# Hoe veilig gedragen wij ons online?

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

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)

# Colofon

Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)
Afdeling Externe Betrekkingen (EWB)
Ministerie van Justitie en Veiligheid

Het onderzoek is in opdracht van het WODC uitgevoerd door onderzoekers van de Haagse Hogeschool en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR):
M.S. (Susanne) van ’t Hoff-de Goede
R. (Rick) van der Kleij
S.G.A. (Steve) van de Weijer
E.R. (Rutger) Leukfeldt

**Begeleidingscommissie**
prof. dr. K. van den Bos (voorzitter)
drs. L.F. Heuts
dr. H. Young
T. Hilbrink
J.P. Raeven
dr. R. Teijl
L.R. de Korte, MSc
Mr. E.C. van Ginkel

# Voorwoord

Burgers in Nederland voeren meer en meer online activiteiten uit. Gingen we in de jaren 90 van de vorige eeuw nog 'het internet op' om een e-mail te versturen of heel gericht informatie te zoeken, tegenwoordig zijn we eigenlijk continue online en zijn online en offline activiteiten met elkaar verweven. De hele dag door kunnen we e-mails checken op onze smartphones, terwijl we onderweg zijn van kantoor naar huis bestellen we snel nog wat kleding en foto's en video's hebben we vaak alleen nog digitaal bewaard.

Een belangrijke vraag is daarom hoe veilig we ons online gedragen. Criminelen maken immers ook gretig gebruik van deze nieuwe digitale activiteiten: burgers krijgen e-mails waarmee criminelen proberen achter hun login gegevens van accounts te komen of waarin een link staat die ervoor zorgt dat er kwaadaardige software op de computer van de gebruiker komt. Dit rapport geeft inzicht in hoe veilig burgers zich online gedragen en wat mogelijke interventies zijn om burgers zich veiliger te laten gedragen. Daarmee kan slachtofferschap van allerlei online delicten worden voorkomen. Daarmee levert dit rapport een bijdrage aan beleid omtrent de preventie van slachtofferschap van online delicten.

Dit onderzoek had niet uitgevoerd kunnen worden zonder de hulp van vele anderen. We willen iedereen bedanken die op wat voor manier dan ook een bijdrage heeft geleverd aan dit onderzoek. Ten eerste de leden van de begeleidingscommissie. Dank voor al jullie nuttige commentaar tijdens de diverse bijeenkomsten en op conceptversies van (delen van) het rapport. Daarnaast bedanken we in het bijzonder Sophie van der Zee, als universitair docent Toegepaste Economie verbonden aan de Erasmus Universiteit Rotterdam. Sophie gaf waardevolle feedback op de vragenlijst. Verder bedanken we de experts die deelnamen aan de discussiebijeenkomst. Jullie feedback op zowel de gebruikte onderzoeksmethoden, de resultaten en de mogelijkheden voor interventies zijn zeer waardevol.

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

# Inhoudsopgave

# Samenvatting


***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?


[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.

4) Kan het cybergedrag[2] van Nederlanders worden verklaard door hun kennis van online veiligheid?
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.

[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.

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 90 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?*

[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.

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 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.

# Summary

## *How safely do we behave online? A study of the relationship between knowledge, opportunity, motivation and the online behaviour of Dutch citizens.*


***Background***

Our offline and online lives are so intertwined that citizens in the Netherlands perform all kinds of online activities throughout the day. However, being online also presents dangers. Online crime is now common and its impact can be severe for victims. Cyber security professionals have tried to reduce online victimisation through technical measures, such as virus scanners and firewalls. These measures often only have a limited effect. To a large extent, victimisation can be traced back to the behaviour of people. After all, internet users click on a hyperlink when they should not, or enter personal data on a phishing[4] website, allowing criminals to misuse that data. In order to reduce victimhood, research into the behaviour of internet users is therefore essential.

***Research objective and research questions***

Knowledge about how citizens behave online and how they (might) defend themselves against online crime is scarce. To date, it is unknown in which ways Dutch citizens behave online and how they protect themselves against online crime, in part because how people *say* they behave online is not always the same as how people *actually behave* online. However, such knowledge is indispensable as empirical support for interventions aimed at influencing behaviour. It is necessary to gain greater insight into the ways in which Dutch citizens behave online and which factors are related to their behaviour. The aim of this research is therefore to discover how Dutch citizens behave online and to explain their online behaviour based on factors that have emerged from the literature, in order to take an initial step towards developing interventions that make Dutch citizens safer online. The main question of this report is: "How safely do Dutch citizens behave online and how can this be explained?" The following sub-questions will be answered in this report:


[4] Phishing is a form of online scam, in which criminals copy the e-mails or websites of legitimate organisations to mislead victims, in order to retrieve login details and gain access to online accounts.

1. How safely do Dutch citizens behave online?
2. Is there a relationship between knowledge, opportunity and motivation?
3. Are there similarities between different online behaviours?
4. Can the online behaviour of Dutch citizens be explained by their knowledge of online security?
5. Can the online behaviour of Dutch citizens be explained by their opportunity for safe online behaviour?
6. Can the online behaviour of Dutch citizens be explained by their motivation for safe online behaviour?
7. Can the online behaviour of Dutch citizens be explained by other factors?
8. Does the online behaviour of Dutch citizens differ between population groups?
9. Are the ways that knowledge, opportunity and motivation affect online behaviour influenced by other factors?

***Research methods***

Various methods were used to answer the research questions: a literature study, an experimental survey and an expert meeting. The research started with the literature study. The literature study was conducted to gain insight into existing knowledge about online behaviour, risk factors associated with being a victim of online crime and unsafe online behaviour, persuasion techniques and factors that are important for behavioural change.

Subsequently, a survey was developed based on the literature study and distributed with the help of a research panel agency. The final sample consists of 2,426 persons and is representative of Dutch society with regard to the characteristics gender, if they are employed (yes / no) and the province in which they live, but respondents are more often highly educated and, on average, they are older. We used a so-called "population-based survey experiment" (experimental survey). In the questionnaire, online behaviour was measured in two ways: 1) self-reporting – by presenting respondents with questions and statements, as well as vignettes; and 2) objective measures – while filling out the survey, respondents encountered (fictional) cyber risk situations, allowing the researchers to analyse how respondents dealt with these situations. These formed the objective measurements of online behaviour. The survey therefore provides insight into the extent to which people *think* they are behaving in a safe or unsafe manner and to what extent people *actually* display safe or unsafe online behaviour.

Finally, the first results of the analyses were discussed with experts from different fields during an expert discussion meeting. The purpose of this meeting was to start developing recommendations that

would be useful in practice for preventing or combating cyber risks. The meeting was therefore preceded by a literature study investigating existing interventions that aim to bring about behavioural change. During the meeting, the results of the experimental survey study and the literature study on interventions were discussed and the experts were able to critically reflect on the research methods used, the results and promising directions for interventions that ensure safe online behaviour.

***Conclusions of the literature study***

The purpose of the literature study was to explain how online behaviour has been researched and measured in previous studies. It was also examined which explanations for the display of unsafe or safe online behaviour were found in previous studies. First, the literature study shows that a risk profile for becoming a victim of online crime cannot be outlined based on personal characteristics or routine activities. A number of factors do, however, emerge that may be relevant to online behaviour and they have therefore been included in the current study. These factors are: age, socio-economic status, gender and family composition. In addition, it appears that research should focus on behaviour as a pillar for decreasing the risk of online victimisation, namely safe online behaviour. This is therefore the main subject of the current study. Furthermore, the literature study shows, on the basis of theoretical explanatory models (in particular the Protection Motivation Theory (PMT) and COM-B, in which knowledge, opportunity and motivation are central), that the extent to which people behave safely online depends on the capacities that people have to behave safely, the opportunity they have to do so and the extent to which they are motivated to behave safely. In addition, the theory points to the importance of self-control and earlier victimisation.

Finally, there are factors that were not derived from these theoretical models but that seem relevant to online behaviour: mood, fear of victimisation, type of device, time pressure and persuasion techniques. A person's mood can influence their decision-making and has an effect on the strategies they choose when making decisions. Fear of victimisation can have various consequences for online behaviour, such as avoidance behaviour but also taking fewer risks online. The device used to go online is also important. Devices that people use at home for online activities, such as a smartphone, tablet, laptop or PC, differ in a number of dimensions that influence online behaviour and can influence victimisation. Time pressure could also cause people to ignore signs (cues) that they are at risk, and thus make them take more risks. The persuasion techniques that cyber criminals use in their attacks also seem important. All factors that emerged from the literature study were included in the present study. The current study

therefore investigated to what extent online behaviour can be explained by all of the above-mentioned factors.

***Results and conclusions of the experimental survey***

*Research question 1: How safely do Dutch citizens behave online?*

It was found that unsafe behaviour is highly prevalent. For example, nearly 90 per cent of respondents use a weak password, 40 per cent download unsafe software and about 30 per cent share personal information, such as their full name, date of birth, and email address. When respondents are presented with phishing emails, more than 20 per cent say they would click on the hyperlink or copy the URL to the web browser, thereby making an unsafe choice.

While the fact that citizens behave unsafely online is partly reflected in the analyses of self-reported behaviour, it becomes especially apparent during the objective measurements of behaviour. However, it appears that there are major differences between self-reported behaviour and objective behaviour. The objective measurements show that people behave even more unsafely than they self-report. Below, we briefly discuss the conclusions for each of the seven online behavioural clusters (use of passwords, saving important files, installing updates, using security software, being alert online, online sharing of personal information, dealing with hyperlinks and attachments in e-mails).

- *Use of passwords.* Respondents self-report that they use safe passwords. They score high on security when it comes to not sharing passwords with others and using difficult passwords. The objective measurements show a different picture: 89 per cent of the respondents used a weak password. Even if we only look at the respondents who indicate, at the end of the questionnaire, that they have chosen a password in the same way as they would normally do, it appears that more than 83 per cent use a weak password. If we look a little more broadly at the password behaviour of the respondents and take as a starting point that only the length of the password matters and we again only look at the group that indicated they had chosen the password in the same way, it appears that 51 per cent choose a password of seven or fewer characters.
- *Saving important files, installing updates and using security software*. Using self-reported data, it was measured how respondents deal with saving files, updating software and using security software. Of all seven behavioural clusters, respondents report, on average, the least secure behaviour in the area

of file storage. In the area of updating software, a high (safe) score was reported on all propositions, such as installing updates on operating systems, apps/software and security software as soon as a new update becomes available.

- *Being alert online.* When we focus on being alert while being online, the same picture appears: respondents indicate through self-reporting that they behave (very) securely (for example not downloading from illegal sources, not using public Wi-Fi), while the objective measurement shows that 40 per cent of the respondents download unknown software if a pop-up appears while attempting to watch an online video.
- *Online sharing of personal information.* Concerning the online sharing of personal data, respondents indicate that they are aware of the dangers of sharing personal data such as a home address, e-mail address or telephone number and connection requests via social media. During the objective measurement, however, respondents often appear willing to provide (very) personal information. For example, a significant proportion gave their date of birth (37.5%), full name (31%), e-mail address (28.1%) and their postcode (27.0%) and street number (20.4%). A small, but significant, part of the respondents (4.8%) is also willing to enter the last three digits of their bank account number.
- *Dealing with attachments and hyperlinks in e-mails.* Respondents self-report safe behaviour when it comes to dealing with attachments and hyperlinks in emails. For example, respondents indicate that they very often delete emails that they do not trust and they almost never open attachments in emails from unknown senders. However, from the vignettes presented to those respondents – three e-mails, two of which were phishing e-mails and one legitimate e-mail – asking them to indicate how they would deal with the e-mails, it appears that 21 per cent would act unsafely: these respondents indicate that they would click on a hyperlink in a phishing e-mail or type the URL into their web browser.

*Research questions 2 and 3: Is there a relationship between knowledge, opportunity and motivation and are there similarities between different online behaviours?*

With the ultimate goal being to identify behavioural interventions that increase the safety of online behaviour of Dutch citizens, it was important to examine how traits and behaviours are distributed among the population. For example, do people with extensive knowledge of online security generally also have more social and material opportunity and motivation for safe online behaviour? The results show that the

answer to that question is no: hardly any correlations are found between underlying characteristics that could explain safe online behaviour.

Next, it was important to investigate whether the various online behaviours are related. For example, on average, do people who choose a strong password behave more safely in respect of other online behaviours as well? This question can also be answered negatively. The results of the current study indicate that how safely people behave in one online behaviour cluster is only minimally related to how safely they behave in another online behaviour cluster. For example, when someone shows safe behaviour when dealing with a phishing e-mail, this does not mean that they will, on average, also behave securely in terms of choosing a strong password. There is even a (very small) negative correlation between password strength and the sharing of personal data, which indicates that the stronger the password that respondents choose, the more unsafely they behave in the area of sharing personal data.

Finally, it may be questioned whether a focus on objective behaviour is necessary in follow-up research. Are self-reported and objective behaviours similar enough to base research on (much easier to collect) self-reported data? The results of the current study underline the importance of taking objective measurements of online behaviour. There is a very limited conformity between how people *say* they behave online and how people *actually behave* in the current study. The explanation for this may lie in what is called the cyber security paradox. Although most people indicate that cyber security is important, their self-reported behaviour does not always correspond to their actual behaviour, as underlined by the current study.

*Research questions 4-7: Can the online behaviour of Dutch citizens be explained by knowledge, opportunity, motivation and other relevant factors?*

Based on the literature, the most important predictive factors included in this study are knowledge, opportunity and motivation. These factors were expected to be associated with online behaviour. The self-reported data confirms this: knowledge, opportunity and motivation are positively related to self-reported safe online behaviour. However, if we look at actual online behaviour, a different picture emerges. Only knowledge appears to be significantly related to two behaviours: password strength and downloading unsafe software. However, the connection is negative: the more knowledge people have, the less strong the password they create. In addition: for every point that respondents score higher on the knowledge test, they become less likely to make a safe choice with the software pop-up. The strength of the chosen password and whether or not they download unsafe software is not significantly related to

the (social or material) opportunity or motivation that respondents have for safe online behaviour. Only one connection between knowledge, opportunity, motivation and objective online behaviour corresponds to expectations from theory: when people have more knowledge of online security, they behave more securely when it comes to sharing personal data.

Based on the literature study, in addition to knowledge, opportunity and motivation, various other factors that may be related to online behaviour were included in the analyses. We examined whether online behaviour is associated with a negative or positive mood, fear of victimisation, earlier victimisation, self-control, device type, time pressure, persuasion techniques used by criminals, threat appraisal, coping appraisal and locus of control.

Self-reported online behaviour is related to a number of these factors. A negative mood is negatively related to self-reported safe online behaviour. In other words, the greater respondents' negative mood, the less safe their (self-reported) online behaviour is. A positive mood, on the other hand, is positively related to the safety of self-reported online behaviour. Based on earlier research, we had expected that a positive mood would be negatively related to safe behaviour. It was expected that citizens would see the outcomes of risky situations as more positive and be more willing to take risks. However, the results show a different picture. An explanation cannot be given based on the current study. Self-control is also significantly associated with self-reported online behaviour. In line with expectations, it was found that the more self-control respondents have, the safer their (self-reported) online behaviour is. The type of device used to fill in the questionnaire is also related to self-reported behaviour: respondents who used a PC or laptop indicate that they behave more safely online than those who used a tablet.

However, if we look at actual behaviour, only a positive mood, fear of victimisation, earlier victimisation, type of device and persuasion techniques remain. A positive mood is related to both password strength and downloading software from an unreliable source, but in opposing directions. The greater respondents' positive mood, the stronger the password they choose. On the other hand, it has been found, in line with the literature, that the greater respondents' positive mood, the greater the likelihood of them making an unsafe choice with the software pop-up ("clicking behaviour"). A positive mood, overall, is therefore related to both safe and unsafe online behaviour; this relationship depends on the type of online behaviour. Fear of victimhood is also significantly related to password strength; the more afraid respondents are of becoming a victim of online crime, the stronger their chosen password. In addition, victimisation is negatively related to actual clicking behaviour; respondents who have previously fallen victim to online crime more often make a safe choice by not downloading software from an unreliable source. The type of device used by respondents has a significant relationship with all objectively

measured behaviours. Respondents who use a PC or laptop choose a less strong password than respondents who use a tablet. They also behave less safely in the areas of downloading software from an unreliable source and sharing personal data. Respondents who used a smartphone make a safe choice more often than respondents using a tablet with respect to downloading software from an unreliable source. Finally, one of the persuasion techniques that cyber criminals use appears to be related to unsafe online behaviour. Respondents to whom the "reciprocity" persuasion technique has been applied share significantly more personal data.

Finally, it was investigated whether the way in which people evaluate the online threat and safety measures influences the extent to which they are motivated to protect themselves. Threat appraisal, coping appraisal and locus of control have a positive connection with the motivation for online self-protection. Based on the Protection Motivation Theory (PMT), this motivation can be expected to influence the safety of online behaviour. However, we cannot draw that conclusion. In fact, if we look at the relationship between threat appraisal, coping appraisal and locus of control and online behaviour, we see only one significant relationship: that between coping appraisal and self-reported online behaviour. Coping appraisal – the extent to which respondents believe that online security measures are effective, the extent to which they are able to take those measures themselves and whether they think the costs of these measures are not too high – is positively related to self-reported online behaviour. The higher the coping appraisal, the more safe online behaviour is reported. However, in respect of all objectively measured online behaviours (password strength, click behaviour and sharing of personal data) and in respect of the "e-mail choice" vignette measurement, no significant relationships with the PMT elements are evident.

*Research question 8: Does the online behaviour of Dutch citizens differ between population groups?*

Several of the background characteristics of respondents are related to self-reported online behaviour. The higher the age, the safer the self-reported online behaviour and the safer the self-reported handling of hyperlinks in phishing emails. For education, the relationship is negative: the higher the education, the less safe the self-reported online behaviour is. Having live-in children under the age of 16 is also related to handling hyperlinks in phishing emails more unsafely.

In terms of actual online behaviour, we also find a number of relationships with respondent characteristics. For example, being employed has a significant relationship with both password strength and whether or not respondents download software from an unreliable source. Employed respondents

choose a less strong password and more often download software from an unreliable source. In addition, respondents with higher education choose a less strong password, but they do behave more securely when it comes to sharing personal data. The clicking behaviour of men is, on average, less safe than that of women and they also share more personal information. Cohabitants, on the other hand, display safer clicking behaviour. Finally, it seems that the older citizens are, the more personal information they share.

*Research question 9: Are the effects of knowledge, opportunity and motivation on online behaviour influenced by other factors?*

It was investigated whether the relationships between knowledge, opportunity and motivation and online behaviour can be explained by interactions between these variables and the following (moderator) variables: negative mood, positive mood, fear of victimisation, previous victimisation (ever) and self-control. Taken together, the results indicate that most interactions are not significant but, in some cases, the relationships between knowledge, opportunity, and motivation and online behaviour are influenced by self-control, mood, fear of victimisation and, in one case, previous victimisation.

Most of the significant interactions were found in the analyses in which self-reported online behaviour and password strength are predicted. A few interactions show that the direction of the relationships found depends on the level of one's scores on the moderator variables. For example, among respondents with very little fear of becoming a victim of online crime, there appears to be a positive link between social opportunity and the safety of self-reported online behaviour. However, as fear of victimisation increases, this connection weakens. For respondents who are (very) fearful of victimisation, the relationship even becomes negative: they report less safe behaviour when social opportunity increases.

In addition, there are a number of interactions in which the relationships found do not change direction but become stronger, as one scores higher or lower on the moderator variables. For example, the positive relationship between motivation and self-reported online behaviour becomes less strong as respondents have a more positive mood and as respondents have a greater fear of victimisation.

***Limitations***

Like all research, this study also has its limitations. Firstly, we do have a relatively large number of respondents who are representative of Dutch society by gender, employment (yes / no) and the province

in which they live, but the data are not entirely representative. For example, on average, respondents are more often highly educated and less often younger than 39 years old.

The significant added value of this study is that not only has self-reported behaviour been measured, but actual behaviour has been measured objectively too. This was moreover done in a large sample, with respondents who answered a variety of questions about their online behaviour on their own device in their own home. However, the objective measures each have their own limitations. Firstly, due to the length of the questionnaire, it was not possible to include objective measures for all seven behavioural clusters. Concerning the data on sharing personal data, we do not know which data was entered and whether this was actual/correct data. Other factors may have influenced the results on downloading unsafe software (clicking behaviour). For example, we used a pop-up that was designed in the style of the Windows operating system. Therefore, non-Windows users would be less familiar with the pop-up. This may make them more suspicious or more likely to say yes. Further research is needed, with a range of pop-ups that are technically realistic and adapted to the device and operating system. Finally, although the method - a survey with experiments - is very appropriate for conducting this type of research, we are of course dealing with respondents who may feel safe in the research panel agency's online environment. As a result, they may have made unsafe choices more quickly than usual.

***Looking to the future: interventions***

The aim of this study was to discover how safely Dutch citizens behave online and to explain this based on factors that have emerged from the literature, in order to take an initial step towards developing interventions to make Dutch citizens safer online. The results of this research were therefore discussed with experts to identify promising directions for interventions.

In summary, it appears that there is no silver bullet for promoting safe online behaviour. Different online behaviours seem to stem from different sources. There is also a perception among experts that people differ in their sensitivity to interventions and that the timing of interventions is crucial to their success. Experts do see a lot of value in interventions that focus on adaptations to the technology that people use for online activities, such that the possibility of unsafe behaviour is reduced and the possibility of safe behaviour is increased – also known as security by design. There is a role here for policy measures encouraging technology manufacturers to make adjustments that make it easier for people to adopt safe behaviours. However, designing specific interventions aimed at manufacturers or citizens themselves is no easy task. Future research could focus on developing and evaluating a specific set of interventions aimed at influencing the unsafe behaviours found in this study.

# 1. Inleiding

### *1.1 Achtergrond*

We brengen een groot deel van ons leven online door. Of beter gezegd: onze offline en online levens zijn zo met elkaar verweven dat burgers in Nederland de hele dag door allerlei online activiteiten uitvoeren. Het CBS (2019) laat zien dat 97,7 procent van de Nederlanders van 12 jaar en ouder dagelijks voor privédoeleinden gebruikt maakt van internet om allerlei activiteiten uit te voeren. Dat doen ze thuis, via een computer of laptop, maar ook op openbare plekken via bijvoorbeeld een smartphone (85%). Uit hetzelfde onderzoek blijkt dat burgers internet vooral gebruiken voor het zoeken naar informatie (98%), het versturen van berichten (95%) en online bankieren (90%). Daarnaast worden veelvuldig online aankopen gedaan (82%), applicaties gedownload (77%) en gebruik gemaakt van sociale media (69%).

Online zijn levert gevaren op. In 2018 gaf 8,5 procent van de internetgebruikers van 12 jaar of ouder aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van online criminaliteit (CBS, 2019b). In totaal zijn 1,2 miljoen Nederlanders dat jaar slachtoffer geworden van online criminaliteit. Zo werd 2,9 procent van de Nederlanders slachtoffer van fraude met online handel en één procent slachtoffer van identiteitsdiefstal (CBS, 2019b). 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, Richards, & Smith, 2016; Jansen & Leukfeldt, 2018; Leukfeldt, Notté, & Malsch, 2018).

Dergelijke delicten worden in de regel in twee categorieën ingedeeld (McGuire & Dowling, 2013). Enerzijds is er sprake van nieuwe delicten, bijvoorbeeld het hacken van een database met persoonsgegevens of het platleggen van websites of netwerken. Dit soort delicten valt onder de noemer cybercrime (ook wel cybercrime in enge zin of *computer dependent* criminaliteit genoemd). Anderzijds zijn er traditionele vormen van criminaliteit waarbij ICT een steeds belangrijkere rol speelt bij de realisatie daarvan. Voorbeelden zijn het plegen van fraude via internet en afpersing. Dergelijke delicten vallen onder de noemer gedigitaliseerde criminaliteit (ook wel cybercrime in brede zin of *computer enabled* criminaliteit genoemd). In dit rapport hanteren we in lijn met recente WODC-publicaties de overkoepelde term “online criminaliteit” voor alle delicten met een digitale component (zie bijvoorbeeld Cuyper & Weijters, 2016; Leukfeldt et al., 2018; Rokven, Weijters, & Laan, 2017). Hieronder vallen zowel delicten onder de noemer cybercrime als gedigitaliseerde criminaliteit.

Online criminaliteit is dus 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 (Munnichs, Kouw, & Kool, 2017; Rutkens, 2018). Gebruikers klikken immers op een hyperlink terwijl ze dat niet moeten doen, of vullen gegevens in op een phishing website waardoor criminelen die gegevens kunnen misbruiken. Om slachtofferschap terug te kunnen dringen is onderzoek naar de gebruiker dan ook van wezenlijk belang (Leukfeldt, 2017; Rhee, Kim, & Ryu, 2009; Talib, Clarke, & Furnell, 2010).

Als we slachtofferschap willen voorkomen, moeten we eerst slachtofferschap verklaren. Eerdere onderzoeken hebben zich daarom tot doel gesteld te verklaren waarom bepaalde mensen slachtoffer worden van online criminaliteit. Het bepalen van een risicoprofiel voor slachtoffers van online criminaliteit lijkt echter lastig te zijn; cybercriminelen proberen op allerlei manieren om hun aanval succesvol te laten zijn. Ze veranderen vaak van werkwijze en passen die werkwijze aan op nieuwe bewustwordingscampagnes of beveiligingsadviezen. Mede hierdoor is het risicoprofiel voor slachtofferschap niet terug te brengen tot persoonskenmerken zoals leeftijd of opleiding (Leukfeldt, 2014; Paulissen & Van Wilsem, 2015).

Kennis over hoe burgers zich (kunnen) weren tegen online criminaliteit is schaars (zie voor een overzicht bijvoorbeeld Leukfeldt, 2017). Het is tot op heden 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 et al., 2013; Debatin, Lovejoy, Horn, & Hughes, 2009; Warkentin, Straub, & Malimage, 2012; Workman, Bommer, & Straub, 2008). 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. De hoofdvraag van dit rapport is dan ook:

*Hoe veilig gedragen Nederlanders zich online en hoe kan dit worden verklaard?*

Het doel van dit onderzoek is 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. Om inzicht te krijgen in online gedrag hebben we gebruik gemaakt van een literatuurstudie en een experimentele surveystudie. Een experimentele surveystudie combineert de kracht van een

vragenlijstonderzoek onder een representatieve groep burgers met de voordelen van labonderzoek, zoals het elimineren of onder controle houden van storende variabelen.

### *1.2 Toegevoegde waarde huidige studie*

Het is duidelijk dat online criminaliteit veelvoorkomend is en dat de impact ervan groot kan zijn. Het doel van dit onderzoek is daarom om in kaart te brengen hoe veilig burgers zich denken te gedragen online én hoe veilig burgers zich daadwerkelijk online gedragen. Online gedrag wordt daarbij in dit rapport vanaf dit punt cybergedrag genoemd, een term die synoniem is aan de term online gedrag en alle cybergedragingen van mensen beslaat.

Heel bewust is er in dit onderzoek voor gekozen om zowel zelf-gerapporteerd (gepercipieerd) 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 (zie hoofdstuk 3).

De literatuurstudie die bij de start van dit onderzoek is uitgevoerd laat duidelijk zien dat er een gebrek is aan onderzoeken waarbij daadwerkelijk gedrag wordt gemeten (zie de samenvatting van de belangrijkste resultaten in paragraaf 3.5). Een verklaring hiervoor is dat dit onderzoeksterrein nog relatief jong is. De meeste studies die zijn uitgevoerd, kunnen worden gezien als verkennend en toetsen vooral of bestaande criminologische of psychologische modellen gebruikt kunnen worden om onveilig cybergedrag of slachtofferschap van een groot aantal vormen van cybercrime te verklaren. De beschikbare studies waarbij wel daadwerkelijk cybergedrag is gemeten, hebben te maken met beperkingen doordat bijvoorbeeld een niet-representatieve steekproef is gebruikt. Bovendien hebben deze studies weliswaar waardevolle resultaten opgeleverd over de prevalentie van onveilig cybergedrag, maar hebben deze studies zich zelden gericht op verklarende factoren. Een eventuele samenhang tussen factoren als kennis en motivatie en de prevalentie van daadwerkelijk (objectief gemeten) cybergedrag is tot op heden nog niet onderzocht.

Het gros van de wetenschappelijke studies richt zich op het in kaart brengen van persoonskenmerken en routine activiteiten die slachtofferschap van allerlei vormen van cybercrime mogelijk kunnen verklaren (Holt & Bossler, 2013). Deze studies maken in de regel gebruik van de routine activiteiten theorie, een criminologische theorie waarbij er vanuit wordt gegaan dat criminaliteit ontstaat als een geschikt doelwit en een gemotiveerde dader zonder tussenkomst van een zogenoemde *capable guardian* in tijd en ruimte samenkomen. De theorie is zeer geschikt om bijvoorbeeld woninginbraak te

verklaren, maar studies naar slachtofferschap van cybercrime laten wisselende resultaten zien. Dit heeft waarschijnlijk voor een groot deel te maken met het feit dat de samenkomst in tijd en ruimte van slachtoffer en dader anders is bij online delicten dan bij offline delicten. Zo kan bijvoorbeeld informatie die gestolen is van een slachtoffer, dagen of weken later nog misbruikt worden door de daders. Andere studies richten zich juist alleen op de motivatie voor gedrag. Deze studies maken veelal gebruik van de *protection motivation theory*. Terwijl verklaringen voor (het ontbreken van) motivatie voor veilig gedrag breeduit onderzocht zijn, wordt veelal aangenomen dat motivatie vervolgens gedrag beïnvloedt zonder dat dit getoetst wordt. Alhoewel de theorie relevant lijkt mist er dus tot op heden een empirische toets op daadwerkelijk cyberveilig gedrag.

De toegevoegde waarde van onderhavig onderzoek is dan ook evident: we gaan verder dan bestaande onderzoeken door gepercipieerd en daadwerkelijk gedrag te meten op basis van een representatieve steekproef. Maar dit onderzoek is ook op een andere manier vernieuwend: we nemen niet slachtofferschap van specifieke vormen van online delicten als uitgangspunt, maar cybergedrag. Het is immers het gedrag dat zorgt voor een verhoogd risico op allerlei vormen van online criminaliteit. Ten slotte onderzoeken we ook wat verklaringen zijn voor cybergedrag. Hieronder zullen we deze drie vernieuwende elementen beknopt toelichten.

Ten eerste het meten van daadwerkelijk gedrag. In dit onderzoek zal een onderzoeksmethode worden gebruikt die vragenlijstonderzoek combineert met ingebouwde experimenten; het *population based survey experiment* (die we hierna “experimentele surveystudie” zullen noemen). Een experimentele surveystudie combineert de kracht van een vragenlijstonderzoek onder een representatieve groep burgers met de voordelen van lab experimenten. In onderzoek naar cybergedrag zou dit betekenen dat respondenten situaties voorgelegd krijgen tijdens het invullen van de vragenlijst die “echte” cyberincidenten nabootsen. In de survey van de huidige studie werden diverse van dergelijke objectieve metingen van gedrag gedaan. De respondent werd bijvoorbeeld gevraagd een filmpje te bekijken, maar het filmpje speelt niet af. Is de respondent bereid onbekende en mogelijk schadelijke software te downloaden of is hij/zij weerbaar en hiertoe niet bereid? Daarnaast kregen de onderzoekers met behulp van de survey inzicht in bijvoorbeeld achtergrondkenmerken, kennis, motivatie en gemoedstoestand van respondenten. In hoofdstuk 4 meer over deze methode en de opzet van de vragenlijst.

Ten tweede het meten van gedrag in plaats van slachtofferschap van specifieke delicten. In de regel richten veel studies zich ten onrechte op het verklaren van slachtofferschap van specifieke delicten door te onderzoeken of bepaalde kenmerken van respondenten of bepaald gerapporteerd gedrag zorgen voor een verhoogde kans op heel specifieke online delicten. In onze studie richten we ons juist op

gedragingen die voor slachtofferschap van diverse vormen van online delicten kunnen zorgen of deze kunnen voorkomen. Bijvoorbeeld het klikken of onveilige hyperlinks of het onnodig delen van informatie. Dit doen we omdat we weten uit onderzoek naar de verdienmodellen en werkwijzen van cybercriminele groepen die phishing en/of malware aanvallen uitvoeren[5], dat cybercriminelen hun modus operandi constant aanpassen, vrij opportunistisch te werk gaan – de ene keer misbruiken ze zelf de verkregen informatie, de andere keer verkopen ze het aan anderen – en ook allerlei andere delicten plegen (zie bijvoorbeeld Leukfeldt 2014; Leukfeldt et al. 2017, Lusthaus, 2018a, 2018b). Ook maken phishers soms gebruik van aanvallen met malware en zijn er social engineers die overal informatie vandaan halen om slachtoffers te maken (Steinmetz, 2016; Button & Cross, 2017; Bazzell, 2018). Het hoeft dus niet zo te zijn dat een bepaalde gedraging altijd tot een bepaalde vorm van slachtofferschap leidt. De ene keer kan het trappen in een phishing e-mail leiden tot een leeggeplunderde bankrekening, terwijl het de andere keer zorgt voor een besmetting met ransomware[6] of het kan het begin zijn van een spear phishing aanval[7] op het bedrijf waar het slachtoffer werkzaam is. Daarnaast laat onderzoek naar de handel op online criminele markten zien dat als het gaat om de handel in data, er naast creditcardgegevens ook veel wordt gehandeld in allerlei persoonsgegevens die misbruikt kunnen worden door criminelen om gericht allerlei aanvallen zoals phishing, malware of ransomware uit te voeren (zie voor een overzicht Leukfeldt, 2017). Dit wordt ook doxing genoemd. Het gaat dan om op het eerste gezicht relatief onschuldige data zoals naam, geboortedatum, Burgerservicenummer, e-mailadressen en sociale media accounts. We kiezen er daarom in dit onderzoek voor om objectief een aantal gedragingen te meten waarvan we weten dat die direct in verband staan met slachtofferschap van diverse online delicten: het geven van informatie, het klikken op onveilige hyperlinks in phishing e-mails en het gebruiken van zwakke wachtwoorden. In paragraaf 3.3 staat een volledige lijst met cybergedrag.

Ten derde het verklaren van cybergedrag. Bestaande studies richten zich met name op het bestuderen van de relatie tussen persoonskenmerken of routine activiteiten en slachtofferschap, of kijken alleen naar attitudes die zouden leiden tot bepaald gedrag. Hoogstens is onderzocht of de mate waarin mensen gemotiveerd zijn zich veilig te gedragen online gerelateerd is aan cybergedrag, maar de invloed van mechanismes als kennis of gelegenheid is daarbij buiten beeld gelaten. In dit onderzoek gaan we veel

[5] 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. Malware is kwaadaardige software die ongevraagd en meestal ongemerkt op uw computer wordt geïnstalleerd. Voorbeelden van malware zijn virussen, trojan horses, wormen en spyware.

[6] Ransomware is kwaadaardige software die een computer blokkeert of bestanden versleutelt. Pas als je losgeld betaalt, zou je de computer of de bestanden weer kunnen gebruiken.

[7] Spear phishing is een gerichte phishing aanval op een persoon of een specifieke groep personen.

verder dan alleen het bestuderen van factoren als persoonskenmerken en routine activiteiten en meten we ook de invloed van kennis, gelegenheid en motivatie. Ten slotte bestuderen we ook nog of verleidingstechnieken die door criminelen worden gebruikt om slachtoffers te maken, ervoor zorgen dat personen eerder cyberonveilig gedrag vertonen én bekijken we wat de invloed is van verschillende andere factoren, zoals de gemoedstoestand van personen en het apparaat waarmee ze online zijn.

### *1.3 Leeswijzer*

Dit rapport start met een uiteenzetting van de onderzoeksvragen en onderzoeksmethoden in hoofdstuk 2. In hoofdstuk 3 wordt de wetenschappelijke literatuur besproken over risicofactoren van slachtofferschap, cybergedrag, en theoretische verklaringen voor cybergedrag. Hoofdstuk 4 zoomt in op de methode die centraal staat in dit onderzoek: de *population based survey experiment*. Het meetinstrument dat we ontwikkeld hebben om cybergedrag te meten, staat in dit hoofdstuk uitgebreid beschreven. Aan bod komt de opzet van de experimentele survey en een beschrijving van de afhankelijke, onafhankelijke en controle variabelen. Hoofdstuk 5 bevat een weergave van de resultaten van dit onderzoek. Aan bod komen onder andere een beschrijving van cybergedrag en verklaringen voor cybergedrag. Hoofdstuk 6 bevat de conclusie en discussie. Hierin volgt ook een doorkijkje naar mogelijke interventies die ontwikkeld kunnen worden op basis van de uitkomsten van dit onderzoek.

# 2. Onderzoeksvragen en -methoden

## *2.1. Inleiding*

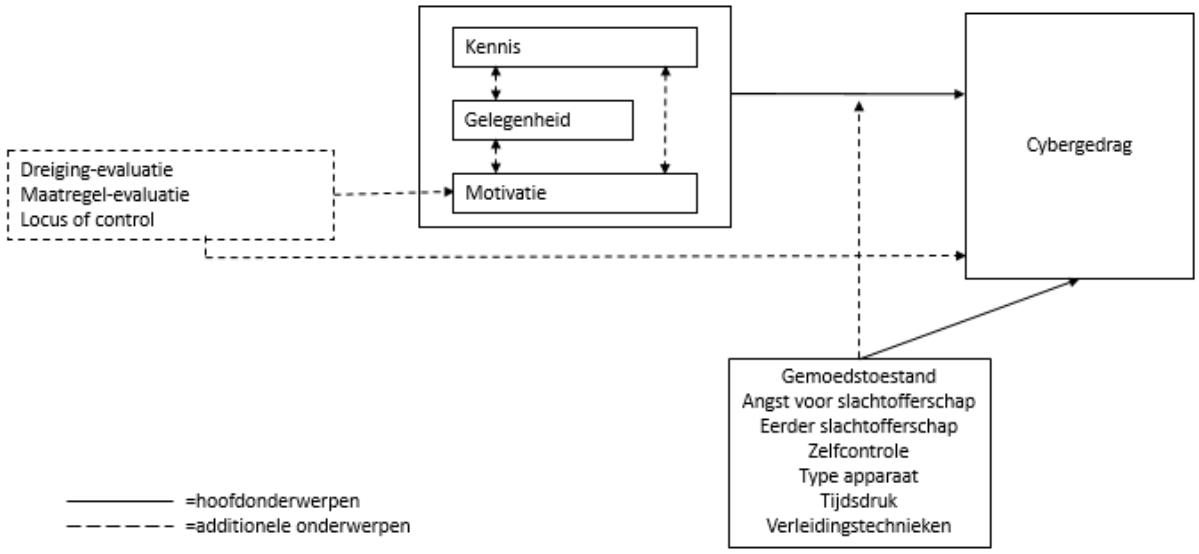
Het doel van dit onderzoek is om in kaart te brengen hoe Nederlanders zich online gedragen en dit te verklaren aan de hand van uit de literatuur naar voren gekomen factoren, om zodoende een eerste aanzet te geven om interventies te ontwikkelen om Nederlanders zich online veiliger te laten gedragen. In dit hoofdstuk bespreken we achtereenvolgens de onderzoeksfocus (paragraaf 2.2), de onderzoeksvragen (paragraaf 2.3) en de gebruikte onderzoeksmethoden (paragraaf 2.4).

## *2.2. Onderzoeksfocus*

Op basis van de literatuurstudie zal het uit te voeren onderzoek zich richten op een aantal hoofdonderwerpen (oranje in figuur 1). In dit onderzoek zal allereerst het cybergedrag[8] van Nederlanders worden onderzocht. Daarbij wordt onderzocht of cybergedrag samenhangt met drie verklarende factoren: kennis, gelegenheid en motivatie (zie hoofdstuk 3). Vervolgens zal het onderzoek zich richten op een aantal additionele factoren die relevant zijn gebleken uit de literatuurstudie (zie hoofdstuk 3, oranje in figuur 1); gemoedstoestand, angst voor slachtofferschap, eerder slachtofferschap, zelfcontrole, type apparaat, tijdsdruk, verleidingstechnieken. Bovendien zal worden bestudeerd of de effecten van kennis, gelegenheid en motivatie op cybergedrag afhankelijk zijn van deze variabelen. Onderzocht zal bijvoorbeeld worden of de mate waarin iemands cybergedrag wordt beïnvloed door zijn/haar kennis mede afhangt van zijn/haar gemoedstoestand.

Daarnaast zal het onderzoek zich richten op een aantal additionele factoren en verbanden die relevant zijn gebleken uit de literatuurstudie (zie hoofdstuk 3, blauw in figuur 1). Allereerst zouden de verklarende factoren kennis, gelegenheid en motivatie kunnen samenhangen en elkaar mogelijk beïnvloeden. Ook komen uit de literatuurstudie een aantal factoren naar voren die de mate waarin personen gemotiveerd zijn zich online veilig te gedragen worden, beïnvloeden; dreiging-evaluatie, maatregel-evaluatie en locus of control. Deze factoren zouden ook mogelijk een direct effect kunnen hebben op cybergedrag. Deze (blauwe) factoren zullen dan ook worden bestudeerd in de huidige studie.

[8] De term cybergedrag staat in dit rapport synoniem aan de term “online gedrag” en beslaat alle gedragingen van mensen online.




*Figuur 1. Schematische weergave van de onderwerpen van deze studie*

### *2.3. Onderzoeksvragen*

*Beschrijvende onderzoeksvragen*

1) Hoe veilig gedragen Nederlanders zich online?
   a) Gedrag 1: gebruik van wachtwoorden *(zelf-gerapporteerd + objectieve meting)*
   b) Gedrag 2: opslaan van belangrijke bestanden *(zelf-gerapporteerd)*
   c) Gedrag 3: installeren van updates *(zelf-gerapporteerd)*
   d) Gedrag 4: gebruik van beveiligingssoftware *(zelf-gerapporteerd)*
   e) Gedrag 5: alertheid tijdens internetgebruik *(zelf-gerapporteerd + objectieve meting)*
   f) Gedrag 6: delen van persoonlijke gegevens *(zelf-gerapporteerd + objectieve meting)*
   g) Gedrag 7: omgaan met bijlagen en hyperlinks in e-mails *(zelf-gerapporteerd + vignet)*

2) Is er een onderlinge samenhang tussen kennis, gelegenheid en motivatie?

3) Is er onderlinge samenhang tussen verschillende cybergedragingen?

*Verklarende onderzoeksvragen*

4) Kan het cybergedrag van Nederlanders worden verklaard door hun kennis van online veiligheid?

5) Kan het cybergedrag van Nederlanders worden verklaard door de gelegenheid die zij hebben voor veilig cybergedrag?
   a) Kan het cybergedrag van Nederlanders worden verklaard door de *sociale* gelegenheid[9] die zij hebben voor veilig cybergedrag?
   b) Kan het cybergedrag van Nederlanders worden verklaard door de *materiële* gelegenheid[10] 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
   a) een negatieve of positieve gemoedstoestand?
   b) angst voor slachtofferschap?
   c) eerder slachtofferschap?
   d) zelfcontrole?
   e) het type apparaat dat wordt gebruikt (pc, laptop, tablet, smartphone)?
   f) tijdsdruk?
   g) verleidingstechnieken die criminelen gebruiken?
   h) hun dreiging-evaluatie?
   i) hun maatregel-evaluatie?
   j) hun locus of control?

8) Verschilt het cybergedrag van Nederlanders tussen bevolkingsgroepen op basis van
   a) geslacht?
   b) opleidingsniveau?

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

c) leeftijd?
d) dagelijkse bezigheid?
e) gezinssamenstelling?

9) Worden de effecten van kennis, gelegenheid en motivatie op cybergedrag beïnvloed (interactie) door
a) een negatieve of positieve gemoedstoestand?
b) angst voor slachtofferschap?
c) eerder slachtofferschap?
d) zelfcontrole?
e) tijdsdruk?
f) verleidingstechnieken die criminelen gebruiken?

## *2.4. Onderzoeksmethode*

### *2.4.1 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. Er is een 3-staps gestructureerde aanpak gevolgd zoals voorgesteld door Webster en Watson (2002).

De eerste stap was het zoeken van relevante literatuur via de zoekmachines Google Scholar, Criminal Justice Abstracts, PsycINFO en Web of Science. De volgende zoektermen zijn (in sommige gevallen gecombineerd) in het Engels en Nederlands (niet weergegeven) gebruikt, in willekeurige volgorde: cyber crime, cyber attacks, cyber security, cyber resilience, (information) security awareness, security compliance, online victimization, cybercrime victimization, cyber hygiene behaviour, online safety behaviour, users' risk taking behaviour, disclosure, online routine activities, security behaviours, protection motivation theory, behavioural information security, password management, precautionary online behaviour, vignet study, phishing / malware / banking fraud, risk perceptions, risk factors, IT knowledge, resources, COM-B, capability, opportunity, motivation, locus of control, HAIS-Q, social engineering, online persuasion, moods, social surroundings.

Als tweede stap is de techniek *backward reference searching* gebruikt. Hierbij wordt gekeken naar de literatuurlijsten van de in stap één geïdentificeerde literatuur om eerder gepubliceerde relevante studies te vinden. Als derde stap is *forward reference searching* gebruikt, waarbij juist wordt gekeken naar

meer recente studies die verwijzen naar sleutelpublicaties die in eerdere stappen zijn geïdentificeerd. Tot slot is contact opgenomen met experts om de meest relevante en recente publicaties te vinden.

### *2.4.2 Experimentele survey*

Een uitgebreide beschrijving van deze methode staat in hoofdstuk 4. In deze paragraaf lichten we alleen kort het benodigde aantal respondenten, de steekproeftrekking en de ethische aspecten rondom deze methode toe.

#### *Benodigde aantal respondenten*

De experimentele survey bestond onder andere uit drie vignetten[11] (waarvan er één legitiem is en twee vals zijn), en drie objectieve metingen van cybergedrag, waaronder één meting met twee condities en één meting met drie condities. De vignetten en de objectieve metingen dienden afgenomen te worden op verschillende apparaten die veelvuldig in gebruik zijn onder burgers, te weten pc, laptop, tablet en smartphone. Om voldoende respondenten per conditie en afdoende statistische power in de analyses te behalen is gekozen om een steekproef van 2.000 personen na te streven. Zelfs bij een extreem scheve verdeling, waarbij bijvoorbeeld slechts vijf procent van de respondenten een tablet gebruikt, leidt dit tot ruim voldoende respondenten per experiment.

#### *Steekproef*

Voor het benaderen van respondenten hebben de onderzoekers een panelbureau (I&O Research) in de arm genomen. Er zijn 12.114 personen uitgenodigd door het panelbureau voor het invullen van de survey. In totaal waren er 6.902 personen die niet op de uitnodiging hebben gereageerd, 26 personen hebben zich afgemeld als lid bij het panelbureau en 2.069 personen hebben op de hyperlink in de uitnodiging geklikt, maar hebben de vragenlijst niet (volledig) ingevuld. Vervolgens hebben 1.859 van de non-respons leden, jonger dan 40 jaar, een tweede uitnodiging ontvangen om de representativiteit in deze leeftijdscategorie te verhogen. In totaal hebben 3.117 personen (25,7%) de vragenlijst ingevuld, tussen 6 mei 2019 en 26 mei 2019. Om de metingen en manipulaties correct te kunnen uitvoeren moesten respondenten de survey in één keer invullen. Om die reden zijn 691 personen uit de data verwijderd - zij

[11] In vragenlijstonderzoek kan (zelf-gerapporteerd) *gepercipieerd* gedrag worden onderzocht met behulp van vignetten en rollenspel. Deze methode maakt het mogelijk om respondenten te vragen naar het gedrag waarvan zij denken dat ze dit zouden vertonen in een fictieve, door de onderzoekers geschetste, situatie.

deden langer dan 60 minuten (596 personen) of korter dan 20 minuten (95 personen) over het invullen van de survey. De uiteindelijke steekproef bestaat uit 2.426 personen.

Op basis van geregistreerde panel bureau data zijn respondenten (N=2.426) vergeleken met non-respondenten (N=9.688). Respondenten zijn vaker man (53% versus 47%, p<.001) en gemiddeld ouder (57.9 versus 54.3 jaar, p<.001) dan non-respondenten maar verschillen nauwelijks in opleidingsniveau of de provincie waarin zij wonen.

Een representatieve steekproef heeft de voorkeur boven een convenience sample vanwege de externe validiteit van de resultaten. De steekproef van de huidige studie is representatief voor de Nederlandse samenleving met betrekking tot de kenmerken geslacht, werkend (ja/nee) en provincie waarin zij woonachtig zijn, maar zijn vaker hoogopgeleid en gemiddeld ouder (zie hoofdstuk 5 voor een uitgebreide bespreking van de kenmerken van de steekproef). Dat de steekproef niet representatief is op alle factoren heeft echter waarschijnlijk beperkte gevolgen voor de validiteit van de experimentele survey, zoals bleek in eerder onderzoek waarin "convenience samples" (gemaks-steekproeven) met representatieve samples werden vergeleken (Mullinix, Leeper, Druckman, & Freese, 2015). Mullinix et al. (2015) vonden bijvoorbeeld in twee studies grote overeenkomsten tussen effecten gemeten in convenience samples (zoals Amazon's Mechanical Turk) en representatieve steekproeven.

*Ethische aspecten van de experimentele survey*

Tijdens de experimentele survey zijn respondenten verschillende fictieve cyberrisico-situaties voorgelegd. Daarnaast zijn de respondenten gevraagd een wachtwoord te creëren en persoonlijke gegevens in te vullen. Deze aspecten van de vragenlijst roepen mogelijke ethische vraagstukken op. Bovendien bestond de zorg dat de (vergeleken met andere studies) opvallende vragen en situaties respondenten zouden afschrikken, wat tot grote uitval of toestroom tot de helpdesk van het panelbureau zou kunnen zorgen[12].

Voordat de survey is uitgezet, is de methodiek dan ook goedgekeurd door de ethische commissie van de Vrije Universiteit (het NSCR maakt standaard gebruik van deze ethische commissie). Het uitvragen van een wachtwoord en persoonlijke gegevens is ethisch toegestaan, mits de antwoorden niet geregistreerd worden. Het is daarom bij de onderzoekers bijvoorbeeld niet bekend welk wachtwoord respondenten hebben gekozen, alleen hoe sterk dit wachtwoord was. Ook zijn de persoonlijke gegevens die respondenten ingevuld hebben niet bekend bij de onderzoekers, alleen of respondenten wel of niet een bepaalde vraag naar persoonlijke gegevens hebben beantwoord. Tot slot zijn alle respondenten

[12] Dit bleek tijdens de dataverzameling nauwelijks te gebeuren.

vooraf (zoveel mogelijk) geïnformeerd middels een “informed consent” en achteraf op de hoogte gebracht van de aan hen voorgelegde cyberrisico-situaties en manipulaties middels een “debriefing” (inclusief respondenten die het invullen van de vragenlijst hebben afgebroken). De informed consent en debriefing zijn opgenomen in bijlage 2 en bijlage 3.

### *2.4.3 Expertbijeenkomst*

De eerste resultaten van de analyses zijn besproken met experts uit verschillende werkvelden tijdens een discussiebijeenkomst. Doel van deze bijeenkomst was om te komen 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.

Experts zijn geselecteerd op basis van de literatuurstudie, de netwerken van de onderzoekers en van de leden van de begeleidingscommissie. In totaal namen zeven experts deel aan de bijeenkomst. De experts zijn werkzaam voor overheden, bedrijfsleven en universiteiten vanuit diverse expertisegebieden, waaronder gedragswetenschappen en informatiebeveiliging. Een overzicht van alle deelnemers staat in bijlage 6.

# 3. Literatuurstudie naar cybergedrag

## *3.1. Inleiding*

Dit hoofdstuk bevat een weergave van de literatuur op het gebied van cybergedrag. In paragraaf 3.2 staat beschreven wat we weten over het risicoprofiel van slachtoffers van online criminaliteit centraal. Aan bod komen achtergrondkenmerken en routine activiteiten van slachtoffers. In paragraaf 3.3 staat cybergedrag centraal. Welke gedragingen leiden tot een verhoogde of verlaagde kans op slachtofferschap? In paragraaf 3.4 presenteren we gedragsmodellen die gebruikt kunnen worden als theoretische verklaringen voor cybergedrag. In paragraaf 3.5 komen gedragsinterventies aan bod. Dit hoofdstuk sluit af met een overzicht van de belangrijkste uitkomsten van de literatuurstudie (paragraaf 3.6).

## *3.2. Risicoprofiel voor slachtofferschap van online criminaliteit?*

Eerdere studies naar slachtofferschap van online criminaliteit hebben zich gericht op het opstellen van een risicoprofiel voor slachtofferschap en probeerden factoren te identificeren die het risico op slachtofferschap zouden kunnen vergroten. Hierna beschrijven we wat we weten over risicoprofielen op basis van persoonskenmerken en routine activiteiten.

### *3.2.1. Risicoprofiel op basis van persoonskenmerken*

In eerdere studies naar risicofactoren voor slachtofferschap van online criminaliteit staan persoonskenmerken vaak centraal. De meeste studies waarbij de samenhang tussen leeftijd en slachtofferschap is onderzocht, wijzen er op dat jongeren vaker slachtoffer worden van online criminaliteit dan oudere personen (Anderson, 2006; Domenie, Leukfeldt, van Wilsem, Jansen, & Stol, 2013; Jansen, Leukfeldt, Wilsem, & Stol, 2013; Ngo & Paternoster, 2011; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010; Van de Weijer & Leukfeldt, 2017; Van Wilsem, 2013a). Er zijn echter ook studies die geen verband vonden tussen leeftijd en online slachtofferschap voor bijvoorbeeld online identiteitsfraude, oplichting en malware (Bossler & Holt, 2009, 2010; Leukfeldt & Yar, 2016).

De samenhang tussen andere persoonskenmerken en slachtofferschap van online criminaliteit lijkt afhankelijk te zijn van het type online criminaliteit waar studies op focussen. Op het gebied van sociaaleconomische status hebben eerdere studies bijvoorbeeld gevonden dat mensen die werken mogelijk vaker slachtoffer worden van malware (Bossler & Holt, 2009) en minder vaak slachtoffer worden

van online intimidatie en laster (Ngo & Paternoster, 2011) dan niet-werkenden, maar voor slachtofferschap van hacken is er juist geen verschil tussen de werkenden en niet-werkenden (Domenie et al., 2013). In de studie van Domenie et al. (2013) blijkt verder in eerste instantie dat niet-werkenden vaker slachtoffer worden van online bedreiging, maar dit werd uiteindelijk verklaard door een verschil in hun internetactiviteiten. Zowel het hebben van een hoge als een lage opleiding lijkt de kans op slachtofferschap van bepaalde types online criminaliteit te verhogen. Hoger opgeleiden en personen met hogere inkomens lijken namelijk vaker slachtoffer te worden van identiteitsfraude (Paulissen & Van Wilsem, 2015) en lager opgeleiden van hacken (Domenie et al., 2013).

Over de relatie tussen geslacht en slachtofferschap bestaat geen eenduidig beeld. Mogelijk worden mannen vaker slachtoffer van bepaalde vormen van online criminaliteit, zoals online consumenten fraude en hacken[13] (Bossler & Holt, 2010; Van de Weijer & Leukfeldt, 2017). Vrouwen zouden juist vaker slachtoffer worden van een malware infectie (Bossler & Holt, 2009; Holt & Bossler, 2013) en phishing (Sheng et al., 2010) en worden vaker online lastig gevallen (Bossler & Holt, 2010). Studies die zich specifiek richten op identiteitsfraude, spreken elkaar tegen en concluderen dat mannen (Paulissen & Van Wilsem, 2015) of juist vrouwen (Anderson, 2006) vaker slachtoffer worden, of dat er geen verschil op basis van geslacht gevonden is (Domenie et al., 2013). Voor andere online delicten, zoals hacken, online stalken en online fraude, vonden studies geen verschillen tussen kans op slachtofferschap tussen mannen en vrouwen (Domenie et al., 2013; Ngo & Paternoster, 2011; Van Wilsem, 2013a).

Daarnaast blijkt uit de studie van Domenie et al. (2013) dat alleenstaanden vaker slachtoffer worden van hacken, maar dit geldt niet voor andere soorten online criminaliteit zoals malware, phishing en cyberstalking (Domenie et al., 2013).

Ten slotte blijkt er tussen etnische groepen geen verschillen in slachtofferschap te bestaan (Bossler & Holt, 2009; Domenie et al., 2013; Ngo & Paternoster, 2011).

Alle studies samengenomen lijkt het dus niet mogelijk om een eenduidig risicoprofiel vast te stellen. Cybercriminelen selecteren blijkbaar niet wie ze aanvallen en zijn niet al te kieskeurig. Iedereen is een potentieel slachtoffer voor online criminaliteit. Er kan zodoende geen profiel worden geschetst van risicovolle persoonskenmerken van burgers voor slachtofferschap van online criminaliteit (Leukfeldt, 2014; Paulissen & Van Wilsem, 2015).

### *3.2.2. Risicoprofiel op basis van routine activiteiten*

[13] De onderzoekers vroegen de respondenten of zij slachtoffer waren geworden van “someone adding, deleting, or changing information in your computer files without your knowledge or permission” (Bossler & Holt, 2010).

Naast persoonskenmerken werden ook online routine activiteiten van internetters in een aantal studies onderzocht. De aanname is dat bepaalde online routine activiteiten ervoor kunnen zorgen dat potentiële slachtoffers zichtbaar zijn voor criminelen. In bepaalde studies wordt er inderdaad een verband gevonden tussen slachtofferschap en online activiteiten. Zo lijken online "conduct" (zoals gericht informatie zoeken op internet en e-mailen) en "exposure" (bijvoorbeeld ongericht surfen, video's kijken en gebruik van sociale media) positief samen te hangen met slachtofferschap (Domenie et al., 2013; Van Wilsem, 2013a). Andere vormen van routine activiteiten die de kans op slachtofferschap lijken te vergroten, zijn internetbankieren, online winkelen, gebruik van sociale media en online gamen (Choi, 2008; Leukfeldt & Yar, 2016; Ovelgönne, Dumitras, Prakash, Subrahmanian, & Wang, 2017; Paulissen & Van Wilsem, 2015; Van Wilsem, 2013a). Het lijkt er echter op dat afzonderlijke routine activiteiten alleen gerelateerd zijn aan slachtofferschap van bepaalde soorten online criminaliteit. Zo verhoogt het gebruik van Twitter de kans op online bedreiging, maar niet op identiteitsdiefstal, hacken of malware (Leukfeldt & Yar, 2016). Bovendien lijken er interactie-effecten te bestaan tussen routine activiteiten en eigenschappen zoals leeftijd en opleiding (Domenie et al., 2013). Het feit dat jongeren bijvoorbeeld vaker online zijn dan ouderen, verklaart mogelijk deels dat jongeren vaker slachtoffer worden (Büchi, Just, & Latzer, 2016).

Echter, niet alle studies laten zien dat routine activiteiten samenhangen met slachtofferschap (Bossler & Holt, 2009; Holt & Bossler, 2013; Jansen et al., 2013; Paulissen & Van Wilsem, 2015). Paulissen en Van Wilsem (2015) vonden bijvoorbeeld in een Nederlandse representatieve steekproef geen verband tussen slachtofferschap van identiteitsfraude en gebruik van sociale media of de hoeveelheid tijd die respondenten op internet actief zijn. Ook de resultaten uit de studie van Jansen et al. (2013) wezen er op dat de hoeveelheid uren dat iemand online is niet samenhangt met de kans op slachtofferschap van online criminaliteit.

Eerdere studies naar de samenhang tussen slachtofferschap van online criminaliteit en de mate waarin burgers zich blootstellen aan dreigingen door online te zijn, laten aldus wisselende resultaten zien. Het lijkt erop dat bepaalde online activiteiten alleen de kans op slachtofferschap van specifieke vormen van cybercrime verhogen. Er lijken samengenomen geen routine activiteiten te zijn die per definitie risico verhogend zijn (Leukfeldt & Yar, 2016). Er kan daarom niet geconcludeerd worden dat er een duidelijk verband gevonden is tussen online routine activiteiten en kans op slachtofferschap van cybercrime in het algemeen.

## *3.3. Cybergedrag en slachtofferschap van online criminaliteit*

### *3.3.1. Cybergedrag*

In plaats van slachtofferschap te zien als een risico dat samenhangt met persoonskenmerken of routine activiteiten, kan ook worden gekeken naar *gedrag* als pijler voor risico op slachtofferschap, namelijk cybergedrag[14]. Onveilig cybergedrag kan direct bijdragen aan een verhoogde kans op slachtofferschap. Slachtoffers van online bankfraude blijken bijvoorbeeld vaak onbedoeld hun persoonlijke informatie aan fraudeurs te hebben gegeven, onder andere door te klikken op een hyperlink in een phishing mail of informatie in te vullen op een phishing website (Jansen, 2018; Jansen & Leukfeldt, 2015, 2016).

Een belangrijke voorwaarde voor online veiligheid is dus veilig cybergedrag (in de literatuur wordt dit ook wel omschreven als cyber hygiëne gedrag, zie bijvoorbeeld Cain, Edwards, & Still, 2018). Mensen die zich online veilig – of cyber hygiënisch- gedragen, houden zich aan "gouden" regels (best practices) en beschermen hun persoonlijke gegevens. Zij vermijden bijvoorbeeld onveilige websites, voorkomen dat ze klikken op onbetrouwbare hyperlinks, gebruiken sterke wachtwoorden en houden hun technische veiligheidsmaatregelen up-to-date (Cain et al., 2018; Crossler, Bélanger, & Ormond, 2017; Symantec, 2018). Er is tot op heden echter nog geen vastomlijnde definitie of gestandaardiseerde operationalisatie van veilig of onveilig cybergedrag in de academische wereld. Op basis van eerdere empirische studies hebben we voor onderhavig onderzoek zeven centrale gedragsclusters geïdentificeerd. Wanneer individuele gebruikers binnen elk cluster veilig gedrag vertonen, zou dit hen kunnen beschermen tegen slachtofferschap van cybercriminaliteit (voor meer informatie, zie Cain et al., 2018; Crossler et al., 2017; Van Schaik et al., 2017). Deze gedragsclusters, in willekeurige volgorde, zijn:

- 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.

[14] Zoals in de inleiding beschreven staat de term cybergedrag in dit rapport synoniem aan de term "online gedrag" en beslaat alle gedragingen van mensen online.

Uit verschillende studies, zowel gebaseerd op zelf-gerapporteerd gedrag als werkelijk gedrag in experiment-setting, is gebleken dat veel mensen zich slechts in beperkte mate veilig gedragen online en zelfs ronduit onveilig gedrag vertonen online. Dit geldt voor elk van de zeven gedragsclusters. Zo blijken veel mensen geen virusscanner of firewall op hun thuiscomputer te hebben, of houden zij deze niet up-to-date (Cain et al., 2018; Van Schaik et al., 2017). Daarnaast zouden jongeren laks zijn met de beveiliging van hun smartphone (Jones & Heinrichs, 2012; Tan & Aguilar, 2012). Hoewel het gebruik van unieke, sterke wachtwoorden een belangrijke beveiligingsmaatregel is, hebben studies aangetoond dat 50-60% van de wachtwoorden wordt hergebruikt op verschillende platforms (Alohali, Clarke, Li, & Furnell, 2018; Cain et al., 2018; Grawemeyer & Johnson, 2011). Ook zou tussen de 30 procent en 95 procent van de mensen hun wachtwoorden delen met anderen (Alohali et al., 2018; Cain et al., 2018; Kaye, 2011). Een ander voorbeeld van onveilig cybergedrag is dat mensen op grote schaal persoonlijke informatie delen op sociale media (Christofides, Muise, & Desmarais, 2012; Debatin et al., 2009; Talib et al., 2010). Veel van de respondenten in de studie van Talib et al. (2010) deelden bijvoorbeeld hun volledige naam en e-mailadres (62%), geboortedatum (45%) of volledige adres (7%) op een online sociaal netwerk. Deze informatie kan door cybercriminelen gebruikt worden om phishing e-mails geloofwaardiger te maken en identiteitsfraude te plegen (Caputo, Pfleeger, Freeman, & Johnson, 2014). Ook het klikken op pop-ups en het openen van bijlagen van onbekende bronnen kan gezien worden als onveilig cybergedrag dat de kwetsbaarheid voor cyberaanvallen vergroot (Choi, 2008; Jansen & Leukfeldt, 2015). Tot slot komt deviant computer gedrag, zoals illegaal downloaden, online pesten en anderen bedreigen, veelvuldig voor en draagt dit bij aan online slachtofferschap, mogelijk vooral onder jongeren (Bossler & Holt, 2009; Holt & Bossler, 2013; Maimon & Louderback, 2019; Ngo & Paternoster, 2011).

Een conclusie die bovendien uit de literatuur getrokken kan worden, is de toegevoegde waarde die een focus op gedrag heeft boven een focus op specifieke cyberdelicten. Slachtofferschap van hacken kan bijvoorbeeld ontstaan door vele uiteenlopende gedragingen. Zo kunnen mensen gehackt worden omdat ze persoonlijke gegevens hebben gedeeld, malware hebben gedownload of geen up-to-date beveiliging hebben. Deze gedragingen kunnen bovendien ook tot slachtofferschap van andere vormen van online criminaliteit leiden, zoals online fraude of identiteitsfraude. Studies die zich richten op specifieke delicten, bieden slechts inzage in een klein deel van de complexiteit van cybergedrag en online criminaliteit. Met een focus op *cybergedrag* kan daarentegen potentieel een breed scala aan cyberdelicten aangepakt worden.

### *3.3.2. Het meten van cybergedrag*

Cybergedrag, en de mate waarin dit veilig of onveilig is, is tot op heden grofweg op twee manieren gemeten. Sommige onderzoekers hebben gepercipieerd gedrag gemeten door te vragen hoe respondenten zich doorgaans gedragen of hoe zij zich in een fictieve situatie zouden gedragen. In andere studies is daadwerkelijk gedrag geobserveerd. In deze paragraaf zal een overzicht worden gegeven van de manieren waarop eerdere studies dit hebben vormgegeven.

*Onderzoek naar zelf-gerapporteerd gedrag*

De meeste eerdere studies naar cybergedrag hebben zich gericht op zelf-gerapporteerd gedrag. Respondenten in deze studies werden bevraagd naar hun gedrag, bijvoorbeeld aan de hand van stellingen ("ik open e-mails van onbekende afzenders – nooit, zelden, soms, vaak") of vragen (welk percentage van uw wachtwoorden verandert u elke drie maanden?) (Cain et al., 2018; Crossler & Bélanger, 2014; Domenie et al., 2013). Een voorbeeld van een onderzoeksinstrument dat werkt met stellingen is de HAIS-Q, ofwel de Human Aspects of Information Security- Questionnaire, een meetmodel gericht op het meten van veilig cybergedrag en achterliggende bronnen (Parsons et al., 2014, 2017). Dit instrument meet kennis, attitudes en gepercipieerd gedrag op een aantal relevante onderwerpen, zoals wachtwoordmanagement en mobiel werken.

In vragenlijstonderzoek kan ook (zelf-gerapporteerd) *gepercipieerd* gedrag worden onderzocht met behulp van vignetten en rollenspel (Downs, Holbrook, & Cranor, 2007; Jong, Leukfeldt, & van de Weijer, 2018; Sheng et al., 2010). Deze methodes maken het mogelijk om respondenten te vragen naar het gedrag waarvan zij denken dat ze dit zouden vertonen in een fictieve, door de onderzoekers geschetste, situatie (Vance, Siponen, & Pahnila, 2012). Een belangrijk voordeel van deze onderzoeksmethode is dat het onderzoekers in staat stelt om situationele factoren, die ruis zouden kunnen veroorzaken in vragenlijstonderzoek, te bepalen. In een rollenspel kunnen onderzoekers enerzijds bepaalde factoren gelijkstellen voor iedereen (stel u voor: uw naam is Henk Jansen en u werkt bij een bakkerij). Anderzijds kunnen onderzoekers factoren manipuleren, waarbij subgroepen respondenten een aangepaste situatie krijgen voorgelegd. De onderzoekers differentiëren bijvoorbeeld tussen subgroep één (stel u voor: u bent nog nooit slachtoffer geweest van een delict) en subgroep twee (stel u voor: u bent in het verleden opgelicht op een online webshop). Op basis van de geschetste omstandigheden kan respondenten worden gevraagd hoe zij zouden handelen in deze situatie (Downs et al., 2007; Jong et al., 2018; Sheng et al., 2010).

Vragenlijstonderzoek heeft als onderzoeksmethode verschillende voordelen. Zo zijn de investeringen die nodig zijn voor vragenlijstonderzoek relatief laag, terwijl een grote representatieve onderzoekspopulatie bereikt kan worden. Ook zijn de antwoorden op gestandaardiseerde vragen geschikt voor kwantitatieve analyse om verklarende factoren te kunnen onderscheiden en zijn antwoorden tussen respondenten goed te vergelijken.

Er kleven echter ook nadelen aan het onderzoeken van gedrag met behulp van vragenlijsten en vignetten. Bij studies naar gepercipieerd gedrag ligt de focus op hoe mensen *zeggen* dat zij zich doorgaans online gedragen of zouden gedragen in een hypothetische situatie. Hoewel de meeste mensen aangeven cybersecurity belangrijk te vinden (Madden & Rainie, 2015) correspondeert hun zelf-gerapporteerd gedrag niet altijd met hun werkelijke gedrag (Smith & Louis, 2008; Spiekermann, Grossklags, & Berendt, 2001; Van Der Zee, 2018). Dit wordt ook wel de cybersecurity paradox genoemd (Van Der Zee, 2018). Een voorbeeld hiervan is dat personen die aangeven in zelfrapportage onderzoek te weten dat zij beter niet op een hyperlink kunnen klikken in een e-mail van een onbekende afzender, dit in de praktijk soms toch doen. Enerzijds kan dit komen omdat mensen niet willen toegeven wat zij online doen of sociaal wenselijke antwoorden geven, maar anderzijds is het ook denkbaar dat niet iedereen zich realiseert dat zij onveilig gedrag vertonen op internet. Wanneer onderzoek zich uitsluitend richt op zelfrapportage van cybergedrag, resulteert dit mogelijk in een onjuist beeld van hoe mensen zich werkelijk online gedragen.

*Onderzoek naar daadwerkelijk gedrag*

In plaats van zelf-gerapporteerd gedrag kan onderzoek ook gericht worden op daadwerkelijk gedrag, het daadwerkelijke cybergedrag van burgers. Trappen ze wel of niet in de val van cybercriminelen? Eerdere studies waar het daadwerkelijke gedrag is gemeten zijn schaars binnen het domein van cyber security. De studies die gedaan zijn richten zich veelal op slachtofferschap van phishing.[15] Degelijke studies gebruiken veelal phishing testen voor het objectief meten van de mate van gevoeligheid voor phishing, oftewel het testen van hun weerbaarheid tegen phishing aanvallen (zie bijvoorbeeld Cain et al. 2018, voor een overzicht). De phishing test bestaat uit een nagemaakte phishing e-mail die de onderzoekers verspreiden onder een onderzoekspopulatie. Door te meten hoe vaak wordt geklikt op de hyperlink in de e-mail en hoe vaak mensen die klikken ook daadwerkelijk vertrouwelijke of persoonlijke informatie achterlaten op een nagemaakte phishing website, kan worden bepaald of een interventie gericht op het terugbrengen

[15] Bij phishing proberen cybercriminelen inloggegevens te achterhalen en toegang te krijgen tot accounts, bijvoorbeeld van online rekeningen. Internetcriminelen doen phishing aanvallen bijvoorbeeld via e-mail of websites (Lastdrager, 2014).

van het aantal incidenten met phishing e-mails succesvol is geweest. Daarbij is het ook van belang te kijken naar het klikgedrag bij legitieme verzoeken in e-mails. Het mag niet zo zijn dat een interventie ertoe heeft geleid dat mensen op geen enkel verzoek om te klikken op een hyperlink of het openen van een bijlage meer reageren. Een belangrijk bezwaar van deze methode is dat je mensen misleidt voor onderzoeksdoeleinden. Deelnemers aan een phishing test hebben veelal vooraf geen toestemming gegeven voor deelname.

Kaptein et al. (2009) hebben gekeken naar hoe makkelijk mensen te verleiden zijn om persoonlijke informatie prijs te geven. Meer specifiek is gekeken naar een type informatie dat cybercriminelen kunnen gebruiken in phishing aanvallen: e-mailadressen. Deelnemers vulden eerst een enquête in. De enquête bestond uit zogenaamde dummy-vragen: de vragen deden er niet toe, maar werden gebruikt voor een ander onderzoek. De werkelijke meting vond plaats nadat de respondenten de enquête hadden ingevuld. Respondenten werd gevraagd naar e-mailadressen van vrienden en bekenden die mogelijk ook mee wilden doen aan het onderzoek. Op dit verzoek werden verschillende verleidingstechnieken toegepast. Respondenten kregen bijvoorbeeld te horen dat andere respondenten al verschillende e-mailadressen hadden gegeven aan de onderzoekers (sociaal bewijs) of dat ze de resultaten van het onderzoek thuisgestuurd zouden krijgen als ze tenminste een e-mailadres zouden opgeven (wederkerigheid). Het toepassen van een verleidingstechniek leidde ertoe dat er significant meer e-mailadressen werden opgehaald. Bovendien werd een relatie gevonden tussen de mate van beïnvloedbaarheid van respondenten en de mate waarin ze gevoelig waren voor de verleidtechnieken (Kaptein et al., 2009). Dit laat zien dat er individuele verschillen bestaan in mate van beïnvloedbaarheid.

Junger et al. (2017) zijn een stapje verder gegaan. Zij hebben gekeken naar hoe makkelijk het is om mensen te verleiden om persoonlijke informatie te geven die gebruikt kan worden in een meer effectieve variant van phishing, namelijk spear phishing, waarbij de persoonlijke gegevens van het slachtoffer worden gebruikt om hem of haar een gevoel van vertrouwen te geven. Op straat werden mensen aangesproken of ze mee wilden doen aan een enquête. In deze enquête werd een aantal vragen gesteld over online koopgedrag: of ze wel eens iets kopen op internet, zo ja, waar en wat. Ook werd gevraagd om een deel van hun IBAN-nummer en hun e-mailadres. Mensen waren verrassend vaak bereid om dergelijke persoonlijke informatie te geven aan de enquêteurs. Met deze informatie kan in potentie een heel gerichte en effectieve (spear) phishing aanval worden gedaan. Mensen lijken zich nauwelijks bewust van de risico's die het weggeven van dit soort informatie met zich meebrengt.

*Zelf-gerapporteerd gedrag versus daadwerkelijk gedrag*

Cybergedrag kan dus op verschillende manieren gemeten worden. Over het algemeen kunnen we stellen dat objectieve metingen van gedrag zijn te prefereren boven zelfrapportages van gedrag. Zelfrapportages kunnen afwijken van de werkelijkheid omdat zij een beroep doen op het geheugen van respondenten of omdat respondenten sociaal wenselijke antwoorden geven. Objectief onderzoek naar cybergedrag kan dan ook een grote bijdrage leveren aan onze kennis over online slachtofferschap en de omstandigheden die cybergedrag beïnvloeden (Maimon & Louderback, 2019). Objectieve metingen hebben echter ook praktische nadelen. Zo zijn objectieve metingen van gedrag niet in alle situaties uitvoerbaar, bijvoorbeeld als we willen weten hoe mensen zich gedragen tijdens een terroristische aanslag. Ook mogen onderzoekers hun respondenten niet misleiden. Objectieve metingen kunnen bovendien kostbaar zijn om uit te voeren en zijn tijdsintensief, zoals in het geval van het observeren van hoe vaak mensen hun laptop in slaapstand zetten in een kantoorsituatie. Per onderzoek zal dan ook bepaald moeten worden wat de meest geschikte manier is van het meten van cybergedrag van burgers in termen van kosten en baten.

## *3.4. Theoretische verklaringen voor cybergedrag*

Hoewel veilig cybergedrag van groot belang is om slachtofferschap van online criminaliteit te voorkomen, komt onveilig cybergedrag veelvuldig voor. In deze paragraaf zullen twee theorieën worden besproken die cybergedrag proberen te verklaren. De *protection motivation theory* is de meest gebruikte theorie om de mate waarin mensen gemotiveerd zijn om zich online veilig te gedrag te verklaren. Omdat cybergedrag ook door andere factoren dan motivatie wordt beïnvloed, zal het *COM-B gedragsmodel* worden besproken (zie bv. MacInnis et al., 1991; Michie, Stralen, & West, 2011 - zie paragraaf 3.4.2). Hierin wordt beargumenteerd dat veilig cybergedrag alleen plaatsvindt wanneer, naast motivatie, capaciteit en gelegenheid voor het gedrag aanwezig zijn.

### *3.4.1. Protection motivation theory*

De protection motivation theory (PMT) is een sociaal cognitieve theorie die gedrag voorspelt en zich richt op de motivatie die mensen hebben om zichzelf te beschermen. PMT werd in 1975 opgesteld door Rogers (1975) en heeft sindsdien een aantal revisies ondergaan (Floyd, Prentice-Dunn, & Rogers, 2000; Milne, Orbell, & Sheeran, 2002; Norman, Boer, & Seydel, 2005). Conceptueel is “protection motivation” hetzelfde als het hebben van een intentie (Floyd et al., 2000). Deze motivatie zou volgens PMT een directe invloed hebben op daadwerkelijk gedrag.

Daarnaast beslaat de theorie een breed spectrum van factoren, die samen voorspellen en verklaren in welke mate mensen gemotiveerd zijn om voorzorgsmaatregelen te nemen en preventief gedrag (*precautionary behaviour*) te vertonen (Floyd et al., 2000; Milne et al., 2002). Volgens PMT raken mensen gemotiveerd om zichzelf te beschermen tegen een dreiging (*threat*) na een evaluatie van 1) de dreiging en 2) de maatregelen tegen deze dreiging. Onderdeel van de dreiging-evaluatie zijn gepercipieerde kwetsbaarheid (inschatting van eigen kwetsbaarheid voor de dreiging) en impact (inschatting van de ernst van de dreiging). Vervolgens evalueert deze persoon de maatregel door beslissingen te nemen over de responseffectiviteit (of een maatregel effectief zal zijn tegen de dreiging), zelfeffectiviteit (of hij/zij in staat is om effectieve maatregel te nemen) en responskosten (of de ingeschatte kosten het waard zijn). In tabel 1 is een overzicht van deze PMT factoren weergegeven. Op basis van deze evaluaties raken mensen gemotiveerd om door te gaan met hun gedrag of om af te zien van een gedraging (Floyd et al., 2000). Hoe mensen scoren op deze factoren, is mogelijk mede afhankelijk van hun geslacht en opleidingsniveau (Jansen, 2018).

*Tabel 1. Cognitieve processen in PMT die cybergedrag verklaren*

| | *Nederlands* | *Engels*[16] |
|---|---|---|
| **Cognitief proces** | **Dreiging-evaluatie** | **Threat appraisal** |
| Onderdelen | Gepercipieerde kwetsbaarheid | Perceived vulnerability |
| | Gepercipieerde impact | Perceived severity |
| | | |
| **Cognitief proces** | **Maatregel-evaluatie** | **Coping appraisal** |
| Onderdelen | Responseffectiviteit | Response-efficacy |
| | Zelfeffectiviteit | Self-efficacy |
| | Responskosten | Response costs |

PMT is eerder toegepast op cybergedrag (Boehmer, LaRose, Rifon, Alhabash, & Cotten, 2015; Crossler & Bélanger, 2014; Jansen, 2018; Shillair et al., 2015; Sommestad, Karlzén, & Hallberg, 2015; Workman et al., 2008). Deze studies hebben aangetoond dat PMT een nuttig theoretisch raamwerk is om het proces te begrijpen dat mensen doorlopen wanneer zij moeten kiezen op welke manier zij zich online willen gedragen (Crossler & Bélanger, 2014; Jansen, 2018). Jansen (2018) onderzocht bijvoorbeeld online

[16] Omwille van de aansluiting met de internationale literatuur zijn de Engelse termen eveneens opgenomen.

bankieren onder Nederlanders en vond dat 64 procent van de variantie in cybergedrag werd verklaard door PMT factoren. Volgens PMT evalueren mensen mogelijke online risico's, zoals de risico's van online betalingen en downloaden. Uit deze evaluatie resulteert een bepaalde mate van motivatie tot zelfbescherming. Terwijl een hoge mate van motivatie tot zelfbescherming ertoe zou leiden dat mensen aanbevolen beschermingsmaatregelen gebruiken (*adaptive coping*), leidt een lage mate van deze motivatie tot het negeren van adviezen en mogelijke blootstelling aan online gevaren (*maladaptive coping*) (Crossler & Bélanger, 2014; Floyd et al., 2000; Jansen, 2018).

Eerdere studies die PMT factoren bestudeerden, vonden dat ingeschatte responseffectiviteit en zelfeffectiviteit belangrijke voorspellers zijn voor veilig cybergedrag (Arachchilage & Love, 2014; Crossler & Bélanger, 2014; Crossler et al., 2017; Jansen & van Schaik, 2017; Rhee et al., 2009; Van Schaik et al., 2017; Workman et al., 2008). Daarnaast lijken de responskosten een belangrijke voorspeller voor veilig cybergedrag (Crossler et al., 2017; Jansen & van Schaik, 2017; Workman et al., 2008). Gepercipieerde kwetsbaarheid hangt echter mogelijk niet op de verwachte wijze samen met veilig cybergedrag. Mensen die zichzelf kwetsbaar inschatten voor cyberaanvallen gedragen zich daardoor niet anders (Jansen, 2018) of zelfs juist onveiliger (Crossler & Bélanger, 2014). Verder vinden de meeste studies een relatie tussen gepercipieerde impact en cybergedrag (Crossler et al., 2017; Jansen, 2018; Jansen & van Schaik, 2017). Alleen Downs, Holbrook en Cranor (2007) zagen dat niet binnen hun sample van 232 computergebruikers, waarbij ze specifiek onderzochten of cybergedrag werd voorspeld door de ingeschatte ernst van de consequenties van een geslaagde phishing aanval.

Onderdeel van PMT zijn ook twee intra-persoonlijke factoren die samenhangen met cybergedrag, namelijk 1) persoonlijkheidskenmerken (zelfcontrole en persoonlijkheidsdimensies) en 2) eerdere ervaringen (Floyd et al., 2000). Dat zelfcontrole relevant is voor cybergedrag wordt buiten PMT ook in andere onderzoeksvelden beargumenteerd (Bossler & Holt, 2010; Ngo & Paternoster, 2011; Van de Weijer & Leukfeldt, 2017; Van Wilsem, 2013b). In de criminologie wordt in de zelfcontrole-theorie gesteld dat mensen met een lage zelfcontrole impulsief zijn, risico's niet mijden en zich vooral richten op de korte termijn (Gottfredson & Hirschi, 1990). Dit zouden samen belangrijke voorspellers zijn voor onveilig cybergedrag en slachtofferschap. Eerdere studies wijzen er op dat personen met lage zelfcontrole mogelijk vaker slachtoffer worden van online criminaliteit (Ngo & Paternoster, 2011; Paulissen & Van Wilsem, 2015; Van Wilsem, 2013a). Impulsieve personen hebben bijvoorbeeld een hoger risico om slachtoffer te worden van online criminaliteit, mogelijk omdat zij vaker online actief zijn (Van Wilsem, 2013a). De samenhang tussen zelfcontrole en slachtofferschap hangt mogelijk ook af van het type online

criminaliteit (Domenie et al., 2013; Paulissen & Van Wilsem, 2015). Domenie et al. (2013) vonden bijvoorbeeld dat geringe zelfcontrole alleen samenhing met verhoogde kans om gehackt te worden en niet met delicten zoals malware en identiteitsfraude. Bovendien wordt het verband tussen zelfcontrole en online slachtofferschap mogelijk verklaard door andere factoren, zoals delinquent gedrag en omgang met delinquenten (Bossler & Holt, 2010).

Op basis van de literatuur zijn naast zelfcontrole een aantal persoonlijkheidsdimensies af te leiden die risicofactoren zouden kunnen vormen voor onveilig cybergedrag, genaamd de "Big 5" - extraversie, zorgvuldigheid, emotionele stabiliteit, openheid voor nieuwe ervaringen en servicegerichtheid (McCrae & Costa, 1999). Er zijn echter slechts enkele studies die zich gericht hebben op het toetsen van de samenhang tussen deze dimensies en cybergedrag (Alohali et al., 2018; Borwell, Jansen, & Stol, 2018; Van de Weijer & Leukfeldt, 2017). Van de Weijer en Leukfeldt (2017) richtten zich op de samenhang tussen de "Big 5" persoonlijkheidsdimensies en slachtofferschap van online criminaliteit onder een representatieve steekproef van Nederlanders. Resultaten toonden aan dat personen die hoog scoren op "zorgvuldigheid" (*conscientiousness*) en "emotionele stabiliteit", een lager risico hebben om slachtoffer te worden van een cyberdelict, terwijl dit risico juist hoger is voor personen die grote openheid voor nieuwe ervaringen hebben. Alleen emotionele stabiliteit lijkt meer samen te hangen met online criminaliteit dan andere criminaliteit. Personen die hoog scoren op emotionele stabiliteit, lijken minder vaak slachtoffer van online criminaliteit te worden dan van traditionele criminaliteit (Van de Weijer & Leukfeldt, 2017). Samengenomen lijken persoonlijkheidskenmerken slechts een kleine verklaarde variantie op te leveren en slachtofferschap van online criminaliteit lijkt dan ook vooral te wijten aan andere factoren (Borwell et al., 2018; Van de Weijer & Leukfeldt, 2017). Een studie die zich richtte op de samenhang tussen persoonlijkheidsdimensies en cybergedrag vond, in lijn met de verwachting, dat mensen die hoog scoren op de dimensie "zorgvuldigheid" minder vaak onveilig cybergedrag vertonen, zoals het klikken op onbetrouwbare e-mail hyperlinks (Alohali et al., 2018).

De tweede intra-persoonlijke factor die onderdeel is van PMT, zijn de eerdere ervaringen die mensen hebben, zoals slachtoffer worden van online criminaliteit. Eerdere ervaringen kunnen een belangrijke voorspeller zijn voor toekomstig gedrag (Debatin et al., 2009; Rhee et al., 2009; Vance et al., 2012). In PMT wordt beargumenteerd dat mensen hun cybergedrag aanpassen nadat zij slachtoffer zijn geworden van een cyberaanval en zodoende zich online veiliger gedragen dan mensen die nog geen slachtoffer zijn geworden. Facebook gebruikers die vervelende ervaringen hebben opgedaan omdat zij persoonlijke informatie hadden gedeeld, zijn zich daarna meer bewust van de risico's en weten zichzelf beter te beschermen (Christofides et al., 2012; Debatin et al., 2009). Niet alle studies wijzen echter in deze

richting. Cain et al. (2018) vonden onder slachtoffers van online criminaliteit geen verband tussen eerdere aanvallen en cyber hygiëne gedrag. Mogelijk lijdt eerder slachtofferschap niet direct tot een verandering in cybergedrag en zijn deze mensen slachtoffer geworden van online criminaliteit, juist omdat zij zich minder veilig gedragen dan niet-slachtoffers (Cain et al., 2018).

### *3.4.2. COM-B model*

Een belangrijke beperking van PMT is dat het alleen de motivatie of intentie tot gedrag voorspelt. Werkelijk cybergedrag kan daar van afwijken (Crossler et al., 2013). Veel studies die PMT als uitgangspunt nemen, hebben bovendien als doel om theoretische verwachtingen te valideren. Zij hebben daardoor een beperkt perspectief op cybergedrag en andere relevante variabelen in het verklaren van gedrag worden veelal buiten beschouwing gelaten. Dit is een belangrijke constatering omdat, zoals al benadrukt door Vroom en Von Solms (2004), het cybergedrag van mensen wordt verklaard door veel meer factoren dan motivatie alleen (zie ook Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).

Het *Capability- Opportunity- Motivation- Behaviour* (COM-B) model stelt dat gedrag van mensen kan worden verklaard door hun capaciteiten en motivatie, gelegenheid en de interactie tussen deze componenten (Michie et al., 2011). Capaciteiten (*capabilities*) worden gedefinieerd als het psychologische en fysieke vermogen van het individu om specifiek gedrag te vertonen. Het omvat het hebben van de nodige kennis en vaardigheden. Gelegenheid (*opportunity*) wordt gedefinieerd als alle factoren die buiten het individu liggen en die het gedrag mogelijk maken of juist weerhouden, zoals het gedrag van huisgenoten of collega's. Motivatie (*motivation*) wordt gedefinieerd als al die hersenprocessen die gedrag activeren en sturen. Hieronder verstaan Michie et al. (2011) niet alleen doelen die mensen zich stellen en bewuste besluitvormingsprocessen, maar ook automatisch en reflexmatig handelen die het gevolg zijn van persoonlijke aanleg, associatieve leerprocessen en emoties. Inzicht in de mate waarin deze componenten een rol spelen in cybergedrag van burgers, is nodig om in een later stadium het gedrag op een effectieve manier te kunnen beïnvloeden door interventies die deze componenten veranderen.

COM-B is vooral toegepast als gedragsveranderingsmodel binnen de marketing en in het gezondheidsdomein, bijvoorbeeld gericht op het ontwerpen van interventies om ongezond gedrag te beïnvloeden en het meten van de effecten hiervan, zoals bij programma's om mensen te helpen met stoppen met roken (zie bv. Brown, Kotz, Michie, Stapleton, Walmsley, & West, 2014). Bestaande meetmodellen zijn dan ook vooral gericht op het in kaart brengen van consumentengedrag en ongezond gedrag (zie bv. Atkins, & Michie, 2013). Er zijn zover bekend nog geen concrete toepassingen van COM-B

in het cyber domein. Wel hebben enkele eerdere studies zich gericht op de afzonderlijke onderdelen van het COM-B model en hun invloed op cybergedrag. Deze studies zullen hier worden toegelicht.

*Capaciteiten/Kennis*

Het begrip 'capaciteit' doelt in het COM-B model op psychologisch en fysiek vermogen voor gedrag. Op het gebied van cybergedrag, echter, ligt de nadruk op psychologisch vermogen voor veilig cybergedrag en wordt fysiek vermogen grotendeels buiten beschouwing gelaten[17]. Psychologisch vermogen voor veilig cybergedrag is bijvoorbeeld de kennis die personen nodig hebben om zich veilig te gedragen online. In het bijzonder betreft dit kennis over onderwerpen zoals online bedreigingen, informatiebeveiliging in het algemeen en beveiligingsmaatregelen.

Eerdere studies hebben onderzocht in welke mate kennis over IT en cyber security invloed heeft op cybergedrag (Alohali et al., 2018; Arachchilage & Love, 2014; Cain et al., 2018; Downs et al., 2007; Holt & Bossler, 2013; Ovelgönne et al., 2017; Parsons et al., 2014; Shillair et al., 2015). Gaan mensen zich online veiliger gedragen of zichzelf beter beschermen wanneer zij meer IT-gerelateerde kennis hebben? Deze eerdere studies hebben echter geen eenduidige resultaten opgeleverd. Zo toonde een pilot studie onder 161 burgers aan dat kennis, zoals het herkennen van een onbetrouwbare URL, zorgt voor een hogere zelfeffectiviteit en zodoende bijdraagt aan phishing-risico-vermijdend gedrag (Arachchilage & Love, 2014). Ook zouden mensen die goed in staat zijn URL's te evalueren, internet iconen kennen (zoals het slotje in de URL balk) en internet termen begrijpen (zoals de termen phishing en cookie), minder kwetsbaar zijn voor phishing aanvallen (Downs et al., 2007). Daarnaast bestaat er een positieve relatie tussen kennis over informatiebeveiligingsbeleid en -procedures binnen een organisatie en zelf-gerapporteerd veilig cybergedrag van medewerkers (Parsons et al., 2014). Deze relatie werd overigens deels gemedieerd door attitude ten aanzien van het volgen van beleid en procedures. Ook zouden mensen die naar eigen zeggen kundig zijn op het gebied van IT minder vaak onveilig cybergedrag vertonen (Alohali et al., 2018). Hiermee hangt mogelijk samen dat mensen hun kennis op het gebied van internetveiligheid in sommige gevallen overschatten (Debatin et al., 2009).

De studie van Cain et al. (2018), waarin respondenten stellingen over online gevaren en IT concepten beantwoordden, toont echter een ander beeld. Mannen leken iets meer kennis te hebben dan vrouwen, maar gedroegen zich daardoor niet veiliger online. Verrassend genoeg scoorden mensen die zichzelf zagen als expert op IT-gebied lager dan niet-experts op kennis. Deze zogenaamde "experts" bleken

[17] De redenering hierbij is dat wanneer iemand fysiek in staat is internet te gebruiken, hij/zij ook fysiek in staat is zich veilig te gedragen online.

zich vervolgens ook minder veilig te gedragen online (Cain et al., 2018). De onderzoekers vonden geen verschil in cyber kennis of gedrag tussen mensen die eerder getraind waren in IT of cyber security of nooit getraind waren (Cain et al., 2018). De onderzoeksbevindingen van Ovelgönne et al. (2017) lijken deze resultaten te ondersteunen. Zo vonden zij dat software ontwikkelaars vaker risicovol cybergedrag vertonen dan andere respondenten (Ovelgönne et al., 2017). Of dit ook de kans verhoogt dat zij slachtoffer worden van online criminaliteit is onduidelijk. Wel vonden Holt en Bossler (2013) dat het hebben van computervaardigheden (skills) samenhangt met een lagere kans op slachtofferschap van malware.

*Gelegenheid*

Kennis alleen is niet voldoende om tot meer cyber veilig gedrag te leiden. Er is ook gelegenheid nodig. Gelegenheid verwijst naar de *sociale* en *materiële* omgeving die gedrag mogelijk of juist onmogelijk maken.

De sociale omgeving verwijst naar hoe de mensen om ons heen invloed hebben op hoe we ons gedragen. Een voorbeeld hiervan is het belang van steun van onze omgeving bij het volhouden van een dieet (Michie et al., 2011). Uit de (beperkt) beschikbare studies blijkt dat anderen ook van invloed zijn op ons cybergedrag. De privacy instellingen van gebruikers van online sociale netwerken worden bijvoorbeeld beïnvloed door het aantal online vrienden met privé profielen (Lewis, Kaufman, & Christakis, 2008). Ook binnen organisaties heeft sociale invloed een grote impact op veilig cybergedrag (Herath & Rao, 2009). Medewerkers interpreteren het cybergedrag van anderen, zoals directe collega's of leidinggevenden, en de verwachtingen die zij hebben over cybergedrag. Deze interpretatie is vervolgens van grote invloed op de intentie die medewerkers hebben om zich aan de cybersecurity-regels te houden. Het sociale klimaat is dan ook zeer belangrijk voor cyber security in organisaties (Herath & Rao, 2009). Met een andere invalshoek hebben enkele studies onderzocht of de nabijheid van cybercriminelen van invloed is op online slachtofferschap. Mensen met cybercriminelen of cyberdelinquenten in hun persoonlijke netwerk lijken zich minder veilig te gedragen online en vaker slachtoffer te worden van online criminaliteit (Bossler & Holt, 2010; Van Wilsem, 2013b). Tot slot is de sociale omgeving van invloed op de bereidheid van slachtoffers van online criminaliteit om aangifte te doen, bijvoorbeeld via de normen en ervaringen van anderen (Van der Weijer, Leukfeldt, & Bernasco, 2018).

Ook de materiële omgeving kan gelegenheid bieden voor gedrag, bijvoorbeeld door de beschikbaarheid van hulpmiddelen die veilig werken ondersteunen, zoals een laptopslot, maar ook door de beschikbaarheid van financiële middelen, tijd, etc. Vele bedrijven hebben beleidsregels omtrent veilig

cybergedrag en bieden hun medewerkers hulpmiddelen om zich aan deze regels te kunnen houden. Deze hulpmiddelen kunnen helpen in het versterken van zelfvertrouwen in het vertonen van gewenst gedrag (*zelfeffectiviteit*) onder medewerkers binnen organisaties (Herath & Rao, 2009). Wanneer er middelen beschikbaar zijn in een organisatie, zoals voorschriften over hoe om te gaan met cyberincidenten of de beschikbaarheid van hulp, hebben medewerkers meer vertrouwen in hun eigen kunnen (zie ook: Siponen, 2000; Saks & Belcourt, 2006). Tot op heden is de rol die de materiële omgeving speelt in cybergedrag buiten bedrijven echter beperkt het onderwerp van onderzoek geweest. Het is dan ook de vraag hoe de materiële omgeving cybergedrag beïnvloedt in de privé setting. De hulpmiddelen zijn in deze setting op een andere manier beschikbaar dan in bedrijven; burgers moeten actief middelen aanschaffen, implementeren en up-to-date houden. De financiële gelegenheid is daarmee een relevante omstandigheid (Cohen, Rust, Steen, & Tidd, 2004). Mensen die weten dat ze persoonlijke foto's beter niet kunnen versturen met gratis transfer-websites (kennis) en gemotiveerd zijn om een veiligere –betaalde – optie te gebruiken (motivatie), moeten ook financiële ruimte hebben om dit te doen (gelegenheid).

*Motivatie*

Het COM-B model veronderstelt dat er naast kennis en gelegenheid ook motivatie voor veilig gedrag aanwezig moet zijn. De component motivatie uit het COM-B model heeft grote overlap met de factoren uit PMT (besproken in paragraaf 3.1). Uit de literatuur komt een additionele factor naar voren, die geen onderdeel uitmaakt van PMT maar die relevant lijkt te zijn voor de motivatie die mensen hebben voor veilig cybergedrag. Het betreft de "locus of control", een term die verwijst naar de mate waarin iemand zich verantwoordelijk voelt voor het voorkomen van een succesvolle aanval[18]. Het betreft het verantwoordelijkheidsgevoel dat mensen hebben op het gebied van hun eigen veiligheid op internet. Of iemand zichzelf verantwoordelijk vindt (ook wel interne locus of control genoemd) of die verantwoordelijkheid legt bij anderen, zoals de politie of de bank (ook wel externe locus of control genoemd), heeft mogelijk effect op de acties die deze persoon neemt om slachtofferschap te voorkomen, oftewel op de manier waarop hij/zij zich online gedraagt (Debatin et al., 2009; Jansen, 2018; Rotter, 1966; Workman et al., 2008). Verwacht wordt dat iemand met een hoge locus of control de verantwoordelijkheid bij zichzelf (intern) legt en gemotiveerd is om zijn/haar online veiligheid in eigen handen te nemen. Eerdere onderzoeken vonden inderdaad een positief significant verband tussen locus

[18] Locus of control heeft raakvlakken met de PMT factor zelfeffectiviteit, maar terwijl zelfeffectiviteit draait om het vermogen om veilig te handelen wijst locus op control op de mate van verantwoordelijkheid die mensen daarbij voelen. Samen kunnen zij gezien worden als iemands gepercipieerde gedragscontrole (Jansen, 2018).

of control en veilig cybergedrag (Boehmer et al., 2015; Jansen, 2018; Workman et al., 2008). Het is echter ook mogelijk dat een groot verantwoordelijkheidsgevoel in enige mate een onterecht veiligheidsgevoel oplevert. Namelijk, wanneer mensen zichzelf verantwoordelijk en capabel achten om zichzelf te beschermen tegen internetcriminelen, schatten zij mogelijk online risico's lager in (Rhee et al., 2009), wat kan resulteren in onveilig cybergedrag.

Ook de mate waarin mensen bang zijn om slachtoffer te worden van online criminaliteit kan van invloed zijn op hun motivatie voor veilig cybergedrag. Veel van het menselijk gedrag wordt bepaald door continue (bewuste en onbewuste) evaluaties van risico's, voor onszelf en anderen. Mensen passen hun gedrag aan op basis van de mate van risico die zij bereid zijn om te nemen (Workman et al., 2008). De manier waarop mensen risico's inschatten is per individu verschillend (Johnson & Tversky, 1983; Slovic, 1987). Risicoperceptie is daarmee een subjectieve maat van een objectief risico; een risico dat voor iedereen hetzelfde is (de kans dat jouw vliegtuig neerstort) kan door de ene persoon laag ingeschat worden, terwijl een ander dit een hoog risico acht (met vliegangst als gevolg) (Garland, 2003). Risicoperceptie speelt een fundamentele rol bij preventief gedrag (Boss, Galletta, Lowry, Moody, & Polak, 2015; Huang, Patrick Rau, Salvendy, Gao, & Zhou, 2011) en heeft dan ook mogelijk een grote invloed op cybergedrag. Hierbij staan de potentiële kosten van slachtofferschap van internetcriminaliteit centraal. Terwijl een te hoge inschatting van de risico's van internetgebruik kunnen leiden tot onwenselijke gevolgen, zoals vermijdingsgedrag, leidt een onderschatting van online risico's mogelijk tot onveilig gedrag (Jansen, 2018). Er is echter beperkt onderzoek gedaan naar de perceptie van online risico's (Boss et al., 2015; Jansen, 2018). Eerder onderzoek naar risicoperceptie onder mensen die online bankieren vond dat 17 procent van de 1200 respondenten in enige of sterke mate bang was om slachtoffer te worden van online bankfraude en dat 22 procent bang was dat anderen toegang zouden kunnen krijgen tot hun bankrekening (Jansen, 2018). In een andere studie gaven Amerikaanse studenten het meest bang te zijn voor online identiteitsdiefstal, keylogging[19], online pesten en social engineering[20] (Van Schaik et al., 2017). Het is tot op heden echter zover bekend niet onderzocht of de angst voor slachtofferschap[21] invloed heeft op het cybergedrag van internetgebruikers. Recent onderzoek richtte zich op de gevolgen van angst op

[19] Hardware of software waarmee de toetsaanslagen van een computergebruiken gelogd kunnen worden (Van Schaik et al., 2017). Op deze manier zijn bijvoorbeeld gebruikersnaam en wachtwoord te achterhalen.

[20] Het manipuleren van mensen om zo informatie los te krijgen die ze eigenlijk niet moeten geven. Zie Mitnick (Mitnick & Simon, 2011) voor een uitgebreide beschrijving van social engineering in de praktijk.

[21] Angst voor slachtofferschap heeft raakvlakken met de PMT factor gepercipieerde kwetsbaarheid. Terwijl die laatste factor draait om een inschatting van de eigen kwetsbaarheid om motivatie voor veilig cybergedrag te voorspellen, draait het bij angst voor slachtofferschap om een inschatting van de impact van een potentieel incident, dat direct effect zou kunnen hebben op gedrag.

motivatie voor het nemen van beschermende maatregelen. Zo zou angst voor slachtofferschap geen effect hebben op de intentie van computergebruikers om hun bestanden te back-uppen, maar vergroot het mogelijk wel de intentie om anti-malware software te gebruiken (Boss et al., 2015). Er is dan ook onderzoek nodig om de vraag te beantwoorden in hoeverre de angst voor slachtofferschap invloed heeft op cybergedrag.

### *3.4.3. Andere verklaringen voor veilig cybergedrag*

In de voorgaande paragrafen is uiteengezet welke factoren mogelijk relevant zijn voor veilig cybergedrag op basis van de verklaringsmodellen PMT en COM-B. Uit het literatuuronderzoek zijn daarnaast nog andere factoren naar voren gekomen die relevant kunnen zijn voor het huidige onderzoek; gemoedstoestand, vatbaarheid voor verleidingstechnieken, het type apparaat dat wordt gebruikt en tijdsdruk.

#### *Gemoedstoestand*

Het is aannemelijk dat de besluitvorming kan worden beïnvloed door de gemoedstoestand van een persoon. Gemoedstoestand is een emotionele toestand die tenminste enige minuten aanhoudt (Matthews et al., 1990). Voorbeelden zijn plezier en angst. Het is al goed gebruik onder artsen om hun patiënten te adviseren om geen belangrijke beslissingen te maken tijdens episodes van depressie (bijvoorbeeld Yuen et al., 2003). De onderbouwing voor deze praktijk kan worden gevonden in diverse onderzoeken. Eerder onderzoek laat bijvoorbeeld zien dat de gemoedstoestand een effect heeft op de werking van het geheugen (Matthews et al., 1995; Natale & Hantas, 1982; Pyszczynski et al., 1989; Teasdale, 1993). Matthews et al (1995) vonden dat informatie die past bij de gemoedstoestand sneller wordt gevonden in het geheugen. Een negatieve gemoedstoestand kan ertoe leiden dat mensen minder risico's nemen, omdat zij makkelijker toegang hebben tot negatieve gedachten over de uitkomst van het risicovolle gedrag.

Ook heeft de gemoedstoestand een effect op de strategieën die we kiezen bij het nemen van beslissingen (Yuen et al., 2003). Het *Elaboration Likelihood Model* (ELM) van Petty en Cacioppo (1986) veronderstelt dat er twee routes zijn voor het verwerken van informatie: een centrale route en een perifere route. De centrale route representeert een diepe en rationele verwerking van informatie, terwijl de perifere route een meer heuristische verwerking van informatie representeert. De gemoedstoestand van een individu beïnvloedt de route van informatieverwerking. Individuen in een positieve

gemoedstoestand kiezen sneller voor de perifere route terwijl mensen die in een negatieve toestand verkeren sneller kiezen voor een centrale route van informatieverwerking (Tellis, 1998).

Yuen et al. (2003) stellen dat deze aspecten bovendien een belangrijke rol spelen bij het inschatten van risico's. Onderzoek laat zien dat een positieve gemoedstoestand ertoe leidt dat mensen meer risico's nemen. Isen (2001) en Nygren et al. (1996) lieten zien dat mensen met een positieve gemoedstoestand beter toegang hebben tot gedachten in het geheugen over de positieve uitkomsten en aspecten van de risicovolle situatie dan mensen in een neutrale gemoedstoestand. Mensen zien de uitkomsten van risicovolle situaties dan ook sneller als meer positief en zijn dan ook meer bereid om risico's te nemen. Mensen in een negatieve toestand, die bijvoorbeeld depressief zijn, zijn meer conservatief en in mindere mate bereid om risico's te nemen. In een negatieve gemoedstoestand wordt de wereld al snel als een bedreigende plek gezien en wordt informatie zorgvuldig gewogen om potentieel verlies tegen te gaan (Jorgensen, 1998).

Omdat gemoedstoestand een rol speelt bij risicovol gedrag, is het aannemelijk dat gemoedstoestand ook een rol speelt bij onveilig cybergedrag. Wanneer iemand zich slecht voelt, zoals nerveus of overstuur, is hij/zij minder alert bij het doen van online betalingen of het klikken op een hyperlink in een (achteraf) verdachte e-mail. Anderzijds zijn mensen die zich goed voelen, zoals enthousiast of uitgelaten, mogelijk eerder bereid persoonlijke gegevens te delen. Ook haast hebben of het doormaken van bepaalde levensgebeurtenissen, zoals een geboorte of sterfgeval, kunnen zorgen dat iemand sneller in de val van een cybercrimineel valt (Jansen, 2018). Zover bekend zijn er echter geen andere studies die een eventueel verband tussen gemoedstoestand en cybergedrag hebben onderzocht.

*Type apparaat*

Apparaten die mensen thuis gebruiken voor online activiteiten, zoals een smartphone, tablet, laptop of pc, verschillen op een aantal dimensies. De belangrijkste dimensies met het oog op online veiligheid zijn de mate van mobiliteit, de schermgrootte, de beschikbaarheid (of juist afwezigheid) van randapparatuur zoals een toetsenbord of muis en het besturingssysteem. Al deze aspecten kunnen van invloed zijn op slachtofferschap.

*Mate van mobiliteit*. Vishwanath (2016) heeft laten zien dat mobiele gebruikers vaker slachtoffer worden van phishing dan gebruikers van een pc. Door hun draagbaarheid, gebruiksgemak en beschikbaarheid, zijn gebruikers van mobiele apparaten meer cognitief ontspannen, wat leidt tot meer gewoontegedrag (automatisch gedrag, zoals het klikken op hyperlinks) en daarmee tot verhoogde kans op slachtofferschap (Vishwanath, 2016). Ook de manier waarop deze apparaten worden gebruikt kan de

kans op slachtofferschap verhogen. Mobiele apparaten worden veelvuldig naast andere activiteiten gebruikt. Hierdoor is de hoeveelheid beschikbare cognitieve hulpbronnen voor het verwerken van informatie op het mobiele apparaat beperkt. De hulpbronnen moeten als het ware worden verdeeld tussen de verschillende taken die aandacht vereisen. Voor het uitvoeren van taken op het apparaat, zoals het beantwoorden van e-mails, zijn dan ook relatief minder mentale hulpbronnen beschikbaar. De gebruiker zal dan eerder geneigd zijn tot het aanwenden van heuristieken voor het uitvoeren van taken (Vishwanath, 2016). Heuristieken zijn vuistregels voor het verwerken van informatie die het ons mogelijk maken snel en gemakkelijk, maar soms ook foutief een situatie te beoordelen.

*Schermgrootte*. Kim en Sundar (2016) en Chae en Kim (2004) hebben gekeken naar het effect van schermgrootte van smartphones op de verwerken van informatie en de uitvoeren van taken. Het onderzoek van Kim en Sundar (2016) laat zien dat de schermgrootte de manier van informatieverwerking beïnvloedt. Grotere schermen bevorderen heuristische informatieverwerking, terwijl kleinere schermen juist een meer systematische gecontroleerde verwerking van informatie stimuleren. Dit kan betekenen dat schermgrootte positief is gerelateerd aan slachtofferschap bij smartphone gebruikers: hoe groter het scherm, hoe groter de kans om slachtoffer te worden van online criminaliteit.

*Randapparatuur*. Wells et al. (2013) onderzochten de effecten van het type apparaat op het invullen van online enquêtes. Er werd alleen een verschil gevonden tussen gebruikers van een pc en mobiele gebruikers bij het invullen van open vragen. Gebruikers van een pc gaven over het algemeen langere antwoorden. Een mogelijke verklaring van Wells et al (2013) is dat het ontbreken van een fysiek toetsenbord bij mobiele gebruikers hen heeft genoopt tot het geven van korte antwoorden.
Wetenschappelijke literatuur over de effecten van randapparatuur op online veiligheid is ons niet bekend. Voor de online veiligheid kan het echter handig zijn om een muis te hebben. Door met de muisaanwijzer boven een hyperlink te gaan staan op een website of in de adresbalk van een e-mail kan meer informatie worden verkregen over het adres waar de hyperlink naar verwijst. Dit kan helpen om te bepalen of er sprake is van een veilige website of een veilig domein. Ook bij mobiele apparaten met touchscreen is deze functionaliteit beschikbaar, door het adres gedurende enkele seconden aan te raken met een stilus of met de vinger, totdat een venster verschijnt met het webadres, maar dit is onder gebruikers minder bekend. Het is daarmee denkbaar dat apparaten die een muis nodig hebben voor bediening, zoals een pc of laptop, de kans op slachtofferschap verlagen, maar waarschijnlijk alleen als er kennis is bij de gebruiker over het herkennen van onveilige webadressen, zoals bij nepwebwinkels.

*Besturingssysteem*. Apparaten verschillen in de meegeleverde software, zoals het besturingssysteem en internetbrowsers die standaard worden meegeleverd, of in de mogelijkheden tot

beveiliging van online activiteiten via de beveiligingsinstellingen. Mobiele besturingssystemen zijn minder gevoelig voor virussen en malware dan bijvoorbeeld het Windows besturingssysteem zoals dat draait op een pc of laptop. Wat veiligheid van mobiele apparaten betreft is IOS beter dan Android (Braam, 2018). Het is niet zo dat er met een iPhone nooit iets mis kan gaan, maar over het algemeen is de software wel wat meer afgesloten voor externe beïnvloeding. Wat ook niet meehelpt is dat veel malware juist is gericht op Android toestellen[22]. Een ander risico op slachtofferschap bestaat uit tekstberichten. Wanneer cybercriminelen "phishen", sturen ze frauduleuze e-mails die gericht zijn om de ontvanger zo ver te krijgen een bijlage met malware te openen of te klikken op een schadelijke koppeling. Smishing gebruikt een tekstbericht in plaats van e-mail en is platformonafhankelijk. Het is niet ondenkbaar dat iPhone- en iPad-gebruikers relatief vaker slachtoffer worden van dit type aanvallen, omdat ze vaak het gevoel hebben immuun te zijn voor aanvallen[23].

Uit onderzoek naar internetbrowsers blijkt dat de Opera browser het beste scoort op veiligheid. Opera beschermt gebruikers het beste tegen kwaadaardige phishing websites (Van Zwet, 2018). Gemiddeld herkennen de browsers op de computer 87 procent van deze phishing websites. De browser geeft dan aan dat deze website gevaarlijk is. Uit het onderzoek blijkt dat Opera veel meer sites tegenhield (96% in Windows, 97% op een Mac). Microsoft Edge scoorde ver onder de maat en hield slechts 65 procent van de kwaadaardige sites tegen. Browsers hebben instellingen die de veiligheid en privacy van gebruikers kunnen beschermen, maar standaard doen ze dit vaak niet.

*Tijdsdruk*

Tijdsdruk hindert de flexibiliteit van besluitvorming door een beperking van het vermogen om alternatieve hypotheses te testen en te genereren (Macquet, 2009). De verhoogde cognitieve belasting die het gevolg is van tijdsdruk, lijkt vooral geheugenprocessen te hinderen. Dit kan verklaren waarom het vermogen om alternatieve hypotheses te genereren wordt beperkt (Dougherty & Hunter, 2003). Een veelgebruikte strategie die mensen hanteren in het omgaan met tijdsdruk is het gebruiken van meer oppervlakkige (heuristische) informatieverwerking (Alison et al., 2013). Dit kan betekenen dat belangrijke informatie over het hoofd wordt gezien. Ask en Granhag (2005) vonden hiervoor bewijs. Onder tijdsdruk blijken mensen vooral te zoeken naar bewijs dat een initiële hypothese ondersteunt en negeren zij bewijs dat hun hypothese zou kunnen weerleggen. Wanneer burgers geconfronteerd worden met tijdsdruk zou het dus kunnen dat zij overgaan op meer heuristische informatieverwerking en belangrijke cues die kunnen

[22] Zie ook: https://www.kaspersky.nl/resource-center/threats/what-is-smishing-and-how-to-defend-against-it
[23] https://www.kaspersky.nl/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

duiden op risico's die zijn verbonden aan het handelen, zoals het klikken op een hyperlink, over het hoofd zien. Eerder onderzoek heeft echter nog niet aangetoond wat de gevolgen van handelen onder tijdsdruk zijn voor cybergedrag.

*Verleidingstechnieken*

Cybercriminelen maken voor veel van hun aanvallen gebruik van "social engineering", waarbij zij niet de beveiligingstechniek maar de gebruiker proberen te misleiden. Criminelen nemen een vertrouwenwekkende rol aan en gebruiken invloed en overreding om waardevolle informatie te verkrijgen van hun slachtoffers (Mitnick & Simon, 2011; Mouton, Leenen, Malan, & Venter, 2014). Bij social engineering maken cybercriminelen gebruik van verleidingstechnieken; technieken uit de economische psychologie om hun slachtoffers te verleiden tot bepaald gedrag, zoals het klikken op een link in een phishing e-mail. In de literatuur worden verschillende taxonomieën onderscheiden, zoals Gragg's psychologische triggers (2003) en Stajano et al. principes of scams (2011). Een veel gebruikte taxonomie van verleidtechnieken zijn de zes verleidingsprincipes van Cialdini (1987) (zie ook Guadagno, & Cialdini, 2005; Ferreira, Coventry & Lenzini, 2015). Deze principes zijn wederkerigheid, sociale bewijskracht, consistentie, sympathie, autoriteit en schaarste. Oorspronkelijk komen deze principes uit de marketing om te beschrijven hoe potentiële kopers overgehaald kunnen worden om producten te kopen die ze misschien helemaal niet nodig hebben (Ferreira et al., 2015). Ferreira et al. hebben onderzocht op welke manieren cybercriminelen deze principes gebruiken in phishing-aanvallen. Criminelen proberen bijvoorbeeld sympathie op te wekken door op een familiaire toon te schrijven, of proberen lezers door middel van autoritaire principes, zoals het tonen van keurmerken of door gebruik te maken van betrouwbare merknamen, over te halen om irrationeel te handelen. Twee verleidingstechnieken die in het bijzonder door cybercriminelen kunnen worden gebruikt zijn autoriteit en wederkerigheid.

Het principe van autoriteit is dat mensen zich graag laten overtuigen door experts (Cialdini, 2007). Mensen doen dan ook graag aankopen bij een partij die in hun ogen geloofwaardig is en kwaliteit levert, zoals bijvoorbeeld vastgesteld door keurmerken of onderzoeksresultaten. Een voorbeeld van een toepassing van het principe van autoriteit, is de expert in een witte jas die wordt getoond in een tv-reclame en vertelt over een bepaald product. Ook gebruikmaking van de naam van bedrijven of instanties met een goede reputatie of gezag vallen onder dit principe.

Het principe van wederkerigheid draait om de onderlinge verplichting binnen een relatie tussen personen om een gift te beantwoorden met een tegengift (zie ook Gouldner, 1960). Volgens Gouldner

(1960) bestaat er zoiets als een wederkerigheidsnorm. De wederkerigheidsnorm houdt in dat mensen diegenen helpen die ook hen geholpen hebben, en dat zij niet iemand schaden die hen geholpen heeft. Een bekend voorbeeld van wederkerigheid als verleidingsprincipe is het pepermuntexperiment, zoals beschreven door Cialdini (2007). Door restaurantgasten na het eten pepermuntjes te geven bij de rekening steeg de fooi met drie procent tot 14 procent.

Kaptein et al. (2009) hebben, tot slot, laten zien dat mensen verschillen in hun gepercipieerde vatbaarheid voor de verschillende verleidingtechnieken. Dit betekent dat de effectiviteit van verleidingstechnieken mogelijk afhankelijk is van het potentiële slachtoffer. Mensen die gevoelig zijn voor autoriteit zijn in hogere mate vatbaar voor verleidtechnieken die hierop inspelen dan mensen die in mindere mate hiervoor vatbaar zijn.

### *3.5. Gedragsinterventies*

Er zijn veel verschillende manieren om gedrag te beïnvloeden (zie, voor een overzicht, Briggs et al., 2017; Michie et al., 2011; Kok et al., 2015; BIN NL, 2017). Michie et al. (2011) beschrijven op basis van een uitgebreide literatuurstudie een raamwerk van negen gedragsinterventie-functies en zeven beleidsmaatregelen die deze interventies kunnen ondersteunen. Dit raamwerk is het Behaviour Change Wheel (BCW) (figuur 2). De kern van het BCW wordt gevormd door het eerder beschreven gedragsmodel COM-B. Het BCW sluit daarmee aan bij de in dit onderzoek gekozen aanpak om cybergedrag van burgers in kaart te brengen. Het raamwerk onderscheidt zich van andere raamwerken in dat het ook automatisch of gewoontegedrag omvat, in tegenstelling tot veel andere modellen van gedrag, die vooral reflectieve en cognitieve processen beschouwen (zoals de theorie van gepland gedrag).

Het wiel vormt de basis voor het maken van een keuze voor geschikte interventies. In de kern van het wiel (het groene deel van het figuur) staan de COM-factoren kennis, gelegenheid en motivatie. In de omliggende (rode) ring liggen negen gedragsinterventie-functies. Dit zijn acties om gedrag te veranderen. De negen interventiefuncties zijn (zie, voor meer informatie, Michie et al., 2011): educatie, overtuigen, aanmoedigen, dwang, training, beperking, herstructurering van de omgeving, modelling en in staat stellen (zie ook tabel 2).

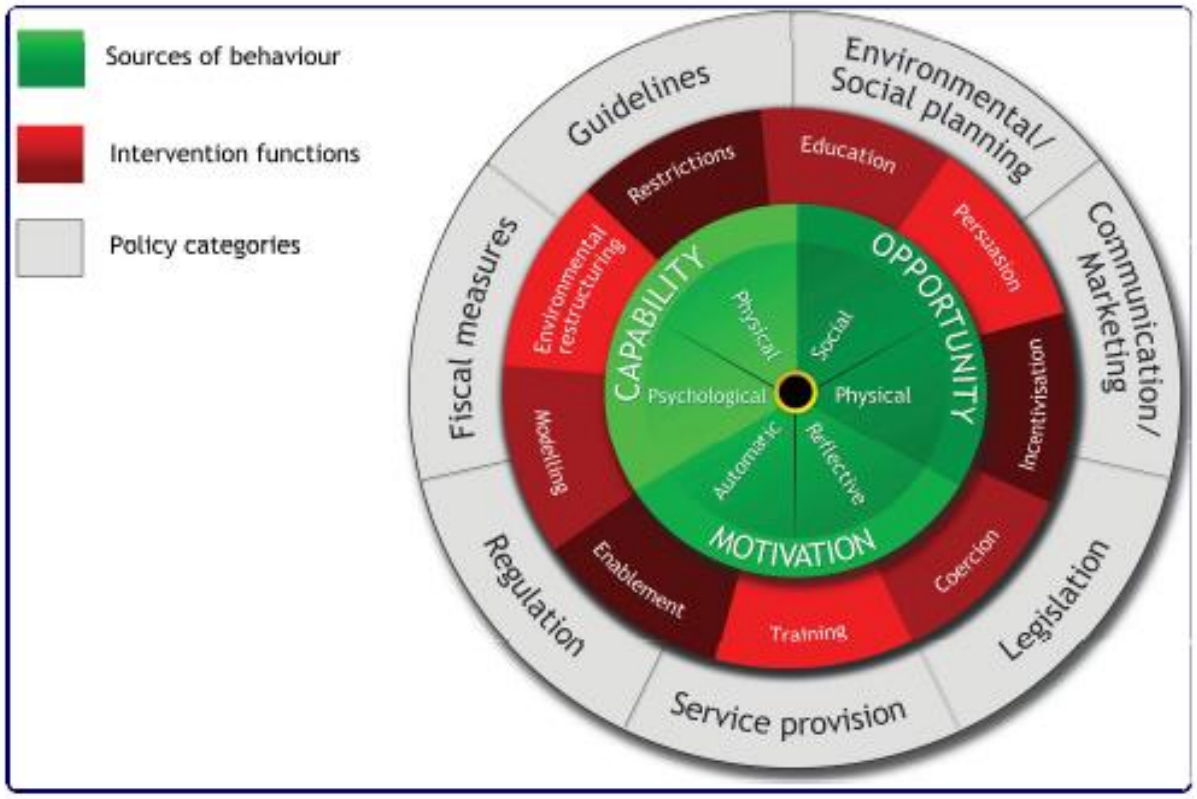
De negen interventiefuncties zijn door Michie en collega's gekoppeld aan specifieke COM-factoren. De effectiviteit van de interventies is dus afhankelijk van welke COM-factoren doel zijn van de beoogde interventie. Zo is training effectief gebleken als het doel is om kennis te vergroten. Training blijkt echter niet geschikt om motivatie te verhogen. Zo zijn er combinaties te maken van COM-factoren en interventiefuncties.

*Tabel 2. Interventiefuncties en definities (vertaald uit Michie et al., 2011)*

| **Interventiefunctie** | **Definitie** |
|---|---|
| Educatie | Het doen laten toenemen van kennis en begrip |
| Overtuigen | Het gebruik van communicatie om positieve of negatieve gevoelens op te wekken of aan te zetten tot actie |
| Aanmoedigen | Het creëren van verwachtingen van beloning |
| Dwang | Het creëren van verwachtingen van straf of kosten |
| Training | Bijbrengen van vaardigheden |
| Beperking | Gebruik van regels om te gelegenheid te beperken tot het vertonen van ongewenst gedrag |
| Herstructurering | Het veranderen van de fysieke of sociale context |
| Modelling | Mensen een voorbeeld bieden om na te streven of om na te doen |
| In staat stellen | Mogelijkheden vergroten of barrières wegnemen om daarmee de gelegenheid voor gewenst gedrag te vergroten |

Voor een toepassing in de praktijk van interventiefuncties zijn meer specifieke gedragsinterventie-technieken nodig, ook wel *behavioural change techniques* (BCT's) genoemd (zie bv. Michie et al., 2009; Michie et al., 2010). Een BCT is dus een concrete uitwerkingen van een interventiefunctie. Michie et al. (2011) stellen dat elke interventiefunctie meerdere specifieke BCT's omvat om gedrag te beïnvloeden. Bijvoorbeeld de interventiefunctie educatie: deze omvat een gamma aan specifieke maatregelen. Een specifieke e-learning module om het kennisniveau op het gebied van risico's bij burgers te vergroten is een voorbeeld van een BCT binnen de functie educatie. Betrouwbare taxonomieën van de specifieke BCT's dienen echter nog te worden ontwikkeld (zie voor een eerste aanzet, Michie et al., 2010). Het gaat dan ook te ver voor deze studie om een overzicht te geven van relevante BCT's.

In de 2$^{e}$ omliggende ring (grijs) van het BCW (zie ook figuur 2) zijn zeven beleidsmaatregelen weergegeven. Het raamwerk onderscheidt de volgende beleidsmaatregelen (zie, voor meer informatie, Michie et al., 2011): communicatie/marketing, richtlijnen, fiscale maatregelen, regulatie, wetgeving, (her)ontwerpen van de sociale of materiële omgeving en dienstverlening (zie ook tabel 3).




*Figuur 2. Het BCW. Het COM-B model staat centraal. Daaromheen 9 interventie-functies en 7 beleidscategorieën.*

*Tabel 3. Beleidsmaatregelen en definities (vertaald uit Michie et al., 2011).*

| **Beleidsmaatregel** | **Definitie** |
|---|---|
| Communicatie/marketing | Het gebruik van media, print, telefoon, etc. |
| Richtlijnen | Het maken van documenten die voorschrijven of aanbevelingen doen voor goed praktijkgebruik |
| Fiscale maatregelen | Via het belastingsysteem verminderen of vermeerderen van financiële kosten |
| Regulatie | Het vaststellen van regels of principes die gedrag in de praktijk voorschrijven |
| Wetgeving | Het maken of veranderen van wetten |
| (her)ontwerpen van de sociale of materiële omgeving | Het ontwerpen of controleren van de fysieke of sociale omgeving |
| Dienstverlening | Het bieden van diensten |

Beleidsmaatregelen kunnen als een soort van hefboom worden ingezet om de effectiviteit van BCT's te vergroten. Zo kan wetgeving worden ingezet door de overheid om de effectiviteit van interventies die moeten helpen om gebruikers in staat te stellen zich veilig te gedragen, te vergroten. Een voorbeeld is wetgeving die fabrikanten verplicht om veiligheidsmaatregelen (zoals een vingerafdrukscanner) onderdeel van het design van digitale apparatuur te maken. Dit kan burgers meer gelegenheid bieden om zich veilig te gedragen. Hieronder volgen voor elk van de drie COM-factoren voorbeelden van BCT's.

Om *capaciteiten* te maximaliseren om het eigen gedrag beter te reguleren kan worden gedacht aan het ontwikkelen van relevante vaardigheden of kennis. Downs, Holbrook, & Cranor (2007 ) concluderen op basis van onderzoek dat gebrek aan kennis over veiligheid op internet, zoals het onvermogen om onveilige webadressen te kunnen onderscheiden van veilige webadressen, bijdraagt aan slachtofferschap van cybercriminaliteit. Downs et al. (2007) deduceren dat gedragsinterventies gericht moeten zijn op het vergroten van kennis bij gebruikers over internet. Ook Bullée, Montoya, Junger, & Hartel (2016) laten zien dat educatie in combinatie met de beleidsfunctie communicatie/marketing gericht op het vergroten van kennis bij de doelgroep over cybercriminaliteit effectief kan zijn, in dit specifieke geval om social engineering door cybercriminelen via de telefoon tegen te gaan. Een aanval die volgt binnen een week na een informatiecampagne, wordt effectief afgeslagen door het merendeel van de medewerkers die deelnamen aan de voorafgaande campagne. Er is een belangrijke kanttekening. Als de aanval niet na één week volgt, maar na twee weken of langer, dan is het effect verdwenen in vergelijking met een controlegroep die geen campagne hadden ontvangen. Het effect van interventies op het gebied van educatie is mogelijk dus beperkt in de tijd.

Voorbeelden van het ontwikkelen van *gelegenheid* om zelfregulatie van gedrag te stimuleren zijn het bieden van sociale ondersteuning of het aanpassen van de werkomgeving (Abraham, Kelly, West & Michie, 2009). Een voorbeeld van hoe een aanpassing van de werkomgeving veilig gedrag kan stimuleren, kan worden gevonden in het werk van Münscher, Vetter en Scheuerle (2016). Zij onderzochten hoe het ontwerp van veiligheidsmaatregelen gebruikers kan verleiden tot het maken van veilige gedragskeuzes. Hiertoe hebben Münscher et al. (2016) een taxonomie ontwikkeld die bestaat uit drie basiscategorieën: Informatie, structuur en ondersteuning. De eerste categorie, informatie, omvat technieken die zich richten op de presentatie van beslisrelevante informatie, zonder de keuzemogelijkheden zelf te veranderen, bijvoorbeeld door het opnieuw indelen van relevante informatie. De tweede categorie, structuur, richt zich op de beschikbaarheid van opties en het beslisformat, bijvoorbeeld door het aanpassen van de beschikbare keuzeopties afhankelijk van de specifieke context. De derde categorie, ondersteuning, richt zich op het bieden van hulp bij de realisatie van gedragsintenties, bijvoorbeeld door

het bieden van herinneringen. De taxonomie omvat in totaal negen technieken die ingezet kunnen worden om via het ontwerp van veiligheidsmaatregelen gebruikers te beïnvloeden in het nemen van veilige beslissingen. Een voorbeeld van een techniek binnen de categorie informatie is het bieden van een sociaal referentiepunt. Ook deze techniek valt weer uiteen in verschillende deeltechnieken, zoals het geven van een descriptieve norm, ofwel wat anderen in een vergelijkbare situatie daadwerkelijk doen (zie bv. Goldstein, Cialdini, & Griskevicius, 2008).

Om de *motivatie* te versterken om mensen het gewenst gedrag te laten vertonen, kan worden gedacht aan het belonen, aanmoedigen of afdwingen van het beoogde doelgedrag via communicatie of marketing. Een voorbeeld: Harrington (2006) onderzocht het effect van de toon van beveiligingsberichten op de motivatie van mensen om zichzelf te beschermen tegen criminaliteit. Er werden berichten gebruikt die negatief van toon zijn en berichten die meer positief van toon zijn. De positieve berichten benadrukken de voordelen van het nemen van beschermende maatregelen, zoals stabiliteit en betrouwbaarheid. De negatieve berichten benadrukken de gevolgen van het niet nemen van beschermende maatregelen, zoals financiële schade. De resultaten laten zien dat vooral de berichten die positief van toon waren, meer succesvol zijn in het beïnvloeden van intentie tot het nemen van beschermende maatregelen.

### *3.6. Resumé*

Het doel van deze literatuurstudie was om uiteen te zetten hoe cybergedrag in eerdere studies is onderzocht en gemeten en welke verklaringen voor het vertonen van onveilig of veilig cybergedrag gevonden zijn. Uit de literatuurstudie blijkt:

- 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 meegenomen worden in de huidige studie, in het bijzonder: leeftijd, sociaaleconomische status, geslacht en gezinssamenstelling.
- Dat onderzoek zich zou moeten richten op *gedrag* als pijler voor risico op slachtofferschap, namelijk veilig cybergedrag. Dit wordt dan ook het onderwerp (en afhankelijke variabele) van de huidige studie.
- Dat cybergedrag gemeten kan worden door middel van zelfrapportage, objectieve metingen of een combinatie van beiden, waarin het gemak van zelfrapportage wordt gecombineerd met de betrouwbaarheid van objectieve metingen in een vragenlijstonderzoek.

- Dat de mate waarin mensen zich online veilig gedragen op basis van theoretische verklaringsmodellen (PMT en COM-B) 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. Deze studie zal dan ook onderzoeken in hoeverre cybergedrag verklaard kan worden door capaciteit, gelegenheid, motivatie, zelfcontrole en eerder slachtofferschap.
- Dat er vijf factoren zijn 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 tekenen (cues) dat zij risico lopen, negeren en zodoende meer risico's nemen. Ook de verleidingstechnieken die cybercriminelen gebruiken bij hun aanvallen lijken belangrijk. De huidige studie zal dan ook onderzoeken in hoeverre cybergedrag verklaard kan worden door gemoedstoestand, angst voor slachtofferschap, type apparaat, tijdsdruk en verleidingstechnieken.

# 4. Naar een meetinstrument om cybergedrag te meten

### *4.1. Population based survey experiment*

De huidige studie maakt gebruik van een "population based survey experiment" (experimentele survey) (Mutz, 2011). In de praktijk bestaat een dergelijke experimentele survey veelal uit een online vragenlijst waarin experimenten zijn ingebouwd. Middels deze experimenten kunnen respondenten worden gemanipuleerd (zoals het opleggen van tijdsdruk). Bovendien kunnen objectieve metingen worden gedaan tijdens de survey. Deze methode combineert de voordelen van vragenlijst onderzoek, zoals de mogelijkheid om een grote representatieve sample te bestuderen, met de voordelen van experimenteel onderzoek, waarin daadwerkelijk gedrag gemeten kan worden en causale verbanden kunnen worden vastgesteld (Mullinix, Leeper, Druckman, & Freese, 2015).

### *4.2. Opzet experimentele survey*

De experimentele survey van de huidige studie bestond uit een vragenlijst met daarin vignetten en objectieve metingen. Een deel van de experimentele survey was bovendien experimenteel van aard. Om bijvoorbeeld naar het effect van tijdsdruk op gedrag te onderzoeken, is ervaren tijdsdruk gemanipuleerd. Hiertoe worden respondenten verdeeld over een controlegroep en een experimentele groep.

In deze vragenlijst werd cybergedrag op twee manieren gemeten: 1) door zelfrapportage, 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 geïnteresseerd waren in hoe de respondenten met deze situaties zouden omgaan. Dit vormde de objectieve metingen van cybergedrag. Samengenomen bestond de studie uit de volgende componenten die gedrag beogen te meten:

- een vragenlijst over zelf-gerapporteerd cybergedrag
- vignetten over zorgvuldig omgaan met e-mails die hyperlinks bevatten (één legitiem en twee vals)
- 3 metingen van daadwerkelijk cybergedrag

Tabel 4 geeft een overzicht van manieren waarop cybergedrag gemeten is in de survey. De keuze om bepaalde gedragingen te onderzoeken met behulp van vignetten en andere gedragingen met behulp van een objectieve meting is weloverwogen gemaakt. Nadat de zeven centrale gedragsclusters zijn

geïdentificeerd (paragraaf 3.3), is voor elk van deze gedragingen nagedacht op welke wijze kan worden bepaald in welke mate respondenten dit gedrag vertonen in hun thuissituatie. Het is om een aantal redenen onmogelijk gebleken om elk gedrag op een objectieve manier te meten. Ten eerste is het nabootsen van online criminaliteit niet altijd mogelijk of moreel verantwoord, bijvoorbeeld in het geval van oplichting via een webwinkel. Ook is het in sommige gevallen technisch of onhaalbaar gebleken om een meting op een goede manier in te bouwen in de vragenlijst. Er is dan ook gekozen voor een pragmatische aanpak en alleen het gedrag op objectieve wijze in kaart te brengen als dat op praktisch haalbare en moreel verantwoorde wijze mogelijk zou zijn. Voor de overige gedragingen is gekozen om deze alleen in kaart te brengen via zelfrapportage.

Zelfrapportage heeft plaatsgevonden voor alle gedragingen, ook de gedragingen die objectief of met vignetten worden gemeten. Er is hierbij voortgeborduurd op bestaande vragenlijsten die, indien nodig, zijn vertaald naar het Nederlands en aangepast aan de specifieke context van deze studie. Als er geen vragenlijst voor handen was, zoals voor het meten van gelegenheid, is een vragenlijst door de onderzoekers zelf gemaakt.

Bij het meten van het omgaan met (phishing) e-mails is gebruik gemaakt van vignetten. Een belangrijk nadeel van de vignettenmethode is de uitdaging van het maken van geschikte vignetten (Maguire et al., 2015). Een geschikt scenario vinden is cruciaal maar niet altijd even makkelijk. Ook hier is op basis van pragmatisme bepaald voor welke gedragingen vignetten worden opgesteld. Er zijn bijvoorbeeld veel realistische voorbeelden van phishing mails in omloop die relatief eenvoudig aangepast kunnen worden voor de doeleinden van deze studie.

Er zijn drie objectieve metingen van daadwerkelijk cybergedrag opgenomen in de experimentele survey, waarbij er bij twee van deze metingen experimentele condities zijn toegevoegd die verschillende tussen-persoons condities hebben gevormd. Hierbij worden er in een meting van daadwerkelijk cybergedrag variaties toegepast die aan verschillende subgroepen respondenten worden voorgelegd. Zo werd bij de objectieve meting “klikgedrag”, een fictieve risico-situatie waarin respondenten werd gevraagd software te downloaden, bij de helft van de respondenten tijdsdruk opgelegd. Bij de objectieve meting “delen van persoonlijke gegevens”, waarin respondenten gevraagd werden persoonlijke gegevens in te vullen zoals hun adres en de laatste drie cijfers van hun rekeningnummer, werden verschillende verleidingstechnieken toegepast om de bereidheid tot het vrijgeven van persoonlijke gegevens te manipuleren (1/3 verleidingstechniek autoriteit, 1/3 verleidingstechniek wederkerigheid, 1/3 geen verleidingstechniek).

*Tabel 4. Overzicht van metingen van cybergedrag per gedragsgebied*

| **Cybergedrag** | **Meetmethode** | | |
|---|---|---|---|
| | Zelfrapportage: Vragenlijst | Zelfrapportage: Vignet | Objectieve meting |
| 1. Gebruik van wachtwoorden | Ja: vragenlijst | | Ja: wachtwoord sterkte<br>*Geen experimentele conditie* |
| 2. Opslaan van belangrijke bestanden | Ja: vragenlijst | | |
| 3. Installeren van updates | Ja: vragenlijst | | |
| 4. Gebruik van beveiligingssoftware | Ja: vragenlijst | | |
| 5. Alertheid tijdens internetgebruik | Ja: vragenlijst | | Ja: klikgedrag<br>*Experimentele conditie: tijdsdruk* |
| 6. Online delen van persoonlijke gegevens | Ja: vragenlijst | | Ja: delen van persoonlijke gegevens<br>*Experimentele conditie: verleidingstechnieken* |
| 7. Omgaan met bijlagen en hyperlinks in e-mails | Ja: vragenlijst | Ja: e-mail keuze | |

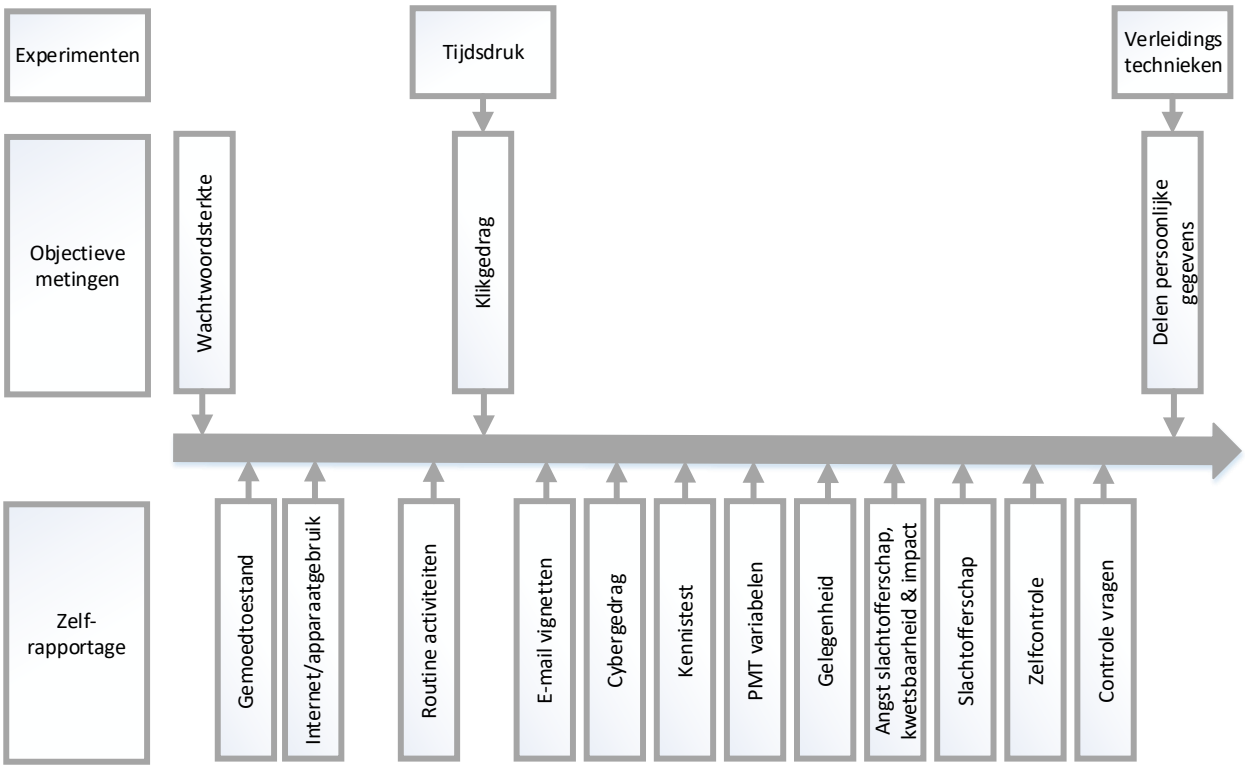
Naast cybergedrag had de experimentele survey betrekking op een groot aantal verklarende factoren. Op basis van de literatuurstudie zijn de beoogde onderwerpen van het huidige onderzoek geïdentificeerd. Tabel 5 geeft alle onderwerpen weer die in de vragenlijst zijn bevraagd. De onderwerpen zijn verdeeld over een aantal onderdelen. Binnen elk onderdeel is een aantal onderwerpen bestudeerd. In de survey is over elk onderwerp één of meerdere items opgenomen.

*Tabel 5. Overzicht van surveyonderwerpen, anders dan cybergedrag*

| **Onderdeel** | **Par.nr. in literatuurstudie** | **Theoretisch model** | **Onderwerpen** |
|---|---|---|---|
| Kennis | 3.4.2 | COM-B | Zelfrapportage kennis online veiligheid |
| | | | Kennistest |
| Gelegenheid | 3.4.2 | COM-B | Materiële omgeving |
| | | | Sociale omgeving |
| Motivatie | 3.4.1 & 3.4.2 | PMT & COM-B | Motivatie voor bescherming |
| Gemoedstoestand | 3.4.3 | | Gemoedstoestand (PANAS) |
| Angst voor slachtofferschap | 3.4.2 | | Angst voor slachtofferschap |
| Eerder slachtofferschap | 3.4.1 | PMT | Eerder slachtofferschap van online criminaliteit |
| Zelfcontrole | 3.4.1 | | Zelfcontrole (BSCS) |
| Type apparaat | 3.4.3 | | Type apparaat waarmee survey is ingevuld |
| Tijdsdruk | 3.4.3 | | Tijdsdruk |
| Verleidingstechnieken | 3.4.3 | | Autoriteit |
| | | | Wederkerigheid |
| Dreiging-evaluatie | 3.4.1 | PMT | Gepercipieerde kwetsbaarheid |
| | | | Gepercipieerde impact |
| Maatregel-evaluatie | 3.4.1 | PMT | Responseffectiviteit |
| | | | Zelfeffectiviteit |
| | | | Responskosten |
| Locus of control | 3.4.2 | | Locus of control |
| Controle factoren | | | Geslacht |
| | | | Opleidingsniveau |
| | | | Leeftijd |
| | | | Dagelijkse bezigheid |

| | | | |
|---|---|---|---|
| | | | Samenwonend (ja/nee) |
| | | | Kinderen (<16 jaar) in huishouden |
| | 3.4.3 | | Type apparaat bij invullen vragenlijst |
| Online apparaten | | | Gebruik van online apparaten |
| | | | Beveiligingssoftware |
| Routine activiteiten | | | Internetgebruik |
| | | | Online activiteiten |

In figuur 3 staat de survey nog eens schematisch weergegeven. De opbouw van de complete experimentele survey, inclusief de (volgorde van) de metingen en de items, is beschreven in bijlage 1.




*Figuur 3: Schematische weergave onderdelen survey*

## *4.3. Operationalisatie*

### *4.3.1. Afhankelijke variabelen*

De survey omvat vijf afhankelijke variabelen die allen (vormen van) cybergedrag hebben gemeten. Alle variabelen zijn dezelfde kant op gecodeerd: hoe hoger de score, hoe veiliger de cybergedraging van de respondent (de precieze meting van alle variabelen in te vinden in bijlage 1).

De variabele *"zelf-gerapporteerd gedrag"* beslaat de meting van cybergedrag zoals dat door de respondenten zelf is gerapporteerd. Deze variabele is gemeten door het voorleggen van 18 stellingen verdeeld over zeven gedragsonderwerpen (zoals wachtwoord gebruik, updaten van software etc.). Antwoordmogelijkheden waren: altijd, vaak, soms, zelden of nooit (5-punts likert schaal) of niet van toepassing. De hoogste score (5) is voor iedere stelling toebedeeld aan de veiligste antwoordmogelijkheid, afhankelijk van de stelling betrof dit het antwoord altijd of nooit. De afhankelijke variabele "zelf-gerapporteerd gedrag" is het gemiddelde van deze 18 stellingen.

De variabele *"e-mail keuze"* is een samengestelde variabele op basis van twee phishing e-mail-vignetten. Onderzocht werd hoe veilig respondenten omgaan met hyperlinks in phishing e-mails. Respondenten kregen eerst de volgende tekst voorgelegd: "Veel mensen worden dagelijks overspoeld met een groot aantal e-mails. We willen graag weten hoe mensen omgaan met e-mails. Er zullen nu een aantal e-mails aan u worden voorgelegd, zoals die binnenkomen in het Postvak In (Inbox) van "Robin de Vries". We willen u vragen te doen alsof u Robin bent. Wat zou Robin met deze e-mails doen?" Respondenten kregen in totaal drie e-mails te zien; twee phishing (onveilige) e-mails, zogenaamd van de Rabobank en een festivalorganisatie, en één legitieme (veilige) e-mail, van KPN (zie paragraaf 5.3.5. voor voorbeelden en bijlage 1 voor de volledige vignetten). Respondenten dienden voor elk van de volgende negen antwoordcategorieën "ja" of "nee" te kiezen: Ik beantwoord de e-mail, Ik verwijder de e-mail, Ik stuur de e-mail door naar iemand anders, Ik kopieer en plak de URL (het www adres) uit de e-mail in een webbrowser, Ik klik op de link in de e-mail, Ik typ de URL (het www adres) over in een webbrowser, Ik bewaar de e-mail, Ik zoek naar meer informatie voordat ik een keuze maak, Ik doe niets. De afhankelijke variabele "e-mail keuze" is binair. Indien de respondent aangegeven heeft bij één of beide phishing e-mails de gelinkte website te openen (i.e., "ja" beantwoord op een van de volgende opties: Ik kopieer en plak de URL (het www adres) uit de e-mail in een webbrowser, Ik klik op de link in de e-mail, Ik typ de URL (het www adres) over in een webbrowser), dan heeft de respondent een onveilige keuze gemaakt (gecodeerd als 0). Alternatief heeft de respondent bij beide phishing e-mails een andere (veilige) keuze heeft gemaakt (gecodeerd als 1).

De overige drie afhankelijke variabelen zijn elk voortgekomen uit een objectieve meting van een van de zeven gedragsclusters. De variabele *"wachtwoord sterkte"* betreft een meting van de sterkte van het wachtwoord dat respondenten gekozen hebben bij het creëren van een (fictief) account in de survey. Aan het begin van de vragenlijst kregen de respondenten het volgende verzoek voorgelegd: "In overeenstemming met wetgeving ten aanzien van gegevensbescherming vragen we u om nu eerst een tijdelijk gebruikersaccount aan te maken. In dit account worden omwille van dit onderzoek enkele persoonlijke gegevens opgeslagen. Dit account heeft u aan het einde van de vragenlijst eenmalig opnieuw nodig. Voer hieronder een gebruikersnaam en wachtwoord in." Op basis van het soort tekens dat door respondenten in hun wachtwoord gebruikt is (kleine letters, hoofdletters, cijfers, speciale tekens) maar vooral de lengte van het wachtwoord (correlatie lengte en entropie: $r = .99$, $p < .001$) is de entropie[24], ofwel sterkte, van het wachtwoord berekend. De scores op deze afhankelijke variabele waren echter linksscheef verdeeld, waarbij veel respondenten hoger scoorden dan het gemiddelde. Om deze afhankelijke variabele meer normaal verdeeld te maken is een worteltransformatie toegepast en is de afhankelijke variabele "wachtwoord sterkte" dus de wortel van deze entropie. Aan het einde van de vragenlijst is een controle vraag gesteld aan de respondenten: "Aan het begin van deze vragenlijst hebben wij u gevraagd een account aan te maken. Is het wachtwoord dat u heeft ingetypt overeenkomstig met hoe u normaal een wachtwoord aanmaakt voor het beschermen van uw persoonlijke gegevens?" Antwoordopties waren: Nee, ik heb een simpeler wachtwoord gekozen dan dat ik normaal zou doen; Nee, ik heb een ingewikkelder wachtwoord gekozen dan dat ik normaal zou doen; Ja, ik heb een wachtwoord gekozen op dezelfde wijze als dat ik normaal zou doen.

De variabele *"klikgedrag"* betreft de keuze die respondenten gemaakt hebben toen hen middels een pop-up gevraagd werd (fictieve) software van een onbekende bron te downloaden om zodoende een filmpje te bekijken dat onderdeel van de survey zou zijn. Respondenten hebben een onveilige keuze gemaakt als zij "ja" hebben geklikt op de pop-up (gecodeerd als 0) of een veilige keuze als zij "nee" hebben aangeklikt of niets hebben aangeklikt op de pop-up (maar hebben geklikt op "verder" naar de volgende vraag) (gecodeerd als 1). In de objectieve meting van "klikgedrag" is geëxperimenteerd met tijdsdruk (zie 4.3.2).

[24] De entropie, ofwel sterkte, van een wachtwoord hangt af van twee factoren: de lengte van het wachtwoord en de mate waarin verschillende karakters (letters, cijfers, speciale tekens etc.) worden gebruikt. De entropie drukt uit hoeveel wachtwoorden gemaakt zouden kunnen worden met de gekozen combinatie van lengte en complexheid, in een verkleinde factor genaamd "bits". Hoe hoger de entropie van een wachtwoord, hoe moeilijker dit wachtwoord te hacken/kraken is. Een wachtwoord met een entropie van minimaal 80 bits wordt gezien als gemiddeld sterk (https://www.informatiebewust.nl/hoe-maak-je-een-sterk-wachtwoord/).

De laatste afhankelijke variabele “delen persoonlijke gegevens” is gemeten door aan het einde van de vragenlijst respondenten te vragen gegevens in te vullen die onveilig zijn om te delen met (niet-geautoriseerde) derden. Het betrof hun volledige naam, e-mailadres, e-mailadres van een bekende, geboortedatum, postcode, huisnummer en de laatste drie cijfers van hun rekeningnummer. Voor elke vraag hadden de respondenten de mogelijkheid “zeg ik liever niet” aan te vinken. Respondenten hebben voor elke vraag een veilige keuze gemaakt wanneer zij “zeg ik liever niet” hebben aangevinkt (gecodeerd als 1) en een onveilige keuze gemaakt wanneer zij een antwoord hebben ingevuld. De afhankelijke variabele “delen persoonlijke gegevens” betreft de som van deze negen variabelen. In verband met privacywetgeving hebben de onderzoekers geen beschikking over de antwoorden van de respondenten. In de objectieve meting van “delen van persoonlijke gegevens” is geëxperimenteerd met de verleidingstechnieken van autoriteit en wederkerigheid (zie 4.3.2).

### *4.3.2. Onafhankelijke variabelen*

Wanneer een onderwerp is uitgevraagd met meer dan één item, zijn constructen samengesteld door het gemiddelde van de items te nemen. (Zie tabel 6 voor de Cronbach’s alfa van alle constructen.)

Voor het meten van de kennis van de respondenten is een kennistest afgenomen, bestaande uit 19 meerkeuzevragen over online veiligheid en aanverwante onderwerpen. De onafhankelijke variabele *“kennis”* betreft het aantal goede antwoorden van respondenten in deze kennistest. (Zie bijlage 1 voor de complete kennistest.)

De gelegenheid die mensen hebben voor veilig cybergedrag, is uitgevraagd middels één stelling betreffende de sociale gelegenheid (“Mensen om mij heen (familie/vrienden/kennissen) vinden online veiligheid belangrijk”) en één stelling betreffende de materiële gelegenheid (“In ons huishouden is er financiële ruimte om beveiligingsmiddelen aan te schaffen, zoals een virusscanner, VPN of clouddienst”). Beide stellingen konden beantwoord worden op een vijf-punts likert schaal van “helemaal mee oneens” tot “helemaal mee eens”, waarbij de hoogste score steeds is toegekend aan de veiligste antwoordoptie. Hoe hoger respondenten scoren op de gelegenheid variabelen, hoe meer gelegenheid zij zeggen te hebben voor veilig cybergedrag.

Voor het meten van “*motivatie”* (protection motivation) zijn drie items gemeten op een vijf-punts likert schaal van “helemaal mee oneens” tot “helemaal mee eens”. De onafhankelijke variabele motivatie betreft het gemiddelde van deze drie items. Een volledig overzicht van de gebruikte stellingen is weergegeven in bijlage 1. Een weergave van het construct motivatie is weergegeven in tabel 6.

Op het gebied van dreiging- en maatregel-evaluatie zijn items opgenomen voor het meten van zelfeffectiviteit, responskosten, responseffectiviteit, gepercipieerde kwetsbaarheid en gepercipieerde impact. Antwoordopties liepen op een vijf-punts likert schaal van “helemaal mee oneens” tot “helemaal mee eens”. Het aantal items en de samengestelde constructen zijn beschreven in tabel 6. Een compleet overzicht van alle gebruikte items is weergegevens in bijlage 1.

Op het gebied van slachtofferschap is “angst voor slachtofferschap” gemeten met zes stellingen (zie bijlage 1) op een vijf-punts likert schaal van “helemaal mee oneens” tot “helemaal mee eens”. “Slachtofferschap” is gemeten door te vragen aan respondenten of zij in aanraking gekomen zijn met 11 vormen van online criminaliteit (zoals phishing, malware, identiteitsfraude etc.). Antwoordopties waren “ja, in de afgelopen 12 maanden”, “ja, langer geleden dan 12 maanden”, “nee”, of “weet ik niet”. Respondenten zijn ooit slachtoffer geworden van online criminaliteit als zij “ja, in de afgelopen 12 maanden” of “ja, langer geleden dan 12 maanden” hebben geantwoord voor één van de 11 vormen van online criminaliteit. Een compleet overzicht van de vormen van online criminaliteit is weergegevens in bijlage 1.

De gemoedstoestand die respondenten hadden tijdens het invullen van de survey is gemeten door het afnemen van het gestandaardiseerde PANAS[25]-instrument (Watson, Clark, & Tellegen, 1988; Engelen, De Peuter, Victoir, Van Diest, & Van den Bergh, 2006). In deze korte vragenlijst worden respondenten gevraagd in welke mate zij 20 gevoelens en emoties ervaren op dit moment; heel weinig (1), een beetje (2), matig (3), veel (4) en heel veel (5). De variabelen “positieve gemoedstoestand” en “negatieve gemoedstoestand” zijn elk gemiddelden van 10 van deze gevoelens en emoties. Bij deze operationalisatie zijn de gestandaardiseerde methodieken aangehouden en zowel een factoranalyse als een betrouwbaarheidsanalyse ondersteunen de hieruit voortgekomen constructen. Een volledig overzicht van de PANAS is weergegeven in bijlage 1. Een weergave van de constructen is weergegeven in tabel 6.

Zelfcontrole is gemeten middels de gestandaardiseerde vragenlijst “Brief Self-Control Scale (BSCS)”, bestaande uit 13 items, gemeten op een vijf-punts likert schaal van “helemaal niet op mij van toepassing” tot “heel erg op mij van toepassing”. Een volledig overzicht van de BSCS is weergegeven in bijlage 1. Het construct is weergegeven in tabel 6.

Dreiging-evaluatie is een gemiddelde maat op basis van één stelling over gepercipieerde kwetsbaarheid en zes stellingen over gepercipieerde impact, allen gemeten op een vijf-punts likert schaal van “helemaal niet op mij van toepassing” tot “heel erg op mij van toepassing”. Maatregel-evaluatie is

[25] Positive and Negative Affect Schedule

een gemiddelde maat op basis van zes stellingen over responseffectiviteit, zeven stellingen over zelfeffectiviteit en acht stellingen over responskosten, allen gemeten op een vijf-punts likert schaal van "helemaal niet op mij van toepassing" tot "heel erg op mij van toepassing". Een volledig overzicht van de stellingen is weergegeven in bijlage 1 en het construct is weergegeven in tabel 6.

Of de locus of control bij respondenten intern of extern is, is gemeten door het gemiddelde te nemen van drie stellingen met verschillende schalen. De stelling "Als het aankomt op mijn veiligheid op internet, ben ik daar in eerste instantie zelf verantwoordelijk voor" kon beantwoord worden op een vijf-punts likert schaal van "helemaal mee oneens" tot "helemaal mee eens". De stelling "Het veilig houden van mijn persoonlijke gegevens" kon beantwoord worden op een vijf-punts likert schaal van "ligt buiten mijn controle" tot "ligt binnen mijn controle". De stelling "De verantwoordelijkheid voor het beschermen van mijn persoonlijke gegevens ligt bij…" " kon beantwoord worden op een vijf-punts likert schaal van "de overheid/politie" tot "mijzelf". Een weergave van het construct is opgenomen in tabel 6.

Tot slot zijn er twee experimenten opgenomen in de survey. Het eerste experiment betreft de ervaring van *tijdsdruk*. Dit experiment is ingebouwd rondom de meting "klikgedrag" (de respondent moest een filmpje bekijken, maar krijgt een pop-up te zien waar staat dat software moet worden gedownload (uit onbetrouwbare bron) om het filmpje te kunnen afspelen – zie bijlage 1). Voordat respondenten gevraagd werd een filmpje te bekijken en hiervoor software te downloaden, kregen de respondenten te lezen: "We gaan u nu vragen stellen over een aantal online activiteiten. U heeft voor dit blok **5 minuten** de tijd". Daarbij kregen zij één van de volgende twee teksten te lezen (50% van de respondenten per tekst). Tekst één (opleg tijdsdruk): "Het is gebleken dat dit voor veel deelnemers niet genoeg tijd is. We willen u vragen in dit blok in een hoog tempo door te werken. Probeer alle vragen af te krijgen in de tijd die u heeft." Tekst twee (controlegroep): "Het is gebleken dat dit voor de meeste deelnemers ruim genoeg tijd is. We willen u vragen in dit blok in uw eigen tempo door te werken." Vervolgens zijn na de meting "klikgedrag" twee controlevragen gesteld (schaal 1-7): Hoeveel tijdsdruk heeft u ervaren bij het maken van uw keuzes in het blok over online activiteiten? En: hoe gehaast voelde u zich tijdens het beantwoorden van de vragen in het blok over online activiteiten?

Het tweede experiment is opgenomen voor de meting "delen persoonlijke gegevens". In dit experiment is een verleidingstechniek toegepast op een deel van de respondenten, om zodoende te kunnen toetsen of mensen eerder geneigd zijn hun persoonlijke gegevens prijs te geven wanneer criminelen een verleidingstechniek gebruiken. Een derde van de respondenten kreeg geen verleidingstechniek te zien, een derde van de respondenten zag tekst één: "Als u onderstaande vragen volledig invult, maakt u kans op een cadeaubon ter waarde van 100 euro" (verleidingstechniek

wederkerigheid) en een derde van de respondenten zag tekst twee: “De onderzoekers van De Haagse Hogeschool en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) verzoeken u met klem om onderstaande vragen volledig in te vullen” (verleidingstechniek autoriteit).

*Tabel 6. Overzicht van samengestelde constructen*

| **Onderwerp** | **Voorbeeld stelling** | **aantal stellingen** | **Cr. Alfa[26]** |
|---|---|---|---|
| Motivatie | Ik wil er alles aan doen om mezelf te beschermen tegen cybercriminaliteit | 3 | .61 |
| Positieve gemoedstoestand | Wilt u alstublieft aangeven in welke mate u deze gevoelens of emoties ervaart: Geïnteresseerd | 10 | .89 |
| Negatieve gemoedstoestand | Wilt u alstublieft aangeven in welke mate u deze gevoelens of emoties ervaart: Overstuur | 10 | .87 |
| Angst voor slachtofferschap | Ik ben bang om slachtoffer te worden van cybercriminaliteit in de nabije toekomst | 6 | .86 |
| Zelfcontrole | Mensen zeggen dat ik een ijzeren zelfdiscipline heb | 13 | .83 |
| Locus of control | Als het aankomt op mijn veiligheid op internet, ben ik daar in eerste instantie zelf verantwoordelijk voor | 3 | .61 |
| Dreiging-evaluatie | Als ik slachtoffer zou worden van cybercriminaliteit, zou dat ernstige gevolgen kunnen hebben | 7 | .69 |
| Maatregel-evaluatie | Het back-uppen van mijn bestanden kost mij veel tijd | 21 | .83 |

### *4.3.3. Controle variabelen*

[26] Voor het samenvoegen van items voor het creëren van 1 construct wordt aangehouden dat de Cronbach’s alfa minimaal .6 dient te zijn (Nunnally & Bernstein, 1994).

Respondenten zijn gevraagd naar hun voornaamste *dagelijkse bezigheid*: Schoolgaand, Ziek/afgekeurd, Zorg voor gezin, Werkloos/werkzoekend, Werkend – betaald, Werkend – onbetaald, Gepensioneerd of anders. Deze categorieën zijn samengevoegd in werkend, betaald of onbetaald (gecodeerd als 1) of anders (gecodeerd als 0). Respondenten zijn gevraagd of zij een partner hebben waarmee ze tenminste drie maanden samen zijn. Respondenten zijn *samenwonend* (1) of niet samenwonend (0). Respondenten zijn vervolgens gevraagd naar het *aantal inwonende kinderen* jonger dan 16 jaar.

Tot slot is een aantal controle variabelen aangeleverd door het panelbureau, namelijk geslacht (man=1, vrouw=0), opleiding (1=laag (geen onderwijs, basisonderwijs, LBO/VBO/VMBO/MBO-1), 2=middel (MBO-2/3/4, HAVO, VWO), 3=hoog (HBO, WO)) en leeftijd (in jaren). Ook op basis van registratiedata van het panelbureau is bekend in welke provincie respondenten wonen: West (Utrecht, Noord-Holland, Zuid-Holland), Noord (Groningen, Friesland, Drenthe), Oost (Overijssel, Gelderland, Flevoland) of Zuid (Zeeland, Noord-Brabant, Limburg).

### *4.4. Analysestrategie*

Beschrijvende resultaten zijn geanalyseerd met frequenties en kruistabellen. De verklarende analyses zijn uitgevoerd met correlaties en multivariate regressiemodellen. Voor de afhankelijke variabelen "zelf-gerapporteerd gedrag" en "wachtwoord sterkte" betreft dit multivariate lineaire regressiemodellen. Voor de afhankelijke variabelen "klikgedrag" en "e-mail keuze" betreft dit logistische regressiemodellen, vanwege de binaire waarden van de afhankelijken. De afhankelijke variabele "delen persoonlijke gegevens" is geanalyseerd met een Poisson regressiemodel[27]. Voor de additionele analyses waarin interacties zijn getoetst, is gebruik gemaakt van gecentraliseerde variabelen (voor elke respondent wordt het groepsgemiddelde in mindering gebracht op de persoonlijke score) om multicollineariteit[28] te voorkomen.

### *4.5 Beperkingen*

[27] Poisson regressiemodellen worden gebruikt om *count* variabelen te modelleren. Aangezien het bij deze afhankelijke variabelen gaat om een telling van het aantal gedeelde persoonlijke gegevens is een Poisson regressie de meest geschikte methode.

[28] Multicollineariteit ontstaat wanneer twee of meerdere onafhankelijke variabelen in het regressiemodel sterk gecorreleerd zijn. Door deze overlap kan de berekening van regressie coëfficiënten beïnvloed worden en wordt de betrouwbaarheid gereduceerd.

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 metingen hebben echter ieder hun eigen beperkingen. De beperkingen staan uitgebreid beschreven in hoofdstuk 6. Deze paragraaf bevat een beknopte weergave. Ten eerste was het door de lengte van de vragenlijst niet mogelijk om objectieve metingen voor alle zeven gedragsclusters op te nemen. Ook weten we bij de variabelen over het delen van persoonlijke gegevens niet welke gegevens 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. 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 (zie paragraaf 6.4). 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. Ondanks dat het juist onze bedoeling was cybergedrag in een ogend veilige omgeving te meten – criminelen bootsen altijd een veilige omgeving (van bijvoorbeeld een bank of webshop) na en verleiden mensen hiermee op de hyperlink klikken of persoonlijke informatie weg te geven – kan het toch tot een vertekening van de resultaten hebben geleid.

# 5. Resultaten

## *5.1. Inleiding*

In dit hoofdstuk laten we op basis van de resultaten van de experimentele survey zien hoe veilig Nederlanders zich online gedragen en hoe dat gedrag kan worden verklaard. Eerst beschrijven we de eigenschappen van de respondenten en mogelijke verklarende eigenschappen (paragraaf 5.2). Vervolgens komen in paragraaf 5.3 de verschillende cybergedragingen aan bod. Zelf-gerapporteerd gedrag en (waar mogelijk) objectief gemeten gedrag met betrekking tot wachtwoordgebruik, het opslaan van bestanden, het updaten van software, online alertheid en het omgaan met bijlagen en hyperlinks in e-mails worden beschreven. In paragraaf 5.4 volgen verklaringen van cybergedrag. We behandelen onder andere verklaringen voor zelf-gerapporteerd cybergedrag, wachtwoord sterkte, de keuze om wel of geen software te downloaden en hoe respondenten omgaan met e-mails. Vervolgens komen in paragraaf 5.5 enkele aanvullende verklaringen van cybergedrag aan bod, zoals dreigings-evaluatie en locus of control. Bovendien worden in deze paragraaf interactie-effecten behandeld. Het hoofdstuk sluit af met een kort resumé waarin de belangrijkste bevindingen staan weergegeven (paragraaf 5.6).

## *5.2. Beschrijving van eigenschappen van respondenten*

### *5.2.1. Beschrijving achtergrondkenmerken*

De achtergrondkenmerken van de 2.426 respondenten zijn uiteengezet in tabel 7 en vergeleken met de Nederlandse bevolking (CBS, 2019a). Respondenten zijn ongeveer gelijk verdeeld tussen mannen (53,5%) en vrouwen (46,5%) en ongeveer de helft van de respondenten werkt (betaald of onbetaald, 48,4%). Terwijl ruim de helft van de respondenten afkomstig is uit een van de westelijke provincies (55,2%), is 22,4 procent woonachtig in een oostelijke provincie en komt respectievelijk 7,5 procent en 15,0 procent uit het noorden of zuiden van Nederland. Respondenten zijn daarmee representatief voor de Nederlandse samenleving op geslacht, werkend (ja/nee) en de provincie waarin zij woonachtig zijn. Respondenten zijn 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%). Ruim twee-derde van de respondenten (69,2%) woont samen met een partner en 14,3 procent rapporteert een inwonend kind, jonger dan 16 jaar. Respondenten hebben de vragenlijst ingevuld op diverse apparaten: het vaakst werd de vragenlijst

ingevuld op een laptop (33,7%), gevolgd door desktop computer (31,2%), tablet (18,3%) en het minst vaak de mobiele telefoon (16,8%).

*Tabel 7. Achtergrondkenmerken onderzoekspopulatie (N=2426) in vergelijking met Nederlandse bevolking*

| | **Respondenten** | | **Nederlandse bevolking (CBS, 2019a)** |
|---|---|---|---|
| **Kenmerk** | **N** | **%** | **%** |
| Geslacht | | | |
| -man | 1297 | 53,5% | 49,6% |
| -vrouw | 1129 | 46,5% | 50,4% |
| Opleiding | | | |
| -laag | 410 | 16,9% | 31,6% |
| -middel | 804 | 33,1% | 38,4% |
| -hoog | 1212 | 50,0% | 30% |
| Leeftijd | | | |
| -18 t/m 39 | 335 | 13,8% | 29,4% |
| -40 t/m 64 | 1180 | 48,6% | 25,6% |
| -65+ | 911 | 37,6% | 7,7% |
| Dagelijkse bezigheid | | | |
| -werkend | 1175 | 48,4% | 50,9% |
| -niet werkend (incl. pensioen, ziek, huishouden) | 1251 | 51,6% | 49,1% |
| Provincie | | | |
| -West (UT, NH, ZH) | 1338 | 55,2% | 45,5% |
| -Noord (GR, FR, DR) | 182 | 7,5% | 10,0% |
| -Oost (OV, GD, FL) | 543 | 22,4% | 21,1% |
| -Zuid (ZL, NB, LB) | 363 | 15,0% | 23,4% |
| Gezinssamenstelling | | | |
| -samenwonend (ja/nee) | 1678 | 69,2% | |
| -inwonende kinderen jonger dan 16 jaar (ja/nee) | 348 | 14,3% | |
| Apparaat gebruikt voor invullen vragenlijst | | | |

| | | | |
|---|---|---|---|
| -tablet | 443 | 18,3% | |
| -mobiele telefoon | 408 | 16,8% | |
| -laptop | 818 | 33,7% | |
| -desktop computer | 757 | 31,2% | |

*5.2.2. Beschrijving onafhankelijke variabelen*

In tabel 8 worden de kenmerken beschreven, die in dit rapport worden gebruikt om de veiligheid van cybergedrag te verklaren. Met betrekking tot kennis, hebben respondenten gemiddeld ruim 12 van de 19 vragen in de kennistest over online veiligheid goed beantwoord (G=12.24). Op het gebied van gelegenheid voor veilig cybergedrag, rapporteren zij nagenoeg een even grote mate van sociale (M = 3.83) en materiële gelegenheid voor veilig cybergedrag (M = 3.85). De motivatie voor veilig cybergedrag is gemiddeld hoog (M = 3.97).

*Tabel 8. Beschrijving van onafhankelijke variabelen (N=2426)*

| | Minimum | Maximum | Gemiddelde | S.E. |
|---|---|---|---|---|
| Kennis | 0.00 | 19.00 | 12.24 | 3.69 |
| Sociale gelegenheid | 1.60 | 5.00 | 3.83 | 0.67 |
| Materiële gelegenheid | 1.00 | 5.00 | 3.85 | 0.86 |
| Motivatie | 1.33 | 5.00 | 3.97 | 0.58 |
| Negatieve gemoedstoestand | 1.00 | 4.20 | 1.33 | 0.46 |
| Positieve gemoedstoestand | 1.00 | 4.90 | 3.01 | 0.70 |
| Angst slachtofferschap | 1.00 | 5.00 | 2.93 | 0.74 |
| Zelfcontrole | 1.54 | 5.00 | 3.58 | 0.60 |
| Ooit slachtoffer | 0.00 | 1.00 | 0.48 | 0.50 |

De negatieve gemoedstoestand van respondenten is gemiddeld laag (M = 1.33), terwijl de positieve gemoedstoestand gemiddeld hoger ligt (M = 3.01). Respondenten rapporteren gemiddeld neutrale mate van angst voor slachtofferschap (M = 2.93); het vaakst waren respondenten het niet eens nog oneens met stellingen over angst voor slachtofferschap. Respondenten beschikken gemiddeld over een zekere mate van zelfcontrole, gemiddeld 3.58 op een schaal van één (laagste maat van zelfcontrole) tot vijf (hoogste maat van zelfcontrole). Slachtofferschap van online criminaliteit is 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) (tabel 8).

*Tabel 9. Slachtofferschap van cybercrime*

| **Cybercrime** | **Ja, <12 maanden** | **Ja, >12 maanden** | **Nee** | **Weet ik niet** | **Schade (incident <12 maanden)** |
|---|---|---|---|---|---|
| Phishing | 70 (2,9%) | 114 (4,7%) | 2110 | 132 | 37 (52,9%) |
| Malware | 177 (7,3%) | 611 (25,2%) | 1417 | 221 | 104 (58,8%) |
| Online aankoopfraude | 48 (2,0%) | 190 (7,8%) | 2172 | 16 | 45 (93,8%) |
| Online identiteitsfraude | 10 (0,4%) | 17 (0,7%) | 2324 | 75 | 8 (80,0%) |
| Voorschotfraude | 7 (0,3%) | 17 (0,7%) | 2392 | 10 | 3 (42,9%) |
| Profielpagina veranderd | 9 (0,4%) | 36 (1,5%) | 2336 | 45 | 5 (55,6%) |
| Online account gehackt | 16 (0,7%) | 61 (2,5%) | 2224 | 125 | 11 (68,8%) |
| Computer gehackt | 9 (0,4%) | 35 (1,4%) | 2322 | 60 | 8 (88,9%) |
| E-mailaccount gehackt | 23 (0,9%) | 74 (3,1%) | 2149 | 180 | 11 (47,8%) |
| Bestanden ontoegankelijk | 9 (0,4%) | 93 (3,8%) | 2206 | 118 | 5 (55,6%) |
| Andere vorm van cybercrime | 29 (1,2%) | 73 (3,0%) | 2192 | 132 | 26 (89,7%) |
| Totaal (unieke personen) | 330 (13,6%) | 951 (39,2%) | | | 214 (64,8%) |

In tabel 9 wordt de prevalentie van slachtofferschap per type delict beschreven. In totaal werd 13,6 procent van de respondenten het afgelopen jaar slachtoffer van online criminaliteit. Respondenten werden afgelopen jaar het vaakst slachtoffer van malware[29] (7,3%), gevolgd door phishing[30] (2,9%) en van

[29] Malware is kwaadaardige software die ongevraagd en meestal ongemerkt op uw computer wordt geïnstalleerd. Voorbeelden van malware zijn virussen, trojan horses, wormen en spyware.

[30] 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.

online aankoopfraude[31] (2,0%). Ook werd 39,2 procent 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 van een e-mailaccount (3,1%)[32]. Het aantal slachtoffers dat schade heeft ondervonden van het slachtofferschap dat afgelopen jaar heeft plaatsgevonden ligt zeer hoog. Gemiddeld rapporteert 64,8% van de respondenten schade, omdat het incident ervoor heeft gezorgd dat zij geld, tijd of bestanden zijn kwijtgeraakt of emotionele schade of andere schade hebben ondervonden (tabel 9). Het percentage slachtoffers dat dergelijke schade ondervindt, is echter afhankelijk van het type delict en varieert tussen 43 procent tot 94 procent.

### *5.2.3. Samenhang onafhankelijke variabelen*

De onafhankelijke variabelen die in de vorige paragraaf zijn beschreven, hangen onderling vaak samen, zoals is weergegeven in tabel 10, maar slechts in zeer geringe mate. Geen van de verbanden is groot genoeg om besproken te worden (correlatie (r) van minimaal .3). Tussen alle onafhankelijke variabelen is er nauwelijks of geen sprake van samenhang ($r < .3$).

## ***5.3. Beschrijving van cybergedrag***

In deze paragraaf zullen de cybergedragingen van respondenten worden beschreven; het betreft hierbij alle zeven gedragsclusters. Een compleet overzicht met alle beschrijvende metingen uit zelf-rapportage en overige metingen (objectieve metingen en vignetten) staat weergegeven in bijlage 1.

### *5.3.1. Gebruik van wachtwoorden*

*Zelf-gerapporteerd gedrag*

[31] 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.

[32] Hierbij moet opgemerkt worden dat het aantal respondenten dat als antwoord 'weet ik niet' invulden sterk verschilt per type delict. Bij slachtofferschap van malware, bijvoorbeeld, antwoordden liefst 221 respondenten 'weet ik niet', wat neer komt 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 was het afgelopen jaar of langer geleden slachtoffer van malware.

*Tabel 10. Correlatietabel onafhankelijke variabelen (Pearsons's r)*

| | **Score kennistest** | **Sociale gelegenheid** | **Materiële gelegenheid** | **Motivatie** | **Negatieve gemoeds-toestand** | **Positieve gemoeds-toestand** | **Angst slachtoffer-schap** | **Ooit slachtoffer** |
|---|---|---|---|---|---|---|---|---|
| **Sociale gelegenheid** | -.084*** | | | | | | | |
| **Materiële gelegenheid** | .177*** | .100*** | | | | | | |
| **Motivatie** | .015 | .238*** | .238*** | | | | | |
| **Negatieve gemoeds-toestand** | -.040* | -.061** | -.127*** | -.019 | | | | |
| **Positieve gemoeds-toestand** | -.076*** | .105*** | .101*** | .145*** | .018 | | | |
| **Angst slachtoffer-schap** | -.195*** | .085*** | -.116*** | .217*** | .179*** | -.041* | | |
| **Ooit slachtoffer** | .194*** | -.048* | .002 | .036 | .062** | -.033 | .040* | |
| **Zelfcontrole** | -.060** | .137*** | .070*** | .135*** | -.214*** | .267*** | -.087*** | -.089*** |

* p<.05, **p<.01, ***p<.001

Respondenten rapporteren gemiddeld veilig om te gaan met wachtwoorden (tabel 11). Het meest veilig zouden zij zijn op het gebied van delen van wachtwoorden met anderen. Respondenten scoren gemiddeld bijna de maximale veilige score (nooit (5)) op deze stelling ("Ik deel mijn persoonlijke wachtwoorden met anderen", G=4.68[33]). Vergeleken met de andere stellingen over wachtwoordgebruik, geven respondenten aan het minst veilig om te gaan met het hergebruiken van wachtwoorden voor verschillende toepassingen (G=3.53, op een schaal van één (altijd) tot vijf (nooit). Gemiddeld gaven respondenten bij de zelfrapportage aan zelden simpele of korte wachtwoorden te gebruiken (G=3.89, op een schaal van één (altijd) tot vijf (nooit).

*Tabel 11. Beschrijving zelf-gerapporteerd gedrag: gebruik van wachtwoorden*

| **Stelling (schaal 1-5, hoe hoger de score hoe veiliger het gedrag)** | **N** | **Gemiddelde** | **S.D.** |
|---|---|---|---|
| Ik deel mijn persoonlijke wachtwoorden met anderen (O[34]) | 2421 | 4.68 | 0.59 |
| Ik gebruik simpele, korte wachtwoorden, met bijvoorbeeld slechts 1 cijfer of hoofdletter (O) | 2405 | 3.89 | 1.15 |
| Ik gebruik hetzelfde wachtwoord voor verschillende toepassingen, bijvoorbeeld zowel voor sociale media als online bankieren en webwinkels (O) | 2403 | 3.53 | 1.21 |

*Daadwerkelijk gedrag*

Uit de objectieve meting van de kenmerken van het zelfgekozen wachtwoord blijkt echter dat 89,2 procent van de respondenten een zwak wachtwoord kiest met een entropie[35] van 79 bits of lager (tabel 12). Dit percentage is 82,7 procent onder de respondenten die achterin de vragenlijst hebben aangegeven dat ze een wachtwoord hebben gekozen op dezelfde wijze als ze dat normaal zouden doen (N=837, niet in tabel). Illustrerend is dat 51 procent van de totale groep respondenten een wachtwoord kiest van zeven

[33] (O)= score van de stelling is omgedraaid. Voor alle stellingen geldt daardoor: hoe hoger de score, hoe veiliger het gedrag.

[34] (O)= score van de stelling is omgedraaid. Voor alle stellingen geldt daardoor: hoe hoger de score, hoe veiliger het gedrag.

[35] De entropie, ofwel sterkte, van een wachtwoord hangt af van twee factoren: de lengte van het wachtwoord en de mate waarin verschillende karakters (letters, cijfers, speciale tekens etc.) worden gebruikt. De entropie drukt uit hoeveel wachtwoorden gemaakt zouden kunnen worden met de gekozen combinatie van lengte en complexheid, in een verkleinde factor genaamd "bits". Hoe hoger de entropie van een wachtwoord, hoe moeilijker dit wachtwoord te hacken/kraken is. Een wachtwoord met een entropie van minimaal 80 bits wordt gezien als gemiddeld sterk (https://www.informatiebewust.nl/hoe-maak-je-een-sterk-wachtwoord/).

of minder tekens – per definitie een zwak wachtwoord[36]. (Dit percentage is 40% onder de respondenten die achterin de vragenlijst hebben aangegeven dat ze een wachtwoord hebben gekozen op dezelfde wijze als ze dat normaal zouden doen (N=837, niet in tabel). Ook gebruikt 45 procent van alle respondenten geen hoofdletters, 85,7 procent geen cijfers, 88,9 procent geen speciale tekens en is bij 2,6 procent van de respondenten het wachtwoord gelijk aan de gebruikersnaam (niet in tabel).

*Tabel 12. Beschrijving objectieve meting gedrag: wachtwoord sterkte*

| | **N** | **%** |
|---|---|---|
| *Totale populatie (N= 2426)* | | |
| Zwak: Entropie <80 | 2165 | 89,2% |
| Sterk: Entropie 80+ | 261 | 10,8% |
| | | |
| *Respondenten die een wachtwoord hebben gekozen op dezelfde wijze als ze dat normaal zouden doen (N=837)* | | |
| Zwak: Entropie <80 | 692 | 82,7% |
| Sterk: Entropie 80+ | 145 | 17,3% |

### *5.3.2. Opslaan bestanden, updaten en gebruik beveiligingssoftware*

Via zelfrapportage is gemeten hoe respondenten omgaan met het opslaan van belangrijke bestanden, installeren van updates en gebruiken van beveiligingssoftware (tabel 13, 14 en 15). Van alle zeven gedragsclusters rapporteren respondenten gemiddeld het minst veilige gedrag omtrent opslaan van bestanden. Wanneer respondenten kunnen kiezen tussen nooit (1), zelden (2), soms (3), vaak (4) of altijd (5) wordt gemiddeld de score “soms tot vaak” gegeven aan het back-uppen van belangrijke bestanden (G=3.30) en “zelden tot soms” voor het versleuteld opslaan van persoonlijke informatie (G=2.33).

Op het gebied van updaten van software werd op alle stellingen gemiddeld een hoge (veilige) score (vaak (4)) gerapporteerd, zoals het installeren van updates van besturingssystemen (G=3.97), apps/software (G=3.97) en beveiligingssoftware (G=4.19) zodra er een nieuwe update beschikbaar is.

Bij het gebruik van beveiligingssoftware is gemiddeld een groot verschil te zien tussen de scores op de twee stellingen. Op de stelling “ik laat beveiligingssoftware mijn apparaten scannen op virussen en andere kwaadaardige software” wordt gemiddeld ”vaak” beantwoord (G=3.95). Op het gebied van

[36] https://www.informatiebewust.nl/hoe-maak-je-een-sterk-wachtwoord/

browser extensies, zoals software om advertenties of pop-ups te blokkeren, wordt echter gemiddeld ”zelden tot soms” gerapporteerd (G=2.73).

*Tabel 13. Beschrijving zelf-gerapporteerd gedrag: opslaan van belangrijke bestanden*

| **Stelling (schaal 1-5, hoe hoger de score hoe veiliger het gedrag)** | **N** | **Gemiddelde** | **S.D.** |
|---|---|---|---|
| Ik maak back-up van belangrijke bestanden | 2377 | 3.30 | 0.70 |
| Ik bewaar persoonlijke informatie op een versleutelde manier zodat anderen deze niet zomaar kunnen lezen | 2284 | 2.33 | 1.29 |

*Tabel 14. Beschrijving zelf-gerapporteerd gedrag: installeren van updates*

| **Stelling (schaal 1-5, hoe hoger de score hoe veiliger het gedrag)** | **N** | **Gemiddelde** | **S.D.** |
|---|---|---|---|
| Ik installeer updates van de besturingssystemen op mijn apparaten zodra ze beschikbaar zijn | 2362 | 3.97 | 1.40 |
| Ik installeer updates van de apps of software die ik gebruik, zodra ze beschikbaar zijn | 2364 | 3.97 | 1.14 |
| Ik update mijn beveiligingssoftware zodra er een nieuwe update beschikbaar is | 2289 | 4.19 | 1.30 |

*Tabel 15. Beschrijving zelf-gerapporteerd gedrag: gebruik van beveiligingssoftware*

| **Stelling (schaal 1-5, hoe hoger de score hoe veiliger het gedrag)** | **N** | **Gemiddelde** | **S.D.** |
|---|---|---|---|
| Ik laat beveiligingssoftware mijn apparaten scannen op virussen en andere kwaadaardige software | 2311 | 3.95 | 1.23 |
| Ik gebruik browser extensies die mij helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren | 2278 | 2.73 | 1.17 |

### *5.3.3. Alertheid tijdens internetgebruik*

*Zelf-gerapporteerd gedrag*

Enerzijds geven respondenten aan zich gemiddeld veilig tot zeer veilig te gedragen online, door zelden (4) tot nooit (5) software, films, games of muziek uit illegale bronnen te downloaden (G=4.75) en soms (3) tot zelden (4) gebruik te maken van openbare WiFi zonder VPN-verbinding (G=3.66) (tabel 16). Anderzijds

gaan respondenten gemiddeld minder veilig om met het controleren van privacy-instellingen van apparaten, apps of sociale media; zij geven gemiddeld aan dit "soms" te doen (G=2.96).

*Tabel 16. Beschrijving zelf-gerapporteerd gedrag: alertheid tijdens internetgebruik*

| **Stelling (schaal 1-5, hoe hoger de score hoe veiliger het gedrag)** | **N** | **Gemiddelde** | **S.D.** |
|---|---|---|---|
| Ik download software, films, games of muziek uit illegale bronnen (O) [37] | 2382 | 4.75 | 1.11 |
| Ik maak gebruik van openbare WiFi (bijvoorbeeld in horeca of openbaar vervoer), zonder VPN verbinding (O) | 2385 | 3.66 | 1.21 |
| Ik controleer de privacy-instellingen van mijn apparaten, apps of sociale media | 2375 | 2.96 | 1.48 |

*Daadwerkelijk gedrag*

In de objectieve meting werden respondenten gevraagd een filmpje te bekijken. Bij het afspelen van dit filmpje verscheen een pop-up met een verzoek tot het downloaden van (fictieve) software. De veilige keuze – het niet downloaden van de software, gezien de bron van de software werd benoemd als "onbekend" – werd genomen door 59,6 procent van de respondenten (tabel 17). Daarentegen maakte 40,4 procent de onveilige keuze, door op "ja" te klikken en goedkeuring te geven voor het downloaden van software van een onbekende bron.

*Tabel 17. Beschrijving objectieve meting gedrag: klikgedrag*

| | **N** | **%** |
|---|---|---|
| Onveilige keuze (op "ja" geklikt) | 980 | 40,4% |
| Veilige keuze (niet op "ja" geklikt) | 1446 | 59,6% |

### *5.3.4. Online delen van persoonlijke gegevens*

*Zelf-gerapporteerd gedrag*

Het delen van persoonlijke gegevens gebeurd veelal via sociale media en kan online criminelen informatie verschaffen voor een spear-phishing attack – een gepersonaliseerde phishing e-mail waarbij de kans op een geslaagde aanval groter is dan bij andere phishing e-mails. Respondenten hebben aangegeven zeer

[37] (O)= score van de stelling is omgedraaid. Voor alle stellingen geldt daardoor: hoe hoger de score, hoe veiliger het gedrag.

veilig om te gaan met het delen van persoonlijke gegevens via sociale media (tabel 18). Zo delen zij gemiddeld zelden (4) tot nooit (5) persoonlijke gegevens, zoals een huisadres, e-mailadres of telefoonnummer via sociale media (G=4.49) en zijn zij gemiddeld vaak (4) tot altijd (5) selectief in het accepteren van connectieverzoeken van anderen tot hun sociale media (G=4.35).

*Tabel 18. Beschrijving zelf-gerapporteerd gedrag: online delen van persoonlijke gegevens*

| **Stelling (schaal 1-5, hoe hoger de score hoe veiliger het gedrag)** | **N** | **Gemiddelde** | **S.D.** |
|---|---|---|---|
| Ik deel persoonlijke informatie, zoals mijn huisadres, e-mailadres of telefoonnummer via sociale media (O) [38] | 2322 | 4.49 | 1.13 |
| Ik ben selectief in het accepteren van connectieverzoeken van anderen tot mijn sociale media | 2114 | 4.35 | 0.64 |

*Daadwerkelijk gedrag*

Tijdens de objectieve meting blijken respondenten echter vaak bereid tot het opgeven van (zeer) persoonlijke gegevens tijdens het invullen van de survey (tabel 19). Het vaakst zijn respondenten bereid tot het invullen van hun volledige naam (31,0%) en geboortedatum (37,5%), gevolgd door hun e-mailadres (28,1%) en hun postcode (27,0%) en huisnummer (20,4%). Een klein, maar desondanks substantieel deel van de respondenten (4,8%) is bovendien bereid tot het invullen van de laatste drie cijfers van hun bankrekeningnummer. Opvallend is dat respondenten aanzienlijk minder bereid zijn tot het invullen van persoonlijke gegevens van anderen. Slechts 1,4 procent vult een e-mailadres van een bekende in.

*Tabel 19. Beschrijving objectieve meting gedrag: online delen van persoonlijke gegevens*

| | **N** | **%** |
|---|---|---|
| Volledige naam | 751 | 31,0% |
| E-mailadres | 681 | 28,1% |
| E-mailadres bekende | 35 | 1,4% |
| Geboortedatum | 910 | 37,5% |
| Postcode | 655 | 27,0% |
| Huisnummer | 496 | 20,4% |
| Laatste drie cijfers rekeningnummer | 116 | 4,8% |

[38] (O)= score van de stelling is omgedraaid. Voor alle stellingen geldt daardoor: hoe hoger de score, hoe veiliger het gedrag.

### *5.3.5. Omgaan met bijlagen en hyperlinks in e-mails*

*Zelf-gerapporteerd gedrag*

Ook op het gebied van omgaan met bijlagen en hyperlinks in e-mails rapporteren respondenten zowel veilig als onveilig gedrag (tabel 20). Zo verwijderen respondenten e-mails die zij niet vertrouwen gemiddeld vaak tot altijd (G=4.74) en openen zij gemiddeld zelden tot nooit bijlagen in e-mails van onbekende afzenders (G=4.62). Wanneer respondenten twijfelen over de echtheid van een e-mail, nemen zij daarentegen gemiddeld zelden (2) tot soms (3) contact op met de afzender om te vragen of er daadwerkelijk een e-mail naar hen verstuurd is (G=2.46).

*Tabel 20. Beschrijving zelf-gerapporteerd gedrag: omgaan met bijlagen en hyperlinks in e-mails*

| **Stelling (schaal 1-5, hoe hoger de score hoe veiliger het gedrag)** | **N** | **Gemiddelde** | **S.D.** |
|---|---|---|---|
| Ik verwijder e-mails die ik niet vertrouw direct | 2414 | 4.74 | 1.02 |
| Wanneer ik twijfel over de echtheid van een e-mail, neem ik contact op met de afzender om te vragen of er daadwerkelijk een e-mail naar mij is verstuurd | 2324 | 2.46 | 1.20 |
| Ik open bijlagen in e-mails, ook als de e-mail afkomstig is van een onbekende afzender (O) [39] | 2418 | 4.62 | 0.59 |

*Vignetten*

Respondenten zijn drie vignetten voorgelegd in willekeurige volgorde (zie paragraaf 4.3.1 voor een verdere beschrijving van de vignetten). We bespreken nu de drie vignetten (tabel 21). Bij één phishing vignet, het Rabobank phishing vignet, werd aangegeven dat de ontvanger van de mail (Robin de Vries) al enige tijd een betaalrekening heeft bij de Rabobank. In totaal gaf 8,9 procent aan op de hyperlink te klikken, dan wel deze te kopiëren naar een internetbrowser of over te typen in een internetbrowser (niet in tabel). Bij het andere phishing vignet, het Armin van Buuren phishing vignet, werd aangegeven dat Robin de Vries fan is van Armin van Buuren en woonachtig is in de omgeving van Leiden. Bij dit vignet lag het percentage dat als “Robin de Vries” op de hyperlink te klikken (of kopiëren of overtypen) hoger: 15,2 procent van de respondenten (niet in tabel). Bij het legitieme vignet, het KPN legitieme vignet, was de introductietekst “Robin is klant bij KPN. Robin vindt het van belang om op de hoogte te blijven over

[39] (O)= score van de stelling is omgedraaid. Voor alle stellingen geldt daardoor: hoe hoger de score, hoe veiliger het gedrag.

ontwikkelingen en actualiteiten op het gebied van online veiligheid. Vooral informatie over hoe Robin zichzelf beter kan beschermen, is interessant." Op basis van deze introductie klikte 22,8 procent van de respondenten op de hyperlink in de e-mail (of zou deze kopiëren of overtypen) (niet in tabel). Wanneer de twee phishing vignetten (Rabobank en Armin van Buuren) worden samengenomen blijkt dat 21,2 procent van de respondenten bij tenminste één van deze twee vignetten een onveilige keuze heeft gemaakt door op de hyperlink te klikken (of deze te kopiëren of over te typen).

*Tabel 21. Vignetten e-mails*

| | **N** | **%** |
|---|---|---|
| Onveilige keuze (tenminste 1x op phishing hyperlink geklikt) | 515 | 21,2% |
| Veilige keuze (2x niet op phishing hyperlink geklikt) | 1911 | 78,8% |

Voor de volledigheid staan in bijlage 4 alle cybergedragingen die zijn gemeten weergegeven.

### *5.3.6. Samenhang tussen cybergedragingen*

In tabel 22 zijn de correlaties tussen de diverse vormen van cybergedrag – de afhankelijke variabelen van dit rapport – weergegeven. Er zijn verschillende zaken die opvallen. Ten eerste is opvallend dat, hoewel er zeker correlaties tussen verschillende gedragingen aanwezig zijn, alle correlaties zeer klein zijn (kleiner dan r=.2, terwijl de correlatie minimaal .3 dient te zijn om te kunnen spreken van een kleine samenhang) en dat daarmee geen van deze correlaties een noemenswaardige grootte heeft (zie tabel 22). Ten tweede valt op dat mate van veiligheid van zelf-gerapporteerd gedrag niet gerelateerd is aan twee van de objectieve metingen van veiligheid van cybergedrag (wachtwoord sterkte en klikgedrag) en slechts zeer beperkt is gerelateerd aan de andere twee objectieve metingen, e-mail keuze (r = 0.07**) en delen van persoonlijke gegevens (r = 0.11***). Ten derde zijn ook de daadwerkelijke cybergedragingen niet of beperkt aan elkaar gerelateerd.

Het nagenoeg ontbreken van samenhang tussen de verschillende cybergedragingen wijst erop dat respondenten per type cybergedrag een andere mate van veiligheid laten zien. Oftewel; wanneer iemand veilig gedrag laat zien met betrekking tot het omgaan met een phishing mail, betekent dit niet dat zij zich gemiddeld ook veilig zullen gedragen op het gebied van het kiezen van een sterk wachtwoord. Wachtwoord sterkte heeft zelfs een (zeer kleine) negatieve samenhang met het delen van persoonlijke gegevens (r = -0.111***), wat erop wijst dat hoe sterker het wachtwoord is dat respondenten kiezen, hoe onveiliger zij zich gedragen bij het invullen van persoonlijke gegevens.

*Tabel 22. Correlatietabel afhankelijke variabelen*

| | Zelf-gerapporteerd gedrag | Wachtwoord sterkte | Klikgedrag | E-mail keuze |
|---|---|---|---|---|
| **Wachtwoord sterkte** | -.039 | | | |
| **Klikgedrag** | -.029 | .019 | | |
| **E-mail keuze** | .067** | .000 | .059** | |
| **Delen persoonlijke gegevens** | .110*** | -.111*** | .096*** | .075*** |

### *5.3.7. Resumé beschrijving van cybergedrag*

In paragraaf 5.3. zijn resultaten beschreven voor alle zeven cybergedragingen die zijn meegenomen in deze studie. Alle gedragingen zijn uitgevraagd via zelfrapportage. Van alle zeven gedragsclusters rapporteren respondenten gemiddeld het minst veilige gedrag omtrent opslaan van bestanden. Voor drie van deze gedragingen zijn ook objectieve metingen gedaan. Ruim 89 procent van de respondenten blijkt een zwak wachtwoord te kiezen voor het beveiligen van hun persoonlijke informatie. Een groot deel van de respondenten (40,4%) maakt bovendien een onveilige keuze bij het downloaden van software en gaat onveilig om met het delen van persoonlijke informatie. Opvallend is het resultaat dat de objectieve metingen niet overeenkomen met de zelf-gerapporteerde metingen van gedrag. Zelf-gerapporteerd gedrag is structureel veiliger dan daadwerkelijk gedrag.

## ***5.4. Verklaringen van cybergedrag***

Uit de voorgaande paragrafen blijkt hoe veilig of onveilig Nederlanders zich online (denken te) gedragen. Om te komen tot interventies die leiden tot gedragsverandering (i.e. veiliger gedrag) is echter inzicht nodig in de factoren die samenhangen met dat gedag. Hieronder bespreken we dan ook hoe de verschillende typen cybergedrag kunnen worden verklaard.

### *5.4.1. Verklaringen voor zelf-gerapporteerd cybergedrag*

Welke factoren hangen samen met veilig zelf-gerapporteerd cybergedrag? In tabel 23 worden de samenhangen tussen diverse onafhankelijke variabelen en zelf-gerapporteerd cybergedrag geschat, waarbij de zeven gedragsclusters zijn samengenomen tot één afhankelijke variabele. Diverse onafhankelijke variabelen hangen significant samen met zelf-gerapporteerd cybergedrag. Ten eerste is

een significant positief verband gevonden voor alle factoren uit het COM-B model. Hoe meer kennis (b= 0.059, p<.001), sociale gelegenheid (b= 0.039, p<.01) en motivatie (b= 0.153, p<.001) respondenten hebben, hoe veiliger hun zelf-gerapporteerde cybergedrag. Alleen materiële gelegenheid hangt niet significant samen met zelf-gerapporteerd cybergedrag.

Bovendien blijken enkele van de overige onafhankelijke variabelen significant gerelateerd te zijn aan zelf-gerapporteerd cybergedrag. Een negatieve gemoedstoestand hangt negatief samen met zelf-gerapporteerd veilig cybergedrag (b= -0.052, p<.01); hoe groter de negatieve gemoedstoestand van respondenten, hoe minder veilig hun (zelf-gerapporteerde) cybergedrag is. Een positieve gemoedstoestand hangt daarentegen positief samen met de veiligheid van zelf-gerapporteerd cybergedrag (b= 0.042, p<.01). Ook zelfcontrole hangt significant samen met zelf-gerapporteerd cybergedrag (b= 0.119, p<.001). Hoe meer zelfcontrole respondenten hebben, hoe veiliger hun (zelf-gerapporteerde) cybergedrag is. Tot slot is één van de controle variabelen significant gerelateerd aan zelf-gerapporteerd cybergedrag. Hoe hoger de leeftijd, hoe veiliger het cybergedrag (b= 0.004, p<.001).

Samengenomen lijken de meeste van de, uit de literatuur naar voren gekomen, onafhankelijke variabelen van invloed te zijn op de veiligheid van zelf-gerapporteerd cybergedrag. Samen verklaren de factoren in tabel 23 26,9 procent van de variatie in veiligheid van dit gedrag. Uiteraard is zelf-gerapporteerd gedrag niet hetzelfde als daadwerkelijk gedrag. In de volgende paragrafen kijken we daarom naar verklarende factoren voor daadwerkelijk gedrag.

*Tabel 23. Multivariaat OLS regressiemodel voor zelf-gerapporteerd gedrag*

| | | **b** | **S.E.** | **Beta** | **sign** |
|---|---|---|---|---|---|
| | | *ongestan-daardiseerd* | | *gestan-daardiseerd* | |
| *Onafhankelijke variabelen* | | | | | |
| Kennis | score op kennistest | 0.059 | 0.003 | 0.439 | *** |
| Gelegenheid | sociaal | 0.039 | 0.014 | 0.053 | ** |
| | materieel | -0.003 | 0.011 | -0.005 | |
| Motivatie | | 0.153 | 0.017 | 0.179 | *** |
| Negatieve gemoedstoestand | | -0.052 | 0.020 | -0.049 | ** |
| Positieve gemoedstoestand | | 0.042 | 0.013 | 0.060 | ** |

| | | | | | |
|---|---|---|---|---|---|
| Angst voor slachtofferschap | | -0.020 | 0.013 | -0.029 | |
| Eerder slachtofferschap | ja | 0.000 | 0.018 | 0.000 | |
| Zelfcontrole | | 0.119 | 0.016 | 0.143 | *** |
| Type apparaat | smartphone | -0.002 | 0.031 | -0.001 | |
| | pc/laptop | 0.041 | 0.023 | 0.039 | |
| | tablet (ref) | | | | |
| | | | | | |
| *Controle variabelen* | | | | | |
| Geslacht | man | 0.012 | 0.019 | 0.012 | |
| Opleiding | | -0.016 | 0.006 | -0.049 | |
| Leeftijd | jaren | 0.004 | 0.001 | 0.113 | *** |
| Werkend | ja | -0.026 | 0.020 | -0.026 | |
| Samenwonend | ja | 0.004 | 0.020 | 0.003 | |
| Inwonend kind | aantal <16 jaar | 0.013 | 0.014 | 0.018 | |
| Constant | | 1.741 | 0.118 | | *** |
| R2 | | .269 | | | |

* p<.05, **p<.01, ***p<.001

### *5.4.2. Verklaringen voor wachtwoord sterkte*

Voor diverse van de gedragsclusters zijn aanvullende analyses uitgevoerd op basis van objectieve metingen. Tabel 24 schat de effecten van diverse onafhankelijke variabelen op een objectieve cybergedraging: wachtwoord sterkte. Welke factoren hangen samen met de sterkte van het wachtwoord dat respondenten kiezen? Een eerste opvallend resultaat is dat kennis negatief gerelateerd is aan wachtwoord sterkte (b= -0.064, p<.001). Dit wijst erop dat hoe meer kennis mensen hebben van online veiligheid, hoe minder sterk het wachtwoord is dat zij kiezen. De sterkte van het gekozen wachtwoord hangt niet significant samen met de (sociale of materiële) gelegenheid of motivatie die respondenten hebben voor veilig cybergedrag.

Drie overige onafhankelijke variabelen blijken ook van invloed te zijn. Hoe groter de positieve gemoedstoestand van respondenten, hoe sterker het gekozen wachtwoord is (b= 0.155, p<.01). Ook angst voor slachtofferschap hangt significant samen met wachtwoord sterkte; hoe meer angst respondenten hebben om slachtoffer te worden van online criminaliteit, hoe sterker het door hen gekozen wachtwoord is (b= 0.142, p<.05). Tot slot blijken respondenten die een pc of laptop gebruiken, een minder sterk

wachtwoord te kiezen dan respondenten die de vragenlijst op een tablet invulden (b= -0.242, p<.05). Daarnaast kiezen respondenten een minder sterk wachtwoord wanneer zij een hogere opleiding hebben (b= -0.082, p<.01) of werken (b= -0.204, p<.05).

Samengenomen lijken de uit de literatuur naar voren gekomen verklarende factoren zeer beperkt van invloed te zijn op de objectieve gedraging "sterkte gekozen wachtwoord". Samen verklaren de factoren in het model slechts 5,5 procent van de variatie in sterkte van het gekozen wachtwoord.

*Tabel 24. Multivariaat OLS regressiemodel voor wachtwoord sterkte*

| | | **b** | **S.E.** | **Beta** | **sign** |
|---|---|---|---|---|---|
| | | *ongestan-daardiseerd* | | *gestan-daardiseerd* | |
| *Onafhankelijke variabelen* | | | | | |
| Kennis | score op kennistest | -0.064 | 0.013 | -0.120 | *** |
| Gelegenheid | sociaal | 0.059 | 0.063 | 0.020 | |
| | materieel | 0.072 | 0.050 | 0.031 | |
| Motivatie | | 0.051 | 0.076 | 0.015 | |
| Negatieve gemoedstoestand | | 0.132 | 0.090 | 0.031 | |
| Positieve gemoedstoestand | | 0.155 | 0.060 | 0.055 | ** |
| Angst voor slachtofferschap | | 0.142 | 0.057 | 0.053 | * |
| Eerder slachtofferschap | ja | 0.022 | 0.082 | 0.006 | |
| Zelfcontrole | | 0.140 | 0.072 | 0.042 | |
| Type apparaat | smartphone | 0.047 | 0.140 | 0.009 | |
| | pc/laptop | -0.242 | 0.105 | -0.059 | * |
| | tablet (ref) | | | | |
| | | | | | |
| *Controle variabelen* | | | | | |
| Geslacht | man | 0.084 | 0.087 | 0.021 | |
| Opleiding | | -0.082 | 0.029 | -0.062 | ** |
| Leeftijd | jaren | 0.004 | 0.004 | 0.029 | |
| Werkend | ja | -0.204 | 0.092 | -0.052 | * |

| | | | | | |
|---|---|---|---|---|---|
| Samenwonend | ja | -0.084 | 0.088 | -0.020 | |
| Inwonend kind | aantal <16 jaar | 0.053 | 0.065 | 0.018 | |
| Constant | | 5.485 | 0.534 | | *** |
| R2 | | .055 | | | |

### *5.4.3. Verklaringen voor klikgedrag*

In tabel 25 zijn in logistische regressiemodellen de effecten geschat van diverse verklaringen op de keuze die respondenten hebben gemaakt bij de software pop-up; de onveilige keuze (ja klikken) of veilige keuze (geen ja klikken). Opvallend is dat, net als bij de verklaring van wachtwoord sterkte, kennis negatief samenhangt met klikgedrag (b= -0.057, p<.001). Voor elke punt die respondenten hoger scoren op de kennistest, wordt de kans zes procent minder groot[40] dat zij een veilige keuze maken bij de software pop-up (OR (odds ratio) = 0.944). Net als bij de verklaring van wachtwoord sterkte, hangen de andere COM-B factoren (gelegenheid en motivatie) niet samen met klikgedrag.

Drie andere onafhankelijke variabelen hebben wel een significant verband met klikgedrag. Hoe groter de positieve gemoedstoestand van respondenten, hoe groter de kans is dat zij een onveilige keuze maken bij de software pop-up (b= -0.146, p<.05, OR = 0.864). Opvallend is dat respondenten die ooit eerder slachtoffer zijn geworden van online criminaliteit, significant minder vaak een veilige keuze maken bij de software pop-up (b= -0.227, p<.05, OR=0.797). Ook lijkt klikgedrag samen te hangen met schermgrootte; respondenten met een pc of laptop maken minder vaak een veilige keuze maken dan tablet-gebruikers (b= -0.490, p<.001, OR=0.613).

Een extra onafhankelijke variabele is tijdsdruk, die is opgelegd door de onderzoekers aan de helft van de respondenten. Wanneer we vergelijken of respondenten een veilige of onveilige keuze maken wanneer zij onder tijdsdruk werken, vergeleken met een controlegroep die geen tijdsdruk is opgelegd, dan is geen significant verschil gevonden.

Wel hangt het klikgedrag, tot slot, samen met verschillende controle variabelen. Mannen (b= -0.263, p<.01). en werkenden (b= -0.340, p<.001) maken significant minder vaak een veilige keuze bij de software pop-up. Respondenten die samenwonen maken juist vaker een veilige keuze (b= 0.216, p<.05).

Samengenomen lijken de uit de literatuur naar voren gekomen verklarende factoren beperkt van invloed te zijn op de daadwerkelijk klikgedrag. Samen verklaren de factoren in dit model slechts 8,1 procent van de variatie in de veiligheid van het klikgedrag.

[40] Feitelijk betreft dit een 6% minder grote odds.

*Tabel 25. Logistisch regressiemodel voor klikgedrag*

| | | B | S.E. | OR | sign |
|---|---|---|---|---|---|
| | | | | *Exp(B)* | |
| *Onafhankelijke variabelen* | | | | | |
| Kennis | score op kennistest | -0.057 | 0.014 | 0.944 | *** |
| Gelegenheid | sociaal | 0.088 | 0.068 | 1.092 | |
| | materieel | -0.067 | 0.055 | 0.935 | |
| Motivatie | | 0.089 | 0.083 | 1.093 | |
| Negatieve gemoedstoestand | | 0.025 | 0.099 | 1.026 | |
| Positieve gemoedstoestand | | -0.146 | 0.066 | 0.864 | * |
| Angst voor slachtofferschap | | -0.068 | 0.063 | 0.935 | |
| Eerder slachtofferschap | ja | -0.227 | 0.088 | 0.797 | * |
| Zelfcontrole | | 0.008 | 0.078 | 1.008 | |
| Type apparaat | smartphone | 0.311 | 0.161 | 1.364 | |
| | pc/laptop | -0.490 | 0.116 | 0.613 | *** |
| | tablet (ref) | | | | |
| Tijdsdruk | opgelegd | -0.059 | 0.086 | 0.943 | |
| | | | | | |
| *Controle variabelen* | | | | | |
| Geslacht | man | -0.263 | 0.094 | 0.769 | ** |
| Opleiding | | 0.016 | 0.031 | 1.016 | |
| Leeftijd | jaren | 0.000 | 0.004 | 1.000 | |
| Werkend | ja | -0.340 | 0.100 | 0.712 | *** |
| Samenwonend | ja | 0.216 | 0.096 | 1.241 | * |
| Inwonend kind | aantal <16 jaar | -0.044 | 0.071 | 0.957 | |
| | | | | | |
| R2 (Nagelkerke) | | .081 | | | |

### *5.4.4. Verklaringen voor e-mail keuze*

Welke factoren kunnen de keuze verklaren om niet op een phishing hyperlink te klikken? In tabel 26 zijn de effecten geschat van verklarende en controle variabelen op de keuze die respondenten hebben gemaakt bij de e-mail vignetten. Geen van de COM-B factoren (kennis, gelegenheid en motivatie) hangt significant samen met de keuze die respondenten maken bij het omgaan met hyperlinks in phishing e-mails.

Een verklarende factor die significant gerelateerd is aan het maken van een veilige keuze is zelfcontrole (b= 0.383, p<.001, OR = 1.467). Hoe meer zelfcontrole respondenten hebben, hoe groter de kans dat zij een veilige keuze maken (niet op de phishing hyperlink te klikken noch de hyperlink over te typen of kopiëren). Bovendien maken respondenten die een groter scherm (pc of laptop) gebruiken, minder vaak een veilige keuze dan respondenten met een tablet (b= -0.417, p<.01).

Tot slot hangen drie controle variabelen samen met de e-mail keuze. Hoe ouder respondenten zijn, hoe groter de kans is op een veilige keuze (b= 0.013, p<.01, OR = 1.013). Voor elk inwonend kind dat respondenten hebben, jonger dan 16 jaar, is de kans op het maken van een veilige keuze juist kleiner (b= -0.162, p<.05, OR = 0.850). De verklaarde variantie van de, uit de literatuur naar voren gekomen, onafhankelijke variabelen is echter laag, namelijk 4,0 procent.

*Tabel 26. Logistisch regressiemodel voor e-mail keuze*

| | | **B** | **S.E.** | **OR** | **sign** |
|---|---|---|---|---|---|
| | | | | *Exp(B)* | |
| *Onafhankelijke variabelen* | | | | | |
| Kennis | score op kennistest | 0.000 | 0.016 | 1.000 | |
| Gelegenheid | sociaal | -0.093 | 0.081 | 0.912 | |
| | materieel | 0.023 | 0.064 | 1.023 | |
| Motivatie | | -0.031 | 0.097 | 0.969 | |
| Negatieve gemoedstoestand | | -0.076 | 0.111 | 0.927 | |
| Positieve gemoedstoestand | | 0.060 | 0.076 | 1.062 | |
| Angst voor slachtofferschap | | -0.043 | 0.074 | 0.958 | |
| Eerder slachtofferschap | ja | 0.003 | 0.105 | 1.003 | |
| Zelfcontrole | | 0.383 | 0.092 | 1.467 | *** |

| | | | | | |
|---|---|---|---|---|---|
| Type apparaat | smartphone | 0.024 | 0.192 | 1.024 | |
| | pc/laptop | -0.417 | 0.145 | 0.659 | ** |
| | tablet (ref) | | | | |
| | | | | | |
| *Controle variabelen* | | | | | |
| Geslacht | man | 0.062 | 0.111 | 1.064 | |
| Opleiding | | 0.005 | 0.037 | 1.005 | |
| Leeftijd | jaren | 0.013 | 0.005 | 1.013 | ** |
| Werkend | ja | 0.046 | 0.116 | 1.047 | |
| Samenwonend | ja | -0.032 | 0.113 | 0.969 | |
| Inwonend kind | aantal <16 jaar | -0.162 | 0.076 | 0.850 | * |
| | | | | | |
| R2 (Nagelkerke) | | .040 | | | |

### *5.4.5. Verklaringen voor delen persoonlijke gegevens*

Tabel 27 schat de effecten van diverse onafhankelijke variabelen op een objectieve cybergedraging: delen van persoonlijke gegevens. Welke factoren hangen samen met het delen van persoonlijke gegevens, zoals een e-mailadres of bankrekeningnummer? Twee verklarende factoren lijken een beschermende functie te hebben voor het delen van persoonlijke gegevens. Hoe meer kennis respondenten hebben van online veiligheid, hoe minder persoonlijke gegevens zij met de onderzoekers delen, oftewel hoe veiliger hun cybergedrag is op het gebied van het delen van persoonlijke gegevens (b= 0.013, p<0.001). Ook het hebben van een hogere opleiding hangt samen met het delen van minder persoonlijke gegevens (b= 0.015, p<0.01).

Verschillende andere variabelen hangen echter samen met het delen van *meer* persoonlijke gegevens. Hoe groter de positieve gemoedstoestand van respondenten, hoe meer persoonlijke gegevens zij delen, oftewel hoe onveiliger hun cybergedrag is op het gebied van het delen van persoonlijke gegevens (b= -0.032, p<0.05). Daarnaast delen respondenten die de vragenlijst op een groter scherm hebben ingevuld (pc of laptop) vergeleken met tablet-gebruikers meer persoonlijke gegevens (b= -0.071, p<0.01). Ook zijn enkele controle variabelen positief gerelateerd aan het delen van persoonlijke gegevens. Zo delen mannen meer persoonlijke gegevens (b= -0.061, p<0.01). Ook is leeftijd positief gerelateerd aan het delen van persoonlijke gegevens; hoe ouder de deelnemer, hoe meer persoonlijke gegevens zijn gedeeld (b= -0.003, p<0.01).

Het experiment met verleidingstechnieken, waarbij onderzocht is of respondenten meer persoonlijke informatie delen wanneer ze blootgesteld worden aan een introductie die bedoeld is om de respondenten te "verleiden" tot het delen van persoonlijke informatie, heeft laten zien dat het gebruiken van de verleidingstechniek "wederkerigheid" ertoe lijdt dat respondenten meer persoonlijke gegevens delen dan wanneer er geen verleidingstechniek wordt gebruikt (b= -0.050, p<0.05). Dit wijst erop dat mensen eerder bereid zijn hun persoonlijke gegevens met derden te delen als ze hier iets voor terug krijgen (in dit geval, kans op een cadeaubon).

*Tabel 27. Poisson regressiemodel voor het delen van persoonlijke gegevens*

| | | B | S.E. | IRR | sign |
|---|---|---|---|---|---|
| *Onafhankelijke variabelen* | | | | | |
| Kennis | score op kennistest | 0.013 | 0.003 | 1.013 | *** |
| Gelegenheid | sociaal | 0.005 | 0.014 | 1.005 | |
| | materieel | -0.003 | 0.011 | 0.997 | |
| Motivatie | | 0.019 | 0.017 | 1.019 | |
| Negatieve gemoedstoestand | | 0.002 | 0.020 | 1.002 | |
| Positieve gemoedstoestand | | -0.032 | 0.013 | 0.969 | * |
| Angst voor slachtofferschap | | 0.023 | 0.013 | 1.024 | |
| Eerder slachtofferschap | ja | -0.018 | 0.018 | 0.983 | |
| Zelfcontrole | | 0.018 | 0.016 | 1.018 | |
| Type apparaat | smartphone | -0.040 | 0.030 | 0.961 | |
| | pc/laptop | -0.071 | 0.023 | 0.931 | ** |
| | tablet (ref) | | | | |
| Verleidingstechniek | wederkerigheid | -0.050 | 0.021 | 0.952 | * |
| | autoriteit | -0.024 | 0.021 | 0.976 | |
| | geen (ref) | | | | |
| | | | | | |
| *Controle variabelen* | | | | | |
| Geslacht | man | -0.061 | 0.019 | 0.941 | ** |
| Opleiding | | 0.015 | 0.006 | 1.015 | * |

| | | | | | |
|---|---|---|---|---|---|
| Leeftijd | jaren | -0.003 | 0.001 | 0.997 | ** |
| Werkend | ja | 0.023 | 0.020 | 0.023 | |
| Samenwonend | ja | 0.036 | 0.020 | 1.036 | |
| Inwonend kind | aantal <16 jaar | -0.006 | 0.014 | 0.994 | |
| | | | | | |
| R2 (Pseudo) | | .013 | | | |

#### *5.4.6. Resumé verklaringen cybergedrag*

Voor diverse factoren is gekeken in welke mate ze samenhangen met zelf-gerapporteerd en daadwerkelijk cybergedrag. Samengenomen lijken de meeste van de uit de literatuur naar voren gekomen verklarende factoren van invloed te zijn op de veiligheid van (zelf-gerapporteerd) cybergedrag. Onder andere kennis, gelegenheid en motivatie verklaren de mate waarin mensen *zeggen* zich veilig te gedragen.

Wanneer we kijken naar daadwerkelijk cybergedrag, onderzocht met behulp van objectieve metingen, ontstaat echter een ander beeld. Samengenomen lijken de uit de literatuur naar voren gekomen verklarende factoren beperkt tot zeer beperkt van invloed te zijn op het objectieve gedrag van burgers, te weten wachtwoord sterkte, klikgedrag en delen persoonlijke gegevens. Zo hangt de veiligheid van daadwerkelijk cybergedrag niet samen met gelegenheid en motivatie en is het verband tussen kennis en daadwerkelijk cybergedrag meermaals negatief: meer kennis van online veiligheid hangt samen met meer onveilig cybergedrag.

### *5.5. Aanvullende verklaringen van cybergedrag*

#### *5.5.1. Dreiging- en maatregelevaluatie en locus of control*

Naast de hoofdeffecten van kennis, gelegenheid en motivatie op cybergedragingen, onderzoeken we ook de mogelijke effecten van aanvullende verklarende factoren. Het betreft dreiging-evaluatie, maatregel-evaluatie en locus of control (zie paragraaf 3.4.1.). De resultaten onderschrijven ten eerste de verwachting van de Protection Motivation Theory (PMT) dat 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 (b= 0.421, p<.001), maatregel-evaluatie (b= 0.151, p<.001) en locus of control (b= 0.105, p<.001) hebben een positieve significante samenhang met de motivatie tot online zelfbescherming (niet in tabel).

PMT verwacht vervolgens dat deze motivatie de veiligheid van cybergedrag beïnvloedt. Zoals in eerdere paragrafen is uiteengezet, ondersteunen de resultaten van dit rapport die verwachting niet. Onderzocht is dan ook of dreiging-evaluatie, maatregel-evaluatie en locus of control mogelijk samenhangen met de veiligheid van cybergedrag (tabel 28). Dit is echter zeer beperkt het geval. Het enige significante verband dat gevonden is, betreft een verband tussen maatregel-evaluatie en de veiligheid van zelf-gerapporteerd cybergedrag (Model I). Wanneer respondenten vinden dat maatregelen voor online veiligheid effectief zijn, zij zelf in staat zijn die maatregelen te nemen en de kosten van deze maatregelen niet te hoog zijn (samengenomen: maatregel-evaluatie), dan rapporteren zij meer veilig cybergedrag (b= 0.469, p<0.001). Zowel dreiging-evaluatie als locus of control hangen echter niet significant samen met de veiligheid van zelf-gerapporteerd cybergedrag.

Er zijn echter geen significante verbanden gevonden tusen dreiging-evaluatie, maatregel-evaluatie en locus of control en de veiligheid van de overige cybergedragingen. Model II toont de verbanden tussen dreiging-evaluatie, maatregel-evaluatie en locus of control en wachtwoord-sterkte. Alle verbanden zijn niet significant en de verklaarde variantie van het totale model (ten opzichte van tabel 24) is nauwelijks (0,1%) toegenomen. Model III geeft weer dat ook voor de objectieve cybergedraging "klikgedrag" (het wel of niet downloaden van software) dreiging-evaluatie, maatregel-evaluatie en locus of control geen significante verklaring bieden. De verklarende variantie van het totale model is niet toegenomen ten opzichte van tabel 25. Model IV toont eenzelfde beeld voor de vignet-meting waarbij is gemeten hoe respondenten omgaan met hyperlinks in phishing e-mails. Zowel dreiging-evaluatie, maatregel-evaluatie als locus of control hebben geen significante samenhang met de e-mail keuze. De verklaarde variantie is ook slechts 0,1 procent toegenomen ten opzichte van tabel 26. Tot slot toont Model V (tabel 28) aan dat ook het delen van persoonlijke gegevens niet samenhangt met dreiging-evaluatie, maatregel-evaluatie of locus of control. Ook de verklaarde variantie is onveranderd gebleven ten opzichte van tabel 27.

### *5.5.2. Interactie effecten*

Nu de samenhang tussen kennis, gelegenheid, motivatie en diverse cybergedragingen is beschreven, zal worden onderzocht of deze hoofdeffecten afhangen van andere omstandigheden. Bijvoorbeeld: hangt de samenhang tussen kennis en cybergedrag af van de gemoedstoestand? Voor het toetsen van mogelijke interactie-effecten zijn additionele analyses uitgevoerd, waarin gebruik is gemaakt van gecentraliseerde variabelen (niet in tabel weergegeven).

*Tabel 28. Regressiemodellen voor de samenhang tussen dreigingsevaluatie, maatregelevaluatie, locus of control en alle cybergedragingen*

| | *Model I* | | | *Model II* | | | *Model III* | | | *Model IV* | | | *Model V* | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Zelf-gerapporteerd cybergedrag[a]** | | | **Wachtwoord sterkte[a]** | | | **Klikgedrag[b]** | | | **E-mail keuze[b]** | | | **Delen van persoonlijke gegevens[c]** | | |
| | **b** | **S.E.** | **sign** | **b** | **S.E.** | **sign** | **B** | **S.E.** | **sign** | **B** | **S.E.** | **sign** | **B** | **S.E.** | **sign** |
| DE | 0.015 | 0.021 | | 0.024 | 0.105 | | -0.062 | 0.115 | | 0.029 | 0.135 | | 0.045 | 0.023 | |
| ME | 0.510 | 0.022 | *** | -0.066 | 0.112 | | -0.038 | 0.122 | | -0.041 | 0.143 | | 0.029 | 0.025 | |
| LC | -0.014 | 0.013 | | 0.087 | 0.063 | | 0.004 | 0.070 | | 0.017 | 0.082 | | -0.026 | 0.014 | |
| R2 | .403 | | | .055 | | | .081 | | | .040 | | | .013 | | |

DE = dreigingsevaluatie, ME = maatregelevaluatie, LC= locus of control

* p<.05, **p<.01, ***p<.001

[a] Multivariaat OLS regressiemodel

[b] Logistisch regressiemodel

[c] Poisson regressiemodel

NB: In modellen analyses is gecontroleerd voor de effecten van kennis, sociale gelegenheid, materiële gelegenheid, motivatie, negatieve gemoedstoestand, positieve gemoedstoestand, angst voor slachtofferschap, eerder slachtofferschap, zelfcontrole, type apparaat en alle controle variabelen (geslacht, opleiding etc.).

In totaal is er voor alle afhankelijke variabelen (zelf-gerapporteerd cybergedrag, klikgedrag, wachtwoord sterkte, e-mail keuze en het online delen van persoonlijke gegevens) onderzocht of de verbanden met kennis, gelegenheid en motivatie verklaard kunnen worden door interacties van deze variabelen met de volgende factoren: negatieve gemoedstoestand, positieve gemoedstoestand, angst voor slachtofferschap, slachtofferschap (ooit) en zelfcontrole. Het merendeel van deze interacties bleek niet significant te 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[41].

Wat betreft *kennis* werd er enkel bij de meting van daadwerkelijk klikgedrag een (negatief) interactie-effect gevonden tussen zelfcontrole en kennis (b=-0.047, p<0.05, niet in tabel). Om deze interactie te kunnen interpreteren is gebruik gemaakt van zogenaamde *simple slopes*.[42] Deze geven weer dat het verband tussen kennis en de veiligheid van klikgedrag bij een gemiddelde zelfcontrole (score 3 op de schaal van 1 op 5) zwak negatief is b=-0.007. Wanneer respondenten echter een hogere mate van zelfcontrole hebben wordt dit negatieve verband sterker: bij een hoge zelfcontrole (score 4) is het verband b=-0.017, en bij een zeer hoge zelfcontrole (score 5) wordt het b=-0.027. Kortom, naarmate de zelfcontrole toeneemt wordt het verband tussen kennis en de veiligheid van klikgedrag significant sterker negatief.

Drie significante interacties zijn er gevonden met *materiële gelegenheid*. Allereerst blijkt dat er bij de veiligheid van zelf-gerapporteerd cybergedrag een negatief interactie-effect bestaat tussen materi*ë*le gelegenheid en angst voor slachtofferschap (b= -0.025, p<0.05, niet in tabel). Uit de simple slopes blijkt dat er bij een gemiddelde angst voor slachtofferschap (score 3 op de schaal van 1-5) een zwak negatief verband is (b=-0.004), wat sterker negatief wordt bij een grote (b=-0.029) of zeer grote (b=-0.054) angst voor slachtofferschap. Dit toont dus aan dat naarmate men meer angst voor slachtofferschap heeft, het verband tussen materi*ë*le gelegenheid en de veiligheid van zelf-gerapporteerd cybergedrag sterker negatief wordt.

[41] In enkele gevallen wordt er ook een significante interactie gevonden met een variabele waarvan in de eerdere analyses nog geen significant verband met cybergedrag wordt gevonden. Er kan hierbij sprake zijn van differentiële effecten, waarbij voor een deel van de steekproef (bijv. respondenten die ooit slachtoffer zijn geworden) een positief verband wordt gevonden, terwijl voor een ander deel (bijv. de niet-slachtoffers) een negatief verband wordt gevonden. Dit kan leiden tot een niet-significant verband in de oorspronkelijke analyses, terwijl de differentiële effecten pas zichtbaar worden met de interactie.

[42] Simple slopes geven het verband tussen de afhankelijke variabele (hier: klikgedrag) en onafhankelijke variabele (kennis) weer wanneer de moderator variabele (zelfcontrole) constant blijft.

Daarnaast wordt er significante negatieve interactie gevonden tussen materiële gelegenheid en zelfcontrole bij het voorspellen van de wachtwoord sterkte (b=-0.172, p<.05). Uit de simple slopes blijkt dat er voor respondenten met een zeer lage mate van zelfcontrole (score 1 op de schaal van 1-5) nog een positief verband is tussen materiële gelegenheid en wachtwoord sterkte (b=0.518). Dit positieve verband wordt echter minder sterk wanneer de mate van zelfcontrole toeneemt: bij een gemiddelde zelfcontrole is het verband nog maar b=0.174 en bij een zeer hoge zelfcontrole wordt het zelfs negatief (b=-0.169).

Tot slot werd er bij de analyses naar een veilige e-mail keuze een significant positief interactie-effect gevonden tussen materiële gelegenheid en eerder slachtofferschap (b=0.265, p<.05). Uit de simple slopes blijkt dat er onder respondenten die nooit eerder slachtoffer zijn geweest een negatief verband wordt gevonden tussen materiële gelegenheid en een veilige e-mail keuze (b=-0.020), terwijl dit verband juist positief is voor de respondenten die wel ooit slachtoffer zijn geweest (b=0.023).

De interacties met *sociale gelegenheid* bleken in twee gevallen significant te zijn. Ten eerste werd er een significante interactie gevonden tussen sociale gelegenheid en angst voor slachtofferschap in het verklaren van zelf-gerapporteerd cybergedrag (b=-0.043, p<.01). Uit deze interactie blijkt dat onder respondenten met zeer weinig angst voor slachtofferschap het verband tussen sociale gelegenheid en de veiligheid van zelf-gerapporteerd cybergedrag positief is (b=0.122). Naarmate de angst voor slachtofferschap toeneemt, wordt dit verband echter telkens zwakker. Bij respondenten met veel (b=-0.005) of zeer veel (b=-0.048) angst voor slachtofferschap is het verband zelfs negatief: zij rapporteren dus minder veilig gedrag wanneer de sociale gelegenheid toeneemt.

Uit de analyses naar wachtwoord sterkte blijkt daarnaast een significante negatieve interactie tussen sociale gelegenheid en een negatieve gemoedstoestand (b=-0.354, p<.01). De simple slopes tonen aan dat er onder respondenten met een zeer lage negatieve gemoedstoestand een positief verband wordt gevonden tussen sociale gelegenheid en wachtwoord sterkte (b=0.183). Echter, naarmate men een negatievere gemoedstoestand heeft wordt dit verband steeds sterker negatief: bij een gemiddelde score op negatieve gemoedstoestand is het verband b=-0.525, en voor respondenten met een zeer negatieve gemoedstand is het zelfs b=-1.232.

Tot slot zijn er drie significante interacties gevonden met betrekking tot *motivatie*. Voor de meting van zelf-gerapporteerd cybergedrag werden significante interacties gevonden van motivatie met zowel een positieve gemoedstoestand (b=-0.047, p<.05) en angst voor slachtofferschap (b=-0.065, p<.001). Alhoewel de interactie tussen motivatie en positieve gemoedstoestand negatief is blijkt uit de simple slopes dat het verband tussen een positieve gemoedstoestand en de veiligheid van zelf-gerapporteerd cybergedrag voor alle respondenten positief blijft. Het verband wordt echter wel steeds minder sterk

naarmate de gemoedstoestand positiever wordt: bij respondenten met een zeer lage score op positieve gemoedstoestand is het verband het sterkst positief (b=0.271) en bij respondenten met de meest positieve gemoedstoestand blijkt het, het minst sterk te zijn (b=0.013). Hetzelfde beeld komt naar voren bij de interactie tussen angst voor slachtofferschap en de veiligheid van zelf-gerapporteerd cybergedrag: dit positieve verband is het meest sterk voor respondenten met de minste angst voor slachtofferschap (b=0.242) en het minst sterk voor degenen met de meeste angst voor slachtofferschap (b=0.054).

Uit de analyses naar wachtwoord sterkte blijkt daarnaast een significant negatief interactie-effect tussen motivatie en zelfcontrole (b=-0.245, p<.05). De simple slopes tonen aan dat er bij een zeer lage (b=0.686), lage (b=0.441) of gemiddelde (b=0.196) mate van zelfcontrole nog sprake is van een positief verband tussen motivatie en wachtwoord sterkte. Echter, wanneer de respondenten een hoge (b=-0.049) of zeer hoge (b=-0.294) mate van zelfcontrole hebben wordt het verband negatief en hang een hogere motivatie dus samen met een minder sterk wachtwoord.

Samengenomen wijzen de resultaten erop dat de verbanden van kennis, gelegenheid en motivatie met de veiligheid van cybergedrag in enkele gevallen beïnvloed worden door zelfcontrole, gemoedstoestand, angst voor slachtofferschap en in één geval ook door eerder slachtofferschap. In de meeste gevallen werden er echter geen significante interacties gevonden.

### *5.6 Resumé*

In dit hoofdstuk is beschreven hoe veilig Nederlanders zich online gedragen en hoe dat gedrag kan worden verklaard. Ook zijn eigenschappen van de respondenten en mogelijke verklarende eigenschappen voor de veiligheid van cybergedrag beschreven. Respondenten zijn representatief voor de Nederlandse samenleving op geslacht, werkend en de provincie waarin zij woonachtig zijn. Respondenten zijn echter vaker dan gemiddeld in Nederland hoogopgeleid. Ook zijn respondenten minder vaak dan gemiddeld jonger dan 39 jaar.

In totaal werd 13,6 procent van de respondenten het afgelopen jaar slachtoffer van online criminaliteit. Afhankelijk van het type delict ondervond 43 procent tot 94 procent 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.

Voor alle zeven cybergedragingen die zijn meegenomen in deze studie, zijn resultaten beschreven. Alle gedragingen zijn uitgevraagd via zelfrapportage. Voor drie van deze gedragingen zijn ook objectieve metingen gedaan. Opvallend is het resultaat dat de objectieve metingen niet overeenkomen

met de zelf-gerapporteerde metingen van gedrag. Zelf-gerapporteerd gedrag is structureel veiliger dan daadwerkelijk gedrag.

Om te komen tot interventies die leiden tot gedragsverandering (i.e. veiliger gedrag) is echter inzicht nodig in de factoren die samenhangen met gedrag. Hiertoe is voor diverse factoren gekeken in welke mate ze samenhangen met zelf-gerapporteerd en daadwerkelijk cybergedrag. Samengenomen lijken de meeste van de uit de literatuur naar voren gekomen verklarende factoren van invloed te zijn op de veiligheid van (zelf-gerapporteerd) cybergedrag.

Wanneer we kijken naar daadwerkelijk cybergedrag, ontstaat echter een ander beeld. Samengenomen lijken de uit de literatuur naar voren gekomen verklarende factoren beperkt tot zeer beperkt van invloed te zijn op het objectieve gedrag van burgers, te weten wachtwoord sterkte, klikgedrag en delen persoonlijke gegevens.

Tot slot zijn additionele analyses uitgevoerd om verklaringen te vinden voor gevonden effecten op cybergedrag. Samengenomen wijzen de resultaten van deze additionele analyses erop dat de verbanden van kennis, gelegenheid en motivatie met de veiligheid van cybergedrag beïnvloed worden door zelfcontrole, gemoedstoestand, angst voor slachtofferschap en in één geval ook door eerder slachtofferschap.

# 6. Discussie

### *6.1 Inleiding*

Het doel van dit onderzoek was om in kaart te brengen hoe Nederlanders zich online gedragen en dit te verklaren aan de hand van factoren, die uit de literatuur naar voren zijn gekomen. Zodoende kan een eerste aanzet worden gegeven voor het ontwikkelen van interventies die ervoor moeten zorgen dat Nederlanders zich online veiliger gaan gedragen. De hoofdvraag van dit rapport was: *Hoe veilig gedragen Nederlanders zich online en hoe kan dit worden verklaard?* In dit hoofdstuk zal deze hoofdvraag worden beantwoord. In paragraaf 6.2 volgen eerst de conclusies van de literatuurstudie. Die studie was immers de basis voor de ontwikkeling van ons meetinstrument en bepalend voor de variabelen die zijn meegenomen in de analyses. Paragraaf 6.3 bevat een weergave van de belangrijkste conclusies van het empirische deel van dit onderzoek. Aan bod komt onder andere hoe veilig Nederlanders zich online gedragen en hoe dat gedrag kan worden verklaard. In paragraaf 6.4 staan de beperkingen van dit onderzoek beschreven en staan mogelijkheden voor toekomstig onderzoek weergeven. In paragraaf 6.5 staat een doorkijkje beschreven naar mogelijk veelbelovende interventies.

### *6.2 Conclusies literatuurstudie*

Voordat we de conclusies presenteren van het empirische deel van dit onderzoek geven we eerst een weergave van de belangrijkste conclusies van de 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 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 (PMT en COM-B) 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 tekenen (cues) 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.

### *6.3 Conclusies empirisch onderzoek*

*Onderzoeksvraag 1: Hoe veilig gedragen Nederlanders zich online?*

Een belangrijke voorwaarde voor online veiligheid is veilig cybergedrag. In dit onderzoek bestudeerden we zeven centrale gedragsclusters; gebruik van wachtwoorden, opslaan van belangrijke bestanden, installeren van updates, gebruik van beveiligingssoftware, alertheid tijdens internetgebruik, delen van persoonlijke gegevens en omgaan met bijlagen en hyperlinks in e-mails. Wanneer individuele gebruikers binnen elk cluster veilig gedrag vertonen, zou dit hen moeten beschermen tegen slachtofferschap van cybercriminaliteit.

Onveilig gedrag blijkt in hoge mate voor te komen. Zo gebruikt bijna 90 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 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 daadwerkelijke 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 per gedragscluster.

- *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 83 procent een zwak wachtwoord gebruikt. Als we nóg iets ruimer 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 gaf een aanzienlijk deel zijn of haar geboortedatum (37,5%), volledig naam (31%), e-mailadres (28,1%), postcode (27,0%) en huisnummer (20,4%). Een klein maar 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 veilig gedrag 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 van een bank – 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.

De belangrijkste conclusie is dus dat Nederlanders zich online vaak niet veilig gedragen. Dat is terug te zien in de cijfers over slachtofferschap. We hebben respondenten namelijk ook gevraagd of ze ooit slachtoffer zijn geworden van een of meerdere vormen van cybercrime. In totaal werd 13,6 procent van de respondenten het afgelopen jaar slachtoffer van online criminaliteit. Respondenten werden afgelopen jaar het vaakst slachtoffer van malware (7,3%), gevolgd door phishing (2,9%) en online aankoopfraude (2,0%). Deze hoge prevalentie van slachtofferschap van online criminaliteit is in lijn met ander recent onderzoek (CBS, 2019b). Als we ons niet beperken tot 12 maanden, maar vragen naar of iemand ooit slachtoffer is geworden, dan blijkt dat bijna 40 procent van de respondenten één of meerdere keren slachtoffer van online criminaliteit is geweest. Ook hier scoren malware (25,2%), online aankoopfraude (7,8%) en phishing (4,7%) hoog. Het aantal slachtoffers dat schade heeft ondervonden van het slachtofferschap dat afgelopen jaar heeft plaatsgevonden is, in lijn met recent onderzoek, zeer groot (Cross, Richards, & Smith, 2016; Jansen & Leukfeldt, 2018; Leukfeldt, Notté, & Malsch, 2018). Afhankelijk van het type delict ondervindt 43 procent tot 94 procent van de slachtoffers schade.

*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 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. Mensen met meer kennis van online veiligheid hebben, in tegenstelling tot wat zou mogen worden verwacht, niet meer materiële gelegenheid voor veilig cybergedrag.

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 objectieve gedragingen noodzakelijk is in vervolgonderzoek. Komen zelf-gerapporteerde en objectieve gedragingen 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. De verklaring hiervoor ligt mogelijk in wat de cybersecurity paradox wordt genoemd (Van Der Zee, 2018). Hoewel de meeste mensen aangeven cybersecurity belangrijk te vinden (Madden & Rainie, 2015) correspondeert hun zelf-gerapporteerd gedrag niet altijd met hun werkelijke gedrag (Smith & Louis, 2008; Spiekermann, Grossklags, & Berendt, 2001; Van Der Zee, 2018), zoals onderschreven wordt door 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 (Floyd et al., 2000; Michie et al., 2011). De verwachting was dat deze factoren samenhangen met cybergedrag. Uit de zelf-rapportage komt ook precies dat beeld: zowel kennis, sociale 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 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 (Boss et al., 2015; Christofides et al., 2012; Cialdini, 1987; Kim en Sundar, 2016; Macquet, 2009; Matthews et al., 1990; Paulissen & Van Wilsem, 2015). 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 (Isen, 2001; Nygren et al., 1996). 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, hoe groter de positieve gemoedstoestand van respondenten, hoe groter de kans is dat zij een onveilige keuze maken bij de software pop-up (klikgedrag). Deze laatste bevinding komt overeen met de verwachting op basis van de literatuur (Isen, 2001; Nygren et al., 1996). Ook angst voor slachtofferschap hangt significant samen met wachtwoord sterkte; hoe meer angst respondenten hebben om slachtoffer te worden van online criminaliteit, hoe sterker het door hen gekozen wachtwoord is. Ook is eerder slachtofferschap negatief gerelateerd aan 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 een significant verband met de veiligheid van alle objectief gemeten gedragingen. 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 Protection Motivation Theory (PMT) kan worden verwacht dat deze motivatie de veiligheid van cybergedrag beïnvloed (Floyd et al., 2000). Die conclusie kunnen we echter niet trekken. Sterker, 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, 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 significante 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 de objectieve metingen van daadwerkelijk cybergedrag vinden we ook een aantal significante kenmerken. 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 regressiemodellen waarin zelf-gerapporteerd cybergedrag en de wachtwoord sterkte worden voorspelt. Uit enkele interacties blijkt 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.

### *6.4 Onderzoeksbeperkingen en mogelijkheden voor toekomstig onderzoek*

Heel bewust is er in dit onderzoek voor gekozen om zowel zelf-gerapporteerd 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 (zie hoofdstuk 3). De literatuurstudie laat duidelijk zien dat er een gebrek is aan onderzoeken waarbij daadwerkelijk gedrag objectief wordt gemeten (zie de samenvatting van de belangrijkste resultaten in paragraaf 3.5).

Door het gebruik van een experimentele surveystudie – een methode die de voordelen van vragenlijstonderzoek combineert met de toegevoegde waarde die experimenten hebben – 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. Maar dit onderzoek is ook op een andere manier vernieuwend: we nemen niet slachtofferschap van specifieke vormen van online delicten als uitgangspunt, maar cybergedrag. Het is immers het gedrag dat zorgt voor een verhoogd risico op allerlei vormen van online criminaliteit. Ten slotte onderzoeken we ook wat verklaringen zijn voor cybergedrag.

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 (50% versus 30%). Ook zijn respondenten minder vaak dan gemiddeld jonger dan 39 jaar (13,8% versus 29,4%). Dat de steekproef niet representatief is op alle factoren heeft echter waarschijnlijk beperkte gevolgen voor de validiteit van de experimentele survey, zoals bleek in eerder onderzoek waarin convenience samples met representatieve samples werden vergeleken (Mullinix, Leeper, Druckman, & Freese, 2015).

Verder hebben we gebruikt gemaakt van respondenten die zijn aangeleverd door een zogenoemd panelbureau. Dit is een organisatie die gespecialiseerd is in het uitvoeren van enquête-onderzoek en zelf beschikt over een grote groep respondenten. Hierdoor kan het zijn dat de groep respondenten in onze steekproef selectief is doordat alle respondenten lid zijn van het panelbureau. Overigens doet de vergelijking met kenmerken van de Nederlandse samenleving vermoeden dat onze steekproef redelijk representatief is.

Daarnaast kan er sprake zijn van selectieve uitval. Niet alle panelleden die zijn uitgenodigd voor het onderzoek hebben de survey volledig ingevuld. Vergeleken met de niet-deelnemers zijn respondenten vaker man (53% versus 47%, $p<.001$) en gemiddeld ouder (57.9 versus 54.3 jaar, $p<.001$) dan non-respondenten maar verschillen nauwelijks in opleidingsniveau of de provincie waarin zij wonen. Echter kunnen niet-deelnemers ook verschillen van respondenten op niet-geregistreerde eigenschappen. Respondenten die het meest wantrouwend/oplettend zijn, zijn mogelijk sneller uitgevallen. Gezien het doel van de studie werden respondenten vooraf niet volledig geïnformeerd over de inhoud van het onderzoek. Respondenten dachten alleen vragen te beantwoorden over wat ze op internet doen. Mogelijk hebben bepaalde vragen de meest wantrouwende deelnemers afgeschrikt.

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 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. Dit kan betekenen dat in de thuissituatie het percentage onveilig gedrag lager is dan door ons is gemeten via het panelonderzoek. Ondanks dat het juist onze bedoeling was cybergedrag in een ogend veilige omgeving te meten – criminelen bootsen altijd een veilige omgeving (van bijvoorbeeld een bank of webshop) na en verleiden mensen hiermee op de hyperlink klikken of persoonlijke informatie weg te geven – kan het toch 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 beter oorzaak en gevolg bestudeerd kunnen worden (uiteraard met toestemming).

Ondanks de hier genoemde beperkingen laat de studie duidelijk zien dat er grote verschillen bestaan tussen zelf-gerapporteerd gedrag en daadwerkelijk gedrag. Als we alleen naar zelf-gerapporteerd gedrag kijken, dan blijken de meeste van de in de literatuur gevonden factoren inderdaad samen te hangen met gedrag. Kijken we echter naar daadwerkelijk gedrag, dan blijken bijna al deze factoren niet relevant voor cybergedrag. Verder zijn er ook verschillen tussen verschillende vormen van daadwerkelijk gedrag. Dus verschillende mensen gedragen zich op verschillende manieren onveilig. Dit is relevant voor de te ontwikkelen interventies die zich op specifieke vormen van gedrag moeten richten. Daarnaast verklaren de modellen die we gebruikt hebben in dit onderzoek (die alle variabelen bevatten die uit de literatuur van belang blijken) maar een zeer klein deel van het objectieve cybergedrag. In toekomstig onderzoek moeten dus andere verklarende factoren worden meegenomen. Ten slotte is het nodig om longitudinaal onderzoek naar gedrag uit te voeren. Hierdoor kunnen de effecten van cybergedrag op slachtofferschap en vice versa over de tijd getoetst worden.

### *6.5 Beleidsimplicaties: veelbelovende richtingen voor 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. Deze paragraaf gaat over die eerste aanzet om interventies te ontwikkelen. De resultaten van dit onderzoek zijn namelijk bediscussieerd met experts. Tijdens de discussiebijeenkomst zijn de resultaten van de

experimentele surveystudie en het literatuuronderzoek naar interventies besproken. Ook zijn veelbelovende richtingen voor interventies die zorgen voor veilig cybergedrag bediscussieerd.

Als we uitgaan van de resultaten van de huidige studie met betrekking tot de zelfrapportage van cybergedrag, dan volgt een eenduidig beeld op de gedrags-beïnvloeders capaciteiten, gelegenheid en motivatie. Op alle zeven in dit onderzoek betrokken gedragsclusters bepalen zij in belangrijke mate het gedrag. Op basis van de zelf-rapportage data kan worden geconcludeerd dat, vergeleken met andere vormen van cybergedrag, respondenten relatief het meest onveilige gedrag vertonen bij het back-uppen van belangrijke bestanden. Hier lijkt winst te behalen via gedragsinterventies.

De resultaten van dit onderzoek laten ons echter ook zien dat scores op zelfrapportage en objectieve bepalingen van gedrag niet altijd overeenkomen. Respondenten lijken een te rooskleurig beeld te hebben van hun eigen cybergedrag wanneer we hun zelf-gerapporteerde 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 procent van de respondenten gebruikt een zwak wachtwoord bestaande uit minder dan zeven karakters voor het beveiligingen van hun persoonsgegevens in dit onderzoek. Capaciteiten, gelegenheid en motivatie zijn bovendien nauwelijks gecorreleerd aan de in dit onderzoek gemeten objectieve gedragingen. Dat maakt het bepalen van geschikte interventies op gedrag complex.

Om naar aanleiding van de resultaten van de huidige studie te komen tot een lijst met mogelijk effectieve gedragsinterventies, zijn de resultaten voorgelegd aan diverse experts tijdens een expertbijeenkomst en is, gezamenlijk met de onderzoekers, gediscussieerd over diverse interventies. Een van de deelnemers aan de expertbijeenkomst merkte op dat een interessant doelgedrag voor gedragsinterventies, het gedrag is waar een groot verschil bestaat tussen zelfperceptie en werkelijk gedrag. Door verkeerde informatie of kennis met als gevolg zelfoverschatting ontstaat een potentieel gevaarlijke situatie voor internetgebruikers, aldus een van de deelnemers. Deze situatie zien we niet alleen bij wachtwoordmanagement, maar ook bij het delen van persoonlijke gegevens online. Respondenten rapporteren over het algemeen zorgvuldig om te gaan met hun persoonlijke gegevens. De objectieve meting in dit onderzoek laat een ander beeld zien. Een groot deel van de respondenten deelt persoonlijke gegevens welke door cybercriminelen te gebruiken zijn voor het uitvoeren van een gerichte aanval op de gebruiker, bijvoorbeeld voor online fraude.

Vervolgens is in meer detail gekeken naar factoren die cybergedrag beïnvloeden. Als we kijken naar capaciteiten, ofwel kennis, dan zien we dat het hebben van relevante kennis er niet per definitie toe leidt dat mensen zich daadwerkelijk veiliger gedragen. De verbanden tussen kennis en de veiligheid van

gedrag zijn bovendien afhankelijk van op welk gedrag de focus ligt. Voor het delen van persoonlijke gegevens lijkt meer kennis een goede beschermingsmaatregel. Voor wachtwoordmanagement is door ons echter een omgekeerd verband gevonden: meer kennis leidt tot meer onveilig gedrag. Ook opleiding laat een negatieve relatie zien met beide gedragingen: hoe hoger de genoten opleiding, hoe onveiliger zich men daadwerkelijk gedraagt. Zelfcontrole lijkt een goede voorspeller. Maar sinds dit over het algemeen wordt beschouwd als een vaste karaktereigenschap, zijn de mogelijkheden om via interventies op zelfcontrole het gedrag te beïnvloeden, beperkt. Ook een positieve gemoedstoestand heeft een positief verband met veilig gedrag. Respondenten die hoger scoren op deze schaal laten over het algemeen meer veilig gedrag zien. Ook hier is echter de potentie van het toepassen van interventies zeer beperkt. Verder zien we dat angst voor slachtofferschap een positief verband houdt met de veiligheid van enkele objectieve cybergedragingen. We zien ook dat eerder slachtofferschap een negatieve relatie heeft met veilig gedrag. Het ligt voor de hand om specifieke interventies te richten op deze doelgroep, bijvoorbeeld via meldpunten van slachtofferschap zoals de fraudehelpdesk. Hierbij dient wel te worden opgemerkt dat, aldus de experts, mensen verschillen in hun gevoeligheid voor interventies. Wat bij de een werkt, kan bij een ander een averechts effect hebben.

Naast specifieke interventies gericht op bovenstaande factoren, zien de experts veel waarde in aanpassingen van de techniek die mensen gebruiken voor online activiteiten, dusdanig dat de mogelijkheid voor onveilig gedrag wordt verkleind, ook wel *security-by-design* genoemd. Voorbeelden zijn het gebruik van biometrische gegevens in plaats van wachtwoorden, het gebruik van twee-factor authenticatie en het uitschakelen van hyperlinks in e-mails van onbekende afzender (Young, Wijn, & Van Rijk, 2018).

Een kanttekening die de deelnemers plaatsen op het verwachte succes van interventies, is dat de timing van gedragsinterventies cruciaal is. Huidige interventies, zoals overheidscampagnes, zijn, in de beleving van deelnemers, niet effectief omdat ze tot je komen op momenten dat dit niet relevant is, zoals via de radio tijdens het rijden in een auto. Interventies zouden moeten plaatsvinden op momenten dat dit ertoe doet, op zogenaamde *teachable, actionable* momenten. Advies over veilig cybergedrag is leerzamer en wordt sneller overgenomen, wanneer deze gegeven wordt op het moment dat de onveilige gedraging (bijna) plaatsvindt. Een recent voorbeeld is de verkoopsite Marktplaats, dat samen met de politie gebruikers waarschuwt tijdens online betaaltransacties voor mogelijke onveilige gedragingen[43]. Voortaan waarschuwt de site als gebruikers een onofficiële betaalomgeving openen.

[43] https://tweakers.net/nieuws/155148/marktplaats-gaat-gebruikers-waarschuwen-voor-links-naar-onofficiele-betaalsites.html

Samenvattend blijkt dat er geen panacee is voor het bevorderen van veilig cybergedrag. Verschillende cybergedragingen lijken andere bronnen te kennen. 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, 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 is een voorbeeld van een type interventie binnen deze categorie. Het ontwerpen van specifieke interventies is echter geen sinecure. Toekomstig onderzoek zou zich kunnen richten op het ontwikkelen en evalueren van een specifieke set van interventies voor de door ons gevonden onveilige gedragingen.

# Literatuur


Abraham, C., Kelly, M. P., West, R., & Michie, S. (2009). The UK National Institute for Health and Clinical Excellence public health guidance on behaviour change: a brief introduction. *Psychology, health & medicine*, *14*(1), 1-8.

Alison, L., van den Heuvel, C., Waring, S., Power, N., Long, A., O'Hara, T., & Crego, J. (2013). Immersive simulated learning environments for researching critical incidents: A knowledge synthesis of the literature and experiences of studying high-risk strategic decision making. *Journal of Cognitive Engineering and decision making*, *7*(3), 255-272.

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and Predicting the Factors Affecting End-Users' Risk-Taking Behavior. *Information and Computer Security*. https://doi.org/10.1108/ICS-03-2018-0037

Anderson, K. B. (2006). Who Are the Victims of Identity Theft? The Effect of Demographics. *Journal of Public Policy & Marketing*, *25*(2), 160–171. https://doi.org/10.1509/jppm.25.2.160

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Ask, K., & Granhag, P. A. (2005). Motivational sources of confirmation bias in criminal investigation: The need for cognitive closure. *Journal of Investigative Psychology and Offender Profiling, 2,* 43–63. https://doi.org/10.1002/jip.19

Atkins, L., & Michie, S. (2013). Changing eating behaviour: What can we learn from behavioural science? *Nutrition Bulletin*, *38*(1), 30-35.

Bazzell, M. (2018). Open source intelligence techniques (6th ed.). CreateSpace Independent Publishing Platform.

BIN NL (2017). Zeven behavioural insights tools. Hoe pas je gedragsinzichten toe in beleid, uitvoering en toezicht? Behavioural Insights Netwerk Nederland. https://www.communicatierijk.nl/documenten/publicaties/2017/11/23/tooloverzicht-bin-nl

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour and Information Technology*, *34*(10), 1022–1035. https://doi.org/10.1080/0144929X.2015.1028448

Borwell, J., Jansen, J., & Stol, W. (2018). Human Factors Leading to Online Fraud Victimisation: Literature Review and Exploring the Role of Personality Traits. In J. Mcalaney, L. A. Frumkin, & V. Benson (Eds.),

*Psychological and behavioural examinations in cyber security*. IGI Global.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *Mis Quarterly*, *39*(4).

Bossler, A. M., & Holt, T. J. (2009). On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, *3*(1), 400–420.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227–236. https://doi.org/10.1016/j.jcrimjus.2010.03.001

Braam, I. (2018). Waarom de keuze tussen iOS en Android nog steeds belangrijk is. Allaboutphones.nl. https://www.allaboutphones.nl/verschillen-android-ios/

Briggs, P., Jeske, D., & Coventry, L. (2017). Behavior change interventions for cybersecurity. *Behavior Change Research and Theory,* 115-136.

Brown, J., Kotz, D., Michie, S., Stapleton, J., Walmsley, M., & West, R. (2014). How effective and cost-effective was the national mass media smoking cessation campaign 'Stoptober'? *Drug and alcohol dependence*, *135*, 52-58.

Büchi, M., Just, N., & Latzer, M. (2016). Modeling the second-level digital divide: A five-country study of social differences in Internet use. *New Media and Society*, *18*(11), 2703–2722. https://doi.org/10.1177/1461444815604154

Bullée, J. W., Montoya, L., Junger, M., & Hartel, P. H. (2016, January). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. In *SG-CRC* (pp. 107-114).

Button, M. & Cross, C. (2017). Cyber frauds, scams and their victims. New York, NY: Routledge.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy*, *12*(1), 28–38. https://doi.org/10.1109/MSP.2013.106

CBS. (2019a). Bevolking; geslacht, leeftijd en burgerlijke staat. Retrieved from https://opendata.cbs.nl/statline/#/CBS/nl/dataset/7461BEV/table?fromstatweb

CBS. (2019b). *Digitale Veiligheid & Criminaliteit 2018*. Den Haag.

Chae, M., & Kim, J. (2004). Do size and structure matter to mobile users? An empirical study of the effects

of screen size, information structure, and task complexity on user activities with standard web phones. *Behaviour & information technology*, *23*(3), 165-181. https://doi.org/10.1080/01449290410001669923

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

Christofides, E., Muise, A., & Desmarais, S. (2012). Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior. *Journal of Adolescent Research*, *27*(6), 714–731. https://doi.org/10.1177/0743558411432635

Cialdini, R. B. (1987). Influence (Vol. 3). Port Harcourt: A. Michel.

Cialdini, R. B., Kallgren, C. A., & Reno, R. R. (1991). A focus theory of normative conduct: A theoretical refinement and reevaluation of the role of norms in human behavior. In *Advances in experimental social psychology* (Vol. 24, pp. 201-234). Academic Press.

Cohen, M. A., Rust, R. T., Steen, S., & Tidd, S. T. (2004). Willingness-to-Pay for Crime Control Programs. *Criminology*, *42*(1), 89–109. https://doi.org/10.2139/ssrn.293153

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends & Issues in Crime and Criminal Justice*, (518).

Crossler, R. E., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *ACM SIGMIS Database*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Crossler, R. E., Bélanger, F., & Ormond, D. (2017). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, 1–15. https://doi.org/10.1007/s10796-017-9755-1

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Cuyper, R. H. De, & Weijters, G. (2016). *Cybercrime in cijfers*. Den Haag: WODC.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Domenie, M., Leukfeldt, E. R., van Wilsem, J. A., Jansen, J., & Stol, W. P. (2013). *Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veel-voorkomende criminaliteit.* Den Haag: Boom Lemma uitgevers.

Dougherty, M. R. P., & Hunter, J. E. (2003). Probability judgment and subadditivity: The role of working memory capacity and constraining retrieval. *Memory & Cognition, 31,* 968–982. https://doi.org/10.3758/BF03196449

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups - 2nd annual eCrime researchers summit* (pp. 37–44). New York, New York, USA: ACM Press. https://doi.org/10.1145/1299015.1299019

Engelen, U., De Peuter, S., Victoir, A., Van Diest, I., & Van den Bergh, O. (2006). Verdere validering van de Positive and Negative Affect Schedule (PANAS) en vergelijking van twee Nederlandstalige versies. *Gedrag en gezondheid*, *34*(2), 61-70.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 36-47). Springer, Cham.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30,*(2,), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Garland, D. (2003). The rise of risk. In R. V. Ericson & A. Doyle (Eds.), *Risk and morality* (pp. 48–86). Toronto: University of Toronto Press.

Goldstein, N. J., Cialdini, R. B., & Griskevicius, V. (2008). A room with a viewpoint: Using social norms to motivate environmental conservation in hotels. *Journal of Consumer Research , 35*, 472–482. 10.1086/586910

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford: Stanford University Press.

Gouldner, A. (1960). The Norm of Reciprocity: A Preliminary Statement. *American Sociological Review*, *25*, 161-178.

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256–267. https://doi.org/10.1016/j.intcom.2011.03.007

Guadagno, R. E., & Cialdini, R. B. (2005). Online persuasion and compliance: Social influence on the Internet and beyond. *The social net: The social psychology of the Internet*, 91-113.

Harrington, M. C. (2006, July). Situational learning in real and virtual space: lessons learned and future directions. In *ACM SIGGRAPH 2006 Educators program* (p. 48). ACM.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Holt, T. J., & Bossler, A. M. (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420–436. https://doi.org/10.1177/1043986213507401

Huang, D. L., Patrick Rau, P. L., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human Computer Studies*, *69*(12), 870–883. https://doi.org/10.1016/j.ijhcs.2011.07.007

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

Jansen, J. (2018). *Do you bend or break? Preventing online banking fraud victimization through online resilience*. Gildeprint.

Jansen, J., & Leukfeldt, R. (2015). How People Help Fraudsters Steal Their Money: An Analysis of 600 Online Banking Fraud Cases. In *Proceedings - 5th Workshop on Socio-Technical Aspects in Security and Trust, STAST 2015* (pp. 24–31). https://doi.org/10.1109/STAST.2015.12

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79–91. https://doi.org/10.5281/zenodo.58523

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

Jansen, J., Leukfeldt, R., Wilsem, J. Van, & Stol, W. (2013). Onlinegedragingen. *Tijdschrift Voor Criminologie*, *2013*(55), 394–408.

Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security*, *25*(2), 165–180. https://doi.org/10.1108/ICS-03-2017-0018

Johnson, E. J., & Tversky, A. (1983). Affect, generalization, and the perception of risk. *Journal of Personality and Social Psychology*, *45*(1), 20–31. https://doi.org/10.1037/0022-3514.45.1.20

Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems*, *53*(2), 22–30.

Jong, L., Leukfeldt, R., & van de Weijer, S. (2018). Determinanten en motivaties voor intentie tot aangifte na slachtofferschap van cybercrime. *Tijdschrift Voor Veiligheid*, *17*(1–2), 66–78. https://doi.org/10.5553/TvV/187279482018017102006

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in human behavior*, *66*, 75-87.

Kaptein, M., Markopoulos, P., de Ruyter, B., & Aarts, E. (2009). Can you be persuaded? individual differences in susceptibility to persuasion. In *IFIP Conference on Human-Computer Interaction* (pp. 115-118). Springer, Berlin, Heidelberg.

Kaye, J. (2011). Self-reported password sharing strategies. *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems - CHI '11*, 2619. https://doi.org/10.1145/1978942.1979324

Kim, K. J., & Sundar, S. S. (2016). Mobile persuasion: can screen size and presentation mode make a difference to trust? Human Communication Research. http://dx.doi.org/10.1111/hcre.12064

Kok, G., Gottlieb, N. H., Peters, G. J. Y., Mullen, P. D., Parcel, G. S., Ruiter, R. A., Fernandez, M.E., Markham, C., & Bartholomew, L. K. (2016). A taxonomy of behaviour change methods: an Intervention Mapping approach. *Health psychology review*, *10*(3), 297-312.

Krupnikov, Y., & Findley, B. (2018). Survey Experiments. In L. R. Atkeson & R. M. Alvarez (Eds.), *The Oxford Handbook of Polling and Survey Methods* (Vol. 1). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190213299.013.32

Lastdrager, E. E. H. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 9. https://doi.org/10.1186/s40163-014-0009-y

Leith, K.P., & Baumeister, R.F. (1996). Why do bad moods increase processing. In: Baddeley, A.D., Weiskrantz, L. (Eds.), *Attention: Selection, Awareness, and Control: A Tribute to Donald Broadbent*. Oxford University Press, New York, pp. 374–389.

Leukfeldt, E. R. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E. R. (Ed.). (2017). *Research Agenda the Human Factor in Cybercrime and Cybersecurity*. Den Haag: Eleven International Publishing.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology*, *57*(3), 704-722. https://doi.org/10.1093/bjc/azw009.

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

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy

settings in an online social network. *Journal of Computer-Mediated Communication*, *14*(1), 79–100. https://doi.org/10.1111/j.1083-6101.2008.01432.x

Lusthaus, J. (2018a). Honour Among (Cyber)thieves? *European Journal of Sociolog*y, 59(2), 191-223.

Lusthaus, J. (2018b). *Industry of Anonymity: Inside the Business of Cybercrime.* Cambridge: Harvard University Press.

MacInnis, D. J., Moorman, C., & Jaworski, B. J. (1991). Enhancing and measuring consumers' motivation, opportunity, and ability to process brand information from ads. *The Journal of Marketing*, 32-53.

Macquet, A. C. (2009). Recognition within the decision-making process: A case study of expert volleyball players. *Journal of Applied Sport Psychology, 21,* 64–79. https://doi.org/10.1080/10413200802575759

Madden, M., & Rainie, L. (2015). Americans' Attitudes About Privacy, Security and Surveillance. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Maguire, N., Beyens, K., Boone, M., Laurinavicius, A., & Persson, A. (2015). Using vignette methodology to research the process of breach comparatively. *European journal of probation*, *7*(3), 241-259.

Maimon, D., & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, *2*(1). https://doi.org/10.1146/annurev-criminol-032317-092057

Matthews, G., Jones, D. M., & Chamberlain, A. G. (1990). Refining the measurement of mood: The UWIST mood adjective checklist. *British journal of psychology*, *81*(1), 17-42.

Matthews, G., Pitcaithly, D., & Mann, R. L. (1995). Mood, neuroticism, and the encoding of affective words. *Cognitive Therapy and Research*, *19*(5), 563-587.

McCrae, R. R., & Costa Jr, P. T. (1999). A five-factor theory of personality. In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research* (*2nd edition)*, 139-153. New York: Guilford.

McGuire, M., & Dowling, S. (2013). Chapter 1: Cyber-dependent crimes. In *Cyber crime : A review of the evidence*.

Michie, S., Abraham, C., Whittington, C., McAteer, J., & Gupta, S. (2009). Effective techniques in healthy eating and physical activity interventions: a meta-regression. *Health Psychology*, *28*(6), 690.

Michie, S., Churchill, S., & West, R. (2010). Identifying evidence-based competences required to deliver behavioural support for smoking cessation. *Annals of Behavioral Medicine*, *41*(1), 59-70.

Michie, S., Hyder, N., Walia, A., & West, R. (2011). Development of a taxonomy of behaviour change techniques used in individual behavioural support for smoking cessation. *Addictive behaviors*, *36*(4), 315-319.

Michie, S., Stralen, M. M. Van, & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions, *42*(6). https://doi.org/10.1186/1748-5908-6-42

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*, *7*(2), 163–184. https://doi.org/10.1348/135910702169420

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014). Towards an Ontological Model Defining the Social Engineering Domain. In *11th IFIP International Conference on Human Choice and Computers (HCC)* (pp. 266–279). Turku, Finland: Springer, IFIP Advances in Information and Communication Technology. https://doi.org/10.1007/978-3-662-44208-1_22

Mullinix, K. J., Leeper, T. J., Druckman, J. N., & Freese, J. (2015). The generalizability of survey experiments. *Journal of Experimental Political Science*, *2*(2), 109-138.

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

Münscher, R., Vetter, M., & Scheuerle, T. (2016). A review and taxonomy of choice architecture techniques. *Journal of Behavioral Decision Making*, *29*(5), 511-524.

Mutz, D. C. (2011). *Population-based survey experiments*. Princeton: Princeton University Press.

Natale, M., & Hantas, M. (1982). Effect of temporary mood states on selective memory about the self. *Journal of Personality and Social Psychology*, *42*(5), 927.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773.

Nunnally, J., & Bernstein, I. (1994). Psychometric Theory 3rd edition (MacGraw-Hill, New York).

Nygren, T. E., Isen, A. M., Taylor, P. J., & Dulin, J. (1996). 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*(1), 59-72.

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection Motivation Theory. In M. Conner & P. Norman (Eds.), *Predicting Health Behaviour* (pp. 81–127). Open University Press.

Ovelgönne, M., Dumitras, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks. *ACM Transactions on Intelligent Systems and Technology*, *8*(4), 1–25. https://doi.org/10.1145/2890509

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, 40-51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Paulissen, L., & Van Wilsem, J. (2015). *Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland.* Politie en Wetenschap, Apeldoorn.

Petty, R.E., & Cacioppo, J.T. (1986). *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*. Springer, UK. New York.

Pyszczynski, T., Hamilton, J. C., Herring, F. H., & Greenberg, J. (1989). Depression, self-focused attention, and the negative memory bias. *Journal of Personality and Social Psychology*, *57*(2), 351.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114.

Rokven, J. J., Weijters, G., & Laan, A. M. Van Der. (2017). *Jeugddelinquentie in de virtuele wereld*. Den Haag: WODC.

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied*, *80*(1).

Russel, J.A. (1979). Affective space is bipolar. *Journal of Personality and Social Psychology, 37*, 345-356.

Rutkens, A. (2018). *Social engineering in de informatiebeveiliging*.

Saks, A. & Belcourt, M. (2006). An investigation of training activities and transfer of training in organizations. *Human Resources Management, 45*(4), 629–648.

Sallis, J. F., & Glanz, K. (2006). The role of built environments in physical activity, eating, and obesity in childhood. *The future of children*, 89-108.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373–382. https://doi.org/10.1145/1753326.1753383

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins

with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*. https://doi.org/10.1016/j.chb.2015.01.046

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security, 8*(1), 31–41.

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280–285. https://doi.org/10.1126/science.3563507

Smith, J. R., & Louis, W. R. (2008). Do as we say and as we do: The interplay of descriptive and injunctive group norms in the attitude-behaviour relationship. *British Journal of Social Psychology*, *47*(4), 647–666. https://doi.org/10.1348/014466607X269748

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy*, *9*(1). https://doi.org/10.4018/IJISP.2015010102

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd Generation E-Commerce : Privacy Preferences versus actual Behavior. *ACM Conference on Electronic Commerce*, 1–10. https://doi.org/10.1145/501158.501163

Stajano, F. & Wilson, P (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM, 54*(3), 70-75.

Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime*. New York: NYU Press.

Symantec. (2018). *Security Center White Papers*. Retrieved from https://www.symantec.com/security-center/white-papers

Teasdale, J. D. (1993). Selective effects of emotion on information-processing. In A. D. Baddeley & L. Weiskrantz (Eds.), *Attention: Selection, awareness, and control: A tribute to Donald Broadbent* (pp. 374-389). New York, NY, US: Clarendon Press/Oxford University Press

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, 196–203. https://doi.org/10.1109/ARES.2010.27

Tan, M., & Aguilar, K. S. (2012). An investigation of students' perception of Bluetooth security. *Information Management and Computer Security*, *20*(5), 364–381. https://doi.org/10.1108/09685221211286539

Van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

Van der Weijer, S. G. A., Leukfeldt, R. E., & Bernasco, W. (2018). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, 1–23. https://doi.org/10.1177/1477370818773610

Van Der Zee, S. (2018). Cyber Security Paradox: When knowing what's right does not lead to doing what's right. In *Security & Human Behavior workshop 2018.* Retrieved from https://www.lightbluetouchpaper.org/2018/05/24/security-and-human-behavior-2018/

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038

Van Wilsem, J. (2013a). "Bought it, but never got it" assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168–178. https://doi.org/10.1093/esr/jcr053

Van Wilsem, J. (2013b). Hacking and Harassment-Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437–453. https://doi.org/10.1177/1043986213507402

Van Zwet, A. (2018). *De beste browser voor je computer*. Consumentenbond. https://www.consumentenbond.nl/laptop/de-beste-browser-voor-je-computer

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4) https://doi.org/10.1016/j.im.2012.04.002

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

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191-198.

Warkentin, M., Straub, D., & Malimage, K. (2012). Featured Talk: Measuring Secure Behavior: A Research Commentary. In *Annual Symposium on Information Assurance & Secure Knowledge Management (ASIA & SKM)*. Albany, NY.

Watson, D., Clark, L.A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: The PANAS scales. *Journal of Personality and Social Psychology, 54*, 1063-1070.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii.

Wells, T., Bailey, J. T., & Link, M. W. (2014). Comparison of smartphone and online computer survey administration. *Social Science Computer Review*, *32*(2), 238-255.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Young, H., Wijn, R., & Van Rijk, R. (2018). Veilig cybergedrag: niet veranderen maar faciliteren. *Beveiliging*, (April), 30–32.

Yuen, K. S., & Lee, T. M. (2003). Could mood state affect risk-taking decisions? *Journal of affective disorders*, *75*(1), 11-18.

# Bijlage 1: Vragenlijst

*[meting sterkte wachtwoord]*

In overeenstemming met wetgeving ten aanzien van gegevensbescherming vragen we u om nu eerst een tijdelijk gebruikersaccount aan te maken. In dit account worden omwille van dit onderzoek enkele persoonlijke gegevens opgeslagen. Dit account heeft u aan het einde van de vragenlijst eenmalig opnieuw nodig.

Voer hieronder een gebruikersnaam en wachtwoord in.

1a. Gebruikersnaam:
1b. Wachtwoord *[gemaskeerd][opmerkingen: 1) geen beperkingen in lengte, we willen ook de mogelijkheid bieden dat respondenten een wachtwoordzin gebruiken 2) geen andere eisen aan wachtwoord stellen 3) geen sterkte-indicatie weergeven voor de respondenten]*:
1c. Vul het wachtwoord nogmaals in *[gemaskeerd]*:

2. *[gemoedstoestand]*

Hieronder staan 20 termen die verwijzen naar een bepaald gevoel of een bepaalde emotie. Wilt u alstublieft aangeven in welke mate u deze gevoelens of emoties ervaart ***op dit moment***. De antwoordmogelijkheden zijn: heel weinig, een beetje, matig, veel en heel veel.

| | | heel weinig | een beetje | matig | veel | heel veel |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| a | Geïnteresseerd | | | | | |
| b | Overstuur | | | | | |
| c | Uitgelaten | | | | | |
| d | Van streek | | | | | |
| e | Sterk | | | | | |
| f | Schuldig | | | | | |
| g | Angstig | | | | | |
| h | Vijandig | | | | | |
| i | Enthousiast | | | | | |
| j | Trots | | | | | |
| k | Prikkelbaar | | | | | |
| l | Alert | | | | | |
| m | Beschaamd | | | | | |
| n | Geïnspireerd | | | | | |
| o | Nerveus | | | | | |
| p | Vastberaden | | | | | |
| q | Aandachtig | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| r | Rusteloos | | | | | |
| s | Actief | | | | | |
| t | Bang | | | | | |

3. Hoe vaak maakt u gebruik van internet voor privé doeleinden? Kies alstublieft een antwoord.
-Minder dan 1 keer per maand
-Minimaal 1 keer per maand, maar niet wekelijks
-Minimaal 1 keer per week, maar niet dagelijks
-Dagelijks
-Meerdere keren per dag
-Minstens ieder uur (tijdens de uren dat ik wakker ben)
-Ik ben (bijna) continu online (tijdens de uren dat ik wakker ben)

4. Gebruikt u wel eens internet op de volgende apparaten voor privé doeleinden?

| | | Nooit | Minder dan 1 keer per week | 1-3 keer per week | (bijna) elke dag | Meerdere keren per dag |
|---|---|---|---|---|---|---|
| a | Tablet | | | | | |
| b | Mobiele telefoon (smartphone) | | | | | |
| c | Laptop of notebook[44] | | | | | |
| d | Desktop computer[45] | | | | | |
| e | Andere apparaten | | | | | |

5. Welk apparaat gebruikt u het meest om te internetten voor privé doeleinden? *[1 antwoord mogelijk]*
-Tablet *(ga naar 6c)*
-Mobiele telefoon (smartphone) *(ga naar 6d)*
-Laptop of notebook *(ga naar 6b)*
-Desktop computer *(ga naar 6a)*

| 6a. Heeft u op uw desktop computer… | Nee | Ja | Weet ik niet |
|---|---|---|---|
| …een virusscanner | | | |
| …een firewall | | | |
| …middelen voor het maken van back-ups[46] van uw bestanden (zoals een fysieke externe harde schijf of de cloud[47]) | | | |
| …een applicatie voor het (illegaal) downloaden van films, muziek en/of games (zoals BitTorrent) | | | |
| …een browser extensie, zoals een adblocker | | | |

[44] Een laptop of een notebook is een draagbare computer.
[45] Een desktop computer staat op een vaste plaats en bestaat uit een computerbehuizing (op/onder bureau), een monitor, muis en/of toetsenbord.
[46] Een back-up is een reservekopie.
[47] Een clouddienst biedt opslagruimte aan op internet voor de opslag van bestanden, zoals foto's.

| | | | |
|---|---|---|---|
| …een VPN verbinding[48] | | | |

*[ga naar vraag 7]*

| 6b. Heeft u op uw laptop of notebook… | Nee | Ja | Weet ik niet |
|---|---|---|---|
| …een virusscanner | | | |
| …een firewall | | | |
| …middelen voor het maken van back-ups[49] van uw bestanden (zoals een fysieke externe harde schijf of de cloud[50]) | | | |
| …een applicatie voor het (illegaal) downloaden van films, muziek en/of games (zoals BitTorrent) | | | |
| ……een browser extensie, zoals een adblocker | | | |
| …een VPN verbinding[51] | | | |

*[ga naar vraag 7]*

| 6c. Heeft u op uw tablet… | Nee | Ja | Weet ik niet |
|---|---|---|---|
| …een virusscanner | | | |
| …een firewall | | | |
| …middelen voor het draadloos maken van back-ups[52] van bestanden en foto's (zoals de cloud[53], Google drive, NAS) | | | |
| …een VPN verbinding[54] | | | |
| …applicaties die niet uit een officiële app winkel (Google Play, App Store) zijn gedownload | | | |

*[ga naar vraag 7]*

| 6d. Heeft u op uw mobiele telefoon (smartphone) … | Nee | Ja | Weet ik niet |
|---|---|---|---|
| …een virusscanner | | | |
| …een firewall | | | |
| …middelen voor het draadloos maken van back-ups[55] van bestanden en foto's (zoals de cloud[56], Google drive, NAS) | | | |

[48] Een VPN (Virtual Private Network) verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.
[49] Een back-up is een reservekopie.
[50] Een clouddienst biedt opslagruimte aan op internet voor de opslag van bestanden, zoals foto's.
[51] Een VPN (Virtual Private Network) verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.
[52] Een back-up is een reservekopie.
[53] Een clouddienst biedt opslagruimte aan op internet voor de opslag van bestanden, zoals foto's.
[54] Een VPN (Virtual Private Network) verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.
[55] Een back-up is een reservekopie.
[56] Een clouddienst biedt opslagruimte aan op internet voor de opslag van bestanden, zoals foto's.

| | | | |
|---|---|---|---|
| …een VPN verbinding[57] | | | |
| …applicaties die niet uit een officiële app winkel (Google Play, App Store) zijn gedownload | | | |

*[ga naar vraag 7]*

7. Welk apparaat gebruikt u voor het invullen van deze vragenlijst? *[1 antwoord mogelijk]*
-Tablet
-Mobiele telefoon (smartphone)
-Laptop of notebook
-Desktop computer

We gaan u nu vragen stellen over een aantal online activiteiten. U heeft voor dit blok **5 minuten** de tijd.*

**[Tijdsdruk – de helft van de respondenten krijgt dit te zien.]*
Het is gebleken dat dit voor veel deelnemers niet genoeg tijd is. We willen u vragen in dit blok in een hoog tempo door te werken. Probeer alle vragen af te krijgen in de tijd die u heeft.

**[Non-Tijdsdruk – de helft van de respondenten krijgt dit te zien.]*
Het is gebleken dat dit voor de meeste deelnemers ruim genoeg tijd is. We willen u vragen in dit blok in uw eigen tempo door te werken.

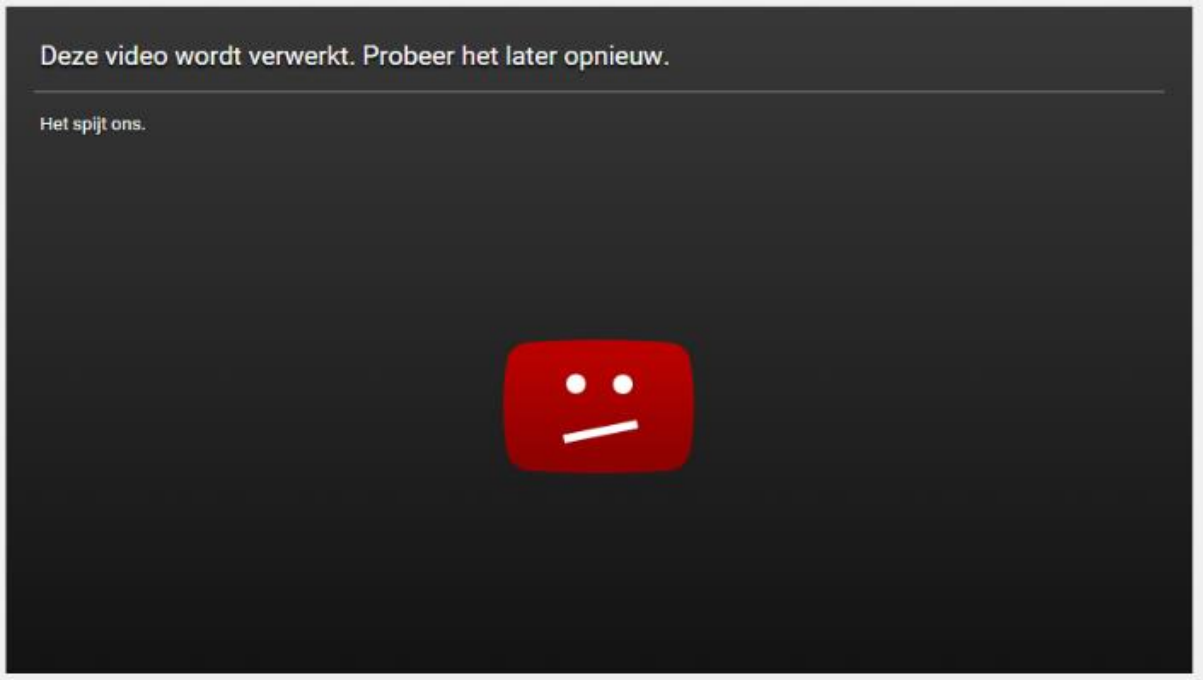
8. Hoe vaak voert u onderstaande online activiteiten uit in uw eigen tijd (buiten werktijd)?

| | | Nooit | Minder dan 1 keer per week | 1-3 keer per week | (bijna) elke dag | Meerdere keren per dag |
|---|---|---|---|---|---|---|
| a | E-mailen | | | | | |
| b | Informatie opzoeken (gericht surfen) | | | | | |
| c | Ongericht surfen | | | | | |
| d | Online bankieren | | | | | |
| e | Online shoppen | | | | | |
| e | Muziek, films, software en/of games downloaden | | | | | |
| f | Videogesprekken voeren, bv. via Skype of Facetime | | | | | |
| g | Online televisie kijken/streamen (bijvoorbeeld op YouTube) | | | | | |
| h | Op sociale media berichten lezen en profielen bekijken (zoals Facebook, Twitter, Instagram en LinkedIn) | | | | | |

[57] Een VPN (Virtual Private Network) verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.

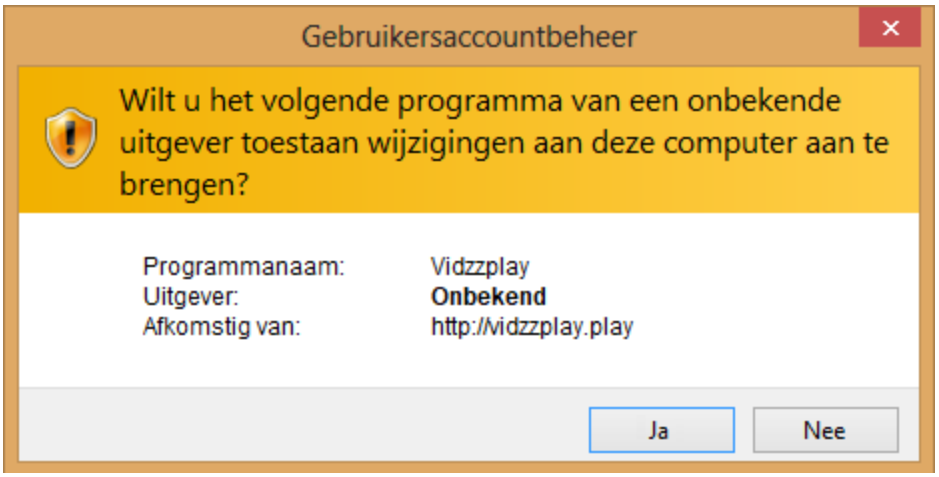
| | | | | | | |
|---|---|---|---|---|---|---|
| i | Op sociale media teksten plaatsen, berichten sturen of berichten van anderen “liken” of delen (zoals Facebook, Twitter, Instagram en LinkedIn) | | | | | |
| j | Chatten via chatsites | | | | | |
| k | Berichten plaatsen in online discussiegroepen/internetfora | | | | | |
| l | Online gamen/spelletjes spelen | | | | | |
| m | Studie-gerelateerde taken op internet | | | | | |
| n | Maken en/of onderhouden van websites | | | | | |

Voordat u de volgende vraag beantwoordt, vragen wij u eerst een kort filmpje over online winkelen te bekijken (30 seconden). Klik in onderstaande scherm op de afspeelknop .




*[vraag 9a verschijnt direct nadat respondent probeert filmpje af te spelen.]*

9a.




10. U kunt via internet producten kopen, zoals kleding, elektronica en toegangskaarten. U kunt uw aankopen doen via webwinkels of rechtstreeks van particulieren kopen, bijvoorbeeld via Markplaats.nl

Heeft u de afgelopen 12 maanden producten gekocht via internet?
-Ja
-Nee

Dit is het einde van blok 2 over “online activiteiten”. We gaven u 5 minuten de tijd voor dit blok.

11a. Hoeveel **tijdsdruk** heeft u ervaren bij het maken van uw keuzes in het blok over online activiteiten?

| Geen tijdsdruk | | | | | | heel veel tijdsdruk |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

11b. Hoe **gehaast** voelde u zich tijdens het beantwoorden van de vragen in het blok over online activiteiten?

| Helemaal niet gehaast | | | | | | Heel gehaast |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

*[vignetten]*

Veel mensen worden dagelijks overspoeld met een groot aantal e-mails. We willen graag weten hoe mensen omgaan met e-mails. Er zullen nu een aantal e-mails aan u worden voorgelegd, zoals die binnenkomen in het Postvak In (Inbox) van “Robin de Vries”. We willen u vragen te doen alsof u Robin bent. Wat zou Robin met deze e-mails doen? U zal ook worden gevraagd hoe zeker u bent van uw keuze en welke aspecten van de e-mail uw keuze hebben beïnvloed.

*[respondent wordt 3 vignetten toegewezen, in willekeurige volgorde):*

*Vignet Armin van Buuren*

U ziet hieronder een afbeelding van een e-mail die Robin heeft ontvangen. Robin is fan van Armin van Buuren en woont in de omgeving van Leiden waar binnenkort Koningsdag wordt gevierd.

**Van**: DJguide [mailto:info@djguides.nl]
**Verzonden**: Dinsdag 12 februari 2019 11:14
**Aan**: robin@devries.nl
**Onderwerp**: Gratis e-ticket Armin van Buuren Kingsday Leiden

**GRATIS E-TICKET**
**ARMIN VAN BUUREN KINGSDAY LEIDEN**



**Armin van Buuren presents Kingsday Leiden**

Armin van Buuren treedt dit jaar weer op in Leiden tijdens Koningsdag. Na het grote succes van vorig jaar vindt het feest 'Armin van Buuren presents Kingsday Leiden' dit jaar weer plaats op de Garenmarkt in de binnenstad van Leiden en jij kan er **GRATIS** bij zijn.

Op dinsdag 27 april vanaf 15.00 uur tot 22.00 uur kunnen oranje fans genieten van diverse optredens met als hoogtepunt een optreden van Leidenaar Armin van Buuren.

Ook dit jaar zal Armin van Buuren de oranjekoorts 'zijn stad' naar ongekende hoogte laten stijgen. Al 13 jaar lang treedt Van Buuren, één van de beroemdste DJ's ter wereld, op tijdens Koningsdag in Leiden. Dit is het hoogtepunt van het feest "Armin van Buuren presents Kingsday Leiden', dat dit jaar weer plaatsvindt op de Garenmarkt. Iedereen vanaf 16 jaar en ouder kan hier genieten van het ultieme Koningsdagfeest!

DOWNLOAD HIER JOU GRATIS TICKET

http://www.djguides.nl/gratis-ticket

12. Wat zou u doen met deze e-mail als u Robin was? Kies alstublieft voor iedere actie “ja” of “nee”.

| | | Ja | Nee |
|---|---|---|---|
| a | Ik beantwoord de e-mail | | |
| b | Ik verwijder de e-mail | | |
| c | Ik stuur de e-mail door naar iemand anders | | |
| d | Ik kopieer en plak de URL (het www adres) uit de e-mail in een webbrowser | | * |
| e | Ik klik op de link in de e-mail | | * |
| f | Ik typ de URL (het www adres) over in een webbrowser | | * |
| g | Ik bewaar de e-mail | | |
| h | Ik zoek naar meer informatie voordat ik een keuze maak | | |
| i | Ik doe niets | | |

13. Hoe zeker bent u van uw keuzes?

| Helemaal niet zeker | | | | Heel zeker |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

14. Welke aspecten van de e-mail hebben uw keuze beïnvloed? U mag meerdere antwoorden kiezen.
-De afzender
-Het onderwerp
-De tekst in de e-mail
-De afbeelding in de e-mail
-De hyperlink in de e-mail
-Het doeladres van de hyperlink (de website waar de link heen verwijst)

*Vignet KPN*

Robin is klant bij KPN. Robin vindt het van belang om op de hoogte te blijven over ontwikkelingen en actualiteiten op het gebied van online veiligheid. Vooral informatie over hoe Robin zichzelf beter kan beschermen, is interessant.

15. Wat zou u doen met deze e-mail als u Robin was? Kies alstublieft voor iedere actie “ja” of “nee”.

| | | Ja | Nee |
|---|---|---|---|
| a | Ik beantwoord de e-mail | | |
| b | Ik verwijder de e-mail | | |
| c | Ik stuur de e-mail door naar iemand anders | | |
| d | Ik kopieer en plak de URL (het www adres) uit de e-mail in een webbrowser | * | |
| e | Ik klik op de link in de e-mail | * | |
| f | Ik typ de URL (het www adres) over in een webbrowser | * | |
| g | Ik bewaar de e-mail | | |
| h | Ik zoek naar meer informatie voordat ik een keuze maak | | |
| i | Ik doe niets | | |

16. Hoe zeker bent u van uw keuzes?

| Helemaal niet zeker | | | | Heel zeker |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

17. Welke aspecten van de e-mail hebben uw keuze beïnvloed? U mag meerdere antwoorden kiezen.

-De afzender
-Het onderwerp
-De tekst in de e-mail
-De afbeelding in de e-mail
-De hyperlink in de e-mail
-Het doeladres van de hyperlink (de website waar de link heen verwijst)

*Vignet Rabobank*

Robin heeft al enige tijd een betaalrekening bij de Rabobank. Op 23 januari ontvangt Robin de onderstaande e-mail in het Postvak In.

**Van**: Rabobank [mailto:bankzaken@rabobank.nl]
**Verzonden**: woensdag 23 januari 2019 17:58
**Aan**: robin@devries.nl
**Onderwerp**: Laatste herinnering: Uw aanvraag is nog niet verwerkt, voorkom een geblokkeerde betaalpas

**Rabobank**

Geachte relatie,

Uit onze administratie is gebleken dat u nog geen gebruik maakt van onze nieuwe betaalpas. De nieuwe betaalpas is beter beveiligd tegen frauduleuze praktijken en voldoet zich aan de Europese veiligheidsvoorschriften betreft bankzaken. Met de nieuwe betaalpas kunt u vertrouwd, veilig en gemakkelijk betalen en geld opnemen zoals u gewend bent en contactloos betalen in meer dan 12.000 winkels in heel Europa. Ook bent u beter beschermd tegen skimming en pinpas-fraude bij geldautomaten.

Het gebruik van uw huidige betaalpas wordt gedeactiveerd. In verband met de veiligheid van onze klanten is het verplicht uw huidige betaalpas te vervangen. Wij bieden onze klanten de mogelijkheid aan om dit kosteloos te doen. Klik hier om kosteloos uw nieuwe betaalpas aan te vragen en volg de benodigde stappen om uw aanvraag te voltooien. U ontvangt uw nieuwe betaalpas binnen **2 werkdagen** per post toegezonden.

Zolang u nog niet in bezit bent van een nieuwe betaalpas kunt u helaas nog geen gebruik maken van onze nieuwe dienstverlening.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd en van dienst te zijn geweest.

Alvast hartelijk dank voor uw medewerking.

Met vriendelijke groet,
Rabobank

Afdeling Internetbankieren

http://rabobank.nl.condodima.com/raboaanvraag/inloggen.html

18. Wat zou u doen met deze e-mail als u Robin was? Kies alstublieft voor iedere actie “ja” of “nee”.

| | | Ja | Nee |
|---|---|---|---|
| a | Ik beantwoord de e-mail | | |
| b | Ik verwijder de e-mail | | |
| c | Ik stuur de e-mail door naar iemand anders | | |
| d | Ik kopieer en plak de URL (het www adres) uit de e-mail in een webbrowser | | * |
| e | Ik klik op de link in de e-mail | | * |
| f | Ik typ de URL (het www adres) over in een webbrowser | | * |
| g | Ik bewaar de e-mail | | |
| h | Ik zoek naar meer informatie voordat ik een keuze maak | | |
| i | Ik doe niets | | |

19. Hoe zeker bent u van uw keuzes?

Helemaal niet zeker Heel zeker

1 2 3 4 5

20. Welke aspecten van de e-mail hebben uw keuze beïnvloed? U mag meerdere antwoorden kiezen.
-De afzender
-Het onderwerp
-De tekst in de e-mail
-De afbeelding in de e-mail
-De hyperlink in de e-mail
-Het doeladres van de hyperlink (de website waar de link heen verwijst)

Dit was de laatste e-mail die we u wilden voorleggen.

21. Nu volgt een aantal stellingen over de manier waarop u omgaat met wachtwoorden, back-ups, updates en beveiligingssoftware in uw eigen tijd (buiten werktijd). U kunt steeds antwoord geven op een schaal van nooit tot altijd.

*[Gedrag: gebruik van wachtwoorden]*

| | | Nooit | Zelden | Soms | Vaak | Altijd | N.V.T. |
|---|---|---|---|---|---|---|---|
| a | Ik deel mijn persoonlijke wachtwoorden met anderen | 5 | 4 | 3 | 2 | 1 | |
| b | Ik gebruik simpele, korte wachtwoorden, met bijvoorbeeld slechts 1 cijfer of hoofdletter | 5 | 4 | 3 | 2 | 1 | |
| c | Ik gebruik hetzelfde wachtwoord voor verschillende toepassingen, bijvoorbeeld zowel voor sociale media als online bankieren en webwinkels | 5 | 4 | 3 | 2 | 1 | |

*[Gedrag: Back-uppen van belangrijke bestanden]*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| d | Ik maak back-ups[58] van belangrijke bestanden | 1 | 2 | 3 | 4 | 5 | |
| e | Ik bewaar persoonlijke informatie op een versleutelde manier zodat anderen deze niet zomaar kunnen lezen | 1 | 2 | 3 | 4 | 5 | |

*[Gedrag: installeren van* software *updates]*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| f | Ik installeer updates van de besturingssystemen op mijn apparaten zodra ze beschikbaar zijn | 1 | 2 | 3 | 4 | 5 | |

[58] Een back-up is een reservekopie.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| g | Ik installeer updates van de apps of software die ik gebruik, zodra ze beschikbaar zijn | 1 | 2 | 3 | 4 | 5 | |

*[Gedrag: Gebruiken van beveiligingssoftware]*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| h | Ik update mijn beveiligingssoftware[59] zodra er een nieuwe update beschikbaar is | 1 | 2 | 3 | 4 | 5 | |
| i | Ik laat beveiligingssoftware[60] mijn apparaten scannen op virussen en andere kwaadaardige software | 1 | 2 | 3 | 4 | 5 | |

22. Nu volgt een aantal stellingen over de manier waarop u in uw eigen tijd (buiten werktijd)internet gebruikt. U kunt steeds antwoord geven op een schaal van nooit tot altijd.

*[Gedrag: Voorzichtig zijn op internet]*

| | | Nooit | Zelden | Soms | Vaak | Altijd | N.V.T. |
|---|---|---|---|---|---|---|---|
| a | Ik download software, films, games of muziek uit illegale bronnen | 5 | 4 | 3 | 2 | 1 | |
| b | Ik gebruik browser extensies[61] die mij helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren | 1 | 2 | 3 | 4 | 5 | |
| c | Ik maak gebruik van openbare WiFi (bijvoorbeeld in horeca of openbaar vervoer), zonder VPN verbinding[62] | 5 | 4 | 3 | 2 | 1 | |

*[Gedrag: Niet zomaar delen van persoonlijke gegevens]*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| d | Ik controleer de privacy-instellingen van mijn apparaten, apps of sociale media | 1 | 2 | 3 | 4 | 5 | |
| e | Ik deel persoonlijke informatie, zoals mijn huisadres, e-mailadres of telefoonnummer via sociale media | 5 | 4 | 3 | 2 | 1 | |

[59] Beveiligingssoftware beschermt apparaten tegen kwaadaardige software, zoals spyware, virussen en ransomware. Voorbeelden zijn Windows Defender Antivirus, Panda Free Antivirus of Norton Security.

[60] Beveiligingssoftware beschermt apparaten tegen kwaadaardige software, zoals spyware, virussen en ransomware. Voorbeelden zijn Windows Defender Antivirus, Panda Free Antivirus of Norton Security.

[61] Een browser extensie is software die een browser extra functionaliteit beidt, zoals het managen van cookies of advertenties tijdens het surfen op internet.

[62] Een VPN (Virtual Private Network) verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| f | Ik ben selectief in het accepteren van connectieverzoeken van anderen tot mijn sociale media | 1 | 2 | 3 | 4 | 5 | |

*[Gedrag: Zorgvuldig omgaan met e-mails die bijlagen of links bevatten].*

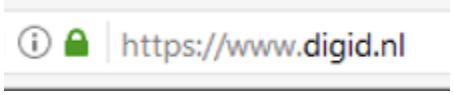
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| g | Ik verwijder e-mails die ik niet vertrouw direct | 1 | 2 | 3 | 4 | 5 | |
| h | Wanneer ik twijfel over de echtheid van een e-mail, neem ik contact op met de afzender om te vragen of er daadwerkelijk een e-mail naar mij is verstuurd | 1 | 2 | 3 | 4 | 5 | |
| i | Ik open bijlagen in e-mails, ook als de e-mail afkomstig is van een onbekende afzender | 5 | 4 | 3 | 2 | 1 | |

*[kennistest. *=juist antwoord]*

23. Hoeveel weet u over computerbeveiliging?
-Heel weinig -Weinig -Redelijk weinig -Gemiddeld -Redelijk veel -Veel -Heel veel

24. Hier ziet u een afbeelding van een adresbalk. Is dit een betrouwbare URL (webadres)?
-Ja
-Nee*
-Weet ik niet


25. Hier ziet u een afbeelding van een adresbalk. Is dit een betrouwbare URL (webadres)?
-Ja*
-Nee
-Weet ik niet




In dit onderdeel willen we u een aantal meerkeuzevragen stellen over computer- en internet-termen. Kies alstublieft steeds het juiste antwoord. Als u het antwoord op de vraag niet weet, kunt u dit aangeven.

26. Welke stelling over het maken van reservekopieën van belangrijke bestanden is juist?
a. Bewaar een fysieke back-up altijd op 2 plaatsen: in huis en buitenshuis

b. Alleen vertrouwen op een online back-up is niet verstandig, want het is maar de vraag of je bestanden er echt veilig zijn
c. Vermijd cd's en dvd’s voor het maken van back-ups
d. Alle bovenstaande stellingen zijn juist*
e. Weet ik niet

27. Wat is encryptie? Dat de inhoud van bestanden…
a. …door alle gebruikers kan worden ingezien
b. …is versleuteld*
c. …is gecontroleerd op virussen
d. …is verwijderd
e. Weet ik niet

28. Welke stelling is juist? Een software-update…
a. …is een programma dat is ontworpen om malware te voorkomen, op te sporen en verwijderen
b. …wordt gebruikt om netwerken of systemen te controleren op kwaadaardige activiteiten
c. …wordt uitgebracht om beveiligingsrisico's te herstellen of om het programma te wijzigen*
d. …is een kopie van gegevens die zich op een gegevensdrager (zoals een computer) bevinden om deze te kunnen herstellen
a. Weet ik niet

29. Welke van deze wachtwoorden is het sterkst?
a. Ik hou van wortels en zwemmen*
b. Pinguin123
c. honD?99
d. F@c3B0oK
e. Weet ik niet

30. Welke stelling is juist? Het installeren van een software update…
a. …dient uiterlijk binnen 1 maand na de uitgave te gebeuren
b. …wordt altijd automatisch gedaan, direct na de uitgave
c. …kan het beste gebeuren direct na de uitgave *
d. …kun je beter uitstellen, om af te wachten of er een fout in de update zit
e. Weet ik niet

31. Wat betekent het als een website is “geïnfecteerd”?
a. Dat de website niet correct wordt weergegeven
b. Dat de website problemen heeft om een verbinding te krijgen met het netwerk
c. Dat de website kwaadaardige software bevat*
d. Geen van de bovenstaande antwoorden is juist
e. Weet ik niet

32. Welke stelling is juist? Een firewall is een systeem dat…
a. …wordt gebruikt om ongewenste e-mail uit de Inbox (Postvak In) te filteren en blokkeren
b. …een netwerk of computer kan beschermen tegen misbruik van buitenaf*

c. …ook wel bekend staat als IDS (Intrusion Detection System)
d. Alle bovenstaande stellingen zijn juist
e. Weet ik niet

33. Wat is een adblocker?
a. Een programma dat ongewenste e-mails tegenhoudt
b. Software die voorkomt dat anderen controle over de computer kunnen overnemen
c. Een programma dat voorkomt dat op websites ongewenste inhoud wordt getoond*
d. Een virus dat computers blokkeert tot de gebruiker losgeld heeft betaald
e. Weet ik niet

34. Welke informatie kun je beter niet openbaar maken via sociale media?
a. Waar je je bevindt
b. Een foto van je rijbewijs
c. Persoonlijke gegevens zoals adres, geboortedatum en telefoonnummer
d. Alle bovenstaande antwoorden zijn juist*
e. Weet ik niet

35. Wat is online identiteitsfraude?
a. Het misbruiken van persoonsinformatie van iemand anders op het internet*
b. Het “vissen” (hengelen) naar inloggegevens en persoonsgegevens van iemand anders
c. Een vorm van pesten via nieuwe communicatietechnologieën
d. De verspreiding van nepnieuws op het internet
e. Weet ik niet

36. Wat is phishing? Een poging om…
a. …de controle te verkrijgen over het besturingssysteem van jouw computer
b. …inloggegevens te achterhalen en toegang te krijgen tot online accounts*
c. …je een nutteloos product te verkopen
d. Geen van de bovenstaande antwoorden is juist
e. Weet ik niet

37. Welke stelling is juist? Een spamfilter wordt gebruikt om…
a. …ongewenste gebruikers toegang te weigeren tot een netwerk
b. …ongewenste advertenties te blokkeren tijdens surfen op het internet
c. …ongewenste e-mails te weren uit de Inbox (Postvak In)*
d. …toegang te beperken tot dubieuze websites
e. Weet ik niet

38. Wat is tweestaps-verificatie?
a. Een extra laag in je beveiliging bovenop je wachtwoord*
b. Een controle of een opgegeven bewijs van identiteit echt is
c. Software die gebruikt wordt om computersystemen te verstoren
d. De combinatie van gebruikersnaam en wachtwoord voor het aanmaken van een account

e. Weet ik niet

*[verder]*

39. Hieronder staan 4 URL's (webadressen). Geef alstublieft aan welke van deze URL's verwijzen naar een betrouwbare (legitieme) website en welke naar een valse (phishing) website. Als u het niet weet, kunt u "weet ik niet" kiezen.

| | | Betrouwbare website | Valse website | Weet ik niet |
|---|---|---|---|---|
| a | www.abnamro.nl/nl/prive/service-en-contact | * | | |
| b | www.bol.com/nl/l/software/N/7000/?view=list | * | | |
| c | www.mijnoverheid.zcards.nl/digid | | * | |
| d | www.nieuwbetaalpas.rabobankinternet.com | | * | |

*[Zelfeffectiviteit]*

40. In dit blok leggen wij u stellingen voor over uzelf en uw eigenschappen. In hoeverre bent u het eens of oneens met onderstaande stellingen? Er zijn geen foute of goede antwoorden.

| | | Helemaal mee oneens | Oneens | Niet mee eens/niet mee oneens | Eens | Helemaal mee eens |
|---|---|---|---|---|---|---|
| a | Ik ben goed in staat om bij ieder account een sterk en uniek wachtwoord te gebruiken | | | | | |
| b | Het is ingewikkeld om te zorgen dat mijn bestanden worden geback-upt[63] (O) | | | | | |
| c | Het up-to-date houden van mijn software is voor mij makkelijk | | | | | |
| d | Het kost mij weinig inspanning om te zorgen dat er een virusscanner en firewall geïnstalleerd is op mijn apparaten | | | | | |
| e | Het is een grote uitdaging om voorzichtig te zijn op internet (O) | | | | | |

[63] Een back-up is een reservekopie.

| | | | | | | |
|---|---|---|---|---|---|---|
| f | Ik ben goed in staat te bepalen wat ik wel en niet veilig kan posten op sociale media | | | | | |
| g | Het is soms lastig te bepalen of ik wel of niet veilig op een link in een e-mail kan klikken (O) | | | | | |

*[Responskosten]*

41. In hoeverre bent u het eens of oneens met onderstaande stellingen? Er zijn geen foute of goede antwoorden.

| | | Helemaal mee oneens | Oneens | Niet mee eens/niet mee oneens | Eens | Helemaal mee eens |
|---|---|---|---|---|---|---|
| a | Het uitsluitend gebruiken van sterke en unieke wachtwoorden zou voor mij een nieuwe gewoonte betekenen, en dat is lastig | | | | | |
| b | Het back-uppen[64] van mijn bestanden kost mij veel tijd | | | | | |
| c | Het is onhandig om steeds mijn software up-to-date te houden | | | | | |
| d | Het kost mij veel moeite om te zorgen voor een goede virusscanner en firewall op al mijn apparaten | | | | | |
| e | Ik vind het vervelend om op te moeten letten dat ik me veilig gedraag op internet | | | | | |
| f | Het kost mij niet veel tijd om na te gaan of ik in een veilige online omgeving ben wanneer ik een online betaling wil doen (O) | | | | | |
| g | Ik vind het lastig dat ik niet zomaar alle bijlagen in e-mails mag openen | | | | | |
| h | Dat je tegenwoordig op zoveel dingen moet letten om veilig te kunnen internetten, vind ik maar een hoop gedoe | | | | | |

[64] Een back-up is een reservekopie.

42. *[a,b,c =protection motivation, d, e, f= locus of control]*

In hoeverre bent u het eens of oneens met deze stellingen? Er zijn geen foute of goede antwoorden.

| | | Helemaal mee oneens | Oneens | Niet mee eens/niet mee oneens | Eens | Helemaal mee eens |
|---|---|---|---|---|---|---|
| a | Als er een belangrijk – betaalbaar – beveiligingsproduct op de markt komt dat bijdraagt aan mijn online veiligheid, dan ben ik bereid daar geld aan uit te geven | | | | | |
| b | Ik wil graag zo min mogelijk risico lopen op cybercriminaliteit[65] | | | | | |
| c | Ik wil er alles aan doen om mezelf te beschermen tegen cybercriminaliteit | | | | | |
| d | Als het aankomt op mijn veiligheid op internet, ben ik daar in eerste instantie zelf verantwoordelijk voor | | | | | |

| | | Ligt buiten mijn controle | | | | Ligt binnen mijn controle |
|---|---|---|---|---|---|---|
| e | Het veilig houden van mijn persoonlijke gegevens | | | | | |

| | | de overheid/ politie | | | | mijzelf |
|---|---|---|---|---|---|---|
| f | De verantwoordelijkheid voor het beschermen van mijn persoonlijke gegevens ligt bij… | | | | | |

43. *[Responseffectiviteit]*

[65] De term cybercriminaliteit, ook wel online criminaliteit genoemd, verwijst naar alle vormen van criminaliteit waarbij ICT of internet gebruikt wordt om het delict te plegen. Voorbeelden zijn online fraude, het hacken van een database met persoonsgegevens en het platleggen van een website van een bank met een DDoS-aanval.

De volgende stellingen gaan over hoe mensen zich op hun computer gedragen. In hoeverre bent u het eens of oneens met de volgende stellingen? Er zijn geen foute of goede antwoorden. We willen u vragen uw mening te geven.

| | | Helemaal mee oneens | Oneens | Niet mee eens/niet mee oneens | Eens | Helemaal mee eens |
|---|---|---|---|---|---|---|
| a | Wanneer je sterke, unieke, wachtwoorden gebruikt, verklein je de kans dat je gehackt[66] wordt | | | | | |
| b | Wanneer je persoonlijke bestanden regelmatig back-upt[67], zijn de gevolgen minder groot als cybercriminelen in jouw computer inbreken | | | | | |
| c | Het up-to-date houden van software verandert niet veel aan de kans dat je slachtoffer wordt van cybercriminaliteit[68] (O) | | | | | |
| d | Als er een firewall op een computer staat, is het voor cybercriminelen moeilijker om in deze computer in te breken | | | | | |
| e | Door goed op te letten wat je doet op internet, zorg je dat je uit de handen blijft van cybercriminelen | | | | | |
| f | Het is veilig om je naam en e-mailadres op sociale media te vermelden (O) | | | | | |

44. *[gelegenheid: sociale gelegenheid]*

De volgende stellingen gaan over uw sociale omgeving. In hoeverre bent u het eens of oneens met onderstaande stellingen?

[66] Hacken is het zonder toestemming binnendringen in een account, computer of ander (deel van een) geautomatiseerd werk.
[67] Een back-up is een reservekopie.
[68] De term cybercriminaliteit, ook wel online criminaliteit genoemd, verwijst naar alle vormen van criminaliteit waarbij ICT of internet gebruikt wordt om het delict te plegen. Voorbeelden zijn online fraude, het hacken van een database met persoonsgegevens en het platleggen van een website van een bank met een DDoS-aanval.

| | | Helemaal mee oneens | Oneens | Niet mee eens/niet mee oneens | Eens | Helemaal mee eens |
|---|---|---|---|---|---|---|
| a | Mensen om mij heen (familie/vrienden/kennissen) sporen mij aan in het maken van back-ups[69] van belangrijke bestanden | | | | | |
| b | Als ik mensen om mij heen (familie/vrienden/kennissen) zou vertellen dat ik heel voorzichtig ben op internet, zouden zij zeggen dat dat een goed idee is | | | | | |
| c | Mensen om mij heen (familie/vrienden/kennissen) vinden online veiligheid belangrijk | | | | | |
| d | Mensen om mij heen (familie/vrienden/kennissen) delen vaak persoonlijke informatie (zoals hun e-mailadres, adres of telefoonnummer) op sociale media (O) | | | | | |
| e | Als ik slachtoffer zou worden van cybercriminaliteit[70], zou ik daarover kunnen praten met mensen om mij heen (familie/vrienden/kennissen) | | | | | |

45. *[gelegenheid: materiële gelegenheid]* De volgende stellingen gaan over uw thuissituatie. In hoeverre bent u het eens of oneens met onderstaande stellingen?

| | | Helemaal mee oneens | Oneens | Niet mee eens/niet mee oneens | Eens | Helemaal mee eens |
|---|---|---|---|---|---|---|
| a | In ons huishouden is er financiële ruimte om beveiligingsmiddelen aan te schaffen, zoals een virusscanner, VPN[71] of clouddienst[72] | | | | | |

[69] Een back-up is een reservekopie.

[70] De term cybercriminaliteit, ook wel online criminaliteit genoemd, verwijst naar alle vormen van criminaliteit waarbij ICT of internet gebruikt wordt om het delict te plegen. Voorbeelden zijn online fraude, het hacken van een database met persoonsgegevens en het platleggen van een website van een bank met een DDoS-aanval.

[71] Een VPN (Virtual Private Network) verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.

[72] Een clouddienst biedt opslagruimte aan op internet voor de opslag van bestanden, zoals foto's.

| | | | | | | |
|---|---|---|---|---|---|---|
| b | Ik heb de beschikking over een wachtwoordmanager[73] voor het veilig opslaan van wachtwoorden | | | | | |
| c | Ik heb toegang tot informatie over online veiligheid, bijvoorbeeld via websites, televisie, sociale media of via nieuwsbrieven | | | | | |

De term cybercriminaliteit, ook wel online criminaliteit genoemd, verwijst naar alle vormen van criminaliteit waarbij ICT of internet gebruikt wordt om het delict te plegen. Voorbeelden zijn online fraude, het hacken van een database met persoonsgegevens en het platleggen van een website van een bank met een DDoS-aanval.

*[Gepercipieerde kwetsbaarheid]*

46. Hoe groot schat u de gemiddelde kans dat iemand in Nederland slachtoffer wordt van cybercriminaliteit in het komende jaar?

*[slider van 0 tot 100%]*

*[page break]*

47. Hoe groot schat u de kans dat u slachtoffer wordt van cybercriminaliteit in het komende jaar?

*[slider van 0 tot 100%]*

48. *[a t/m f= angst voor slachtofferschap, g= Gepercipieerde kwetsbaarheid, h= Gepercipieerde impact]*

In hoeverre bent u het eens of oneens met onderstaande stellingen? Er zijn geen foute of goede antwoorden.

| | | Helemaal mee oneens | Oneens | Niet mee eens/niet mee oneens | Eens | Helemaal mee eens |
|---|---|---|---|---|---|---|
| a | Ik ben bang om slachtoffer te worden van cybercriminaliteit in de nabije toekomst | | | | | |
| b | Het idee dat iemand zonder toestemming in mijn online | | | | | |

[73] Een wachtwoordmanager of wachtwoordkluis is een veilige digitale kluis voor het maken, gebruiken en versleuteld bewaren van je wachtwoorden.

| | | | | | | |
|---|---|---|---|---|---|---|
| | bankrekening kan inloggen maakt me bang | | | | | |
| c | Ik maak me zorgen dat ik slachtoffer kan worden van phishing[74] | | | | | |
| d | Ik maak me druk over de mogelijkheid dat mijn computer gehackt[75] kan worden | | | | | |
| e | Ik denk dat het makkelijk kan gebeuren dat ik online word opgelicht | | | | | |
| f | Dat er ransomware[76] op mijn computer kan komen, maakt me ongerust | | | | | |
| g | Het is goed mogelijk dat ik het komende jaar slachtoffer word van cybercriminaliteit | | | | | |
| h | Als ik slachtoffer zou worden van cybercriminaliteit, zou dat ernstige gevolgen kunnen hebben | | | | | |

49. *[Gepercipieerde impact]*

Wij willen graag weten hoe erg u het zou vinden als onderstaande dingen zouden gebeuren. Er zijn geen foute of goede antwoorden. U kunt antwoorden op een schaal van helemaal niet erg tot heel erg.

| | Hoe erg zou het zijn als... | Helemaal niet erg | | | | Heel erg |
|---|---|---|---|---|---|---|
| a | ...al uw waardevolle bezittingen werden gestolen, terwijl u geen verzekering had en er geen mogelijkheid was om een deel terug te krijgen | 0 | 1 | 2 | 3 | 4 |
| b | …iemand uw creditcard-informatie zou stelen en betalingen deed met uw creditcard | 0 | 1 | 2 | 3 | 4 |
| c | …iemand zou inloggen in uw online bankrekening en uw geld zou stelen | 0 | 1 | 2 | 3 | 4 |

[74] 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.

[75] Hacken is het zonder toestemming binnendringen in een account, computer of ander (deel van een) geautomatiseerd werk.

[76] Ransomware is kwaadaardige software die een computer blokkeert of bestanden versleutelt. Pas als je losgeld betaalt, zou je de computer of de bestanden weer kunnen gebruiken.

| | | | | | | |
|---|---|---|---|---|---|---|
| d | …uw apparaat traag wordt omdat er malware[77] op staat | 0 | 1 | 2 | 3 | 4 |
| e | …iemand uw identiteit zou misbruiken | 0 | 1 | 2 | 3 | 4 |
| f | …uw e-mailaccount automatisch schadelijke software, zoals een virus, zou versturen aan iedereen in uw contactenlijst | 0 | 1 | 2 | 3 | 4 |
| g | …iemand die u niet kent, alles kon zien wat u op uw computer typt | 0 | 1 | 2 | 3 | 4 |

*[slachtofferschap]*

Kunt u alstublieft aangeven of u in aanraking bent gekomen met de volgende vormen van cybercriminaliteit:

| | | Ja, in de afgelopen 12 maanden | Ja, langer geleden dan 12 maanden | Nee | Weet ik niet |
|---|---|---|---|---|---|
| 50a | Bent u weleens slachtoffer geworden van phishing[78]? | [ga door naar 50b] | | | |
| 51a | Heeft u weleens gemerkt dat u malware[79] had op uw apparaat (computer/laptop/smartphone/tablet)? | [ga door naar 51b] | | | |
| 52a | Heeft u weleens een product of dienst via internet gekocht en ten minste een deel daarvan betaald, waarna het product of de dienst nooit geleverd is, omdat de verkoper u heeft opgelicht? | [ga door naar vraag 52b] | | | |
| 53a | Bent u weleens slachtoffer geworden van online identiteitsfraude[80]? | [ga door naar 53b] | | | |
| 54a | Bent u weleens opgelicht doordat u geld overmaakte naar iemand die u via e-mail of internet benaderde met verhalen over snel geld verdienen via een erfenis, | [ga door naar 54b] | | | |

[77] Malware is kwaadaardige software die ongevraagd en meestal ongemerkt op uw computer wordt geïnstalleerd. Voorbeelden van malware zijn virussen, trojan horses, wormen en spyware.

[78] 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.

[79] Malware is kwaadaardige software die ongevraagd en meestal ongemerkt op uw computer wordt geïnstalleerd. Voorbeelden van malware zijn virussen, trojan horses, wormen en spyware.

[80] Identiteitsfraude houdt in dat iemand zonder uw toestemming uw persoonlijke of financiële gegevens gebruikt om er zelf geld aan te verdienen. Iemand koopt bijvoorbeeld producten op uw naam of vraagt officiële documenten aan op uw naam. Meestal is identiteitsfraude een gevolg van diefstal van identiteitsgegevens, maar het kan ook zijn dat u zelf de identiteitsgegevens heeft verstrekt.

| | | | | | |
|---|---|---|---|---|---|
| | investering, loterij of iets dergelijks (online voorschotfraude[81])? | | | | |
| 55a | Heeft iemand weleens zonder uw toestemming uw webpagina en/of profielpagina (bijv. Facebook) veranderd? | [ga door naar 55b] | | | |
| 56a | Heeft iemand zich weleens zonder uw toestemming toegang verschaft tot uw online account(s), bijvoorbeeld door het wachtwoord te raden? | [ga door naar 56b] | | | |
| 57a | Is het weleens voorgekomen dat iemand heeft ingebroken in uw computer en gegevens heeft vernietigd, veranderd of gestolen? | [ga door naar 57b] | | | |
| 58a | Heeft iemand weleens zonder toestemming op uw e-mailaccount ingelogd? | [ga door naar 58b] | | | |
| 59a | Zijn uw digitale bestanden weleens ontoegankelijk gemaakt, bijvoorbeeld door ransomware? | [ga door naar 59b] | | | |
| 60a | Bent u weleens slachtoffer geworden van een andere vorm van cybercriminaliteit? | [ga door naar 60b] | | | |

50b. U heeft aangegeven dat u in de afgelopen 12 maanden slachtoffer bent geworden van phishing.
51b. U heeft aangegeven dat u in de afgelopen 12 maanden heeft gemerkt dat u malware op uw apparaat had.
52b. U heeft aangegeven dat u in de afgelopen 12 maanden online door een verkoper bent opgelicht.
53b. U heeft aangegeven dat u in de afgelopen 12 maanden slachtoffer bent geworden van online identiteitsfraude.
54b. U heeft aangegeven dat u in de afgelopen 12 maanden slachtoffer bent geworden van online voorschotsfraude.
55b. U heeft aangegeven dat iemand in de afgelopen 12 maanden zonder uw toestemming uw webpagina en/of profielpagina heeft veranderd.
56b. U heeft aangegeven dat iemand in de afgelopen 12 maanden zonder uw toestemming zich toegang heeft verschaft tot uw online account(s).
57b. U heeft aangegeven dat iemand in de afgelopen 12 maanden heeft ingebroken in uw computer en gegevens heeft vernietigd, veranderd of gestolen.
58b. U heeft aangegeven dat iemand in de afgelopen 12 maanden zonder toestemming op uw e-mailaccount heeft ingelogd.
59b. U heeft aangegeven dat in de afgelopen 12 maanden uw digitale bestanden ontoegankelijk gemaakt zijn.
60b. U heeft aangegeven dat u in de afgelopen 12 maanden slachtoffer bent geworden van een andere vorm van cybercriminaliteit.

[81] Online voorschotfraude is een vorm van internetfraude. Kern van voorschotfraude is dat slachtoffers een voorschot moeten betalen om een groot bedrag te ontvangen. Het gaat dan bijvoorbeeld om een zogenaamde erfenis, investering of loterij.

*[voor elke vraag worden de volgende vervolgvragen gesteld:]*

c. Heeft u aan het (meest recente) incident schade ondervonden?

| | | Ja | Nee |
|---|---|---|---|
| a | Geld kwijtgeraakt | | |
| b | Bestanden kwijtgeraakt | | |
| c | Tijd kwijtgeraakt | | |
| d | Emotionele schade | | |
| e | Andere schade | | |

d. Wij willen graag weten of uw ervaring met cybercriminaliteit invloed heeft gehad op uw latere online gedrag. Gedraagt u zich door het (meest recente) incident meer of minder voorzichtig op internet?

-Veel minder voorzichtig
-Iets minder voorzichtig
-Ik ben me niet meer/minder voorzichtig gaan gedragen
-Iets voorzichtiger
-Veel voorzichtiger

*61. [zelfcontrole]*

De volgende uitspraken gaan over hoe u tegen uzelf aankijkt. Wilt u alstublieft aangeven in hoeverre deze uitspraken op u van toepassing zijn?

| | | Helemaal niet op mij van toepassing | | | | Heel erg op mij van toepassing |
|---|---|---|---|---|---|---|
| a | Ik vind het moeilijk om met slechte gewoontes te stoppen | 1 | 2 | 3 | 4 | 5 |
| b | Ik ben lui | 1 | 2 | 3 | 4 | 5 |
| c | Ik zeg ongepaste dingen | 1 | 2 | 3 | 4 | 5 |
| d | Ik doe wel eens dingen die slecht voor me zijn, omdat ze leuk zijn | 1 | 2 | 3 | 4 | 5 |
| e | Ik zou willen dat ik meer zelfdiscipline had | 1 | 2 | 3 | 4 | 5 |
| f | Pleziertjes weerhouden me er soms van mijn (huis)werk af te krijgen | 1 | 2 | 3 | 4 | 5 |
| g | Ik heb moeite met concentreren | 1 | 2 | 3 | 4 | 5 |
| h | Soms kan ik mezelf er niet van weerhouden iets te doen, zelfs als ik weet dat het verkeerd is | 1 | 2 | 3 | 4 | 5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| i | Ik doe vaak dingen zonder goed na te denken over mogelijke alternatieven | 1 | 2 | 3 | 4 | 5 |
| j | Ik kan verleidingen goed weerstaan | 5 | 4 | 3 | 2 | 1 |
| k | Ik kan goed werken aan lange termijn doelen | 5 | 4 | 3 | 2 | 1 |
| l | Ik weiger dingen die slecht voor me zijn | 5 | 4 | 3 | 2 | 1 |
| m | Mensen zeggen dat ik een ijzeren zelfdiscipline heb | 5 | 4 | 3 | 2 | 1 |

62. We zouden u graag een aantal vragen willen stellen over uw achtergrondkenmerken.

a. Wat is uw voornaamste dagelijkse bezigheid?
-Schoolgaand
-Ziek/afgekeurd
-Zorg voor gezin
-Werkloos/werkzoekend
-Werkend, betaald
-Werkend, onbetaald
-Gepensioneerd
-Anders, namelijk

b. Heeft u een partner, waarmee u tenminste 3 maanden samen bent?
-Nee, ik heb geen partner
-Ja, ik woon samen met een partner (getrouwd of ongetrouwd)
-Ja, maar ik woon niet samen

c. Uit hoeveel personen bestaat uw huishouden, inclusief uzelf?
.. personen van 16 jaar of ouder
.. personen jonger dan 16 jaar

*[objectieve meting delen persoonlijke gegevens]*

*[verleidingstechniek "autoriteit" toepassen bij 1/3 van deelnemers:]*
De onderzoekers van De Haagse Hogeschool en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) verzoeken u met klem om onderstaande vragen volledig in te vullen.

*[verleidingstechniek "wederkerigheid" toepassen bij 1/3 van deelnemers:]*
Als u onderstaande vragen volledig invult, maakt u kans op een cadeaubon ter waarde van 100 euro.

*[geen verleidingstechniek toepassen bij 1/3 van deelnemers]*

d. Wat is uw volledige naam (voornamen en achternaam)?

[] zeg ik liever niet

e. Wat is uw e-mailadres?

[] zeg ik liever niet

f. Wat is het e-mailadres van één van uw bekenden, vrienden of familieleden? *(wij benaderen hen uitsluitend om deel te nemen aan deze studie)*

[] zeg ik liever niet

g. Wat is uw geboortedatum?

[] zeg ik liever niet

h. Wat is uw postcode (1234AA)?

[] zeg ik liever niet

i. Wat is uw huisnummer?

[] zeg ik liever niet

j. Vul hier alstublieft de ontbrekende tekens van uw bankrekeningnummer in. Let op: het gaat uit privacy overwegingen om slechts enkele tekens.

xxxxxxxxxxxxxxxx□□ □ [] zeg ik liever niet

63. Aan het begin van deze vragenlijst hebben wij u gevraagd een account aan te maken. Is het wachtwoord dat u heeft ingetypt overeenkomstig met hoe u normaal een wachtwoord aanmaakt voor het beschermen van uw persoonlijke gegevens?

-Nee, ik heb een simpeler wachtwoord gekozen dan dat ik normaal zou doen
-Nee, ik heb een ingewikkelder wachtwoord gekozen dan dat ik normaal zou doen
-Ja, ik heb een wachtwoord gekozen op dezelfde wijze als dat ik normaal zou doen

# Bijlage 2: Informed consent

**Online activiteiten van Nederlandse burgers**

Dank dat u wilt deelnemen aan dit onderzoek. Uw mening en ervaringen zijn erg belangrijk voor ons en we stellen het zeer op prijs dat u mee doet.

*Waarover gaat deze vragenlijst?*
Onderzoekers van de Haagse hogeschool en het NSCR willen graag weten hoe u denkt over online activiteiten en wat u doet op dit gebied. Het draait daarbij om de activiteiten die u doet in uw eigen tijd (buiten werktijd). Voorbeelden van vragen zijn: Hoe vaak bent u online? En heeft iemand zonder uw toestemming uw webpagina of profielpagina (bijv. Facebook) wel eens veranderd? Ook komen er stellingen aan bod. Een voorbeeld van een stelling is: Het up-to-date houden van mijn software is voor mij makkelijk. U kunt dan antwoorden met: helemaal mee eens, mee eens, neutraal, mee oneens, helemaal mee oneens. Ook leggen we u een aantal situaties voor die u zou kunnen tegenkomen op internet. We vragen u daarbij dan wat u zou doen in deze situatie. Het invullen zelf neemt ongeveer 25 minuten in beslag.

*Alles blijft geheim!*
We willen u nadrukkelijk erop wijzen dat uw deelname vrijblijvend is. Uw antwoorden worden volledig anoniem verwerkt. Uw privacy is volledig gewaarborgd. Mocht u niet willen dat uw data gebruikt wordt, dan kan de informatie te allen tijde en zonder opgave van reden teruggetrokken worden.

*Hoe geeft u antwoord?*
- Per vraag kunt u meestal één antwoord geven, behalve wanneer expliciet vermeld staat dat u meerdere antwoorden kunt geven.
- Passen de antwoorden niet helemaal bij uw situatie? Kies dan het antwoord dat het beste bij u past.

**Belangrijk**: We willen u verzoeken de vragenlijst in één keer volledig in te vullen en niet tussentijds te stoppen of te wisselen van apparaat dat u gebruikt voor het invullen.

Als u meer informatie over het onderzoek wilt dan kunt u contact opnemen met [panelbureau helpdesk]

□ Ik heb de informatie hierboven gelezen en doe mee met het onderzoek

# Bijlage 3: Debriefing

Dit is het einde van deze vragenlijst. Allereerst willen wij u bedanken voor uw deelname aan dit onderzoek.

Ook willen wij u graag nog wat meer informatie geven over de vragenlijst die u zojuist heeft ingevuld. Aan het begin van de vragenlijst hebben wij aangegeven dat dit onderzoek zou gaan over online activiteiten. Het onderzoek ging echter ook over een ander onderwerp: veilig internet gebruik. Met de onderzoeksresultaten kunnen de onderzoekers in kaart brengen hoe Nederlanders zich gedragen op internet, met als uiteindelijke doel dat we Nederlanders kunnen helpen zichzelf beter te beschermen tegen internetcriminelen.

Om dit onderwerp goed te kunnen onderzoeken was het noodzakelijk om u op enkele punten in het onderzoek niet te informeren over de werkelijke reden dat wij bepaalde vragen aan u hebben gesteld. Hieronder vertellen we u op welke momenten dit heeft plaatsgevonden, hoe en waarom.

Aanmaken van een account:
Helemaal aan het begin van het onderzoek kreeg u het verzoek tot het aanmaken van een account. Het doel van deze vraag was om te bepalen of Nederlanders weten waaraan een sterk wachtwoord voldoet en of men deze kennis in de praktijk ook daadwerkelijk toepast. Met een speciaal programma dat wachtwoorden analyseert op sterkte zal worden bepaald wat de sterkte is van uw wachtwoord. Uw wachtwoord zelf wordt niet opgeslagen door het panelbureau en ook op geen enkele wijze met de onderzoekers of anderen gedeeld. Alleen de sterkte van uw wachtwoord wordt met de onderzoekers gedeeld.

Klikken op een link:
Hierna kreeg u het verzoek om een bestand te installeren via een link, zogenaamd omdat een filmpje niet wilde afspelen. Het doel van deze vraag was om te onderzoeken of deelnemers van dit onderzoek klikken op een link om software te installeren, wanneer er tekenen zijn dat dit software betreft van dubieuze oorsprong. Ongeacht uw antwoord is er op geen enkele manier daadwerkelijk software op uw apparaat geïnstalleerd. Ook werd u medegedeeld dat u 5 minuten tijd had voor het maken van dit onderdeel. Aan een aantal deelnemers is gevraagd tijdens dit blok flink door te werken. Hiermee wilden de onderzoekers bepalen of deelnemers eerder geneigd zijn software te downloaden onder tijdsdruk.

Delen van persoonlijke informatie:
Aan het einde van het onderzoek kreeg u het verzoek om persoonlijke informatie met ons te delen, zoals een deel van uw rekeningnummer. Het doel van deze vraag was om te onderzoeken of respondenten dergelijke persoonlijke informatie delen met derden. Het panelbureau zal de door u ingevulde gegevens op geen enkele wijze opslaan en de onderzoekers zullen alleen te weten komen dat u iets heeft ingevuld, maar niet wat u heeft ingevuld.

Wij hopen op uw begrip en danken u nogmaals voor uw deelname.

Voor meer informatie of vragen kunt u contact opnemen met de helpdesk van het panelbureau.

De onderzoekers

# Bijlage 4: Compleet overzicht van resultaten voor alle gemeten gedragingen

*Beschrijving zelf-gerapporteerd gedrag*

| Type cybergedrag | Stelling (schaal 1-5, hoe hoger de score hoe veiliger het gedrag) | N | Gemiddelde | S.D. |
|---|---|---|---|---|
| Wachtwoord gebruik | Ik deel mijn persoonlijke wachtwoorden met anderen (O[82]) | 2421 | 4.68 | 0.59 |
| | Ik gebruik simpele, korte wachtwoorden, met bijvoorbeeld slechts 1 cijfer of hoofdletter (O) | 2405 | 3.89 | 1.15 |
| | Ik gebruik hetzelfde wachtwoord voor verschillende toepassingen, bijvoorbeeld zowel voor sociale media als online bankieren en webwinkels (O) | 2403 | 3.53 | 1.21 |
| Opslaan van belangrijke bestanden | Ik maak back-up van belangrijke bestanden | 2377 | 3.30 | 0.70 |
| | Ik bewaar persoonlijke informatie op een versleutelde manier zodat anderen deze niet zomaar kunnen lezen | 2284 | 2.33 | 1.29 |
| Installeren van updaten | Ik installeer updates van de besturingssystemen op mijn apparaten zodra ze beschikbaar zijn | 2362 | 3.97 | 1.40 |
| | Ik installeer updates van de apps of software die ik gebruik, zodra ze beschikbaar zijn | 2364 | 3.97 | 1.14 |
| | Ik update mijn beveiligingssoftware zodra er een nieuwe update beschikbaar is | 2289 | 4.19 | 1.30 |
| Gebruik van beveiligingssoftware | Ik laat beveiligingssoftware mijn apparaten scannen op virussen en andere kwaadaardige software | 2311 | 3.95 | 1.23 |

[82] (O)= score van de stelling is omgedraaid. Voor alle stellingen geldt daardoor: hoe hoger de score, hoe veiliger het gedrag.

| | | | | |
|---|---|---|---|---|
| | Ik gebruik browser extensies die mij helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren | 2278 | 2.73 | 1.17 |
| Alertheid tijdens internetgebruik | Ik download software, films, games of muziek uit illegale bronnen (O) | 2382 | 4.75 | 1.11 |
| | Ik maak gebruik van openbare WiFi (bijvoorbeeld in horeca of openbaar vervoer), zonder VPN verbinding (O) | 2385 | 3.66 | 1.21 |
| | Ik controleer de privacy-instellingen van mijn apparaten, apps of sociale media | 2375 | 2.96 | 1.48 |
| Online delen van persoonlijke gegevens | Ik deel persoonlijke informatie, zoals mijn huisadres, e-mailadres of telefoonnummer via sociale media (O) | 2322 | 4.49 | 1.13 |
| | Ik ben selectief in het accepteren van connectieverzoeken van anderen tot mijn sociale media | 2114 | 4.35 | 0.64 |
| Omgaan met bijlagen en hyperlinks in e-mails | Ik verwijder e-mails die ik niet vertrouw direct | 2414 | 4.74 | 1.02 |
| | Wanneer ik twijfel over de echtheid van een e-mail, neem ik contact op met de afzender om te vragen of er daadwerkelijk een e-mail naar mij is verstuurd | 2324 | 2.46 | 1.20 |
| | Ik open bijlagen in e-mails, ook als de e-mail afkomstig is van een onbekende afzender (O) | 2418 | 4.62 | 0.59 |
| Totaal gemiddelde | Gemiddelde van 18 stellingen over (zelf-gerapporteerd) gedrag | 2419 | 3.81 | 0.81 |

*Beschrijving overige metingen gedrag*

| | *N* | *%* |
|---|---|---|
| **Wachtwoord sterkte** | | |
| Zwak: Entropie <48 | 1653 | 68,1% |
| Sterk: Entropie 48+ | 773 | 31,9% |
| | | |
| **Keuze software** | | |
| Onveilige keuze (op “ja” geklikt) | 980 | 40,4% |
| Veilige keuze (niet op “ja” geklikt) | 1446 | 59,6% |
| | | |
| **E-mail keuze** | | |
| Onveilige keuze (tenminste 1x op phishing hyperlink geklikt) | 515 | 21,2% |
| Veilige keuze (2x niet op phishing hyperlink geklikt) | 1911 | 78,8% |
| | | |
| **Delen persoonlijke gegevens** | | |
| Volledige naam | 751 | 31,0% |
| E-mailadres | 681 | 28,1% |
| E-mailadres bekende | 35 | 1,4% |
| Geboortedatum | 910 | 37,5% |
| Postcode | 655 | 27,0% |
| Huisnummer | 496 | 20,4% |
| Laatste 3 cijfers rekeningnummer | 116 | 4,8% |

# Bijlage 5: Begeleidingscommissie

Voorzitter begeleidingscommissie
de heer prof. dr. K. van den Bos
UU - Faculteit Recht, Economie Bestuur en Organisatie (REBO)

Lid begeleidingscommissie
de heer drs. L.F. Heuts
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Lid begeleidingscommissie
mevrouw dr. H. Young
TNO

Lid begeleidingscommissie
de heer T. Hilbrink
XS4ALL internet B.V.

Lid begeleidingscommissie
de heer J.P. Raeven
JenV, Directie Rechtshandhaving en Criminaliteitsbestrijding (DRC)

(Tijdelijk) lid begeleidingscommissie
de heer dr. R. Teijl
JenV, Dir.-Generaal Rechtspleging & Rechtshandhaving (DGRR)

(Tijdelijk) lid begeleidingscommissie
mevrouw L.R. de Korte, MSc
JenV, Directie Rechtshandhaving en Criminaliteitsbestrijding (DRC)

(Tijdelijk) lid begeleidingscommissie (in de afrondende fase van het onderzoek)
mevrouw Mr. E.C. van Ginkel
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

# Bijlage 6: Expertbijeenkomst

Bij de expertbijeenkomst, gehouden op 17 juli 2019, waren naast de onderzoekers aanwezig:

Boris de Ruyter, Principal Scientist, Philips Research

Remco Wijn, Behavioral researcher, TNO

Esther Spaans, Sociaal Psycholoog Cybersecurity & Compliance, Hoffmann

Diederik van Luijk, Cyber Security Future Strategist, Nederlandse overheid

Thomas Dirkmaat, Coordinator Behavioral Insights Team, Ministerie van Economische zaken

Marianne Junger, Hoogleraar Cyber Security and Business, Universiteit Twente

Raoul Notté, docent-onderzoeker, Haagse Hogeschool