantec, 2017). Daarnaast wordt social engineering gebruikt als springplank in andere aanvallen, bijvoorbeeld als het starten van malafide Microsoft Office-macro's, het installeren van Trojaanse paarden of ransomware (Symantec, 2017). Aanvallers gebruiken liever mensen dan techniek om veiligheidsmaatregelen te omzeilen (Proofpoint, 2016). We leggen dit uit met een voorbeeld. Een bekende casus uit 2016 is het hacken van het Gmail-account van de campagnebaas van Hillary Clinton, John Podesta. Op 19 maart 2016 ontving John een spear phishingmail. De e-mail was op zo'n manier opgesteld dat het leek alsof deze van Gmail zelf afkomstig was en suggereerde dat het e-mailaccount gecompromitteerd was. De e-mail bevatte een link om het wachtwoord te resetten, in werkelijkheid leidde de link naar een sprekend lijkende vervalste pagina om wachtwoorden te resetten. Het was niet nodig om malware of bugs in software te gebruiken bij deze aanval. Het gebruik van social engineering was voldoende om het wachtwoord in handen te krijgen (Symantec, 2017). Geschat wordt dat 1 op de 131 e-mails malafide is. Dit laat zien dat social engineering populair is, effectief is en als een serieuze dreiging beschouwd moet worden. Dit artikel heeft daarom als doel inzicht te verschaffen in zowel het succes van de social engineering-aanvalstactiek als interventies. Voor zover bij ons bekend, is dit het eerste artikel dat een samenvatting geeft van drie social engineering-onderzoeken met verschillende modaliteiten binnen één organisatie.

### *1.1 Social engineering uitgelegd met een script*

Social engineering kan op verschillende plaatsen voorkomen. In dit artikel zal gekeken worden naar social engineering binnen een organisatie. Beschouw Scenario 1 als een voorbeeld van een social engineering-aanval (The SANS Institute, 2012). Het scenario zal worden ontleed om social engineering te verklaren en te relateren aan de bestaande literatuur uit de criminologie en sociale psychologie. Eerst zal de Routine Activity Theory (RAT) gebruikt worden om inzicht te geven in de oorzaak van de misdaad. Daarna zullen overtuigingsprincipes, denkfouten en andere sociaalpsychologische theorieën gebruikt worden om social engineering te verklaren.

Scenario 1: Verkrijg creditcardinformatie

Je bent aan het reizen en hebt net ingecheckt in het hotel. Wanneer je je kamer binnenloopt, gaat de telefoon. Een vriendelijke dame stelt zich voor als Rebecca van de incheckbalie. Ze legt uit dat er iets is misgegaan en ze heeft je creditcardgegevens nodig. Onder de aanname dat ze vanuit het hotel belt, geef je haar de gegevens. Ze zegt dat alles nu goed is en wenst je een fijne dag.

Helaas was de persoon aan de telefoon niet Rebecca van de balie. Het was een aanvaller die iedere hotelkamer belde in een poging om iemand tot slachtoffer te maken. Wat gebeurde er nu eigenlijk waardoor de reiziger de creditcardinformatie aan een vreemde gaf?
De Problem Analysis Triangle (PAT), een element uit de RAT, beschouwt drie belangrijk elementen: 1) aanvallers, 2) doelwitten/slachtoffers en 3) locaties. Een misdaad vindt plaats wanneer een gemotiveerde aanvaller en een passend doelwit samenkomen op eenzelfde tijd en plaats met het gebrek aan effectieve controleurs (Cohen & Felson, 1979; Felson, 1995).
Binnen het scenario kunnen de drie elementen uit de RAT worden geïdentificeerd. De aanvaller is de persoon die belt, het doelwit is de reiziger en de locatie is de telefoon in de hotelkamer van de reiziger.
Er kunnen bovendien vanuit een psychologisch perspectief vier facetten worden onderscheiden; twee gerelateerd aan de aanvaller en twee aan het doelwit: 1) de aanvaller gebruikt misleiding door imitatie, 2) de aanvaller maakt gebruik van overtuigingsprincipes om het verhaal geloofwaardiger te maken, 3) er ontstaat een denkfout bij het doelwit en 4) het doelwit is zich niet bewust van gepaste verdedigingstechnieken. De twee facetten gerelateerd aan de aanvaller relateren ook aan de definitie van social engineering. Ieder facet zal in meer detail besproken worden.

- *Misleiding door imitatie*

Misleiding is essentieel in social engineering. Zonder misleiding zou het namelijk een legitieme vraag zijn. Buller en Burgoon (1996) definiëren misleiding als volgt:

> 'Misleiding ontstaat wanneer communicatoren de informatie in hun berichten aanpassen om een betekenis over te brengen die afwijkt van de waarheid zoals zij die kennen.'

Het zich voordoen als iemand anders wordt door veel social engineers gebruikt (Bosworth, Kabay & Whyne, 2014). Door het aannemen van een andere identiteit krijgen aanvallers een andere status. Veel voorkomende doelwitten om te worden geïmiteerd zijn systeemadministrators, helpdeskmedewerkers of CEO's. Aanvallers kiezen voor deze specifieke rollen, omdat mensen die rol vertrouwen. Dit


Tijdschrift voor Veiligheid 2018 (17) 1-2
doi: 10.5553/TvV/187279482018017102004

draagt bij aan de kans dat het doelwit de aanvaller vertrouwt (Bosworth, Kabay & Whyne, 2014).
Het onvermogen van mensen om leugens te herkennen verklaart het succes van misleiding en imitatie (Vrij, Granhag & Porter, 2010). De moeilijkheid zit hem in de afwezigheid van een eenduidige aanwijzing die betrouwbaar is (e.g. de neus van Pinokkio) (Vrij, Granhag & Porter, 2010). Gemiddeld herkennen mensen waarheid en leugen in 54% van de gevallen correct, wat veel lijkt op de uitkomst van gokken (Bond & DePaulo, 2006).
In Scenario 1 liegt de aanvaller over de identiteit van Rebecca. Door deze identiteit aan te nemen is de vraag naar creditcardinformatie iets dat binnen de context past en wordt beschouwd als legitiem.

- *Overtuigingsprincipes*

Wanneer een persoon doelwit is, kan de aanvaller sociale beïnvloeding gebruiken om de kansen in haar/zijn voordeel te krijgen. Er zijn zes overtuigingsprincipes die gebruikt kunnen worden om de kans op succes van de aanvaller te vergroten: autoriteit, conformiteit, wederkerigheid, vasthoudendheid, schaarste en sympathie (Cialdini, 2009). Voor ieder overtuigingsprincipe is een verduidelijking gegeven:

1 Autoriteit beschrijft het principe dat mensen 'luisteren' naar autoritaire figuren. Wanneer mensen zelf niet in staat zijn om een doordachte keuze te maken, geven zij deze verantwoordelijkheid aan de persoon waarvan zij denken dat die de leiding heeft.
2 Conformiteit, ook wel groepsdruk, is het imiteren van gedrag van anderen. Door iemand het idee te geven dat anderen een bepaald gedrag vertonen, zijn mensen geneigd dit gedrag ook te vertonen.
3 Wederkerigheid verwijst naar de onderlinge bereidheid om een gift te beantwoorden met een tegengift. Een doelwit voelt zich verschuldigd om een tegengebaar te maken, zelfs het kleinste gebaar kan je een voordeel geven.
4 Vasthoudendheid verwijst naar het blijven vasthouden aan een belofte of overeenkomst. In het algemeen hebben mensen de neiging om een gedane belofte na te komen. Een eerdere, kleine belofte vergroot de kans op volgzaamheid in een vervolgstap.
5 Schaarste ontstaat wanneer een product, dienst of informatie beperkte beschikbaarheid heeft. Schaarste verhoogt de gepercipieerde waarde en aantrekkelijkheid van producten.
6 Sympathie kan iemand een voordeel geven. Mensen hebben de tendens om anderen met dezelfde interesses, attitudes en overtuigingen aardiger te vinden (Cialdini, 2009).

In Scenario 1 gebruikt de aanvaller het Autoriteitsprincipe door zich voor te doen als Rebecca. Dit was een tactische actie van de aanvaller, omdat baliepersoneel verantwoordelijkheid heeft over de registratie van gasten, kamertoewijzing en kredietcontrole. Het was hierdoor 'toegestaan' dat Rebecca over creditcardinformatie beschikt. Een gepaste manier voor de reiziger om te reageren is om goed na

te denken met wie je in gesprek bent. Over dit laatste volgen meer details in de subparagraaf hierna over verdediging tegen social engeneering.

- *Cognitieve fout en heuristieken*

De duale systeemtheorie, ook wel bekend als Systeem 1 en Systeem 2, verklaart de denkfout (Kahneman, 2011). Systeem 1 is een automatisch systeem dat snel, onbewust en met weinig moeite redeneert op basis van heuristieken. Systeem 2 is een gecontroleerd systeem dat bewust en relatief langzaam redeneert (Kahneman, 2011). Aangezien mensen niet voldoende cognitieve capaciteit hebben om alle sensorische input te verwerken, worden beslissingen vaak gemaakt aan de hand van vuistregels (i.e. heuristieken); dit gebeurt in Systeem 1 (Cialdini, 2009). Heuristieken werken goed in de meeste situaties, totdat een heuristiek faalt en er een denkfout ontstaat (Tversky & Kahneman, 1974).
Een mogelijke verklaring voor het gedrag van de reiziger is het beschikbaarheidsheuristiek. Dit is gebaseerd op de eerste gedachte die opkomt in een specifieke context. Dit heuristiek heeft het volgende onderliggende mechanisme: wanneer iets onmiddellijk herinnerd wordt, is het belangrijker dan wanneer iets niet onmiddellijk herinnerd wordt. Een consequentie hiervan is dat mensen hun oordeel baseren op recente informatie (Esgate, Groome & Baker, 2005). In Scenario 1 is de reiziger in de context van een hotel en herinnert zich dat de creditcard is gebruikt als betaalmethode.
Tevens speelt ook het optimisme-bias een rol. Mensen geloven dat positieve gebeurtenissen vaker bij zichzelf voorkomen dan bij anderen (Weinstein, 1980). Het omgekeerde is ook waar: mensen geloven dat negatieve gebeurtenissen vaker voorkomen bij anderen dan bij zichzelf (Weinstein, 1980). Als de reiziger uit Scenario 1 zich bewust was van het gevaar van social engineering, zou een mogelijke gedachte kunnen zijn: 'Het is waarschijnlijker dat iemand anders doelwit is dan ik, maar wanneer ik doelwit zou zijn ben ik beter in staat om mij te verweren dan iemand anders.'

- *Verdediging tegen social engineering*

Het is moeilijk om je te verdedigen tegen iets waarvan je het bestaan niet kent. De eerste stap in het reduceren van het social engineering-gevaar is om mensen bewust te maken van zowel het bestaan ervan, als wat ze moeten doen om zich te verweren (Bosworth, Kabay & Whyne, 2014). In Scenario 1 was de reiziger niet in staat om het voorval te identificeren als een bedreiging of bedrog en kon daarom niet de juiste actie ondernemen. Het waarheidsbias zit hierin verankerd. Dit gaat ervan uit dat mensen niet liegen tegen elkaar en dat de meeste communicatie eerlijk is (McCornack & Parks, 1986). Een betere actie zou geweest zijn om gebruik te maken van de terugbel-aanpak. De gedachte achter deze aanpak is om de identiteit te achterhalen via een vertrouwde en geverifieerde route (Gragg, 2003). De te ondernemen stappen zijn om eerst de verbinding te verbreken en dan zelf de balie te bellen op een bekend nummer. Een alternatief is om zelf naar de balie gaan. Deze tegenmaatregelen zijn twee voorbeelden van een doelwit dat zijn eigen controleur is.


Tijdschrift voor Veiligheid 2018 (17) 1-2
doi: 10.5553/TvV/187279482018017102004

## 2 Experimenten

In deze paragraaf worden drie experimenten besproken, elk met een andere modaliteit, namelijk: face-to-face (f2f), telefoon en e-mail. Er is voor deze experimenten gekozen, omdat deze alle drie door dezelfde onderzoekers zijn gedaan. Tevens is het bij dezelfde organisatie gedaan, wat als voordeel heeft dat de organisatiecultuur gelijk is. Tijdens het eerste experiment zijn medewerkers in hun kantoor door de aanvaller bezocht met de vraag om hun kantoorsleutel te overhandigen (Bullée, Montoya, Junger & Hartel, 2015). Tijdens het tweede experiment is geprobeerd om medewerkers via de telefoon te overtuigen om van een onbetrouwbare bron software te downloaden en installeren (Bullée, Montoya, Junger & Hartel, 2016). Bij het derde experiment zijn phishingmails naar medewerkers verstuurd met het verzoek om hun gebruikersnaam en wachtwoord te valideren op een onbetrouwbare, externe website (Bullée, Montoya, Pieters, Junger & Hartel, 2017).

### *2.1 Face-to-face social engineering*

De hoofdvraag bij de f2f-studie was: 'In hoeverre zijn mensen vatbaar voor f2f-oplichting?' Omdat er een verschil kan bestaan tussen wat mensen zeggen en wat zij daadwerkelijk doen (Crowne & Marlowe, 1960; Van Dijk & Nijenhuis, 1979), is in het f2f-onderzoek gebruikgemaakt van zowel 1) een veldonderzoek als 2) een vragenlijst om het succes van social engineering te meten.

De totale steekproef bestaat uit 118 proefpersonen (die deelnamen aan de veldstudie) en 49 respondenten (die de vragenlijst invulden) werkzaam aan de Universiteit Twente. Alleen onderzoekers (i.e. aio's, postdocs, universitair docenten en hoofddocenten) die aanwezig waren en met een Winkhaus blueChip-slot in hun kantoordeur zijn benaderd.

Voor de start van het experiment is goedkeuring van de ethische commissie van de Universiteit Twente gekregen. Middels willekeurige toewijzing ontving een deel van de proefpersonen ($N$ = 46) in de veldstudie een interventie, bestaande uit drie elementen: 1) een flyer met uitleg wat social engineering is, waarom het gevaarlijk is, hoe je het kunt herkennen en hoe je jezelf kan beschermen. De ontvangers worden opgeroepen om geen credentials en gevoelige informatie te delen. Kritisch zijn naar de informatieaanvrager en deze uitdagen zijn identiteit te laten bewijzen worden juist wel aangeraden; 2) een sleutelhanger met de tekst 'Don't give me to a stranger'; 3) een poster met de expliciete opmerking om niet je pin, sleutel of wachtwoord te delen. De interventiematerialen zijn een week voor het experiment via e-mail verspreid en de sleutelhanger is door de secretaresse overhandigd. De controle- en interventiegroep zijn ongelijk, omdat niet iedereen op de dag van de datacollectie aanwezig was. De proefpersonen in het veldonderzoek zijn op hun werkplek door een studentonderzoeker, die zij niet kenden, benaderd met het script dat is beschreven in Scenario 2.

Scenario 2: Verkrijgen kantoorsleutel

Goedemorgen, ik ben [Naam] en ik werk voor de afdeling facilitaire dienstverlening. Ik heb een vraag over het slot in uw deur. We hebben verschillende klachten ontvangen over het slot en de sleutels. Heeft u ooit problemen ondervonden met het van het slot doen van de deur? We hebben contact opgenomen met de leverancier over dit probleem en er zijn meer klachten binnengekomen. Om het probleem op te lossen hebben we dit kastje ontvangen om de sleutels die in gebruik zijn te meten. Ik moet toegeven, ik weet niet precies wat het kastje meet, maar de verzamelde data zijn noodzakelijk voor de leverancier om het probleem te analyseren en hopelijk tot een oplossing te komen. Mag ik uw sleutel om te meten?

Na het meten van de sleutel: Ik moet u wel mededelen dat na het meten van de sleutel, deze automatisch gereset is en beneden weer geactiveerd moet worden. Ik vind het geen probleem om dit voor u te doen.
**Vraag**: Is het akkoord dat ik de heractivatie van de sleutel voor u doe?

De respondenten van de vragenlijst zijn benaderd met de vraag of ze mee wilden doen aan een onderzoek naar informatiebeveiliging. Er werd stap voor stap gevraagd wat de respondent zou doen wanneer deze zich in Scenario 2 zou begeven. Bijvoorbeeld: 'Een student komt naar je kantoor en zegt voor de afdeling facilitaire dienstverlening te werken. Deze vraagt of je wel eens problemen hebt ervaren met het van het slot doen van de kantoordeur.' Keuzes hierbij waren: A) Ik beantwoord de vraag. B) Ik geef geen antwoord/beëindig het gesprek. De proefpersonen uit het veldonderzoek hebben niet deelgenomen aan de vragenlijst en respondenten uit de vragenlijst niet aan het veldonderzoek.
De resultaten laten zien dat de proefpersonen in het veldonderzoek (controle conditie) in 58,62% van de gevallen gehoor gaven aan het verzoek van de aanvaller, in vergelijking met 3,1% die de vragenlijst invulde ($\chi^2$ = 30.139, $df$ = 1, $p$ = .000). Dit verschil kan worden verklaard door het optimisme-bias (Weinstein, 1980). Het waargenomen verschil moet worden meegenomen in het ontwerp van de tegenmaatregelen. Mensen zien social engineering niet als een dringend probleem dat hen mogelijk slachtoffer maakt, dus waarom zouden zij dan een tegenmaatregel accepteren? Een mogelijke gedachte van een medewerker zou kunnen zijn: 'Het is waarschijnlijker dat een collega doelwit is dan ik, maar wanneer ik doelwit zou zijn ben ik beter in staat om mij te verweren dan mijn collega. Daarom is een tegenmaatregel niet op mij van toepassing.'
Van de proefpersonen die geen interventie hebben ontvangen (controlegroep) stemde 62,5% in met het verzoek van de aanvaller, terwijl dit 37,0% is in de interventiegroep ($\chi^2$ = 7.34, $df$ = 1, $p$ = .007). Tevens is er gekeken naar het effect van sekse, leeftijd en lengte van het dienstverband op slachtofferschap; er is geen effect gevonden.


Tijdschrift voor Veiligheid 2018 (17) 1-2
doi: 10.5553/TvV/187279482018017102004

*Tabel 1 Overzicht van percentage slachtoffers per modaliteit per conditie*

| | Face-to-face | Telefoon | E-mail |
|---|---|---|---|
| Wat mensen zeggen | 3,1% | 0,0% | - |
| Controle conditie | 62,5% | 40,0% | 19,3% |
| Interventie 1 week | 37,0% | 17,2% | - |
| Interventie 2 weken | - | 42,9% | - |
| Gepersonaliseerd | - | - | 28,9% |

De interventie heeft invloed op het gedrag van de medewerker. Dit onderzoek bevestigt dat het informeren van medewerkers kan leiden tot gedragsverandering. Kennis over social engineering-aanvallen helpt om, via het gedrag van de medewerkers, de veiligheid van de organisatie te verhogen. Een samenvatting van alle resultaten is weergegeven in tabel 1.

*2.2 Telefoon social engineering*

De hoofdvraag bij de telefoonstudie was: 'In hoeverre zijn mensen vatbaar voor telefoonfraude?' Dit is getest bij onderzoekers (i.e. aio's, postdocs, universitair docenten en hoofddocenten) binnen één faculteit van de Universiteit Twente. De totale steekproef bestond uit 92 proefpersonen (die deelnamen aan de veldstudie) en 31 respondenten (die de vragenlijst invulden). Alleen medewerkers met een eigen werkplek en die aanwezig waren om de telefoon op te nemen zijn benaderd.
Voor de start van het experiment is goedkeuring van de ethische commissie van de Universiteit Twente gekregen. Middels willekeurige toewijzing zijn de doelwitten aan een van de condities toegewezen. Een derde van de doelwitten ontving twee weken voor het experiment een interventie ($N$ = 28) en een derde ontving een week voor het experiment een interventie ($N$ = 29). Deze interventie bestond uit twee delen: 1) een flyer met uitleg wat telefoonfraude is, waarom het gevaarlijk is, hoe je het kunt herkennen en hoe je je kan beschermen De ontvanger wordt opgeroepen om goed de bron van een link te inspecteren, niet blindelings te klikken en te zorgen dat de software op de pc up-to-date is. Het wordt echter afgeraden om de instructies op te volgen om software op de pc te installeren wanneer een vreemde dat vraagt; 2) een herinnering in de vorm van een pashouder met de tekst '*Beware of scams. Verify all requests. Report all incidents*'. De flyer is voor het experiment via e-mail aan de proefpersonen verspreid en de pashouder is door de secretaresse overhandigd. De proefpersonen in het veldonderzoek werden via de telefoon benaderd met het script dat is beschreven in Scenario 3.

Scenario 3: Download en installeer software

Goedemorgen, U spreekt met [naam]. We hebben ontdekt dat uw computer gebruikt wordt om spam e-mails te versturen.
Deze e-mails worden verstuurd door een kwaadaardig programma dat op de achtergrond draait. Is het u opgevallen dat uw computer de laatste tijd wat langzamer is? U hoeft zich nergens voor te schamen. Er zijn meer mensen met hetzelfde probleem. Ik heb deze ochtend al 3 mensen geholpen. Gelukkig is er een eenvoudige manier om dit probleem op te lossen.
Heeft u 2 of 3 minuten de tijd, zodat we dit samen kunnen oplossen? Zou u op de link willen klikken die in het chatscherm verschijnt? URL: http://removespam.utwente.info.
Om door te gaan met de download, moet u de validatiecode invullen. Dit is uw volledige medewerkersnummer. U kunt uw volledige nummer op de achterkant van uw medewerkerskaart vinden. Sla alstublieft het bestand op uw bureaublad op en voer het uit.

Voor de vragenlijst werden de respondenten in persoon benaderd met de vraag of ze mee wilden doen aan een onderzoek naar informatiebeveiliging. Er werd gevraagd wat de respondent zou doen wanneer deze zich in Scenario 3 zou begeven. Bijvoorbeeld: 'Je wordt door een anoniem nummer op je kantoortelefoon gebeld. Wat doe je?' A) Ik beantwoord de oproep. B) Ik beantwoord de oproep niet. De proefpersonen uit het veldonderzoek hebben niet deelgenomen aan de vragenlijst en respondenten uit de vragenlijst niet aan het veldonderzoek.
De resultaten laten zien dat de proefpersonen uit het veldonderzoek (controle conditie) in 40,0% van de gevallen gehoor gaf aan het verzoek van de aanvaller, in vergelijking met 0,0% die de vragenlijst invulde ($\chi^2 = 17.911$, $df = 1$, $p = .000$).
Van de proefpersonen die geen interventie ontvingen (controlegroep), stemde 40,0% in met het verzoek van de aanvaller, terwijl dit 17,2% is in de groep die één week van tevoren een interventie ontving ($\chi^2 = 3.935$, $df = 1$, $p = .047$). Echter, de duur van de effectiviteit is beperkt, bij de tweewekengroep verdween het effect en steeg het percentage slachtoffers naar 42,9% ($\chi^2 = .052$, $df = 1$, $p = .819$). Tevens is er gekeken naar de invloed van sekse, leeftijd en lengte van het dienstverband op slachtofferschap; er is geen effect gevonden.
Een verklaring voor de beperkte duur zou de modaliteit van de interventie kunnen zijn (i.e. tekstueel). Glenberg heeft aangetoond dat auditief gepresenteerde stimuli beter herinnerd worden dan visueel gepresenteerde stimuli (i.e. vierletterwoorden) (Glenberg, 1984). Een andere verklaring zou kunnen zijn dat de proefpersonen zich niet konden identificeren met de interventie en van mening waren dat het niet op hen van toepassing is (i.e. optimisme-bias).

### *2.3 E-mail social engineering*

De hoofdvraag bij het e-mailexperiment was: 'In hoeverre zijn mensen vatbaar voor een phishingmail?' De ethische commissie van de Universiteit Twente heeft


Tijdschrift voor Veiligheid 2018 (17) 1-2
doi: 10.5553/TvV/187279482018017102004

de studie goedgekeurd. Er is gekeken naar het effect van personalisatie in de aanhef. De steekproef bestond uit 596 proefpersonen; deze ontvingen een phishingmail met het verzoek om hun gebruikersnaam en wachtwoord te valideren op een externe site. De helft van de proefpersonen ontving een e-mail met een algemene aanhef (i.e. Beste medewerker), terwijl de andere helft een e-mail ontving met een gepersonaliseerde aanhef (i.e. Beste [voornaam] [achternaam]). De content van de e-mail is weergegeven in Scenario 4. Er waren drie karakteristieken waaraan kon worden herkend dat de e-mail nep was: 1) de URL's in het bericht verwezen niet naar de organisatie, 2) de afsluiting van de e-mail was van een fictief persoon, die geen medewerker is van de universiteit en 3) 'IT-Helpdesk' was genoemd als afdeling in plaats van 'ICTS'.

Scenario 4: Wachtwoord Synchronisatie

Beste medewerker,

Door recente veranderingen in het UT-computersysteem zijn complicaties opgetreden in de databaseservers. Dit systeem bevat jullie gebruikersnamen en wachtwoorden, en is momenteel niet juist gesynchroniseerd.

Jullie data zijn niet aangetast. Om in de toekomst problemen te voorkomen, wordt er binnenkort een complete synchronisatie tussen de servers uitgevoerd. Wanneer je account niet correct gesynchroniseerd wordt kun je niet meer inloggen.

Het wachtwoord van je IT-account moet voor 29-10-2015 worden gesynchroniseerd, dit kan alleen gedaan worden via login.utwente.nl.[1] Klik op 'Sync password' en je wachtwoord zal automatisch worden gesynchroniseerd. Wanneer je je wachtwoord niet synchroniseert met deze link, kan je niet langer gebruikmaken van de IT-faciliteiten. Het IT-account wordt gebruikt voor inloggen op de pc, e-mail, wifi-netwerk, vpn-verbinding en toegang tot verschillende UT online diensten.

Synchroniseer je wachtwoord binnen 3 dagen.
Om je wachtwoord te synchroniseren, klik hier.[1]

Met vriendelijke groet,
Jort Welp
Security Manager IT-helpdesk

De resultaten laten zien dat 19,3% van de proefpersonen meeging in het verzoek van de aanvaller bij een niet-gepersonaliseerde e-mail, terwijl dit 28,9% is bij een gepersonaliseerde e-mail ($\chi^2$ = 7.368, *df* = 1, *p* = .007). Verder is er gekeken naar

1 De URL's verwijzen naar het domein utvvente.nl in plaats van utwente.nl.

het effect van sekse, leeftijd en lengte dienstverband. Dit doen we om een beter beeld te krijgen van welke groepen het meeste kans hebben om slachtoffer te worden en dus het meeste baat hebben bij een interventie. Sekse had geen invloed op slachtofferschap (*OR* = .825, *CI* [0.48, 1.43], *p* = .492), net als voor leeftijd is er geen hoofdeffect gevonden (leeftijd: *OR* = 0.865, *CI* = [0.72, 1.04], *p* = .126; leeftijd$^2$: *OR* = 1.002, *CI* = [1.00, 1.00], *p* = .117). Het aantal jaren dat iemand in dienst is voor de organisatie had wel effect (*OR* = 0.855, *CI* = [0.77, 0.94], *p* = .002); medewerkers die kort in dienst zijn, werden vaker slachtoffer. Tot slot is er een interactie-effect tussen leeftijd en dienstjaren gevonden (*OR* = 1.005, *CI* = [1.00, 1.01], *p* = .041). Dit betekent dat jonge medewerkers met weinig dienstjaren de grootste kans hebben om slachtoffer te worden.

## 3 Conclusie

In dit artikel is social engineering geïllustreerd met een voorbeeld en uitgelegd aan de hand van theorieën uit de criminologie en psychologie. Er zijn drie social engineering-experimenten besproken.
Bij f2f-social engineering is het effect van een interventie onderzocht. Bewustwording van de gevaren, karakteristieken en tegenmaatregelen van social engineering tonen aan dat dit een effectieve manier is om de aanvaller te neutraliseren.
In het telefoonexperiment is bovendien het effect van een interventie over tijd onderzocht. Dit onderzoek suggereert dat een interventie alleen op korte termijn een effect heeft op het reduceren van het aantal slachtoffers.
In het e-mailexperiment is gekeken naar het effect van personalisatie in de aanhef en de demografie van de ontvangers. De resultaten laten zien dat het effect van een phishingmail groter is bij een gepersonaliseerde e-mail. Daarnaast heeft de groep jonge medewerkers die tevens kort in dienst is het meeste baat bij een interventie.

## 4 Implicaties voor de praktijk

Wat opvalt aan de onderzoeksresultaten is het hoge aantal slachtoffers; mensen zijn dus erg kwetsbaar. Daarnaast hebben de onderzoeksresultaten de volgende implicaties voor de praktijk:

1 Bewustwording van de gevaren, kenmerken en tegenmaatregelen van social engineering reduceert de kans op slachtofferschap. Daaruit komen twee suggesties voor een training voort: hoe kun je de verschillende overtuigingsprincipes herkennen en hoe reageer je daarop? Daarnaast is het belangrijk om de partij die contact met jou opneemt te laten bewijzen dat ze zijn wie ze zeggen te zijn.
2 De studie die een vervolgmeting hield, liet zien dat een bewustwordingsinterventie voor een beperkte tijd invloed heeft. Dit suggereert, meer in het algemeen, dat een enkele keer een interventie geven niet voldoende is. Aan de andere kant, heel vaak dezelfde boodschap herhalen is ook niet de oplossing,


Tijdschrift voor Veiligheid 2018 (17) 1-2
doi: 10.5553/TvV/187279482018017102004

dit kan zelfs tegenwerken (Stewart & Martin, 1994). De ideale interventie is nog niet gevonden en is dus een suggestie voor vervolgonderzoek.

3 Er is een groot verschil gevonden tussen wat mensen zeggen en wat zij daadwerkelijk doen. Wees daarom voorzichtig met het uitrollen van bewustwordingscampagnes. Wanneer mensen niet beseffen dat ze gevaar lopen, zullen ze ook moeilijker tegenmaatregelen accepteren.

4 Geef kwetsbare groepen meer aandacht. Jong personeel dat tevens kort in dienst is, heeft meer kans om slachtoffer te worden. Een eenvoudige manier om de kwetsbaarheid te verminderen is om deze groep een training te geven. Er is geen invloed van sekse of leeftijd op slachtofferschap gevonden; daarom is een training speciaal voor vrouwen, mannen, jongeren en ouderen niet noodzakelijk.

## 5 Vervolgonderzoek

We hebben laten zien dat f2f- en telefoon-social engineering kan worden tegengegaan. Vervolgonderzoek is nodig om beter inzicht te krijgen in hoe op een efficiënte manier het gevaar verminderd kan worden:

1 De interventie had een effect van korte duur. Hoe kunnen 'snelle' herhalingstrainingen worden ingezet om het vervaleffect tegen te gaan? Dit idee is in de context van reanimatievaardigheden getoetst (Sutton et al., 2011). In deze studie kregen de proefpersonen iedere één, twee en drie maanden een vier minuten durende opfristraining. Het eindresultaat (na zes maanden) was een stijging van ca. 20% naar ca. 70% goed uitgevoerde reanimatiehandelingen.

2 De experimenten waren een 'snapshot' van de organisatie op één moment in de tijd. Hoe verandert die snapshot over de tijd? Zijn de proefpersonen die slachtoffer zijn geworden nu beter in staat om zich te verweren dan voor het experiment? Een longitudinale studie kan antwoord geven op deze vragen.

## Literatuur

Bond, C. & B. DePaulo (2006) Accuracy of Deception Judgments. *Personality and Social Psychology Review*, 214-234.

Bond, R. & P. Smith (1996) Culture and conformity: A meta-analysis of studies using Asch's (1952b, 1956) line judgment task. *Psychological Bulletin*, 111-137.

Bosworth, S., M. Kabay & E. Whyne (2014) *Computer Security Handbook*. New Jersey: John Wiley en Sons.

Bullée, J.H. (2017) *Experimental Social Engineering* (diss.). Retrieved from https://research.utwente.nl/en/publications/experimental-social-engineering-investigation-and-prevention .

Bullée, J.H., L. Montoya, M. Junger & P. Hartel (2016) Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. *The singapore cyber-security conference (sg-crc)* (p. 107-114). Singapore: IOS Press.

Bullée, J.H., L. Montoya, M. Junger & P. Hartel (2017) Spear Phishing in Organisations Explained. *Information and Computer Security*, *25*(5), 593-613.

Bullée, J.H., L. Montoya, W. Pieters, M. Junger & P. Hartel (2015) The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, 97-115.

Buller, D. & J. Burgoon (1996) Interpersonal Deception Theory. *Communication Theory*, 1468-2885.

Chmielewski, D. (2015) *Balabit CSI Report*. Retrieved August 05, 2016, from www.balabit.com/news/press/social-engineering-leads-the-top-10-list-of-most-popular-hacking-methods-balabit-survey-results-from-black-hat-usa.

Cialdini, R. (2009) *Influence*. New York: HarperCollins.

Cohen, L. & M. Felson (1979) Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 588-608.

Crowne, D. & D. Marlowe (1960) A new scale of social desirability independent of psychopathology. *Journal of consulting psychology*, 349-354.

Esgate, A., D. Groome & K. Baker (2005) *An Introduction to Applied Cognitive Psychology*. New York: Psychology Press.

Felson, M. (1995) Those who discourage crime. *Crime and place*, *4*, 53-66.

Glenberg, A. (1984) A retrieval account of the long-term modality effect. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 16-31.

Gragg, D. (2003) A multi-level defense against social engineering. *SANS Reading Room*, 2-21.

Graves, R. (1992) *The Greek Myths*. London: Penguin Books.

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

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

ISACA and RSA Conference (2015) State of Cybersecurity: Implications for 2015. In C. Hadnagy & P. Wilson, *Social engineering: The art of human hacking*. NY: Wiley 2010.

Kahneman, D. (2011) *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

McCornack, S. & M. Parks (1986) Deception Detection and Relationship Development: The Other Side of Trust. *Annals of the International Communication Association* , 377-389.

Proofpoint (2016) *The human factor 2016*. Sunnyvale, California: Proofpoint.

Schneier, B. (2000) *Secrets and lies: digital security in a networked world*. New York: John Wiley & Sons.

Stewart, D. & I. Martin (1994) Intended and unintended consequences of warning messages: A review and synthesis of empirical research. *Journal of Public Policy & Marketing*, 1-19.

Sutton, R., D. Niles, P. Meaney, R. Aplenc, B. French, B. Abella, et al. (2011) Low-Dose, High-Frequency CPR Training Improves Skill Retention of In-Hospital Pediatric Providers. *Pediatrics*, 145-151.

The SANS Institute. (2012) *Cyber Security Newsletter (Social Engineering - Hacking Your Mind)*. Retrieved from www.uab.edu/it/home/images/Module02-SocialEngineering-Newsletter.pdf.

Tversky, A. & D. Kahneman (1974) Judgment under Uncertainty: Heuristics and Biases. *Science*, 1124-1131.

Van Dijk, J. & N. Nijenhuis (1979) Ja zeggen, nee doen? Een onderzoek naar de overeenkomst tussen verbale attitudes en feitelijk gedrag bij angstgevoelens tav criminaliteit. *Tijdschrift voor criminologie*, 257-273.

Vrij, A., P. Granhag & S. Porter (2010) Pitfalls and Opportunities in Nonverbal and Verbal Lie Detection. *Psychological Science in the Public Interest*, 89-121.

Weinstein, N. (1980) Unrealistic optimism about future life events. *Journal of personality and social psychology*, 806-820.