Universiteit Leiden
The Netherlands

Veilige toegang en verantwoord delen: psychologische determinanten van veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens. KCPEG onderzoeksrapport in opdracht van WODC

Mors, E. ter; Lelieveld, G.-J.; Noordewier, M.; Vliet, A. van der; Hilgevoord, V.; Dijkstra, R.; Dijk, W. van

Citation
Mors, E. ter, Lelieveld, G. -J., Noordewier, M., Vliet, A. van der, Hilgevoord, V., Dijkstra, R., & Dijk, W. van. (2022). *Veilige toegang en verantwoord delen: psychologische determinanten van veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens. KCPEG onderzoeksrapport in opdracht van WODC*. Leiden: KCPEG. Retrieved from https://hdl.handle.net/1887/3629743

Version:	Publisher's Version
License:	Leiden University Non-exclusive license
Downloaded from:	https://hdl.handle.net/1887/3629743

Note: To cite this publication please use the final published version (if applicable).

Kenniscentrum
Psychologie en Economisch Gedrag

Veilige toegang en verantwoord delen: Psychologische determinanten van veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens

Gedragsverandering ter voorkoming van slachtofferschap cybercriminaliteit

Auteurs: Dr. Emma ter Mors, Dr. Gert-Jan Lelieveld, Dr. Marret Noordewier, Alien van der Vliet, MSc, Vera Hilgevoord, MSc, Ruth Dijkstra, MSc, Prof. Dr. Wilco van Dijk.

Leiden, 1 juli 2022

Het Kenniscentrum Psychologie en Economisch Gedrag is verbonden aan de sectie Sociale, Economische en Organisatiepsychologie van de Universiteit Leiden.

www.kcpeg.nl

Veilige toegang en verantwoord delen: Psychologische determinanten van veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens

Gedragsverandering ter voorkoming van slachtofferschap cybercriminaliteit

Dr. Emma ter Mors

Dr. Gert-Jan Lelieveld

Dr. Marret Noordewier

Alien van der Vliet, MSc

Vera Hilgevoord, MSc

Ruth Dijkstra, MSc

Prof. Dr. Wilco van Dijk

Het Kenniscentrum Psychologie en Economisch Gedrag is verbonden aan de sectie Sociale, Economische en Organisatiepsychologie van de Universiteit Leiden.

Colofon

Dit onderzoek is in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) uitgevoerd door onderzoekers van het Kenniscentrum Psychologie en Economisch Gedrag (KCPEG, www.kcpeg.nl). Het KCPEG is verbonden aan de Sectie Sociale, Economische en Organisatiepsychologie van de Universiteit Leiden. Het onderzoeksteam bestond uit:

Dr. Emma ter Mors – Projectleiding

Dr. Gert-Jan Lelieveld

Dr. Marret Noordewier

Alien van der Vliet, MSc

Vera Hilgevoord, MSc

Ruth Dijkstra, MSc

Prof. Dr. Wilco van Dijk

Stagiairs/onderzoeksassistent

Jens Nilsen, Susanne Marr, Linda Bomm, Lara Meijer

Justin de Jong

Begeleidingscommissie

Prof. Dr. Marcel Zeelenberg – Voorzitter

Dr. Maureen Turina-Tumewu

Mr. Mariëlle Kolff

Drs. Antoinette de Kroon

Dr. Karin Bongers

Dr. Rutger Leukfeldt

Dr. Inge Wetzer

Voorwoord

Voor u ligt het rapport 'Veilige toegang en verantwoord delen: Psychologische determinanten van veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens'. Dit onderzoek is – in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) – uitgevoerd door het Kenniscentrum Psychologie en Economisch Gedrag (KCPEG, www.kcpeg.nl). Het KCPEG is verbonden aan de Sectie Sociale, Economische en Organisatiepsychologie van de Universiteit Leiden. Het rapport geeft inzicht in hoe veilig burgers online omgaan met hun wachtwoorden en het delen van persoonsgegevens, en welke factoren belangrijk zijn bij het opzetten van mogelijke interventies om burgers zich online veiliger te laten gedragen.

Graag willen wij iedereen bedanken die een bijdrage heeft geleverd aan dit onderzoek. Ten eerste willen we een woord van dank uitspreken aan de voorzitter en leden van de begeleidingscommissie voor het meedenken en feedback geven tijdens diverse begeleidingsbijeenkomsten. Ook willen we stagiairs Jens Nilsen, Linda Bomm, Susanne Marr en Lara Meijer en onderzoeksassistent Justin de Jong bedanken voor hun waardevolle bijdragen aan het onderzoek.

Voor vragen of feedback over het onderzoek kunt per e-mail contact opnemen met de verantwoordelijke onderzoeker: Dr. Emma ter Mors, emors@fsw.leidenuniv.nl.

Inhoudsopgave

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.

Summary

Background

To prevent becoming a victim of cybercrime, it is important that people behave safely when performing online activities. Although measures such as firewalls, virus scanners, and two-step verification contribute to mitigate the risks of unsafe password behaviour and unsafe sharing of personal data, a significant part of victimization can be traced back to human behaviour. Previous research by the WODC (Research and Documentation Centre) (Van 't Hoff-de Goede et al., 2019) has focused on the question of how safe Dutch citizens behave online and how this can be explained. One of the main conclusions of this study was that, while both self-reported and observed online behaviour were found to be unsafe, people behaved more unsafe than they reported, especially with regards to password use and the sharing of personal data. The current research focused specifically on the latter two behaviours. The research consisted of a literature review and two empirical studies. It was investigated which psychological factors play a role in 1) whether people generate safe passwords and 2) whether people share their personal data online only when it is safe and/or necessary. In addition, we developed and tested an intervention to increase safe password behaviour and safe online sharing of personal data.

Conclusions of the literature study

In the current study, based on the protection motivation theory (PMT), the following psychological factors have been measured to investigate the extent to which they play a role in safe password behaviour and the safe sharing of personal data online: response cost, perceived vulnerability, perceived severity, perceived self-efficacy, and response efficacy. In addition to the PMT factors, we also investigated the role of responsibility in both target behaviours.

Literature on *response cost* showed a negative relation between response cost (the estimation of the cost incurred to execute the target behaviour) and self-reported safe online behaviour: the higher the response cost, the less people behave safely in terms of password behaviour and the sharing of personal data online. Regarding the perceived *vulnerability* to negative consequences of unsafe online behaviour, the literature showed that people often perceive a low vulnerability, and that vulnerability is positively related to safe password behaviour and the safe sharing of personal data online: the higher the perceived vulnerability, the safer the behaviour. While vulnerability refers to the probability of the negative consequences of unsafe online behaviour occurring, perceived *severity* refers to how serious those negative consequences are perceived to be. Research showed a positive relationship between the perceived severity of consequences of unsafe online behaviour and how safe people behave online: the higher the perceived severity, the safer the behaviour. The literature study also revealed that the extent to which people feel able to counteract risks as a determining factor for displaying safe online behaviour. A distinction is made between *response efficacy* and *self-efficacy*. Self-efficacy is the degree to which a person feels capable of executing the target behaviour and response efficacy is the degree to which a person expects that executing the target behaviour will remove the risks. The literature review by Van 't Hoff-de Goede et al. (2019)

showed that both types of efficacy play an important role in safe online behaviour. Subsequent studies showed similar results: People who feel unable to counteract the risks associated with unsafe online behaviour are also more likely victims of cybercrime. Lastly, the literature showed that *responsibility* also plays a role in safe online behaviour. People who perceive online safety as their own personal responsibility are more likely to take protective measures and display safe behaviour.

In Study 1, we investigated which of these psychological factors promote or hinder safe password behaviour and the safe sharing of personal data online. Next, an intervention was developed and tested in Study 2, that was aimed at important psychological factors as identified in Study 1.

Study 1

Study 1 was a survey study in which we examined which psychological factors promote and hinder safe password behaviour and the safe sharing of personal data online. To examine this, we used a behavioural measure (i.e., strength and uniqueness of a generated password; participation in an online raffle and the amount and type of personal data shared) and a self-report measure of safe online behaviour (i.e., the extent to which participants reported to use strong and unique passwords; the extent to which participants reported to share personal data online in a safe way). The psychological factors were assessed with multiple statements. The study included several open-ended questions and background questions to provide an even more complete picture of the promoting and inhibiting factors of safe online behaviour.

The results of Study 1 showed that unsafe online behaviour occurred to a high extent for both target behaviours. Around 84% of participants displayed unsafe password behaviour by generating weak to very weak passwords. In addition, part of the participants reused passwords. Further, about 81% of the participants participated in the online raffle. With their participation, participants agreed to sharing their personal data online. Over 70% of the participations who chose to participate in the raffle shared all of their personal data, including the last three digits of their bank account (85.2% of participants), while it was not required to share all data. To conclude, there is a lot of room for improvement in both target behaviours.

Next, we looked at which psychological factors predicted *safe password behaviour*. The results of Study 1 revealed response cost, self-efficacy, and severity as important predictors of safe password behaviour. The lower the perceived response cost and the higher the perceived self-efficacy and severity of risks, the safer the password behaviour. The results of the open-ended questions about promoting and inhibiting factors underlined the importance of the abovementioned factors. The most frequently mentioned factor was self-efficacy: participants reported difficulty remembering safe passwords. The response cost associated with safe passwords was also mentioned as an inhibiting factor. The open-ended question about promoting factors showed that participants expressed the need for password managers/applications that can help them to display safer password behaviour.

In addition, we examined which psychological factors predicted the *safe sharing of personal data online*. Of the factors studied, self-efficacy and severity were important predictors of the safe

sharing of personal data online. The higher the perceived self-efficacy and severity of risks, the safer the behaviour. The results of the open-ended questions about the promoting and inhabiting factors confirmed self-efficacy as an inhibiting factor in the safe sharing of personal data online. In addition, response cost emerged as an inhibiting factor. The open-ended question about promoting factors showed that responsibility was an important factor: participants mentioned that websites/applications should request and collect fewer personal data and indicate more clearly which data are required (i.e., mandatory) and which are not. In addition, technical solutions were mentioned as an important promoting factor: participants indicated than an extra security program or two-step verification would help to display more safe online behaviour.

Study 2

Based on previous research on behavioural change, recent studies in the context of cyber security, and the results of Study 1, in Study 2 we tested by means of an experiment whether increasing the perceived severity of risks of unsafe behaviour and increasing the perceived self-efficacy of execution of safe behaviour results in safer password behaviour and safer sharing of personal data online. Our intervention consisted of the communication of risks of unsafe behaviour (severity), how safe behaviour can be performed (self-efficacy), or a combination of both, with a control group as a reference group.

The results of Study 2 showed that our intervention was effective, as it resulted in safer online behaviour. For *safe password behaviour*, we found that participants who received information about self-efficacy, on its own or combined with severity of risks, generated stronger passwords than participants in the control condition who had not received this information. Passwords had higher entropy scores, more frequently met criteria for strong passwords, and less frequently contained personal information. The passwords of participants who only received information about the severity of risks also in part were safer than the passwords of participants who had not received the information, but the effects overall were weaker.

The results for differences between groups in society showed that the effectiveness of the intervention for password entropy did not depend on participants' gender, age, or education level. Gender did not affect whether the generated password met criteria for strong passwords or whether it contained personal information either. The measure of whether the generated password met criteria for strong passwords did reveal that the effect of the intervention varied as a function of participants' age and education level. While self-efficacy resulted in stronger passwords in all age groups, severity (in particular in combination with self-efficacy) was only effective among middle-aged and older participants. For education level we found that self-efficacy, on its own or combined with severity, resulted in the safest passwords among highly and moderately educated participants. We did not find differences in conditions among low educated participants.

For the *sharing of personal data online*, we found that participants who participated in the online raffle shared a remarkable amount of non-required personal data, both in the control condition and in the intervention conditions. We did find that our intervention was effective here as well, as it resulted in safer online behaviour. Participants that received information about self-efficacy, on its

own or in combination with severity of risks, shared less non-required personal data compared to participants in the control condition who had not received this information. The condition in which only information about severity of risks was provided did not differ from the control condition in the amount of non-required personal data shared, but participants in this condition did more frequently decide to not participate in the online raffle compared to participants in the control condition. By not participating in the raffle, they also were not required to share their personal data.

The results for differences between groups in society showed that the effectiveness of the intervention on participation in the online raffle varied as a function of participants' gender (a significant effect for women, not men), but not as a function of participants' age or education level. The results did show main effects of age and education level on the sharing of personal information in the raffle. The older the participants, the more frequently they shared non-required personal data. De results for education level showed that the higher the participants' education level, the more frequently they shared non-required personal data.

Limitations and future research

The current research provides insight in the psychological factors that play a role in safe password behaviour and safe sharing of personal data online. The research further demonstrates that and how an intervention aimed at raising/activating perceived severity of risks and self-efficacy can promote safer online behaviour. Future interventions that based on the current research are developed can potentially make an important contribution to prevent victimization of cybercrime. Nevertheless, there are several aspects of the current research that make it important to interpret the conclusions of the study with care.

Although the intervention in Study 2 resulted in safer online behaviour, we see that passwords in the intervention conditions were still weak, and participants often still shared their personal data online even when they were not required to do so. The passwords were less weak compared to the control condition, and less non-required personal data were shared, but there is still a lot of room for approvement.

In addition, although we had a large sample for both empirical studies that was largely representative of the Dutch population, we cannot fully conclude that the sample was representative. We had more highly educated participants and fewer lower educated participants and more younger and fewer older participants. In addition, participant dropout levels were higher when they were asked to share their personal data as part of an online raffle compared to when they were asked to generate a password. This shows potential selective dropout of participants, and that a specific group of participants possibly has not completed the studies.

A strength of the current research is the central position of actual behaviour. Participants generated a password and were offered the choice to share or not share specific personal data online. The behavioural measures used do have limitations.

For password behaviour, we used an entropy score to determine the strength of the generated password. However, this does ignore some aspects of password strength. For example, a password may score high in entropy, but still use an existing word, and because of this be relatively unsafe. In Study 2, we have in part addressed this issue by adding a question that assessed whether the generated password contained personal information. Future research could, in addition to the entropy score and questions whether generated passwords are unique and whether they contain personal information, also assess other aspects of safe passwords. This would provide important information about how to promote these specific aspects of safe password behaviour.

The behavioural measure for the safe sharing of personal data online also has limitations. Our participants shared their personal data in the context of participation in an online study. Possibly, participants shared more personal data because they believed they were in a safe environment. In the current research we have not distinguished between websites where it is safe or required to share sensitive personal data vs. websites whether this is not safe or required. Future research could assess the target behaviour in different contexts, to examine whether the same psychological factors play a role, and whether the intervention that was tested in the current research is as effective in different contexts.

Finally, it is worth recognizing that while Study 2 showed that it was a good choice to target our intervention on perceived self-efficacy and severity of risks, we could have chosen to target the intervention on one of the other psychological factors investigated in Study 1. Responsibility, for example, also could be a relevant factor in the safe online sharing of personal data. Future research could focus on increasing people's perceived own responsibility to make them more aware of their own role in safe behaviour, and in this way promote safe online behaviour.

Policy implications and interventions

The aim of the current research was to identify which psychological factors play a role in safe password behaviour and safe sharing of personal data online, and to test whether influencing these factors through an intervention results in safer online behaviour. It was not our goal to develop a ready-to-use intervention that can be implemented by the government, websites, or other institutions to promote safe online behaviour for a wide range of online applications. However, the results can provide a basis for developing interventions.

In addition to showing that interventions aimed at perceived severity in combination with perceived self-efficacy can be effective, Study 1 showed that other interventions may also be effective in promoting safe online behaviour. One concrete advice we would like to give based on Study 1, is that regarding safe password behaviour, interventions aimed at promoting the use of password managers can be effective.

In addition, the tested intervention for safe passwords and safe sharing of personal data online can (in part) be combined with other intervention techniques. For example, a lot can be achieved by the use of technology or adapting the user environment. One could, for instance, make use of two-step verification or biometric data to access accounts or protect personal data from access by cyber

criminals (Young et al., 2018). It could also be effective to adjust legislation and force websites to provide information about the perceived severity of the risks or about perceived self-efficacy before users create an account or share personal data. In addition, websites and apps could only be allowed to ask for necessary personal data. In combination with the intervention that was tested in the current research that targeted psychological factors, these technological, environmental, and legislation factors could increase the desired behaviour even more.

Finally, it is important to note that an intervention may not be equally suitable for every subpopulation in society. The analyses in Study 2 clearly showed differences between subgroups in the effectiveness of the intervention on safe online behaviour, and (in both Study 1 and Study 2) on safe online behaviour itself. This means that a careful translation is needed from the current findings into policy, where it must be examined and tested for whom the intervention is most effective and how it can best be used.

To conclude, the current research shows that Dutch citizens display unsafe password behaviour and unsafe sharing of personal data online. Our intervention aimed at increasing perceived self-efficacy and perceived severity of the risks of unsafe behaviour resulted in safer password behaviour and safer sharing of personal data online, but there is still much room for improvement. This may be achieved with technology, adjustments to the user environment, and by changes in legislation.

1. Introductie

1.1 Achtergrond

Mensen in Nederland maken veelvuldig gebruik van het internet. Statistieken van het CBS (2021b) laten zien dat 97% van de Nederlanders thuis toegang heeft tot internet en 88% dagelijks gebruik maakt van het internet. Nederlanders gebruiken internet voornamelijk voor het versturen en ontvangen van berichten via e-mail (89%) of WhatsApp (88%), online aankopen (86%), bankieren (85%), het volgen van nieuws (75%), en sociale media (69%).

Bij online activiteiten is het belangrijk dat mensen zich veilig gedragen, om te voorkomen dat ze slachtoffer worden van cybercriminaliteit (’t Hoff-de Goede et al., 2019). Zo is het bijvoorbeeld van belang om accounts af te schermen met veilige wachtwoorden. Als wachtwoorden niet veilig genoeg zijn, lopen mensen het risico om gehackt te worden, waarbij criminelen toegang krijgen tot privégegevens of accounts. Dit kan verschillende negatieve gevolgen hebben, zoals het verlies van belangrijke gegevens, blokkeren van toegang tot systemen, of financiële schade door aankopen op kosten van de gebruiker (Notoatmodjo & Thomborson, 2009). Daarnaast is het van belang om niet te veel persoonsgegevens te delen. Als persoonsgegevens te veel worden gedeeld (bv. via sociale media of bij online aankopen) bestaat het risico op phishing of identiteitsfraude (Jansen, 2018). Bij phishing maken criminelen met behulp van gerichte en persoonlijke nepberichten contact met gebruikers, waarmee ze geld of andere waardevolle spullen of informatie proberen te verkrijgen (Frauenstein & Flowerday, 2020; Sheng et al., 2010). Bij identiteitsfraude nemen criminelen de identiteit van gebruikers aan bij bijvoorbeeld aankopen of criminele activiteiten (Andersons, 2016).

Het *Centre for Strategic and International Studies* schatte de jaarlijkse wereldwijde kosten van cybercriminaliteit in 2018 op $600 miljard, ongeveer 1% van het mondiale BBP (Lewis, 2018). Naast de financiële schade die mensen kunnen oplopen, leidt dit soort criminaliteit vaak ook tot emotionele schade. Zo kunnen mensen schaamte ervaren wanneer ze slachtoffer worden van cybercriminaliteit, verdriet over wat er van hen gestolen is en onzekerheid over toekomstig online gedrag (Borwell et al., 2021). Het is dus relevant te weten hoe we veilig gedrag kunnen bevorderen. 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.

Zo heeft eerder onderzoek vanuit het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC; Van ’t Hoff-de Goede et al., 2019) zich gericht op de vraag hoe veilig Nederlanders zich online gedragen en hoe dit kan worden verklaard. De onderzoekers richtten zich op verschillende gedragingen, zoals veilig wachtwoordgedrag, het installeren van updates, het delen van persoonsgegevens en het omgaan met bijlagen en hyperlinks in e-mails. Eén van de belangrijkste conclusies uit het onderzoek was dat zowel zelfgerapporteerd gedrag als geobserveerd gedrag onveilig bleek: Deelnemers gebruikten zwakke wachtwoorden, installeerden onbekende software op hun apparaat, deelden veel persoonsgegevens en klikten op links in phishing e-mails. Bovendien

bleken er grote verschillen tussen het zelfgerapporteerde gedrag en het geobserveerde gedrag. Mensen gedroegen zich onveiliger dan dat ze zelf rapporteerden, met name bij het gebruik van wachtwoorden en het delen van persoonsgegevens. Het huidige onderzoek richt zich specifiek op deze laatste twee doelgedragingen.

1.2 Het huidige onderzoek

We onderzoeken welke psychologische factoren een rol spelen bij 1) of mensen veilige wachtwoorden aanmaken, en 2) of mensen hun persoonsgegevens online alleen delen wanneer dit veilig en/of noodzakelijk is. We richten ons op veilig wachtwoordgedrag, omdat het wachtwoord de meest gebruikte authenticatiemethode is om systemen en online informatie van gebruikers te beschermen (Alohali et al., 2018). Zo goed als iedereen die online actief is, heeft verschillende wachtwoorden om toegang te krijgen tot accounts, profielen en/of systemen. De beveiliging van veel systemen en apparaten hangt af van de geheimhouding van een enkel wachtwoord. Het achterhalen van dit wachtwoord verschaft toegang tot alle bronnen die door dit wachtwoord worden beheerd. Dat maakt veilig wachtwoordgedrag dus van cruciaal belang. Het wachtwoordgedrag van mensen is echter niet altijd veilig. Mensen maken vaak zwakke wachtwoorden aan (Notoatmodjo & Thomborson, 2009), hergebruiken wachtwoorden (Cain et al., 2018; Grawemeyer & Johnson, 2011) en delen hun wachtwoorden regelmatig met anderen (Alohali et al., 2018). Het delen en hergebruiken van wachtwoorden vergroot het risico op cybercriminaliteit (Alohali et al., 2018). Door zwakke wachtwoorden, hergebruik en het delen van wachtwoorden zijn gebruikers de ‘zwakste schakel’ in wachtwoordbeheer. Daarom is het belangrijk om te onderzoeken welke psychologische factoren veilig wachtwoordgedrag kunnen bevorderen en belemmeren.

We richten ons daarnaast op het delen van persoonsgegevens, omdat mensen vaak onnodig veel persoonsgegevens delen op sociale media of bij het aanmaken van accounts voor bijvoorbeeld webshops of applicaties (Tamrin et al., 2021). Hoewel eerdere studies laten zien dat het onveilig delen van persoonsgegevens een belangrijk probleem is (Addae et al., 2017), zijn er relatief weinig studies die de rol van menselijk gedrag in deze context onderzoeken. Volgens een landelijk onderzoek uitgevoerd door de Consumer Resorts National Research Center, deelt meer dan 40% van de online gebruikers hun privégegevens online (Hajli & Lin, 2016). Dit is lang niet altijd nodig. Daarnaast vinden mensen het moeilijk om in te schatten wanneer het veilig is om iets te delen en wanneer niet (Tamrin et al., 2021).

We beschrijven de psychologische factoren die een potentieel belangrijke rol kunnen spelen bij (on)veilig online gedrag (zie “literatuuroverzicht”). We doen dit op basis van eerder wetenschappelijk onderzoek over hoe menselijk gedrag bijdraagt aan online gedrag in het algemeen en de twee doelgedragingen in het bijzonder. Het doel van het huidige onderzoek is om te onderzoeken welke van deze factoren daadwerkelijk een rol spelen bij de twee doelgedragingen. Dit onderzoeken we door middel van een vragenlijststudie (Studie 1). Daarnaast hebben we een

interventie getest om veilig wachtwoordgedrag en het online veilig delen van persoonsgegevens te bevorderen (Studie 2).

Concreet zijn de onderzoeksvragen:

1) Welke factoren bevorderen en welke factoren belemmeren veilig wachtwoordgedrag en het online veilig delen van persoonsgegevens?
2) Kunnen we veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens bevorderen met een interventie?

Deze onderzoeksvragen worden beantwoord met twee studies. In Studie 1 hebben we met een vragenlijst onderzocht welke factoren een rol spelen bij veilig wachtwoordgedrag en het online veilig delen van persoonsgegevens. De factoren die zijn onderzocht zijn: kennis, responskosten, kwetsbaarheid, ernst, zelfeffectiviteit, responseffectiviteit en verantwoordelijkheid. Mede op basis van de resultaten van Studie 1 hebben we in Studie 2 een interventie ontwikkeld, en getest of we veilig wachtwoordgedrag en het online veilig delen van persoonsgegevens konden bevorderen.

Voordat we Studies 1 en 2 en de resultaten beschrijven, geven we een overzicht van de relevante literatuur. Deze literatuur wordt samengevat in een model (zie Figuur 1).

1.3 Literatuuroverzicht

Het huidige onderzoek richt zich specifiek op twee doelgedragingen: veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens. Om te bepalen welke psychologische factoren een rol spelen bij deze twee doelgedragingen is het noodzakelijk om eerst veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens te definiëren.

Veilig wachtwoordgedrag

Adams en Sasse (1999) noemen verschillende criteria voor veilig wachtwoordgedrag: 1) een veilige samenstelling van het wachtwoord, 2) een korte levensduur van het wachtwoord (i.e. frequent het wachtwoord veranderen) en 3) individueel eigendom van het wachtwoord. Hoe minder een wachtwoord voldoet aan bovenstaande criteria, hoe onveiliger het wachtwoord, waarmee de kans verhoogd wordt dat een gebruiker gehackt wordt.

Een veilige samenstelling van een wachtwoord is moeilijk te bepalen doordat cybercriminelen steeds beter worden in het achterhalen van wachtwoorden. Hierdoor worden regels en maatregelen voor veilige wachtwoorden vaak aangepast. Daarnaast geven verschillende instanties, wetenschappers en websites ook verschillende richtlijnen voor het aanmaken van wachtwoorden. De Consumentenbond (2021) zegt bijvoorbeeld dat het verstandig is om 1) minimaal 12 tekens aan te houden, 2) zowel cijfers, hoofdletters als speciale tekens te gebruiken, en 3) geen persoonlijke informatie te gebruiken in het wachtwoord (zoals naam, geboortedatum of adres). Wetenschappelijke literatuur heeft echter vaak strengere aanbevelingen. Zo raden Cain en collega's

(2018) aan om geen woorden uit het woordenboek te gebruiken; een verzameling letters en tekens is een beter alternatief. Dit type wachtwoorden kan echter lastig te onthouden zijn. In het huidige onderzoek komt onze definitie van een veilige wachtwoordsamenstelling overeen met die van de Consumentenbond, zoals hierboven beschreven.

Naast de samenstelling van het wachtwoord, is het ook belangrijk dat gebruikers hun wachtwoord regelmatig wijzigen en niet hergebruiken voor verschillende websites (Gaw & Felten, 2006). De Consumentenbond (2021) raadt aan wachtwoorden minimaal 1 keer per jaar aan te passen en het wachtwoord niet te hergebruiken. Ten slotte is het belangrijk dat gebruikers hun wachtwoorden niet opschrijven op plaatsen waar criminelen het makkelijk kunnen vinden (bv. op een laptop) en dat alleen de gebruiker weet wat het wachtwoord is (Adams & Sasse 1999; Barton & Barton 1984; Dhamija & Perrig, 2000; Horowitz, 2001). Mensen delen echter regelmatig wachtwoorden met hun partner, vrienden of familie, of verzenden hun wachtwoord per tekstbericht of e-mail (Meter & Bauman, 2015). Hoe meer mensen het wachtwoord weten en hoe vaker het onveilig gedeeld wordt met anderen, hoe onveiliger het wachtwoord is (Notoatmodjo & Thomborson, 2009).

Veilig online delen persoonsgegevens

Naast veilig wachtwoordgedrag richt het huidige onderzoek zich op het veilig online delen van persoonsgegevens. Er zijn veel soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers, postcodes met huisnummers, of een bankrekeningnummer zijn persoonsgegevens. Meer indirecte persoonsgegevens zijn gegevens die in combinatie met andere gegevens iets zeggen over een persoon of waardoor een persoon herleidbaar is (Autoriteit Persoonsgegevens, z.d.).

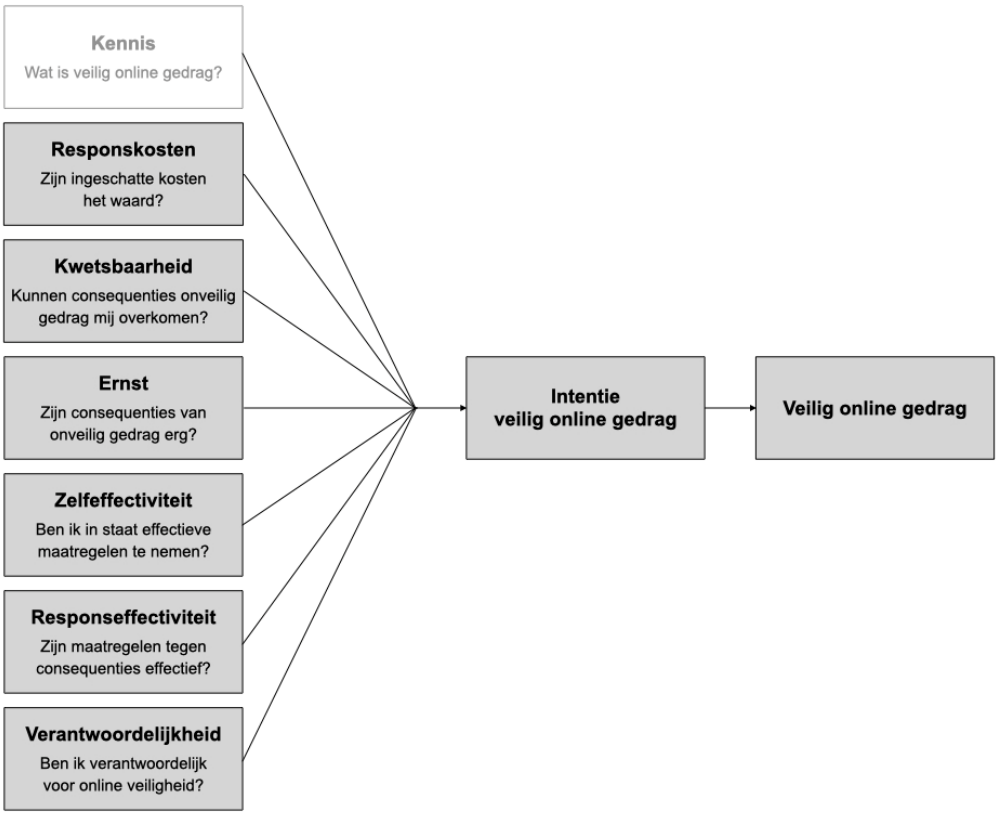
We definiëren veilig online delen van persoonsgegevens op basis van drie criteria: 1) een check van de veiligheid van de website of applicatie (Christofides et al., 2012), 2) niet méér delen dan noodzakelijk (terughoudendheid) en 3) het maken van onderscheid tussen verschillende typen persoonsgegevens (Veiliginternetten, z.d.). Allereerst is het dus belangrijk om de veiligheid van de online omgeving te bepalen (zie ook Christofides et al., 2012). Hoewel dit moeilijk is voor een gebruiker, is een belangrijk onderdeel van het doelgedrag dat een gebruiker een moment neemt om te kijken of de website of applicatie veilig is (Consumentenbond, 2021). Gebruikers kunnen bijvoorbeeld nagaan of het een bekende en veelgebruikte website of applicatie is, of dat het een nieuwe of onbekende website of applicatie is. Dit kunnen ze doen door op zoek te gaan naar ervaringen met de website van andere mensen (bv. via een zoekmachine zoals Google). Daarnaast is het belangrijk dat er niet onnodig persoonsgegevens worden verstrekt. Vaak wordt op websites of bij het aanmaken van accounts aangegeven welke gegevens verplicht zijn om in te vullen en welke niet. Dit wordt dan bijvoorbeeld aangegeven met een sterretje (*). Als het noodzakelijk is om specifieke persoonsgegevens te delen, dan wordt het aangeraden om te kijken of de applicatie veilig is. Wanneer het niet verplicht is, wordt er aangeraden om ook geen persoonsgegevens te delen (Consumentenbond, 2021). Ten slotte wordt aangeraden om onderscheid te maken tussen persoonsgegevens die wel veilig zijn om te delen en persoonsgegevens die niet of minder veilig zijn

om te delen. Zo is het vaak prima om je naam te delen, maar je rekeningnummer of wachtwoord niet (Veiliginternetten, z.d.).

Psychologische factoren

Nu we een definitie hebben van de doelgedragingen is de vraag welke psychologische factoren van invloed zijn op deze twee doelgedragingen. Veel van de factoren die in de literatuur naar voren komen als mogelijke voorspellers van veilig online gedrag zijn gebaseerd op de *protection motivation theory* (PMT; Rogers, 1975). PMT richt zich op de motivatie (of intentie) van mensen om zichzelf te beschermen (De Kimpe et al., 2021; Floyd et al., 2000; Milne et al., 2002; Norman et al., 2005). Deze motivatie wordt voorspeld door verschillende psychologische factoren (Floyd et al., 2000; Milne et al., 2002). Zo evalueren mensen als eerste de dreiging van de situatie, gebaseerd op een inschatting van de eigen kwetsbaarheid voor de dreiging en de ernst van de dreiging. Daarna evalueren mensen mogelijke beschermingsmaatregelen om de dreiging te verminderen. Dit is gericht op responseffectiviteit (of een maatregel effectief zal zijn tegen de dreiging), zelfeffectiviteit (of ze in staat zijn om de maatregel te nemen) en responskosten (of de ingeschatte kosten het waard zijn). Op basis van deze evaluaties raken mensen meer of minder gemotiveerd om voorzorgsmaatregelen te nemen of om preventief gedrag te vertonen (Floyd et al., 2000).

In het huidige onderzoek worden de psychologische factoren van de PMT (responskosten, kwetsbaarheid, ernst, zelfeffectiviteit en responseffectiviteit) gemeten om te onderzoeken in hoeverre deze factoren een rol spelen bij veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens. Naast de factoren uit de PMT onderzoeken we in het huidige onderzoek ook de invloed van kennis en verantwoordelijkheid (zie ook Figuur 1). In de volgende paragrafen zullen we per factor toelichten hoe deze veilig online gedrag mogelijk beïnvloedt.



Figuur 1

Noot. De samenhang tussen verschillende psychologische factoren en veilig online gedrag (i.e. veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens).

Kennis

Allereerst lijkt het logisch te veronderstellen dat kennis van veilig online gedrag een belangrijke basis is voor het daadwerkelijk tonen van dit gedrag. Wetenschappelijke literatuur schetst echter geen eenduidig beeld. De literatuur besproken in het eerdere onderzoek vanuit het WODC (Van ’t Hoff-de Goede et al., 2019) liet ook al zien dat sommige studies een positieve relatie aantonen tussen kennis en veilig online gedrag (Arachchilage & Love, 2014; Downs et al., 2007), maar andere studies een negatieve relatie aantonen (Cain et al., 2018; Ovelgönne et al., 2017). Van ’t Hoff-de Goede et al. (2019) lieten in hun onderzoek zien dat kennis van veilig gedrag positief samenhangt met zelfgerapporteerd veilig online gedrag. Voor daadwerkelijk gedrag was het echter minder eenduidig. Kennis had een negatieve relatie met geobserveerd wachtwoordgedrag: hoe meer kennis gebruikers hadden, hoe minder sterk het wachtwoord was dat ze aanmaakten in het onderzoek. Kennis had in het onderzoek van Van 't Hoff-de Goede et al. (2019) een positieve relatieve relatie met het veilig online delen van persoonsgegevens: wanneer gebruikers meer kennis hadden van online veilig gedrag, gedroegen zij zich veiliger op het gebied van het delen van persoonlijke gegevens.

Recenter onderzoek maakt het beeld niet duidelijker. Van der Kleij et al. (2020) lieten zien dat kennis essentieel is voor het voorkomen van datalekken in financiële organisaties. Zwilling et al. (2020) toonden aan dat kennis bovendien leidt tot meer bewustzijn van cyberveiligheid en, relevant voor het huidige onderzoek, het minder delen van persoonsgegevens online. Andere onderzoeken lieten juist negatieve relaties zien. Kovačević (2020) toonde aan dat mensen met meer kennis over online veilig gedrag juist vaker slachtoffer zijn van cybercriminaliteit. De Kimpe et al. (2021) lieten zien dat mensen met meer kennis over online veilig gedrag zich minder kwetsbaar voelen voor cybercriminaliteit en dan juist minder geneigd zijn om veiligheidsmaatregelen te nemen.

Hoewel kennis dus wel degelijk een verband lijkt te hebben met veilig online gedrag, is dit verband dus soms positief en soms negatief. In het huidige onderzoek hebben we kennis gemeten door specifieke kennis over de twee doelgedragingen te toetsen. Dus niet kennis over veilig online gedrag in het algemeen, maar kennis over veilig wachtwoordgedrag en over het veilig online delen van persoonsgegevens. Het doel was om specifieker te toetsen of kennis samenhangt met veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens. Hoewel kennis inderdaad een relevante rol zou kunnen spelen bij beide doelgedragingen, lieten de data het niet toe om duidelijke conclusies te trekken over de invloed van kennis. Zoals ook wordt uitgelegd in de procedure van Studie 1 (Sectie 2.1.2) twijfelden we over de kwaliteit van de vragen die we gebruikt hebben om kennis over beide doelgedragingen te meten. Om deze reden hebben we besloten wel de literatuur over kennis te bespreken in het huidige rapport, maar de resultaten voor kennis niet op te nemen in het rapport. Dat is ook de reden dat het tekstblokje van Kennis in Figuur 1 een andere kleur heeft.

Responskosten

Responskosten verwijzen naar de inschatting van de kosten die gemaakt worden om het doelgedrag te vertonen (Blythe & Coventry, 2018; Reeves et al., 2021). Het gaat hier dus niet om de inschatting dat mensen het gedrag wel of niet *kunnen* uitvoeren (dit is zelfeffectiviteit); het gaat hier om de inschatting dat dit energie of gedoe met zich meebrengt. Voor veilig wachtwoordgedrag gaat het om de ervaren moeite (bv. tijd) van het aanmaken en onthouden van verschillende en sterke wachtwoorden. Voor het veilig online delen van persoonsgegevens gaat het om de moeite die het kost om uit te zoeken of persoonsgegevens veilig kunnen worden gedeeld of niet.

Van ’t Hoff-de Goede et al. (2019) bespraken al literatuur die laat zien dat responskosten een belangrijke voorspellende factor is voor veilig online gedrag (Crossler et al., 2017; Jansen & Van Schaik, 2016; Workman et al., 2008). Ze vonden dat responskosten negatief samenhing met zelfgerapporteerd veilig online gedrag. Gebruikers kunnen aanvankelijk wel de intentie hebben om veilig online gedrag te vertonen, maar als ze de responskosten (te) hoog inschatten leidt dit uiteindelijk niet tot veilig gedrag. Hoewel de responskosten anders zijn voor wachtwoordgedrag dan voor het online delen van persoonsgegevens, verwachten we dezelfde negatieve relatie tussen responskosten en beide doelgedragingen: hoe hoger de responskosten, hoe minder veilig het wachtwoordgedrag en hoe minder veilig persoonsgegevens online worden gedeeld.

Kwetsbaarheid

Een andere belangrijke factor die wordt onderzocht is waargenomen kwetsbaarheid van de gebruikers. Een reden voor mensen om onveilig online gedrag te vertonen is dat ze kunnen denken dat hen toch niets overkomt, of dat zij geen aantrekkelijk doelwit zijn. Naast kennis van veilig online gedrag is het dus van belang dat mensen een reële kijk hebben op de risico's van onveilig online gedrag en hun kwetsbaarheid. Dit betekent dat ze zich moeten realiseren dat de negatieve gevolgen van onveilig wachtwoordgedrag en het onveilig online delen van persoonsgegevens hen daadwerkelijk kunnen overkomen. Het is goed om een realistische inschatting te hebben van de kans op die gevolgen.

Eerder onderzoek laat zien dat mensen online vaak een lage kwetsbaarheid ervaren (Cho et al., 2010). Als we specifiek naar onze doelgedragingen kijken zien we ook een positieve relatie tussen kwetsbaarheid en veilig online gedrag. Tam et al. (2010) onderzochten de invloed van gevoelens van kwetsbaarheid op wachtwoordgedrag en toonden aan dat mensen zwakke wachtwoorden aanmaakten omdat ze niet de negatieve consequenties inzagen van hun gedrag. Deze resultaten laten zien dat kwetsbaarheid een belangrijke rol lijkt te spelen bij veilig wachtwoordgedrag. Ook bij het online delen van persoonsgegevens spelen gevoelens van kwetsbaarheid een belangrijke rol (Beldad et al., 2011). Hajli en Lin (2016) onderzochten het delen van persoonsgegevens op sociale media en lieten zien dat gebruikers die de risico's van het delen van persoonsgegevens op sociale media minder negatief inschatten, vaker hun persoonsgegevens deelden. Op basis van deze literatuur verwachten we een positieve relatie tussen gevoelens van kwetsbaarheid en veilig online gedrag, bij zowel veilig wachtwoordgedrag als het veilig online delen van persoonsgegevens.

Ernst

Waar kwetsbaarheid zich voornamelijk richt op hoe groot de kans is dat negatieve consequenties van onveilig online gedrag optreden, richt ernst zich meer op hoe erg die negatieve consequenties nu precies gevonden worden. Gebruikers kunnen wellicht goed inschatten wat de kans is dat zij worden gehackt, of dat hun identiteit wordt gestolen, maar het vervolgens niet erg vinden dat dit gebeurt, omdat ze de ernst van de consequenties niet inzien.

Eerder onderzoek laat zien dat er een positieve relatie is tussen hoe mensen de ernst van de consequenties van onveilig online gedrag inschatten en hoe veilig ze zich online gedragen (Crossler et al., 2017; Jansen, 2018; Jansen & van Schaik, 2016). Deze onderzoeken richtten zich niet specifiek op veilig wachtwoordgedrag of het veilig online delen van persoonsgegevens. Op basis van deze literatuur verwachten we een positieve relatie tussen ingeschatte ernst van risico's aan de ene kant en veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens aan de andere kant.

Zelfeffectiviteit en responseffectiviteit

Volgens de PMT is er een positieve relatie tussen waargenomen kwetsbaarheid en ernst, en veilig online gedrag, maar alleen wanneer mensen denken dat ze in staat zijn om het veilige gedrag te vertonen (Aurigemma et al., 2019; Blythe & Coventry, 2018). Hierbij wordt onderscheid gemaakt tussen zelfeffectiviteit en responseffectiviteit (Hong & Furnell, 2021). Zelfeffectiviteit is de mate dat

iemand zichzelf in staat acht het gewenste gedrag te vertonen (bv. de mate waarin iemand denkt de verschillende wachtwoorden te kunnen onthouden; de mate waarin iemand denkt de veiligheid van een website te kunnen controleren). Responseffectiviteit is de mate dat iemand denkt dat het vertonen van het gewenste gedrag de risico's zal wegnemen (bv. dat een veilig wachtwoord de kans op een hack verlaagt, Howell, 2021; dat het veilig online delen van persoonsgegevens de kans op phishing verlaagt).

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 (Arachchilage & Love, 2014; Crossler & Bélanger, 2014; Crossler et al., 2017; Jansen & van Schaik, 2016; Rhee et al., 2009; Van Schaik et al., 2017; Workman et al., 2008). Onderzoeken die daarna zijn uitgevoerd laten eenzelfde beeld zien. Reyns et al. (2019) onderzochten verschillende vormen van cybercriminaliteit zoals hacking en identiteitsfraude en lieten zien dat mensen die zich niet in staat voelden om te handelen tegen deze risico's, ook vaker slachtoffer waren van cybercriminaliteit. Onderzoek gericht op het delen van persoonsgegevens op sociale media liet zien dat wanneer mensen zich in staat voelden om te stoppen met het delen van persoonsgegevens, ze ook de intentie hadden om minder specifieke gegevens te delen op Facebook (zie ook Hsu et al., 2007). Op basis van deze eerdere studies verwachten we dat zowel zelfeffectiviteit als responseffectiviteit een positieve relatie heeft met veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens.

Verantwoordelijkheid

Naast kennis van veilig online gedrag en de PMT factoren, lijken verantwoordelijkheidsgevoelens ook van belang voor veilig online gedrag. Gebruikers vinden het niet altijd hun eigen verantwoordelijkheid om ervoor te zorgen dat zij veilige wachtwoorden gebruiken en hun persoonsgegevens veilig online delen. In plaats daarvan leggen ze de verantwoordelijkheid soms bij websites, applicaties, of de overheid (bv. Boehmer et al., 2015). Dit kan een reden zijn voor mensen om te besluiten minder aandacht of moeite te steken in veilig online gedrag (Grawemeyer & Johnson, 2011).

De koppeling tussen de PMT factoren en verantwoordelijkheid komt ook terug in onderzoek van Boehmer et al. (2015). Zij onderzochten of gebruikers met een hoge eigen verantwoordelijkheid vaker beschermende acties ondernemen (bv. de computer scannen op spyware, gegevens verwijderen na het browsen) en minder geneigd zijn om onbeschermde (risicovolle) acties te ondernemen (bv. creditcard gegevens opslaan, veiligheid van browser te laag instellen). De resultaten van het onderzoek toonden aan dat eigen verantwoordelijkheid inderdaad een belangrijke voorspeller was voor veilig online gedrag, bovenop de factoren van de PMT. Bij deelnemers die online veiligheid als hun eigen verantwoordelijkheid beschouwden, was het waarschijnlijker dat zij beschermende maatregelen namen, terwijl bij deelnemers die de verantwoordelijkheid bij iemand anders legden, het onwaarschijnlijker was dat zij zich veilig gingen gedragen (zie ook Shillair et al., 2015). Hoewel dit onderzoek zich niet richtte op onze doelgedragingen, verwachten we ook een positieve relatie tussen eigen verantwoordelijkheid en

veilig online gedrag voor beide doelgedragingen: hoe hoger de eigen verantwoordelijkheid, hoe veiliger het wachtwoordgedrag en hoe veiliger persoonsgegevens online worden gedeeld.

Samengevat biedt de besproken literatuur een basis om te voorspellen dat veilig online gedrag wordt voorspeld door de psychologische factoren kennis, responskosten, kwetsbaarheid, ernst, zelf- en responseffectiviteit en verantwoordelijkheid. In Studie 1 hebben we onderzocht welke van deze psychologische factoren een rol spelen bij veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens. Vervolgens hebben we op basis van de resultaten van Studie 1 in Studie 2 een interventie ontwikkeld, en getest of we veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens kunnen bevorderen.

2. Studie 1

Studie 1 had als doel inzicht te krijgen in welke psychologische factoren veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens belemmeren en bevorderen. De studie bestond uit een vragenlijst, waarin we ons richtten op hoe (geobserveerd en zelfgerapporteerd) online gedrag relateert aan de factoren kennis, responskosten, kwetsbaarheid, ernst, zelf- en responseffectiviteit en verantwoordelijkheid. Het geobserveerde gedrag bestond uit het aanmaken van een wachtwoord en het al dan niet delen van persoonsgegevens bij een winactie. Het zelfgerapporteerde gedrag werd gemeten met verschillende stellingen over hoe deelnemers zich normaalgesproken gedragen. De verschillende psychologische factoren werden ook uitgevraagd met verschillende stellingen. De studie had daarnaast verschillende open vragen en achtergrondvragen, om een nog vollediger beeld te krijgen van bevorderende en belemmerende factoren van veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens.

2.1 Methode

De studie is opgezet en ontworpen door de onderzoekers van het Kenniscentrum voor Psychologie en Economisch Gedrag (KCPEG). Het KCPEG is verbonden aan de Sectie Sociale, Economische en Organisatiepsychologie van de Universiteit Leiden. Onderzoeksbureau Markteffect heeft de studie vervolgens geprogrammeerd en de deelnemers geselecteerd en geworven. Ook de kwaliteitsanalyse van de data is verzorgd door Markteffect. Onderzoekers van KCPEG waren verantwoordelijk voor de data-analyse en rapportage. De dataverzameling heeft plaatsgevonden in de periode van 27 december 2021 t/m 4 januari 2022.

2.1.1 Deelnemers

Werving van deelnemers

De deelnemers zijn geworven uit drie verschillende panels van onderzoeksbureau Markteffect. Deelnemers logden in op hun eigen account in het portal van Markteffect. In dit portal staan lopende onderzoeken waar men aan mee kan doen.

Het doel was een representatieve steekproef van de Nederlandse bevolking op geslacht, leeftijd (18+), opleiding en regio. Tijdens dit onderzoek is tweemaal “geboost” op jongeren omdat de respons in deze groep achter bleef. Dit houdt in dat deze specifieke groep vanuit het panel een herinnering kreeg om aan onderzoek mee te doen. Deze herinnering is dus niet specifiek voor ons onderzoek, maar gericht op alle lopende onderzoeken. Hierdoor kan geen informatie worden gegeven over de response rate.

Screening van de data

De data zijn door onderzoeksbureau Markteffect allereerst gecontroleerd op dubbele personen en zogenoemde speeders, straightliners en toetsenrammelaars. Dubbele personen werden gevonden door te kijken naar gebruik van hetzelfde e-mailadres, dezelfde gebruikersnaam of wachtwoord en dezelfde achtergrondkenmerken. Speeders zijn de 5% snelste invullers van de vragenlijst. Antwoorden van deze deelnemers zijn handmatig nagelopen op een logisch antwoordpatroon. Straightliners geven meer dan 80% dezelfde antwoorden bij matrixblokken (bv. helemaal mee oneens- helemaal mee eens). Van deze deelnemers zijn de antwoorden handmatig nagelopen. Ten slotte is er handmatig naar de open antwoorden gekeken en gezocht naar toetsenrammelaars (bv. het invullen van jgkgrxhg). Van de 1051 deelnemers werden 53 deelnemers verwijderd op grond van bovenstaande criteria, 998 deelnemers werden behouden in de dataset. Voor de volledige onderzoek verantwoording verwijzen we naar de onderzoek verantwoording van Markteffect die hier te vinden is: https://easy.dans.knaw.nl/ui/home.

De achtergrondkenmerken van de 998 deelnemers zijn uiteengezet in Tabel 1 en vergeleken met de Nederlandse bevolking (CBS, 2021a). De steekproef is representatief voor de Nederlandse bevolking qua geslacht en regio. De steekproef wijkt iets af qua opleidingsniveau vergeleken met de Nederlandse bevolking. Zo hebben deelnemers vaker een midden (42.8% vs. 36.5%) en hoog (39.5% vs. 34.8%) opleidingsniveau en zijn zij minder vaak laag opgeleid (15.6% vs. 28.8%). Ten slotte zijn deelnemers minder vaak dan gemiddeld in de Nederlandse bevolking tussen de 18 en 24 jaar (3.8% vs. 10.9%).

Naast de socio-demografische variabelen is ook eerder slachtofferschap van internetcriminaliteit gemeten en uiteengezet in Tabel 1. Van de deelnemers aan het onderzoek is 15.9% wel eens slachtoffer geweest van internetcriminaliteit. Internetcriminaliteit (cybercriminaliteit of online criminaliteit) is het inzetten van het internet om criminele activiteiten mee uit te voeren.

Tabel 1

Achtergrondkenmerken deelnemers (*N* = 998) *in vergelijking met Nederlandse bevolking van 18+ naar data van het CBS (2021a)*

	Deelnemers		Nederlandse bevolking
	N	%	%
Geslacht			
Man	506	50.7	49.7
Vrouw	490	49.1	50.3
Anders	1	0.1	
Wil ik liever niet zeggen	1	0.1	
Opleidingsniveau[a]			
Laag	156	15.6	28.8
Midden	427	42.8	36.5
Hoog	397	39.8	34.8
Anders	13	1.3	
Wil ik liever niet zeggen	5	0.5	
Regio			
West (UT, NH, ZH)	408	40.9	45.6
Noord (GR, FR, DR)	123	12.3	9.9
Oost (OV, GD, FL)	200	20.0	21.1
Zuid (ZL, NB, LB)	267	26.8	23.3
Leeftijd			
18 t/m 24	38	3.8	10.9
25 t/m 34	144	14.4	15.9
35 t/m 44	145	14.5	14.7
45 t/m 54	198	19.8	17.0
55 t/m 65	225	22.5	16.9
65+	242	24.2	24.6
Wil ik liever niet zeggen	6	0.6	
Eerder slachtofferschap van internetcriminaliteit			
Ja, in de afgelopen 12 maanden	60	6.0	
Ja, langer geleden dan 12 maanden	97	9.7	
Nee	789	79.1	
Weet ik niet	52	5.2	

Noot. [a] Hoogst afgeronde opleiding: laag (geen onderwijs, basisonderwijs, LBO/VBO/VMBO/MBO-1), midden (MBO 2/3/4, HAVO, VWO), hoog (HBO, WO).

2.1.2 Onderzoeksopzet en procedure

De onderzoeksvragen zijn onderzocht middels een online vragenlijst. Aan het begin van de vragenlijst kregen deelnemers informatie over het onderzoek en gaven zij toestemming voor deelname. Daarna vulden ze de vragenlijst in.

Iedere deelnemer ontving na het afronden van de vragenlijst punten, welke vervolgens konden worden ingewisseld voor geld of producten. Daarnaast werd een cadeaubon van 100 euro verloot onder alle deelnemers van de vragenlijst die aangaven mee te willen doen aan de verloting. Het meedoen aan de verloting (ofwel winactie) en het daarbij invullen van persoonsgegevens was de gedragsmaat voor het veilig online delen van persoonsgegevens in ons onderzoek (zie Sectie 2.1.4.1 voor meer details). Aan het eind van het onderzoek werden deelnemers bedankt en kregen ze meer informatie over het doel van het onderzoek (debriefing). Na afloop van het onderzoek ontvingen de deelnemers de toegezegde punten voor deelname aan het onderzoek en vond de verloting van de tegoedbon ter waarde van 100 euro plaats.

Tabel 2 geeft de opbouw van de vragenlijst weer, inclusief de vragen die zijn gesteld aan de deelnemers. Voor de leesbaarheid van het rapport presenteren we de meest relevante resultaten (aangegeven met het groene vinkje in Tabel 2). De resultaten voor vragen over wachtwoordmanagers zijn opgenomen in Bijlage B (aangegeven met een B in Tabel 2). Voor de overige resultaten en materialen verwijzen we naar de onderzoekdocumentatie behorende bij Studie 1 die hier te vinden is: https://easy.dans.knaw.nl/ui/home.

Zoals weergegeven in Tabel 2 en ook besproken in de Inleiding rapporteren we de resultaten voor kennis niet (i.e. een van de psychologische factoren in ons model, zie Sectie 2.1.3.2). Bij het analyseren van de antwoorden van deelnemers op de kennis vragen twijfelden we over de kwaliteit van de vragen. Daarom hebben we ervoor gekozen om de resultaten voor kennis niet op te nemen in het rapport.

Tabel 2

Opbouw vragenlijst

	Blok	Vragen	Gerapporteerd
1	Informatiebrief, informed consent en leeftijd	Informed consent	✓
		Leeftijd	✓
2	Gedragsmaten	Persoonsgegevens: delen persoonsgegevens	✓
		Wachtwoorden: entropie	✓
3	Online activiteiten	Frequentie internetgebruik	X
		Gebruikt apparaat	X
4	Wachtwoorden en Persoonsgegevens	Kennis	X
		Zelfrapportage gedrag	✓
		Beoordeling eigen gedrag	X
		Gedragsintentie	X
		Belemmerende/bevorderende factoren	✓
		Responskosten	✓
		Zelfeffectiviteit	✓
		Ernst	✓
		Kwetsbaarheid	✓
		Responseffectiviteit	✓
		Verantwoordelijkheid	✓
5	Wachtwoordmanager	Kennis wachtwoordmanager	B
		Gebruik wachtwoordmanager	B
		Toelichting wachtwoordmanager gebruik	B
		Welke wachtwoordmanager	B
6	Overige vragen	Geslacht	✓
		Hoogst afgeronde opleiding	✓
		Postcode (voor berekening regio)	✓
		Aangemaakt wachtwoord: zoals normaal	X
		Aangemaakt wachtwoord: hergebruik	✓
		Aangemaakt wachtwoord: gebruik wachtwoordmanager	✓
		Persoonsgegevens: zoals normaal	X
		Persoonsgegevens: echte gegevens	✓
		Persoonlijke relevantie online veiligheid	X
		Eerder slachtofferschap	✓
		Vertrouwen	X
		Opmerkingen	X

7	Debriefing

Noot. De volgorde waarin deelnemers bij Blok 4 de vragen over wachtwoorden/persoonsgegevens beantwoordden was gerandomiseerd om mogelijke volgorde effecten uit te balanceren. De helft van de deelnemers beantwoordde eerst de vragen over wachtwoorden gevolgd door de vragen over persoonsgegevens: de andere helft van de deelnemers beantwoordde eerst de vragen over persoonsgegevens gevolgd door de vragen over wachtwoorden.

De vragenlijst startte, na het geven van informed consent en het beantwoorden van de leeftijd vraag, met de gedragsmaten voor zowel wachtwoorden als persoonsgegevens, gevolgd door algemene vragen over online gedrag en het uitvragen van alle psychologische factoren per doelgedrag. Aan het einde van de vragenlijst volgden socio-demografische gegevens en overige vragen. Waar relevant sluiten de vragen aan bij het eerdere onderzoek van het WODC (Van 't Hoff-de Goede et al., 2019).

2.1.3 Meetinstrumenten wachtwoorden

2.1.3.1 Gedragsmaten en zelfrapportage gedrag

Sterkte wachtwoorden

In de gedragsmaat werd gekeken naar de samenstelling van wachtwoorden, één van de criteria van Adams en Sasse (1999) bij veilig wachtwoordgedrag. Wachtwoordsamenstelling werd gemeten door deelnemers aan het begin van de vragenlijst te vragen een gebruikersaccount aan te maken (zie Van 't Hoff-de Goede et al., 2019). Deelnemers kregen de volgende informatie: "In overeenstemming met wetgeving op het gebied van de bescherming van persoonsgegevens vragen we u om nu eerst een gebruikersaccount aan te maken. Dit account heeft u aan het einde van het onderzoek opnieuw nodig." Hierna werd hen gevraagd een gebruikersnaam en wachtwoord in te voeren.

De sterkte van het aangemaakte wachtwoord is uitgedrukt in entropie. De entropie van het aangemaakte wachtwoord is berekend aan de hand van de lengte van het wachtwoord en de mogelijke variatie van de gebruikte karakterset (kleine letters, hoofdletters, speciale tekens en cijfers). De karakterset beslaat het aantal waarden dat elk teken in een wachtwoord kan aannemen. We keken daarbij naar het aantal mogelijke combinaties van kleine letters (29), hoofdletters (26), cijfers (10) en speciale tekens (33). Een wachtwoord van vier tekens dat bestaat uit alleen cijfers, denk bijvoorbeeld aan een pincode, kan voor elk van de vier tekens tien waarden aannemen (de cijfers 0 t/m 9). Bij een wachtwoord met alleen kleine letters bestaat de set uit 26 karakters. Elk teken in het wachtwoord kan 1 van 26 karakters aannemen. Wanneer iemand naast kleine letters ook hoofdletters gebruikt, bestaat de set uit 52 karakters. Hoe groter de karakterset, hoe moeilijker het wachtwoord te raden is.

Voor het berekenen van de entropie is de volgende formule gebruikt (zie ook Van 't Hoff-de Goede et al., 2019): $\log_2(karakterset^{wachtwoordlengte})$. Entropie wordt uitgedrukt in bits waarbij een

wachtwoord dat in een eerste poging de helft van de tijd geraden wordt een entropie van 1 bit heeft. De entropie is vervolgens geïnterpreteerd van zeer zwak naar zeer sterk op basis van criteria van de password-manager Keepass (Keepass, z.d.). Een zwak wachtwoord heeft een entropiescore lager dan 80 bits, een sterk wachtwoord een entropiescore tussen 112-128 bits, en een zeer sterk wachtwoord heeft een entropiescore van meer dan 128 bits.

Unieke wachtwoorden

Veilig wachtwoordgedrag bestaat niet alleen uit het aanmaken van sterke wachtwoorden, maar ook uit het gebruiken van unieke wachtwoorden (Gaw & Felten, 2006). Om na te kunnen gaan of deelnemers een uniek of hergebruikt wachtwoord aangemaakt hadden vroegen we hen aan het einde van de vragenlijst: “Gebruikt u het wachtwoord dat u heeft aangemaakt ook voor andere accounts?” (Ja; Nee; Zeg ik liever niet).

Zelfrapportage gedrag

De zelfrapportage van wachtwoordgedrag werd op een 5-puntsschaal (van *nooit* tot *altijd*) gemeten, met vijf stellingen: twee stellingen over de sterkte van wachtwoorden, twee stellingen over het gebruik van unieke wachtwoorden, en een stelling over het delen van wachtwoorden met anderen:

- “Mijn wachtwoorden bestaan uit minstens 12 tekens.” [sterkte wachtwoorden]
- “Mijn wachtwoorden bestaan uit verschillende tekens (kleine letters, hoofdletters, getallen en speciale tekens).” [sterkte wachtwoorden]
- “Ik gebruik hetzelfde wachtwoord voor verschillende apps of websites (bijvoorbeeld zowel voor sociale media als online bankieren, of voor verschillende webwinkels).” (Van ‘t Hoff-de Goede et al., 2019). [unieke wachtwoorden]
- “De wachtwoorden die ik gebruik lijken op elkaar.” [unieke wachtwoorden]
- “Ik deel mijn persoonlijke wachtwoorden met anderen.” (Van ‘t Hoff-de Goede et al., 2019). [niet delen van wachtwoorden]

2.1.3.2 Psychologische factoren

Na de gedragsmaten en de algemene vragen over online gedrag volgden de vragen over de psychologische factoren. Tenzij anders aangegeven werden vragen beantwoord op een 5-puntsschaal (1 = *helemaal mee oneens*, 2 = *enigszins mee oneens,* 3 = *niet mee oneens maar ook niet mee eens*, 4 = *enigszins mee eens*, 5 = *helemaal mee eens*).

Responskosten

De responskosten van veilig wachtwoordgedrag werd gemeten met: “Het kost veel tijd om veilige wachtwoorden te gebruiken”, “Het kost veel moeite om veilige wachtwoorden te gebruiken”, en “Het kost veel moeite om verschillende wachtwoorden voor verschillende websites te bedenken”.

Zelfeffectiviteit

De zelfeffectiviteit van veilig wachtwoordgedrag werd gemeten met drie stellingen: een stelling over het bedenken van wachtwoorden (“Ik vind het moeilijk om een veilig wachtwoord te bedenken”),

een stelling over het onthouden van wachtwoorden (“Ik vind het moeilijk een veilig wachtwoord te onthouden”) en een stelling over hergebruik van wachtwoorden (“Ik vind het moeilijk om verschillende wachtwoorden te gebruiken voor verschillende websites”).

Ernst, kwetsbaarheid en responseffectiviteit

Om ervoor te zorgen dat alle deelnemers de ernst en kwetsbaarheid van dezelfde risico’s evalueerden, gaven we deelnemers voorafgaand aan deze vragen de volgende informatie: “Het gebruiken van onveilige wachtwoorden kan verschillende negatieve gevolgen hebben. Iemand kan bijvoorbeeld toegang krijgen tot uw foto’s, uw webcam of uw sociale media accounts. Ook kan er geld worden gestolen van uw bankrekening of kunnen bestellingen op uw naam worden gedaan bij webwinkels.”

Daarna werd ernst gemeten met “De negatieve gevolgen van het gebruiken van onveilige wachtwoorden zijn ernstig” en kwetsbaarheid met “De negatieve gevolgen van het gebruiken van onveilige wachtwoorden kunnen mij overkomen”. Tot slot werd responseffectiviteit gemeten met “Wanneer ik een veilig wachtwoord gebruik, verklein ik de kans op de negatieve gevolgen die hierboven beschreven staan”.

Verantwoordelijkheid

De verantwoordelijkheid voor veilig wachtwoordgedrag werd gemeten met drie stellingen: een stelling over de eigen verantwoordelijkheid (“Het is mijn eigen verantwoordelijkheid dat ik veilige wachtwoorden gebruik”) en twee stellingen over de verantwoordelijkheid van anderen (“Het is de verantwoordelijkheid van de website of app, dat ik veilige wachtwoorden gebruik”, “Het is de verantwoordelijkheid van de overheid, dat ik veilige wachtwoorden gebruik”).

2.1.3.3 Belemmerende en bevorderende factoren

De vragenlijst bevatte ook open vragen gericht op belemmerende en bevorderende factoren om veiligere wachtwoorden te gebruiken. Deze vragen zijn gesteld om na te kunnen gaan in hoeverre deelnemers onze psychologische factoren zelf zouden noemen en of deelnemers nog andere factoren zouden noemen. Specifiek stelden we (voorafgaand aan de vragen over de psychologische factoren) de volgende twee open vragen:

- “We zijn geïnteresseerd in factoren die u zouden kunnen belemmeren om veiligere wachtwoorden te gebruiken. Wat zou u kunnen tegenhouden om veiligere wachtwoorden te gebruiken? Denk hierbij bijvoorbeeld aan bepaalde situaties, omstandigheden, persoonlijke eigenschappen, uw sociale omgeving, de online omgeving, technieken.”
- “We zijn geïnteresseerd in factoren die u zouden kunnen bevorderen om veiligere wachtwoorden te gebruiken. Wat zou u kunnen helpen om veiligere wachtwoorden te gebruiken? Denk hierbij bijvoorbeeld aan bepaalde situaties, omstandigheden, persoonlijke eigenschappen, uw sociale omgeving, de online omgeving, technieken.”

2.1.3.4 Overige vragen

Omdat het wachtwoordgedrag mogelijk kon worden beïnvloed door het gebruik van een wachtwoordmanager vroegen we (na een korte uitleg over wat een wachtwoordmanager is): “Heeft u bij het aanmaken van het wachtwoord gebruik gemaakt van een wachtwoordmanager of suggestie vanuit de browser?” (Ja; Nee).

2.1.4 Meetinstrumenten persoonsgegevens

2.1.4.1 Gedragsmaten en zelfrapportage gedrag

Gedragsmaat

Het delen van persoonsgegevens werd gemeten door deelnemers te vragen of ze deel wilden nemen aan een verloting van een waardebon van 100 euro, en door de deelnemers die “Ja” antwoordden vervolgens hun persoonsgegevens op een formulier in te laten vullen. Deze meting komt deels overeen met de objectieve gedragsmeting van het online delen van persoonsgegevens in het eerdere onderzoek van het WODC (Van ‘t Hoff-de Goede et al., 2019), met als belangrijkste verschil dat in dit eerdere onderzoek de context geen winactie was, maar een vraag op het einde van het onderzoek. Ook werd deelnemers in het eerdere onderzoek, anders dan in het huidige onderzoek, na elk invulveld de expliciete mogelijkheid geboden om de gevraagde persoonsgegevens niet te delen. Deelnemers aan het huidige onderzoek kregen de volgende informatie: “Iedere deelnemer aan de vragenlijst ontvangt na het afronden van de vragenlijst punten. Als extra bedankje wordt onder alle deelnemers van de vragenlijst een mooie prijs verloot: een cadeaubon van 100 euro. Deze verloting en het versturen van de prijs wordt verzorgd door een extern bedrijf.” Vervolgens konden deelnemers aangeven of ze wel of niet mee wilden doen aan de verloting. Deelnemers die niet mee wilden doen gingen door naar de rest van de vragenlijst. Deelnemers die wel mee wilden doen gingen door naar het formulier. Op het formulier konden deelnemers hun volledige naam, e-mailadres, telefoonnummer, geboortedatum, postcode, huisnummer en de laatste drie cijfers van hun bankrekeningnummer invullen. Alleen het invullen van de volledige naam en het e-mailadres was verplicht, de overige velden waren niet verplicht. Verplichte velden werden aangeven met een rood sterretje achter de vraag (*). In lijn met richtlijnen van de commissie ethiek kregen deelnemers onderaan het formulier de optie om deelname aan de verloting alsnog te annuleren. De gedragsmaat bestond dus uit a) deelname aan de verloting (percentage wel vs. niet) en b) het totaal aantal en type (verplichte vs. niet-verplichte) ingevulde persoonsgegevens.

Zelfrapportage gedrag

De zelfrapportage over het online veilig delen van persoonsgegevens werd op een 5-puntsschaal (van *nooit* tot *altijd*) gemeten met:

- “Ik deel mijn persoonsgegevens op websites (bijvoorbeeld bij een online prijsvraag, bij online winkelen).”

- "Ik deel mijn persoonsgegevens op sociale media (bijvoorbeeld in mijn profielinformatie, in reacties op berichten)."
- "Voor ik mijn persoonsgegevens invul op een website, kijk ik eerst of deze website veilig is."
- "Voor ik mijn persoonsgegevens invul op een website, kijk ik of dat echt nodig is."
- "Ik maak onderscheid tussen welke persoonsgegevens ik wel of niet deel op een website of sociale media (bijvoorbeeld telefoonnummer wel maar rekeningnummer niet)."

2.1.4.2 Psychologische factoren

Na de gedragsmaten en de algemene vragen over online gedrag volgden de vragen over de psychologische factoren. Tenzij anders aangegeven werden vragen beantwoord op een 5-puntsschaal, van *helemaal mee oneens* tot *helemaal mee eens*.

Responskosten

De responskosten van het online veilig delen van persoonsgegevens werd gemeten met "Het kost veel tijd om na te denken over of ik persoonsgegevens wel of niet online kan delen", "Het kost veel moeite om mijn persoonsgegevens niet online te delen, omdat het vaak nodig is voor toegang tot een website of app", en "Het kost veel moeite om na te denken over of ik persoonsgegevens online kan delen".

Zelfeffectiviteit

Zelfeffectiviteit bij het online veilig delen van persoonsgegevens is gemeten met drie stellingen: een stelling over het inschatten van de veiligheid ("Ik vind het moeilijk om in te schatten wanneer het veilig is om persoonsgegevens online te delen"), een stelling over het niet delen van persoonsgegevens ("Ik vind het moeilijk om ervoor te kiezen om persoonsgegevens online niet te delen") en een stelling over het maken van onderscheid ("Ik vind het moeilijk om onderscheid te maken in welke persoonsgegevens ik beter wel en niet online kan delen").

Ernst, kwetsbaarheid, responseffectiviteit

Om ervoor te zorgen dat alle deelnemers de ernst en kwetsbaarheid van dezelfde risico's evalueerden, gaven we ook hier voorafgaand aan de vragen de volgende informatie: "Het onveilig online delen van persoonsgegevens kan verschillende negatieve gevolgen hebben. Als deze gegevens in bezit komen van criminelen dan kunnen deze gegevens bijvoorbeeld worden gebruikt voor identiteitsfraude. Identiteitsfraude houdt in dat iemand zonder uw toestemming uw persoonlijke gegevens gebruikt om er zelf geld aan te verdienen. Iemand koopt bijvoorbeeld producten op uw naam of vraagt officiële documenten aan op uw naam. De kans op oplichting (denk bijvoorbeeld aan oplichting via Whatsapp of via e-mail) is ook groter, doordat criminelen persoonlijke informatie over u hebben waarvan u dat niet verwacht."

Daarna werd ernst gemeten met "De negatieve gevolgen van het onveilig online delen van persoonsgegevens zijn ernstig" en kwetsbaarheid met "De negatieve gevolgen van het onveilig online delen van persoonsgegevens kunnen mij overkomen". Tot slot werd responseffectiviteit

gemeten met “Wanneer ik online veilig omga met mijn persoonsgegevens, verklein ik de kans op de negatieve gevolgen die hierboven beschreven staan”.

Verantwoordelijkheid

De verantwoordelijkheid voor het veilig online delen van persoonsgegevens werd gemeten met drie stellingen: een stelling over de eigen verantwoordelijkheid (“Het is mijn eigen verantwoordelijkheid dat ik online veilig omga met mijn persoonsgegevens”) en twee stellingen over de verantwoordelijkheid van anderen (“Het is de verantwoordelijkheid van de website of app, dat ik online veilig omga met mijn persoonsgegevens”, “Het is de verantwoordelijkheid van de overheid, dat ik online veilig omga met mijn persoonsgegevens”).

2.1.4.3 Belemmerende en bevorderende factoren

Net als bij wachtwoorden hebben we ook bij persoonsgegevens open vragen gesteld over belemmerende en bevorderende factoren om online veiliger om te gaan met persoonsgegevens, om na te kunnen gaan in hoeverre deelnemers onze psychologische factoren zelf zouden noemen en of deelnemers nog andere factoren zouden noemen. Specifiek stelden we (voorafgaand aan de vragen over de psychologische factoren) de volgende twee open vragen:

- “We zijn geïnteresseerd in factoren die u zouden kunnen belemmeren om online veiliger om te gaan met persoonsgegevens. Wat zou u kunnen tegenhouden om online veiliger om te gaan met persoonsgegevens? Denk hierbij bijvoorbeeld aan bepaalde situaties, omstandigheden, persoonlijke eigenschappen, uw sociale omgeving, de online omgeving, technieken.”
- “We zijn geïnteresseerd in factoren die u zouden kunnen bevorderen om online veiliger om te gaan met persoonsgegevens. Wat zou u kunnen helpen om online veiliger om te gaan met persoonsgegevens? Denk hierbij bijvoorbeeld aan bepaalde situaties, omstandigheden, persoonlijke eigenschappen, uw sociale omgeving, de online omgeving, technieken.”

2.1.4.4 Overige vragen

Om na te kunnen gaan of de gedeelde persoonsgegevens echt waren werd aan het einde van de vragenlijst gevraagd: “Zijn alle persoonsgegevens die u heeft ingevuld op het formulier uw echte gegevens?” (Alle gegevens zijn mijn echte gegevens; Een deel zijn mijn echte gegevens; Geen van de gegevens zijn mijn echte gegevens).

2.1.5 Socio-demografische gegevens en eerder slachtofferschap

Om de representativiteit van onze steekproef te kunnen controleren vroegen we deelnemers verschillende socio-demografische gegevens te rapporteren: Deelnemers werden gevraagd naar hun geslacht, leeftijd, hoogst afgeronde opleiding en de vier cijfers van hun postcode (voor de classificatie van de regio waarin zij woonachtig zijn).

Slachtofferschap van internetcriminaliteit werd gemeten met de volgende vraag: "Internetcriminaliteit (cybercrime of online criminaliteit) is het inzetten van het internet om criminele activiteiten mee uit te voeren. Bent u weleens slachtoffer geworden van internetcriminaliteit?" (Ja, in de afgelopen 12 maanden; Ja, langer geleden dan 12 maanden; Nee; Weet ik niet).

2.1.6 Ethische toetsing

Dit onderzoek is voorgelegd aan en goedgekeurd door de Commissie Ethiek Psychologie (CEP) van het Instituut Psychologie, Universiteit Leiden (CEP 2021-12-01-E. ter Mors-V1-3587). Het uitvragen van persoonsgegevens en een wachtwoord is toegestaan volgens richtlijnen van de CEP, mits deze antwoorden niet worden opgeslagen. Zo waren de persoonsgegevens die deelnemers hebben ingevuld niet bekend bij de onderzoekers; deze zijn niet gedeeld door onderzoeksbureau Markteffect. In de door Markteffect opgeleverde dataset is alleen opgenomen of de deelnemers deze vragen wel of niet hadden beantwoord. Daarnaast waren de aangemaakte wachtwoorden van deelnemers niet bekend bij de onderzoekers, enkel wat de kenmerken en entropie van deze wachtwoorden waren (zoals gecodeerd door Markteffect). Ten slotte werden deelnemers vooraf aan het invullen van de vragenlijst zoveel mogelijk geïnformeerd over het onderzoek in de informatiebrief en werd om toestemming gevraagd om hun gegevens te mogen gebruiken voor huidig onderzoek in het "informed consent". Na het invullen van de vragenlijst werden deelnemers in de "debriefing" op de hoogte gesteld van de gedragsmaten en het doel en belang van de studie.

2.2 Resultaten

In deze sectie beschrijven we de resultaten van Studie 1. De resultaten geven inzicht in hoe veilig deelnemers zich gedragen als het gaat om het gebruik van veilige wachtwoorden (Sectie 2.2.1) en het veilig online delen van persoonsgegevens (Sectie 2.2.2).

2.2.1 Wachtwoorden

We richtten ons in de analyse van het gebruik van veilige wachtwoorden op de resultaten voor de totale steekproef (N = 998). Voor we deze resultaten bespreken is het relevant om te vermelden dat een deel van de deelnemers (10.4%) aangaf een wachtwoordmanager te hebben gebruikt bij het aanmaken van het wachtwoord. In Bijlage A beschrijven we hoe dit de resultaten in Sectie 2.2.1.1 (gedragsmaten) heeft beïnvloed. We hebben ervoor gekozen om deze deelnemers niet uit te sluiten in de analyses, omdat het gebruik van een wachtwoordmanager een goede strategie is voor het maken van een sterk en uniek wachtwoord. Ook wezen de data erop dat niet alle deelnemers die aangaven een wachtwoordmanager te hebben gebruikt dit daadwerkelijk gedaan hebben (zie uitleg in Bijlage A).

2.2.1.1 Gedragsmaten

Sterkte wachtwoorden

De resultaten voor de sterkte en kenmerken van de aangemaakte wachtwoorden zijn weergegeven in Tabellen 3 en 4. De entropie van het wachtwoord geeft de sterkte van het wachtwoord aan. De entropie wordt berekend op basis van de lengte en de samenstelling van het wachtwoord (zie Sectie 2.1.3.1).

Het merendeel van de deelnemers maakte zwakke tot zeer zwakke wachtwoorden aan (83.8%). Het merendeel van de deelnemers (74.2%) had een wachtwoord dat bestond uit minder dan 12 tekens (niet in tabel). Ook gebruikte 32.1% van de deelnemers geen hoofdletters, 20.2% geen cijfers, en 62.2% geen speciale tekens (niet in tabel). Een criterium voor sterke wachtwoorden is dat wachtwoorden bestaan uit minstens 12 tekens, minstens 1 kleine letter, 1 hoofdletter, 1 speciaal teken en 1 cijfer. Bij slechts 13.5% procent van de deelnemers voldeed het aangemaakte wachtwoord aan deze voorwaarden (niet in tabel).

Het aantal deelnemers dat een zwak tot zeer zwak wachtwoord aanmaakte is in lijn met de resultaten uit eerder onderzoek van 't Hoff-de Goede et al. (2019), waarbij 89.2% van de deelnemers (*N* = 2426) een zwak wachtwoord aanmaakte. In dit onderzoek werd als criterium van een zwak wachtwoord ook een entropie lager dan 80 aangehouden.

Tabel 3

Wachtwoorden gedragsmaat: sterkte aangemaakte wachtwoorden uitgedrukt in entropie

	Deelnemers	
	N	%
Zeer zwak (0.00-63.99 bits)	628	62.9
Zwak: (64.00-79.99 bits)	209	20.9
Gemiddeld: (80.00-111.99 bits)	103	10.3
Sterk: (112.00-127.99 bits)	9	0.9
Zeer sterk: (≥ 128 bits)	49	4.9

Noot. *N* = 998.

Tabel 4

Wachtwoorden gedragsmaat: kenmerken aangemaakte wachtwoorden

	Minimum	Maximum	Mediaan	*M*	*SD*
Entropie	4.70	210.24	56.87	60.54	27.02
Lengte	1	32	9	10.18	3.83
Kleine letters	0	21	6	6.19	3.43
Hoofdletters	0	14	1	1.07	1.46
Speciale tekens	0	10	0	0.52	0.84
Cijfers	0	11	2	2.40	1.99

Noot. N = 998.

Unieke wachtwoorden

Op de vraag of deelnemers het aangemaakte wachtwoord ook gebruiken voor andere accounts beantwoordde 22.3% van de deelnemers deze vraag bevestigend (vs. 67.1% “Nee”; 10.5% “Zeg ik liever niet”). Dit betekent dat bij een deel van de deelnemers sprake was van niet-unieke wachtwoorden.

2.2.1.2 Zelfrapportage gedrag

We legden deelnemers ook een aantal stellingen voor over veilig wachtwoordgedrag. Deze stellingen meten diverse aspecten van veilig wachtwoordgedrag bij de deelnemers, namelijk: de sterkte van wachtwoorden, het gebruik van unieke wachtwoorden en het niet delen van wachtwoorden met anderen. De antwoorden van de deelnemers (N = 998) op de stellingen worden weergegeven in Tabel 5.

Sterkte wachtwoorden

Wat betreft de sterkte van wachtwoorden gaf een minderheid van de deelnemers (36.2%) aan vaak of altijd wachtwoorden te gebruiken die bestaan uit minstens 12 tekens. Daarentegen gaf het merendeel van de deelnemers (80.4%) aan vaak of altijd wachtwoorden te gebruiken die bestaan uit verschillende tekens. Deze resultaten komen grotendeels overeen met de bevindingen bij de gedragsmaat (zie Sectie 2.2.1.1), waar we vonden dat de wachtwoorden die deelnemers aanmaakten veelal korter waren dan 12 tekens en dat de meeste deelnemers naast kleine letters ook andere tekens (hoofletter, cijfer, of speciaal teken) gebruikten.

Unieke wachtwoorden

Op het gebied van gebruik van unieke wachtwoorden gaf een deel van de deelnemers (27.5%) aan vaak of altijd hetzelfde wachtwoord te gebruiken. Ook gaf een deel van de deelnemers (26.6%) aan dat de gebruikte wachtwoorden vaak of altijd op elkaar lijken. Deze resultaten wijzen erop dat de wachtwoorden die deelnemers gebruiken (deels) niet uniek zijn, wat wijst op onveilig wachtwoordgedrag. Deze resultaten komen overeen met de bevindingen bij de gedragsmaat (zie

Sectie 2.2.1.1), waar we vonden dat een deel van de deelnemers aangaf geen uniek wachtwoord te hebben gebruikt.

Niet delen van wachtwoorden

Het delen van wachtwoorden met anderen lijkt op basis van de zelfrapportage in mindere mate een probleem dan het gebruik van zwakke wachtwoorden en het gebruik van niet unieke wachtwoorden. Slechts een kleine minderheid van de deelnemers (2.4%) gaf aan vaak of altijd wachtwoorden te delen met anderen.

Tabel 5

Zelfrapportage veilig wachtwoordgedrag

	Antwoordoptie (%)					*M*	*SD*
	1 Nooit	2 Zelden	3 Soms	4 Vaak	5 Altijd		
Sterke wachtwoorden							
Mijn wachtwoorden bestaan uit minstens 12 tekens	7.3	25.6	31.0	27.2	9.0	3.05	1.09
Mijn wachtwoorden bestaan uit verschillende tekens (kleine letters, hoofdletters, getallen en speciale tekens)	0.9	3.8	14.9	39.3	41.1	4.16	0.88
Unieke wachtwoorden							
Ik gebruik hetzelfde wachtwoord voor verschillende apps of websites (bijvoorbeeld zowel voor sociale media als online bankieren, of voor verschillende webwinkels)	17.3	19.4	35.7	24.2	3.3	2.77	1.10
De wachtwoorden die ik gebruik lijken op elkaar	14.1	20.6	38.6	23.6	3.0	2.81	1.05
Niet delen wachtwoorden							
Ik deel mijn persoonlijke wachtwoorden met anderen	73.3	19.0	5.2	1.7	0.7	1.37	0.72

Noot. N = 998.

2.2.1.3 Psychologische factoren

In deze sectie bespreken we de resultaten voor de psychologische factoren responskosten, zelfeffectiviteit, ernst, kwetsbaarheid en responseffectiviteit. De antwoorden van de deelnemers (N = 998) worden weergegeven in Tabel 6.

Responskosten

Bij responskosten gaven deelnemers aan dat het veel moeite kost om verschillende wachtwoorden voor verschillende websites te bedenken (67.9% van de deelnemers antwoordde enigszins of helemaal mee eens). Een meerderheid van de deelnemers gaf daarnaast aan dat het veel tijd en moeite kost om veilige wachtwoorden te gebruiken (respectievelijk 58.4% en 57.2% van de deelnemers antwoordde enigszins of helemaal mee eens).

Zelfeffectiviteit

Bij zelfeffectiviteit gaven deelnemers aan het moeilijk te vinden om veilige wachtwoorden te onthouden en om verschillende wachtwoorden te gebruiken voor verschillende websites (respectievelijk 77.5% en 67.2.% van de deelnemers antwoordde enigszins of helemaal mee eens). Daarnaast gaf een aanzienlijk deel van de deelnemers aan het moeilijk te vinden om een veilig wachtwoord te bedenken (43.1% van de deelnemers antwoordde enigszins of helemaal mee eens).

Ernst, kwetsbaarheid, responseffectiviteit

Na het lezen van de informatie over de gevolgen van onveilig wachtwoordgedrag (zie Sectie 2.1.3.2) gaven deelnemers aan de gevolgen ernstig te vinden en dat de gevolgen hen kunnen overkomen (respectievelijk 88.7% en 73.3% van de deelnemers antwoordde enigszins of helemaal mee eens). Ook gaven de deelnemers aan dat het gebruik van veilige wachtwoorden de kans op negatieve gevolgen verkleint (88.5% van de deelnemers antwoordde enigszins of helemaal mee eens). Deze resultaten laten zien hoe deelnemers de risico's en responseffectiviteit beoordeelden nadat ze hier over geïnformeerd waren en deze saillant waren gemaakt. We kunnen niet concluderen hoe deelnemers zonder deze informatie deze risico’s en de responseffectiviteit zouden hebben beoordeeld.

Verantwoordelijkheid

Bij verantwoordelijkheid gaven deelnemers aan dat ze zelf verantwoordelijk zijn voor het gebruik van veilige wachtwoorden (90.6% antwoordde enigszins of helemaal mee eens). Een deel van de deelnemers gaf aan dat websites en apps (45.1% antwoordde enigszins of helemaal mee eens) en/of de overheid (29.9% antwoordde enigszins of helemaal mee eens) ook (mede) verantwoordelijk zijn.

Tabel 6

Psychologische factoren wachtwoorden

	Antwoordcategorie (%)					*M*	*SD*
	1	2	3	4	5		
Responskosten							
Het kost veel tijd om veilige wachtwoorden te gebruiken	12.3	11.8	17.4	41.0	17.4	3.39	1.25
Het kost veel moeite om veilige wachtwoorden te gebruiken	11.3	13.3	18.1	39.1	18.1	3.39	1.24
Het kost veel moeite om verschillende wachtwoorden voor verschillende websites te bedenken	9.6	9.4	13.1	35.6	32.3	3.71	1.27
Zelfeffectiviteit							
Ik vind het moeilijk om een veilig wachtwoord te bedenken	16.6	21.5	18.7	31.2	11.9	3.00	1.29
Ik vind het moeilijk een veilig wachtwoord te onthouden	6.7	4.9	10.9	32.4	45.1	4.04	1.17
Ik vind het moeilijk om verschillende wachtwoorden te gebruiken voor verschillende websites	9.8	8.5	14.5	38.0	29.2	3.68	1.25
Ernst[a]							
De negatieve gevolgen van het gebruiken van onveilige wachtwoorden zijn ernstig	1.2	1.7	8.4	29.1	59.6	4.44	0.81
Kwetsbaarheid[a]							
De negatieve gevolgen van het gebruiken van onveilige wachtwoorden kunnen mij overkomen	2.3	5.3	19.1	41.5	31.8	3.95	0.96
Responseffectiviteit[a]							
Wanneer ik een veilig wachtwoord gebruik, verklein ik de kans op de negatieve gevolgen die hierboven beschreven staan	1.2	2.6	7.7	36.3	52.2	4.36	0.83
Verantwoordelijkheid							
Het is mijn eigen verantwoordelijkheid dat ik veilige wachtwoorden gebruik	0.4	0.6	8.4	26.5	64.1	4.53	0.71
Het is de verantwoordelijkheid van de website of app, dat ik veilige wachtwoorden gebruik	14.1	16.5	24.2	33.8	11.3	3.12	1.23

Het is de verantwoordelijkheid van de overheid, dat ik veilige wachtwoorden gebruik	25.2	19.9	24.9	21.7	8.2	2.68	1.28

Noot. *N* = 998. Antwoordschaal: 5-puntsschaal (1 = *helemaal mee oneens*, 2 = *enigszins mee oneens*, 3 = *niet mee oneens maar ook niet mee eens*, 4 = *enigszins mee eens*, 5 = *helemaal mee eens*).

[a] De ernst, kwetsbaarheid en responseffectiviteit antwoorden zijn geïnformeerde antwoorden: deelnemers lazen voor het beantwoorden van de stellingen informatie over negatieve gevolgen van onveilig wachtwoordgedrag (zie Sectie 2.1.3.2).

2.2.1.4 Verbanden

We hebben vervolgens gekeken in hoeverre veilig wachtwoordgedrag (gedragsmaten, zelfrapportage gedrag) verband houdt met de psychologische factoren responskosten, zelfeffectiviteit, ernst, kwetsbaarheid, responseffectiviteit en verantwoordelijkheid. We richtten ons hierbij op de sterkte van wachtwoorden en het gebruik van unieke wachtwoorden, niet op het delen van wachtwoorden met anderen, omdat bij eerstgenoemde aspecten met name onveilig gedrag optreedt. We hebben schalen gemaakt voor de variabelen responskosten, zelfeffectiviteit en "verantwoordelijkheid anderen". De correlaties tussen (geobserveerd en zelfgerapporteerd) wachtwoordgedrag en de psychologische factoren staan in Tabel 7. De resultaten lieten zwakke tot middelmatige verbanden (Cohen, 1988) in de verwachte richting zien tussen de psychologische factoren en wachtwoordgedrag, met uitzondering van kwetsbaarheid.

Hoe hoger de deelnemers de *responskosten* inschatten, hoe onveiliger hun geobserveerde en zelfgerapporteerde wachtwoordgedrag was. Voor *zelfeffectiviteit* lieten de resultaten zien dat hoe hoger de waargenomen zelfeffectiviteit was, hoe veiliger het geobserveerde en zelfgerapporteerde wachtwoordgedrag van de deelnemers was.

Voor *ernst* en *responseffectiviteit* waren er geen significantie correlaties met de entropie van het aangemaakte wachtwoord. De resultaten lieten wel zien dat dat hoe hoger de waargenomen ernst en responseffectiviteit, hoe vaker de deelnemers aangaven een uniek wachtwoord te hebben gemaakt en hoe veiliger het zelfgerapporteerde gedrag was (met uitzondering van het aantal tekens in wachtwoorden voor responseffectiviteit).

Voor *kwetsbaarheid* waren de resultaten anders dan verwacht: Hoe hoger de kwetsbaarheid hoe *lager* de entropie van het aangemaakte wachtwoord en hoe *onveiliger* de zelfrapportage van gedrag. Er waren geen significante correlaties met de uniekheid van het aangemaakte wachtwoord.

Tot slot waren er voor *verantwoordelijkheid* minder duidelijke verbanden. Er waren geen significante correlaties met geobserveerd wachtwoordgedrag. Wel was het zo dat hoe sterker de eigen verantwoordelijkheid was, hoe meer verschillende tekens de deelnemers zeiden te gebruiken en hoe minder de deelnemers aangaven wachtwoorden te hergebruiken. Daarnaast lieten de resultaten

zien dat hoe meer de deelnemers de verantwoordelijkheid bij een ander legden, hoe minder ze aangaven verschillende tekens te gebruiken.

Tabel 7

Correlaties veilig wachtwoordgedrag (gedragsmaten, zelfrapportage gedrag) en psychologische factoren

Psychologische factoren	Gedragsmaten		Zelfrapportage gedrag			
	Sterkte wachtwoorden	Unieke wachtwoorden	Sterkte wachtwoorden	Sterkte wachtwoorden	Unieke wachtwoorden	Unieke wachtwoorden
	Entropie aangemaakt wachtwoord	Aangemaakt wachtwoord ook in gebruik voor andere accounts (0 = "Nee", 1 = "Ja")[a, b]	Mijn wachtwoorden bestaan uit minstens 12 tekens	Mijn wachtwoorden bestaan uit verschillende tekens (kleine letters, hoofdletters, getallen en speciale tekens)	Ik gebruik hetzelfde wachtwoord voor verschillende apps of websites (bijvoorbeeld zowel voor sociale media als online bankieren, of voor verschillende webwinkels)	De wachtwoorden die ik gebruik lijken op elkaar
Responskosten (schaal, 3 stellingen, α = .87)	-.13**	.15**	-.25**	- .13**	.27**	.30**
Zelfeffectiviteit (schaal, 3 stellingen, omgecodeerd, α = .75)	.11**	-.16**	.25**	.16**	-.31**	-.29**
Ernst	.06	-.12**	.09**	.19**	-.19**	-.10**
Kwetsbaarheid	-.07*	.03	-.12**	-.04	.08*	.19**
Responseffectiviteit	.05	-.07*	.04	.20**	-.15*	-.07*
Verantwoordelijkheid						

Eigen	.00	-.00	.00	.21**	-.07*	-.06
Anderen (schaal, 2 stellingen, r = .69, p < .001)	-.05	-.01	.02	-.10**	-.02	.04

Noot. N = 998. Antwoordschaal stellingen psychologische factoren: 5-puntsschaal (1 = *helemaal mee oneens*, 2 = *enigszins mee oneens*, 3 = *niet mee oneens maar ook niet mee eens*, 4 = *enigszins mee eens*, 5 = *helemaal mee eens*). Hogere scores geven, respectievelijk, hogere waargenomen responskosten, zelfeffectiviteit, ernst, kwetsbaarheid, responseffectiviteit, en verantwoordelijkheid weer (zelfeffectiviteit antwoorden zijn omgecodeerd). Voor de volledige vragen, zie Tabel 6.
Niet in tabel: de gedragsmaat sterkte wachtwoorden correleerde, zoals verwacht, positief met de zelfrapportage over de sterkte van wachtwoorden (r = .34, p < .001, r = .19, p < .001, respectievelijk, N = 998). Dit betekent dat deelnemers die sterkere wachtwoorden aanmaakten ook bij de zelfrapportage (iets) vaker aangaven sterke wachtwoorden te gebruiken. De gedragsmaat unieke wachtwoorden correleerde verder, zoals verwacht, positief met de zelfrapportage over unieke wachtwoorden (r_{pb} = .33, p < .001, r = .30, p < .001, respectievelijk, N = 893). Deelnemers die bij de gedragsmaat aangaven een eerder wachtwoord te hebben hergebruikt, gaven ook (iets) vaker bij de zelfrapportage aan wachtwoorden te hergebruiken.
[a] Deelnemers die "Wil ik niet zeggen" antwoordden zijn niet meegenomen in de analyse, N = 893 voor deze stelling. [b] Punt-biseriële correlaties.
* p < 0.05, ** p < .01.

We hebben vervolgens regressieanalyses uitgevoerd op veilig wachtwoordgedrag (gedragsmaten, zelfrapportage gedrag) met de volgende voorspellende variabelen: psychologische factoren, socio-demografische variabelen (geslacht, leeftijd en hoogst afgeronde opleiding), eerder slachtofferschap, en (bij de gedragsmaat voor sterkte van wachtwoorden) het gebruik van een wachtwoordmanager bij het aanmaken van het wachtwoord. De resultaten worden weergegeven in Tabel 8.

Met betrekking tot de psychologische factoren lieten de resultaten zien dat met name ernst, zelfeffectiviteit en responskosten een rol spelen bij veilig wachtwoordgedrag. Ernst was een significante voorspeller van veilig wachtwoordgedrag: hoe hoger de waargenomen ernst van de risico's van onveilig wachtwoordgedrag, hoe hoger de entropie van het aangemaakte wachtwoord, hoe unieker het aangemaakte wachtwoord en hoe veiliger het zelfgerapporteerde gedrag. Zelfeffectiviteit was geen significante voorspeller van geobserveerd gedrag (we vonden geen relatie met de entropiemaat of met de gedragsmaat unieke wachtwoorden), maar voorspelde wel het zelfgerapporteerde gedrag. Hoe hoger de inschatting van zelfeffectiviteit, hoe veiliger het zelfgerapporteerde wachtwoordgedrag. Responskosten was ook geen significante voorspeller van entropie, maar wel van de gedragsmaat unieke wachtwoorden en van een deel van het zelfgerapporteerde gedrag. Hoe hoger de inschatting van responskosten, hoe minder uniek de wachtwoorden en hoe minder vaak wachtwoorden bestonden uit minstens 12 tekens. Kwetsbaarheid, responseffectiviteit en verantwoordelijkheid (eigen, anderen) voorspelden zeer beperkt veilig wachtwoordgedrag (zie Tabel 8, slechts bij één zelfrapportage item een significante voorspeller).

Met betrekking tot de socio-demografische variabelen bleek dat sekse geen significante voorspeller was van veilig wachtwoordgedrag, en dat opleidingsniveau ook een beperkte rol speelde (alleen voorspeller van de zelfrapportage “wachtwoorden bestaan uit verschillende tekens”: veiliger wachtwoordgedrag bij opleiding hoog deelnemers vergeleken met opleiding midden deelnemers). Leeftijd speelde alleen een rol bij zelfrapportage van unieke wachtwoorden: hoe hoger de leeftijd, hoe minder deelnemers aangaven wachtwoorden te hergebruiken en hoe veiliger het zelfgerapporteerde gedrag.

Eerder slachtofferschap was geen significante voorspeller van veilig wachtwoordgedrag. Het gebruik van een wachtwoordmanager bij het aanmaken van het wachtwoord was wel een significante voorspeller van de entropie van het aangemaakte wachtwoord (zie ook Bijlage A); het wachtwoord van deelnemers die een wachtwoordmanager hadden gebruikt was sterker dan het wachtwoord van deelnemers die geen wachtwoordmanager hadden gebruikt.

Tabel 8

Regressies veilig wachtwoordgedrag (gedragsmaten, zelfrapportage gedrag)

Voorspellers	Gedragsmaten *B* (*SE*) β		Zelfrapportage gedrag *B* (*SE*) β			
	Sterkte wachtwoorden	Unieke wachtwoorden	Sterkte wachtwoorden	Sterkte wachtwoorden	Unieke wachtwoorden	Unieke wachtwoorden
	Entropie aangemaakt wachtwoord	Aangemaakt wachtwoord ook in gebruik voor andere accounts (0 = “Nee”, 1 = "Ja”)	Mijn wachtwoorden bestaan uit minstens 12 tekens	Mijn wachtwoorden bestaan uit verschillende tekens (kleine letters, hoofdletters, getallen en speciale tekens)	Ik gebruik hetzelfde wachtwoord voor verschillende apps of websites (bijvoorbeeld zowel voor sociale media als online bankieren, of voor verschillende webwinkels)	De wachtwoorden die ik gebruik lijken op elkaar
Constante	141.19 (10.14)**	-0.28 (1.02)	2.87 (0.42)**	2.41 (0.33)**	5.09 (0.41)**	3.40 (0.39)**
Responskosten (schaal, 3 stellingen, α = .87)	-1.60 (1.01) -0.07	0.24 (0.11)* 	-0.13 (0.05)** -.14**	-0.01 (0.04) -.02	0.07 (0.04) .07	0.13 (0.04)** .14**
Zelfeffectiviteit (schaal, 3 stellingen, omgecodeerd, α = .75)	-0.31 (1.14) -0.01	-0.25 (0.13) 	0.17 (0.05)** .16**	0.11 (0.04)** .13**	-0.29 (0.05)** -.26**	-0.14 (0.05)** -.14**
Ernst	2.80 (1.15)* 0.09*	-0.46 (0.12)**	0.21 (0.05)** .16**	0.13 (0.04)** .12**	-0.26 (0.05)** -.19**	-0.19 (0.05)** -.15**
Kwetsbaarheid	-1.77 (0.91) -0.06	0.01 (0.10) 	-0.06 (0.04) -.05	-0.05 (0.03) -.06	0.06 (0.04) .05	0.16 (0.04)** -.14**
Responseffectiviteit	0.81 (1.11) 0.03	-0.05 (0.12) 	-0.02 (0.05) -.02	0.09 (0.04)* .08*	-0.06 (0.05) -.05	0.02 (0.05) .01
Verantwoordelijkheid						

Eigen	-1.88 (1.28) -0.05	0.14 (0.14)	-0.05 (0.06) -.03	0.14 (0.05)** .11**	0.05 (0.06) .03	-0.02 (0.05) -.01
Anderen (schaal, 2 stellingen, r = .69, p < .001)	-0.59 (0.68) -0.03	-0.01 (0.07)	0.03 (0.03) .03	-0.03 (0.02) -.04	-0.07 (0.03)* -.07**	-0.00 (0.03) -.00
Leeftijd	0.04 (0.06) 0.02	0.007 (0.006)	-0.004 (0.003) -.06	0.004 (0.002) .07	-0.013 (0.002)** -.18**	-0.011 (0.002)** -.17**
Vrouw[c]	1.41 (1.59) 0.03	0.07 (0.17)	0.03 (0.07) .01	-0.04 (0.06) -.02	-0.02 (0.07) -.01	0.08 (0.07) .04
Opleidingsniveau[d]						
Laag	-3.85 (2.26) -0.05	0.31 (0.24)	0.05 (0.10) .02	0.00 (0.08) .00	0.08 (0.10) .03	0.18 (0.09) .06
Hoog	0.01 (1.73) 0.00	0.01 (0.19)	-0.07 (0.08) -.03	0.22 (0.06)** .12**	0.01 (0.08) .00	0.01 (0.07) .00
Eerder slachtofferschap[e]						
Ja, korter dan 12 maanden geleden	-3.68 (3.18) -0.03	0.42 (0.32)	.01 (.15) .00	0.15 (0.11) .04	0.14 (0.14) .03	0.13 (0.13) .03
Ja, langer dan 12 maanden geleden	-0.56 (2.52) -0.01	0.48 (0.25)	.01 (.11) .00	-0.08 (0.09) -.03	0.01 (0.11) .00	0.15 (0.10) .04
Gebruik wachtwoordmanager[f]	39.65 (2.48)** 0.47**	n.v.t.	n.v.t.	n.v.t.	n.v.t	n.v.t
Adjusted R^2	0.24	.09[a]	.09	.10	.17	.15
N	920[b]	835	923	923	923	923

Noot. N is kleiner dan 998 door missing values bij de variabelen leeftijd, geslacht, opleidingsniveau en eerder slachtofferschap, en bij de gedragsmaat voor unieke wachtwoorden. Antwoordschaal stellingen psychologische factoren: 5-puntsschaal (1 = *helemaal mee oneens*, 2 = *enigszins mee oneens*, 3 = *niet mee oneens maar ook niet mee eens*, 4 = *enigszins mee eens*, 5 = *helemaal mee eens*). Voor de volledige vragen, zie Tabel 6. Voor de analyses is gebruik gemaakt van multipele regressie, en in het geval van de gedragsmaat voor unieke wachtwoorden een logistische regressie met een binaire uitkomstvariabele.

[a] Nagelkerke R square. [b] Drie outliers op de variabele entropie zijn uitgesloten van deze analyse. [c] Dummy-variabele met 0 = man en 1 = vrouw. [d] Dummy-variabelen met 0 = opleidingsniveau midden en respectievelijk 1 = opleidingsniveau laag en 1 = opleidingsniveau hoog. [e] Dummy-variabelen met 0 = geen eerder slachtofferschap en

respectievelijk 1 = eerder slachtofferschap in de afgelopen 12 maanden en 1 = eerder slachtofferschap langer dan 12 maanden geleden. [f] Dummy-variabele met 0 = geen wachtwoordmanager gebruikt en 1 = wel wachtwoordmanager gebruikt.
* $p < .05$, ** $p < .01$.

2.2.1.5 Belemmerende en bevorderende factoren

Voordat de deelnemers de stellingen over de psychologische factoren beantwoordden, stelden we hen twee open vragen over factoren die hen belemmeren en bevorderen om veiliger wachtwoordgedrag te vertonen. Hierbij kregen zij eerst uitleg over wat veilig wachtwoordgedrag inhoudt (zie Sectie 2.1.3.3 voor de informatie en de vraagstelling).

Om de antwoorden te analyseren heeft het onderzoeksteam codeerschema's gemaakt. De psychologische factoren uit het onderzoeksmodel (zie Figuur 1) vormden de basis van het schema, met categorieën zoals zelfeffectiviteit (F). Binnen deze categorieën werd op basis van een steekproef uit de antwoorden subcategorieën gemaakt, zoals moeite met het onthouden van veilige wachtwoorden (F1). Vervolgens werd door een andere onderzoeker bij het antwoord van de deelnemers gecodeerd welke belemmerende of bevorderende factoren in deze stelling terugkwamen. Een steekproef hiervan werd steeds door een tweede onderzoeker apart gecodeerd, waarbij afgestemd kon worden over twijfelgevallen en de mate van overeenkomst gecontroleerd kon worden. We beschrijven hier de hoofdlijnen van de bevindingen uit de open vragen (N = 998, 1202 coderingen voor de belemmerende factoren; N = 998, 1055 coderingen voor de bevorderende factoren). De gedetailleerde codeerschema's en de resultaten van de analyses (i.e., frequenties per code categorie, antwoorden van deelnemers en toegewezen codeercodes) zijn hier beschikbaar: https://easy.dans.knaw.nl/ui/home.

Belemmerende factoren

De meest genoemde belemmerende factor was met afstand zelfeffectiviteit (47.3% van de antwoorden), en binnen deze antwoordcategorie dan met name het onthouden van wachtwoorden (36.7%van de antwoorden). Deelnemers gaven aan het moeilijk te vinden om veilige wachtwoorden te onthouden, ook gelinkt aan de hoeveelheid accounts en wachtwoorden die ze hebben. Voorbeelden van antwoorden waren "Veilige wachtwoorden zijn lastiger te onthouden" en "Ik vergeet de wachtwoorden". Responskosten werd daarnaast door een deel van de deelnemers (12.9% van de antwoorden) als belemmerende factor genoemd. Deelnemers gaven hier onder andere aan dat het veel tijd en/of moeite kost om veilige wachtwoorden te gebruiken. Voorbeelden van antwoorden waren "Lastig om overal alles aan te passen, duurt lang", en "Aantal wachtwoorden is zo groot, veel werk om ze te wijzigen".

Bevorderende factoren

Over het algemeen bleek dat deelnemers op de vraag over bevorderende factoren minder samenhangende antwoorden gaven dan bij de vraag over de belemmerende factoren. Mogelijk werd de vraag over bevorderende factoren verkeerd begrepen, of had het te maken met het feit dat de vraag over belemmerende factoren als eerste werd gesteld.

Op de vraag "Wat zou u kunnen helpen om veiligere wachtwoorden te gebruiken?" gaf een deel van de deelnemers (23.4% van de antwoorden) een antwoord in de codeercategorie "wachtwoordmanagers". Deelnemers gaven aan dat een app die hen zou helpen wachtwoorden aan te maken en te onthouden veilig gedrag zou bevorderen. Hieruit bleek dat niet iedereen bekend was

met wachtwoordmanagers (zie ook Bijlagen B en D). Voorbeelden van antwoorden waren: “Als er een veilige manier was om ze op een handige manier op te slaan” en “Makkelijke wachtwoorden beheren via een beveiligde app”. Verder ging 9.7% van de antwoorden over zelfeffectiviteit. Deelnemers gaven aan dat ze veiliger wachtwoordgedrag zouden vertonen als ze zelf meer “Creatief zijn” of gebruik konden maken van “Ezelsbruggetjes”. Ook kwetsbaarheid werd door een deel van de deelnemers als een bevorderende factor voor veilig wachtwoordgedrag genoemd (ongeveer 9.3% van de antwoorden). Bijvoorbeeld preventief “Voor de veiligheid van mijn gegevens”, maar ook uit angst voor hackers “Ik ben veel te bang om gehackt te worden”.

De resultaten op de belemmerende en bevorderende factoren waren in lijn met de resultaten van op de psychologische factoren. Net als de resultaten beschreven in Sectie 2.2.1.3, lijken zelfeffectiviteit en responskosten belangrijke factoren bij de beslissing om wel of geen veilig wachtwoordgedrag te vertonen. De kwetsbaarheid resultaten lieten, in tegenstelling tot de resultaten beschreven in Sectie 2.2.1.3, zien dat deelnemers veilig wachtwoordgedrag vertonen omdat ze zich kwetsbaar voelen. Het is niet duidelijk waarom het verband tussen kwetsbaarheid en veilig wachtwoordgedrag negatief was bij de verbanden analyse. Op basis van eerdere literatuur over kwetsbaarheid (Tam et al., 2009) en deze open vragen over de belemmerende en bevorderende factoren, denken we dat het bevorderen van gevoelens van kwetsbaarheid wel degelijk zou kunnen zorgen voor veilig wachtwoordgedrag. Toekomstig onderzoek zou hier dieper op in kunnen gaan.

2.2.1.6 Samenvatting resultaten wachtwoorden

De resultaten van Studie 1 laten onveilig wachtwoordgedrag zien. De wachtwoorden die deelnemers aanmaakten waren veelal zwak en er was sprake van hergebruik van wachtwoorden. Als belemmerende factoren voor veilig wachtwoordgedrag kwamen responskosten en zelfeffectiviteit naar voren: veilig wachtwoordgedrag kost in de ogen van de deelnemers veel tijd en moeite, en deelnemers achtten zich beperkt in staat om veilige wachtwoorden aan te maken en/of te onthouden. Ook vonden we relaties in de verwachte richting tussen responskosten en zelfeffectiviteit en veilig wachtwoordgedrag: hoe hoger de responskosten en hoe lager de zelfeffectiviteit, hoe minder veilig het wachtwoordgedrag. Naast responskosten en zelfeffectiviteit kwam ernst ook naar voren als een belangrijke voorspeller van veilig wachtwoordgedrag: deelnemers erkenden—na het lezen van informatie over risico's—de ernst van de risico's van onveilig wachtwoordgedrag, en hoe meer ze de gevolgen als ernstig beoordeelden, hoe veiliger hun wachtwoordgedrag was.

Geslacht speelde geen rol bij veilig wachtwoordgedrag in Studie 1, en ook opleiding speelde slechts beperkt een rol. Leeftijd leek wel relevant op het gebied van uniekheid van wachtwoorden, maar dan alleen bij zelfrapportage, niet bij de gedragsmaten: oudere deelnemers gaven vaker aan unieke wachtwoorden te gebruiken dan jongere deelnemers. Het gebruik van een wachtwoordmanager bij het aanmaken van het wachtwoord resulteerde verder in sterkere wachtwoorden. Eerder

slachtofferschap van cybercriminaliteit was geen significante voorspeller van veilig wachtwoordgedrag.

2.2.2 Persoonsgegevens

In deze sectie beschrijven we de resultaten voor het veilig online delen van persoonsgegevens. Bij analyses met de gedragsmaat richtten we ons op de deelnemers die meededen aan de winactie en die deze deelname niet later hebben geannuleerd (*N* = 803). In de rest van de analyses richtten we ons op de resultaten voor de totale steekproef (*N* = 998).

2.2.2.1 Gedragsmaten

Niet alle deelnemers namen deel aan de verloting. Van de 998 deelnemers antwoordden 97 deelnemers (9.7%) “Nee” op de vraag of ze mee wilden doen aan de verloting. Daarnaast kozen 98 deelnemers (9.8%) er na het verschijnen van het formulier voor om hun deelname te annuleren. In totaal nam het merendeel van de deelnemers deel aan de verloting, namelijk 803 deelnemers (80.5%). Met deze deelname stemden ze dus in met het online delen van hun persoonsgegevens. Belangrijk om hierbij te vermelden is dat de 80.5% mogelijk in werkelijkheid (iets) lager is: onderzoeksbureau Markteffect meldde dat bij het verschijnen van het formulier het aantal deelnemers dat stopte met de vragenlijst in verhouding hoger was dan bij andere onderdelen in de vragenlijst (voor meer informatie; zie de onderzoek verantwoording van Markteffect die hier te vinden is: https://easy.dans.knaw.nl/ui/home). Een reden voor het stoppen met de vragenlijst kan zijn dat deelnemers toch niet wilden deelnemen aan de verloting en de annuleren knop niet gezien of overwogen hebben.

Tabel 9 geeft de verdeling van de hoeveelheid en het type gedeelde persoonsgegevens weer onder de 803 deelnemers die deelnamen aan de verloting. Uit de resultaten blijkt dat deze veel persoonsgegevens deelden, ook niet-verplichte gegevens. Een kleine minderheid van de deelnemers deelde alleen de niet-verplichte persoonsgegevens (9.3%) (niet in tabel). Het merendeel van de deelnemers (70.9%) deelde alle zeven persoonsgegevens (niet in tabel). Opvallend is dat maar liefst 85.2% van de deelnemers de laatste drie cijfers van hun bankrekening invulden, terwijl het niet verplicht was deze gegevens te delen. Dit percentage ligt in dit onderzoek een stuk hoger dan de gedragsmeting in het eerdere onderzoek van het WODC, waarbij "slechts" 4.8% van de deelnemers bereid was tot het invullen van de laatste drie cijfers van hun bankrekeningnummer (Van ‘t Hoff-de Goede et al., 2019). De context van dit eerdere onderzoek en vraagstelling was wel anders dan in het huidige onderzoek (zie ook Sectie 2.1.4.1). Van ’t Hoff-de Goede et al. (2019) vroegen hun deelnemers om hun persoonsgegevens te delen zonder dit te koppelen aan een verloting (zoals in het huidige onderzoek het geval was) en boden bij elk invulveld een expliciete mogelijkheid om de gevraagde persoonsgegevens niet te delen (anders dan in het huidige onderzoek). Wanneer er een verloting plaatsvindt en de ‘opt out’ keuze om gevraagde persoonsgegevens niet te delen minder laagdrempelig is, zoals in het huidige onderzoek, zijn deelnemers wellicht meer bereid om hun

rekeningnummer te geven dan wanneer dit niet het geval is. Dit geeft aan dat de context een grote invloed kan hebben op hoe (on)veilig mensen zich online gedragen.

Op de vraag of alle persoonsgegevens die de deelnemers hebben ingevuld op het formulier echte gegevens betroffen, gaven vrijwel alle deelnemers (91.3%) aan dat dit het geval was (vs. 7.6% "Deel echte gegevens, deel verzonnen" en 1.1% "Geen van de ingevulde gegevens zijn eigen gegevens").

Tabel 9

Gedragsmaat persoonsgegevens: Gedeelde persoonsgegevens door deelnemers die deelnamen aan de verloting

	Deelnemers	
	N	%
Volledige naam *	803	100.0
E-mailadres *	803	100.0
Telefoonnummer	590	73.5
Geboortedatum	714	88.9
Postcode	717	89.3
Huisnummer	692	86.2
Laatste drie cijfers van bankrekeningnummer	684	85.2

Noot. *N* = 803. * Verplicht in te vullen.

2.2.2.2 Zelfrapportage gedrag

Wat betreft de zelfrapportage van het online delen van persoonsgegevens (zie Tabel 10) gaf een minderheid van de deelnemers aan vaak of altijd persoonsgegevens te delen op websites (13.7%) of op sociale media (2.2%). Op het gebied van het herkennen van onveilige situaties gaf de meerderheid van de deelnemers (61.6%) aan vaak of altijd eerst te kijken of de website veilig is voor zij hun persoonsgegevens delen. Een merendeel van de deelnemers (77.3%) gaf aan vaak of altijd te kijken of het delen van persoonsgegevens echt nodig is. Ten slotte, bij het maken van onderscheid tussen welke persoonsgegevens wel en niet veilig zijn om online te delen, gaf het grootste deel van de deelnemers (76.1%) aan vaak of altijd onderscheid te maken in welke gegevens wel of niet veilig zijn om te delen.

De gedragsmeting liet zien dat van de deelnemers die deelnamen aan de verloting van de prijs maar liefst 70.9% alle zeven persoonsgegevens deelde, waarvan er vijf niet verplicht waren (waaronder de laatste drie cijfers van het rekeningnummer) (zie Sectie 2.2.2.1). De zelfrapportage van gedrag kwam daarmee beperkt overeen met de resultaten op de gedragsmaat (zie ook de noot onder Tabel 12).

Tabel 10

Zelfrapportage online delen persoonsgegevens

	Antwoordcategorie (%)					*M*	*SD*
	1 Nooit	2 Zelden	3 Soms	4 Vaak	5 Altijd		
Ik deel mijn persoonsgegevens op websites (bijv. bij een online prijsvraag, bij online winkelen)	16.4	26.4	43.5	12.1	1.6	2.56	0.96
Ik deel mijn persoonsgegevens op sociale media (bijv. in mijn profielinformatie, in reacties op berichten)	60.8	25.8	11.2	1.7	0.5	1.55	0.80
Voor ik mijn persoonsgegevens invul op een website, kijk ik eerst of deze website veilig is	4.6	9.6	24.2	33.4	28.2	3.71	1.11
Voor ik mijn persoonsgegevens invul op een website, kijk ik of dat echt nodig is	2.1	5.1	15.5	39.8	37.5	4.05	0.96
Ik maak onderscheid tussen welke persoonsgegevens ik wel of niet deel op een website of sociale media (bijv. telefoonnummer wel, maar rekeningnummer niet)	3.0	4.1	16.8	34.6	41.5	4.07	1.01

Noot. N = 998.

2.2.2.3 Psychologische factoren

In deze sectie bespreken we de resultaten voorde de psychologische factoren responskosten, zelfeffectiviteit, ernst, kwetsbaarheid en responseffectiviteit. De antwoorden van de deelnemers (N = 998) worden weergegeven in Tabel 11.

Responskosten

Bij responskosten gaf een deel van de deelnemers aan dat het veel tijd kost om na te denken of persoonsgegevens wel of niet online gedeeld kunnen worden (39.2% antwoordde enigszins of helemaal mee eens). Een meerderheid van de deelnemers gaf daarnaast aan dat het veel moeite kost om persoonsgegevens niet online te delen, omdat het vaak nodig is voor toegang tot een website of app (55.7% antwoordde enigszins of helemaal mee eens). Ten slotte gaf een deel van de deelnemers aan dat het veel moeite kost om na te denken of persoonsgegevens online gedeeld kunnen worden (36.7% antwoordde enigszins of helemaal mee eens).

Zelfeffectiviteit

Een deel van de deelnemers gaf aan het moeilijk te vinden om in te schatten wanneer het veilig is om persoonsgegevens online te delen (46.0% antwoordde enigszins of helemaal mee eens). Daarnaast gaf een minderheid van de deelnemers aan het moeilijk te vinden om ervoor te kiezen persoonsgegevens online niet te delen (26.8% antwoordde enigszins of helemaal eens) of het moeilijk te vinden een onderscheid te maken tussen welke persoonsgegevens beter wel en niet online gedeeld kunnen worden (32.7% antwoordde enigszins of helemaal eens).

Ernst, kwetsbaarheid, responseffectiviteit

Na het lezen van de informatie over de gevolgen van het online onveilig delen van persoonsgegevens (zie Sectie 2.1.3.2) gaven bijna alle deelnemers aan de gevolgen ernstig te vinden (91.5%) antwoordde enigszins of helemaal mee eens). Daarnaast gaf het merendeel van de deelnemers aan dat de gevolgen hen kunnen overkomen (75.3% antwoordde enigszins of helemaal mee eens). Ook dachten de meeste deelnemers dat het veilig omgaan met persoonsgegevens de kans op de negatieve gevolgen verkleint (86.3% van de deelnemers antwoordde enigszins of helemaal mee eens). Deze resultaten lieten zien hoe deelnemers de risico's en responseffectiviteit beoordeelden nadat ze hier over geïnformeerd waren en deze saillant waren gemaakt. We kunnen niet concluderen hoe deelnemers zonder deze informatie deze risico’s en de responseffectiviteit hadden beoordeeld (zie ook Sectie 2.2.1.3 bij wachtwoorden).

Verantwoordelijkheid

Bij verantwoordelijkheid gaf het merendeel van de deelnemers aan zelf verantwoordelijk te zijn voor het veilig online delen van hun persoonsgegevens (88.3% antwoordde enigszins of helemaal mee eens). Het merendeel van de deelnemers gaf daarnaast aan dat websites en apps (mede) verantwoordelijk zijn (58.7% antwoordde enigszins of helemaal mee eens). Ten slotte gaf een deel van de deelnemers aan dat de overheid (mede) verantwoordelijk is (42% antwoordde enigszins of helemaal mee eens).

Deelnemers legden de verantwoordelijkheid voor het online veilig delen van persoonsgegevens meer elders, in vergelijking met de resultaten bij wachtwoorden (zie ook de resultaten bij de open vragen in Sectie 2.2.2.5). Dit is mogelijk te verklaren door het feit dat mensen niet altijd controle hebben over het al dan niet delen van persoonsgegevens, doordat het delen soms verplicht is (of zo wordt gezien).

Tabel 11

Psychologische factoren persoonsgegevens

	Antwoordcategorie (%)					*M*	*SD*
	1	2	3	4	5		
Responskosten							
Het kost veel tijd om na te denken over of ik persoonsgegevens wel of niet online kan delen	15.3	22.5	22.9	32.1	7.1	2.93	1.20
Het kost veel moeite om mijn persoonsgegevens niet online te delen, omdat het vaak nodig is voor toegang tot een website of app	9.8	14.4	20.0	41.1	14.6	3.36	1.18
Het kost veel moeite om na te denken over of ik persoonsgegevens online kan delen	14.9	23.7	24.6	29.6	7.1	2.90	1.19
Zelfeffectiviteit							
Ik vind het moeilijk om in te schatten wanneer het veilig is om persoonsgegevens online te delen	10.5	19.9	23.5	34.2	11.8	3.17	1.19
Ik vind het moeilijk om ervoor te kiezen om persoonsgegevens online niet te delen	21.8	24.6	26.7	22.5	4.3	2.63	1.18
Ik vind het moeilijk om onderscheid te maken welke persoonsgegevens ik beter wel en niet online kan delen	16.4	26.6	24.3	26.7	6.0	2.79	1.18
Ernst							
De negatieve gevolgen van het onveilig online delen van persoonsgegevens zijn ernstig	0.5	1.0	6.9	23.9	67.6	4.57	0.71
Kwetsbaarheid							
De negatieve gevolgen van het online onveilig delen van persoonsgegevens kunnen mij overkomen	1.0	5.6	18.1	42.4	32.9	4.01	0.91
Responseffectiviteit							
Wanneer ik online veilig omga met mijn persoonsgegevens, verklein ik de kans op de negatieve gevolgen die hierboven beschreven staan	1.1	2.9	9.7	41.3	45.0	4.26	0.83
Verantwoordelijkheid							
Het is mijn eigen verantwoordelijkheid dat ik online veilig omga met mijn persoonsgegevens	0.4	1.9	9.4	35.5	52.8	4.38	0.77

Het is de verantwoordelijkheid van de website of app, dat ik online veilig omga met mijn persoonsgegevens	9.5	10.8	20.9	43.3	15.4	3.44	1.16
Het is de verantwoordelijkheid van de overheid, dat ik online veilig omga met mijn persoonsgegeven	16.3	15.6	26.1	30.4	11.6	3.05	1.26

Noot. N = 998. Antwoordschaal: 5-puntsschaal (1 = *helemaal mee oneens*, 2 = *enigszins mee oneens*, 3 = *niet mee oneens maar ook niet mee eens*, 4 = *enigszins mee eens*, 5 = *helemaal mee eens*).

2.2.2.4 Verbanden

We hebben vervolgens gekeken in hoeverre het veilig online delen van persoonsgegevens (gedragsmaten, zelfrapportage gedrag) verband houdt met de psychologische factoren responskosten, zelfeffectiviteit, ernst, kwetsbaarheid, responseffectiviteit en verantwoordelijkheid. We hebben schalen gemaakt voor de variabelen responskosten, zelfeffectiviteit en 'verantwoordelijkheid anderen'. De correlaties tussen het veilig online delen van persoonsgegevens (geobserveerd en zelfrapportage) en de psychologische factoren staan in Tabel 12. De resultaten lieten zwakke tot middelmatige verbanden (Cohen, 1988) in de verwachte richting zien tussen de psychologische factoren en het online veilig delen van persoonsgegevens, met uitzondering van kwetsbaarheid en (deels) verantwoordelijkheid zelf.

Voor *responskosten, zelfeffectiviteit, ernst* en *responseffectiviteit* waren er geen significante correlaties met de gedragsmaten. Wel was het zo dat hoe hoger deelnemers de responskosten inschatten, hoe onveiliger het zelfgerapporteerde gedrag was. Ook lieten de resultaten zien dat hoe hoger de geschatte zelfeffectiviteit, ernst en responseffectiviteit waren, hoe veiliger het zelfgerapporteerde gedrag was (met uitzondering van het delen van persoonsgegevens op websites voor ernst en responseffectiviteit).

Voor *kwetsbaarheid* waren er minder duidelijke relaties. Er was een onverwachte, positieve correlatie met deelname aan de verloting. Deelnemers die dachten dat negatieve gevolgen van online delen van persoonsgegevens hen kunnen overkomen, namen *vaker* deel aan de verloting, en gedroegen zich hiermee *onveiliger* op het gebied van het online delen van persoonsgegevens. Daarnaast was er een verwachte, positieve correlatie met het zelfgerapporteerde onderscheid maken tussen welke gegevens deelnemers wel en niet online delen. Deelnemers die inschatten dat negatieve gevolgen van het online delen van persoonsgegevens hen kunnen overkomen, maken naar eigen zeggen vaker onderscheid tussen welke persoonsgegevens ze wel en niet op sociale media en websites delen.

Voor *verantwoordelijkheid zelf* waren er minder duidelijke relaties. Er was een onverwachte, positieve correlatie met gedrag: hoe meer deelnemers zichzelf verantwoordelijk voelden voor het veilig online delen van persoonsgegevens, hoe *vaker* ze deelnamen aan de verloting van de prijs, en hoe *onveiliger* ze zich hiermee gedroegen op het gebied van het online delen van persoonsgegevens.

We gaan in Sectie 2.2.2.6 dieper in op dit onverwachte resultaat. De relaties op het zelfgerapporteerde gedrag waren wel zoals verwacht: hoe meer deelnemers zichzelf verantwoordelijk voelden voor het veilig online delen van persoonsgegevens, hoe minder ze aangaven dat ze persoonsgegevens op sociale media delen, en hoe meer ze aangaven de veiligheid van websites te controleren en te kijken of het nodig is om persoonlijke gegevens te delen. Voor *verantwoordelijkheid anderen* was er alleen een negatieve correlatie met gedeelde persoonsgegevens: hoe meer deelnemers de verantwoordelijk voor veilig online gedrag bij anderen legden, hoe meer niet-verplichte gegevens ze deelden.

Het is opvallend dat er minder correlaties waren tussen de psychologische factoren en het delen van persoonsgegevens op websites in vergelijking met het delen van persoonsgegevens op sociale media (zelfrapportage gedrag). Dit suggereert dat gedrag mogelijk afhangt van de context; in dit geval of het gedrag plaatsvindt in de context van het delen van persoonsgegevens op een website of in de context van sociale media. Een verklaring kan zijn dat mensen minder controle hebben op het delen van persoonsgegevens op websites, waar delen soms verplicht is of zo wordt gezien (zie ook Sectie 2.2.2.3 over verantwoordelijkheid).

Tabel 12

Correlaties veilig online delen van persoonsgegevens (gedragsmaat, zelfrapportage gedrag) en psychologische factoren

Psychologische factoren	Gedragsmaat		Zelfrapportage				
	Deelname aan verloting (0 = “Nee”, 1 = "Ja”)[a]	Gedeelde persoons-gegevens (0 = Alleen 2 verplichte gegevens, 1 = Ook 1-5 niet-verplichte gegevens)[b, c]	Ik deel mijn persoons-gegevens op websites	Ik deel mijn persoons-gegevens op sociale media	Voor ik mijn persoons-gegevens invul op een website, kijk ik eerst of deze website veilig is	Voor ik mijn persoons-gegevens invul op een website, kijk ik of dat echt nodig is	Ik maak onderscheid tussen welke persoons-gegevens ik wel of niet deel op een website of sociale media
Responskosten (schaal, 3 stellingen, α = .79)	.03	.04	.12**	.10**	-.13**	-.15**	-.16**
Zelfeffectiviteit (schaal, 3 stellingen, α = .80, omgescoord)	-.00	-.06	-.10**	-.18**	.19**	.23**	.26**
Ernst	.06	.03	-.04	-.21**	.18**	.23**	.24**
Kwetsbaarheid	.06*	.02	.03	-.05	-.01	.03	.07*
Responseffectiviteit	.04	.04	-.02	-.18**	.17**	.20**	.23**
Verantwoordelijkheid							
Eigen	.10**	.04	.01	-.16**	.12**	.16**	.20**
Anderen (schaal, 2 stellingen, r = .62, p < .001)	.00	-.07*	.001	.04	.05	.01	-.01

Noot. N = 998. Antwoordschaal psychologische factoren: 5-puntsschaal (1 = *helemaal mee oneens*, 2 = *enigszins mee oneens,* 3 = *niet mee oneens maar ook niet mee eens*, 4 = *enigszins mee eens*, 5 = *helemaal mee eens*).

Hogere scores geven, respectievelijk, hogere waargenomen responskosten, ernst, zelfeffectiviteit, kwetsbaarheid, responseffectiviteit en verantwoordelijkheid weer (zelfeffectiviteit antwoorden zijn omgecodeerd). Voor de volledige vragen, zie Tabel 11.

Niet in tabel: De gedragsmaat deelname aan de verloting correleerde, zoals verwacht, positief met “Ik deel mijn persoonsgegevens op websites” (r_{pb} = .12, p < .001). Dit betekent dat deelnemers die deelnamen aan de verloting (iets) vaker aangaven persoonsgegevens te delen op websites. Ook correleerde deze gedragsmaat onverwacht positief met “Ik maak onderscheid tussen welke persoonsgegevens ik wel of niet deel op een website of sociale media” (r_b = .08, p = .010). Dit betekent dat deelnemers die deelnamen aan de verloting (iets) *vaker* aangaven onderscheid te maken tussen welke persoonsgegevens ze deelden. Er waren geen significante correlaties tussen de gedragsmaat gedeelde persoonsgegevens en de zelfrapportage van gedrag.

[a] Punt-biseriële correlaties. [b] Biseriële correlaties. [c] Alleen deelnemers die hebben meegedaan aan de verloting en niet op annuleren hebben geklikt zijn meegenomen in de analyse, N = 803.

* p < .05, ** p ≤ .01.

We hebben vervolgens regressieanalyses uitgevoerd op het veilig online delen van persoonsgegevens (gedragsmaten, zelfrapportage gedrag) met de volgende voorspellende variabelen: psychologische factoren, socio-demografische variabelen (geslacht, leeftijd en hoogst afgeronde opleiding), en eerder slachtofferschap. De resultaten worden weergegeven in Tabel 13.

Met betrekking tot de psychologische factoren lieten de resultaten zien dat met name ernst en zelfeffectiviteit een rol spelen bij het veilig online delen van persoonsgegevens. Ernst was een significante voorspeller van het zelfgerapporteerde gedrag: hoe hoger de waargenomen ernst van de risico's van het onveilig online delen van persoonsgegevens, hoe meer deelnemers aangaven te kijken of websites wel veilig zijn, of het delen van persoonsgegevens echt nodig is, en hoe minder deelnemers aangaven persoonsgegevens te delen op sociale media. Ook zelfeffectiviteit was een significante voorspeller van het zelfgerapporteerde gedrag: hoe hoger de geschatte zelfeffectiviteit, hoe veiliger deelnemers aangaven zich te gedragen op het gebied van het online delen van persoonsgegevens. Responseffectiviteit en verantwoordelijkheid (anderen) voorspelden beperkt het veilig online delen van persoonsgegevens. Hoe hoger de waargenomen responseffectiviteit, hoe meer deelnemers aangaven te kijken of een website veilig is en of het delen van persoonsgegevens echt nodig is. In het geval van verantwoordelijkheid (ander) was er een verband in een onverwachte richting: hoe meer de verantwoordelijkheid bij anderen werd gelegd hoe *meer* deelnemers aangaven te kijken of een website veilig is en of het delen van persoonsgegevens echt nodig is.

Met betrekking tot de socio-demografische variabelen zagen we dat geslacht een significante voorspeller was van zelfgerapporteerd gedrag. Vrouwen geven aan minder persoonsgegevens op sociale media te delen dan mannen en meer te bekijken of het delen van persoonsgegevens echt nodig is. Opleidingsniveau speelde ook een rol bij een deel van de zelfrapportage maten. Een hoog vs. midden opleidingsniveau, hing samen met het minder delen van niet-verplichte gegevens op de gedragsmaat, en bij zelfgerapporteerd gedrag hing het samen met meer kijken of het delen van gegevens echt nodig is. Een hoog opleidingsniveau hing echter ook samen met *meer* gedeelde persoonsgegevens op websites op de zelfrapportage maat. Het is dus onduidelijk of een hoge opleiding samenhangt met het veiliger online delen van persoonsgegevens. Voor leeftijd zagen we dat een hogere leeftijd *positief* samenhing met veiliger zelfgerapporteerd gedrag, maar *negatief* samenhing met veilige geobserveerd gedrag. Dus, hoe hoger de leeftijd, hoe veiliger het zelfgerapporteerde gedrag, maar hoe onveiliger het geobserveerde gedrag op het gebied van het online delen van persoonsgegevens. Eerder slachtofferschap was beperkt een voorspeller van het veilig online delen van persoonsgegevens.

Tabel 13

Regressies veilig online delen persoonsgegevens (gedragsmaten, zelfrapportage gedrag)

Voorspellers	Gedragsmaten *B* (*SE*) β		Zelfrapportage gedrag *B* (*SE*) β			
	Deelname aan verloting (0 = "Nee", 1 = "Ja")	Gedeelde persoonsgegevens (0 = alleen 2 verplichte gegevens, 1 = ook 1-5 niet-verplichte gegevens) [b]	Ik deel mijn persoonsgegevens op websites	Ik deel mijn persoonsgegevens op sociale media	Voor ik mijn persoonsgegevens invul op een website, kijk ik eerst of deze website veilig is	Voor ik mijn persoonsgegevens s invul op een website, kijk ik of dat echt nodig is
Constante	-0.43 (1.03)	1.35 (1.74)	3.07 (0.37)**	3.80 (0.30)**	1.13 (0.43)**	1.00 (0.36)*
Responskosten (schaal, 3 stellingen, α = .79)	0.14 (0.12)	0.15 (0.21)	0.07 (0.04) .08	-0.04 (0.03) -.05	-0.02 (0.05) -.02	0.01 (0.04) .01
Zelfeffectiviteit (schaal, 3 stellingen, omgecodeerd, α = .80)	0.02 (0.13)	0.15 (0.21)	-0.10 (0.04)* -.11*	-0.19 (0.04)** -.24*	0.18 (0.05)** .17**	0.23 (0.04)** .24**
Ernst	0.05 (0.14)	0.04 (0.22)	-0.04 (0.05) -.03	-0.12 (0.04)** -.11**	0.22 (0.06)** .14**	0.21 (0.05)** .16**
Kwetsbaarheid	0.10 (0.10)	-0.10 (0.17)	-0.01 (0.04)	-0.02 (0.03)	-0.01 (0.04)	0.02 (0.04)

			-.01	-.03	-.01	.02
Responseffectiviteit	-0.05 (0.12)	-0.02 (0.18)	0.01 (0.04) .01	-0.05 (0.03) -.05	0.11 (0.05)* .08*	0.09 (0.04)* .08*
Verantwoordelijkheid						
Eigen	0.16 (0.12)	0.18 (0.20)	0.09 (0.04) .07	-0.03 (0.04) -.03	0.01 (.05) .00	0.00 (0.04) .00
Anderen (schaal, 2 stellingen, r = .62, p < .001)	0.02 (0.08)	-0.25 (0.14)	-0.04 (0.03) -.04	0.00 (0.02) .00	0.11 (.03)** .11**	0.06 (0.03)* .07*
Leeftijd	0.00 (0.01)	0.04 (0.01)**	-0.01 (0.00)** -.18**	-0.01 (0.00)** -.16**	0.01 (.00)** .10**	0.01 (0.00)** 0.18**
Vrouw[c]	0.07 (0.18)	-0.15 (0.29)	-0.01 (0.06) -.00	-0.21 (0.05)** -.13**	-0.04 (.07) -.02	0.16 (0.06)** .08**
Opleidingsniveau[d]						
Laag	0.33 (0.27)	0.61 (0.65)	-0.13 (0.09) -.05	-0.03 (0.07) -.02	0.11 (0.10) .04	0.04 (0.09) .02
Hoog	0.14 (0.19)	-0.72 (0.31)*	0.18 (0.07)* .09*	-0.05 (0.06) -.03	-0.05 (0.08) -.02	0.17 (0.07)** .09**
Eerder slachtofferschap[e]						
Ja, korter dan 12 maanden geleden	0.35 (0.40)	1.59 (1.03)	0.00 (0.13) .00	0.21 (0.10) .06	-0.28 (0.15) -.06	-0.30 (0.12)* -.08*

Ja, langer dan 12 maanden geleden	-0.11 (0.27)	-0.41 (0.40)	0.16 (0.10) .05	0.10 (0.08) .04	-0.13 (0.12) -.04	0.01 (0.10) .00
Adjusted R^2	0.02[a]	0.16 [a]	.07	.11	.09	.14
N	923	750	923	923	923	923

Noot. N is kleiner dan 998 door missing values bij variabelen leeftijd, geslacht, opleidingsniveau en eerder slachtofferschap, en bij de gedragsmaat voor het aantal gedeelde persoonsgegevens. Antwoordschaal stellingen psychologische factoren: 5-puntsschaal (1 = *helemaal mee oneens*, 2 = *enigszins mee oneens*, 3 = *niet mee oneens maar ook niet mee eens*, 4 = *enigszins mee eens*, 5 = *helemaal mee eens*). Voor de volledige vragen, zie Tabel 11. Voor de analyses is gebruik gemaakt van multipele regressie, en in het geval van de gedragsmaten logistische regressie met een binaire uitkomstvariabele.

[a] Nagelkerke R square. [b] Alleen deelnemers die hebben meegedaan aan de verloting en niet op annuleren hebben geklikt zijn meegenomen in de analyse. Drie datapunten zijn als outliers gemarkeerd en niet meegenomen in de analyse. [c] Dummy-variabele met 0 = man en 1= vrouw. [d] Dummyvariabelen met 0 = opleidingsniveau midden en respectievelijk 1 = opleidingsniveau laag en 1 = opleidingsniveau hoog. [e] Dummy-variabelen met 0 = Geen eerder slachtofferschap en respectievelijk 1 = Eerder slachtofferschap in de afgelopen 12 maanden en 1 =Eerder slachtofferschap langer dan 12 maanden geleden.

* $p < .05$, ** $p < .01$

2.2.2.5 Belemmerende en bevorderende factoren

Voordat de deelnemers de stellingen over de psychologische factoren beantwoordden, stelden we hen twee open vragen naar factoren die hen belemmeren en bevorderen om online veiliger om te gaan met persoonsgegevens. Hierbij kregen zij uitleg over wat wordt verstaan onder het veilig online omgaan met persoonsgegevens voor ze de vragen beantwoordden.

Om de antwoorden te analyseren zijn op dezelfde manier als bij wachtwoorden codeerschema's gemaakt (zie Sectie 2.2.1.5). We beschrijven hier de hoofdlijnen van de bevindingen uit de open vragen (*N* = 998, 1083 coderingen voor de belemmerende factoren; *N* = 998, 1076 coderingen voor de bevorderende factoren).

Belemmerende factoren

Over het algemeen bleek dat deelnemers op de vraag over de belemmerende factoren minder samenhangende antwoorden gaven dan op de vraag over bevorderende factoren. Mogelijk werd de vraag verkeerd geïnterpreteerd. De meeste antwoorden vielen dan ook in de antwoordcategorie "Overig" (61.8%). Daarnaast gaf een deel van de deelnemers aan responskosten als een belemmerende factor te zien (18.3% van de antwoorden). Hierbij gaven deelnemers onder andere aan dat het veel tijd en/of moeite kost om online veilig om te gaan met persoonsgegevens. Voorbeelden van antwoorden waren "Weinig tijd dus niet checken", "Je neemt er niet altijd de tijd voor, het zou makkelijker moeten", en "Allemaal te veel gedoe". Ten slotte gaf een deel van de deelnemers aan belemmeringen met betrekking tot zelfeffectiviteit te ervaren (10.0% van de antwoorden). Zo vonden zij het moeilijk in te schatten wanneer een site betrouwbaar is of dachten zij dat het noodzakelijk/verplicht is om een account aan te maken of gegevens te delen. Voorbeelden van antwoorden waren "Het is soms lastig om onveilige situaties te herkennen doordat oplichters steeds professioneler te werk gaan", en "Soms zijn het verplichte velden en kun je er niet omheen".

Bevorderende factoren

Op de vraag "Wat zou u kunnen helpen om online veiliger om te gaan met persoonsgegevens?" viel 16.7% van antwoorden van de deelnemers in de codeercategorie "Verantwoordelijkheid". Deelnemers gaven aan dat websites zowel minder om persoonsgegevens zouden moeten vragen als mensen erop zouden moeten attenderen wanneer vragen niet verplicht zijn om in te vullen. Voorbeelden van antwoorden waren "Dat ze om minder vragen en het verbieden door de overheid", "Als je er nog meer op geattendeerd zou worden", en "Duidelijker aangeven wat niet verplicht is". Verder viel 9.8% van de antwoorden van de deelnemers in de codeercategorie "Techniek". Deelnemers gaven aan dat bijvoorbeeld een extra beveiligingsprogramma of een tweestapsverificatie hen zou helpen om online veiliger om te gaan met hun persoonsgegevens. Voorbeelden van antwoorden waren "Als er meer veiligheidsstappen zijn zoals een sms code sturen", en "Dubbele verificatie". Ten slotte, viel een groot deel van de antwoorden in de categorie "Overig" (48.2%).

Net als de resultaten beschreven in Sectie 2.2.2.3, lijken responskosten en zelfeffectiviteit belangrijke belemmerende factoren bij de beslissing om veilig online persoonsgegevens te delen. Ook bleek voor verantwoordelijkheid, net zoals bij de resultaten in Sectie 2.2.2.3, dat deelnemers de verantwoordelijkheid voor het veilig online delen van persoonsgegevens deels bij anderen (websites, apps, overheid) leggen.

2.2.2.6 Samenvatting resultaten persoonsgegevens

Studie 1 lieten zien dat deelnemers hun gedrag op het vlak van het online delen van persoonsgegevens veelal als veilig inschatten. De gedragsmaat liet echter een ander beeld zien. De meerderheid van de deelnemers nam deel aan een winactie waar persoonsgegevens gedeeld moesten worden, en de meerderheid van de deelnemers aan de winactie deelde alle persoonsgegevens (inclusief niet-verplichte, gevoelige gegevens).

Als belangrijke belemmerende factor voor het veilig online delen van persoonsgegevens kwam, net als bij veilig wachtwoordgedrag, zelfeffectiviteit naar voren: deelnemers achtten zichzelf beperkt in staat online veilig om te gaan met hun persoonsgegevens. De resultaten lieten ook relaties in de verwachte richting tussen zelfeffectiviteit en het veilig online delen van persoonsgegevens zien: hoe hoger de waargenomen zelfeffectiviteit, hoe veiliger het zelfgerapporteerde gedrag. Naast zelfeffectiviteit kwam, net als bij veilig wachtwoordgedrag, ernst ook naar voren als een belangrijke voorspeller van het veilig online delen van persoonsgegevens: deelnemers erkenden de ernst van de risico's van het onveilig online delen van persoonsgegevens, en hoe meer deelnemers de gevolgen als ernstig zagen, hoe veiliger hun zelfgerapporteerde gedrag was. Verder leek verantwoordelijkheid een rol te spelen in veilig online delen van persoonsgegevens en kan hier ook een link gemaakt worden met zelfeffectiviteit: deelnemers gaven aan dat de verantwoordelijkheid voor het veilig online delen van persoonsgegevens niet alleen bij henzelf ligt, maar ook bij anderen (websites, apps, overheid) en voelden zich verplicht om gegevens te delen. Wat opviel was dat deelnemers die zich persoonlijk verantwoordelijk voelden voor het online veilig delen van persoonsgegevens, juist vaker deelnamen aan de verloting van de prijs, en hiermee er vaker voor kozen om hun persoonsgegevens te delen. Een verklaring voor dit onverwachte resultaat kan zijn dat de vraag over verantwoordelijkheid volgde op de gedragsmaat. Wellicht leidde de deelname aan de verloting eerder in het onderzoek, een keuze een keuze die de deelnemer zelf had gemaakt, later in het onderzoek tot de conclusie zelf verantwoordelijk te zijn voor het veilig online delen van persoonsgegevens. Het kan zijn dat wanneer deelnemers eerst de verantwoordelijkheid vraag in hadden gevuld en pas daarna de keuze kregen om mee te doen aan de verloting, dat de verwachte negatieve relatie tussen persoonlijk verantwoordelijk voelen voor het veilig online delen van persoonsgegevens en deelname aan de verloting van de prijs was gevonden. Ten slotte, anders dan bij veilig wachtwoordgedrag, leken responskosten een beperkte rol te spelen bij het veilig online delen van persoonsgegevens.

Socio-demografische variabelen lijken een grotere rol te spelen bij het veilig online delen van persoonsgegevens vergeleken met veilig wachtwoordgedrag. Oudere deelnemers gaven aan zich

veiliger te gedragen, maar de resultaten op de gedragsmaat wezen erop dat oudere deelnemers *meer* persoonsgegevens deelden en zich hiermee *onveiliger* gedroegen. Daarnaast gaven vrouwen in de zelfrapportage aan zich wat veiliger te gedragen dan mannen. Voor opleiding zagen we verschillen tussen hoogopgeleide deelnemers en middelopgeleide deelnemers, maar de resultaten waren hier niet helemaal consistent; hoogopgeleide deelnemers toonden veiliger gedrag, maar de zelfrapportage van gedrag liet een wisselend patroon zien. Eerder slachtofferschap van cybercriminaliteit was beperkt een voorspeller van het veilig online delen van persoonsgegevens.

3. Studie 2

In Studie 2 hebben we getoetst of het verhogen de *ernst van de risico's van onveilig gedrag* en de *zelfeffectiviteit van veilig gedrag* tot veiliger online gedrag leidt, voor zowel wachtwoorden (Studie 2a) als persoonsgegevens (Studie 2b). Deze keuze voor ernst en zelfeffectiviteit is gebaseerd op de bevindingen in Studie 1. In Studie 1 zagen we zien dat de risico's van onveilig online gedrag als ernstig werden beoordeeld en dat ernst (deels) een positieve relatie had met (zelfgerapporteerd en geobserveerd) veilig gedrag. Daarnaast zagen we in Studie 1 dat dat zelfeffectiviteit een belangrijke belemmerende factor was voor veilig gedrag, en een positieve relatie had met (zelf gerapporteerd/geobserveerd) veilig gedrag. We vonden dit patroon voor zowel wachtwoorden als persoonsgegevens.

Deze combinatie tussen ernst van risico's en zelfeffectiviteit komt bovendien veel terug in onderzoek naar gedragsverandering (bv. in gezondheidscommunicatie; Kok et al., 2018; Peters et al., 2012; Ruiter et al., 2001; Tannenbaum et al., 2015; Witte & Allen, 2000). Het communiceren van risico's of gevaar blijkt vooral effectief bij gedragingen waar risico's nog niet volledig duidelijk zijn (Kok et al., 2018). Dit past goed bij ons doelgedrag, omdat studies laten zien dat de risico's in de context van online privacy (Cho et al., 2010; Debatin et al., 2009) en onveilige wachtwoorden (Tam et al., 2010) niet altijd goed worden ingeschat. Daarnaast blijkt voor gedragsverandering de combinatie met informatie over zelfeffectiviteit essentieel. Met informatie over zelfeffectiviteit weten mensen hoe ze de risico's kunnen voorkomen (Kok et al., 2018). Ze worden dus niet enkel gewaarschuwd, maar weten nu ook wat ze zelf kunnen doen (Kok et al., 2018; zie ook Bigsby & Albarracín, 2022; Peters et al., 2018).

Recente studies in de context van cyberveiligheid ondersteunen het idee dat veilig gedrag kan worden bevorderd door het communiceren van informatie over risico's en zelfeffectiviteit. Een studie met een (experimenteel nagemaakte) online webshop liet bijvoorbeeld zien dat het communiceren van risico's van onveilig gedrag resulteerde in veiliger online gedrag (bv. sterkere wachtwoorden, kiezen voor veiligere verbindingen; zie ook Jenkins et al., 2014), en dan vooral wanneer deze risico's werden gecombineerd met informatie over hoe veilig gedrag eruitziet (Van Bavel et al., 2019). Een studie in de context van wachtwoordgedrag liet een vergelijkbaar effect zien, waarbij de combinatie tussen informatie over risico's en zelfeffectiviteit resulteerde in de sterkste intenties voor veilig wachtwoordgedrag (Dupuis et al., 2021; zie ook Dupuis & Renaud, 2021). Het communiceren van risico's zou veilig online gedrag dus kunnen bevorderen en dan vooral wanneer het wordt gecombineerd met informatie over hoe veilig gedrag eruitziet.

Onze interventie bestond daarom uit het communiceren van risico's van onveilig gedrag (ernst), hoe veilig gedrag uitgevoerd kan worden (zelfeffectiviteit), of een combinatie van beide. In de communicatie van de risico's werden de gevolgen van onveilig gedrag als gevaarlijk beschreven en vervolgens gaven we concrete risico's om het mogelijke gevaar dichterbij te brengen (Scheutz et al., 2020). Daarbij spraken we de lezer direct aan, om persoonlijke relevantie te verhogen (Ruiter et al., 2001). De risico's van onveilig gedrag zijn gekozen op basis van literatuur over online gevaren en

angsten (Brands & Wilsem, 2021; Hille et al., 2015; Elhai & Hall, 2016; De Kimpe et al. 2021). Hieruit blijkt dat mensen onder meer bang zijn voor hackers en dat vreemden toegang krijgen tot persoonlijke informatie (bv. e-mail of bankgegevens).

In de communicatie over zelfeffectiviteit gaven we concrete voorbeelden van hoe het veilige gedrag eruitziet, met een nadruk op uitvoerbaarheid (bv. “Dat doet u zo”). Voor *wachtwoorden* richtten we ons op de samenstelling van een veilig wachtwoord en daarmee dus op de zelfeffectiviteit voor het *maken* van wachtwoorden. Dit is relevant omdat Studie 1 liet zien dat de kwaliteit van de wachtwoorden die mensen gebruiken laag is. We richten ons dus niet op het onthouden van (meerdere) wachtwoorden. Hoewel Studie 1 liet zien dat deelnemers hier duidelijk problemen ervaren, nemen we dit niet op in de interventie omdat dit binnen de huidige studiecontext lastig te onderzoeken was. Voor *persoonsgegevens* richtten we ons met de zelfeffectiviteit op concrete stappen hoe veilig online delen van persoonsgegevens eruitziet (i.e., een moment nemen om te beoordelen of het nodig is en veilig kan; zie ook Veiliginternetten, z.d.). Zie Sectie 3.1.3 voor de specifieke uitwerking van de interventie bij wachtwoorden en bij persoonsgegevens.

3.1 Methode

Studie 2 is opgezet en ontworpen door de onderzoekers van het Kenniscentrum voor Psychologie en Economisch Gedrag. Het KCPEG is verbonden aan de Sectie Sociale, Economische en Organisatiepsychologie van de Universiteit Leiden. Onderzoeksbureau Markteffect heeft de studie vervolgens geprogrammeerd en de deelnemers geselecteerd en geworven. Ook de kwaliteitsanalyse van de data is verzorgd door Markteffect. Onderzoekers van KCPEG waren verantwoordelijk voor de data-analyse en rapportage. De dataverzameling heeft plaatsgevonden in de periode van 14 april t/m 28 april 2022.

3.1.1 Deelnemers

Werving van deelnemers

De deelnemers werden op dezelfde manier geworven als in Studie 1, met als aanvullend wervingscriterium dat deelnemers aan Studie 2 niet deelgenomen hadden aan Studie 1. Het doel was een steekproef van 2000 deelnemers, representatief voor de Nederlandse bevolking op geslacht, leeftijd (18+), opleiding en regio. Toen ongeveer 75% van de dataverzameling compleet was, bleek dat het aantal deelnemers met een laag opleidingsniveau en het aantal deelnemers jonger dan 35 jaar iets achterbleef. Omdat dit niet volledig kon worden gecorrigeerd binnen de beoogde 2000 deelnemers hebben we het doel van representativiteit deels losgelaten.

Screening van de data

De kwaliteit van de data is door onderzoeksbureau Markteffect op dezelfde manier gecontroleerd als in Studie 1. Van de 2189 deelnemers werden 102 deelnemers verwijderd op grond van de criteria

dubbele personen, speeders, straightliners, en/of toetsenrammelaars (zie Studie 1 voor meer informatie), 2087 deelnemers werden behouden in de dataset.

De achtergrondkenmerken van de 2087 deelnemers zijn uiteengezet in Tabel 14 en vergeleken met de Nederlandse bevolking (CBS, 2021a). De steekproef is representatief voor de Nederlandse bevolking qua geslacht, regio en leeftijd. De steekproef wijkt iets af qua opleidingsniveau vergeleken met de Nederlandse bevolking. Zo hebben deelnemers vaker een gemiddeld (42.3 vs. 36.5) of hoog opleidingsniveau (39.4% vs. 34.8%) en hebben ze minder vaak een laag opleidingsniveau (16.8% vs. 28.8%).

Naast de socio-demografische variabelen is ook eerder slachtofferschap van internetcriminaliteit gemeten en uiteengezet in Tabel 14. Van de deelnemers aan het onderzoek is 17.5% (17.2% Studie 2a, 17.7% Studie 2b) wel eens slachtoffer geweest van internetcriminaliteit.

Tabel 14

Achtergrondkenmerken deelnemers in vergelijking met Nederlandse bevolking van 18+ naar data van het CBS (2021a)

	Deelnemers Studie 2a (wachtwoorden) *N* = 1075		Deelnemers Studie 2b (persoonsgegevens) *N* = 1012		Nederlandse bevolking
	N	%	*N*	%	%
Geslacht					
Man	505	47.0	489	48.3	49.7
Vrouw	563	52.4	519	51.3	50.3
Anders	3	0.3	2	0.2	
Wil ik liever niet zeggen	4	0.4	2	0.2	
Opleidingsniveau[a]					
Laag	160	14.9	170	16.8	28.8
Midden	416	38.7	428	42.3	36.5
Hoog	486	45.2	399	39.4	34.8
Anders	7	0.7	6	0.6	
Wil ik liever niet zeggen	6	0.6	9	0.9	
Regio					
West (UT, NH, ZH)	449	41.8	410	40.5	45.6
Noord (GR, FR, DR)	116	10.8	130	12.8	9.9
Oost (OV, GD, FL)	246	22.9	231	22.8	21.1
Zuid (ZL, NB, LB)	262	24.4	240	23.7	23.3
Anders[b]	2	0.2	1	0.1	
Leeftijd					
18 t/m 24	58	5.4	44	4.3	10.9
25 t/m 34	175	16.3	150	14.8	15.9
35 t/m 44	194	18.0	162	16.0	14.7
45 t/m 54	214	19.9	201	19.9	17.0
55 t/m 65	220	20.5	219	21.6	16.9
65+	205	19.1	225	22.2	24.6
Wil ik liever niet zeggen	9	0.8	11	1.1	
Eerder slachtofferschap van internetcriminaliteit					
Ja, in de afgelopen 12 maanden	56	5.2	54	5.3	
Ja, langer geleden dan 12 maanden	131	12.2	125	12.4	

Nee	830	77.2	764	75.5
Weet ik niet	58	5.4	69	6.8

Noot. [a] Hoogst afgeronde opleiding: laag (geen onderwijs, basisonderwijs, LBO/VBO/VMBO/MBO-1), midden (MBO 2/3/4, HAVO, VWO), hoog (HBO, WO). [b] Deelnemers in de categorie "Anders" vulden een onbekende postcode in.

3.1.2 Onderzoeksopzet en procedure

Aan het begin van de studie kregen deelnemers informatie over het onderzoek en gaven zij toestemming voor deelname. Daarna werden deelnemers random toegewezen aan de experimentele studie over wachtwoorden (Studie 2a) of de experimentele studie over het online delen van persoonsgegevens (Studie 2b) en aan één van de vier interventiecondities: ernst, zelfeffectiviteit, ernst + zelfeffectiviteit, controle conditie. Zie Sectie 3.1.3 voor nadere toelichting van de interventie condities. Vervolgens beantwoordden de deelnemers vragen in de vragenlijst.

Iedere deelnemer ontving na het afronden van de studie punten, welke vervolgens konden worden ingewisseld voor geld of producten. Daarnaast werd een cadeaubon van 100 euro verloot onder alle deelnemers die aangaven mee te willen doen aan de verloting. Het meedoen aan de verloting (ofwel winactie) en het daarbij invullen van persoonsgegevens was de gedragsmaat voor het veilig online delen van persoonsgegevens in ons onderzoek (zie Sectie 2.1.4 voor meer details). Aan het eind van het onderzoek werden deelnemers bedankt en kregen ze meer informatie over het doel van het onderzoek en over de interventie (debriefing). Na afloop van het onderzoek ontvingen de deelnemers de toegezegde punten voor deelname aan het onderzoek en vond de verloting van de tegoedbon ter waarde van 100 euro plaats.

Tabel 15 geeft de opbouw van de studie weer, inclusief de vragen die zijn gesteld aan de deelnemers. Voor de leesbaarheid van het rapport presenteren we de meest relevante resultaten (aangegeven met het groene vinkje in Tabel 15). De resultaten voor vragen over wachtwoordmanagers zijn opgenomen in Bijlage D (aangegeven met een B in Tabel 15). Voor de overige resultaten en materialen verwijzen we naar de onderzoekdocumentatie behorende bij Studie 2 die hier te vinden is: https://easy.dans.knaw.nl/ui/home.

Tabel 15

Opbouw interventiestudie (Studie 2a wachtwoorden, Studie 2b persoonsgegevens)

	Blok	Vragen	Gerapporteerd
1	Informatiebrief, informed consent en leeftijd	Informed consent	✓
		Leeftijd	✓
2	Interventie	Informatie afhankelijk van conditie:	
		- Ernst	✓
		- Zelfeffectiviteit	✓
		- Ernst + zelfeffectiviteit	✓
		- Controle conditie	✓
3	Gedragsmaten	2a: Entropie wachtwoord	✓
		2b: Delen persoonsgegevens	✓
4	Interventie checks	Zelfeffectiviteit	✓
		Ernst	✓
5	Overige vragen	Kwetsbaarheid	✓
		Ernst specifieke risico's	✓
		Responseffectiviteit	✓
		Beoordeling eigen gedrag	X
		Gedragsintentie	X
		2a: Kennis wachtwoordmanager	B
		2a: Gebruik wachtwoordmanager	B
		2a: Intentie wachtwoordmanager	B
		2a: Aangemaakt wachtwoord: zoals normaal	✓
		2a: Aangemaakt wachtwoord: persoonlijke informatie	✓
		2a: Aangemaakt wachtwoord: hergebruik	✓
		2a: Aangemaakt wachtwoord: gebruik wachtwoordmanager	✓
		2a: Verloting prijs	X
		2b: Persoonsgegevens: zoals normaal	X
		2b: Persoonsgegevens: echte gegevens	✓
		Geslacht	✓
		Hoogst afgeronde opleiding	✓
		Postcode (voor berekening regio)	✓
		Persoonlijke relevantie online veiligheid	X
		Eerder slachtofferschap	✓

	Vertrouwen	X
	Frequentie internetgebruik	X
	Gebruikt apparaat	X
	Opmerkingen	X
6	Debriefing	

Noot. Vragen met 2a waren onderdeel van Studie 2a over wachtwoorden, vragen met 2b waren onderdeel van Studie 2b over het online delen van persoonsgegevens; de overige vragen werden aan alle deelnemers gesteld (in zowel Studie 2a als Studie 2b).

3.1.3 Interventie

De interventie bestond uit het communiceren van risico's van onveilig gedrag (ernst), hoe veilig gedrag uitgevoerd kan worden (zelfeffectiviteit), een combinatie van beide teksten (ernst + zelfeffectiviteit), of geen communicatie (controle conditie).

3.1.3.1 Studie 2a: Interventie wachtwoorden

Ter introductie lazen alle deelnemers in Studie 2a het volgende: "We hebben tegenwoordig voor heel veel verschillende websites en apps een gebruikersaccount nodig. Bij het aanmaken van een gebruikersaccount wordt gevraagd om een gebruikersnaam en wachtwoord te kiezen. Met sterke wachtwoorden beschermt u de gegevens op uw computer, tablet en smartphone, en ook uw e-mail, sociale media, en data die opgeslagen zijn in de cloud." Vervolgens was de informatie afhankelijk van conditie.

In de ernst conditie lazen deelnemers:

Het is belangrijk dat u het volgende over wachtwoorden weet:
Als u zwakke wachtwoorden gebruikt loopt u gevaar:

- Criminelen kunnen zwakke wachtwoorden in korte tijd achterhalen
- Criminelen krijgen dan toegang tot uw accounts, e-mail, webcam, of bankrekening
- Criminelen kunnen dan bijvoorbeeld uw geld stelen. Daarnaast kunnen ze uw persoonlijke foto's en berichten delen op het internet

In de zelfeffectiviteit conditie lazen deelnemers:

Het is belangrijk dat u het volgende over wachtwoorden weet:

Sterke wachtwoorden maakt u zo:

- Sterke wachtwoorden bestaan uit minstens 12 tekens
- Sterke wachtwoorden hebben minstens één hoofdletter, één cijfer en één speciaal teken. Voorbeelden van speciale tekens zijn: @ + $ & % =
- Sterke wachtwoorden bevatten geen persoonlijke informatie. Gebruik dus geen namen, verjaardagen of adressen in uw wachtwoorden

Zo krijgt u sterke wachtwoorden die moeilijk te raden zijn!

In de ernst + zelfeffectiviteit-conditie lazen deelnemers de combinatie van beide teksten. De volgorde van de teksten werd hierbij systematisch gevarieerd. In de controle conditie werd alleen de introductietekst weergegeven

3.1.3.2 Studie 2b: Interventie persoonsgegevens

Ter introductie lazen deelnemers in Studie 2b het volgende: “Persoonsgegevens zijn alle gegevens van een persoon, zoals naam, adres, telefoonnummer, geboortedatum, bankrekeningnummer, Burgerservicenummer (BSN).” Vervolgens was de informatie afhankelijk van conditie.

In de ernst conditie lazen deelnemers:

Het is belangrijk dat u het volgende over persoonsgegevens weet:

Als u online onveilig omgaat met uw persoonsgegevens loopt u gevaar:

- Uw persoonsgegevens kunnen in handen komen van criminelen
- Criminelen kunnen geld stelen van familie en vrienden, door te doen alsof ze u zijn via WhatsApp of e-mail
- Criminelen kunnen ook uw persoonsgegevens gebruiken bij het plegen van misdrijven (zoals het downloaden van kinderporno, of grote aankopen doen zonder te betalen), waardoor de politie u als verdachte ziet

In de zelfeffectiviteit conditie lazen deelnemers:

Het is belangrijk dat u het volgende over persoonsgegevens weet:

Veilig online omgaan met uw persoonsgegevens doet u zo:

- Stap 1: Neem een moment om te kijken of de website veilig is
- Stap 2: Als u de website niet kent, ga dan op zoek naar ervaringen met de website van andere mensen (bijvoorbeeld via een zoekmachine zoals Google)
- Stap 3: Deel online alleen uw persoonsgegevens als het echt moet. Het is vaak niet verplicht om al uw persoonsgegevens te delen. De persoonsgegevens die verplicht zijn worden vaak aangegeven met een sterretje (*)

Zo gaat u online veilig om met uw persoonsgegevens!

In de ernst + zelfeffectiviteit-conditie lazen deelnemers de combinatie van beide teksten. De volgorde van de teksten werd hierbij systematisch gevarieerd. In de controle conditie werd alleen de introductietekst weergegeven.

3.1.4 Studie 2a: Meetinstrumenten wachtwoorden

3.1.4.1 Gedragsmaat en zelfrapportage gedrag

Deelnemers in Studie 2a werden gevraagd een wachtwoord aan te maken voor een gebruikersaccount, op dezelfde manier als in Studie 1 (gedragsmaat). Net als in Studie 1 richtte de gedragsmaat zich op de samenstelling (sterkte) van de aangemaakte wachtwoorden. Daarnaast is een belangrijk kenmerk van sterke wachtwoorden dat deze geen persoonlijke informatie (zoals namen, verjaardagen of adres) bevatten (Consumentenbond, 2021). Daarom vroegen we deelnemers: “Bevat het wachtwoord dat u heeft aangemaakt persoonlijke informatie? Heeft u bijvoorbeeld een naam, verjaardag of adres gebruikt in uw wachtwoord?” (Ja; Nee; Zeg ik liever niet).

3.1.4.2 Interventie checks

Na de gedragsmaat volgden de interventie checks (i.e., om na te gaan of de interventie het beoogde effect had). *Zelfeffectiviteit* werd gemeten met “Ik weet hoe ik een sterk wachtwoord kan maken” en “Ik ben in staat sterke wachtwoorden te maken”. *Ernst* werd gemeten met “Het is gevaarlijk om zwakke wachtwoorden te gebruiken”. Deze stellingen werden beantwoord op een 5-puntsschaal, van *helemaal mee oneens* tot *helemaal mee eens*.

3.1.4.3 Overige vragen

Vervolgens stelden we de deelnemers verschillende overige vragen. Tenzij anders aangegeven werden deze beantwoord op een 5-puntsschaal, van *helemaal mee oneens* tot *helemaal mee eens*. Allereerst wilden we nagaan of onze interventie ook effect hadt op kwetsbaarheid en responseffectiviteit. *Kwetsbaarheid* werd gemeten met "Als ik zwakke wachtwoorden gebruik dan kan het mij overkomen dat criminelen…", met vervolgens de risico's: "…mijn wachtwoorden achterhalen", "… toegang krijgen tot mijn accounts, e-mail, webcam, of bankrekening", "… mijn geld stelen", en "… mijn persoonlijke foto's en berichten delen op het internet". *Responseffectiviteit* werd gemeten met "Als ik sterke wachtwoorden gebruik loop ik minder risico om slachtoffer te worden van online criminaliteit".

Tot slot wilden we beter inzicht krijgen in welk type risico's vooral als ernstig worden ervaren. Daarom vroegen we deelnemers om voor specifieke risico's de ernst te rapporteren. Dit deden we met: "Ik zou het erg vinden als criminelen…" met vervolgens specifieke risico's (in random volgorde), "… toegang krijgen tot mijn accounts", "toegang krijgen tot mijn e-mail", "… toegang krijgen tot mijn webcam", "… toegang krijgen tot mijn bankrekening", "… mijn geld stelen", "… mijn persoonlijke foto's en berichten delen op het internet".

3.1.5 Studie 2b: Meetinstrumenten persoonsgegevens

3.1.5.1 Gedragsmaat en zelfrapportage gedrag

Deelnemers in Studie 2b werden gevraagd persoongegevens te delen als onderdeel van de winactie, op dezelfde manier als in Studie 1 (gedragsmaat). In aanvulling op Studie 1 bevatte het formulier dat deelnemers invulden een legenda waarin werd aangegeven dat de velden met sterretjes erachter verplichte velden betroffen. Aan het einde van de vragenlijst vroegen we de deelnemers of de gedeelde gegevens echte gegevens waren (zelfrapportage gedrag; zelfde vraag als Studie 1).

3.1.5.2 Interventie checks

Na de gedragsmaat volgden de interventie checks (i.e., om na te gaan of de interventie het beoogde effect had). *Zelfeffectiviteit* van het online veilig delen van persoonsgegevens werd gemeten met "Ik weet hoe ik online veilig om kan gaan met mijn persoonsgegevens" en "Ik ben in staat om online veilig om te gaan met mijn persoonsgegevens". *Ernst* werd gemeten met "Het is gevaarlijk om online onveilig om te gaan met mijn persoonsgegevens".

3.1.5.3 Overige vragen

Vervolgens stelden we de deelnemers verschillende overige vragen. Tenzij anders aangegeven werden deze beantwoord op een 5-puntsschaal, van *helemaal mee oneens* tot *helemaal mee eens*.

Om na te gaan of onze interventie ook effect had op kwetsbaarheid en responseffectiviteit werd *kwetsbaarheid* gemeten met "Als ik online onveilig omga met mijn persoonsgegevens dan kan het mij overkomen …" met vervolgens de risico's: "… dat mijn persoonsgegevens in handen komen van criminelen", "… dat criminelen geld stelen van familie en vrienden door te doen of ze mij zijn via Whatsapp of e-mail", en "….dat criminelen mijn persoonsgegevens gebruiken bij het plegen van misdrijven (zoals het downloaden van kinderporno, of grote aankopen doen zonder te betalen) waardoor de politie mij als verdachte ziet". *Responseffectiviteit* werd gemeten met "Als ik online veilig omga met mijn persoonsgegevens loop ik minder risico om slachtoffer te worden van online criminaliteit".

Om beter inzicht te krijgen in welk type risico's vooral als ernstig worden ervaren, vroegen we deelnemers om voor specifieke risico's de ernst te rapporteren. Dit deden we met: "Ik zou het erg vinden als..." met vervolgens specifieke risico's (in random volgorde), "… mijn persoonsgegevens in handen komen van criminelen", "… criminelen geld stelen van familie en vrienden, door te doen alsof ze mij zijn via WhatsApp of e-mail", "… criminelen mijn persoonsgegevens gebruiken bij het downloaden van kinderporno, waardoor de politie mij als verdachte ziet", "… criminelen mijn persoonsgegevens gebruiken om grote aankopen te doen zonder te betalen, waardoor de politie mij als verdachte ziet".

3.1.6 Socio-demografische gegevens en eerder slachtofferschap

Om de representativiteit van onze steekproef te kunnen controleren vroegen we deelnemers om verschillende socio-demografische gegevens te rapporteren: deelnemers werden gevraagd naar hun geslacht, leeftijd, hoogst afgeronde opleiding en de vier cijfers van hun postcode (voor de berekening van de regio waarin zijn woonachtig zijn). Slachtofferschap van internetcriminaliteit werd met dezelfde vraag als in Studie 1 gemeten.

3.1.7 Ethische toetsing

Dit onderzoek is voorgelegd aan en goedgekeurd door de Commissie Ethiek Psychologie (CEP) van het Instituut Psychologie, Universiteit Leiden (CEP 2022-04-11-E. ter Mors-V3-3942). Voor Studie 2 gelden dezelfde richtlijnen en overwegingen als in Studie 1 (zie Sectie 2.1.6). De reden om op het einde van Studie 2a de wachtwoorden deelnemers ook de mogelijkheid te geven om deel te nemen aan de verloting (winactie) is dat toewijzing aan condities random was, en we alle deelnemers de mogelijkheid wilden bieden om de tegoedbon te winnen.

3.2 Resultaten

In deze sectie beschrijven we de resultaten van Studie 2. De resultaten geven inzicht in of het verhogen van de *ernst van de risico's van onveilig gedrag* en/of de *zelfeffectiviteit van veilig gedrag*

tot veiliger gedrag leidt, voor zowel wachtwoorden (Studie 2a) als persoonsgegevens (Studie 2b). Ook geven de resultaten inzicht in of de effectiviteit van deze interventie verschillend of hetzelfde is voor verschillende groepen in de samenleving.

3.2.1 Studie 2a Wachtwoorden

We richtten ons in de analyses op de wachtwoorden resultaten voor de totale steekproef (*N* = 1075). Voor we deze resultaten bespreken is het relevant om te vermelden dat een deel van de deelnemers (13.8% controle conditie, 16.4% ernst conditie, 17.1% zelfeffectiviteit conditie, 18.8% ernst + zelfeffectiviteit conditie) aangaf een wachtwoordmanager te hebben gebruikt bij het aanmaken van het wachtwoord. In Bijlage C geven we weer hoe dit de resultaten in Sectie 3.2.1.1 (gedragsmaat en zelfrapportage gedrag) heeft beïnvloed. We hebben er net als in Studie 1 voor gekozen om deze deelnemers niet uit te sluiten in de analyses, omdat het gebruik van een wachtwoordmanager een goede strategie is voor het maken van een sterk en uniek wachtwoord. Ook wezen de data erop dat niet alle deelnemers die aangaven een wachtwoordmanager te hebben gebruikt dit daadwerkelijk gedaan hebben (zie uitleg in Bijlage C).

3.2.1.1 Gedragsmaat en zelfrapportage gedrag

De resultaten voor de sterkte en kenmerken van de aangemaakte wachtwoorden zijn weergegeven in Tabel 16. De entropie van het wachtwoord geeft de sterkte van het wachtwoord aan. De entropie wordt berekend op basis van de lengte en de samenstelling van het wachtwoord (zie Sectie 2.1.3).

Net zoals in Studie 1 (zie ook Sectie 2.2.1.1) was het aangemaakte wachtwoord bij deelnemers die een account aanmaakten zonder informatie te ontvangen over de ernst van risico's en/of zelfeffectiviteit met een gemiddelde entropiewaarde van 58.62 zeer zwak. Het geven van informatie over de ernst van risico's van onveilig gedrag en/of zelfeffectiviteit van veilig gedrag in de interventie condities leidde tot een significante toename in de entropie van aangemaakte wachtwoorden vergeleken met de controle conditie (zie Tabel 16). Deelnemers die informatie over de ernst van risico's en/of zelfeffectiviteit hadden gekregen maakten sterkere wachtwoorden aan dan deelnemers die deze informatie niet hadden gekregen. De wachtwoorden van deze deelnemers waren over de hele linie genomen langer, bevatten meer kleine letters, meer hoofdletters en meer speciale tekens. De resultaten op entropie lieten ook het belang van het geven van zelfeffectiviteit informatie zien. De entropie van het aangemaakte wachtwoord was het hoogst wanneer deelnemers informatie over zelfeffectiviteit, al dan niet in combinatie met informatie over ernst van risico's, hadden ontvangen.

Tabel 16

Wachtwoorden gedragsmaat: kenmerken aangemaakte wachtwoorden als functie van Conditie

	Conditie				ANOVA
	Controle (*N* = 239) *M* (*SD*)	Ernst (*N* = 281) *M* (*SD*)	Zelfeffectiviteit (*N* = 299) *M* (*SD*)	Ernst + zelfeffectiviteit (*N* = 256) *M* (*SD*)	
Entropie	58.62[a] (25.29)	70.16[b] (32.98)	74.81[b] (28.92)	75.64[b] (27.75)	$F = 18.20$, $p < .001$, $\eta_p^2 = .05$
Lengte	9.88[a] (3.61)	11.61[b] (4.79)	11.98[b] (4.24)	12.12[b] (4.02)	$F = 14.94$, $p < .001$, $\eta_p^2 = .04$
Kleine letters	5.91[a] (3.41)	6.85[b] (3.97)	6.87[b] (4.20)	6.79[ab] (3.81)	$F = 3.58$, $p = .013$, $\eta_p^2 = .01$
Hoofdletters	1.02[a] (1.31)	1.41[b] (1.07)	1.40[ab] (1.63)	1.67[b] (1.90)	$F = 5.98$, $p < .001$, $\eta_p^2 = .02$
Speciale tekens	0.48[a] (0.76)	0.74[b] (1.36)	0.97[bc] (0.93)	1.05[c] (1.10)	$F = 14.36$, $p < .001$, $\eta_p^2 = .04$
Cijfers	2.48[a] (1.85)	2.60[a] (1.97)	2.74[a] (1.82)	2.61[a] (1.87)	$F < 1$, $p = .443$

Noot. $N = 1075$. Per rij verschillen gemiddelden met een verschillende superscript letter statistisch significant van elkaar op $p < .05$ (Tukey HSD posthoc toetsen).

Een criterium voor sterke wachtwoorden is dat wachtwoorden bestaan uit minstens 12 tekens, minstens 1 kleine letter, 1 hoofdletter, 1 speciaal teken en 1 cijfer. In de controle conditie voldeed slechts bij 11.7% van de deelnemers het aangemaakte wachtwoord aan deze voorwaarden. In de interventie condities was dit percentage significant hoger (zie Tabel 17). Het geven van informatie over zelfeffectiviteit, al dan niet gecombineerd met informatie over ernst van risico's, leidde tot de sterkste wachtwoorden. De wachtwoorden in de zelfeffectiviteit conditie en ernst + zelfeffectiviteit conditie waren significant sterker dan de wachtwoorden in de ernst conditie en de controle conditie (zie Tabel 17).

Tabel 17

Wachtwoorden gedragsmaat: Bestaat het wachtwoord uit minstens 12 tekens, minstens 1 kleine letter, 1 hoofdletter, 1 speciaal teken en 1 cijfer? als functie van Conditie

	Conditie (%)			
	Controle (*N* = 239)	Ernst (*N* = 281)	Zelfeffectiviteit (*N* = 299)	Ernst + zelfeffectiviteit (N = 256)
Ja	11.7[a]	20.3[b]	31.4[c]	32.4[c]
Nee	88.3[a]	79.7[b]	68.6[c]	67.6[c]

Noot. $N = 1075$. χ^2 (3) = 40.42, $p < .001$. Per rij verschillen percentages met een verschillende superscript letter significant van elkaar op $p < .05$ (*Z* posthoc proportietoetsen).

Op de vraag of het aangemaakt wachtwoord overeenkomt met hoe deelnemers normaal een wachtwoord aanmaken lieten de resultaten ook zien dat de combinatie van ernst en zelfeffectiviteit resulteerde in veiliger wachtwoordgedrag vergeleken met de controle conditie (zie Tabel 18). Na informatie over ernst en zelfeffectiviteit (vs. geen informatie in de controle conditie) gaven deelnemers vaker aan een ingewikkelder wachtwoord dan normaal te hebben aangemaakt, en minder vaak aan een simpeler wachtwoord te hebben aangemaakt. Het geven van informatie over de risico's van onveilige wachtwoorden in combinatie met hoe wachtwoorden sterker kunnen worden gemaakt heeft dus een positief effect op veilig wachtwoordgedrag. Opvallend in de resultaten was dat deelnemers in de interventie condities ook vaker dan deelnemers in de controle conditie aangaven een wachtwoord te hebben gekozen op dezelfde wijze dat ze normaal zouden doen. Dit kan erop wijzen dat als mensen zich veilig achten (zoals het geval is in de Markteffect omgeving), dat ze zich minder veilig gedragen dan ze in andere situaties zouden doen.

Tabel 18

Aangemaakte wachtwoord overeenkomstig met hoe deelnemer normaal een wachtwoord aanmaakt als functie van Conditie

	Conditie (%)			
	Controle (*N* = 239)	Ernst (*N* = 281)	Zelfeffectiviteit (*N* = 299)	Ernst + zelfeffectiviteit (*N* = 256)
Nee ik heb een simpeler wachtwoord aangemaakt	48.5[a]	26.0[b]	19.4[bc]	17.2[c]
Nee, ik heb een ingewikkelder wachtwoord aangemaakt	13.0[a]	17.4[ab]	17.1[a]	23.8[b]
Ja, ik heb een wachtwoord gekozen op dezelfde wijze als dat ik normaal zou doen	38.5[a]	56.6[b]	63.5[b]	59.0[b]

Noot. $N = 1075$. χ^2 (6) = 81.64, $p \leq .001$. Per rij verschillen percentages met een verschillende superscript letter significant van elkaar op $p < .05$ (*Z* posthoc proportietoetsen).

Daarnaast bevatten de wachtwoorden van de deelnemers in de condities waar informatie over zelfeffectiviteit werd gegeven minder persoonlijke informatie dan de wachtwoorden van deelnemers in de controle conditie (zie Tabel 19). Het geven van informatie over het aanmaken van sterke wachtwoorden, al dan niet in combinatie met informatie over ernst van risico's, resulteerde in de veiligste wachtwoorden.

Tabel 19

Aangemaakte wachtwoord bevat persoonlijke informatie als functie van Conditie

	Conditie (%)			
	Controle (*N* = 239)	Ernst (*N* = 281)	Zelfeffectiviteit (*N* = 299)	Ernst + zelfeffectiviteit (*N* = 256)
Ja	31.0[a]	24.6[ab]	19.4[bc]	15.2[c]
Nee	62.8[a]	69.4[ab]	73.9[bc]	78.5[c]
Zeg ik liever niet	6.3[a]	6.0[a]	6.7[a]	6.3[a]

Noot. $N = 1075$. χ^2 (6) = 20.36, $p = .002$. Per rij verschillen percentages met een verschillende superscript letter significant van elkaar op $p < .05$ (*Z* posthoc proportietoetsen).

Verschillen tussen groepen in effectiviteit interventie

Bij het toetsen van de effectiviteit van interventies op gedrag is het belangrijk om te controleren of deze effecten vergelijkbaar zijn voor verschillende groepen in de samenleving. Om dit te onderzoeken hebben we getoetst of Conditie interacteerde met de socio-demografische variabelen

Geslacht (man, vrouw: *N* = 1068), Leeftijd (laag 18-39 jaar, midden 40-55 jaar, hoog 56+ jaar: *N* = 1066) en Opleiding (laag, midden, hoog: *N* = 1062) op de entropie van het aangemaakte wachtwoord, of het aangemaakte wachtwoord voldeed aan voorwaarden van sterke wachtwoorden, en of het aangemaakte wachtwoord persoonlijke informatie bevatte.

Geslacht

Een ANOVA op entropie van het aangemaakte wachtwoord liet geen significante interactie zien tussen Conditie en Geslacht, F (3, 1060) < 1, p = .941. Ook liet de analyse geen hoofdeffect van Geslacht zien, F (1, 1060) < 1, p = .812. Dit betekent dat het effect van de interventie op entropie en de entropie zelf niet verschilde tussen mannen en vrouwen.

De maat of het aangemaakte wachtwoord voldeed aan voorwaarden voor sterke wachtwoorden liet zowel voor mannen (*N* = 505) als vrouwen (*N* = 563) een significant effect van Conditie zien (mannen χ^2 (3) = 17.03, p < .001; vrouwen χ^2 (3) = 23.39, p < .001). Het patroon van resultaten was vergelijkbaar voor mannen en vrouwen en *Z* proportietoetsen lieten zien dat percentages binnen de condities niet significant verschilden tussen mannen en vrouwen. Dit betekent dat ook voor deze maat het effect van de interventie vergelijkbaar was voor mannen en vrouwen, en dat de mate waarin het aangemaakte wachtwoord voldeed aan voorwaarden voor sterke wachtwoorden niet verschilde tussen mannen en vrouwen.

De maat of het aangemaakte wachtwoord persoonlijke informatie bevatte liet zowel voor mannen (*N* = 505) als vrouwen (*N* = 563) een significant effect van Conditie zien (mannen χ^2 (6) = 17.15, p = .009; vrouwen χ^2 (6) = 13.11, p = .041). Het patroon van resultaten was vergelijkbaar voor mannen en vrouwen en *Z* proportietoetsen lieten zien dat percentages binnen de condities niet verschilden tussen mannen en vrouwen. Dit betekent dat we ook voor deze maat vonden dat het effect van de interventie vergelijkbaar was voor mannen en vrouwen, en dat de mate waarin het aangemaakte wachtwoord persoonlijke informatie bevatte niet verschilden tussen mannen en vrouwen.

Leeftijd

De ANOVA op entropie van het aangemaakte wachtwoord liet geen significante interactie zien tussen Conditie en Leeftijd, F (6, 1054) = 1.55, p = .157. Ook liet de analyse geen hoofdeffect van Leeftijd zien, F (2, 1054) < 1, p = .986. Dit betekent dat het effect van de interventie op entropie en de entropie zelf niet verschilde tussen de leeftijdsgroepen laag, midden en hoog.

De maat of het aangemaakte wachtwoord voldeed aan de voorwaarden voor sterke wachtwoorden liet voor zowel leeftijd laag (*N* = 258), leeftijd midden (*N* = 409) en leeftijd hoog (*N* = 399) een significant effect van Conditie zien (leeftijd laag χ^2 (3) = 17.20, p < .001; leeftijd midden χ^2 (3) = 17.08, p < .001; leeftijd hoog χ^2 (3) = 15.44, p = .001). Het patroon van resultaten liet zowel overeenkomsten als verschillen zien in hoe de interventie uitwerkte tussen leeftijd laag (10.8% controle, 15.4% ernst, 37.8% zelfeffectiviteit, 22.2% ernst + zelfeffectiviteit), leeftijd midden (10.5% controle, 26.7% ernst, 31.7% zelfeffectiviteit, 35.7% ernst + zelfeffectiviteit) en leeftijd hoog (13.8% controle, 16.8% ernst, 25.2% zelfeffectiviteit, 35.3% ernst + zelfeffectiviteit). Bij leeftijd laag leek met name zelfeffectiviteit tot sterke wachtwoorden te leiden; bij leeftijd midden leken zowel ernst,

zelfeffectiviteit als de combinatie van ernst en zelfeffectiviteit effectief te zijn; bij leeftijd hoog leek vooral zelfeffectiviteit, al dan niet in combinatie met ernst, effectief te zijn.

De maat of het aangemaakte wachtwoord persoonlijke informatie bevatte liet alleen een significant effect voor Conditie zien voor leeftijd midden (N = 409, χ^2 (6) = 20.75, p = .002), niet voor leeftijd laag (N = 258, χ^2 (6) = 7.05, p = .316) of leeftijd hoog (N = 399, χ^2 (6) = 7.94, p = .242). Het patroon van de resultaten voor leeftijd midden was hierbij vergelijkbaar met dat in Tabel 19 (controle 31.4%, ernst 27.6%, zelfeffectiviteit 17.5%, ernst + zelfeffectiviteit 11.2%), waarbij zelfeffectiviteit, al dan niet in combinatie met ernst, tot de veiligste wachtwoorden leidde. Het uitblijven van een significant effect van Conditie binnen leeftijd laag wordt waarschijnlijk (deels) veroorzaakt doordat wachtwoorden in de controle conditie van deze leeftijdscategorie al relatief beperkt persoonlijke informatie bevatte (26.2%).

Opleiding

De ANOVA op entropie van het aangemaakte wachtwoord liet geen significante interactie zien tussen Conditie en Opleiding, F (6, 1054) = 1.01, p = .414. Ook liet de analyse geen hoofdeffect van Opleiding zien, F (2, 1054) = 1.66, p = .191. Dit betekent dat het effect van de interventie op entropie en de entropie zelf niet verschilde tussen de leeftijdsgroepen laag, midden en hoog.

De maat of het aangemaakte wachtwoord voldeed aan de voorwaarden voor sterke wachtwoorden liet een significant effect van Conditie zien voor opleiding midden (N = 416; χ^2 (3) = 25.33, p < .001) en voor opleiding hoog (N = 482; χ^2 (3) = 13.89, p = .003), niet voor opleiding laag (N = 160; χ^2 (3) = 3.71, p = .295). Het patroon van de resultaten voor opleiding midden (6.7% controle, 21.1% ernst, 32.0% zelfeffectiviteit, 35.2% ernst + zelfeffectiviteit) en opleiding hoog (16.1% controle, 19.8% ernst, 32.4% zelfeffectiviteit, 32.8% ernst + zelfeffectiviteit) was hierbij vergelijkbaar; zelfeffectiviteit, al dan niet in combinatie met ernst, resulteerde in de veiligste wachtwoorden.

De maat of het aangemaakte wachtwoord persoonlijke informatie bevatte liet alleen een significant effect voor Conditie zien voor opleiding hoog (N = 486, χ^2 (6) = 18.76, p = .005), niet voor opleiding laag (N = 160, χ^2 (6) = 5.13, p = .527) of opleiding midden (N = 416, χ^2 (6) = 8.16, p = .227). Het patroon van de resultaten voor opleiding hoog was hierbij vergelijkbaar met dat in Tabel 19 (31.3% controle, 21.6% ernst, 12.9% zelfeffectiviteit, 13.4% ernst + zelfeffectiviteit controle), waarbij zelfeffectiviteit, al dan niet in combinatie met ernst, resulteerde in de veiligste wachtwoorden.

3.2.1.2 Interventie checks

De interventie richtte zich op het verhogen van de zelfeffectiviteit van veilig gedrag en/of het verhogen van de ernst van de risico's van onveilig gedrag. De antwoorden van de deelnemers op de interventie check vragen geven inzicht in of de interventie het beoogde effect had op ernst en zelfeffectiviteit. De resultaten voor de interventie checks zijn weergegeven in Tabel 20.

De zelfeffectiviteit check vragen lieten zien dat deelnemers zich gemiddeld genomen in staat achtten om sterke wachtwoorden te maken. Tegen de verwachting in was zelfeffectiviteit niet hoger in de zelfeffectiviteit condities vergeleken met de andere condities. Een mogelijke verklaring is dat deelnemers al wisten hoe ze een veilig wachtwoord moeten aanmaken, waardoor de informatie in de zelfeffectiviteit condities niet veel extra inzicht bood.

De resultaten voor de ernst check vraag lieten zien dat deelnemers gemiddeld genomen het gevaar van het gebruik van zwakke wachtwoorden erkenden. Tegen de verwachting in was de waargenomen ernst van risico's van onveilig gedrag niet hoger in de ernst condities vergeleken met de andere condities. Ook hier kan het zijn dat deelnemers zich al bewust waren van de gevaren van zwakke wachtwoorden. Daardoor leidde de informatie in de ernst condities wellicht niet tot een hogere waargenomen ernst van risico's van onveilig gedrag.

De effectiviteit van de interventie op gedrag zou dan met name te verklaren zijn door een activatie van de zelfeffectiviteit en ernst informatie. Deze informatie zit dan tijdelijk meer in het hoofd van de deelnemers (in plaats van dat de interventie de deelnemers daadwerkelijk nieuwe informatie gaf).

Tabel 20

Interventie checks wachtwoorden als functie van Conditie

	Conditie				ANOVA
	Controle (N = 239) M (SD)	Ernst (N = 281) M (SD)	Zelfeffectiviteit (N = 299) M (SD)	Ernst + zelfeffectiviteit (N = 256) M (SD)	
Zelfeffectiviteit					
Ik weet hoe ik een sterk wachtwoord kan aanmaken	4.30[a] (0.86)	4.22[a] (0.83)	4.32[a] (0.85)	4.24[a] (0.91)	F < 1, p = .479
Ik ben in staat om sterke wachtwoorden te maken	4.26[a] (0.91)	4.19[a] (0.85)	4.30[a] (0.87)	4.28[a] (0.91)	F < 1, p = .455
Ernst					
Het is gevaarlijk om zwakke wachtwoorden te gebruiken	4.23[a] (0.97)	4.41[a] (0.86)	4.27[a] (0.94)	4.36[a] (0.87)	F = 2.10, p = .099

Noot. N = 1075. Per rij verschillen gemiddelden met een verschillende superscript letter statistisch significant van elkaar op p < .05 (Tukey HSD posthoc toetsen).

Verschillen tussen groepen in effectiviteit interventie

Bij het toetsen van de effectiviteit van de interventie is het ook bij de interventie checks belangrijk om te controleren of het effect van de interventie vergelijkbaar is voor verschillende groepen in de samenleving. Om dit te onderzoeken hebben we met ANOVAs getoetst of Conditie interacteerde met de socio-demografische variabelen Geslacht (man, vrouw: *N* = 1068), Leeftijd (laag 18-35 jaar, midden 36-55 jaar, hoog 56+ jaar: *N* = 1066) en Opleiding (laag, midden, hoog: *N* = 1062) op de interventie check vragen.

Zelfeffectiviteit checks

De resultaten lieten geen interactie-effecten met Conditie van de socio-demografische variabelen zien op de zelfeffectiviteit check vragen, *F*s ≤ 1.15, *p*s ≥ .330 Dit betekent dat het effect van de interventie op zelfeffectiviteit niet verschilde tussen mannen en vrouwen, of tussen leeftijdsgroepen of opleidingsniveaus. Wel vonden we een hoofdeffect van Geslacht op de "Ik ben in staat" vraag, *F* (1, 1060) = 12.33, *p* < .001, η_p^2 = .01: Mannen achtten zich meer in staat om sterke wachtwoorden te maken (*M* = 4.35, *SD* = 0.83) dan vrouwen (*M* = 4.17, *SD* = 0.92). Ook vonden we een hoofdeffect van Opleiding op de zelfeffectiviteit check vragen, *F* (2, 1050) = 7.43/9.55, *p*s < .001, η_p^2 = .01/.02: Hoogopgeleide deelnemers rapporteerden een hogere zelfeffectiviteit (*M* = 4.37, *SD* = 0.78; *M* = 4.38, *SD* = 0.77) vergeleken met laagopgeleide (*M* = 4.08, *SD* = 0.96; *M* = 4.06, *SD* = 1.01) en midden opgeleide deelnemers (*M* = 4.23, *SD* = 0.89; *M* = 4.20, *SD* = 0.93), *p*s ≤ .035.

Ernst check

De resultaten lieten geen interactie-effect zien van Conditie en Geslacht op de ernst check vraag, of van Conditie en Opleiding op ernst check vraag, *F*s < 1, *p*s ≥. 524. Dit betekent dat het effect van Conditie op ernst niet verschilde tussen mannen en vrouwen, of tussen opleidingsniveaus. Wel lieten de resultaten een significante Conditie x Leeftijd interactie op de ernst check vraag zien, *F* (6, 1054) = 2.36, *p* = .029, η_p^2 = .01. Om deze interactie te interpreteren hebben we per leeftijdscategorie (laag, midden, hoog) getoetst of er een significant effect van Conditie was. Dit bleek het geval te zijn in de leeftijd hoog categorie [*N* = 399, *F* (3, 395) = 3.78, *p* = .011, η_p^2 = .03], maar niet in de leeftijd laag categorie [*N* = 258, *F* (3, 254) = 1.32, *p* = .268] of de leeftijd midden categorie [*N* = 409, *F* (3, 405) = 1.93, *p* = .124]. In de leeftijd hoog categorie was waargenomen ernst significant hoger in de ernst conditie (*M* = 4.68, *SD* = 0.64) dan in de zelfeffectiviteit conditie (*M* = 4.33, *SD* = 0.96, *p* = 0.13). Daarnaast liet de analyse een hoofdeffect van Leeftijd op de ernst check vraag zien, *F* (2, 1054) = 12.72, *p* < .001, η_p^2 = .02: Deelnemers in de leeftijd hoog categorie achtten het gevaarlijker om zwakke wachtwoorden te gebruiken (*M* = 4.50, *SD* = 0.84) dan deelnemers in de leeftijd laag (*M* = 4.17, *SD* = 0.93) en leeftijd midden (*M* = 4.23, *SD* = 0.94) categorieën, *p*s < .001.

3.2.1.3 Overige vragen

Kwetsbaarheid, responseffectiviteit en ernst van specifieke risico's verschilden niet als functie van Conditie, *F*s (3, 1071) ≤ 1.66, *p*s ≥ .174. In deze sectie bespreken we daarom de resultaten voor kwetsbaarheid, responseffectiviteit en ernst van specifieke risico's voor de hele steekproef (*N* = 1075).

Kwetsbaarheid

Deelnemers erkenden gemiddeld genomen dat als ze zwakke wachtwoorden gebruiken, ze slachtoffer van online criminaliteit kunnen worden. Meer specifiek erkenden deelnemers dat het hen kan overkomen dat criminelen wachtwoorden achterhalen (*M* = 4.35, *SD* = 0.80), dat criminelen toegang krijgen tot hun accounts, e-mail, webcam of bankrekening (*M* = 4.32, *SD* = 0.81), dat criminelen hun geld stelen (*M* = 4.07, *SD* = 0.99), en dat criminelen hun persoonlijke foto's en berichten delen op het internet (*M* = 4.21, *SD* = 0.86).

Responseffectiviteit

Deelnemers erkenden gemiddeld genomen dat ze als ze sterke wachtwoorden gebruiken minder risico lopen om slachtoffer te worden van online criminaliteit (*M* = 4.38, *SD* = 0.80).

Ernst specifieke risico's

De resultaten lieten zien dat deelnemers alle risico's als ernstig beoordeelden. Gemiddelde scores voor de specifieke risico's lagen tussen 4.54 (*SD* = 0.89: "Ik zou het erg als criminelen toegang krijgen tot mijn webcam") en 4.81 (*SD* = 0.57: '"Ik zou het erg vinden als criminelen mijn geld stelen").

3.2.1.4 Samenvatting resultaten wachtwoorden

Samengevat bleek uit Studie 2a, zoals verwacht, dat het communiceren van informatie over zelfeffectiviteit, al dan niet in combinatie met informatie over de ernst van risico's, resulteerde in veiligere wachtwoorden. Het aangemaakte wachtwoord had een hogere entropie, voldeed vaker aan de voorwaarden van een sterk wachtwoord en bevatte minder vaak persoonlijke informatie. De conditie waarin alleen informatie over de ernst van de risico's werd gecommuniceerd verschilde niet van de controle conditie op entropie. Wel waren in deze conditie kenmerken van het wachtwoord deels veiliger dan in de controle conditie. Het aangemaakte wachtwoord voldeed vaker aan de voorwaarden van een veilig wachtwoord en bevatte bijvoorbeeld meer hoofdletters of speciale tekens. De effecten in de ernst conditie leken wel zwakker dan de effecten in de andere interventie condities. Tot slot gaven deelnemers in alle interventie condities (vs. de controle conditie) aan dat het aangemaakte wachtwoord ingewikkelder was dan deelnemers normaal zouden doen, wat laat zien dat de geteste interventie effectief was.

Hoewel de interventie resulteerde in veiliger wachtwoordgedrag, zagen we geen effecten van de interventie op de interventie check metingen van ernst en zelfeffectiviteit. Opvallend waren hierbij de relatief hoge ernst en zelfeffectiviteit scores in de controle conditie, wat suggereert dat deelnemers zich al redelijk bewust waren van de ernst van risico's en dat ze een zeker mate van zelfeffectiviteit ervoeren. Het lijkt er dus op dat met name de (extra) activatie van de ernst en de zelfeffectiviteit de gedragseffecten verklaart. We bespreken deze mogelijkheid uitgebreider in Hoofdstuk 4.

Verder werden de specifieke risico's van onveilig wachtwoordgedrag als ernstig beoordeeld. Daarnaast erkenden deelnemers dat ze kwetsbaar zijn voor online criminaliteit als ze zwakke

wachtwoorden gebruiken en het werd het gebruik van sterke wachtwoorden als een manier gezien om risico's te verminderen.

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 voorwaarden, of dat het wachtwoord persoonlijke informatie bevatte. We vonden bij de maat of het aangemaakte 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. Dit resultaat is in lijn met de resultaten op de ernst interventie check, die lieten zien dat oudere deelnemers het gevaarlijker achtten om zwakke wachtwoorden te gebruiken dan jongere deelnemers. Voor opleidingsniveau vonden we ook verschillen: zelfeffectiviteit, al dan niet in combinatie met ernst, leidde tot de veiligste wachtwoorden onder hoog- en middenopgeleide deelnemers. Onder laagopgeleide deelnemers vonden we geen verschillen tussen condities. Dit is in lijn met de resultaten op de zelfeffectiviteit interventie check vragen, die lieten zien dat hoger opgeleide deelnemers een hogere zelfeffectiviteit rapporteerden dan lager opgeleide deelnemers.

3.2.2 Studie 2b Persoonsgegevens

3.2.2.1 Gedragsmaat en zelfrapportage gedrag

Niet alle deelnemers namen deel aan de verloting. Van de 1012 deelnemers antwoordden 193 deelnemers (19.1%) "Nee" op de vraag of ze meewilden doen aan de verloting. Van de deelnemers die "Ja" antwoordden op de vraag (*N* = 819) hebben vervolgens 216 deelnemers (26.4%) hun deelname geannuleerd. Uiteindelijk deden dus 603 deelnemers (59.6%) mee aan de verloting van de prijs. Belangrijk om hierbij te vermelden is dat de 59.6% mogelijk in werkelijkheid (iets) lager is: onderzoeksbureau Markteffect meldde dat bij het verschijnen van het formulier het aantal deelnemers dat stopte met de studie in verhouding hoger was dan bij andere onderdelen in de studie (voor meer informatie; zie de onderzoek verantwoording van Markteffect die hier te vinden is: https://easy.dans.knaw.nl/ui/home).

Interessant om te zien (zie Tabel 21: grijs gearceerd) is dat deelname aan de verloting significant verschilde tussen condities. Deelname aan de verloting was significant lager in de ernst conditie dan in de controle conditie. Dit betekent dat deelnemers in de ernst conditie er minder vaak voor kozen om online hun persoonsgegevens te delen dan deelnemers in de controle conditie.

Tabel 21

Persoonsgegevens gedragsmaat: Deelname aan verloting prijs als functie van Conditie

	Conditie (%)			
	Controle (*N* = 264)	Ernst (*N* = 265)	Zelfeffectiviteit (*N* = 234)	Ernst + zelfeffectiviteit (*N* = 249)
Meedoen aan verloting (*N* = 1012)				
Ja	83.3	77.4	81.6	81.5
Nee	16.7	22.6	18.4	18.5
Annuleren deelname onder 'Ja' deelnemers (*N* = 819)				
Ja	20.9	30.7	25.7	28.6
Nee	79.1	69.3	74.3	71.4
Deelname aan verloting (*N* = 1012)				
Ja	65.9^{a}	53.6^{b}	60.7^{ab}	58.2^{ab}
Nee	34.1^{a}	46.4^{b}	39.3^{ab}	41.8^{ab}

Noot. Deelname aan verloting: X^2 (3) = 8.65, p = .034. Per rij verschillen percentages met een verschillende superscript letter significant van elkaar op $p < .05$ (*Z* posthoc proportietoetsen).

Vervolgens hebben we onder de deelnemers die meededen aan de verloting (*N* = 603) geanalyseerd hoeveel en welk type persoonsgegevens zij deelden. De resultaten worden weergegeven in Tabel 22. De overkoepelende toets was niet significant (p = .055), maar posthoc toetsen lieten significante verschillen tussen condities zien. In de controle conditie koos slechts 11.5% van de deelnemers die meededen met de verloting ervoor om alleen de niet-verplichte gegevens te delen. Dit percentage was significant hoger onder deelnemers in de zelfeffectiviteit conditie en de ernst + zelfeffectiviteit conditie. Na informatie over zelfeffectiviteit, al dan niet in combinatie met ernst van risico's, kozen deelnemers er vaker voor om alleen de twee verplichte persoonsgegevens te delen vergeleken met deelnemers in de controle conditie.

Deelnemers in alle condities bleken veel persoonsgegevens te delen, ook niet-verplichte informatie. Het merendeel van de deelnemers (61.4%) deelde alle zeven persoonsgegevens (niet in tabel: geen significant verschil tussen condities). Opvallend is dat maar liefst 76.3% van de deelnemers de laatste drie cijfers van hun bankrekening invulden, terwijl het niet verplicht was deze gegevens te delen. Op de vraag of alle persoonsgegevens die de deelnemers hebben ingevuld op het formulier echte gegevens betroffen, gaven vrijwel alle deelnemers (91.4%) aan dat dit het geval was (vs. 7.6% "Deel echte gegevens, deel verzonnen" en 1.0% "Geen van de ingevulde gegevens zijn eigen gegevens".

Tabel 22

Gedragsmaat persoonsgegevens: Gedeelde persoonsgegevens door deelnemers die deelnamen aan de verloting als functie van Conditie

	Conditie (%)			
	Controle (*N* = 174)	Ernst (*N* = 142)	Zelfeffectiviteit (*N* = 142)	Ernst + zelfeffectiviteit (*N* = 145)
Volledige naam *	100	100	100	100
E-mailadres *	100	100	100	100
Telefoonnummer	66.1	67.6	62.7	63.4
Geboortedatum	83.9	81.0	76.1	75.9
Postcode	85.6	83.1	77.5	77.9
Huisnummer	83.3	78.9	74.6	75.2
Laatste drie cijfers van bankrekeningnummer	80.5	78.9	72.5	72.4
Gedeelde persoonsgegevens				
Alleen de twee verplichte gegevens	11.5^{a}	12.7^{ab}	20.4^{b}	20.0^{b}
Verplichte gegevens plus 1-5 niet-verplichte gegevens	88.5^{a}	87.3^{ab}	79.6^{b}	80.0^{b}

Noot. *N* = 603. * Verplicht in te vullen. Gedeelde persoonsgegevens: X^2 (3) = 7.62, *p* = .055. Per rij verschillen percentages met een verschillende superscript letter significant van elkaar op *p* < .05 (*Z* posthoc proportie toetsen).

Verschillen tussen groepen in effectiviteit interventie

Bij het toetsen van de effectiviteit van interventies op gedrag is het belangrijk om te controleren of deze effecten vergelijkbaar zijn voor verschillende groepen in de samenleving. Om dit te onderzoeken hebben we getoetst of de socio-demografische variabelen Geslacht (man, vrouw), Leeftijd (laag 18-35 jaar, midden 36-55 jaar, hoog 56+ jaar) en opleiding (laag, midden, hoog) interacteerden met de hierboven gerapporteerde resultaten voor deelname aan de verloting. We hebben dezelfde analyse uitgevoerd voor gedeelde persoonsgegevens, maar dan alleen voor de variabele Geslacht, niet voor de variabelen Leeftijd en Opleiding. Bij de variabele gedeelde persoonsgegevens was de overall *N* lager (*N* = 603) dan bij deelname aan de verloting (*N* = 1012). Daarnaast was er bij Leeftijd en Opleiding, anders dan bij Geslacht, een ongelijke verdeling in *N* tussen leeftijdsgroepen en opleidingsniveaus. Dit, gecombineerd met de kleine proportie deelnemers die alleen verplichte persoonsgegevens deelde, maakt dat de *N* in sommige cellen laag was, en we niet denken dat de resultaten van de analyse robuust of betrouwbaar zouden zijn. We hebben voor gedeelde persoonsgegevens wel getoetst of er over condities heen een verschil was tussen leeftijdsgroepen en opleidingsniveaus.

Geslacht

De maat deelname aan de verloting liet alleen een significant effect voor Conditie zien voor vrouwen [N = 519, χ^2 (3) = 9.73, p = .021], niet voor mannen [N = 489, χ^2 (3) = 3.07, p = .381]. Het patroon van de resultaten voor vrouwen was hierbij vergelijkbaar met dat in Tabel 21 (61.1% controle, 50.0% ernst, 63.4% zelfeffectiviteit, 53.0% ernst + zelfeffectiviteit controle), waarbij de ernst conditie in de laagste deelname resulteerde. Het percentage deelnemers dat over condities heen deelnam aan de verloting verschilde niet tussen mannen en vrouwen, p = .317.

De maat gedeelde persoonsgegevens liet geen significant effect voor Conditie zien voor mannen [N = 300, χ^2 (3) = 5.81, p = .118] of vrouwen [N = 302, χ^2 (3) = 3.83, p = .281. Het patroon van resultaten voor zowel mannen als vrouwen kwam overeen met het patroon in Tabel 22. Het percentage deelnemers dat over condities heen alleen verplichte persoonsgegevens deelde verschilde niet tussen mannen en vrouwen, p = .327.

Leeftijd

De maat deelname aan de verloting liet geen significant effect voor Conditie zien voor leeftijd laag [N = 212, χ^2 (3) = 2.66, p = .448], leeftijd midden [N = 374, χ^2 (3) = 7.10, p = .069], of leeftijd hoog [N = 421, χ^2 (3) = 4.11, p = .250]. Het percentage deelnemers dat over condities heen deelnam aan de verloting verschilde niet tussen leeftijdscategorieën, ps ≥. 190.

De maat gedeelde persoonsgegevens liet zien dat het percentage deelnemers dat over condities heen alleen verplichte persoonsgegevens deelde significant verschilde tussen leeftijdscategorieën (leeftijd laag N = 118, 30.3%: leeftijd midden N = 224, 17.4%: leeftijd hoog N = 259, 8.1%; ps ≤ .002). Hoe ouder de deelnemers, hoe onveiliger ze zich gedroegen op het vlak van het online delen van persoonsgegevens. Dit resultaat is in lijn met de regressieresultaten in Studie 1.

Opleiding

De maat deelname aan de verloting liet geen significant effect voor Conditie zien voor opleiding laag [N = 170, χ^2 (3) = 1.92, p = .588], opleiding midden [N = 428, χ^2 (3) = 6.57, p = .087], of opleiding hoog [N = 399, χ^2 (3) = 2.07 p = .559]. Het percentage deelnemers dat over condities heen deelnam aan de verloting verschilde niet tussen opleidingsniveaus, ps ≥ .379

De maat gedeelde persoonsgegevens liet zien dat het percentage deelnemers dat over condities heen alleen verplichte persoonsgegevens deelde significant verschilde tussen de opleidingsniveaus (opleiding laag N = 103, 5.8%: opleiding midden N = 263, 13.7%: opleiding hoog N = 233, 22.3%; ps ≤ .034). Hoe hoger het opleidingsniveau van de deelnemers, hoe veiliger ze zich gedroegen. Dit resultaat is in lijn met de regressieresultaten in Studie 1.

3.2.2.2 Interventie checks

De interventie richtte zich op het verhogen van de zelfeffectiviteit van veilig gedrag en/of het verhogen van de ernst van de risico's van onveilig gedrag. De antwoorden van de deelnemers op de interventie check vragen geven inzicht in of de interventie het beoogde effect had op ernst en zelfeffectiviteit. De resultaten voor de interventie checks zijn weergegeven in Tabel 23.

De zelfeffectiviteit check vragen lieten zien dat deelnemers zich gemiddeld genomen redelijk in staat achtten om online veilig om te gaan met hun persoonsgegevens. Zoals verwacht, was waargenomen zelfeffectiviteit in de zelfeffectiviteit conditie hoger dan in de controle conditie. De resultaten voor de ernst + zelfeffectiviteit conditie lieten hetzelfde verwachte verschil zien, maar dan alleen op de tweede check vraag.

De resultaten voor ernst check vraag lieten zien dat deelnemers gemiddeld genomen het gevaar van het online onveilig omgaan met hun persoonsgegevens erkenden. Tegen de verwachting in was de waargenomen ernst van risico's van onveilig gedrag niet hoger in de ernst condities vergeleken met de controle conditie. Het kan zijn dat deelnemers zich al bewust waren van de gevaren van online onveilig omgaan met persoonsgegevens. Daardoor leidde de informatie in de ernst condities wellicht niet tot een hogere waargenomen ernst van risico's van onveilig gedrag.

Tabel 23

Interventie checks persoonsgegevens als functie van Conditie

	Conditie				ANOVA
	Controle (*N* = 264) *M* (*SD*)	Ernst (*N* = 265) *M* (*SD*)	Zelfeffectiviteit (*N* = 234) *M* (*SD*)	Ernst + zelfeffectiviteit (*N* = 2549) *M* (*SD*)	
Zelfeffectiviteit					
Ik weet hoe ik online veilig om kan gaan met mijn persoonsgegevens	3.79[a] (0.91)	3.83[ab] (0.83)	3.99[b] (0.81)	3.96[ab] (0.82)	F = 3.22, p = .022, η_p^2 = .01
Ik ben in staat om online veilig om te gaan met mijn persoonsgegevens	3.85[a] (0.97)	3.95[ab] (0.86)	4.05[b] (0.81)	4.05[b] (0.81)	F = 3.22, p = .022, η_p^2 = .01
Ernst					
Het is gevaarlijk om online onveilig om te gaan met mijn persoonsgegevens	4.27[a] (0.99)	4.39[a] (1.01)	4.44[a] (0.86)	4.47[a] (0.91)	F = 2.02, p = .081

Noot. N = 1012. Per rij verschillen gemiddelden met een verschillende superscript letter statistisch significant van elkaar op $p \leq .05$ (Tukey HSD posthoc toetsen).

Verschillen tussen groepen in effectiviteit interventie

Bij het toetsen van de effectiviteit van de interventie is het ook bij de interventie checks belangrijk om te controleren of het effect van de interventie vergelijkbaar is voor verschillende groepen in de samenleving. Om dit te onderzoeken hebben we met ANOVAs getoetst of Conditie interacteerde met de socio-demografische variabelen Geslacht (man, vrouw: N = 1008), Leeftijd (laag 18-35 jaar,

midden 36-55 jaar, hoog 56+ jaar: *N* = 1007) en Opleiding (laag, midden, hoog: *N* = 997) op de check vragen.

Zelfeffectiviteit checks

De resultaten lieten geen interactie-effecten met Conditie of hoofdeffecten van de socio-demografische variabelen op de zelfeffectiviteit check vragen zien, *F*s ≤ 2.54, *p*s ≥ .080. Dit betekent dat het effect van de interventie op zelfeffectiviteit en zelfeffectiviteit zelf niet verschilde tussen mannen en vrouwen, of tussen leeftijdsgroepen of opleidingsniveaus.

Ernst check

De resultaten lieten geen interactie-effect met Conditie zien op de ernst check vraag, *F*s ≤ 1.819, *p*s ≥ .094. Dit betekent dat het effect van de interventie op zelfeffectiviteit niet verschilde tussen mannen en vrouwen, of tussen leeftijdsgroepen of opleidingsniveaus. Wel was er een significant effect van Leeftijd op de ernst check vraag, F (2, 995) = 8.47, $p < .001$, $\eta_p^2 = .02$, waarbij hoogopgeleide deelnemers het gevaarlijker achtten om online onveilig om te gaan met persoonsgegevens (*M* = 4.53, *SD* = 0.89) dan laagopgeleide (*M* = 4.33, *SD* = 0.95) en middenopgeleide deelnemers (*M* = 4.27, *SD* = 0.99), *p*s ≤ .025.

3.2.2.3 Overige vragen

Kwetsbaarheid, responseffectiviteit en ernst van specifieke risico's verschilden niet als functie van Conditie, *F*s ≤ 2.46, *p*s ≥ .061. In deze sectie bespreken we daarom de resultaten voor kwetsbaarheid, responseffectiviteit en ernst van specifieke risico's voor de hele steekproef (*N* varieerde van 1007-1012; door een programmeerfout hebben sommige deelnemers niet alle vragen beantwoord).

Kwetsbaarheid

Deelnemers erkenden gemiddeld genomen dat als ze online onveilig omgaan met hun persoonsgegevens, ze slachtoffer van online criminaliteit kunnen worden. Meer specifiek erkenden deelnemers dat het hen kan overkomen dat hun persoonsgegevens in handen komen van criminelen (*M* = 4.49, *SD* = 0.79), dat criminelen geld stelen van familie en vrienden door te doen of ze de deelnemers zijn via WhatsApp of e-mail (*M* = 4.23, *SD* = 0.96), dat criminelen hun persoonsgegevens gebruiken bij het plegen van misdrijven waardoor de politie hen als verdachte ziet (*M* = 4.25, *SD* = 0.90).

Responseffectiviteit

Deelnemers erkenden gemiddeld genomen dat ze als ze online veilig omgaan met hun persoonsgegevens minder risico lopen om slachtoffer te worden van online criminaliteit (*M* = 4.15, *SD* = 0.91).

Ernst specifieke risico's

De resultaten lieten zien dat de deelnemers alle risico's als ernstig beoordeelden. Gemiddelde scores voor de specifieke risico's lagen tussen 4.75 (*SD* = 0.64: "Ik zou het erg als mijn persoonsgegevens in handen komen van criminelen") en 4.77 (*SD* = 0.64: "Ik zou het erg vinden als criminelen geld stelen van familie en vrienden, door te doen alsof ze mij zijn via WhatsApp of e-mail"; *SD* = 0.64 "Ik zou het erg vinden als criminelen mijn persoonsgegevens gebruiken bij het downloaden van kinderporno, waardoor de politie mij als verdachte ziet").

3.2.2.4 Samenvatting resultaten persoonsgegevens

Samengevat bleek uit Studie 2b, zoals verwacht, dat het communiceren van informatie over zelfeffectiviteit, al dan niet in combinatie met informatie over de ernst van risico's, resulteerde in het minder delen van niet-verplichte persoonsgegevens. 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 deelnemers in de controle conditie vaker afzagen van deelname aan de verloting. Door niet mee te doen aan de verloting hoefden ze ook geen persoonsgegevens te delen. Het percentage deelnemers dat veel niet-verplichte persoonsgegevens deelde was opvallend hoog, ook in de interventie condities.

Naast het effect van de interventie op veilig gedrag, waren er ook effecten van de interventie in de verwachte richting op de interventie check metingen van zelfeffectiviteit. Waargenomen zelfeffectiviteit was (deels) hoger in de zelfeffectiviteit condities dan in de controle conditie. Er was echter geen effect van de interventie op de interventie check meting van ernst. Net als bij het wachtwoordgedrag in Studie 2a waren er relatief hoge ernst scores in de controle conditie, wat suggereert dat deelnemers zich al redelijk bewust waren van de ernst van risico's van het onveilig online delen van persoonsgegevens.

Verder werden de specifieke risico's van het onveilig delen van persoonsgegevens als ernstig beoordeeld. Daarnaast erkenden deelnemers dat ze kwetsbaar zijn voor online criminaliteit als ze online onveilig omgaan met hun persoonsgegevens en werd het veilig online delen van persoonsgegevens gezien als een manier gezien om risico's te verminderen.

De resultaten voor verschillen tussen groepen in de samenleving lieten zien dat het effect van de interventie op deelname aan de verloting afhing van geslacht (het effect was significant voor vrouwen, niet mannen), maar niet van leeftijd of opleidingsniveau van de deelnemers. Ook lieten de resultaten zien dat leeftijd en opleiding van invloed waren op het veilig online delen van persoonsgegevens. Hoe ouder de deelnemers waren, hoe vaker ze niet-verplichte persoonsgegevens deelden. Hoewel oudere deelnemers zich onveiliger gedroegen op het gebied van het online delen van persoonsgegevens, lieten de resultaten op de ernst interventie check maat (net zoals in Studie 1) zien dat oudere deelnemers het online onveilig delen van persoonsgegevens wel gevaarlijker achtten dan jongere deelnemers. De resultaten voor opleiding lieten zien dat hoe hoger opgeleid de deelnemers waren, hoe vaker ze niet-verplichte persoonsgegevens deelden.

4. Discussie

4.1 Inleiding

Het huidige onderzoek is een vervolg op eerder onderzoek dat uitgevoerd is in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC; Van 't Hoff-de Goede et al., 2019). Dit eerdere onderzoek richtte zich op de vraag hoe veilig Nederlanders zich online gedragen en hoe dit kan worden verklaard. De onderzoekers richtten zich op veel verschillende gedragingen, zoals veilig wachtwoordgedrag, het installeren van updates, het delen van persoonsgegevens en het omgaan met bijlagen en hyperlinks in e-mails. 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 doel van het onderzoek was om te onderzoeken welke psychologische factoren een rol spelen bij veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens. Daarnaast hebben we interventie ontwikkeld en getest om veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens te bevorderen.

Kracht huidige onderzoek

In Studie 1 hebben we met een vragenlijst onderzocht welk van de psychologische factoren uit het model in Figuur 1 (zie Sectie 1.3) een rol spelen bij veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens. Op basis van de resultaten van Studie 1 hebben we in Studie 2 een interventie ontwikkeld en getest of we veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens konden bevorderen. Door ons te richten op twee specifieke doelgedragingen konden we ten opzichte van het eerdere onderzoek dieper ingaan op verklarende factoren en deze factoren ook meer toespitsen op het onderzochte doelgedrag.

Juist omdat Van 't Hoff-de Goede et al. (2019) lieten zien dat er een verschil was tussen geobserveerd gedrag en zelfgerapporteerd gedrag, hebben we zowel daadwerkelijk gedrag als zelfgerapporteerd gedrag gemeten. Hoewel deelnemers in Studie 1 hun online gedrag als relatief veilig inschatten, wezen gedragsmaten uit dat een aanzienlijk deel van de deelnemers zich onveilig gedroeg. In onderzoek naar veilig online gedrag wordt vaak alleen zelfgerapporteerd gedrag gemeten. Het huidige onderzoek laat zien hoe belangrijk het is om (ook) daadwerkelijk gedrag te meten. Daarnaast werden het wachtwoordgedrag en het gedrag op het vlak van het online delen van persoonsgegevens in beide studies gemeten aan het begin van het onderzoek zodat het gedrag niet beïnvloed werd door verdiepende vragen over de psychologische factoren die volgden.

Naast dat we geïnteresseerd waren in hoe (on)veilig mensen zich online gedragen op het gebied van het gebruik van veilige wachtwoorden en het veilig online delen van persoonsgegevens, hebben we ons ook gericht op het in kaart brengen van onderliggende processen. Meer specifiek hebben we

onderzocht welke psychologische factoren veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens bevorderen en belemmeren. We hebben hierbij gebruikt gemaakt van zowel gesloten vragen als open vragen. De antwoorden op deze vragen valideerden ons model in Figuur 1, en de antwoorden op de open vragen gaven extra inzichten die niet uit onze gesloten vragen naar voor kwamen.

Ten slotte was het doel van het huidige onderzoek om onze onderzoeksvragen te testen onder een representatieve steekproef van de Nederlandse bevolking. Hier zijn we redelijk in geslaagd, hoewel we iets meer hoger opgeleide deelnemers hadden en iets minder jonge deelnemers.

We zullen nu eerst bespreken welke conclusies er getrokken kunnen worden uit de literatuurstudie en de twee empirische studies. Daarna worden de beperkingen van het onderzoek en suggesties voor toekomstig onderzoek besproken. We sluiten af met een bespreking van beleidsimplicaties en aanbevelingen voor specifieke interventies.

4.2 Conclusies literatuurstudie

Het doel van de literatuurstudie was om uiteen te zetten wat er verstaan wordt onder veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens, en om in kaart te brengen welke psychologische factoren een rol zouden kunnen spelen bij deze doelgedragingen.

Op basis van de literatuurstudie kan veilig wachtwoordgedrag gedefinieerd worden aan de hand van drie criteria: 1) een veilige samenstelling van het wachtwoord, 2) een korte levensduur van het wachtwoord (i.e., frequent het wachtwoord veranderen) en 3) individueel eigendom van het wachtwoord. Het huidige onderzoek richtte zich vooral op de samenstelling van het wachtwoord. Het online veilig delen van persoonsgegevens kan ook worden gedefinieerd aan de hand van drie criteria: 1) een beoordeling van de veiligheid van de website of applicatie, 2) dat mensen niet méér delen dan noodzakelijk (terughoudendheid) en 3) dat mensen onderscheid moeten maken tussen verschillende typen persoonsgegevens. In onze studies hebben we vooral gemeten of mensen persoonsgegevens deelden, hoeveel persoonsgegevens mensen deelden, en of mensen meer informatie deelden dan noodzakelijk.

Daarnaast hebben we op basis van de literatuurstudie bepaald welke psychologische factoren een rol zouden kunnen spelen bij beide doelgedragingen. We hebben de volgende factoren gemeten in Studie 1: kennis, responskosten, kwetsbaarheid, ernst, zelfeffectiviteit, responseffectiviteit en verantwoordelijkheid (zie ook Figuur 1). Hoewel we de resultaten over *kennis* uiteindelijk niet hebben meegenomen in het huidige rapport, bespreken we wel de literatuur over de rol van kennis bij onze doelgedragingen. Deze literatuur liet zien dat kennis een verband lijkt te hebben met veilig online gedrag, maar dat dit verband soms positief en soms negatief is. Literatuur over *responskosten* (de inschatting van kosten die gemaakt worden om het doelgedrag te vertonen) liet zien dat responskosten negatief samenhangen met 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 negatieve consequenties van 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 mensen 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 achter het gewenste gedrag te vertonen, en responseffectiviteit is de mate waarin iemand verwacht dat het vertonen van het gewenste gedrag 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.

Samengevat bood de besproken literatuur een basis om te voorspellen dat veilig online gedrag wordt voorspeld door de psychologische factoren kennis, responskosten, kwetsbaarheid, ernst, zelf- en responseffectiviteit en verantwoordelijkheid. In Studie 1 hebben we onderzocht welke van deze psychologische factoren een rol spelen bij deze veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens. Vervolgens hebben we in Studie 2 een interventie ontwikkeld en getest, die gericht was op belangrijke psychologische factoren zoals geïdentificeerd in Studie 1.

4.3 Conclusies empirisch onderzoek

4.3.1 Studie 1

4.3.1.1 Gedragsmaten en zelfrapportagegedrag

In Studie 1 onderzochten we welke psychologische factoren veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens belemmeren en bevorderen. 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). We keken daarnaast welke psychologische factoren deze doelgedragingen belemmeren of bevorderen.

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 deelden 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.

Het zelfgerapporteerde gedrag kwam meer overeen met het geobserveerde gedrag bij wachtwoordgedrag dan bij het online delen van persoonsgegevens. Bij het online delen van persoonsgegevens liepen het geobserveerde en zelfgerapporteerde gedrag meer uiteen. Waar het geobserveerde gedrag liet zien dat veel deelnemers deelnamen aan de winactie en vrijwel alle deelnemers aan de winactie onnodig veel persoonsgegevens deelden, gaf slechts een minderheid van de deelnemers bij de zelfrapportage aan dat ze hun persoonsgegevens delen op websites (13.7%) en een meerderheid van de deelnemers gaf aan dat ze kijken of het nodig is dat ze hun persoonsgegevens delen (77.3%).

4.3.1.2 Psychologische factoren wachtwoorden

De resultaten voor de psychologische factoren lieten zien dat deelnemers met betrekking tot veilig wachtwoordgedrag hoge responskosten en lage zelfeffectiviteit rapporteerden: veilig wachtwoordgedrag kost in de ogen van de deelnemers veel tijd en moeite, en deelnemers achtten zich beperkt in staat om veilige wachtwoorden aan te maken en/of te onthouden. Daarnaast gaven de meeste deelnemers aan de gevolgen van onveilig wachtwoordgedrag ernstig te vinden en dat het gebruik van veilige wachtwoorden de kans op negatieve gevolgen verkleint. Ook gaf de meerderheid van de deelnemers aan dat de verantwoordelijkheid voor veilig wachtwoordgedrag bij henzelf ligt.

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 zouden helpen met veilig wachtwoordgedrag. Op de bevorderende factor wachtwoordmanagers wordt dieper ingegaan in Sectie 4.4.2.

4.3.1.3 Psychologische factoren persoonsgegevens

De resultaten voor psychologische factoren lieten zien dat ook bij het online delen van persoonsgegevens de gerapporteerde zelfeffectiviteit laag was: deelnemers achtten zich beperkt in staat om in te schatten of en wanneer het online delen van (specifieke) persoonsgegevens veilig is. Daarnaast gaven de meeste deelnemers aan de gevolgen van het onveilig online delen van persoonsgegevens ernstig te vinden en dat het veilig online delen van persoonsgegevens de kans op negatieve gevolgen verkleint. Wat betreft verantwoordelijkheid lieten de resultaten zien dat, in vergelijking met veilig wachtwoordgedrag, de deelnemers hier de verantwoordelijkheid meer bij websites, apps, en de overheid legden. Dit is mogelijk te verklaren door het feit dat mensen niet altijd controle (denken te) hebben over het al dan niet delen van persoonsgegevens online.

Vervolgens hebben we gekeken welke psychologische factoren het veilig online delen van persoonsgegevens (gedragsmaten, zelfrapportage gedrag) voorspelden. De resultaten van Studie 1 lieten zien dat van de onderzochte factoren met name zelfeffectiviteit en ernst belangrijke voorspellers waren 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 zelfeffectiviteit een belangrijke 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.

4.3.2 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.

4.3.2.1 Wachtwoorden

De resultaten van Studie 2 lieten zien dat onze interventie effectief was, in de zin dat deze leidde tot veiliger gedrag. Deelnemers die informatie over zelfeffectiviteit hadden ontvangen, al dan niet in combinatie met informatie over de ernst van risico's, maakten veiligere wachtwoorden aan 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.

Hoewel de interventie resulteerde in veiliger wachtwoordgedrag, vonden we geen effecten van de interventie op de interventie check metingen van ernst en zelfeffectiviteit. De relatief hoge ernst en zelfeffectiviteit scores in de controle conditie suggereren dat deelnemers zich al redelijk bewust waren van de ernst van risico's en dat ze een zeker mate van zelfeffectiviteit ervoeren.

Verder werden de specifieke risico's van onveilig wachtwoordgedrag als ernstig beoordeeld. Daarnaast erkenden deelnemers dat ze kwetsbaar zijn voor online criminaliteit als ze zwakke wachtwoorden gebruiken en het werd het gebruik van sterke wachtwoorden als een manier gezien om risico's te verminderen.

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 voorwaarden, of dat het wachtwoord persoonlijke informatie bevatte. We vonden bij de maat of het aangemaakte 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. Dit resultaat is in lijn met de resultaten op de ernst interventie check, die lieten zien dat oudere deelnemers het gevaarlijker achtten om zwakke wachtwoorden te gebruiken dan jongere deelnemers. 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. Dit is in lijn met de resultaten op de zelfeffectiviteit interventie check vragen, die lieten zien dat hoger opgeleide deelnemers een hogere zelfeffectiviteit rapporteerden dan lager opgeleide deelnemers.

4.3.2.2 Persoonsgegevens

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 deelnemers in de controle conditie vaker afzagen van deelname aan de verloting. Door niet mee te doen aan de verloting hoefden ze ook geen persoonsgegevens te delen.

Naast het effect van de interventie op veilig gedrag, waren er ook effecten van de interventie in de verwachte richting op de interventie check metingen van zelfeffectiviteit. Waargenomen zelfeffectiviteit was (deels) hoger in de zelfeffectiviteit condities dan in de controle conditie. Er was echter geen effect van de interventie op de interventie check meting van ernst. Net als bij het wachtwoordgedrag waren er relatief hoge ernst scores in de controle conditie, wat suggereert dat deelnemers zich al redelijk bewust waren van de ernst van risico's van het onveilig online delen van persoonsgegevens. Daarnaast erkenden deelnemers dat ze kwetsbaar zijn voor online criminaliteit als ze online onveilig omgaan met hun persoonsgegevens en werd het veilig online delen van persoonsgegevens als een manier gezien om risico's te verminderen.

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. Hoewel oudere deelnemers zich onveiliger gedroegen op het gebied van het online delen van persoonsgegevens, lieten de resultaten op de ernst interventie check maat (net zoals in Studie 1) zien dat oudere deelnemers het onveilig online delen van persoonsgegevens wel gevaarlijker achtten dan jongere deelnemers. De resultaten voor opleiding lieten zien dat hoe hoger opgeleid de deelnemers waren, hoe vaker ze niet-verplichte persoonsgegevens deelden.

4.4 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. Allereerst zullen we ingaan op specifieke beperkingen van Studies 1 en 2. Vervolgens zullen we een aantal algemene beperkingen van het huidige onderzoek bespreken, alsmede suggesties voor toekomstig onderzoek.

4.4.1 Specifieke beperkingen van Studie 1 en van Studie 2 en toekomstig onderzoek

Voor Studie 1 is het goed om op te merken dat deelnemers de vragenlijst altijd in één bepaalde volgorde invulden: de vragenlijst begon met de gedragsmaat voor persoonsgegevens, gevolgd door de gedragsmaat voor wachtwoorden, waarna de verdiepende vragen over onder andere de psychologische factoren volgden. Het zou kunnen dat er volgorde effecten zijn ontstaan, waar het wachtwoordgedrag beïnvloed werd door het invullen van de persoonsgegevens. Toekomstig onderzoek zou de verschillende maten in de studie kunnen counterbalancen (elke deelnemer ontvangt dan een andere volgorde) om zo eventuele volgorde effecten te ondervangen.

Om er in Studie 1 voor te zorgen dat alle deelnemers de ernst en kwetsbaarheid en responseffectiviteit evalueerden met dezelfde van dezelfde risico's van onveilig online gedrag in hun achterhoofd, gaven we deelnemers voorafgaand aan deze vragen informatie over de potentiële risico's. Dit zijn dus niet noodzakelijkerwijs de risico's zoals mensen ze zelf inschatten. Deze resultaten laten dus zien hoe deelnemers de risico's en responseffectiviteit beoordeelden nadat ze hier over geïnformeerd waren en deze saillant waren gemaakt. We kunnen niet concluderen hoe deelnemers zonder deze informatie deze risico's en de responseffectiviteit beoordeeld zouden hebben. Het feit dat we deelnemers informeerden over de risico's kan geleid hebben tot het hoger inschatten van de risico's. Dat maakt de controle conditie van Studie 2 waarin geen informatie over risico's werd verstrekt dus ook beperkt vergelijkbaar.

Hoewel we in Studie 1 kennis hebben gemeten om te kijken of dit een rol speelt bij veilig online gedrag, was deze meting niet optimaal. Het is moeilijk om kennis over online gedrag te meten met gesloten vragen zonder te veel weg te geven in de potentiële antwoorden. Wanneer open vragen worden gesteld of deelnemers worden geïnterviewd, is er wellicht een beter beeld te schetsen van de kennis van deelnemers. Dit is echter erg tijdsintensief, en dan is het nog steeds niet altijd duidelijk of deelnemers bijvoorbeeld bepaalde aspecten of risico's van veilig gedrag niet noemen omdat ze er niet vanaf weten, of dat ze deze vergeten te noemen. Naast dat kennis moeilijk te meten is, veranderen richtlijnen over online veilig gedrag ook voortdurend. Cybercriminelen vinden steeds nieuwe manier om mensen op te lichten, waarmee potentiële risico's of criteria voor veilig gedrag regelmatig veranderen. Toekomstig onderzoek zou kennis op een andere manier kunnen meten op basis van de laatste inzichten uit de literatuur en de praktijk, om zo beter te onderzoeken of kennis een rol speelt bij veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens.

Studie 2 liet mooie resultaten van de interventie zien op beide doelgedragingen, maar ook deze studie kent enkele beperkingen. Allereerst zien we dat hoewel de interventie resulteerde in veiliger online gedrag, de wachtwoorden in de interventie condities nog steeds zwak waren, en deelnemers nog steeds vaak al 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. In Sectie 4.5 doen we aanvullende suggesties voor interventies om online gedrag nog veiliger te maken.

Daarnaast richtte de ernst interventie in Studie 2 zich vooral op gevaren bij belangrijke accounts, zoals e-mail, bankapps, of webwinkel accounts. Het is waarschijnlijk dat het account waarvoor in Studie 2 een wachtwoord werd aangemaakt niet per se als belangrijk werd gezien. Uit de open vragen over de bevorderende en belemmerende factoren voor veilig wachtwoordgedrag bleek dat mensen onderscheid maken tussen belangrijke en minder belangrijke accounts (zie https://easy.dans.knaw.nl/ui/home). Sommige mensen gebruiken bijvoorbeeld vaker sterke wachtwoorden voor belangrijke accounts en minder sterke wachtwoorden voor minder belangrijke accounts. Toekomstig onderzoek zou onderscheid kunnen maken tussen belangrijke en onbelangrijke accounts, om te zien of specifieke interventies alleen bij een bepaalde type accounts effectief zijn.

Ten slotte is het belangrijk om te benadrukken dat hoewel de interventie effectief was in het bevorderen van veilig online gedrag, we vrijwel geen effect van de interventie op de interventie checks voor zelfeffectiviteit en ernst vonden. De informatie over zelfeffectiviteit leidde slechts beperkt tot een hogere zelfgerapporteerde zelfeffectiviteit, en de informatie gericht op de ernst van risico's van onveilig gedrag leidde niet tot hogere zelfgerapporteerde ernst. In Sectie 3.2.1.4 wordt hier al een mogelijk verklaring voor gegeven. De effectiviteit van de interventie op gedrag kan mogelijk verklaard worden door een activatie van de zelfeffectiviteit en ernst informatie. Deze informatie zit dan tijdelijk meer in het hoofd van de deelnemers, in plaats van dat de interventie de deelnemers daadwerkelijk nieuwe informatie geeft. Priming is een voorbeeld van zulke onbewuste gedragsverandering, waar mensen (tijdelijk) associaties kunnen vormen tussen informatie in één context en informatie of gedrag in een andere context (Chartrand & Bargh, 1996). Wellicht vond deze vorm van onbewuste gedragsverandering ook plaats in het huidige onderzoek. Als dit het geval is, dan is het relevant om te onderzoeken hoelang de interventie effectief blijft, en of de effecten op gedrag verdwijnen als mensen vaker aan dezelfde informatie worden blootgesteld. Toekomstig onderzoek zou de langetermijneffecten van de interventie kunnen toetsen om zo te zien of de huidige interventie alleen op korte termijn effectief is of ook een langdurig effect heeft.

4.4.2 Algemene beperkingen en toekomstig onderzoek

Als we kijken naar het onderzoek als geheel 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 van 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 bevatten. Wachtwoordgedrag in het dagelijks leven is bovendien ook complex. Mensen moeten niet alleen rekening houden met een sterk wachtwoord dat een hoge entropie heeft en geen bestaande woorden bevat, maar ze moeten er ook rekening mee houden dat ze verschillende wachtwoorden voor verschillende accounts aanmaken, dat het wachtwoord goed te onthouden is, en dat ze hun wachtwoord niet met anderen delen. Dat entropie in onze studies vrij centraal stond heeft te maken met dat dit een continue maat is, die goed meetbaar is binnen de beperkingen die we hadden binnen het onderzoek (bv. in verband met de ethiek van het onderzoek was het geen optie om de aangemaakte wachtwoorden te ontvangen en zelf te coderen op of ze bestaande woorden bevatten). Deze maat werd daarnaast ook gebruikt in het eerdere onderzoek door Van ’t Hoff-de Goede et al. (2019). 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. Deelnemers gaven inderdaad aan de betrokken partijen binnen het onderzoek (Markteffect, het externe bedrijf dat zogenaamde de verloting afhandelde en Universiteit Leiden) te vertrouwen (zie https://easy.dans.knaw.nl/ui/home). Daarnaast hadden de deelnemers wellicht kennis over de huidige privacyregels die het niet toelaten om gegevens van deelnemers verder te verspreiden zonder toestemming. Toch kan dit ook in het dagelijkse leven een rol spelen, dat deelnemers zich veilig wanen op de website van bijvoorbeeld een bank en ervan uitgaan dat dit soort organisaties de veiligheid wel op orde heeft. Ten slotte is het goed om, net als bij veilig wachtwoordgedrag, aan te geven dat het online delen van persoonsgegevens vaak complexer is dan hoe we dit in het huidige onderzoek hebben gemeten. We hebben in het huidige onderzoek beperkt onderscheid gemaakt tussen verschillende type persoonsgegevens, en 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. De context waarin gebruikers wordt gevraagd hun persoonsgegevens online te delen is dus erg belangrijk. De resultaten van Studie 1 lieten bijvoorbeeld zien dat de psychologische factoren uit ons onderzoeksmodel een sterkere voorspeller waren van het zelfgerapporteerde veilig online delen van persoonsgegevens als dit delen van persoonsgegevens plaatsvindt in de context van delen op websites dan in de context van delen op sociale media. 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.

De interventie voor het veilig online delen van persoonsgegevens in Studie 2 kent ook beperkingen. In de informatie over zelfeffectiviteit die de deelnemers lazen werd de deelnemers uitgelegd dat ze goed moeten kijken of de website veilig is. Dit is voor veel mensen echter helemaal niet makkelijk om te bepalen. Om zelfeffectiviteit te verhogen is het belangrijk om meer concrete handvatten te bieden om te bepalen of een website veilig is. Zo zouden mensen kunnen kijken naar het type URL, of er een hangslotsymbool te vinden is in de zoekbalk van de browser, of het taalgebruik op de website in orde is, of de domeinnaam logisch is en klopt bij de website en of contactgegevens en links op de website wel kloppen (Fraud-detector, 2022). Er is in Studie 2 voor gekozen om de interventie kort en krachtig te houden, zodat de deelnemers alle informatie voldoende zouden kunnen verwerken. Toekomstig onderzoek zou de zelfeffectiviteit echter verder kunnen verhogen door in de interventie betere handvatten te bieden voor hoe deelnemers kunnen bepalen of een website veilig is of niet. Dit zou men echter ook uit de handen van mensen kunnen nemen. Er zou kunnen worden nagedacht over hoe technologie kan helpen in de vorm van security by design. Websites en applicaties zouden zelf aanpassingen kunnen maken in de interface en lay-out, zodat mensen duidelijker kunnen zien of de website veilig is of niet.

Onze interventie was succesvol in het bevorderen van veiliger gedrag voor beide doelgedragingen. Toch is er nog steeds veel winst te behalen: het gedrag dat deelnemers in de studies vertoonden was nog steeds relatief onveilig. Toekomstig onderzoek zou zich nog kunnen richten op andere (deel)oorzaken van onveilig online gedrag. Zo lieten de resultaten van Studie 1 zien dat het niet kunnen onthouden van sterke wachtwoorden voor verschillende toepassingen een belangrijke belemmerende factor was voor veilig wachtwoordgedrag. Dat de sterkte van de aangemaakte wachtwoorden verbeterd is in de interventiecondities in Studie 2, hoeft niet te betekenen dat deelnemers het wachtwoord ook onthouden. In het dagelijks leven is het waarschijnlijk dat mensen een wachtwoord aanmaken dat ze kunnen onthouden, omdat ze herhaaldelijk toegang moeten hebben tot een website of account. We denken dat mensen redelijke kennis hebben over wat veilig wachtwoordgedrag inhoudt, maar dat ze het niet altijd vertonen omdat ze sterke, unieke wachtwoorden voor de vele accounts die ze hebben niet kunnen onthouden. Dit is gerelateerd aan zelfeffectiviteit van het *onthouden* van veilige wachtwoorden, waar de interventie in het huidige onderzoek zich richtte op zelfeffectiviteit van het *aanmaken* van veilige wachtwoorden. Toekomstig onderzoek zou zich kunnen richten op hoe gebruikers niet alleen wachtwoorden aanmaken die sterk en uniek zijn, maar die ook goed te onthouden zijn.

Een manier om sterke, unieke wachtwoorden aan te maken zonder dat deze zelf onthouden moeten worden, is door gebruik te maken van een wachtwoordmanager. Wachtwoordmanagers kunnen automatisch veilige, sterke wachtwoorden aanmaken voor gebruikers, die niet onthouden hoeven te worden, omdat de managers deze voor de gebruiker opslaan voor elke toepassing. Onderzoek heeft aangetoond dat mensen minder kwetsbaar zijn voor phishing en andere negatieve consequenties van onveilig wachtwoordgedrag, wanneer ze een wachtwoordmanager gebruiken (Gasti & Rasmussen, 2012). Het is om deze reden relevant om meer onderzoek te doen naar de bereidheid van mensen om wachtwoordmanagers te gebruiken, ook gezien het feit dat criteria voor veilige wachtwoorden steeds veranderen. Een deel van de deelnemers gaf in antwoorden over bevorderende factoren voor het gebruik van veilige wachtwoorden in Studie 1 aan dat ze graag

wachtwoordmanagers zouden wilden gebruiken en eenzelfde beeld komt naar voren in Studie 2 (zie Bijlage D). Uit de resultaten van Studie 1 en Studie 2 (zie Bijlage B en Bijlage D) blijkt echter ook dat deelnemers nog maar beperkt wachtwoordmanagers gebruiken en dat lage kennis, responseffectiviteit en zelfeffectiviteit en hoge responskosten hier mogelijk een rol in spelen. Eerder onderzoek liet ook zien dat de gebruiksvriendelijkheid van wachtwoordmanagers vaak ondermaats is (Seiler-Hwang et al., 2019) en dat is voor veel mensen een drempel om zich te verdiepen in wat een goede wachtwoordmanager is en hoe het werkt (Pearman et al., 2019). Toekomstig onderzoek zou zich kunnen richten op hoe deze drempels verlaagd kunnen worden zodat meer mensen gebruik gaan maken van wachtwoordmanagers.

Van alle psychologische factoren die we hebben onderzocht in Studie 1, hebben we op basis van de resultaten van Studie 1 en literatuur over gedragsverandering en veilig online gedrag ervoor gekozen om de interventie in Studie 2 te richten op de ernst van risico's van onveilig gedrag en zelfeffectiviteit. Studie 2 liet zien dat dit een goede keuze was, maar dat neemt niet weg dat 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 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.

4.5 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 kunnen wel een basis kan bieden voor het ontwikkelen van interventies.

Naast dat het huidige onderzoek laat zien dat interventies gericht op ernst van risico's in combinatie met zelfeffectiviteit effectief kunnen zijn, laat 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. Naast dat een wachtwoordmanager mensen suggesties voor sterke en unieke wachtwoorden geeft, neemt dit ook het probleem weg dat sterke en unieke wachtwoorden niet goed te onthouden zijn. De interventies zouden zich vooral moeten richten op het verlagen van de drempel voor mensen om zich te verdiepen in hoe wachtwoordmanagers werken en om wachtwoordmanagers daadwerkelijk te gebruiken. Hierbij is het belangrijk om eerst de belangrijkste belemmerende en bevorderende factoren voor dit specifieke doelgedrag verder in kaart te brengen. In zowel Studie 1 als Studie 2

hebben we onze deelnemers vragen gesteld over wachtwoordmanagers, de antwoorden op deze vragen kunnen gebruikt worden voor vervolgonderzoek (zie Bijlage B en Bijlage D).

Daarnaast kan de geteste interventie (deels) goed gecombineerd kunnen worden met andere interventietechnieken. Er kan bijvoorbeeld ook veel bereikt worden door in te zetten op techniek of aanpassingen van 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. Ook 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, en 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 de 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 gedrag 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, aanpassingen van de gebruikersomgeving en aanpassingen in wetgeving.

5. Literatuur

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40-46.

Addae, J. H., Brown, M., Sun, X., Towey, D., & Radenkovic, M. (2017). Measuring attitude towards personal data for adaptive cybersecurity. *Information & Computer Security, 25*(5), 560-579. https://doi.org/10.1108/ICS-11-2016-0085

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information & Computer Security, 26*(3), 306-326. 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

Aurigemma, S., Mattson, T., & Leonard, L. N. (2019). Evaluating the core and full protection motivation theory nomologies for the voluntary adoption of password manager applications. *AIS Transactions on Replication Research, 5*(1), 1-21. https://doi.org/10.17705/1atrr.00035

Autoriteit Persoonsgegevens, (z.d.). Wat zijn persoonsgegevens? Geraadpleegd in november 2021, van https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens

Barton, B. F., & Barton, M. S. (1984). User-friendly password methods for computer-mediated information systems. *Computers & Security, 3*(3), 186-195. https://doi.org/10.1016/0167-4048(84)90040-3

Beldad, A., De Jong, M., & Steehouder, M. (2011). I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior, 27*(6), 2233-2242. https://doi.org/10.1016/j.chb.2011.07.002

Bigsby, E., & Albarracín, D. (2022). Self-and response efficacy information in fear appeals: A meta-analysis. *Journal of Communication, 72*(2), 241-263. https://doi.org/10.1093/joc/jqab048

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior, 87*, 87-97. https://doi.org/10.1016/j.chb.2018.05.023

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

Borwell, J., Jansen, J., & Stol, W. (2021). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review, 18*(2), 213-234. https://doi.org/10.1177/0894439320983828

Brands, J., & van Wilsem, J. (2021). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology, 18*(2), 213-234. https://doi.org/10.1177/1477370819839619

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

CBS (2021a). Bevolking; geslacht, leeftijd en burgerlijke staat [data set]. Geraadpleegd op 3 mei 2022, van https://opendata.cbs.nl/#/CBS/nl/dataset/03759ned/table?dl=39E0B

CBS (2021b). Internettoegang en internetactiviteiten; persoonskenmerken [data set]. Geraadpleegd op 3 mei 2022, van https://www.cbs.nl/nl-nl/cijfers/detail/84888NED

Chartrand, T. L., & Bargh, J. A. (1996). Automatic activation of impression formation and memorization goals: Nonconscious goal priming reproduces effects of explicit task instructions. *Journal of Personality and Social Psychology, 71*, 464-478. https://doi.org/10.1037/0022-3514.71.3.464

Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*(5), 987-995. https://doi.org/10.1016/j.chb.2010.02.012

Christofides, E., Muise, A., & Desmarais, S. (2012). Hey mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science, 3*(1), 48-54. https://doi.org/10.1177/1948550611408619

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

Cohen, J. (1988). *The effect size. Statistical power analysis for the behavioral sciences.* (2e editie) Abingdon-on-Thames: Routledge Academic. https://doi.org/10.4324/9780203771587

Consumentenbond (2021). Datalekken: de gevaren en wat moet je doen? Geraadpleegd op 5 november 2021, van https://www.consumentenbond.nl/veilig-internetten/datalekken-de-gevaren-en-wat-moet-je-doen

Consumentenbond (2021). Wachtwoord maken en onthouden. Geraadpleegd in april 2022, van https://www.consumentenbond.nl/internet-privacy/wachtwoord-onthouden

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, 21*(2), 343-357. https://doi.org/10.1007/s10796-017-9755-1

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology, 41*(8) 1-13. https://doi.org/10.1080/0144929x.2021.1905066

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

Dhamija, R., & Perrig, A. (2000, juni). Déjà-vu: A user study. Using images for authentication. In *Proceedings of the 9th USENIX Security Symposium*. Denver, Colorado, Verenigde Staten.

Geraadpleegd van https://www.usenix.org/legacy/publications/library/proceedings/sec2000/full_papers/dhamija/dhamija.pdf 45-48.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007, oktober). Behavioral response to phishing risk. In *Proceedings of the Anti-phishing Working Groups 2nd Annual eCrime Researchers Summit,* 37-44. https://doi.org/10.1145/1299015.1299019

Dupuis, M., Jennings, A., & Renaud, K. (2021, oktober). Scaring people is not enough: an examination of fear appeals within the context of promoting good password hygiene. In *Proceedings of the 22st Annual Conference on Information Technology Education,* 35-40. https://doi.org/10.1145/3450329.3476862

Dupuis, M., & Renaud, K. (2021). Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology, 23*(3), 265-284. https://doi.org/10.1007/s10676-020-09560-0

Elhai, J. D., & Hall, B. J. (2016). Anxiety about internet hacking: Results from a community sample. *Computers in Human Behavior, 54*, 180-185. https://doi.org/10.1016/j.chb.2015.07.057

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

Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security, 94*, 1-18. https://doi.org/10.1016/j.cose.2020.101862

Fraud detector (2022). Checklist om de veiligheid en betrouwbaarheid van een website te beoordelen. Geraadpleegd in juni 2022, van https://fraud-detector.nl/checklist-veiligheid-en-betrouwbaarheid-van-een-website-beoordelen

Gasti, P., & Rasmussen, K. B. (2012, September). On the security of password manager database formats. In *European Symposium on Research in Computer Security,* 770-787. https://doi.org/10.1007/978-3-642-33167-1_44

Gaw, S., & Felten, E. W. (2006, July). Password management strategies for online accounts. In *Proceedings of the Second Symposium on Usable Privacy and Security,* 44-55. https://doi.org/10.1145/1143120.1143127

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

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics, 133*(1), 111-123. https://doi.org/10.1007/s10551-014-2346-x

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30*, 1-19. https://doi.org/10.1016/j.intmar.2014.10.001

Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications, 57*, 1-9. https://doi.org/10.1016/j.jisa.2020.102710

Horowitz, A. S. (2001). Top 10 security mistakes. *Computerworld, 35*(28), 38-38.

Howell, C. J. (2021). *Self-protection in cyberspace: Assessing the processual relationship between thoughtfully reflective decision making, protection motivation theory, cyber hygiene, and victimization.* University of South Florida.

Hsu, M. H., Ju, T. L., Yen, C. H., & Chang, C. M. (2007). Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *International Journal of Human-Computer Studies, 65*(2), 153-169. https://doi.org/10.1016/j.ijhcs.2006.09.003

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

Jansen, J., & Van Schaik, P. (2016, juli). Understanding precautionary online behavioural intentions: A comparison of three models. In *Proceedings of the Tenth International Symposium on Human Aspects of Information Security and Asssurance (HAISA),* 1-11.

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development, 20*(2), 196-213. https://doi.org/10.1080/02681102.2013.814040

Keepass (z.d.). Password quality estimation. Geraadpleegd op 26 april 2022, van https://keepass.info/help/kb/pw_quality_est.html

Kok, G., Peters, G. J. Y., Kessels, L. T., Ten Hoor, G. A., & Ruiter, R. A. (2018). Ignoring theory and misinterpreting evidence: the false belief in fear appeals. *Health Psychology Review, 12*(2), 111-125. https://doi.org/10.1080/17437199.2017.1415767

Kovačević, A., & Radenković, S. D. (2020). SAWIT—Security awareness improvement tool in the workplace. *Applied Sciences, 10*(9), 1-13. ps://doi.org/10.3390/app10093065

Lewis, J. (2018). *Economic impact of cybercrime, no slowing down.* The Center for Strategic and International Studies. Geraadpleegd van https://www.csis.org/analysis/economic-impact-cybercrime

Meter, D. J., & Bauman, S. (2015). When sharing is a bad idea: the effects of online social networking engagement and sharing passwords with friends on cyberbullying involvement. *Cyberpsychology Behavior and Social Networking, 18*(8), 437-442. https://doi.org/10.1089/cyber.2015.0081

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.

Norman, P., Boer, H., Seydel, E. R., & Mullan, B. (2005). Protection motivation theory. In M. Connor and P. Norman (eds) *Predicting and Changing Health Behavior: Research and Practice with Social Cognition Models*, 70-106. Milton Keynes, Engeland: Open University Press.

Notoatmodjo, G., & Thomborson, C. (2009, januari). Passwords and perceptions. In *Proceedings of the Seventh Australasian Conference on Information Security* (AICS 2009). Wellington, Nieuw Zeeland. Geraadpleegd van https://www.cs.auckland.ac.nz/~cthombor/Pubs/IdMgmt/gno09.pdf

Ovelgönne, M., Dumitraş, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the relationship between human behavior and susceptibility to cyberattacks: a data-driven approach. *ACM Transactions on Intelligent Systems and Technology, 8*(4), 1-25. https://doi.org/10.1145/2890509

Pearman, S., Zhang, S. A., Bauer, L., Christin, N., & Cranor, L. F. (2019, augustus). Why people (don't) use password managers effectively. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security* (SOUPS 2019), Santa Clara, CA, Verenigde Staten.

Peters, G.-J. Y, Ruiter, R. A. C. & Kok, G. (2012). Threatening communication: A critical re-analysis and a revised meta-analytic test of fear appeal theory. *Health Psychology Review, 7*(1), 8-31. https://doi.org/10.1080/17437199.2012.703527

Peters, G. J. Y., Ruiter, R. A., Ten Hoor, G. A., Kessels, L. T., & Kok, G. (2018). Towards consensus on fear appeals: a rejoinder to the commentaries on Kok, Peters, Kessels, ten Hoor, and Ruiter (2018). *Health Psychology Review, 12*(2), 151-156. https://doi.org/10.1080/17437199.2018.1454846

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *Sage Open, 11*(1). http://doi.org/10.1177/21582440211000049

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice, 44*(1), 63-82. https://doi.org/10.1007/s12103-018-9447-5

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. https://doi.org/10.1080/00223980.1975.9915803

Ruiter, R. A. C., Abraham, C. & Kok, G. (2001). Scary warnings and rational precautions: A review of psychology of fear appeals. *Psychology & Health, 16*(6), 613-630. https://doi.org/10.1080/08870440108405863

Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems, 37*(3), 723-757. https://doi.org/10.1080/07421222.2020.1790187

Seiler-Hwang, S., Arias-Cabarcos, P., Marín, A., Almenares, F., Díaz-Sánchez, D., & Becker, C. (2019, november). "I don't see why I would ever want to use it": analyzing the usability of popular smartphone password managers. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security.* Londen, Verenigd Koninkrijk. https://doi.org/10.1145/3319535.3354192

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. and Downs, J. (2010, april). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the CHI Conference on Human Factors in Computing Business*. Atlanta, GA, Verenigde Staten. 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,* 199-207. https://doi.org/10.1016/j.chb.2015.01.046

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour & Information Technology, 29*(3), 233-244. https://doi.org/10.1080/01449290903121386

Tamrin, S. I., Norman, A. A., & Hamid, S. (2021). Intention to share: The relationship between cybersecurity behaviour and sharing specific content in Facebook. *Information Research: An International Electronic Journal, 26*(1). https://doi.org/10.47989/irpaper894

Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., Jacobs, S., Wilson, K., & Albarracín, D. (2015). Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin*, *141*(6), 1178. https://doi.org/10.1037/a0039729

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 123*, 29-39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Van der Kleij, R., Wijn, R., & Hof, T. (2020). An application and empirical test of the capability opportunity motivation-behaviour model to data leakage prevention in financial organizations. *Computers & Security, 97,* 101970-101976. https://doi.org/10.1016/j.cose.2020.101970

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 ’t Hoff-de Goede, S., van der Kleij, R., van de Weijer, S., & Leukfeldt, R. (2019). Hoe veilig gedragen wij ons online? *Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).* Geraadpleegd in november 2021, van https://repository.wodc.nl/handle/20.500.12832/2433

Veiliginternetten (z.d.) Privacyverklaring generator. Geraadpleegd op 30 april 2021, van https://veiliginternetten.nl/privacyverklaring-generator/generate/

Witte, K. & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education and Behavior, 27*(5)*,* 591-615. https://doi.org/10.1177/109019810002700506

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. *TNO Publications*, 30-32. Geraadpleegd van http://resolver.tudelft.nl/uuid:225a4bdb-bed8-43db-a026-4962f05b7a6d

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 18*(8), 1-16. https://doi.org/10.12700/aph.18.8.2021.8.4

Bijlage A: Studie 1: Resultaten gedragsmaten uitgesplitst voor wachtwoordmanager gebruik

Een deel van de deelnemers (10.4 %) gaf aan een wachtwoordmanager gebruikt te hebben bij het aanmaken van het wachtwoord in Studie 1. In deze bijlage geven we de resultaten weer voor veilig wachtwoordgedrag (gedragsmaten), uitgesplitst voor deelnemers die wel vs. geen wachtwoordmanager hebben gebruikt.

Sterkte wachtwoorden: entropie

Tabellen A1 en A2 geven de resultaten weer voor de sterkte van het aangemaakte wachtwoord, uitgesplitst voor het gebruik van een wachtwoordmanager bij het aanmaken van het wachtwoord. De resultaten laten zien dat deelnemers die aangaven een wachtwoordmanager te hebben gebruikt bij het aanmaken van het wachtwoord, een sterker wachtwoord hebben aangemaakt dan deelnemers die geen wachtwoordmanager hebben gebruikt. Van de deelnemers die hebben aangegeven een wachtwoordmanager te hebben gebruikt maakte 50.0% een wachtwoord aan dat zowel uit minstens 12 tekens, als uit minstens 1 kleine letter, 1 hoofdletter, 1 speciaal teken en 1 cijfer bestond (niet in tabel). Bij de deelnemers die geen wachtwoordmanager hebben gebruikt was dat 9.7% (niet in tabel).

Tabel A1

Wachtwoorden gedragsmaat: sterkte aangemaakte wachtwoorden uitgedrukt in entropie, uitgesplitst voor wachtwoordmanager gebruik

	Wachtwoordmanager gebruikt bij het aanmaken van het wachtwoord					
	Ja (*N* = 104)		Nee (*N* = 894)		Totaal (*N* = 998)	
	N	%	*N*	%	*N*	%
Zeer zwak (0.00-63.99 bits)	27	26.0	601	67.2	628	62.9
Zwak: (64.00-79.99 bits)	6	5.8	203	22.7	209	20.9
Gemiddeld: (80.00-111.99 bits)	30	28.8	73	8.2	103	10.3
Sterk: (112.00-127.99 bits)	2	1.9	7	0.8	9	0.9
Zeer sterk: (≥128 bits)	39	37.5	10	1.1	49	4.9

Tabel A2

Wachtwoorden gedragsmaat: kenmerken aangemaakte wachtwoorden uitgesplitst voor wachtwoordmanager gebruik

	Wachtwoordmanager gebruikt bij het aanmaken van het wachtwoord					
	Ja (*N* = 104)		Nee (*N* = 894)		Totaal (*N* = 998)	
	M	*SD*	*M*	*SD*	*M*	*SD*
Entropie	96.29	38.21	56.38	21.92	60.54	27.02
Lengte	15.32	5.31	9.59	3.12	10.18	3.83
Kleine letters	9.04	5.21	5.86	3.00	6.19	3.43
Hoofdletters	2.79	3.10	0.87	0.95	1.07	1.46
Speciale tekens	1.11	1.09	0.46	0.78	0.52	0.84
Cijfers	2.38	1.79	2.40	2.01	2.40	1.99

Unieke wachtwoorden

Tabel A3 geeft de resultaten weer voor de vraag of deelnemers het aangemaakte wachtwoord ook gebruiken voor andere accounts, uitgesplitst voor het gebruik van een wachtwoordmanager bij het aanmaken van het wachtwoord. De resultaten suggereren dat deelnemers die aangaven een wachtwoordmanager te hebben gebruikt bij het aanmaken van het wachtwoord, iets vaker een uniek wachtwoord hebben gebruikt (i.e., er in mindere mate sprake was van hergebruik van een wachtwoord) dan deelnemers die geen wachtwoordmanager hebben gebruikt.

Tabel A3

Wachtwoorden gedragsmaat: unieke wachtwoorden, uitgesplitst voor wachtwoordmanager gebruik

Aangemaakte wachtwoord ook in gebruik voor andere accounts	Wachtwoordmanager gebruikt bij het aanmaken van het wachtwoord		
	Ja (*N* = 104)	Nee (*N* = 894)	Totaal (*N* = 998)
Ja	14.4%	23.3%	22.3%
Nee	78.8%	65.8%	67.1%
Zeg ik liever niet	6.7%	11.0%	10.5%

Bovenstaande tabellen laten ook zien dat de vraag of er een wachtwoordmanager was gebruikt bij het aanmaken van het wachtwoord door een deel van de deelnemers wellicht niet helemaal goed begrepen is. Wanneer een wachtwoord wordt aangemaakt middels een wachtwoordmanager is dit per definitie een uniek en sterk wachtwoord. Als het wachtwoord vaker wordt gebruikt, of een lage entropie heeft, kan dit een teken zijn dat de deelnemer het wachtwoord bijvoorbeeld alleen heeft

opgeslagen in een wachtwoordmanager, of de vraag op een andere manier verkeerd begrepen heeft.

Bijlage B: Studie 1: Resultaten wachtwoordmanager vragen

In deze bijlage beschrijven we de resultaten voor de wachtwoordmanager vragen in Studie 1. Tabel B1 geeft de resultaten weer voor kennis. Voordat deelnemers de kennisvraag beantwoordden lazen ze de volgende informatie: “Met een wachtwoordmanager kunt u wachtwoorden veilig opslaan. Een wachtwoordmanager kan ook suggesties doen voor het aanmaken van sterke wachtwoorden die moeilijk te raden zijn.". De resultaten lieten zien dat een minderheid van de deelnemers aangaf zowel gehoord te hebben van een wachtwoordmanager als er veel vanaf te weten (18.0%).

Tabel B1

Kennis wachtwoordmanager

	Had u voorafgaand aan dit onderzoek al weleens gehoord van een wachtwoordmanager?	
	N	%
Nee	297	29.8
Ja, maar ik weet er weinig vanaf	521	52.2
Ja, en ik weet er veel vanaf	180	18.0

Noot. N = 998.

Deelnemers beantwoordden ook twee vragen over het gebruik van een wachtwoordmanager. Tabel B2 geeft de resultaten weer. De resultaten laten zien dat meerderheid van de deelnemers aangaf nooit gebruik te maken van een wachtwoordmanager (63.7% en 62.8%, respectievelijk).

Tabel B2

Gebruik wachtwoordmanager

	Maakt u gebruik van een wachtwoordmanager voor het opslaan van wachtwoorden?		Maakt u gebruik van de suggesties voor sterke wachtwoorden van uw wachtwoordmanager?	
	N	%	*N*	%
Nooit	636	63.7	627	62.8
Soms	237	23.7	276	27.7
Altijd	125	12.5	95	9.5

Noot. N = 998.

Vervolgens beantwoordden deelnemers een open vraag waarin hen werd gevraagd hun antwoord op de eerste stelling in Tabel B2 toe te lichten ("U heeft aangegeven dat u nooit/soms/altijd een wachtwoordmanager gebruikt voor het opslaan van wachtwoorden. Kunt u toelichten waarom dit zo is?). Om de antwoorden te analyseren heeft het onderzoeksteam codeerschema's gemaakt. Net als bij de codering van belemmerende en bevorderende factoren (zie Sectie 2.2.1.5) vormden de psychologische factoren uit het onderzoeksmodel (zie Figuur 1) de basis van de schema's en werd er binnen categorieën op basis van een steekproef uit de antwoorden subcategorieën gemaakt. Vervolgens werd door een andere onderzoeker bij elk antwoord genoteerd in welke categorie dit antwoord terugkwam. Een steekproef hiervan werd steeds door een tweede onderzoeker apart gecodeerd, waarbij afgestemd kon worden over twijfelgevallen en de mate van overeenkomst gecheckt kon worden. We beschrijven hier de hoofdlijnen van de bevindingen uit de open vragen. De gedetailleerde codeerschema's en de gecodeerde antwoorden van deelnemers zijn hier beschikbaar: https://easy.dans.knaw.nl/ui/home.

Toelichting deelnemers die nooit een wachtwoordmanager gebruiken voor het opslaan van wachtwoorden

De antwoorden van deelnemers die aangaven nooit een wachtwoordmanager te gebruiken (*N* = 636, 682 coderingen) lieten zien dat een gebrek aan kennis hierbij een belangrijke rol speelt: 43.1% van de antwoorden viel binnen deze categorie. Deelnemers gaven aan niet of weinig te weten over wachtwoordmanagers (35.9% van de antwoorden: "Onbekend mee", "Weet niet wat het is"), er nooit mee bezig geweest te zijn (5.9% van de antwoorden: "Ik ben daar niet te bewust mee bezig"), en niet te weten welke managers goed zijn (1.3% van de antwoorden: "Niet bekend mee welke het beste is"). Verder ging 12.5% van de antwoorden over responseffectiviteit. Deelnemers gaven aan dat het gebruik van wachtwoordmanagers niet per se leidt tot een kleinere kans op negatieve gevolgen en dat wachtwoordmanagers niet per se veilig zijn ("Als die gehackt wordt ben je nog verder van huis", "Zijn die wel te vertrouwen of ook van iemand met valse intenties?"). Verder ging 7.9% van de antwoorden over zelfeffectiviteit als belemmerende factor ("Te ingewikkeld", "Ik ben een digibeet") en 6.6% van de antwoorden over responskosten als belemmerende factor ("Te veel gedoe", "Kost geld").

Toelichting deelnemers die soms een wachtwoordmanager gebruiken voor het opslaan van wachtwoorden

De antwoorden van deelnemers die aangaven soms een wachtwoordmanager te gebruiken (*N* = 237, 257 coderingen) lieten zien dat responskosten hierbij een belangrijke rol spelen: 36.2% van de antwoorden viel binnen deze categorie. Het merendeel van de antwoorden wees in de richting dat wachtwoordmanagers tijd en moeite besparen (19.8% van de antwoorden: "Handig", "Dat is makkelijk"). Een minderheid van de antwoorden wees in de richting dat wachtwoordmanagers juist gepaard gaan met hoge responskosten, waarbij met name genoemd werd dat ze niet te gebruiken zijn op alle apparaten (4.7% van de antwoorden: "Het wachtwoord dat ik op mijn Iphone laat aanmaken, wordt niet onthouden op mijn laptop"). Verder ging 21.8% van de antwoorden over zelfeffectiviteit. Het merendeel van de antwoorden wees in de richting dat wachtwoordmanagers problemen met zelfeffectiviteit adresseren, en dan met name het probleem dat deelnemers wachtwoorden niet kunnen onthouden (19.5% van de antwoorden: "Dan hoef ik het niet zelf te

onthouden", "Voor het eenvoudig onthouden"). Tenslotte ging 12.5% van de antwoorden over responseffectiviteit, waarbij het merendeel van de antwoorden in de richting wees dat wachtwoordmanagers leiden tot een kleinere kans op negatieve gevolgen (11.3% van de antwoorden: "Lijkt mij veiliger", "Omdat het veiliger is").

Toelichting deelnemers die altijd een wachtwoordmanager gebruiken voor het opslaan van wachtwoorden

De antwoorden van deelnemers die aangaven altijd een wachtwoordmanager te gebruiken (*N* =125, 164 coderingen) lieten zien dat zelfeffectiviteit hierbij een belangrijke rol speelt: 36.6% van de antwoorden viel binnen deze categorie. Deelnemers gaven aan dat wachtwoordmanagers hen helpen om wachtwoorden te onthouden (29.3% van de antwoorden: "Omdat ik al die verschillende wachtwoorden niet kan onthouden"). Verder ging 32.3% van de antwoorden over responskosten. Deelnemers gaven aan dat het gebruik van een wachtwoordmanager tijd en moeite bespaart (26.8% van de antwoorden: "Makkelijk", "Als je goed met wachtwoorden om wilt omgaan is dat het gemakkelijkst"). Ten slotte ging 22.6% van de antwoorden over responseffectiviteit. Deelnemers gaven aan dat het gebruik van een wachtwoordmanager leidt tot een kleinere kans op negatieve gevolgen ("Veiliger", "Het is een simpele manier om mijn veiligheid online te verbeteren").

Welke wachtwoordmanager gebruiken deelnemers

Ter afsluiting van het vragenblok over wachtwoordmanagers beantwoordden deelnemers die aan hadden gegeven soms of altijd een wachtwoordmanager te gebruiken voor het opslaan van wachtwoorden de volgende open vraag: "Welke wachtwoordmanager(s) gebruikt u?". Om de antwoorden te coderen heeft het onderzoeksteam een codeerschema gemaakt waarin onderscheid is gemaakt tussen verschillende typen wachtwoordmanagers. De gedetailleerde codeerschema's en de resultaten van de analyses zijn hier beschikbaar: https://easy.dans.knaw.nl/ui/home.

De resultaten (*N* = 362, 392 coderingen) lieten zien dat ongeveer een derde van de antwoorden (27.3% van de antwoorden) wachtwoordmanagers van partijen zoals Lastpass, Keepass en 1 Password betrof. Een vergelijkbaar deel van antwoorden ging over wachtwoordmanagers die in de categorie "browser" vallen (23.7% van de antwoorden): het gaat hierbij met name om Google/Chrome (20.9% van de antwoorden). Ten slotte gaven deelnemers aan zogenaamde "Apparaat gebonden managers" te gebruiken (20.9% van de antwoorden), zoals standaard geïnstalleerde wachtwoordmanagers op smartphones en andere apparaten.

Bijlage C: Studie 2a: Resultaten gedragsmaten uitgesplitst voor wachtwoordmanager gebruik

Een deel van de deelnemers (16.6 %) gaf aan een wachtwoordmanager gebruikt te hebben bij het aanmaken van het wachtwoord in Studie 2. In deze bijlage geven we de resultaten voor wachtwoordgedrag weer (gedragsmaten), uitgesplitst voor deelnemers die wel vs. geen wachtwoordmanager hebben gebruikt.

Sterkte wachtwoorden (entropie)

Tabellen C1 en C2 geven de resultaten weer voor de sterkte van het aangemaakte wachtwoord, uitgesplitst voor het gebruik van een wachtwoordmanager bij het aanmaken van het wachtwoord. De resultaten lieten zien dat deelnemers die aangaven een wachtwoordmanager te hebben gebruikt een sterker wachtwoord hebben aangemaakt dan deelnemers die geen wachtwoordmanager hebben gebruikt. Van de deelnemers die hebben aangegeven een wachtwoordmanager te hebben gebruikt maakte over de condities heen 33.7% een wachtwoord aan dat zowel uit minstens 12 tekens, als uit minstens 1 kleine letter, 1 hoofdletter, 1 speciaal teken en 1 cijfer bestond (niet in tabel). Bij de deelnemers die geen wachtwoordmanager hebben gebruikt was dat over condities heen 22.5% (niet in tabel). De resultaten lieten verder, zoals verwacht, zien dat de interventie alleen invloed had op de sterkte van de aangemaakte wachtwoorden van deelnemers die geen wachtwoordmanager hebben gebruikt.

Tabel C1

Wachtwoord gedragsmaat: sterkte aangemaakte wachtwoorden (uitgedrukt in entropie) als functie van Conditie en wachtwoordmanager gebruik

	Conditie				
	Controle *M* (*SD*)	Ernst *M* (*SD*)	Zelfeffectiviteit *M* (*SD*)	Ernst + zelfeffectiviteit *M* (*SD*)	ANOVA
Wachtwoordmanager	(*N* = 33) 87.88[a] (31.17)	(*N* = 46) 93.95[a] (44.97)	(*N* = 51) 90.28[a] (32.71)	(*N* = 48) 100.81[a] (31.21)	*F* = 1.09, *p* = .356
Geen wachtwoordmanager	(*N* = 206) 53.93[a] (20.77)	(*N* = 235) 65.51[b] (27.92)	(*N* = 248) 71.63[bc] (27.07)	(*N* = 208) 69.83[c] (23.37)	*F* = 21.50, *p* < .001, η_p^2 = .07
Totaal	(*N* = 239) 58.62[a] (25.29)	(*N* = 281) 70.16[b] (32.98)	(*N* = 299) 74.81[c] (28.92)	(*N* = 256) 75.64[c] (27.75)	*F* = 18.20, *p* < .001, η_p^2 = .05

Noot. Per rij verschillen gemiddelden met een verschillende superscript letter statistisch significant van elkaar op *p* < .05 (Tukey HSD posthoc toetsen).

Tabel C2

Wachtwoord gedragsmaat: Bestaat het wachtwoord uit minstens 12 tekens, minstens 1 kleine letter, 1 hoofdletter, 1 speciaal teken en 1 cijfer? als functie van Conditie en wachtwoordmanager gebruik

	Conditie (%)			
	Controle	Ernst	Zelfeffectiviteit	Ernst + zelfeffectiviteit
Wachtwoordmanager	*N* = 33	*N* = 46	*N* = 51	*N* = 48
Ja	30.3[a]	28.3[a]	35.3[a]	39.6[a]
Nee	69.7[a]	71.7[a]	64.7[a]	60.4[a]
Geen wachtwoordmanager	*N* = 206	*N* = 235	*N* = 248	*N* = 208
Ja	8.7[a]	18.7[b]	30.6[c]	30.8[c]
Nee	91.3[a]	81.3[b]	69.4[c]	69.2[c]
Totaal	*N* = 239	*N* = 281	*N* = 299	*N* = 256
Ja	11.7[a]	20.3[b]	31.4[c]	32.4[c]
Nee	88.3[a]	79.7[b]	68.6[c]	67.6[c]

Noot. Geen wachtwoordmanager: χ^2 (3) = 1.58, *p* = .664. Wachtwoordmanager: χ^2 (3) = 41.86, *p* < .001. Totaal: χ^2 (3) = 40.42, *p* < .001. Per rij verschillen percentages met een verschillende superscript letter significant van elkaar op *p* < .05 (*Z* posthoc proportietoetsen).

Tabel C3 geeft de resultaten weer voor of het aangemaakte wachtwoord persoonlijke informatie bevatte, uitgesplitst voor Conditie en of deelnemers een wachtwoordmanager hebben gebruikt bij het aanmaken van het wachtwoord. De resultaten lieten zien dat van de deelnemers die aangaven een wachtwoordmanager te hebben gebruikt, over condities heen 16.3% ook aangaf dat het wachtwoord persoonlijke informatie bevatte (vs. 80.9% “Nee” en 2.8% “Zeg ik liever niet”). Bij de deelnemers die aangaven geen wachtwoordmanager te hebben gebruikt was dit over condities heen 23.5% (vs. 69.5% “Nee” en 7.0% “Wil ik niet zeggen”). De resultaten lieten verder, zoals verwacht, zien dat de interventie met name invloed had op de aangemaakte wachtwoorden van deelnemers die geen wachtwoordmanager hebben gebruikt.

Tabel C3

Aangemaakte wachtwoord bevat persoonlijke informatie als functie van Conditie en wachtwoordmanager gebruik

	Conditie (%)			
	Controle	Ernst	Zelfeffectiviteit	Ernst + zelfeffectiviteit
Wachtwoordmanager	*N* = 33	*N* = 46	*N* = 51	*N* = 48
Ja	24.2^{a}	13.0^{ab}	21.6^{ab}	8.3^{b}
Nee	69.7^{a}	84.8^{ab}	74.5^{ab}	91.7^{b}
Zeg ik liever niet	6.1^{a}	2.2^{a}	3.9^{a}	0.0^{a}
Geen wachtwoordmanager	*N* = 206	*N* = 235	*N* = 248	*N* = 208
Ja	32.0^{a}	26.8^{a}	19.0^{b}	16.8^{b}
Nee	61.7^{a}	66.4^{ab}	73.8^{bc}	75.5^{c}
Zeg ik liever niet	6.3^{a}	6.8^{a}	7.3^{a}	7.7^{a}
Totaal	*N* = 239	*N* = 281	*N* = 299	*N* = 256
Ja	31.0^{a}	24.6^{ab}	19.4^{bc}	15.2^{c}
Nee	62.8^{a}	69.4^{ab}	73.9^{bc}	78.5^{c}
Zeg ik liever niet	6.3^{a}	6.0^{a}	6.7^{a}	6.3^{a}

Noot. Wachtwoordmanager χ^2 (6) = 8.74, p = .189. Geen wachtwoordmanager χ^2 (6) = 17.80, p = .007. Totaal χ^2 (6) = 20.36, p = .002. Per rij verschillen percentages met een verschillende superscript letter significant van elkaar op $p < .05$ (*Z* posthoc proportietoetsen).

Bovenstaande tabellen laten ook zien dat de vraag of er een wachtwoordmanager was gebruikt bij het aanmaken van het wachtwoord door een deel van de deelnemers wellicht niet helemaal goed begrepen is. Wanneer een wachtwoord wordt aangemaakt middels een wachtwoordmanager is dit per definitie een sterk wachtwoord dat geen persoonlijke gegevens bevat. Als het wachtwoord niet voldoet aan voorwaarden voor sterke wachtwoorden of persoonlijke gegevens bevat, kan dit een

teken zijn dat de deelnemer het wachtwoord bijvoorbeeld alleen heeft opgeslagen in een wachtwoordmanager, of de vraag op een andere manier verkeerd begrepen heeft.

Bijlage D: Studie 2a: Resultaten wachtwoordmanager vragen

In deze bijlage beschrijven we de resultaten voor de wachtwoordmanager vragen in Studie 2a. Tabel D1 geeft de resultaten weer voor kennis. Voordat deelnemers de kennisvraag beantwoordden lazen ze de volgende informatie: “Met een wachtwoordmanager kunt u wachtwoorden veilig opslaan. Een wachtwoordmanager kan ook suggesties doen voor het aanmaken van sterke wachtwoorden die moeilijk te raden zijn.". De resultaten laten zien dat een minderheid van de deelnemers zowel gehoord heeft van een wachtwoordmanager als er veel vanaf weet (20.8%).

Tabel D1

Kennis wachtwoordmanager

	Had u voorafgaand aan dit onderzoek al weleens gehoord van een wachtwoordmanager?	
	N	%
Nee	333	31.0
Ja, maar ik weet er weinig vanaf	518	24.8
Ja, en ik weet er veel vanaf	224	20.8

Noot. N = 1075.

Deelnemers beantwoordden ook twee vragen over het gebruik van een wachtwoordmanager. Tabel D2 geeft de resultaten weer. De resultaten laten zien dat meerderheid van de deelnemers nooit gebruik maakt van een wachtwoordmanager (55.6% en 57.5%, respectievelijk).

Tabel D2

Gebruik wachtwoordmanager

	Maakt u gebruik van een wachtwoordmanager voor het opslaan van wachtwoorden?		Maakt u gebruik van de suggesties voor sterke wachtwoorden van uw wachtwoordmanager?	
	N	%	*N*	%
Nooit	598	55.6	618	57.5
Soms	313	29.1	318	29.6
Altijd	164	15.3	139	12.9

Noot. N = 1075.

Tenslotte beantwoordden deelnemers die op de tweede vraag in Tabel D2 “nooit” of “soms” hadden geantwoord een aantal vragen over hun intentie om een wachtwoordmanager te gebruiken. Tabel D3 geeft de resultaten weer. De resultaten laten zien dat ongeveer de helft van de deelnemers die nooit of soms een wachtwoordmanager gebruiken aangaf uit te gaan zoeken hoe een wachtwoordmanager werkt (49.5% antwoordde enigszins of helemaal mee eens). Een deel gaf ook aan (vaker) een wachtwoordmanager te gaan gebruiken voor accounts (39.2% antwoordde enigszins of helemaal mee eens). Een minderheid van de deelnemers gaf aan op zoek te gaan naar iemand die hen kan helpen met het installeren van een wachtwoordmanager (26.6% antwoordde enigszins of helemaal mee eens).

Tabel D3

Intentie wachtwoordmanager.

	Antwoordcategorie (%)					*M*	*SD*
	1	2	3	4	5		
Ik ga (vaker) een wachtwoordmanager gebruiken voor mijn accounts	12.1	10.4	38.3	30.1	9.1	3.14	1.11
Ik ga uitzoeken hoe een wachtwoordmanager werkt	11.0	10.6	28.9	33.8	15.7	3.33	1.19
Ik ga op zoek naar iemand die mij kan helpen met het installeren van een wachtwoordmanager	25.2	18.6	29.6	16.8	9.8	2.67	1.28

Noot. *N* = 911. Antwoordschaal: 5-puntsschaal (*1 = helemaal mee oneens, 2 = enigszins mee oneens, 3 = niet mee oneens maar ook niet mee eens, 4 = enigszins mee eens, 5 = helemaal mee eens*).

Kenniscentrum
Psychologie en Economisch Gedrag

Auteurs: Dr. Emma ter Mors, Dr. Gert-Jan Lelieveld, Dr. Marret Noordewier, Alien van der Vliet, MSc, Vera Hilgevoord, MSc, Ruth Dijkstra, MSc, Prof. Dr. Wilco van Dijk

Datum: 1 juli 2022