# Samenvatting

## Achtergrond

Bij online activiteiten is het belangrijk dat mensen zich veilig gedragen, om te voorkomen dat ze slachtoffer worden van cybercriminaliteit. Hoewel maatregelen als firewalls, virusscanners, en tweestapsverificatie goed werken om de risico's van onveilig wachtwoordgedrag en het onveilig delen van persoonsgegevens tegen te gaan, is een aanzienlijk deel van het slachtofferschap terug te voeren op menselijk gedrag. Eerder onderzoek vanuit het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC; Van 't Hoff-de Goede et al., 2019) heeft zich gericht op de vraag hoe veilig Nederlanders zich online gedragen en hoe dit kan worden verklaard. Eén van de belangrijkste conclusies uit het onderzoek was dat, hoewel zowel zelfgerapporteerd gedrag als geobserveerd gedrag onveilig bleek, mensen zich onveiliger gedroegen dan dat ze zelf rapporteerden, met name bij het gebruik van wachtwoorden en het online delen van persoonsgegevens. Het huidige onderzoek richtte zich specifiek op deze laatste twee doelgedragingen. Het onderzoek bestond uit een literatuurstudie en twee empirische studies. Onderzocht is welke psychologische factoren een rol spelen bij 1) of mensen veilige wachtwoorden aanmaken en 2) of mensen online hun persoonsgegevens alleen delen wanneer dit veilig en/of noodzakelijk is. Daarnaast hebben we een interventie ontwikkeld en getest om veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens te bevorderen.

## Conclusies literatuurstudie

In het huidige onderzoek zijn op basis van de *protection motivation theory* (PMT) de volgende psychologische factoren gemeten om te onderzoeken in hoeverre deze factoren een rol spelen bij veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens: responskosten, kwetsbaarheid, ernst, zelfeffectiviteit en responseffectiviteit. Naast de factoren uit de PMT is ook de rol van verantwoordelijkheid bij beide doelgedragingen onderzocht. Literatuur over *responskosten* (de inschatting van kosten die gemaakt worden om het doelgedrag te vertonen) liet zien dat responskosten negatief samenhangen met zelf zelfgerapporteerd veilig online gedrag: Hoe hoger de responskosten, hoe minder veilig het wachtwoordgedrag en hoe minder veilig persoonsgegevens online worden gedeeld. Wat betreft de *kwetsbaarheid* van mensen voor negatieve consequenties van onveilig online gedrag, liet de literatuur zien dat mensen online vaak een lage kwetsbaarheid ervaren. Ook liet de literatuur zien dat er een positieve relatie is tussen kwetsbaarheid en veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens: hoe hoger de waargenomen kwetsbaarheid, hoe veiliger het online gedrag. Waar kwetsbaarheid zich voornamelijk richt op hoe groot de kans is dat de negatieve consequenties van onveilig online gedrag optreden, richt *ernst* zich meer op hoe erg die negatieve consequenties nu precies gevonden worden. Onderzoek liet zien dat er een positieve relatie is tussen hoe mensen de ernst van de consequenties van onveilig gedrag inschatten en hoe veilig ze zich online gedragen: hoe hoger de waargenomen ernst, hoe veiliger het online gedrag. Verder bleek ook uit de literatuurstudie dat de mate waarin iemand zich in staat voelt om de risico's tegen te gaan ook een bepalende factor is voor het vertonen van veilig online gedrag. Hierbij wordt onderscheid gemaakt tussen *responseffectiviteit* en *zelfeffectiviteit*. Zelfeffectiviteit is de mate waarin iemand zichzelf in staat acht het gewenste gedrag te

vertonen, en responseffectiviteit is de mate waarin iemand verwacht dat het vertonen van het gewenste gedrag de risico's zal wegnemen. Uit het literatuuroverzicht van Van 't Hoff-de Goede et al. (2019) bleek al dat beide vormen van effectiviteit een belangrijke rol spelen bij veilig online gedrag. Onderzoeken die daarna zijn uitgevoerd lieten eenzelfde beeld zien: mensen die zich niet in staat voelen om de risico's tegen te gaan, zijn ook vaker slachtoffers van cybercriminaliteit. Ten slotte bleek uit de literatuur dat *verantwoordelijkheid* ook een rol speelt bij veilig online gedrag. Bij mensen die online veiligheid als hun persoonlijke verantwoordelijkheid beschouwen, is het waarschijnlijker dat zij beschermende maatregelen nemen.

In Studie 1 hebben we onderzocht welke van deze psychologische factoren veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens bevorderen en belemmeren. Vervolgens hebben we in Studie 2 een interventie ontwikkeld en getest, die gericht was op belangrijke psychologische factoren zoals geïdentificeerd in Studie 1.

## Studie 1

In Studie 1 onderzochten we met een vragenlijst onderzocht welke psychologische factoren uit het model in Figuur 1 een rol spelen bij veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens. We gebruikten hiervoor een *gedragsmaat* (i.e., sterkte en uniekheid van een aangemaakt wachtwoord; deelname aan een winactie en het aantal en type gedeelde persoonsgegevens) en *zelfrapportage* van gedrag (i.e., mate waarin deelnemers sterke en unieke wachtwoorden gebruiken; mate waarin deelnemers veilig online persoonsgegevens delen). De psychologische factoren zijn uitgevraagd met verschillende stellingen De studie bevatte daarnaast verschillende open vragen en achtergrondvragen, om een nog vollediger beeld te krijgen van de bevorderende en belemmerende factoren van veilig online gedrag.

De resultaten van Studie 1 lieten zien dat onveilig gedrag in hoge mate voorkwam bij beide doelgedragingen. Bijna 84% van de deelnemers liet onveilig wachtwoordgedrag zien door een zwak of zeer zwak wachtwoord aan te maken, ook was er bij een deel van de deelnemers sprake van hergebruik van wachtwoorden. Daarnaast nam bijna 81% van de deelnemers deel aan de winactie. Met deze deelname stemden deelnemers dus in het met online delen van hun persoonsgegevens. Meer dan 70% van de deelnemers die deelnamen aan de winactie deelde hierbij alle persoonsgegevens, waaronder ook de laatste drie cijfers van hun bankrekening (85.2% van de deelnemers), terwijl het niet verplicht was om al deze gegevens te delen. Er is bij beide doelgedragingen dus veel ruimte voor verbetering.

Vervolgens hebben we gekeken welke psychologische factoren *veilig wachtwoordgedrag* (gedragsmaten, zelfrapportage gedrag) voorspelden. De resultaten van Studie 1 lieten zien dat van de onderzochte factoren met name responskosten, zelfeffectiviteit en ernst belangrijke voorspellers van veilig wachtwoordgedrag waren. Hoe lager de inschatting van responskosten en hoe hoger de inschatting van zelfeffectiviteit en de ernst van risico's, hoe veiliger het wachtwoordgedrag. De resultaten op de open vragen over de belemmerende en bevorderende factoren onderschreven het belang van bovengenoemde factoren. Eén van de meest genoemde belemmerende factoren was zelfeffectiviteit:

deelnemers vonden het met name moeilijk om veilige wachtwoorden te onthouden. De responskosten die gepaard gaan met veilig wachtwoordgedrag werden ook genoemd als belemmerde factor. De vraag over de bevorderende factoren liet zien dat deelnemers aangaven behoefte te hebben aan wachtwoordmanagers/apps die hen helpen met veilig wachtwoordgedrag.

Daarnaast hebben we gekeken welke psychologische variabelen het *veilig online delen van persoonsgegevens* voorspelden. Van de onderzochte factoren waren met name zelfeffectiviteit en ernst belangrijke voorspellers van het veilig online delen van persoonsgegevens. Hoe hoger de inschatting van zelfeffectiviteit en de ernst van risico's, hoe veiliger het gedrag. De resultaten op de open vragen over de belemmerende en bevorderende factoren onderschreven dat bij het veilig online delen van persoonsgegevens zelfeffectiviteit een belemmerende factor was. Hiernaast kwamen responskosten ook naar voren als belemmerende factor. De vraag over bevorderende factoren liet zien dat verantwoordelijkheid een belangrijke factor was: deelnemers gaven aan dat websites/apps zowel minder om persoonsgegevens zouden moeten vragen, als mensen erop zouden moeten attenderen wanneer gegevens niet verplicht zijn om in te vullen. Ook leek techniek een belangrijke bevorderende factor: deelnemers gaven aan dat een extra beveiligingsprogramma of een tweestapsverificatie hen zou helpen om online veiliger om te gaan met hun persoonsgegevens.

## Studie 2

Op basis van eerder onderzoek naar gedragsverandering, recente studies in de context van cyberveiligheid, en de bevindingen van Studie 1 hebben we in Studie 2 door middel van een experiment getoetst of het verhogen van de ernst van de risico’s van onveilig gedrag en/of de zelfeffectiviteit van veilig gedrag leidt tot veiliger wachtwoordgedrag en het veiliger online delen van persoonsgegevens. Onze interventie bestond uit het communiceren van risico’s van onveilig gedrag (ernst), hoe veilig gedrag uitgevoerd kan worden (zelfeffectiviteit), of een combinatie van beide, met een controle conditie als referentiegroep. De gebruikte gedragsmaten van veilig gedrag in Studie 2 waren vergelijkbaar met die in Studie 1.

De resultaten van Studie 2 lieten zien dat onze interventie effectief was, in de zin dat deze leidde tot veiliger online gedrag. Voor *veilig wachtwoordgedrag* vonden we dat deelnemers die informatie over zelfeffectiviteit hadden gekregen, al dan niet in combinatie met informatie over de ernst van risico's, veiligere wachtwoorden aanmaakten dan deelnemers in de controle conditie die deze informatie niet hadden gekregen. De wachtwoorden van deze deelnemers hadden een hogere entropie, voldeden vaker aan de voorwaarden van een sterk wachtwoord en bevatten minder vaak persoonlijke informatie. De wachtwoorden van deelnemers die alleen informatie over de ernst van risico’s hadden gekregen waren ook deels veiliger dan de wachtwoorden van deelnemers die deze informatie niet hadden gekregen, maar deze effecten waren zwakker.

De resultaten voor verschillen tussen groepen in de samenleving lieten zien dat het effect van de interventie op entropie van het aangemaakte wachtwoord niet afhing van geslacht, leeftijd of opleidingsniveau van de deelnemers. Geslacht beïnvloedde ook niet of het wachtwoord voldeed aan de

voorwaarden voor sterke wachtwoorden, of dat het wachtwoord persoonlijke informatie bevatte. We vonden bij de maat of het wachtwoord voldeed aan de voorwaarden voor sterke wachtwoorden wel dat het effect van de interventie verschilde als functie van leeftijd en als functie van opleidingsniveau. Waar zelfeffectiviteit in alle leeftijdsgroepen resulteerde in sterkere wachtwoorden, was ernst (voornamelijk in combinatie met zelfeffectiviteit) alleen effectief bij deelnemers van gemiddelde of oudere leeftijd. Voor opleidingsniveau vonden we ook verschillen: zelfeffectiviteit, al dan niet in combinatie met ernst, resulteerde in de veiligste wachtwoorden onder hoog- en middenopgeleide deelnemers. Onder laagopgeleide deelnemers vonden we geen verschillen tussen condities.
Bij het *veilig online delen van persoonsgegevens* vonden we dat deelnemers die deelnamen aan de winactie opvallend veel niet-verplichte gegevens deelden, ook in de interventie condities. Toch vonden we ook hier dat dat de interventie effectief was, in de zin dat deze leidde tot veiliger online gedrag. Deelnemers die informatie over zelfeffectiviteit hadden ontvangen, al dan niet in combinatie met informatie over de ernst van risico's, deelden minder niet-verplichte persoonsgegevens dan deelnemers in de controle conditie die deze informatie niet hadden gekregen. De conditie waarin alleen informatie over de ernst van risico's werd gegeven verschilde niet van de controle conditie in hoeveel niet-verplichte persoonsgegevens werden gedeeld. Wel was het zo dat deelnemers vergeleken met de controle conditie vaker afzagen van deelname aan de winactie. Door niet mee te doen aan de verloting hoefden ze ook geen persoonsgegevens te delen.

De resultaten voor verschillen tussen groepen in de samenleving lieten zien dat het effect van de interventie op deelname aan de winactie afhing van geslacht (het effect was significant voor vrouwen, niet mannen), maar niet van leeftijd of opleidingsniveau. Ook lieten de resultaten zien dat leeftijd en opleiding van invloed waren op het delen van persoonsgegevens bij de winactie. Hoe ouder de deelnemers, hoe vaker ze niet-verplichte persoonsgegevens deelden. De resultaten voor opleiding lieten zien dat hoe hoger opgeleid de deelnemers waren, hoe vaker ze niet-verplichte persoonsgegevens deelden.

## Beperkingen en toekomstig onderzoek

Het huidige onderzoek biedt inzicht in welke psychologische factoren een rol spelen bij veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens. Ook laat het onderzoek zien hoe een interventie die ernst en zelfeffectiviteit verhoogt/activeert, veiliger online gedrag kan bevorderen. Toekomstige interventies die op basis van het huidige onderzoek worden ontwikkeld kunnen hierbij potentieel een belangrijke bijdrage leveren aan het voorkomen van slachtofferschap van cybercriminaliteit. Toch zijn er verschillende aspecten van het huidige onderzoek die maken dat goed is om voorzichtig om te gaan met de conclusies uit het onderzoek.

Hoewel de interventie in Studie 2 resulteerde in veiliger online gedrag, zien we dat de wachtwoorden in de interventie condities nog steeds zwak waren, en deelnemers nog steeds vaak hun persoonsgegevens deelden terwijl dat niet nodig was. De wachtwoorden waren niet zo zwak als in de controle conditie of

als in Studie 1, en er werden ook echt minder niet-verplichte persoonsgegevens gedeeld, maar er valt nog steeds veel winst te behalen.

Daarnaast zien we dat, hoewel we voor beide empirische studies een grote steekproef hadden die grotendeels representatief was voor de Nederlandse bevolking, we niet helemaal kunnen concluderen dat de steekproef representatief was. We hadden iets meer hoger opgeleide dan lager opgeleide deelnemers en iets minder jongere dan oudere deelnemers. Daarnaast hadden we meer uitval van deelnemers wanneer hen gevraagd werd hun persoonsgegevens bij de winactie te delen vergeleken met wanneer ze een wachtwoord aanmaakten. Dit laat zien dat er mogelijk een selectieve uitval was deelnemers, en dat een specifieke groep deelnemers de studies mogelijk niet heeft afgerond.

Eén van de sterke punten van het huidige onderzoek is de centrale rol van daadwerkelijk online gedrag. Deelnemers maakten een wachtwoord aan en kregen de keuze om bepaalde persoonsgegevens wel of niet te delen. Toch hebben deze gedragsmaten enkele beperkingen. Wat betreft het wachtwoordgedrag hebben we een entropiescore gebruikt om de sterkte van het aangemaakte wachtwoord te bepalen. Dit laat echter enkele kenmerken van veilige wachtwoorden buiten beschouwing. Het kan bijvoorbeeld zijn dat een wachtwoord een hoge entropie heeft, maar nog steeds een bestaand woord gebruikt, en daardoor geen veilig wachtwoord is. We hebben dit in Studie 2 deels ondervangen door een vraag toe te voegen of het aangemaakte wachtwoord persoonlijke informatie bevatte. Toekomstig onderzoek zou, naast de entropie score en de vragen over of wachtwoorden unieke wachtwoorden waren en of wachtwoorden persoonlijke informatie bevatten, ook andere aspecten van veilige wachtwoorden kunnen meten. Dit levert belangrijke informatie op hoe we deze specifieke aspecten van veilig wachtwoordgedrag kunnen verbeteren.

De gedragsmaat voor het veilig online delen van persoonsgegevens kent ook enkele beperkingen. Onze deelnemers deelden hun persoonsgegevens in de context van een onderzoek. Mogelijk deelden deelnemers meer persoonsgegevens doordat ze het idee hadden in een veilige omgeving te zijn. We hebben in het huidige onderzoek geen onderscheid gemaakt tussen websites waar het wel veilig of zelfs noodzakelijk is om gevoelige persoonsgegevens te delen en websites waar dit niet veilig of noodzakelijk is. Toekomstig onderzoek zou het doelgedrag kunnen meten in verschillende contexten, om te zien of dezelfde psychologische factoren een rol spelen en of de in het huidige onderzoek onderzochte interventie even effectief is in verschillende contexten.

Ten slotte is het goed om te benoemen dat hoewel Studie 2 liet zien dat het een goede keuze was om onze interventie te richten op ernst van risico's en zelfeffectiviteit, we er ook voor hadden kunnen kiezen om de interventie te richten op één van de andere in Studie 1 onderzochte psychologische factoren. Verantwoordelijkheid lijkt bijvoorbeeld ook een relevante factor bij het veilig online delen van persoonsgegevens. Toekomstig onderzoek zou zich specifiek kunnen richten op het versterken van de eigen verantwoordelijkheid om mensen meer bewust te maken van hun rol in veilig online gedrag en zo veilig online gedrag te bevorderen.

## Beleidsimplicaties en interventies

Het doel van het huidige onderzoek was om in kaart te brengen welke psychologische factoren een rol spelen bij veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens, en om te onderzoeken of het beïnvloeden van deze factoren door middel van een interventie leidt tot veiliger online gedrag. Ons doel was dus niet om een kant-en-klare interventie te ontwikkelen, die gebruikt kan worden door de overheid, websites, of andere instellingen om veilig online gedrag te bevorderen voor een breed scala aan online toepassingen. De resultaten van het huidige onderzoek kunnen wel een basis bieden voor het ontwikkelen van interventies.

Naast dat het huidige onderzoek heeft laten zien dat een interventie gericht op ernst van risico's in combinatie met zelfeffectiviteit effectief kan zijn, liet Studie 1 zien dat andere interventies wellicht ook goed kunnen werken om veilig online gedrag te bevorderen. Eén concreet advies dat we mee willen geven op basis van de resultaten van Studie 1 is dat bij veilig wachtwoordgedrag, interventies gericht op het bevorderen van het gebruik van wachtwoordmanagers effectief kunnen zijn.

Daarnaast zou de geteste interventie bij wachtwoorden en persoonsgegevens (deels) goed gecombineerd kunnen worden met andere interventietechnieken. Er kan bijvoorbeeld veel bereikt worden door in te zetten op techniek of aanpassingen aan de gebruikersomgeving. Zo zou er gebruikt kunnen worden gemaakt van tweestapsverificatie of biometrische gegevens om toegang te krijgen tot een account en zouden persoonsgegevens beter beschermd kunnen worden tegen toegang van cybercriminelen (Young et al., 2018). Ook zou een aanpassing in wetgeving effectief kunnen zijn, die websites bijvoorbeeld verplicht om informatie te verschaffen over de ernst van de risico´s of de zelfeffectiviteit voordat gebruikers een account aanmaken of hun persoonsgegevens delen. Daarnaast zouden websites en apps verplicht kunnen worden om alleen noodzakelijke persoonsgegevens uit te vragen. In combinatie met de interventie die getest is in het huidige onderzoek, die zich richtte op psychologische factoren, zouden deze technische, omgeving en wetgeving factoren het gewenste gedrag nog meer kunnen bevorderen.

Ten slotte is het belangrijk op te merken dat interventies mogelijk niet voor elke groep in de samenleving even geschikt zijn, zoals blijkt uit de analyses die verschillen aantoonden tussen groepen in de samenleving in de effectiviteit van de interventie in Studie 2 en in hoe veilig het online gedrag was in Studie 1 en Studie 2. Dit betekent dat er een zorgvuldige vertaalslag nodig is van de huidige bevindingen naar beleid, waar bij de interventie (of aspecten van de interventie) gekeken en getoetst moet worden voor wie de interventie het meest effectief is en op wat voor manier deze het best ingezet kan worden.

Samenvattend blijkt uit het huidige onderzoek dat Nederlandse burgers onveilig wachtwoordgedrag vertonen en online onveilig persoonsgegevens delen. Onze interventie gericht op het verhogen van zelfeffectiviteit en ernst van de risico's van onveilig gedrag resulteerde in veiligere wachtwoorden en veiliger online delen van persoonsgegevens, maar er is nog steeds veel winst te behalen. Deze winst is mogelijk te behalen door in te zetten op techniek en aanpassingen van de gebruikersomgeving en aanpassingen in wetgeving.