Ons cybergedrag is veel onveiliger dan we zelf denken

Implicaties voor effectief beïnvloedingsbeleid door de overheid

Rick van der Kleij, Susanne van 't Hoff-de Goede, Steve van de Weijer en Rutger Leukfeldt*

In 2018 gaf 8,5% van de internetgebruikers van 12 jaar of ouder aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van online criminaliteit (CBS 2019). In totaal zijn dat jaar 1,2 miljoen Nederlanders slachtoffer geworden van online criminaliteit. Zo werd 2,9% van de Nederlanders slachtoffer van fraude met online handel en 1% slachtoffer van identiteitsdiefstal (CBS 2019). Recente studies laten zien dat de impact van slachtofferschap van dergelijke delicten hoog kan zijn en dat slachtoffers naast financiële schade diverse vormen van psychologische en emotionele schade ervaren (Cross e.a. 2016; Jansen & Leukfeldt 2018; Leukfeldt e.a. 2018; 2019).
Slachtofferschap van online fraude komt dus veel voor en de impact ervan kan groot zijn voor slachtoffers. Cybersecurityprofessionals hebben geprobeerd slachtofferschap terug te dringen met technische maatregelen, zoals software voor het detecteren van datalekken. Deze maatregelen hebben veelal maar beperkt effect (bijv. Hauer 2015). Een groot deel van slachtofferschap van cybercriminaliteit is terug te voeren op het online gedrag van mensen (Munnichs e.a. 2017; Ancher e.a. 2019). Dit geldt ook voor slachtofferschap van online oplichting en fraude. Internetgebruikers die onbetrouwbare webshops en phish-

* Dr. R. van der Kleij werkt als senior onderzoeker bij het lectoraat Cybersecurity in het mkb aan de Haagse Hogeschool en als senior onderzoeker bij TNO. Dr. S. van 't Hoff-de Goede is als onderzoeker verbonden aan het lectoraat Cybersecurity in het mkb aan de Haagse Hogeschool. Dr. S. van de Weijer is als onderzoeker verbonden aan het NSCR. Dr. E.R. Leukfeldt werkt als lector Cybersecurity in het mkb aan de Haagse Hogeschool en als senior onderzoeker bij het NSCR. Dit artikel bevat een weergave van de belangrijkste uitkomsten van een recent onderzoek naar cybergedrag dat door de auteurs is uitgevoerd in opdracht van het WODC. Delen van dit artikel zijn ook te vinden in Van 't Hoff-de Goede e.a. 2019. Het doel van dit artikel is om op basis van de belangrijkste uitkomsten implicaties voor beleidsmakers te schetsen.

doi: 10.5553/JV/016758502020046002011

ingmails niet herkennen, hebben een grote kans om opgelicht te worden. Daarnaast kan het veelvuldig delen van persoonlijke gegevens de kans op identiteitsdiefstal verhogen. Een belangrijke vraag is daarom hoe veilig we ons online gedragen, en om slachtofferschap van online oplichting en fraude terug te kunnen dringen, is onderzoek naar het online gedrag van mensen dan ook van wezenlijk belang (Leukfeldt 2017; Rhee e.a. 2009; Talib e.a. 2010).

Zeggen is een, doen is twee

Kennis over hoe gebruikers zich (kunnen) weren tegen online criminaliteit is schaars (zie voor een overzicht bijv. Leukfeldt 2017). Het is tot op heden grotendeels onbekend hoe Nederlanders zich 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 (Crossler e.a. 2013; Debatin e.a. 2009; Warkentin e.a. 2012; Workman e.a. 2008).
Voor het empirisch onderbouwen van eventueel beïnvloedingsbeleid door de overheid op het gedrag van internetgebruikers, zoals een publiekscampagne, is dusdanige kennis echter onontbeerlijk. Daarmee kan slachtofferschap van cybercriminaliteit mogelijk zelfs worden voorkomen. Daarom hebben de Haagse Hogeschool en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) een onderzoek uitgevoerd in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) om in kaart te brengen hoe veilig Nederlanders zich online zeggen te gedragen, hoe (on)veilig ze zich daadwerkelijk gedragen en welke verklaringen hiervoor zijn (Van 't Hoff-de Goede e.a. 2019). In dit artikel gaan wij in op de belangrijkste uitkomsten van dit onderzoek, en hierbij staan de volgende onderzoeksvragen centraal: Welke factoren hangen samen met veilige online gedragingen? En wat zijn hiervan de beleidsimplicaties om slachtofferschap van cybercriminaliteit te voorkomen?
Om cybergedrag in kaart te brengen maakten we gebruik van het COM-B-gedragsmodel (Capability, Opportunity, Motivation – Behaviour), wat veronderstelt dat Capability, Opportunity en Motivation (COM) gezamenlijk leiden tot Behaviour (B). In het Nederlands: gedrag wordt aangedreven door kennis, gelegenheid en motivatie. Op basis van dit theoretische verklaringsmodel verwachten we aldus dat

doi: 10.5553/JV/016758502020046002011

de mate waarin mensen zich online veilig gedragen, afhangt van de kennis die mensen bezitten over risico's en manieren om zichzelf te beschermen, de gelegenheid die zij daartoe hebben en de mate waarin zij gemotiveerd zijn om zich veilig te gedragen (zie ook Michie e.a. 2011). Deze factoren hebben we meegenomen in ons onderzoek. Dit gedragsmodel is nog niet eerder gebruikt om cybergedrag te onderzoeken. Daarnaast nemen we ook andere factoren mee die in de literatuur worden genoemd als mogelijk relevant voor cybergedrag. In dit artikel bespreken we een selectie van deze factoren, namelijk: gemoedstoestand, angst voor slachtofferschap, eerder slachtofferschap, type apparaat en tijdsdruk.

De gemoedstoestand kan besluitvorming beïnvloeden en heeft een effect op de strategieën die we kiezen bij het nemen van beslissingen. Gemoedstoestand wordt gedefinieerd als een emotionele toestand die ten minste enige minuten aanhoudt (Matthews e.a. 1995). Deze gemoedstoestand kan positief zijn of negatief. Voorbeelden van positieve dan wel negatieve gemoedstoestanden zijn respectievelijk enthousiast en overstuur. Matthews en collega's (1995) vonden dat informatie die past bij de gemoedstoestand sneller wordt gevonden in het geheugen. Een negatieve gemoedstoestand kan er bijvoorbeeld toe leiden dat mensen minder risico's nemen, omdat zij makkelijker toegang hebben tot negatieve gedachten over de uitkomst van het risicovolle gedrag. Daarnaast kan angst voor slachtofferschap of eerder slachtofferschap verschillende gevolgen hebben voor cybergedrag, zoals vermijdingsgedrag, maar ook het nemen van minder risico's online (Boss e.a. 2015). 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 desktopcomputer, verschillen op een aantal dimensies die van invloed zijn op cybergedrag, en kunnen van invloed zijn op slachtofferschap. Vishwanath (2016) heeft al laten zien dat mobiele gebruikers vaker slachtoffer worden van phishing dan gebruikers van een desktopcomputer. Door de draagbaarheid, het gebruiksgemak en de beschikbaarheid zijn gebruikers van mobiele apparaten meer cognitief ontspannen, zo luidt de verklaring, wat leidt tot meer gewoontegedrag (zoals het klikken op hyperlinks) en daarmee tot verhoogde kans op slachtofferschap. Tot slot zou tijdsdruk ervoor kunnen zorgen dat mensen signalen dat zij risico lopen, negeren en zodoende meer risico's nemen. Een veelgebruikte strategie die mensen hanteren in het omgaan met tijdsdruk is

doi: 10.5553/JV/016758502020046002011

het gebruiken van meer oppervlakkige (heuristische) informatieverwerking (Alison e.a. 2013). Dit kan betekenen dat zij belangrijke cues die kunnen duiden op risico's die zijn verbonden aan het handelen, zoals het klikken op een hyperlink, over het hoofd zien. De huidige studie heeft dan ook onderzocht in hoeverre cybergedrag kan worden verklaard door alle hierboven genoemde factoren.
Dit artikel vat de belangrijkste resultaten samen van het door de auteurs uitgevoerde onderzoek en sluit af met enkele beleidsimplicaties. Wie meer wil lezen over het onderzoek verwijzen we naar het onderzoeksrapport (Van 't Hoff-de Goede e.a. 2019). De volgende paragraaf behandelt de methodologie die is gebruikt voor het onderzoek. In de paragraaf daarna worden de belangrijkste bevindingen van het vragenlijstonderzoek en de gedragsmetingen gepresenteerd. Deze paragraaf focust op het beantwoorden van de belangrijkste onderzoeksvragen, die aan de basis lagen van dit onderzoek. De laatste paragraaf staat stil bij de beleidsimplicaties en vervolgonderzoek.

Methode

Voor de uitvoering van het onderzoek zijn verschillende methoden gebruikt: een vragenlijst, objectieve gedragsmetingen en een discussiebijeenkomst. Op basis van een systematische literatuurstudie is een vragenlijst 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 geslacht, arbeidsstatus en de provincie waarin men woont. Respondenten zijn echter vaker dan gemiddeld in Nederland hoogopgeleid (50,0% versus 30,0%). Ook zijn respondenten minder vaak dan gemiddeld jonger dan 39 jaar (13,8% versus 29,4%). In de vragenlijst is cybergedrag gemeten door enerzijds vragen, stellingen en vignetten voor te leggen aan de respondenten. Anderzijds zijn objectieve metingen van gedrag gedaan. Tijdens het invullen van de vragenlijst zijn respondenten drie gesimuleerde cyberrisicosituaties tegengekomen, waar zij onwetend van waren. Hierbij hebben wij bekeken hoe de respondenten met deze situaties omgingen. Allereerst is de respondenten aan het begin van de vragenlijst gevraagd om een gebruikersnaam en wachtwoord aan te maken, waarbij wij de sterkte van het gekozen wachtwoord konden achterhalen. Verder verscheen er tijdens de vragenlijst ineens een

doi: 10.5553/JV/016758502020046002011

pop-up, waarin stond dat om verder te kunnen gaan met de vragenlijst er software moest worden gedownload. Deze software was afkomstig uit een onbetrouwbare bron. Ook hier konden we zien welke keuze de respondenten maakten: downloaden, niet downloaden of zelfs helemaal stoppen met de vragenlijst. Tot slot werden de respondenten aan het eind van de vragenlijst nog gevraagd om de volgende gegevens: volledige naam, e-mailadres, e-mailadres van een bekende, geboortedatum, postcode, huisnummer en de laatste drie cijfers van hun rekeningnummer. Voor elk van deze gegevens konden wij inzien of ze waren ingevuld of niet. Door deze combinatie van metingen geeft het onderzoek 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.
Ten slotte zijn de 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 bediscussieerd en konden de experts kritisch reflecteren op de gebruikte onderzoeksmethoden, de resultaten en veelbelovende richtingen voor interventies die zorgen voor veilig cybergedrag.

Vragenlijstonderzoek en gedragsmetingen

Slachtofferschap van online criminaliteit

Allereerst tonen wij in deze paragraaf in hoeverre slachtofferschap van online criminaliteit voorkomt binnen de steekproef. Slachtofferschap van online criminaliteit blijkt hoog; bijna de helft van de respondenten (48,1%) is ooit slachtoffer geworden van een online delict (in het afgelopen jaar en/of langer dan een jaar geleden).
In tabel 1 wordt de prevalentie van slachtofferschap per type delict beschreven. In totaal werd 13,6% van de respondenten het afgelopen jaar slachtoffer van online criminaliteit. Respondenten werden afgelo-

doi: 10.5553/JV/016758502020046002011

Tabel 1 Prevalentie van slachtofferschap en geleden schade per type delict

Cybercrime	Ja, <12 maanden	Ja, >12 maanden	Nee	Weet ik niet	Schade (incident <12 maanden)
Phishing	70 (2,9%)	114 (4,7%)	2.110	132	37 (52,9%)
Malware	177 (7,3%)	611 (25,2%)	1.417	221	104 (58,8%)
Online aankoopfraude	48 (2,0%)	190 (7,8%)	2.172	16	45 (93,8%)
Online identiteitsfraude	10 (0,4%)	17 (0,7%)	2.324	75	8 (80,0%)
Voorschotfraude	7 (0,3%)	17 (0,7%)	2.392	10	3 (42,9%)
Profielpagina veranderd	9 (0,4%)	36 (1,5%)	2.336	45	5 (55,6%)
Online account gehackt	16 (0,7%)	61 (2,5%)	2.224	125	11 (68,8%)
Computer gehackt	9 (0,4%)	35 (1,4%)	2.322	60	8 (88,9%)
E-mailaccount gehackt	23 (0,9%)	74 (3,1%)	2.149	180	11 (47,8%)
Bestanden ontoegankelijk	9 (0,4%)	93 (3,8%)	2.206	118	5 (55,6%)
Andere vorm van cybercrime	29 (1,2%)	73 (3,0%)	2.192	132	26 (89,7%)
Totaal (unieke personen)	**330 (13,6%)**	**951 (39,2%)**			**214 (64,8%)**

pen jaar het vaakst slachtoffer van malware[1] (7,3%), gevolgd door phishing[2] (2,9%) en online aankoopfraude[3] (2,0%). Ook werd 39,2% van de respondenten langer dan een jaar geleden één of meerdere keren slachtoffer van online criminaliteit. Ook in deze periode is slachtofferschap het hoogst voor malware (25,2%), online aankoopfraude (7,8%) en phishing (4,7%), gevolgd door 'bestanden zijn ontoegankelijk gemaakt' (bijvoorbeeld door ransomware) (3,8%) en hacking

1 Malware is kwaadaardige software die ongevraagd en meestal ongemerkt op de computer wordt geïnstalleerd. Voorbeelden van malware zijn virussen, Trojan horses, wormen en spyware.
2 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.
3 Hierbij wordt een product of dienst via internet gekocht en is ten minste een deel daarvan betaald, waarna het product of de dienst nooit geleverd is.

doi: 10.5553/JV/016758502020046002011

van een e-mailaccount (3,1%).[4] Slachtofferschap van andere vormen van online fraude – identiteitsfraude en voorschotfraude – kwam slechts in beperkte mate voor binnen deze steekproef. Het aantal slachtoffers dat schade heeft ondervonden van het slachtofferschap dat afgelopen jaar heeft plaatsgevonden, is – in lijn met recent onderzoek – zeer groot (Cross e.a. 2016; Jansen & Leukfeldt 2018; Leukfeldt e.a. 2018). Gemiddeld rapporteert 64,8% van de slachtoffers schade, omdat het incident ervoor heeft gezorgd dat zij geld, tijd of bestanden zijn kwijtgeraakt of emotionele schade of andere schade hebben ondervonden (tabel 1). Het percentage slachtoffers dat dergelijke schade ondervindt, is echter afhankelijk van het type delict en varieert tussen 43% tot 94%.

Hoe veilig gedragen Nederlanders zich online?

Dat burgers zich online onveilig gedragen, komt deels naar voren uit de analyses over zelfgerapporteerd gedrag, maar vooral ook tijdens de objectieve metingen van gedrag. Onveilig gedrag blijkt in hoge mate voor te komen. Zo gebruikt meer dan 40% een zwak wachtwoord van zeven of minder tekens,[5] downloadt 40% onveilige software en deelt ongeveer 30% van de respondenten persoonlijke gegevens, zoals hun volledige naam, geboortedatum en e-mailadres.
Het blijkt echter dat er grote verschillen bestaan tussen het zelfgerapporteerde gedrag en het objectieve gedrag. Uit de objectieve metingen blijkt steeds dat mensen zich nog onveiliger gedragen dan ze rapporteren te doen. Respondenten geven, bijvoorbeeld, middels zelfrapportage aan zich (zeer) veilig online te gedragen (bijvoorbeeld niet downloaden uit illegale bron en geen gebruik maken van openbare wifi), terwijl uit objectieve metingen blijkt dat 40% van de respondenten onbekende software downloadt als er een pop-up verschijnt tijdens een video die niet wil afspelen. De resultaten van de huidige studie onderschrijven dan ook het belang van het doen van objectieve metingen van cybergedrag.

4 Hierbij moet worden opgemerkt dat het aantal respondenten dat als antwoord 'weet ik niet' invulde, sterk verschilt per type delict. Bij slachtofferschap van malware, bijvoorbeeld, antwoordden liefst 221 respondenten 'weet ik niet', wat neerkomt op 9,1% van de totale steekproef. Dit betekent dat het percentage respondenten dat slachtoffer is geworden van malware ook toeneemt wanneer alleen gekeken zou worden naar de respondenten die deze vraag wel beantwoord hebben: respectievelijk 8,0% en 27,7% van deze respondenten waren het afgelopen jaar of langer geleden slachtoffer van malware.

5 Zie www.informatiebewust.nl/hoe-maak-je-een-sterk-wachtwoord/.

doi: 10.5553/JV/016758502020046002011

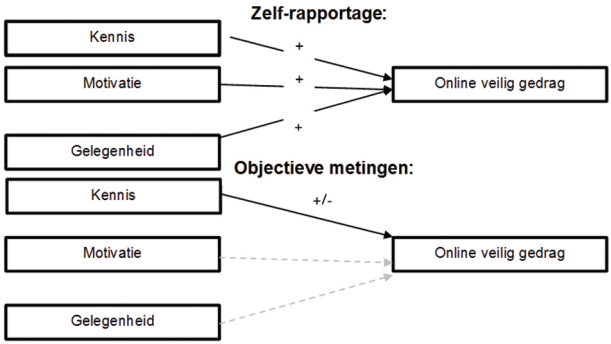
We onderzochten ook of de verschillende cybergedragingen samenhangen. Bijvoorbeeld, gedragen mensen die een sterk wachtwoord kiezen zich gemiddeld ook veiliger op andere cybergedrag? Deze vraag kan eveneens negatief worden beantwoord. De resultaten van de huidige studie wijzen erop dat hoe veilig mensen 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 phishinge-mail veilig gedrag laat zien, betekent dit niet dat hij zich gemiddeld ook veilig zal gedragen op het gebied van het kiezen van een sterk wachtwoord.
Een kanttekening is hierbij op zijn plaats. 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. Dit kan betekenen dat in de thuissituatie het percentage onveilig gedrag lager is dan door ons is gemeten via het panelonderzoek. Overigens was het juist onze bedoeling om cybergedrag in een veilige omgeving te meten – criminelen bootsen immers altijd een veilige omgeving (van bijvoorbeeld een bank of webshop) na en verleiden mensen hiermee op de hyperlink te klikken of persoonlijke informatie weg te geven –, maar toch kan deze methode tot een vertekening van de resultaten hebben geleid. Daadwerkelijk gedrag zou dus ook in andere contexten moeten worden gemeten. Bijvoorbeeld door het loggen van computers over een langere periode, waardoor oorzaak en gevolg beter bestudeerd kunnen worden.

Kan het cybergedrag worden verklaard door kennis, motivatie of gelegenheid?

Op basis van de literatuur kan worden geconcludeerd dat kennis, gelegenheid en motivatie van gebruikers belangrijke voorspellende factoren van gedrag zijn. De verwachting was dat deze factoren ook samenhangen met cybergedrag. Uit de zelfrapportage komt ook precies dat beeld: zowel kennis als gelegenheid en motivatie hangen positief samen met zelfgerapporteerd veilig cybergedrag. Als we echter kijken naar daadwerkelijk cybergedrag, dan ontstaat er een ander beeld. Alleen kennis blijkt significant samen te hangen met een drietal gedra-

doi: 10.5553/JV/016758502020046002011

Figuur 1 Resultaten COM-B-model



gingen: het delen van persoonlijke gegevens, wachtwoordsterkte en het downloaden van onveilige software. Hoe meer kennis respondenten hebben van online veiligheid, hoe veiliger hun cybergedrag is op het gebied van het delen van persoonlijke gegevens. Het verband tussen kennis en de overige twee gedragingen komt echter niet overeen met de verwachting uit de theorie: deze verbanden zijn negatief. Hoe meer kennis mensen bezitten over risico's en manieren om zichzelf te beschermen, hoe minder sterk het wachtwoord dat ze aanmaken en hoe makkelijker ze onveilige software downloaden. Een mogelijke verklaring is dat mensen zich door deze kennis veilig wanen en bereid zijn meer risico's nemen. Figuur 1 vat de resultaten met betrekking tot het COM-B-model samen.

Welke andere factoren spelen een rol?

Naast kennis, gelegenheid en motivatie zijn op basis van de literatuurstudie verschillende andere factoren meegenomen in de analyses die mogelijk samenhangen met cybergedrag. We bekeken daarom of cybergedrag samenhangt met gemoedstoestand, angst voor slachtofferschap, eerder slachtofferschap, type apparaat en tijdsdruk. Om tijdsdruk te manipuleren zijn de respondenten willekeurig toegewezen aan twee tijdsdrukcondities (hoog, laag). In alle analyses is bovendien

doi: 10.5553/JV/016758502020046002011

gecontroleerd voor demografische factoren en de zelfcontrole van respondenten.

Zelfgerapporteerd cybergedrag hangt samen met een aantal van de hierboven genoemde factoren. Een negatieve gemoedstoestand hangt negatief samen met zelfgerapporteerd veilig cybergedrag. Ofwel, hoe groter de negatieve gemoedstoestand van respondenten, hoe minder veilig hun zelfgerapporteerde cybergedrag is. Een positieve gemoedstoestand hangt daarentegen positief samen met de veiligheid van zelfgerapporteerd cybergedrag. Op basis van eerder onderzoek hadden we verwacht dat een positieve gemoedstoestand juist negatief zou samenhangen met veilig gedrag (Isen 2001; Nygren e.a. 1996). Nederlanders met een positieve gemoedstoestand 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. Het type apparaat waarop de vragenlijst is ingevuld, hangt ook samen met zelfgerapporteerd gedrag: respondenten die een pc of laptop gebruikten, geven aan zich veiliger online te gedragen dan respondenten die een tablet gebruikten.

Kijken we echter naar daadwerkelijk gedrag, dan blijven alleen een positieve gemoedstoestand, angst voor slachtofferschap, eerder slachtofferschap en type apparaat over. Een positieve gemoedstoestand hangt samen met zowel de wachtwoordsterkte als het downloaden van software van een 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 softwarepop-up. 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 wachtwoordsterkte: 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 softwarepop-up. Het type apparaat heeft ook invloed op daadwerkelijk

doi: 10.5553/JV/016758502020046002011

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 een 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 vinden we dat tijdsdruk geen effect heeft op het cybergedrag van Nederlanders.

Verschilt het cybergedrag van Nederlanders tussen bevolkingsgroepen?

Enkele van de achtergrondkenmerken van respondenten hangen samen met zelfgerapporteerd cybergedrag. Hoe hoger de leeftijd, hoe veiliger het gerapporteerde cybergedrag en hoe veiliger omgegaan wordt met hyperlinks in phishinge-mails. Voor opleiding is de relatie negatief: hoe hoger de opleiding, hoe minder veilig het zelfgerapporteerde cybergedrag is.
Bij daadwerkelijk cybergedrag vinden we ook een aantal relaties met kenmerken van respondenten, waarvoor we overigens geen verklaring hebben. Zo heeft het hebben van werk een significant verband met zowel wachtwoordsterkte als het wel of niet downloaden van software van een 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 Nederlanders zijn, hoe meer persoonlijke gegevens zij delen.

Beleidsimplicaties

Heel bewust is er in dit onderzoek voor gekozen om zowel zelfgerapporteerd cybergedrag als daadwerkelijk cybergedrag te meten. We weten immers dat hoewel de meeste mensen aangeven cybersecurity belangrijk te vinden, het werkelijke gedrag van mensen lang niet altijd gelijk is aan hun attitudes of gepercipieerd gedrag. Toch wordt beleid

doi: 10.5553/JV/016758502020046002011

regelmatig gebaseerd op zogenaamde flitspeilingen, ofwel korte enquêtes, onder de Nederlandse bevolking (zie bijv. Paardekoper 2019). Onze studie laat zien dat respondenten een te rooskleurig beeld lijken te hebben van hun eigen cybergedrag wanneer we hun zelfgerapporteerde scores van gedrag vergelijken met hun daadwerkelijke gedrag. Een voorbeeld: daar waar respondenten over het algemeen rapporteren een veilig wachtwoordbeleid te voeren, komt uit de objectieve meting een heel ander beeld naar voren. Meer dan 40% van de respondenten gebruikt een zwak wachtwoord bestaande uit minder dan zeven karakters voor het beveiligen van hun persoonsgegevens in dit onderzoek. Een vergelijkbaar beeld komt naar voren voor wat betreft het downloaden van software van een onbetrouwbare bron. Ook hier zien we dat meer dan 40% van de respondenten onveilig gedrag vertoont door goedkeuring te geven voor het downloaden van software van een onbekende bron. De waarde van flitspeilingen of andere vormen van vragenlijstonderzoek voor het vaststellen van beleid valt daarmee dus te betwisten. Wij pleiten er dan ook voor om beleid te baseren op objectieve metingen van gedrag. Door het gebruik van objectieve metingen van gedrag is de toegevoegde waarde van onderhavig onderzoek dan ook evident: we gaan verder dan bestaande onderzoeken door gepercipieerd en daadwerkelijk gedrag te meten op basis van een representatieve steekproef.

Het belang van meer kennis bij het bestrijden van online criminaliteit wordt bovendien overschat door de overheid, zo blijkt uit de vele zogenaamde bewustmakingscampagnes die door haar worden gefinancierd. Bewustmakingscampagnes worden vaak gelanceerd vanuit de veronderstelling dat kennis over cybersecurity ontbreekt. Terwijl in feite andere factoren leiden tot onveilig digitaal gedrag, zoals slecht ontworpen securitydesign van alledaagse toepassingen of rationaliseringstechnieken die mensen gebruiken om hun eigen onveilige gedrag te rechtvaardigen. Bewustmakingscampagnes zijn dan ook veelal onsuccesvol (Blythe & Coventry 2018). Om goed beleid te ontwikkelen is een gedegen analyse van het onveilige gedrag van mensen nodig. Ten eerste is het van belang te begrijpen waarom mensen zich onveilig gedragen. Op basis van deze inzichten kunnen dan maatregelen worden genomen die de oorzaken wegnemen van het onveilige gedrag. Deze studie laat echter zien dat verschillende mensen zich op verschillende manieren onveilig gedragen. Kennis, gelegenheid en motivatie zijn bovendien nauwelijks gecorreleerd aan de in dit onder-

doi: 10.5553/JV/016758502020046002011

zoek gemeten objectieve gedragingen. Dat maakt het bepalen van geschikte interventies op gedrag nog complexer.
Desalniettemin zou het uitgangspunt bij het ontwerpen van interventies naar onze mening moeten zijn dat het onveilige gedrag van mensen op voorhand wordt verhinderd en veilig gedrag wordt gestimuleerd. Om dit te bereiken is het aanpassen van het securitydesign waarschijnlijk het meest effectief. Door in de ontwerpfase al bewust online diensten in te richten op veilig gebruik wordt de eindgebruiker ontlast of gedwongen veilig te handelen.[6] In de praktijk is momenteel nog onvoldoende aandacht voor het aanpassen van het securitydesign. Bij het ontwerpen van online diensten moet van de grond af aan worden nagedacht over de veiligheid van de eindgebruiker. Dit zogenaamde *security by design*-denken staat echter nog in de kinderschoenen.[7] Om digitaal gedrag van eindgebruikers te beïnvloeden via het design van het systeem is meer kennis nodig. Vervolgens dient deze te worden vertaald naar concrete handvatten voor securityprofessionals in de praktijk.

Literatuur

Alison e.a. 2013
L. Alison, B. Doran, M.L. Long, N. Power, e.a., 'The effects of subjective time pressure and individual differences on hypotheses generation and action prioritization in police investigations', *Journal of Experimental Psychology: Applied, 19*(1), p. 83-93.

Ancher e.a. 2019
M. Ancher, R. van der Kleij & E.R. Leukfeldt, 'Studenten treden in voetsporen cybercrimineel om meer inzicht te krijgen in sociaal engineering', *Informatiebeveiliging Magazine* (19) 2019, afl. 2, p. 26-33.

6 Zie ook KIA veiligheid, oktober 2019, www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/KIA%20Veiligheid%20-%2020191016%20definitief.pdf.
7 Zie www.computable.nl/artikel/opinie/security/6305688/1509029/security-by-design-in-9-stappen.html.

doi: 10.5553/JV/016758502020046002011

Boss e.a. 2015
S.R. Boss, D. Galletta, P.B. Lowry, P. Polak, 'What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users', *MIS Quarterly* 39(4), p. 837.

Blythe & Coventry 2018
J. Blythe & L. Coventry, 'Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, vol. 87 2018, p. 87-97.

CBS 2019
CBS, *Digitale veiligheid & criminaliteit 2018*, Den Haag 2019.

Cross e.a. 2016
C. Cross, K. Richards & R.G. Smith, 'The reporting experiences and support needs of victims of online fraud', *Trends & Issues in Crime and Criminal Justice* 2016, afl. 518, p. 1-14.

Crossler e.a. 2013
R.E. Crossler, A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin & R. Baskerville, 'Future directions for behavioral information security research', *Computers and Security* (32) 2013, p. 90-101.

Debatin e.a. 2009
B. Debatin, J.P. Lovejoy, A.K. Horn & B.N. Hughes, 'Facebook and online privacy: Attitudes, behaviors, and unintended consequences', *Journal of Computer-Mediated Communication* (15) 2009, afl. 1, p. 83-108.

Hauer 2015
B. Hauer, 'Data and information leakage prevention within the scope of information security', *IEEE Access* (3) 2015, p. 2554-2565.

Van 't Hoff-de Goede e.a. 2019
S. van 't Hoff-de Goede, R. van der Kleij, S. van de Weijer & E.R. Leukfeldt, *Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders*, Den Haag: WODC, Ministerie van Justitie en Veiligheid 2019.

Isen 2001
A.M. Isen, 'An influence of positive affect on decision making in complex situations: Theoretical issues with practical implications', *Journal of Consumer Psychology* (11) 2001, afl. 2, p. 75-85.

doi: 10.5553/JV/016758502020046002011

Jansen & Leukfeldt 2018
J. Jansen & E.R. Leukfeldt, 'Coping with cybercrime victimization: An exploratory study into impact and change', *Journal of Qualitative Criminal Justice & Criminology* (6) 2018, afl. 2, p. 205-228.

Leukfeldt 2017
E.R. Leukfeldt (red.), *Research agenda. The human factor in cybercrime and cybersecurity*, Den Haag: Eleven International Publishing 2017.

Leukfeldt e.a. 2018
E.R. Leukfeldt, R. Notté & M. Malsch, *Slachtofferschap van online criminaliteit*, Den Haag: WODC 2018.

Leukfeldt e.a. 2019
E.R. Leukfeldt, R.J. Notté & M. Malsch, 'Exploring the needs of victims of cyber-dependent and cyber-enabled crimes', *Victims and Offenders* (15) 2019, afl. 1, p. 60-77.

Matthews e.a. 1995
G. Matthews, D. Pitcaithly & R.L.E. Mann, 'Mood, neuroticism, and the encoding of affective words', *Cognitive Therapy and Research*, 19, p. 563-587.

Michie e.a. 2011
S. Michie, M.M. van Stralen & R. West, 'The behaviour change wheel: A new method for characterising and designing behaviour change interventions', *Implementation Science* (6) 2011/42.

Munnichs e.a. 2017
G. Munnichs, M. Kouw & L. Kool, *Een nooit gelopen race. Over cyberdreigingen en versterking van weerbaarheid*, Den Haag: Rathenau Instituut 2017.

Nygren e.a. 1996
T.E. Nygren, A.M. Isen, P.J. Taylor & J. Dulin, 'The influence of positive affect on the decision rule in risk situations: Focus on outcome (and especially avoidance of loss) rather than probability', *Organizational Behavior and Human Decision Processes* (66) 1996, afl. 1, p. 59-72.

Paardekoper 2019
A. Paardekooper, 'Flitspeilingen voor burgerparticipatie: de aanpak van Utrecht & Tilburg', *Frankwatching* 2019, www.frankwatching.com/archive/2019/03/22/flitspeilingen-voor-burgerparticipatie-de-aanpak-van-utrecht-tilburg/.

Rhee e.a. 2009
H.S. Rhee, C. Kim & Y.U. Ryu, 'Self-efficacy in information security: Its influence on end users' information security practice behavior', *Computers and Security* (28) 2009, afl. 8, p. 816-826.

doi: 10.5553/JV/016758502020046002011

Talib e.a. 2010
S. Talib, N.L. Clarke & S.M. Furnell, 'An analysis of information security awareness within home and work environments', *ARES 2010 – 5th International Conference on Availability, Reliability, and Security*, 2010, p. 196-203.

Vishwanath 2016
A. Vishwanath, 'Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks', *Computers in Human Behavior, 63*, p. 198-207.

Warkentin e.a. 2012
M. Warkentin, D. Straub & K. Malimage, 'Featured talk. Measuring secure behavior: A research commentary', *Annual Symposium on Information Assurance & Secure Knowledge Management (ASIA & SKM)*, 2012.

Workman e.a. 2008
M. Workman, W.H. Bommer & D. Straub, 'Security lapses and the omission of information security measures: A threat control model and empirical test', *Computers in Human Behavior* (24) 2008, afl. 6, p. 2799-2816.

doi: 10.5553/JV/016758502020046002011