Hoe veilig gedragen wij ons online?

Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders

SAMENVATTING

Dr. Susanne van ’t Hoff-de Goede

Dr. Rick van der Kleij

Dr. Steve van de Weijer

Dr. Rutger Leukfeldt

Den Haag, 2019

Centre of Expertise Cybersecurity, De Haagse Hogeschool

Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)

Achtergrond

Onze offline en online levens zijn zo met elkaar verweven dat burgers in Nederland de hele dag door allerlei online activiteiten uitvoeren. Online zijn levert echter ook gevaren op. Online criminaliteit is inmiddels veelvoorkomend en de impact ervan kan groot zijn voor slachtoffers. Cybersecurity professionals hebben geprobeerd slachtofferschap terug te dringen met technische maatregelen, zoals virusscanner en firewalls. Deze maatregelen hebben veelal maar beperkt effect. Een groot deel van slachtofferschap is terug te voeren op het gedrag van mensen. Gebruikers klikken immers op een hyperlink terwijl ze dat niet moeten doen. Of vullen gegevens in op een phishing[1] website waardoor criminelen die gegevens kunnen misbruiken. Om slachtofferschap terug te kunnen dringen is onderzoek naar het gedrag van mensen dan ook van wezenlijk belang.

Onderzoeksdoel en onderzoeksvragen

Kennis over hoe burgers zich online gedragen en hoe zij zich (kunnen) weren tegen online criminaliteit is schaars. Het is tot op heden onbekend hoe Nederlanders zich online gedragen en beschermen tegen online criminaliteit, onder andere omdat hoe mensen zeggen zich online te gedragen niet altijd hetzelfde is als hoe mensen zich daadwerkelijk online gedragen. Voor het empirisch onderbouwen van eventuele interventies op gedrag is dergelijke kennis echter onontbeerlijk. Het is daarom noodzakelijk om meer inzicht te krijgen in de wijze waarop Nederlanders zich online gedragen en welke factoren hiermee samenhangen. Het doel van dit onderzoek is dan ook om in kaart te brengen hoe veilig Nederlanders zich online gedragen en dit te verklaren aan de hand van uit de literatuur naar voren gekomen factoren. Hiermee kan een eerste aanzet worden gegeven om interventies te ontwikkelen om Nederlanders zich online veiliger te laten gedragen. De hoofdvraag van dit rapport is: “Hoe veilig gedragen Nederlanders zich online en hoe kan dit worden verklaard?” De volgende deelvragen worden beantwoord in dit rapport:

1) Hoe veilig gedragen Nederlanders zich online?
2) Is er een onderlinge samenhang tussen kennis, gelegenheid en motivatie?
3) Is er onderlinge samenhang tussen verschillende cybergedragingen?
4) Kan het cybergedrag[2] van Nederlanders worden verklaard door hun kennis van online veiligheid?

[1] Phishing is een vorm van online oplichting, waarbij criminelen e-mails of websites van legitieme instanties namaken om slachtoffers te misleiden, om zodoende inloggegevens te achterhalen en toegang te krijgen tot online accounts.
[2] Online gedrag wordt in dit rapport cybergedrag genoemd, een term die synoniem is aan de term online gedrag en alle cybergedragingen van mensen beslaat.

5) Kan het cybergedrag van Nederlanders worden verklaard door de gelegenheid die zij hebben voor veilig cybergedrag?
6) Kan het cybergedrag van Nederlanders worden verklaard door de motivatie die zij hebben voor veilig cybergedrag?
7) Kan het cybergedrag van Nederlanders worden verklaard door andere factoren?
8) Verschilt het cybergedrag van Nederlanders tussen bevolkingsgroepen?
9) Worden de effecten van kennis, gelegenheid en motivatie op cybergedrag beïnvloed door andere factoren?

Onderzoeksmethoden

Om de onderzoeksvragen te beantwoorden zijn verschillende methoden gebruikt: een literatuurstudie, een experimentele survey en een discussiebijeenkomst. Het onderzoek is gestart met de literatuurstudie. De literatuurstudie is uitgevoerd om inzicht te krijgen in bestaande kennis over cybergedrag, risicofactoren die samenhangen met slachtofferschap van online criminaliteit en onveilig cybergedrag, factoren die van belang zijn voor gedragsverandering en verleidingstechnieken.

Vervolgens is op basis van de literatuurstudie een survey ontwikkeld die met behulp van een panelbureau is uitgezet. De uiteindelijke steekproef bestaat uit 2.426 personen en is representatief voor de Nederlandse samenleving met betrekking tot de kenmerken geslacht, werkend (ja/nee) en provincie waarin zij woonachtig zijn, maar respondenten zijn vaker hoogopgeleid en gemiddeld ouder. We maken gebruik van een zogenaamde “population based survey experiment” (experimentele survey). In de vragenlijst werd cybergedrag op twee manieren gemeten: 1) door zelf-rapportage, door enerzijds vragen en stellingen en anderzijds vignetten voor te leggen aan de respondent 2) daarnaast zijn respondenten tijdens het invullen van de vragenlijsten (fictieve) cyberrisico-situaties tegenkomen, waarbij de onderzoekers bekeken hoe de respondenten met deze situaties omgaan. Dit vormde de metingen van het daadwerkelijke cybergedrag van respondenten. De survey geeft dan ook inzicht in welke mate mensen denken zich veilig of onveilig te gedragen en in welke mate mensen daadwerkelijk veilig of onveilig cybergedrag vertonen.

Tenslotte zijn de eerste resultaten van de analyses besproken met experts uit verschillende werkvelden tijdens een discussiebijeenkomst. Doel van deze bijeenkomst was om te komen tot een eerste aanzet tot praktisch bruikbare aanbevelingen om cyberrisico’s te voorkomen of tegen te gaan. Daarom is voorafgaand aan de bijeenkomst eerst een literatuurstudie gedaan naar bestaande interventies die gedragsverandering bewerkstelligen. Tijdens de bijeenkomst zijn de resultaten van de experimentele

surveystudie en het literatuuronderzoek naar interventies bediscussieerd en konden de experts kritisch reflecteren op de gebruikte onderzoeksmethoden, de resultaten en veelbelovende richtingen voor interventies die zorgen voor veilig cybergedrag.

Conclusies literatuurstudie

Het doel van de literatuurstudie was om uiteen te zetten hoe cybergedrag in eerdere studies is onderzocht en gemeten. Ook is gekeken welke verklaringen voor het vertonen van onveilig of veilig cybergedrag gevonden zijn. Allereerst laat de literatuurstudie zien dat het schetsen van een risicoprofiel voor slachtofferschap van online criminaliteit niet mogelijk is op basis van persoonskenmerken of routine activiteiten. Wel komen enkele factoren naar voren die mogelijk relevant zijn voor cybergedrag en om die reden zijn meegenomen in de huidige studie. Deze factoren zijn: leeftijd, sociaaleconomische status, geslacht en gezinssamenstelling. Daarnaast blijkt dat onderzoek zich zou moeten richten op *gedrag* als pijler voor het verlagen van het risico op slachtofferschap, namelijk veilig cybergedrag. Dit is dan ook het hoofdonderwerp van de huidige studie. Verder laat de literatuurstudie zien dat de mate waarin mensen zich online veilig gedragen op basis van theoretische verklaringsmodellen (in het bijzonder de Protection Motivation Theory (PMT) en het COM-B ('Capability', 'Opportunity', 'Motivation' en 'Behaviour') model, waar kennis, gelegenheid en motivatie centraal staan) afhangt van de capaciteiten die mensen hebben om zich veilig te gedragen, de gelegenheid die zij daartoe hebben en de mate waarin zij gemotiveerd zijn om zich veilig te gedragen. Daarnaast wijst de theorie op het belang van zelfcontrole en eerder slachtofferschap. Ten slotte zijn er factoren die niet zijn afgeleid uit deze theoretische modellen maar wel relevant lijken voor cybergedrag: gemoedstoestand, angst voor slachtofferschap, type apparaat, tijdsdruk en verleidingstechnieken. Gemoedstoestand kan besluitvorming beïnvloeden en heeft een effect op de strategieën die we kiezen bij het nemen van beslissingen. Angst voor slachtofferschap kan verschillende gevolgen hebben voor cybergedrag, zoals vermijdingsgedrag maar ook het nemen van minder risico's online. Ook is het apparaat dat gebruikt wordt om online te gaan van belang. Apparaten die mensen thuis gebruiken voor online activiteiten, zoals een smartphone, tablet, laptop of pc, verschillen op een aantal dimensies die van invloed zijn op cybergedrag en kunnen van invloed zijn op slachtofferschap. Tijdsdruk zou ervoor kunnen zorgen dat mensen signalen dat zij risico lopen, negeren en zodoende meer risico's nemen. Ook de verleidingstechnieken die cybercriminelen gebruiken bij hun aanvallen lijken belangrijk. Alle factoren die uit de literatuurstudie naar voren kwamen, zijn in onderhavig onderzoek meegenomen. De huidige studie heeft dan ook onderzocht in hoeverre cybergedrag kan worden verklaard door alle hierboven genoemde factoren.

Resultaten en conclusies experimentele survey

Onderzoeksvraag 1: Hoe veilig gedragen Nederlanders zich online?

Onveilig gedrag blijkt in hoge mate voor te komen. Zo gebruikt bijna 60 procent een zwak wachtwoord, download 40 procent onveilige software, en deelt ongeveer 30 procent van de respondenten persoonlijke gegevens, zoals hun volledige naam, geboortedatum en e-mailadres. Als respondenten phishing e-mails krijgen voorgelegd dan blijkt dat ruim 20 procent een onveilige keuze maakt: ze klikken naar eigen zeggen op de hyperlink of kopiëren de URL naar de webbrowser.

Dat burgers zich online onveilig gedragen komt deels naar voren uit de analyses over zelf-gerapporteerd gedrag, maar vooral ook tijdens de objectieve metingen van gedrag. Het blijkt echter dat er grote verschillen bestaan tussen het zelf-gerapporteerde gedrag en het objectieve gedrag. Uit de objectieve metingen blijkt steeds dat mensen zich nog onveiliger gedragen dan dat ze rapporteren te doen. Hieronder bespreken we beknopt de conclusies voor elk van de zeven gedragsclusters (gebruik van wachtwoorden, opslaan van belangrijke bestanden, installeren van updates, gebruik van beveiligingssoftware, alertheid tijdens internetgebruik, online delen van persoonlijke gegevens en omgaan met bijlagen en hyperlinks in e-mails).

- *Gebruik van wachtwoorden*. Respondenten rapporteren zelf dat ze veilig omgaan met wachtwoorden. Ze scoren hoog op veiligheid als het gaat om het niet delen van wachtwoorden met anderen en het gebruik van moeilijke wachtwoorden. De objectieve metingen laten een ander beeld zien: 89 procent van de respondenten heeft een zwak wachtwoord gebruikt. Zelfs als we alleen kijken naar de respondenten die aan het eind van de vragenlijst aangeven dat ze een wachtwoord hebben gekozen op dezelfde wijze als ze dat normaal zouden doen, dan blijkt dat ruim 83 procent een zwak wachtwoord gebruikt. Als we nóg iets specifieker kijken naar het gedrag van de respondenten en als uitgangspunt nemen dat alleen de lengte van het wachtwoord ertoe doet en we weer alleen kijken naar de groep die aan heeft gegeven op eenzelfde wijze het wachtwoord te hebben gekozen, blijkt dat 51 procent een wachtwoord van zeven of minder tekens kiest.
- *Opslaan van belangrijke bestanden, installeren van updates en gebruik van beveiligingssoftware.* Via zelfrapportage is gemeten hoe respondenten omgaan met het opslaan van bestanden, updaten van software en gebruiken van beveiligingssoftware. Van alle zeven gedragsclusters rapporteren

respondenten gemiddeld het minst veilige gedrag omtrent het opslaan van bestanden. Op het gebied van updaten van software werd op alle stellingen gemiddeld een hoge (veilige) score gerapporteerd, zoals het installeren van updates van besturingssystemen, apps/software en beveiligingssoftware zodra er een nieuwe update beschikbaar is.

- *Alertheid tijdens internetgebruik.* Bij het online alert zijn zien we eenzelfde beeld: respondenten geven middels zelfrapportage aan zich (zeer) veilig te gedragen (bijvoorbeeld niet downloaden uit illegale bron, geen gebruik maken van openbare wifi), terwijl uit de objectieve meting blijkt dat 40 procent van de respondenten onbekende software download als er een pop-up verschijnt tijdens een video die niet wil afspelen.
- *Online delen van persoonlijke gegevens*. Bij het delen van persoonlijke gegevens geven respondenten aan zich bewust te zijn van de gevaren van het delen van persoonlijke gegevens zoals een huisadres, e-mailadres of telefoonnummer en connectieverzoeken via sociale media. Tijdens de objectieve meting blijken respondenten echter vaak bereid tot het opgeven van (zeer) persoonlijke gegevens. Zo geeft een aanzienlijk deel zijn of haar geboortedatum (37,5%), volledig naam (31%), e-mailadres (28,1%) en hun postcode (27,0%) en huisnummer (20,4%). Een klein maar toch substantieel deel van de respondenten (4,8%) is bovendien bereid tot het invullen van de laatste drie cijfers van hun bankrekeningnummer.
- *Omgaan met bijlagen en hyperlinks in e*-mails. Respondenten rapporteren zich veilig te gedragen als het aankomt op het omgaan met bijlagen en hyperlinks in e-mails. Zo verwijderen respondenten e-mails die zij niet vertrouwen heel vaak en openen zij bijna nooit bijlagen in e-mails van onbekende afzenders. Uit de vignetten die die respondenten zijn voorgelegd – drie e-mails waarvan twee phishing e-mails en één legitieme e-mail – waarbij ze moesten aangeven hoe ze zouden omgaan met de e-mails blijkt echter dat 21 procent een onveilige handeling verricht: ze klikken op de hyperlink van een phishing e-mail, of typen de URL over de in webbrowser.

Onderzoekvraag 2 en 3: Is er een onderlinge samenhang tussen kennis, gelegenheid en motivatie en is er onderlinge samenhang tussen verschillende cybergedragingen?

Met het uiteindelijke doel om tot gedragsinterventies te komen die de veiligheid van online gedrag van Nederlanders verhogen, was het van belang om te proberen te achterhalen hoe eigenschappen en gedragingen over de populatie zijn verdeeld. Hebben mensen met veel kennis van online veiligheid

bijvoorbeeld over het algemeen ook meer sociale en materiële gelegenheid[3] en motivatie voor veilig online gedrag? De resultaten tonen aan dat het antwoord op die vraag nee is; er zijn nauwelijks verbanden tussen achterliggende kenmerken die veilig cybergedrag zouden kunnen verklaren.

Vervolgens was het van belang te onderzoeken of de verschillende cybergedragingen samenhangen. Bijvoorbeeld, gedragen mensen die een sterk wachtwoord kiezen zich gemiddeld ook veiliger op andere cybergedragingen? Deze vraag kan eveneens negatief beantwoord worden. De resultaten van de huidige studie wijzen erop dat hoe veilig mensen zich gedragen in een bepaald cybergedragscluster zeer beperkt samenhangt met hoe veilig zij zich gedragen in een ander cybergedragscluster. Wanneer iemand bijvoorbeeld met betrekking tot het omgaan met een phishing e-mail veilig gedrag laat zien, betekent dit niet dat zij zich gemiddeld ook veilig zullen gedragen op het gebied van het kiezen van een sterk wachtwoord. Er is zelfs een (zeer kleine) negatieve samenhang gevonden tussen wachtwoord sterkte en het delen van persoonlijke gegevens, wat erop wijst dat hoe sterker het wachtwoord is dat respondenten kiezen, hoe onveiliger zij zich gedragen bij het invullen van persoonlijke gegevens.

Tot slot kan worden gevraagd of een focus op daadwerkelijk gedrag noodzakelijk is in vervolgonderzoek. Komen zelf-gerapporteerde en objectieve metingen van gedrag genoeg overeen om onderzoek te baseren op (het veel eenvoudiger te verzamelen) zelf-gerapporteerde data? De resultaten van de huidige studie onderschrijven het belang van het doen van objectieve metingen van cybergedrag. Er is zeer beperkte overeenkomst tussen hoe mensen *zeggen* zich online te gedragen en hoe mensen zich *daadwerkelijk* blijken te gedragen in de huidige studie.

Onderzoeksvraag 4-7: Kan het cybergedrag worden verklaard door kennis, motivatie, gelegenheid of andere relevante factoren?

Op basis van de literatuur zijn de belangrijkste voorspellende factoren die zijn meegenomen in dit onderzoek kennis, gelegenheid en motivatie. De verwachting was dat deze factoren samenhangen met cybergedrag. Uit de zelf-rapportage komt ook precies dat beeld: zowel kennis, gelegenheid als motivatie hangen positief samen met zelf-gerapporteerd veilig cybergedrag. Als we echter kijken naar daadwerkelijk cybergedrag, dan ontstaat er een ander beeld. Alleen kennis blijkt significant samen te hangen met een

[3] De sociale omgeving (de mensen om ons heen) kan gelegenheid bieden voor gedrag, bijvoorbeeld door het steunen van gewenst gedrag. De materiële omgeving kan gelegenheid bieden voor gedrag, bijvoorbeeld door de beschikbaarheid van hulpmiddelen.

tweetal gedragingen: wachtwoord sterkte en het downloaden van onveilige software (klikgedrag). Echter, het verband is een negatieve: hoe meer kennis mensen hebben, hoe minder sterk het wachtwoord dat ze aanmaken. En: voor elke punt die respondenten hoger scoren op de kennistest, wordt de kans minder groot dat zij een veilige keuze maken bij de software pop-up. De sterkte van het gekozen wachtwoord en het al dan niet downloaden van onveilige software hangt niet significant samen met de (sociale of materiële) gelegenheid of motivatie die respondenten hebben voor veilig cybergedrag. Slechts één verband tussen kennis, gelegenheid, motivatie en de veiligheid van objectieve cybergedragingen komt overeen met de verwachting uit de theorie: wanneer mensen meer kennis hebben van online veiligheid, gedragen zij zich veiliger op het gebied van het delen van persoonlijke gegevens.

Naast kennis, gelegenheid en motivatie zijn op basis van de literatuurstudie verschillende overige factoren meegenomen in de analyses die mogelijk samenhangen met cybergedrag. We bekeken daarom of cybergedrag samenhangt met een negatieve of positieve gemoedstoestand, angst voor slachtofferschap, eerder slachtofferschap, zelfcontrole, type apparaat, tijdsdruk, verleidingstechnieken die criminelen gebruiken, dreiging-evaluatie, maatregel-evaluatie en locus of control.

Zelf-gerapporteerd cybergedrag hangt samen met een aantal van de hierboven genoemde factoren. Een negatieve gemoedstoestand hangt negatief samen met zelf-gerapporteerd veilig cybergedrag. Ofwel, hoe groter de negatieve gemoedstand van respondenten, hoe minder veilig hun zelf-gerapporteerde cybergedrag is. Een positieve gemoedstoestand hangt daarentegen positief samen met de veiligheid van zelf-gerapporteerd cybergedrag. Op basis van eerder onderzoek hadden we juist verwacht dat een positieve gemoedstoestand negatief zou samenhangen met veilig gedrag. Burgers zien de uitkomsten van risicovolle situaties sneller als meer positief en zijn dan ook meer bereid om risico's te nemen, zo was de verwachting. De resultaten laten echter een ander beeld zien. Een verklaring kan op basis van de huidige studie niet worden gegeven. Ook zelfcontrole hangt significant samen met zelf-gerapporteerd cybergedrag. In lijn met de verwachting is gevonden dat hoe meer zelfcontrole respondenten hebben, hoe veiliger hun (zelf-gerapporteerde) cybergedrag is. Het type apparaat waarop de vragenlijst is ingevuld, hangt ook samen met zelf-gerapporteerd gedrag: respondenten die een pc of laptop gebruikten geven aan zich veiliger online te gedragen dan zij die een tablet gebruikten.

Kijken we echter naar daadwerkelijk gedrag, dan blijven alleen een positieve gemoedstoestand, angst voor slachtofferschap, eerder slachtofferschap, type apparaat en verleidingstechnieken over. Een positieve gemoedstoestand hangt samen met zowel de wachtwoord sterkte als het downloaden van software uit onbetrouwbare bron, maar in tegenovergestelde richting. Hoe groter de positieve

gemoedstoestand van respondenten, hoe sterker het gekozen wachtwoord. Daarentegen is, in lijn met de literatuur, gevonden dat hoe groter de positieve gemoedstoestand van respondenten, hoe groter de kans is dat zij een onveilige keuze maken bij de software pop-up (klikgedrag). De positieve gemoedstoestand hangt samengenomen dan ook samen met zowel veilig als onveilig cybergedrag; afhankelijk van het type cybergedrag is dit verband negatief of positief. Angst voor slachtofferschap hangt positief samen met wachtwoord sterkte: hoe meer angst respondenten hebben om slachtoffer te worden van online criminaliteit, hoe sterker het door hen gekozen wachtwoord is. Eerder slachtofferschap daarentegen is negatief gerelateerd aan de veiligheid van daadwerkelijk klikgedrag: respondenten die ooit eerder slachtoffer zijn geworden van online criminaliteit maken significant minder vaak een veilige keuze bij de software pop-up. Het type apparaat heeft ook invloed op daadwerkelijk cybergedrag. Respondenten die een pc of laptop gebruiken kiezen een minder sterk wachtwoord dan respondenten die een tablet gebruiken. Datzelfde geldt voor het wel of niet downloaden van software van onbetrouwbare bron en het delen van persoonlijke gegevens. Respondenten die een smartphone gebruikten maken bovendien vaker een veilige keuze dan respondenten op een tablet bij het downloaden. Tot slot blijkt een van de verleidingstechnieken die cybercriminelen gebruiken samen te hangen met onveilig cybergedrag. Respondenten op wie de verleidingstechniek wederkerigheid is toegepast, delen significant meer persoonlijke gegevens.

Ten slotte is onderzocht of de manier waarop mensen de dreiging en maatregelen van online veiligheid evalueren, invloed heeft op de mate waarin zij gemotiveerd zijn zichzelf te beschermen. Zowel dreiging-evaluatie, maatregel-evaluatie en locus of control hebben een positieve samenhang met de motivatie tot online zelfbescherming. Op basis van de PMT kan worden verwacht dat deze motivatie de veiligheid van cybergedrag beïnvloed. Die conclusie kunnen we echter niet trekken. Als we kijken naar de relatie tussen dreiging-evaluatie, maatregel-evaluatie en locus of control en cybergedrag, dan zien we slechts één significant verband: die van maatregel-evaluatie op de veiligheid van zelf-gerapporteerd cybergedrag. Maatregel-evaluatie, de mate waarin respondenten vinden dat maatregelen voor online veiligheid effectief zijn en zij zelf in staat zijn die maatregelen te nemen en de kosten van deze maatregelen niet te hoog zijn, hangt positief samen met zelf-gerapporteerd cybergedrag. Hoe hoger de maatregel-evaluatie, hoe meer veilig cybergedrag wordt gerapporteerd. Bij alle objectief gemeten cybergedragingen (wachtwoord sterkte, klikgedrag en het delen van persoonlijke gegevens) en bij de vignet meting (e-mail keuze) zien we zelfs helemaal geen verbanden met de elementen uit de PMT.

Onderzoeksvraag 8: Verschilt het cybergedrag van Nederlanders tussen bevolkingsgroepen?

Enkele van de achtergrondkenmerken van respondenten hangen samen met zelf-gerapporteerd cybergedrag. Hoe hoger de leeftijd, hoe veiliger het gerapporteerde cybergedrag en hoe veiliger omgegaan wordt met hyperlinks in phishing e-mails. Voor opleiding is de relatie negatief: hoe hoger de opleiding, hoe minder veilig het zelf-gerapporteerde cybergedrag is. Het hebben van inwonende kinderen, jonger dan 16 jaar, hangt tot slot samen met minder veilig omgaan met hyperlinks in phishing e-mails.

Bij daadwerkelijk cybergedrag vinden we ook een aantal relaties met kenmerken van respondenten. Zo heeft het hebben van werk een significant verband met zowel wachtwoord sterkte als het wel of niet downloaden van software van onbetrouwbare bron. Werkenden kiezen een minder sterk wachtwoord en downloaden vaker de software uit onbetrouwbare bron. Daarnaast kiezen respondenten met een hogere opleiding een minder sterk wachtwoord, maar gedragen zij zich wel veiliger op het gebied van delen van persoonlijke gegevens. Het klikgedrag van mannen is gemiddeld minder veilig dan dat van vrouwen en zij delen eveneens meer persoonlijke gegevens. Samenwonenden vertonen daarentegen juist veiliger klikgedrag. Tot slot lijkt het erop dat hoe ouder burgers zijn, hoe meer persoonlijke gegevens zij delen.

Onderzoeksvraag 9: Worden de effecten van kennis, gelegenheid en motivatie op cybergedrag beïnvloed door andere factoren?

Onderzocht is of de verbanden van kennis, gelegenheid en motivatie met de veiligheid van cybergedrag verklaard kunnen worden door interacties van deze variabelen met de volgende (moderator) variabelen: negatieve gemoedstoestand, positieve gemoedstoestand, angst voor slachtofferschap, slachtofferschap (ooit) en zelfcontrole. Samengenomen wijzen de resultaten erop dat de meeste interacties niet significant zijn, maar in enkele gevallen worden de verbanden van kennis, gelegenheid en motivatie met de veiligheid van cybergedrag beïnvloed door zelfcontrole, gemoedstoestand, angst voor slachtofferschap en in één geval ook door eerder slachtofferschap

De meeste significante interacties zijn gevonden in de analyses waarin zelf-gerapporteerd cybergedrag en de wachtwoord sterkte worden voorspeld. Uit enkele interacties blijkt dat de richting van de gevonden verbanden afhangt van hoe hoog men scoort op de moderator variabelen. Zo blijkt bijvoorbeeld dat onder respondenten met zeer weinig angst voor slachtofferschap het verband tussen sociale gelegenheid en de veiligheid van zelf-gerapporteerd cybergedrag positief is. Echter, naarmate de angst voor slachtofferschap toeneemt, wordt dit verband telkens zwakker. Bij respondenten met (zeer)

veel angst voor slachtofferschap is het verband zelfs negatief: zij rapporteren dus minder veilig gedrag wanneer de sociale gelegenheid toeneemt.

Daarnaast zijn er een aantal interacties waarbij de gevonden verbanden niet van richting veranderen maar sterker worden, naarmate men hoger of lager scoort op de moderatie-variabelen. Het positieve verband tussen motivatie en de veiligheid van zelf-gerapporteerd cybergedrag wordt bijvoorbeeld minder sterk naarmate respondenten een positiever gemoedstoestand hebben en naarmate respondenten meer angst voor slachtofferschap hebben.

Onderzoeksbeperkingen

Zoals elke onderzoek kent ook dit onderzoek beperkingen. Ten eerste hebben we dan wel een relatief groot aantal respondenten die representatief zijn voor de Nederlandse samenleving op geslacht, werkend (ja/nee) en de provincie waarin zij woonachtig zijn, maar helemaal representatief zijn de data niet. Zo zijn respondenten vaker dan gemiddeld in Nederland hoogopgeleid en zijn respondenten minder vaak dan gemiddeld jonger dan 39 jaar.

De grote toegevoegde waarde van deze studie is dat niet alleen zelf-gerapporteerd gedrag is gemeten, maar ook daadwerkelijk gedrag op objectieve wijze is gemeten. Dit is ook nog eens gedaan op een grote steekproef door mensen die op hun eigen apparaat in hun eigen huis allerlei vragen beantwoorden over hun cybergedrag. De experimenten hebben echter ieder hun eigen beperkingen. Ten eerste was het door de lengte van de vragenlijst niet mogelijk om experimenten voor alle zeven gedragsclusters op te nemen. Ook weten we bij de variabelen over het delen van persoonlijke gegevens niet welke gegevens door de respondenten zijn ingevuld en of dit werkelijk/juiste gegevens waren. Bij de meting over het al dan niet downloaden van onveilige software (klikgedrag) zijn mogelijk andere factoren van invloed geweest op de resultaten. Zo maakten we gebruik van een pop-up die was gemaakt in de stijl van het Windows besturingssysteem. Dus niet-Windows gebruikers zijn minder bekend met de pop-up. Hierdoor zijn zij mogelijk wantrouwender of juist eerder geneigd ja te zeggen. Verder onderzoek is nodig, met verschillende pop-ups die ook technisch werkelijk pop-ups zijn en zich aanpassen aan apparaat en besturingssysteem. Tenslotte, hoewel de methode – een survey met experimenten – heel geschikt is om dit soort onderzoek te doen, hebben we natuurlijk ook te maken met respondenten die zich misschien veilig wanen in de online omgeving van het panelbureau. Hierdoor hebben zij mogelijk sneller onveilige keuzes gemaakt dan anders.

Een doorkijkje: interventies

Het doel van dit onderzoek was om in kaart te brengen hoe Nederlanders zich online gedragen en dit te verklaren aan de hand van uit de literatuur naar voren gekomen factoren, om zodoende een eerste aanzet te geven om interventies te ontwikkelen om Nederlanders zich online veiliger te laten gedragen. De resultaten van dit onderzoek zijn dan ook bediscussieerd met experts om veelbelovende richtingen voor interventies te identificeren.

Samenvattend blijkt dat er geen panacee is voor het bevorderen van veilig cybergedrag. Verschillende cybergedragingen lijken andere oorzaken te hebben. Ook bestaat het beeld onder de experts dat mensen verschillen in hun gevoeligheid voor interventies en dat de timing van interventies cruciaal is voor het doen slagen van beïnvloeding. De experts zien wel veel waarde in interventies die zich richten op aanpassingen van de techniek die mensen gebruiken voor online activiteiten, dusdanig dat de mogelijkheid voor onveilig gedrag wordt verkleind en de mogelijkheid voor veilig gedrag wordt vergroot, ook wel security-by-design genoemd. Het stimuleren van fabrikanten van technologie via beleidsmaatregelen tot het maken van aanpassingen die het voor mensen makkelijker maakt om zich veilig te gedragingen kan hieraan bijdragen. Het ontwerpen van specifieke interventies gericht op fabrikanten of burgers zelf is echter geen sinecure. Toekomstig onderzoek zou zich kunnen richten op het ontwikkelen en evalueren van een specifieke set van interventies voor het beïnvloeden van de door ons gevonden onveilige gedragingen.