Oud en Wijs Genoeg voor de Digitale Wereld? Succesfactoren voor Digitale Weerbaarheidsinterventies gericht op Ouderen

30-6-2025

Kimberly Bluhm[1] MSc & dr. Jurjen Jansen[1,2]
[1]NHL Stenden Hogeschool, [2]Politieacademie

Inhoudsopgave

1 Inleiding

In dit hoofdstuk wordt allereerst de aanleiding van het project besproken (par. 1.1). Daarna gaan we in op de context van het project (par. 1.2) en staan we stil bij de definitie van digitale weerbaarheid (par. 1.3). Het hoofdstuk wordt afgesloten met een leeswijzer (par. 1.4).

1.1 Aanleiding

Dit onderzoeksrapport gaat over het bevorderen van de digitale weerbaarheid van ouderen. Onder ouderen verstaan we binnen dit project mensen van 55 jaar en ouder die gebruikmaken van internet. Ouderen begeven zich steeds vaker op het internet en komen daarmee ook steeds vaker in aanraking met cyberdreigingen en online criminaliteit (van der Meer & Lenssink, 2019; van Deursen, 2019). Het is dus van belang dat zij digitaal weerbaar zijn (zie par. 1.3).

Er bestaan meerdere initiatieven om de digitale weerbaarheid van ouderen te verhogen. Om de doelgroep effectief te bereiken en de aanpak te versterken, zijn coördinatie en samenwerking essentieel. In dit project worden bestaande theoretisch onderbouwde interventies geïmplementeerd en geëvalueerd om de digitale weerbaarheid van ouderen in Noord-Nederland (provincies Friesland, Groningen, Drenthe) te bevorderen. Het beoogde resultaat daarvan is om een ‘zinvolle en geborgde’ aanpak te ontwikkelen. In dit rapport ligt de focus op de theoretische onderbouwing van interventies, wat uitmondt in een handzame checklist dat helpt bij het selecteren ervan (zie bijlage I).

Vanuit de Werkgroep Cyberveiligheid Noord-Nederland, en onder coördinatie van de kwartiermaker cyberweerbare ouderen, is expliciet de wens uitgesproken om samen te werken aan de digitale weerbaarheid van ouderen (RBPO, 2024). De netwerksamenwerking die reeds in Noord-Nederland is opgezet wordt benut, geformaliseerd en uitgebouwd om te voorkomen dat organisaties en initiatieven los van elkaar opereren. Aan dit

netwerk nemen gemeenten, politie, RIEC en OM deel en wordt verbinding gezocht met andere publieke en private organisaties. Voor dit specifieke project zijn dat SeniorWeb, Fraudehelpdesk, Rabobank, Koninklijke Bibliotheek (KB), het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en MeiJo (zorginstelling voor ouderen en onderdeel van Kwadrant).

1.2 Context

Online criminaliteit, soms ook digitale criminaliteit genoemd, is criminaliteit waarbij computers en technologie een cruciale rol spelen bij het plegen van het delict. Door digitalisering zijn er nieuwe vormen van criminaliteit ontstaan (cybercriminaliteit) en hebben veel traditionele misdrijven een digitale verschijningsvorm (gedigitaliseerde criminaliteit). Beide vormen, en hun mengvormen, noemen we in dit rapport online criminaliteit.

Volgens recente cijfers van het CBS is ruim zestien procent van de Nederlandse burgers van vijftien jaar en ouder in één jaar tijd slachtoffer van een of meerdere vormen van online criminaliteit (Arends et al., 2025). Burgers zijn vooral slachtoffer van online oplichting en fraude. Het is belangrijk te vermelden dat het CBS niet alle soorten online criminaliteit in kaart brengt. In werkelijkheid kan het aandeel slachtofferschap dus nog hoger zijn, ook gelet op het feit dat mensen soms niet door hebben dat ze slachtoffer zijn, bijvoorbeeld wanneer gegevens gestolen zijn, of virussen onopgemerkt op hun apparaten ronddwalen.

Uit onderzoek blijkt dat de impact van online criminaliteit vergelijkbaar is met die van traditionele misdrijven (Bluhm et al., 2022; Borwell et al., 2021; Borwell et al., 2022; Leukfeldt et al., 2018). Naast financiële schade ervaren slachtoffers ook internaliserende en externaliserende problemen (Borwell et al., 2025). Internaliserende problemen zijn naar binnen gericht en omvatten depressie, lichamelijke klachten en sociaal terugtrekken. Externaliserende problemen zijn naar buiten gericht en omvatten boosheid, wraakgevoelens en angst voor

herhaling. De impact van online criminaliteit kan in sommige gevallen zelfs als heftiger worden ervaren (Borwell et al., 2025).

Gemeenteambtenaren en experts vanuit bijvoorbeeld politie, banken en kennisinstellingen beschouwen ouderen als een kwetsbare groep voor online criminaliteit (Spithoven et al., 2022). In een peiling in opdracht van KBO-PCOB[1] onder 1.050 ouderen geeft één op de tien respondenten aan ooit slachtoffer te zijn geweest van online criminaliteit en vier op de tien respondenten geven aan hier bang voor te zijn (van der Meer & Lenssink, 2019). Een recentere peiling door SeniorWeb onder 900 ouderen laat zien dat 11% slachtoffer is geworden van online oplichting en 71% hier bang voor is.[2] Regelmatig mijden ouderen daarom het gebruik van digitale middelen (van Deursen, 2019). Dit betekent dat ouderen potentiële kansen die digitalisering biedt daarmee missen. Het is daarom, zoals eerder vermeld, van belang dat ouderen weerbaarder zijn tegen online criminaliteit.

Gelukkig zijn er steeds meer initiatieven die specifiek gericht zijn op het digitaal weerbaar maken van ouderen. Deze initiatieven zijn veelal gebaseerd op het principe van inslijpen[3] en oefenen, en het verhogen van bewustwording. Dat wil zeggen dat door middel van oefenen, trainingen en educatie (inslijpen en oefenen) of door middel van communicatie-campagnes (verhogen van bewustwording) ouderen kennis en inzicht verkrijgen over cyberdreigingen en hoe zij hiermee kunnen omgaan. Denk bijvoorbeeld aan de campagne ‘Maak het oplichters niet te makkelijk’.[4]

De focus op inslijpen, oefenen en bewustwording zijn verschillende manieren om veilig gedrag te bewerkstelligen. Het is echter aannemelijk

---

[1] Een grote seniorenorganisatie in Nederland.
[2] https://veiliginternetten.nl/nieuws/angst-bij-ouderen-voor-online-fraude/#:~:text=Veel%20senioren%20vinden%20het%20steeds,daadwerkelijk%20gedupeerd%20door%20online%20oplichting.
[3] Inslijpen verwijst naar het systematisch en herhaaldelijk oefenen van een vaardigheid of handeling, zodanig dat deze ‘geautomatiseerd’ wordt (de Bruine, 2018).
[4] https://www.maakhetzenietteemakkelijk.nl/senioren-en-veiligheid.

dat ouderen minder snel nieuwe informatie vergaren (Boulton-Lewis, 2010). Dijkstra (2009) benoemt bijvoorbeeld dat de cognitieve vaardigheden afnemen bij ouderen, waardoor het langer kan duren voor hen om informatie op te nemen en te verwerken. Het is daarom de vraag in hoeverre de methode van inslijpen en oefenen een effectieve manier is om deze doelgroep digitaal weerbaarder te maken.

Een tweede manier om veilig gedrag te bewerkstelligen is gericht op het inrichten van een veilig ontwerp (de Bruine, 2018). Dit betekent dat door aanpassingen aan het ontwerp van een applicatie, procedure of omgeving verleidingen om onveilig gedrag te vertonen zoveel mogelijk worden weggenomen en dat het gemakkelijker wordt gemaakt om veilig gedrag te vertonen. Zo zien we bijvoorbeeld dat deze methode effectief kan zijn om ouderen te helpen bij veilig online winkelen (Esposito et al., 2017) en bij veilig autorijden (Ruer et al., 2016).

Van Steen en De Busser (2021) hebben voor het Nationaal Cyber Security Centrum (NCSC) een overzicht gepubliceerd welke technieken mogelijk zijn om digitale ontwerpen inherent veiliger te maken op basis van gedragsprincipes. Denk hierbij aan verschillende nudging-principes. Nudging (letterlijk: ‘een duwtje geven’) houdt in dat aanpassingen in de omgeving leiden tot een (on)bewuste gedragsverandering (Blatter & Bakhuys Roozeboom, 2018; Thaler & Sunstein, 2022). Voorbeelden hiervan zijn standaard veilige instellingen (‘updates staan al op automatisch’), sociaal bewijs (‘anderen gingen u voor’) en directe feedback (‘gevolgen van keuze benoemen’). In hoofdstuk 4 gaan we dieper in op interventies die als doel hebben gedrag te veranderen.

1.3 Digitale weerbaarheid op hoofdlijnen

Digitale weerbaarheid verwijst naar ‘het vermogen om (relevante) risico’s tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken,

schade te beperken en herstel eenvoudiger te maken' (NCSC, 2022, p. 9). Wij voegen daar het aspect 'leervermogen' aan toe (zie ook Jansen (2025)).

Het doel van digitale weerbaarheid is niet om alle aanvallen te voorkomen, aangezien dit vaak onhaalbaar is, maar om de kans op en impact van incidenten te verlagen. Naast preventieve maatregelen (preventie en detectie) omvat digitale weerbaarheid ook repressieve maatregelen (respons en herstel). Digitale weerbaarheid draait om de samenwerking tussen mens, techniek en organisatie, waarbij veerkracht net zo belangrijk is als het tegenhouden van aanvallen (Coventry et al., 2014; Furnell & Clarke, 2012; Jansen, 2018; NCSC, 2022; Rothrock, 2022).

Om het concreet te maken voor de ouderendoelgroep zijn twee aspecten essentieel. De eerste is het hebben van een adequate risicoperceptie, waarbij ouderen zich bewust zijn van de mogelijke digitale dreigingen en risico's, en de gevolgen daarvan. De tweede omvat het zelfbeschermend gedrag, waarbij ouderen (pro)actieve stappen zetten om hun digitale veiligheid te waarborgen, zoals het gebruik van sterke wachtwoorden, het herkennen van phishing-pogingen en het regelmatig updaten van software. Naast basismaatregelen (cyberhygiëne) kan het gaan om gedragingen die betrekking hebben op het voorkomen van specifieke vormen van online criminaliteit.

1.4 Leeswijzer

In hoofdstuk 2 staan we stil bij de doel- en vraagstelling van dit onderzoek, en in hoofdstuk 3 bespreken we de gehanteerde onderzoeksmethoden. Vervolgens bespreken we in hoofdstuk 4 de resultaten. Daarin staan we stil bij interventies die bijdragen aan het vergroten van digitale weerbaarheid, de onderwerpen die daarin centraal staan, verklarende theorie, het bereiken van ouderen, en de werkzame elementen en randvoorwaarden voor de ouderendoelgroep. Tot slot staan in hoofdstuk 5 in de belangrijkste conclusies centraal, voeren we discussie daarover en bespreken we beperkingen van het onderzoek.

2 Doel- en vraagstelling

In dit hoofdstuk worden de doel- (par. 2.1) en vraagstelling (par. 2.2) gepresenteerd.

2.1 Doelstelling

Het doel van het dit onderzoek is om in kaart te brengen waar een interventie gericht op het vergroten van de digitale weerbaarheid van ouderen aan moet voldoen om uitspraken te kunnen doen over de mogelijke effectiviteit van een interventie.

2.2 Vraagstelling

De volgende onderzoeksvraag staat in deze rapportage centraal: "*Welke indicatoren zijn volgens de theorie essentieel in interventies gericht op het verhogen van de digitale weerbaarheid van ouderen (55+)?".* Om deze hoofdvraag te beantwoorden, zijn onderstaande deelvragen opgesteld:

1. Welke bestaande interventies richten zich op het vergroten van digitale weerbaarheid van ouderen?
2. Welke gedragsonderwerpen of -categorieën worden binnen interventies aangesproken om de digitale weerbaarheid van deelnemers aan die interventies te vergroten?*
3. Welke theoretische constructen/modellen/theorieën verklaren de ontwikkeling of het vergroten van digitale weerbaarheid?
4. Wat zijn werkzame elementen en randvoorwaarden van interventies gericht op het vergroten van digitale weerbaarheid?
5. Op welke manieren kan de doelgroep ouderen worden bereikt om hen deel te laten nemen aan interventies gericht op het vergroten van de digitale weerbaarheid?
6. Welke werkzame elementen en randvoorwaarden van interventies zijn relevant voor de doelgroep ouderen?

*Het is belangrijk om te beseffen dat er vooralsnog geen consensus is over de adviezen rondom veilig online gedrag, en dat deze soms tegenstrijdig zijn (Reeder et al., 2017; Redmiles et al., 2020). Bovendien is het onbegonnen werk om op voorhand alle mogelijke doelgedragingen op te sommen. Per situatie moet worden bekeken welke uitkomst gewenst is en welke concrete doelgedragingen daarbij passen om die uitkomst te bewerkstelligen. Daarom spreken we in deze vraag niet van 'gedrag', maar van 'gedragsonderwerpen' of 'gedragscategorieën'.

3 Onderzoeksmethoden

In dit hoofdstuk zijn de onderzoeksmethoden beschreven. Hierbij maken we onderscheid tussen het literatuuronderzoek (par. 3.1) en de startbijeenkomst (par. 3.2). In Tabel 3.1 is de methodenmatrix te vinden waarin we presenteren op welke manier de resultaten voor de deelvragen zijn verzameld.

Tabel 3.1: Methodenmatrix

Deelvraag	**Methoden**	
	Literatuur-onderzoek	Start-bijeenkomst
1. Interventies die bijdragen aan digitale weerbaarheid	X	X
2. Gedragsverandering door interventies	X	
3. Theoretische constructen/modellen/ theorieën ter verklaring	X	
4. Werkzame elementen en randvoorwaarden van interventies	X	
5. Bereiken van de doelgroep ouderen	X	X
6. Werkzame elementen en randvoor-waarden voor de doelgroep ouderen	X	

3.1 Literatuuronderzoek

Alle onderzoeksvragen zijn (gedeeltelijk) door middel van literatuuronderzoek beantwoord. Met dit literatuuronderzoek willen we inzicht verkrijgen in de bestaande kennis over interventies gericht op het verhogen van de digitale weerbaarheid (van ouderen). We hebben allereerst gebruik gemaakt literatuur die reeds bekend was. Daarnaast zijn drie databases gebruikt om (relevante) literatuur te vinden en te bestuderen, namelijk Google Scholar, Science Direct en de mediatheek van NHL Stenden Hogeschool.

De volgende zoektermen zijn (zowel in het Nederlands als in het Engels, en in sommige gevallen in combinatie met elkaar) gebruikt:

cybercriminaliteit, digitale criminaliteit, online criminaliteit, digitale weerbaarheid, cyberweerbaarheid, bewustwording, gedragsverandering, effectiviteit, gedragsverandering, interventies, ouderen, COM-B, Protection Motivation Theory, Reasoned Action Approach, senioren, leren, werving, bereiken. Aanvullend is middels de sneeuwbalmethode gezocht naar relevante literatuur. De literatuurlijsten van de geraadpleegde bronnen zijn bestudeerd om te zoeken naar relevante, verwante artikelen.

3.2 Startbijeenkomst

Tijdens de startbijeenkomst op woensdag 25 september 2024 (10:00 – 13:00 uur) is informatie voor het huidige onderzoek opgehaald. Het doel van deze startbijeenkomst was om de verschillende partijen kennis met elkaar te laten maken. Hierbij waren de volgende partijen aanwezig: kwartiermakers ouderen en de aanjager digitale weerbaarheid vanuit het RBPO, Openbaar Ministerie (OM), Politie, NHL Stenden Hogeschool, Koninklijke Bibliotheek (KB), Rabobank, SeniorWeb en het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Daarnaast zijn allereerst een aantal procesmatige onderdelen besproken, namelijk een toelichting op het projectplan, de rolverdeling tijdens het project en het in kaart brengen van wensen en verwachtingen van de partners.

Tijdens deze bijeenkomst is aan de aanwezigen ook gevraagd om input te leveren op twee inhoudelijke onderdelen. In het eerste onderdeel is in kaart gebracht welke interventies reeds door de partners worden of zijn uitgevoerd. De partners schreven dit individueel op post-its en daarna werden de resultaten plenair besproken. In het tweede onderdeel is aan de partners gevraagd op welke manier de organisatie de doelgroep ouderen bereikt. Dit is tevens middels post-its in kaart gebracht. De projectleiders hebben de bevindingen van beide onderdelen verzameld en omgezet in een overzicht. De informatie uit dit overzicht is gebruikt om de eerste en vijfde deelvraag te beantwoorden (zie hoofdstuk 4).

4 Resultaten

In dit hoofdstuk zijn de resultaten per deelvraag beschreven. De deelvragen richten zich op: bestaande interventies die kunnen bijdragen aan het vergroten van digitale weerbaarheid van ouderen (par. 4.1), de na te streven gedragsverandering door interventies (par. 4.2), de theoretische constructen/modellen/theorieën die de ontwikkeling of het vergroten van digitale weerbaarheid verklaren (par. 4.3), de werkzame elementen en randvoorwaarden van interventies (par. 4.4), het bereiken van de doelgroep ouderen (par. 4.5), en de werkzame elementen en randvoorwaarden van interventies voor de doelgroep ouderen (par. 4.6).

4.1 Bestaande interventies gericht op het vergroten van digitale weerbaarheid

In deze paragraaf zijn de resultaten voor de eerste deelvraag gerapporteerd: *Welke bestaande interventies richten zich op het vergroten van digitale weerbaarheid van ouderen?* Hierbij hebben we onderscheid gemaakt tussen bestaande interventies vanuit de Database Lokale Cyberprojecten van het CCV (par. 4.1.1) en interventies die reeds door de betrokken partners worden uitgevoerd (par. 4.1.2). Om álle interventies in kaart te brengen en te beschrijven valt buiten de scope van dit onderzoek.

4.1.1 Bestaande interventies vanuit bredere werkveld

Het doel van een interventie is het in beweging brengen van een individu, groep of organisatie. Hiervoor kan gebruik worden gemaakt van een instrument, model, tool, spel of werkvorm; al ligt de nadruk op de bewuste handeling(en) die met de interventie te weeg worden gebracht (Janssen et al., 2024).

Diverse organisaties ontwikkelen en implementeren interventies om de digitale weerbaarheid van ouderen te vergroten. Voor het huidige onderzoek beperken we ons tot de interventie die vanuit de Database

Lokale Cyberprojecten van het CCV worden aangeboden. Uit deze database komt naar voren dat drie interventies zich richten op de doelgroep ouderen.

De eerste interventie is 'Storytelling Cybercrime' en is ontwikkeld door het Regiobureau Integrale Veiligheid Oost-Brabant.[5] Het doel van deze interventie is om bewustwording te creëren over digitale gevaren en de digitale weerbaarheid bij ouderen te verhogen om zo de kans op slachtofferschap van online criminaliteit te verlagen (Bluhm et al., 2024-a). In deze interventie worden verhalenvertellers opgeleid om verhalen, gebaseerd op ervaringen van slachtoffers, aan de doelgroep te vertellen. Op deze manier wordt het verhaal authentiek en geloofwaardig overgebracht. Typen criminaliteit die centraal staan zijn onder andere de digitale babbeltruc en phishing.

De tweede interventie is de interactieve film 'Echt of nep?' en is ontwikkeld door de Veiligheidsalliantie Rotterdam (VAR).[6] Het doel van deze interventie is om gemeenten bij te staan in het digitaal weerbaar maken van inwoners. In deze interventie worden aanwezigen meegenomen in een interactieve film waarin keuzemogelijkheden zitten die verband houden met verschillende vormen van online criminaliteit (Bluhm et al., 2024-a), zoals WhatsApp-fraude, bankhelpdeskfraude en phishing. De aanwezigen dienen op deze momenten te bepalen welke keuze zij in een dergelijke situatie zouden maken. De ervaring die wordt opgedaan wanneer een bepaalde keuze wordt gemaakt, bijvoorbeeld wanneer de aanwezigen meegaan in het delict, zouden ervoor kunnen zorgen dat de aangeboden kennis beter beklijft.

De derde interventie is de serious game 'Weerbaar op het web' en is ontwikkeld door de gemeente Coevorden, Gemeente Dordrecht en

[5] https://hetccv.nl/themas/cyberveiligheid/cybercrime/database-lokale-cyberprojecten/storytelling-cybercrime/
[6] https://hetccv.nl/themas/cyberveiligheid/cybercrime/database-lokale-cyberprojecten/interactieve-training-cyberweerbaarheid-senioren/

Raccoon Serious Games.[7] Deze interventie bevat een toolkit met daarin een fysiek spel en een bijpassende handleiding (Bluhm et al., 2024-a). In dit spel wordt kennis aangereikt over het thema online veilig gedrag, bijvoorbeeld welke persoonsgegevens online gedeeld mogen worden. Het inzetten van een fysiek bordspel wordt aangehaald als meer passend bij de doelgroep dan een digitale variant.

4.1.2 Bestaande interventies vanuit partners

Tijdens de startbijeenkomst is aan de aanwezige partners gevraagd welke interventies zij reeds aanbieden. Uit de inventarisatie komt naar voren dat de betrokken partijen verschillende interventies uitvoeren. Deze zijn opgenomen in Tabel 4.1.

Tabel 4.1

Overzicht van interventies per betrokken partner

Partij	**Interventie(s)**
Rabobank	Presentatie veilig bankieren (i.s.m. SeniorWeb) Internet- en sociale mediacampagnes gericht op (gevaren van) oplichting Cybermarkt
SeniorWeb	Webinars (i.s.m. SIDN en Fraudehelpdesk) Activiteiten in (520) leslocaties tijdens themamaanden
CCV	Storytelling Cybercrime Interactieve film “Echt of Nep?” Serious game “Weerbaar op het Web”
Koninklijke Bibliotheek (KB)	Kleinste privacyshow van Nederland Nationale cursus digitale weerbaarheid
MeiJo	Cafébijeenkomsten

[7] https://hetccv.nl/themas/cyberveiligheid/cybercrime/database-lokale-cyberprojecten/serious-game-cyberweerbaarheid-laaggeletterden/

4.2 Na te streven gedragsonderwerpen of -categorieën door interventies

Het is van belang om in kaart te brengen wat het gewenste gedrag is wat middels interventies gepoogd wordt om te bereiken. In deze paragraaf zijn de resultaten voor de tweede deelvraag gerapporteerd: *Welke gedragsonderwerpen of -categorieën worden binnen interventies aangesproken om de digitale weerbaarheid van deelnemers aan die interventies te vergroten?*

Uit de wetenschappelijke en grijze literatuur komt geen eenduidige definitie voor gewenst online veilig gedrag naar voren, al zien we veel overlap. Voor het huidige onderzoek hebben we twee artikelen nader geanalyseerd waarin maatregelen op het gebied van cyberhygiëne centraal staan.

Van 't Hoff - de Goede et al. (2019) onderscheiden, op basis van eerdere empirische studies, in hun onderzoek zeven clusters gericht op online veilig gedrag waarmee individuen zich kunnen beschermen tegen slachtofferschap van online criminaliteit. Hierbij gaat het om:

- Het gebruik van wachtwoorden
- Het opslaan van belangrijke bestanden
- Het installeren van updates
- Het gebruik van beveiligingssoftware
- De alertheid tijdens internetgebruik
- De voorzichtigheid bij het online delen van persoonlijke gegevens
- Het voorzichtig omgaan met bijlagen en hyperlinks in e-mails

Daarnaast hebben Coventry et al. (2014) *best practices* op het gebied van cybersecurity in kaart gebracht door diverse online bronnen over maatregelen te reviewen en input op te halen bij experts. Op basis van deze bevindingen onderscheiden zij tien maatregelen die individuen dienen te

treffen om online veilig gedrag te vertonen. Een aantal maatregelen overlappen met de bovengenoemde.

- Gebruik van sterke wachtwoorden en het veilig managen ervan
- Gebruik van antivirus software en firewalls
- Software up-to-date houden
- Uitloggen op websites na gebruik ervan en het afsluiten van de computer
- Enkel vertrouwde en beveiligde connecties, computers en apparaten gebruiken (inclusief Wi-Fi)
- Enkel vertrouwde en beveiligde websites en services gebruiken
- Geïnformeerd blijven over risico's (kennis, intuïtie). Vermijden van scams en phishing
- Zo minimaal mogelijk persoonlijke informatie delen tijdens online interacties en identiteit beschermen
- Opletten wat in de fysieke omgeving gebeurt
- Aangifte/melding doen bij slachtofferschap van online criminaliteit

4.3 Verklarende theorieën voor de ontwikkeling van digitale weerbaarheid

Om de digitale weerbaarheid te kunnen bevorderen, moeten we factoren die van invloed zijn op menselijk gedrag allereerst goed begrijpen. In deze paragraaf zijn de resultaten voor de derde deelvraag beschreven: *Welke theoretische constructen/modellen/theorieën verklaren de ontwikkeling of het vergroten van digitale weerbaarheid?* Het gebruik van theorie is belangrijk voor het *evidence-informed* of *theory-informed* bevorderen van de digitale weerbaarheid van doelgroepen. Hierdoor kunnen we beter begrijpen wat onveiligheid veroorzaakt of veiligheid bevordert, en hoe we dit kunnen veranderen c.q. versterken (Bartholomew Elredge et al., 2016).

Uit de literatuur komen diverse theorieën en modellen naar voren die uitspraken doen over (het mogelijk aanzetten tot) veilig (digitaal)

gedrag. Hieronder hebben we de *Protection Motivation Theory (PMT),* de *Reasoned Action Approach (RAA)* en het *Capability-Opportunity-Motivation-Behaviour* (*COM-B)* model uiteengezet die in de praktijk en wetenschap veelvuldig worden toegepast.[8] Bij een probleemgerichte aanpak – zoals het inzetten van interventies ter bevordering van digitale weerbaarheid gezien kan worden – kunnen meerdere theorieën of theoretische inzichten tegelijkertijd worden ingezet (Bartholomew Elredge et al., 2016). Deze auteurs geven aan dat hoewel het nuttig kan zijn dat de interventies eveneens bijdragen aan verdere theorieontwikkeling, dit van ondergeschikt belang is voor het proces van probleemoplossing. Aanvullend hebben we aandacht besteed aan de praktische onderbouwing van een interventie (par. 4.3.4).

We beschrijven hierna theoretische inzichten die gericht zijn op individuen. Gezien de doelgroep en betrokken partijen is er iets voor te zeggen om ook rekening te houden met diens omgeving (Joinson et al., 2023). Hiervoor is de routineactiviteitentheorie (Cohen & Felson, 1979) een interessante invalshoek. Deze theorie veronderstelt dat criminaliteit waarschijnlijk is wanneer er sprake is van een gemotiveerde dader (buiten de scope van dit onderzoek), een geschikt doelwit (de doelgroep die weerbaarder kan worden gemaakt) en de afwezigheid van toezicht (hierin kunnen, naast technische tools, ook familie, vrienden en andere partijen die in contact staan met de doelgroep een rol spelen, zoals medewerkers van zorginstellingen en bibliotheken (Burton et al., 2022).

[8] Overige theorieën en modellen die toegepast kunnen worden, maar die we nu buiten beschouwing laten, zijn onder andere het Health Belief Model (Rosenstock, 1974), het (Extended) Parallel Processing Model (Leventhal, 1970; Witte, 1991), en het Risk Information Seeking & Processing Model (Griffin et al., 1999), zie ook Jansen (2018) en Moody et al. (2018). Tevens kan worden gekeken naar persoonlijkheidskenmerken (zie bijvoorbeeld Borwell et al. (2021)), maar daarvan is de praktische toepasbaarheid lastig.

4.3.1 Protection Motivation Theory (PMT)

De *Protection Motivation Theory* (PMT) van Rogers (1975) is een veelgebruikte theorie om de motivatie voor het treffen van beschermende maatregelen in kaart te brengen. Aanvankelijk werd het model voornamelijk ingezet op het gebied van gezondheidsinterventies (Floyd et al., 2000), al is de theorie veelvuldig ingezet op het thema van digitaal veilig gedrag (Crossler & Bélanger, 2014; De Kimpe et al., 2022; Jansen, 2018; Martens et al., 2019; Shillair et al., 2015; Van ’t Hoff - de Goede et al., 2019).

PMT maakt onderscheid tussen twee cognitieve processen die invloed hebben motivatie om zichzelf te beschermen (De Kimpe et al., 2022; Martens et al., 2019; Rogers, 1975; Van ’t Hoff - de Goede et al., 2019). De evaluatie van (1) de dreiging (*threat appraisal*); en (2) de te treffen maatregelen tegen de dreiging (*coping appraisal*) resulteren volgens de theorie in de motivatie om zelfbeschermend gedrag te vertonen. Met andere woorden, deze twee evaluaties resulteren in de intentie tot digitaal veilig gedrag, wat een directe invloed kan hebben op daadwerkelijk gedrag (Jansen, 2018; Van ’t Hoff - de Goede et al., 2019).

De evaluatie van de dreiging bevat twee constructen: (1) de gepercipieerde kans (i.e., de inschatting van de waarschijnlijkheid van de dreiging); en (2) de gepercipieerde impact (i.e., de inschatting van de ernst van de dreiging) (Crossler & Bélanger, 2014; De Kimpe et al., 2022; Martens et al., 2019). Voor de gepercipieerde kans komen uit de literatuur wisselende resultaten naar voren over de invloed op (de intentie tot) veilig digitaal gedrag. Zowel positieve (Thompson et al., 2017), niet-significante (Martens et al., 2019) als negatieve (Tsai et al., 2016) relaties tussen dit construct en (de intentie tot) veilig gedrag zijn gevonden. Desalniettemin, is in de initiële theorie van Rogers (1975) gesuggereerd dat gepercipieerde kans een positieve invloed heeft op (de intentie tot) veilig digitaal gedrag (Anderson & Agarwal, 2010; De Kimpe et al., 2022; Fisher, 2024; Jansen, 2018; Martens et al., 2019).

Wat betreft de impact zien we ook wisselende bevindingen op (de intentie tot) veilig digitaal gedrag. Een aantal studies suggereren een positieve invloed (Hassan et al., 2024; Jansen, 2018; Martens et al., 2019; Warkentin et al., 2016), terwijl andere een niet-significante of negatieve invloed suggereren (Fisher, 2024; Thompson et al., 2017; Verkijika, 2018).

De evaluatie van de te treffen maatregelen tegen de dreiging omvat drie constructen, namelijk: (1) zelfeffectiviteit (i.e., het vertrouwen in eigen kunnen om een maatregel uit te voeren); (2) responseffectiviteit (i.e., de verwachte effectiviteit van een maatregel); en (3) responsekosten (i.e., de inschatting van de kosten, zoals tijd en geld, die met de maatregel gemoeid zijn) (Arachchilage & Love, 2014; Burns et al., 2017; Clubb & Hinkle, 2015; De Kimpe et al., 2022; Martens et al., 2019). Op basis van deze evaluaties raken personen volgens de theorie gemotiveerd om zichzelf te beschermen. Hiervoor geldt dat de eerste twee constructen een hoge score vereisen, en de derde een lage.

Uit de literatuur komt naar voren dat zelfeffectiviteit en responseffectiviteit de belangrijkste voorspellers lijken te zijn voor (de intentie tot) digitaal veilig gedrag (Arachchilage & Love, 2014; Crossler & Bélanger, 2014; De Kimpe et al., 2022; Fisher, 2024; Hassan et al., 2024; Jansen, 2018). Hassan et al. (2024) splitsen zelfeffectiviteit op in twee componenten, namelijk kennis en vaardigheden. Uit eerdere studies blijkt dat zelfeffectiviteit niet altijd een significante invloed heeft op (de intentie tot) veilig gedrag. Kennis wordt hierbij gedefinieerd als bewustwording of begrip van online veilig gedrag (bijvoorbeeld weten wat antivirussoftware is en doet). Vaardigheden richten zich op de competenties om maatregelen te kunnen uitvoeren (bijvoorbeeld het installeren en updaten van antivirussoftware). Hun bevindingen suggereren dat deze twee componenten samen een positieve invloed hebben op (de intentie tot) online veilig gedrag. Dit impliceert dat het opleiden en trainen noodzakelijk is om kennis en vaardigheden over te brengen (Hassan et al., 2024).

Over de invloed van responsekosten op de motivatie voor digitaal veilig gedrag komen uit de literatuur wisselende bevindingen naar voren. Sommige studies stellen een negatieve invloed vast (Verkijika, 2018; Tsai et al., 2016; Vance et al., 2016). Gurung et al. (2009) suggereren dat responsekosten geen significante invloed hebben op (de intentie tot) veilig online gedrag, omdat een overvloed aan gratis maatregelen beschikbaar is. Ook in andere studies werden geen significante verbanden gevonden (zie o.a. Fisher, 2024). Hoewel responsekosten in sommige contexten geen directe voorspellers zijn van digitaal veilig gedrag, betekent dit niet dat ze geen rol spelen. Hun impact is afhankelijk van de contextuele drempels die worden ervaren. Zodra deze drempels stijgen, bijvoorbeeld door geld te vragen voor deelname aan interventies, neemt de (negatieve) invloed op motivatie waarschijnlijk toe.

Uit studies wordt duidelijk dat in communicatie-uitingen of interventies in bredere zin een boodschap over risico's (*threat appeal*) tevens vergezeld dient te worden van een (liefst zo praktisch mogelijke) boodschap hoe met dergelijke risico's om te gaan (*efficacy appeal*) (Jansen & van Schaik, 2019; Witte & Allen, 2000). In de PMT-literatuur wordt verondersteld dat men op twee manieren kan reageren op dergelijke uitingen, namelijk *problem-focused coping* en *emotion-focused coping* (Lazarus & Folkman, 1984). De eerste manier is de meest wenselijke, omdat men dan een probleem bij de hoorns vat en probeert daar op een directe wijze iets aan te doen, bijvoorbeeld acties uitvoeren om een dreiging of gevaar weg te nemen dan wel de impact ervan te minimaliseren.

De tweede manier richt zich op het veranderen van ongewenste gevoelens en emoties ten opzichte van een probleem of bedreiging, zoals stress, angst, verdriet en hulpeloosheid, zonder de oorzaak aan te pakken. Voorbeelden zijn cognitieve strategieën zoals vermijding en selectieve aandacht, en gedragsstrategieën zoals mediteren, emotionele steun zoeken en verdovende middelen gebruiken. Hoewel deze aanpak de objectieve realiteit niet verandert, helpt het individuen hun emoties te

beheersen, wat belangrijk is voor effectieve coping. Emotiegerichte coping wordt vaak gebruikt als men denkt dat een situatie niet te veranderen is, terwijl probleemgerichte coping wordt toegepast als men denkt dat de situatie wel te veranderen is (Lazarus & Folkman, 1984). Beide strategieën kunnen elkaar aanvullen en beïnvloeden.

Ten slotte hebben we in kaart gebracht hoe een interventie gebaseerd op PMT eruit kan zien. Hiervoor gebruiken we een voorbeeld uit de gezondheidszorg, de initiële focus van PMT. Nouri et al. (2024) ontwikkelden een interventie gericht op beroepsrisico's op de eerste hulp in het ziekenhuis. In deze interventie werden meerdere methoden (presentatie, Q&A-sessies, en het verspreiden van informatie via diverse platformen) geïntegreerd in een training, waarin de verschillende PMT-constructen aan bod kwamen.

Voor de gepercipieerde kans en gepercipieerde impact ontvingen deelnemers informatie in een presentatie over prevalentie, ofwel de kans dat zij hiermee te maken krijgen, en de effecten hiervan. Vervolgens is hen informatie aangeboden over zelfeffectiviteit, responseffectiviteit en responskosten, inclusief de handelingen die deelnemers kunnen treffen om de kans op beroepsrisico's tegen te gaan, wat de verwachte effecten hiervan zijn en de moeite die bepaalde handelingen kosten, zoals het dragen van een mondkapje. Ter afsluiting werden de aangeleerde handelingen in de praktijk geoefend, zodat deelnemers direct het gewenste gedrag kunnen oefenen/vertonen.

De bevindingen van deze studie suggereren dat het implementeren van een interventie gebaseerd op PMT effectief kan zijn om zelf-beschermend gedrag van verpleegkundigen te verhogen. Hierbij maken de auteurs de kanttekening dat het enkel aanbieden van kennis onvoldoende is en enkele randvoorwaarden, zoals een faciliterende omgeving, van belang zijn (Nouri et al., 2024).

4.3.2 Reasoned Action Approach (RAA)

Hoewel specifieke theorieën de voorkeur hebben bij het bestuderen van specifiek gedrag, kunnen meer algemene theorieën of raamwerken voor het voorspellen van gedrag variabelen bevatten die belangrijk zijn binnen de onderzochte context. Een van deze conceptuele raamwerken is de *Reasoned Action Approach* (RAA) van Fishbein en Ajzen (2010). RAA is een verfijning en uitbreiding van de *Theory of Reasoned Action* (Ajzen & Fishbein, 1974) en de *Theory of Planned Behaviour* (Ajzen, 1991). De kern van het raamwerk is dat houding (*attitude*) ten opzichte van gedrag, waargenomen normen (*perceived norms*) en waargenomen gedragscontrole (*perceived behavioural control*) de intentie van gebruikers bepalen om bepaald gedrag uit te voeren (Fishbein & Ajzen, 2010). Er wordt aangenomen dat gedragsintentie daadwerkelijk gedrag voorspelt. De auteurs betogen dat hun benadering inzetbaar is voor diverse vormen van gedrag, dus ook voor gedragingen in relatie tot digitale weerbaarheid.

De houding weerspiegelt de positieve of negatieve gevoelens van een individu ten opzichte van het doelgedrag (Ajzen & Fishbein, 1974). Een positieve houding ten opzichte van bepaald gedrag lijkt dat gedrag positief te beïnvloeden. Denk zoal aan het gebruik van sterke wachtwoorden en tweefactorauthenticatie, omdat een individu gelooft dat deze maatregelen diens persoonlijke en bedrijfsgegevens beter beschermen tegen cyberaanvallen. De relatie tussen houding en intentioneel gedrag is uitgebreid getest en bevestigd (Venkatesh et al., 2003).

Waargenomen normen, uniek in RAA vergeleken met PMT, verwijzen naar waargenomen sociale invloed en bestaan uit injunctieve normen – percepties van wat anderen denken dat zou moeten worden gedaan – en descriptieve normen – percepties van of anderen het doelgedrag uitvoeren (Fishbein & Ajzen, 2010). Beide type normen zouden een positieve relatie hebben met intenties. Ter illustratie, als het gebruik van sterke wachtwoorden en tweefactorauthenticatie als de norm wordt gezien binnen een organisatie, voelen medewerkers sociale druk om deze

praktijken te volgen. Dit kan verder worden versterkt door leidinggevenden die het goede voorbeeld geven.

Fishbein en Ajzen (2010) beschrijven waargenomen gedragscontrole als percepties over het vermogen om het doelgedrag uit te voeren en/of er controle over te hebben. Een medewerker voelt zich bijvoorbeeld in staat om sterke wachtwoorden te creëren en te beheren, omdat de organisatie gebruiksvriendelijke tools en richtlijnen biedt. Dit gevoel van controle kan worden vergroot door trainingen en hulpmiddelen zoals wachtwoordmanagers aan te bieden.

Waargenomen gedragscontrole wordt gezien als een combinatie van zelfeffectiviteit (ook aanwezig in PMT) en locus of control. Locus of control is intern of extern (Rotter, 1966; Workman et al., 2008). Individuen met een hoog niveau van interne locus of control geloven dat ze de uitkomsten van een bepaalde gebeurtenis onder controle hebben. In deze context kan interne locus of control zich vertalen in proactief gedrag door individuen, waarbij ze verantwoordelijkheid nemen voor hun online veiligheid. Individuen met een hoge mate van externe locus of control geloven dat de uitkomst wordt gecontroleerd door machtige anderen of door het lot. Dit kan zich vertalen in reactief gedrag, waarbij de verantwoordelijkheid voor de eigen online veiligheid aan anderen wordt overgelaten.

4.3.3 Capability-Opportunity-Motivation-Behaviour model (COM-B)

Een belangrijke beperking van PMT en RAA is dat de voorspelling zich beperkt tot de intentie tot gedrag (Jansen, 2018; Van ’t Hoff - de Goede et al., 2019) en dat daadwerkelijk gedrag hiervan kan afwijken (Sheeran, 2002). Ook wordt kritiek geuit op deze modellen in die zin dat ze uitgaan van rationeel gedrag, terwijl menselijk gedrag vaak niet rationeel is (Kahneman, 2011). Daarnaast blijkt uit verschillende studies dat naast motivatie ook andere factoren een rol kunnen spelen bij digitaal veilig gedrag (Parsons et al., 2014; Vroom & von Solms, 2004).

Het *Capability-Opportunity-Motivation-Behaviour* (COM-B) model van Michie et al. (2011) onderscheidt drie determinanten van gedrag: capaciteiten (*capability*), gelegenheid (*opportunity*) en motivatie (*motivation*). Deze determinanten en hun onderlinge interactie bieden inzicht in de verklaring van gedrag. Het model is al veelvuldig ingezet in het marketing- en gezondheidsdomein, maar wordt sinds kort ook toegepast om veilig digitaal gedrag te verklaren (o.a., van der Kleij et al. (2020)).

Capaciteiten omvat het psychologische en fysieke vermogen van een persoon om bepaald gedrag uit te voeren. Hieronder valt het beschikken over de benodigde kennis en vaardigheden (bijvoorbeeld weten wat een datalek is en hoe daar een melding van te maken). De *gelegenheid* omvat alle factoren die buiten de desbetreffende persoon liggen en die het specifieke gedrag bevorderen of beperken (bijvoorbeeld een toegankelijk meldingssysteem en een veiligheidscultuur waarin melden wordt aangemoedigd). Ook het gedrag van peers speelt hierin een rol (mensen die zich in een vergelijkbare positie of situatie bevinden als iemand anders). *Motivatie* is de laatste determinant en activeert en stuurt het gedrag via cognitieve processen (bijvoorbeeld het erkennen van de voordelen van melden). Dit omvat zowel bewust als automatisch c.q. reflexmatig handelen (i.e., systeem-1 en systeem-2 denken (Kahneman, 2011)); allen het gevolg van de individuele aanleg, leerprocessen en emoties (Michie et al., 2011; Van ’t Hoff - de Goede et al., 2019).

Het COM-B model is tevens bedoeld om te helpen bij het selecteren en ontwerpen van specifieke interventies om gedrag te veranderen. Om dit te ondersteunen, hebben onderzoekers het zogenaamde gedragveranderingswiel (*behaviour change wheel*) ontwikkeld (Michie et al., 2011). Naast de drie bronnen voor gedrag, beschrijven zij daarin negen interventiefuncties (Tabel 4.2) en zeven beleidscategorieën. Die laatste laten we, gelet op de scope van het onderzoek, hier buiten beschouwing.

Tabel 4.2

Interventiefuncties van het gedragsveranderingswiel per gedragsbron (Michie et al., 2011)

Capaciteiten (psychologisch en fysiek)	**Gelegenheid** (sociaal en fysiek)	**Motivatie** (automatisch en reflectief)
Modellering (voorbeeld stellen): Het tonen van gewenst gedrag door rolmodellen, zodat anderen dit gedrag kunnen observeren, leren en overnemen.	Educatie: Het verstrekken van informatie om mensen bewust te maken van het gewenste gedrag en de voordelen daarvan. Dit kan via campagnes, brochures of trainingen.	Faciliteren: Het wegnemen van barrières en het creëren van een ondersteunende omgeving die het gewenste gedrag mogelijk maakt. Dit kan door het verbeteren van infrastructuur of het bieden van hulpmiddelen.
Aanpassen van de omgeving: Het veranderen van de fysieke of sociale omgeving om het gewenste gedrag te bevorderen. Dit kan door het herinrichten van fysieke ruimtes, het herontwerpen van applicaties, of het aanpassen van sociale normen.	Overtuigen: Het gebruik van communicatie om mensen te motiveren en te overtuigen om bepaald gedrag aan te nemen. Dit kan door middel van argumenten, verhalen of emotionele oproepen.	Training: Het bieden van mogelijkheden om vaardigheden en capaciteiten te ontwikkelen die nodig zijn voor het gewenste gedrag. Dit kan via workshops, cursussen of praktijkoefeningen.
Beperking: Het beperken of verminderen van de mogelijkheden om ongewenst gedrag uit te voeren. Dit kan bijvoorbeeld door toegang tot bepaalde middelen of data te beperken.	Prikkelen: Het aanbieden van positieve prikkels of beloningen om gewenst gedrag te stimuleren. Dit kan materieel zijn (zoals geld of cadeaus) of immaterieel (zoals lof of erkenning).	Dwang: Het opleggen van regels of sancties om ongewenst gedrag te ontmoedigen. Dit kan door middel van wetten, boetes of andere strafmaatregelen.

COM-B is in een eerdere studie gebruikt om te bepalen of zogenoemd ‘cybergedrag’ (gebruik van sterke wachtwoorden of het minimaal delen van persoonsgegevens) kan worden verklaard door kennis, motivatie en/of gelegenheid (Van der Kleij et al., 2020). Uit hun literatuurstudie komt naar voren dat deze drie elementen mogelijk essentiële voorspellers zijn voor gedrag. Vervolgens zijn deze drie onderdelen bij hun participanten (*N* = 2.426) bevraagd en de resultaten impliceren dat, op basis van zelfrapportage, de drie elementen samenhangen met zelf-gerapporteerd veilig digitaal gedrag. In hun studie hebben zij tevens daadwerkelijk gedrag in kaart gebracht. Op basis van deze bevindingen komen andere resultaten naar voren, namelijk dat kennis enkel samenhangt met het delen van identiteitsgegevens.

Ook Stokkel et al. (2023) onderzochten het verband tussen COM-B en daadwerkelijk gedrag. In hun onderzoek is een vragenlijst verspreid en een meting uitgevoerd naar daadwerkelijk informatieveilig gedrag onder 12.343 medewerkers. Uit de resultaten komt naar voren dat alle constructen slechts in beperkte mate samenhangen met daadwerkelijk informatieveilig gedrag. Ook uit andere studies komt naar voren dat er vaak een verschil is tussen wat mensen rapporteren en het gedrag dat zij in werkelijkheid vertonen (Parry et al., 2021; Sharif et al., 2018). De meeste studies baseren hun resultaten op zelf-gerapporteerd gedrag, waardoor weinig informatie beschikbaar is over hoe daadwerkelijk gedrag eruitziet; ook op lange termijn.

4.3.4 Practice-informed

Bij het ontwerpen van een interventie is het essentieel om niet uitsluitend te steunen op theoretische modellen of evidence-based inzichten, maar ook expliciet gebruik te maken van practice-informed kennis. Denk hierbij aan ervaringskennis, routines en contextspecifieke inzichten van professionals in het veld (Bluhm et al., 2024-a).

Deze kennis is diepgeworteld in de dagelijkse praktijk en biedt waardevolle informatie over wat werkt, voor wie en onder welke

omstandigheden. Door deze vorm van kennis actief mee te nemen in het ontwerpproces, ontstaat een interventie die niet alleen inhoudelijk relevant is, maar ook aansluit bij bestaande praktijken en (daardoor) beter verankerd raakt in de organisatie. Dit vergroot de kans op draagvlak, praktische toepasbaarheid én duurzame implementatie.

4.4 Werkzame elementen en randvoorwaarden van interventies

In deze paragraaf zijn de resultaten voor de vierde deelvraag opgenomen: *Wat zijn werkzame elementen en randvoorwaarden van interventies gericht op het vergroten van digitale weerbaarheid?* Op basis van deze informatie kunnen we bepalen in hoeverre de bestaande interventies hieraan voldoen. Hierbij maken we onderscheid tussen algemene randvoorwaarden voor interventies (par. 4.4.1), gaan we in op effectmetingen (par. 4.4.2), focussen we op online veilig gedrag (par. 4.4.3) en staan we stil bij ethische richtlijnen (par. 4.4.4).

4.4.1 Algemene randvoorwaarden voor interventies

Volgens Bartholomew Elredge et al. (2016) bestaat het opzetten van een interventie uit zes stappen, gevolgd door de implementatie en evaluatie van de interventie. Zij beschrijven per stap een aantal taken die moeten worden uitgevoerd. Deze stappen fungeren in deze rapportage als vertrekpunt.

De *eerste stap* is het in kaart brengen van de randvoorwaarden van het probleem/de thematiek. Bij deze stap wordt de context van het probleem in kaart gebracht (inclusief populatie/doelgroep en betrokken partijen), een behoeftepeiling uitgevoerd en een algemene doelstelling bepaald. Het kan hierbij tevens gaan om omgevingsfactoren die van invloed kunnen zijn op het probleem.

De *tweede stap* is het bepalen van concrete doelstellingen en uitkomsten van de interventie. Dit zijn bijvoorbeeld kennis en

vaardigheden die deelnemers na afloop dienen te bezitten. De doelstelling moet meetbaar zijn (SMART-geformuleerd), zodat na afloop in kaart kan worden gebracht in hoeverre deze doelstelling is behaald (Bluhm et al., 2024-b). In deze stap worden ook de determinanten in kaart gebracht om de gewenste gedrags- en/of omgevingsverandering teweeg te brengen (doelgedragingen).

De *derde stap* is het ontwerpen van het interventieprogramma. Hierbij gaat het om de invulling van de thema's die in de interventie worden besproken, inclusief de scope. Daarnaast is het van belang om te onderbouwen op welke manier de doelgroep tot stand is gekomen, bijvoorbeeld via een theoretische onderbouwing en/of praktijkervaring. Ook de onderbouwing voor de interventie, zowel theoretisch als praktijkgericht (ervaring professionals, ontwikkelingen op thematiek), dient in kaart te worden gebracht. Hiermee kunnen geleerde lessen in interventies worden geïmplementeerd en wordt voorkomen dat men het wiel opnieuw uitvindt (Al Shaikh et al., 2019; Bluhm et al., 2024-b; Booijink, n.d). Al deze onderdelen worden in deze fase vertaald naar praktisch toepasbare elementen (Bartholomew Elredge et al., 2016).

De *vierde stap* is het produceren van het programma, waarin plannen worden gemaakt voor het materiaal dat gedurende de interventie wordt ingezet. Deze plannen worden vervolgens vertaald naar bruikbare materialen en protocollen, die vervolgens worden opgesteld en eventueel worden verbeterd (Bartholomew Elredge et al., 2016). Dit dient aan te sluiten bij de eerder opgestelde doelstellingen en moet passend zijn voor de doelgroep (Booijink, n.d.). Pas wanneer de eerste vier stappen zijn doorlopen kan worden geëvalueerd in hoeverre bestaande materialen passend zijn ten aanzien van de interventiedoelen (Bartholomew Elredge et al., 2016).

De *vijfde stap* is het opstellen van een implementatieplan. Het nadenken over implementatie begint overigens al bij stap één en loopt door tot en met deze stap (Bartholomew et al., 2016). Bij deze stap worden

de verschillende betrokken partijen gecategoriseerd in gebruikers (de gekozen doelgroep), uitvoerders en onderhouders. Een essentieel onderdeel van deze stap is dat de projectteamleden c.q. initiatiefnemers nadenken over wie de interventie uitvoert. Dit hoeven namelijk niet dezelfde partijen te zijn. De 'onderhouders' kunnen later in het proces een rol spelen. Denk bijvoorbeeld aan een schooldirecteur die meewerkt aan een interventie, en daarna zelf aan de slag gaat om het onderwerp actueel te houden, bijvoorbeeld door nieuw beleid en procedures te implementeren (Bartholomew Elredge et al., 2016).

De *zesde stap* is het opstellen van een evaluatieplan. In dit plan worden de indicatoren opgesteld voor de proces- en effectevaluatie van de interventie (Bartholomew Elredge et al., 2016). Ook aan deze stap wordt dus min of meer al vanaf het eerste moment gewerkt. Daarnaast wordt hierin beschreven hoe de evaluatie wordt uitgevoerd (zie ook par. 4.4.2). Hiervoor is een duidelijke planning van belang, zodat na afloop in kaart kan worden gebracht in hoeverre de interventie is verlopen zoals aanvankelijk is bedacht (procesevaluatie) en wat de uitkomsten ervan zijn (effectevaluatie).

Gedurende het verloop van de interventie kan tevens gemonitord worden welke (tussentijdse) resultaten worden behaald (Bluhm et al., 2024-b). Voor beide evaluaties is het van belang om gebruik te maken van een bepaalde methodiek, zodat gestructureerd in kaart wordt gebracht hoe dit is verlopen. Voor een procesevaluatie kan bijvoorbeeld gebruik worden gemaakt van de QUALIPREV methodiek.[9] Dit is een laagdrempelige methodiek om de kwaliteit van de interventie en de uitvoering ervan te bepalen. De mogelijke uitvoering van een effectevaluatie bespreken we in paragraaf 4.4.2.

[9] https://eucpn.org/document/qualiprev-assessment-tool-for-prevention-initiatives

Na het uitvoeren van deze zes stappen wordt de interventie daadwerkelijk geïmplementeerd en geëvalueerd. Vanuit deze evaluatie kunnen de zes stappen opnieuw worden gevolgd om de interventie te verbeteren (Bartholomew Elredge et al., 2016).

4.4.2 Effectmeting

Nijland et al. (2018) passen het RE-AIM-raamwerk toe. Volgens dit raamwerk bepalen de effectiviteit en uitvoering samen in hoeverre een interventie effect kan hebben. Dit raamwerk beschrijft vijf aspecten waaraan interventies dienen te voldoen (Glasgow et al., 1999):

- *Reach*: het inzetten op het bereiken van de doelgroep.
- *Effective*: het inzetten van effectieve elementen in een interventie, passend bij de doelgroep.
- *Adoption*: de bereidheid van de uitvoerders van de interventie om deze goed uit te voeren.
- *Implementation*: het uitvoeren van de interventie volgens het aanvankelijk opgestelde plan, waarbij de werkzame elementen op een correcte manier worden ingezet.
- *Maintenance*: het aanvankelijk nadenken over de borging van de interventie.

Bij een effectmeting is een nulmeting essentieel. Met een nulmeting wordt de huidige stand van zaken in kaart gebracht. Hoe deze nulmeting wordt vormgegeven, is afhankelijk van de situatie. Na het uitvoeren van de interventie kan een eenmeting worden uitgevoerd, waarmee het mogelijke effect van de interventie wordt gemeten. Hierbij dienen dezelfde aspecten te worden gemeten als in de nulmeting (NCSC, 2025). Dit wordt ook wel aangeduid als een pre-post-design. Dit kan desgewenst worden uitgebreid met follow-up metingen om de stabiliteit van effecten over de tijd te meten. Bijvoorbeeld na drie maanden (korte termijn), zes maanden (middellange termijn) en twaalf maanden (lange termijn).

Bij het evalueren van interventies gericht op het vergroten van digitale weerbaarheid onder ouderen, kan het uitvoeren van een klassieke nul- en eindmeting niet altijd haalbaar zijn. Dit heeft enerzijds te maken met praktische belemmeringen, zoals beperkte tijd, middelen en capaciteit om twee metingen af te nemen, en anderzijds met inhoudelijke uitdagingen. Ouderen beschikken aan het begin van een interventie mogelijk nog niet over voldoende kennis van het onderwerp, waardoor zij niet in staat zijn om hun beginsituatie realistisch te beoordelen. Dit wordt ook wel *response shift bias* genoemd. Deze bias kan ertoe leiden dat de uitkomsten van een traditionele pre-postmeting een vertekend beeld geven van de werkelijke effectiviteit van de interventie.

Een passend alternatief lijkt het zogenoemde 'retrospective post-then-pre design', waarbij deelnemers aan het einde van een interventie zowel hun huidige situatie als (hun terugblik op) de beginsituatie rapporteren (The Board of Regents of the University of Wisconsin, 2021). Doordat beide beoordelingen plaatsvinden ná afloop van de interventie, hebben deelnemers een beter referentiekader om hun eigen ontwikkeling in te schatten. Zeker bij ouderen, voor wie abstracte digitale concepten mogelijk minder vertrouwd zijn, biedt deze aanpak een laagdrempelige en efficiënte manier om veranderingen in kennis, vaardigheden of houding ten aanzien van digitale veiligheid in kaart te brengen. Bovendien maakt deze methode het mogelijk om data anoniem te verzamelen zonder dat vooraf complexe koppelingen nodig zijn tussen meetmomenten.

Effectevaluaties kunnen positieve, negatieve of gemixte effecten als uitkomst hebben, of helemaal geen effect laten zien. Het is belangrijk om redenen daarachter inzichtelijk te maken (Bartholomew Elredge et al., 2016). Het belang van een evaluatie geldt niet alleen voor de individuele interventie en de daarbij betrokken partijen, maar is ook van belang als we als maatschappij op een systematische wijze willen werken aan het verhogen van de digitale weerbaarheid.

Ten slotte richten we ons op de implementatie van de interventie. Een goed implementatieproces is van essentieel belang voor de uitvoering en mogelijke effectiviteit van de interventie (Daamen, 2015; Durlak & DuPre, 2008). Stals (2012) onderscheidt vier stappen in dit implementatieproces. Per fase kunnen verschillende activiteiten worden ingezet. Deze worden in het rapport van Daamen (2015) nader toegelicht.

1. *Verspreiding*: de betrokkenen nemen kennis van de interventie.
2. *Adoptie*: de betrokkenen ontwikkelen een positieve houding ten opzichte van de interventie en besluiten deze uit te gaan voeren.
3. *Invoering*: de betrokkenen voeren de interventie daadwerkelijk uit.
4. *Borging*: de betrokkenen hebben de interventie onderdeel gemaakt van de reguliere werkzaamheden.

4.4.3 Interventies gericht op online veilig gedrag

Daarnaast hebben we in de literatuur gezocht naar interventies die zich richten op het thema digitale veiligheid om te bepalen in hoeverre bepaalde elementen hierin noodzakelijk zijn. Een meta-analyse richt zich op de effecten van interventies gericht op social-engineeringsaanvallen (Bullée & Junger, 2020). De auteurs impliceren dat, op basis van hun analyse, een ideale interventie aan vier onderdelen voldoet:

1. De interventie heeft een interactief karakter (bijvoorbeeld met spelelementen).
2. Als de interventie wordt uitgevoerd is er contact met de deelnemers (bijvoorbeeld middels een les).
3. De interventie richt zich op concrete onderwerpen binnen een overkoepelend thema.
4. De interventie is enigszins intensief.

In een andere studie zijn diverse bewustwordingscampagnes gericht op digitale veiligheid onderzocht (Bada et al., 2019). Uit de resultaten komt naar voren dat een aantal factoren een positieve invloed kunnen hebben op de effectiviteit van huidige en toekomstige campagnes, zoals (1) dat het opwekken van enkel angst geen effectieve tactiek lijkt te zijn; en (2) dat educatie verder moet gaan dan het enkel aanbieden van kennis aan deelnemers. De kennis die wordt aangereikt, dient gericht, actiegericht, uitvoerbaar en feedback te bevatten. Verder geven ze aan (3) dat op het moment dat deelnemers het gewenste gedrag willen uitvoeren, training en feedback tijdens dit proces noodzakelijk is; en (4) dat het belangrijk is om culturele en persoonlijke kenmerken mee te nemen.

Het enkel aanbieden van kennis en bewustwording over het gewenste gedrag lijkt dus onvoldoende te zijn om een gedragsverandering teweeg te brengen (Bada et al., 2019; Van Steen, 2024). Daarnaast komt naar voren dat bewustwording geen opzichzelfstaand element is in veelgebruikte theoretische modellen, zoals PMT, RAA en COM-B (zie par. 4.3). Veelal is bewustwording onderdeel van bestaande elementen, zoals de constructen ‘dreiging’ in PMT of ‘motivatie’ in COM-B. Het enkel inzetten op bewustwording om een positieve gedragsverandering teweeg te brengen, lijkt dus onvoldoende te zijn. Hiermee lijkt enkel bewustwording over het gewenste gedrag te worden gecreëerd in plaats van dat het gewenste gedrag daadwerkelijk wordt uitgevoerd. Er zitten mogelijk een aantal stappen tussen bewustwording en het uitvoeren van het gewenste gedrag (Van Steen, 2024).

Traditionele overheidscampagnes waarmee wordt gepoogd om gedragsverandering teweeg te brengen, zijn veelal gebaseerd op de aanname dat wanneer mensen zich bewustzijn van een risico zij het gedrag gaan vertonen om dat risico tegen te gaan (Van Steen et al., 2020). Desalniettemin, blijkt dus dat enkel het inzetten op bewustwording onvoldoende is (Bada et al., 2019) en dat campagnes moeten worden uitgebreid, zodat gedragsverandering wel plaats zou kunnen vinden

(Ashenden & Lawrence, 2013). De focus verschuift hiermee van bewustwording naar vaardigheden (ENISA, 2019). Een eerste stap om van bewustwordingscampagnes naar daadwerkelijke gedragsverandering te gaan, is door te focussen op specifieke gedragingen en doelgroepen, waarbij onderscheid wordt gemaakt in hoeverre een gedraging relevant is voor een specifiek delict of meerdere delicten. Hedendaagse campagnes maken daarentegen veelal gebruik van een '*one-size-fits-all*'-principe (Van Steen et al., 2020).

4.4.4 Ethische richtlijnen

Ten slotte is het van belang om bij het opzetten en uitvoeren van een interventie ethische richtlijnen in acht te nemen (Nederlands Instituut van Psychologen, n.d.). In de literatuur wordt onderscheid gemaakt tussen vijf ethische principes:

1. Het nemen van verantwoordelijkheid voor de gedragsbeïnvloeding die plaatsvindt. Betrokkenen bij de interventie dienen rekening te houden met het voorkomen/beperken van eventuele schade en kennismisbruik. Daarnaast is het van belang om anderen op het ethisch handelen te attenderen.
2. De gedragsbeïnvloeding is integer. Dit betekent dat de beïnvloeding en/of aangereikte informatie op een betrouwbare manier plaatsvindt en de betrokkenen (bijvoorbeeld uitvoerders) openheid tonen over de kwalificaties die zij bezitten. Hiermee voorkomen zij het veroorzaken van mogelijke misleiding.
3. De gedragsbeïnvloeding dient op een gerespecteerde manier plaats te vinden. Hierbij wordt expliciet aandacht besteed aan de doelgroep en mogelijke kwetsbare leden van de doelgroep.
4. De gedragsbeïnvloeding vindt op een deskundige manier plaats. Betrokkenen dienen rekening te houden met ontwikkelingen in het vakgebied en de eigen professionele grenzen te bewaken.

5. Het gebruik van data vindt op een rechtmatige en betrouwbare manier plaats. Dit betekent dat de betrokkenen rekening houden met de privacywetgeving en zorg dragen voor valide data.

4.5 Bereiken van de doelgroep ouderen

De voorgaande resultaten richten zich voornamelijk op interventies in de breedste zin van het woord. In het huidige project richten we ons op één specifieke doelgroep, namelijk ouderen. Het is essentieel om een interventie af te stemmen op de voorkeuren, kenmerken, percepties en huidige gedragingen van de doelgroep (Kievik, 2017). Daarom is het van belang om tevens in kaart te brengen hoe we deze doelgroep kunnen bereiken. Hiervoor is de vijfde deelvraag opgesteld: *Op welke manieren kan de doelgroep ouderen worden bereikt om hen deel te laten nemen aan interventies gericht op het vergroten van de digitale weerbaarheid?* Hiervoor hebben we eerst in de literatuur gezocht naar *best practices* (par. 4.5.1). Daarnaast is in de startbijeenkomst aan de betrokken partijen gevraagd op welke manier(en) zij de doelgroep bereiken (par. 4.5.2).

4.5.1 Bevindingen literatuur

Om te bepalen welke manieren/kanalen volgens de theorie ingezet kunnen worden om ouderen te bereiken, hebben we literatuuronderzoek verricht. Hiervoor hebben we gefocust op het bereiken van ouderen voor interventies in het algemeen in plaats van enkel te focussen op het werven van ouderen voor digitale weerbaarheidsinterventies. We kunnen mogelijk lering trekken uit de werving voor andere initiatieven.

Uit de literatuur komt naar voren dat het betrekken van de ouderenbond bij eerdere interventies is uitgevoerd. Zij kunnen hun leden informeren over interventies, bijvoorbeeld middels (online) nieuwsbrieven en het blad van de ouderenbond. Ook reclame maken in huis-aan-huisbladen en de lokale, regionale of wijkkrant wordt genoemd (Bluhm et al., 2024-a; Fokkema & Van Tilburg, 2006; Preller & de Zeeuw, 2018).

Fokkema en Van Tilburg (2006) benoemen tevens het verspreiden van folders (in buurthuizen), het informeren van welzijns- en gemeentelijke instanties en het aankondigen van de interventie op (regionale) radiozenders als opties om de doelgroep te werven. Het inzetten van enthousiaste peers, sleutelfiguren of boegbeelden voor de doelgroep kan mogelijk ook helpen om ouderen te enthousiasmeren voor een interventie (Preller & De Zeeuw, 2018). Daarnaast stellen zij voor om betrokkenen bij een interventie aan te laten sluiten bij bijeenkomsten die de doelgroep toch al bezoekt, zodat zij op die manier geïnformeerd kunnen worden over de interventie.

Burton et al. (2022) noemen informatiecampagnes gericht op werknemers die in contact staan met ouderen en familieleden van ouderen als mogelijkheid om de doelgroep te bereiken. Deze tussenpersonen kunnen hulp bieden bij het detecteren en oplossen van incidenten; ook wanneer ouderen zich niet bewust van slachtofferschap zijn.

Van Scherpenseel et al. (2022) hebben verschillende manieren in kaart gebracht om de doelgroep ouderen te bereiken voor valpreventie-interventies. Hiervoor hebben zij eerst bevorderlijke en belemmerende factoren middels literatuuronderzoek en het interviewen van de doelgroep voor deelname aan valpreventie-interventies in kaart gebracht. De meest genoemde bevorderlijke factoren zijn sociale interactie en het vooruitzicht om onafhankelijk te blijven na deelname aan de interventie. De meest genoemde belemmeringen die hierbij naar voren is gekomen, zijn een negatief stigma rondom het probleem, waardoor de doelgroep zich niet aangesproken kan voelen, en interventies die niet op maat gemaakt zijn. In hun artikel beschrijven zij vervolgens zes potentiële strategieën om de doelgroep te bereiken:

1. Het framen van de interventie, waarbij het van belang is om positieve formuleringen te gebruiken in plaats van negatief beladen formuleringen.

2. Het informeren over de voordelen, waarbij het van belang is om dit op een realistische manier te doen.
3. Het bewustmaken van risico's, waarbij objectieve informatie, zoals prevalentie, wordt aangereikt.
4. Het gebruik maken van de sociale omgeving om de doelgroep te bereiken en het gesprek te starten. Het kan gaan om bestaande netwerken, verenigingen en georganiseerde activiteiten.
5. Het aanbieden van interventies op maat en aansluiten bij onderliggende behoeften, zoals het samenzijn met anderen.
6. Het rekening houden met praktische randvoorwaarden, zoals toegankelijkheid (locatie, bereikbaarheid, kosten).

4.5.2 Mogelijkheden vanuit partners

Daarnaast is tijdens de startbijeenkomst aan de betrokken partners gevraagd op welke manier zij de doelgroep ouderen (trachten te) bereiken. Deze bevindingen zijn in tabel 4.2 gerapporteerd.

Tabel 4.2: Bereiken van de doelgroep via partners

Partij	**Manieren om doelgroep te bereiken**
Politie	Zorgorganisaties: wijkzorg/verpleging Media (brochures, radio, televisie, video, podcasts) Sociale media (via wijkagenten) Ouderenorganisaties (hobbyclubs, regionale plaatselijke belangenclubs) Beurzen Ambassadeurs Communicatie vanuit politieoverleg
Rabobank	Op locatie en telefonisch het gesprek aangaan
SeniorWeb	Samenwerkingen Nieuwsbrief en andere media
CCV	Fraudehelpdesk Vrijwilligerspoules (Pilot in Oost-Nederland)

Tabel 4.2 (vervolg): Bereiken van de doelgroep via partners

Partij	Manieren om doelgroep te bereiken
Openbaar Ministerie (OM)	Openbaar Ministerie (OM)
Koninklijke Bibliotheek (KB)	Fysieke locaties bibliotheek
MeiJo	Nieuwsbrief naar leden Cliënten van kwadrantgroep

4.6 Werkzame elementen en randvoorwaarden voor de doelgroep ouderen

Om te bepalen welke elementen in interventies voor de doelgroep ouderen relevant zijn, worden hier de resultaten voor de zesde deelvraag gepresenteerd: *Welke werkzame elementen en randvoorwaarden van interventies zijn relevant voor de doelgroep ouderen?*

4.6.1 Werkzame elementen in interventies

Preller en De Zeeuw (2018) hebben mogelijk werkzame elementen voor interventies in kaart gebracht die gericht zijn op het meer te laten bewegen van ouderen. Zij onderscheiden hierbij de volgende elf punten:

1. De interventie is persoonsgericht; afgestemd op de interesses en voorkeuren van de doelgroep.
2. Samenwerken met uitvoerders van de interventie die gekwalificeerd zijn en ervaring te hebben in het uitvoeren van interventies bij de doelgroep. Deze uitvoerders hebben affiniteit met de doelgroep en zijn in staat om het niveau van de interventie afstemmen op het individu en/of de groep.
3. Het inzetten op positiviteit, bijvoorbeeld wat zij met de interventie kunnen bereiken in plaats van de focus op de negatieve aspecten van het te bespreken fenomeen.
4. Het benadrukken en inzetten op de sociale voordelen die de interventie teweeg kan brengen, bijvoorbeeld het sociale contact

met andere leden van de doelgroep. Ouderen hechten hier mogelijk waarde aan.

5. De interventie uit verschillende onderdelen laten bestaan. Deze afwisseling werkt mogelijk bevorderlijk, omdat een combinatie van elementen de kans vergroot voor een blijvende deelname.
6. Het inzetten op het bevorderen van de eigen effectiviteit, i.e., zelfeffectiviteit; het vertrouwen in het eigen kunnen om een bepaald gedrag te vertonen. Dit kan bijvoorbeeld worden gedaan door angst voor het thema weg te nemen.
7. De omgeving van de interventie passend laten zijn bij de kenmerken van de doelgroep, waarbij rekening wordt gehouden met angst voor negatieve effecten of negatieve associaties.
8. Het aanpassen van de intensiteit van de oefeningen/inhoud op de doelgroep.
9. De informatie in de interventie relevant maken voor het dagelijks leven van de doelgroep.
10. Het samen met de doelgroep reflecteren op de resultaten/ gemaakte keuzes. Dit kan mogelijk bijdragen aan de motivatie van de deelnemers.
11. De duur en het aanbod van de interventie lang genoeg laten zijn om een duurzame gedragsverandering teweeg te brengen. Dit kan onder andere door een nazorgtraject aan te bieden na de interventie om terugvalgedrag te voorkomen. Bij kortdurende interventies dient er sowieso een vervolgaanbod te zijn. Hierbij is het van belang dat er geen gat valt tussen de initiële interventie en het vervolgaanbod en dat het nieuwe aanbod op dezelfde locatie wordt aangeboden als de initiële interventie.

Aanvullend benoemt Dijkstra (2009) dat in een gemiddeld verouderingsproces de cognitieve vaardigheden van ouderen enigszins afnemen. Het duurt bij ouderen bijvoorbeeld langer om aangeleverde

informatie te verwerken en te onthouden. Hierbij gaat het veelal om informatie en vaardigheden die weinig tot niet worden ingezet.

Zaid et al. (2022) onderzochten vijftien interventies die zich richten op het verbeteren van digitale geletterdheid bij ouderen. Uit hun review komt naar voren dat goede communicatie binnen de interventie en het inzetten van een specifieke manier van leren van essentieel belang zijn. Een manier om deze communicatie tot stand te brengen, is door een intergenerationele manier van leren in te zetten, waarbij jongeren de ouderen iets leren. Voorbeelden zijn het inzetten van (klein)kinderen (Rolandi et al., 2022; Zaid et al., 2022). Dit kan door ouderen als prettig worden ervaren. Ouderen zouden zich comfortabel voelen om kennis op te doen met anderen die meer kennis hebben van technologische middelen en de jongeren hebben geduld om de vaardigheden aan te leren. Voorbeelden van interventies gericht op digitale weerbaarheid waarin dit principe tot uiting komt zijn HackShield uit Nederland (Bluhm et al., 2024-b) en The Cyber School for Grandparents, uit Italië (Rolandi et al., 2022).

Andere communicatieaspecten die worden aangehaald, zijn groepsactiviteiten en het gezamenlijk leren (Nicholson et al., 2021). In dit laatste geval zou het gezamenlijk opdoen van kennis effectiever zijn dan wanneer ouderen dit alleen zouden doen. In deze review wordt tevens een voorbeeld aangehaald, waarin ouderen gezamenlijk een (realistisch) probleem oplossen. Hierdoor zou zowel hun cognitieve als probleemoplossend vermogen verbeteren en zouden zij de geleerde lessen in toekomstige scenario's kunnen toepassen. In het verlengde hiervan worden interactie tussen de deelnemers en andere betrokkenen, en een comfortabele leeromgeving als essentieel gezien. Ook het aanhalen van herkenbare situaties en hen kennis laten opdoen met behulp van technologie kan helpen om zogenoemde cyberfobie af te laten nemen (Zaid et al., 2022).

5 Conclusie en discussie

In dit hoofdstuk zijn als eerste de antwoorden op de verschillende deelvragen gerapporteerd (par. 5.1). Op basis van deze bevindingen hebben we de hoofdvraag beantwoord (par. 5.2). Vervolgens zijn de discussie (par. 5.3) en beperkingen (par. 5.4) beschreven.

5.1 Beantwoording deelvragen

5.1.1 Welke bestaande interventies richten zich op het vergroten van digitale weerbaarheid van ouderen?

De eerste deelvraag richt zich op welke bestaande interventies gericht op het vergroten van de digitale weerbaarheid van ouderen. Om deze vraag te beantwoorden, hebben we ons beperkt tot de interventies uit de database Lokale cyberprojecten van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en interventies die door de betrokken partijen worden uitgevoerd.

De betrokken partners voeren opgeteld elf interventies uit. De Rabobank voert drie interventies uit: (1) het geven van een presentatie over veilig bankieren (in samenwerking met SeniorWeb); (2) het inzetten van internet- en sociale mediacampagnes gericht op (de gevaren van) online oplichting; en (3) het organiseren van cybermarkten. SeniorWeb voert twee interventies uit: (4) het organiseren van webinars (in samenwerking met de Fraudehelpdesk); en (5) het organiseren van activiteiten in themamaanden in de 520 leslocaties. Uit de database van het CCV komt naar voren dat drie interventies zich richten op de doelgroep ouderen: (6) ‘Storytelling Cybercrime’; (7) de interactieve film ‘Echt of nep?’; en (8) de serious game ‘Cyberweerbaar op het web’. De Koninklijke Bibliotheek (KB) voert twee interventies uit, namelijk: (9) de kleinste privacyshow van Nederland; en (10) een nationale cursus gericht op digitale weerbaarheid. MeiJo organiseert ten slotte (11) cafébijeenkomsten over het thema.

5.1.2 Welke gedragsonderwerpen of -categorieën worden binnen interventies aangesproken om de digitale weerbaarheid van deelnemers aan die interventies te vergroten?

Voor de beantwoording van de tweede deelvraag hebben we in de literatuur gekeken naar het gewenste gedrag op het gebied van digitale veiligheid. De literatuur laat zien dat er geen uniform of definitief antwoord is. Desalniettemin, zien we een aantal gedragingen die veelal naar voren komen, namelijk:

- Het gebruik van sterke wachtwoorden en het veilig managen hiervan
- Het installeren van updates om software up-to-date te houden
- Het gebruik van beveiligingssoftware (antivirus, firewalls)
- Het alert zijn tijdens internetgebruik (gebruik maken van beveiligde sites/services/connecties, voorzichtigheid met bijlagen/hyperlinks in e-mails en uitloggen op websites na gebruik)
- Het minimaal delen van persoonlijke gegevens
- Aangifte/melding doen bij slachtofferschap van online criminaliteit

Hierbij moet worden gezegd dat bovenstaande gedragingen algemene gedragingen betreffen die iets zeggen over iemands zogenoemde cyberhygiëne en niet per definitie over de digitale weerbaarheid. Net zoals persoonlijke hygiëne helpt om de gezondheid en het welzijn van een individu te behouden, helpt cyberhygiëne om gegevens veilig en beschermd te houden tegen diefstal en aanvallen van buitenaf. Als individuen zich tegen bepaalde vormen van online criminaliteit willen beschermen, staan specifiekere doelgedragingen centraal, wat mogelijk een positief effect heeft op het uiteindelijke gedrag. Denk bijvoorbeeld aan het niet zomaar toegang geven tot een computer aan onbekenden die zich voordoen als bankmedewerkers in geval van bankhelpdeskfraude. Een ander voorbeeld is het via een ander kanaal direct contact opnemen met

iemand die om geld vraagt om de echtheid van het bericht te verifiëren in geval van vriend-in-noodfraude.

5.1.3 Welke theoretische constructen/modellen/theorieën verklaren de ontwikkeling of het vergroten van digitale weerbaarheid?

Uit de wetenschappelijke literatuur komen diverse theorieën, raamwerken en modellen naar voren die zich richten op gedragsverandering en in diverse gevallen zijn toegepast op digitaal veilig gedrag. Voor het huidige onderzoek hebben we een theorie, een theoretisch raamwerk en een model nader uitgelegd, namelijk de *Protection Motivation Theory (PMT),* de *Reasoned Action Approach (RAA),* en het *Capability-Opportunity-Motivation-Behaviour model (COM-B)*.

Als we deze samennemen, zien we dat intenties in theorie voorafgaan aan daadwerkelijk gedrag. Er zit echter een gat tussen intentie en gedrag (Sheeran, 2002). Mensen beweren vaak bepaald (veilig) gedrag te willen vertonen, maar dit gebeurt niet altijd in de praktijk. Verschillende factoren hebben hier invloed op, zoals gewoontegedrag, eerdere ervaringen en daadwerkelijke vaardigheden (Fishbein & Ajzen, 2010).

PMT stelt dat er bij een confrontatie met risico's of bedreigingen twee cognitieve processen gelijktijdig optreden: (1) het evalueren van de dreiging en (2) het evalueren van de te nemen maatregelen. De uitkomst van dit proces bepaald in hoeverre een individu gemotiveerd is (intentie) om beschermende maatregelen te nemen. Wanneer we kijken naar PMT in relatie tot digitale dreigingen en risico's zien we dat zelfeffectiviteit en responseffectiviteit de meeste invloed lijken te hebben op de motivatie om maatregelen te nemen, al is de evaluatie van de dreiging ook van belang.

Vanuit RAA zijn drie componenten van invloed op de intentie tot gedrag, waarbij gepercipieerde (ervaren) gedragscontrole sterke overeenkomsten heeft met zelfeffectiviteit. RAA omvat daarnaast nog de houding van een individu tegenover het gedrag en de gepercipieerde (ervaren) norm (descriptief en injuctief). Deze norm wordt beïnvloed door

wat men anderen ziet doen (descriptief) en wat men denkt dat anderen ergens van vinden (injuctief).

Vanuit COM-B wordt ook nadrukkelijk de motivatie benoemd als een van de drie criteria die aanwezig moet zijn om gedragsverandering te realiseren. Daarnaast stelt dit model dat ook voldoende capaciteiten aanwezig moeten zijn om het gedrag uit te voeren (onder andere kennis en vaardigheden). Dit sluit sterk aan op het construct 'zelfeffectiviteit' uit PMT en 'gepercipieerde gedragscontrole' uit RAA. Tot slot moet een individu in de gelegenheid worden gesteld om het gedrag daadwerkelijk uit te voeren, waarbij ook faciliterende aspecten in de (directe) omgeving en fysieke context een rol spelen. Interventies lijken zich nog weinig op dit criterium te richten.

Kortom, om gedragsverandering te realiseren moet aan diverse aspecten aandacht worden gegeven. Om daadwerkelijk in actie te komen moet men zowel de risico's als oplossingen kennen, kunnen en willen uitvoeren en zich in een omgeving begeven die daarin ondersteund en faciliteert.

Tot slot zien we dat lering getrokken kan worden uit de praktijk, bijvoorbeeld door te kijken naar de ervaringen van professionals en ontwikkelingen binnen de doelgroep.

5.1.4 Wat zijn werkzame elementen en randvoorwaarden van interventies gericht op het vergroten van digitale weerbaarheid?

Een solide basis is belangrijk voor een succesvolle interventie en effect bij de doelgroep. Uit de literatuur komt naar voren dat het opzetten van een interventie doorgaans uit zes stappen bestaat, waarbij elke stap specifieke taken en activiteiten omvat. Het systematisch in kaart brengen van deze stappen is van belang voor de evaluatie, omdat het inzicht biedt in de mate waarin de interventie is uitgevoerd zoals oorspronkelijk bedoeld.

De eerste stap is het in kaart brengen van (de randvoorwaarden van) het thema, inclusief behoeftepeiling, context en een algemene

doelstelling. De tweede stap betreft het bepalen van concrete doelstellingen en uitkomsten van de interventie. Deze doelstelling dient concreet en meetbaar (SMART) geformuleerd te zijn. Daarnaast is het formuleren van doelgedragingen onderdeel van deze stap. De derde stap is het ontwerpen van het interventieprogramma. Hierbij wordt invulling gegeven aan thema's binnen de interventie en wordt de doelgroep nader gedefinieerd. De bevindingen worden vertaald naar praktisch toepasbare elementen in een interventie.

De vierde stap is het produceren van het programma, waarbij plannen worden gemaakt voor het materiaal dat onderdeel is van het programma. Deze materialen sluiten aan bij de eerder opgestelde doelstellingen en de doelgroep. Stap vijf is het opzetten van een implementatieplan, al wordt hier vanaf stap één al over nagedacht. Het vormgeven van het implementatieproces kan conform de volgende vier fasen: (1) verspreiding, (2) adoptie, (3) invoering en (4) borging. De zesde stap is het opzetten van een evaluatieplan, waarin indicatoren worden geformuleerd zowel de proces- als de effectevaluatie. Hoewel deze stap formeel als laatste wordt benoemd, begint het opzetten van het evaluatieplan feitelijk al vanaf stap één en loopt het als een rode draad door het gehele interventieproces.

Hoewel de presentatie van de zes stappen de indruk kan wekken dat het om een lineair proces gaat, benadrukken Bartholomew Eldredge et al. (2016) dat het plannen van interventies juist gezien moet worden als een iteratief proces, waarin terugkoppeling, bijstelling en herziening voortdurend plaatsvinden.

Uit een meta-analyse komt verder naar voren dat een effectieve interventie idealiter voldoet aan de volgende vier kenmerken: (1) een interactief karakter; (2) direct contact met deelnemers tijdens de uitvoering; (3) een duidelijke focus op een concreet en relevant thema; en (4) een zekere mate van intensieve participatie door de deelnemers.

Meer onderzoek is nodig om harde uitspraken te kunnen doen over wat werkt, voor wie, onder welke condities en voor hoe lang. Wel is duidelijk dat bewustwording alleen onvoldoende is om doelgroepen over te laten gaan tot digitaal veilig gedrag. Aannames dat bijvoorbeeld meer kennis leidt tot verandering in gedrag zijn dan ook niet juist.

Om veilig gedrag te promoten, kunnen aanpassingen worden gemaakt in systemen en processen (*by design*), maar ook interventies worden ontwikkeld voor de doelgroepen. De interventies kunnen zich richten op een of meerdere elementen die zijn beschreven in de vorige paragraaf. Omdat we het over menselijk gedrag hebben en de elementen en constructen relatief subjectief van aard zijn en van persoon tot persoon kunnen variëren, is het belangrijk om deze te meten.

Dit doen we het liefst allereerst *voorafgaand* aan een interventie om de huidige stand van zaken in kaart te brengen (nulmeting). Dit betekent dat naast een concrete doelstelling ook concrete doelgedragingen geformuleerd moeten worden. Hoewel we het een nulmeting noemen, spreken we niet per se van een nul-situatie, omdat de meeste mensen in bepaalde mate wel eens zijn geconfronteerd met risico's of risicocommunicatie. Vervolgens wordt *na* de interventie opnieuw gemeten hoe het ervoor staat (eenmeting), bij voorkeur meerdere keren, om te kijken in hoeverre een effect is opgetreden en hoe lang dit effect zichtbaar is. In het geval dat een dergelijke effectmeting niet haalbaar is, lijkt het 'retrospective post-then-pre design' een passend alternatief te zijn. Bij deze evaluatiemethode rapporteren deelnemers aan het einde van een interventie zowel hun huidige situatie (post) als de beginsituatie (then-pre).

Het is gewenst dat de effectmeting door een onafhankelijke partij wordt uitgevoerd, zodat een objectief oordeel kan worden gegeven. De opgehaalde informatie van deze effectiviteit kan worden gedeeld met (toekomstige) gebruikers, zodat zij hier tevens lering uit kunnen trekken.

Ten slotte is het van belang om rekening te houden met de ethische richtlijnen. In de literatuur worden vijf leidende principes onderscheiden

voor verantwoorde gedragsbeïnvloeding: het nemen van verantwoordelijkheid, het handelen met integriteit, het respectvol benaderen van de doelgroep, het werken vanuit deskundigheid, en het zorgvuldig en rechtmatig omgaan met data.

5.1.5 Op welke manieren kan de doelgroep ouderen worden bereikt om hen deel te laten nemen aan interventies gericht op het vergroten van de digitale weerbaarheid?

Voor de beantwoording van de vijfde deelvraag hebben we in de literatuur gezocht naar manieren om de doelgroep ouderen voor interventies te bereiken. Hierbij is de scope verbreed door ook te kijken naar interventies voor ouderen gericht op andere thema's, omdat hier mogelijk lering uit kan worden getrokken. Daarnaast is in de startbijeenkomst op 25 september 2024 aan betrokken partijen gevraagd welke manieren/kanalen zij (kunnen) inzetten om de doelgroep te bereiken.

Manieren om de doelgroep te bereiken

Uit de literatuur komt naar voren dat het inzetten van een voor de ouderen bekende partij veelal plaatsvindt. De ouderenbond wordt in onderhavige context genoemd, omdat zij in contact staan met de doelgroep en hun leden over de interventie kunnen informeren. Dit kunnen zij bijvoorbeeld doen door reclame te maken voor de interventie in (online) nieuwsbrieven of het blad van de ouderenbond. Daarnaast kan informatie over de interventie worden verspreid op plekken en kanalen die aansluiten bij doelgroep, i.e., waar de doelgroep aanwezig is of bekend mee is.

Als het gaat om het inzetten van media, worden vooral lokale initiatieven genoemd. Hierbij gaat het bijvoorbeeld om reclame maken op (regionale) radiozenders en in regionale- en/of wijkkranten, en het verspreiden van folders op veel bezochte plekken, zoals buurthuizen, welzijns- en/of gemeentelijke organisaties. Ten slotte wordt benoemd dat de interventie kan aansluiten bij bestaande initiatieven waar de doelgroep

al betrokken is en kan de sociale omgeving, waaronder enthousiaste peers, actief worden ingezet om het bereik te vergroten.

Let op dat verdere afbakening van de doelgroep 'ouderen' gewenst is. Zo laten cijfers van het CBS bijvoorbeeld zien dat op 1 januari 2024 in Nederland bijna 3,7 miljoen 65-plussers kent.[10] De groep 55-plussers is dus nog groter en diverser. Het Loket Gezond Leven van het Rijksinstituut voor Volksgezondheid en Milieu stelt dan ook dat dé oudere niet bestaat.[11] Het betreft een diffuse doelgroep met verschillende eigenschappen en voorkeuren, ook qua bereik en interventies

Uit de startbijeenkomst komt daarnaast naar voren dat partijen verschillende kanalen (kunnen) inzetten om de doelgroep te bereiken. Hierbij komen veelal dezelfde manieren naar voren als die in de literatuur zijn genoemd, namelijk het inzetten van verschillende (sociale) mediakanalen, contact met partijen die als sleutelfiguur kunnen dienen en het aansluiten bij initiatieven die reeds worden uitgevoerd.

Framing van de informatie

De framing van de informatie over de interventie lijkt tevens van belang te zijn. Het thema dat tijdens interventies wordt besproken, dient positief te zijn geformuleerd. Hiermee zou de doelgroep zich meer aangesproken voelen dan wanneer dit negatief wordt geformuleerd. Wanneer een negatieve formulering wordt gebruikt, kan het zijn dat de doelgroep dit als stigma ervaart en zich niet aangesproken voelt. Ook in een recente studie naar mensgerichte cyberweerbaarheid komt het positief formuleren van boodschappen rondom digitale veiligheid terug als een belangrijke basisregel (Spithoven et al., 2024).

[10] https://www.cbs.nl/nl-nl/visualisaties/dashboard-bevolking/leeftijd/ouderen
[11] https://www.loketgezondleven.nl/gezondheidsthema/gezond-en-vitaal-ouder-worden/feiten-en-cijfers-ouderen

Daarnaast is het belangrijk dat voor de doelgroep aanvankelijk duidelijk is welke voordelen deelname aan de interventie heeft. Enerzijds kan dit betrekking hebben op de voordelen die specifiek voortkomen uit de besproken thematiek. Anderzijds kunnen ook bijkomende voordelen worden benoemd, zoals de sociale setting waarin de interventie plaatsvindt. Mogelijk kan dit de doelgroep aanspreken om aan de interventie deel te nemen.

5.1.6 Welke werkzame elementen en randvoorwaarden van interventies zijn relevant voor de doelgroep ouderen?

Voor de beantwoording van de zesde deelvraag hebben we in de literatuur gezocht naar *best practices* en randvoorwaarden voor interventies gericht op ouderen. Hierin hebben we tevens lering getrokken uit interventies die zich richten op andere thema's. Uit de resultaten komen een aantal randvoorwaarden naar voren.

De interventie dient te worden afgestemd op de behoeften en voorkeuren van de doelgroep. Er zou geen '*one-size-fits-all*'-principe bestaan om alle ouderen te bereiken, omdat binnen de doelgroep meerdere subgroepen aanwezig zijn. De omgeving waarin de interventie wordt uitgevoerd, lijkt tevens van essentieel belang te zijn. De framing van de interventie is hierbij van belang. In het verlengde hiervan, moet de omgeving waarin de interventie wordt uitgevoerd passen bij de doelgroep.

Ten slotte dient de duur en het aanbod in de interventie voldoende te zijn om daadwerkelijk een duurzame gedragsverandering bij de doelgroep te creëren. Een nazorgtraject kan mogelijk terugvalgedrag voorkomen. Indien een interventie kortdurend is, lijkt het per definitie noodzakelijk om een vervolgaanbod aan te bieden. De initiële interventie en de eventuele nazorg of vervolgsessies dienen qua doorloop goed op elkaar aan te sluiten, zodat er geen groot tijdsbestek zit tussen deze twee onderdelen.

Wat betreft de inhoud van de interventie lijkt het essentieel te zijn dat een interventie uit meerdere onderdelen bestaat, omdat deze afwisseling bevorderlijk kan werken en kan zorgen voor een blijvende deelname. Ook de intensiteit van de interventie en de manier waarop wordt gecommuniceerd tijdens de interventie dient te worden afgestemd op de mogelijkheden van de doelgroep. Bij ouderen kan het verouderingsproces leiden tot een afname van cognitieve vaardigheden. Hierdoor kan het voor deze doelgroep meer tijd kosten om de aangereikte informatie te verwerken en te onthouden. De wijze waarop informatie wordt aangeboden, kan variëren, maar dient altijd te worden afgestemd op de specifieke behoeften en mogelijkheden van de doelgroep.

5.2 Beantwoording hoofdvraag

Op basis van de beantwoording van de verschillende deelvragen formuleren we nu een antwoord op de hoofdvraag: "*Welke indicatoren zijn volgens de theorie essentieel in interventies gericht op het verhogen van de digitale weerbaarheid van ouderen (55+)?"* Met deze indicatoren kunnen we beoordelen in hoeverre bestaande interventies *theory-informed* zijn, i.e., voldoen aan verschillende onderdelen die conform de grijze en wetenschappelijke literatuur van belang lijken te zijn. Hierbij maken we onderscheid tussen de verschillende thema's die bij de beantwoording van de deelvragen naar voren zijn gekomen.

5.2.1 Theorie als gids voor interventies

Om te bepalen in hoeverre bestaande interventies voldoen aan theoretische belangrijke indicatoren, hebben we een checklist opgesteld (zie bijlage I). In deze checklist zijn de resultaten van de deelvragen vertaald naar indicatoren. De checklist bestaat uit vier stappen, gebaseerd op de Intervention Mapping methodiek (Bartholomew Elredge et al., 2016) De laatste twee stappen van de methodiek zijn niet in de checklist opgenomen, omdat deze focussen op het implementeren en evalueren van

de interventie. Dit heeft derhalve geen betrekking op de inhoud van de interventie, maar op de uitvoering ervan, en valt om die reden buiten de reikwijdte van het bepalen van theoretisch onderbouwde indicatoren.

In de checklist wordt onderscheid gemaakt tussen de volgende vier stappen: (1) het in kaart brengen van het probleem/thema; (2) het bepalen van de doelstelling(en); (3) het ontwerpen van het interventieprogramma; en (4) het bepalen van activiteiten in het interventieprogramma. Een interventie heeft meer kans van slagen wanneer zij in alle stappen aansluit bij de gestelde indicatoren.

De eerste stap richt zich op het *in kaart brengen van het thema/probleem.* Dit betreft het startpunt dat is gecreëerd om de interventie vorm te geven. Bij deze indicatoren gaat het onder andere over een gemaakte analyse van het op te lossen probleem en de uitvoering van een behoeftepeiling.

De tweede stap is het *formuleren van doelstellingen*. In deze stap gaat het onder andere om in hoeverre de doelgroep, doelstelling en doelgedragingen zijn bepaald. De checklist bevat een algemene omschrijving van doelgedragingen, die zowel betrekking kunnen hebben op cyberhygiëne als op specifieke delicten. In de toelichting van de checklist hebben we veelgebruikte cyberhygiëne doelgedragingen opgenomen. Mocht een interventie zich op een specifiek delict of specifieke delicten richten, dan kunnen hiervoor een of meerdere doelgedraging(en) worden opgesteld, passend bij het thema van de interventie. Daarnaast wordt gekeken naar het betrekken van relevante partijen en het opgestelde plan van aanpak (inclusief planning).

De derde stap is het *ontwerpen van het interventieprogramma*. In deze stap wordt de theoretische en praktijkgerichte onderbouwing gecheckt. Ook wordt expliciet aandacht gegeven aan in hoeverre de interventie aan de ethische richtlijnen voldoet. We hebben drie theorieën/modellen (PMT, RAA, COM-B) in het huidige onderzoek uiteengezet, waarbij een aantal onderdelen in deze theorieën/modellen

naar voren komen die een positieve gedragsverandering teweeg kunnen brengen.[12] De onderdelen uit PMT hebben we opgenomen in de checklist, omdat deze noodzakelijk zijn. De andere twee zijn aan de toelichting toegevoegd, zodat betrokkenen hier aanvullend rekening mee kunnen houden. Een opmerking die we maken is dat wanneer relatief veel theoretische determinanten relevant lijken, er een selectie gemaakt moeten worden om een interventie praktisch te houden. Dat kan aan de hand van (1) de mate van belangrijkheid (aangetoond causaal verband tussen determinant en het te veranderen gedrag) en (2) de mate van veranderbaarheid (op basis van bewijs dat verandering daadwerkelijk kan worden gerealiseerd).

De vierde stap is het *bepalen van activiteiten in het interventieprogramma*. Uit de literatuur komen een aantal onderdelen naar voren waaraan een succesvolle interventie dient te voldoen. Bij deze onderdelen maken we onderscheid tussen wat relevant is voor interventies in het algemeen en specifiek voor de doelgroep ouderen.

5.3 Discussie

Onderdeel van de checklist (zie bijlage I) is het formuleren van doelgedragingen. Aanvankelijk was het idee om deze vooraf te definiëren, zodat kan worden vastgesteld in hoeverre de interventies daarop gericht zijn. Echter kwam uit een projectoverleg op 9 januari 2025 naar voren dat de wens is om deze niet aanvankelijk te bepalen, maar dat per interventie wordt bekeken op welke doelgedraging de interventie zich richt. Desalniettemin, is het van belang dat deze doelgedragingen concreet te

[12] Hoewel deze drie theoretische inzichten waardevol zijn, is het belangrijk om niet blind te staren op slechts deze drie. Andere theoretische perspectieven die ten grondslag liggen aan een interventie kunnen eveneens waardevolle bijdragen leveren aan het versterken van digitale weerbaarheid onder doelgroepen. Bij de selectie van een interventie wordt derhalve aangemoedigd om aanbieders hierop te bevragen, mochten de door ons genoemde elementen niet zichtbaar terug komen in een betreffende interventie.

formuleren. Om deze reden zijn de doelgedragingen die voortkomen uit de literatuur (par. 4.2) in de checklist opgenomen.

Daarnaast is het mogelijk dat een interventie niet aan alle onderdelen van de checklist voldoet. Bestaande onderdelen uit de checklist, bijvoorbeeld het aanbieden van nazorg, kunnen echter aan een interventie worden toegevoegd. Hierdoor kan een interventie, en de effecten daarvan, potentieel naar een hoger niveau worden getild.

5.4 Beperkingen

Het huidige onderzoek kent enkele beperkingen. De bevindingen uit de literatuur suggereren dat de onderdelen die zijn opgenomen in de checklist een positieve invloed kunnen hebben op de effectiviteit van de interventie. Ondanks deze positieve geluiden is er geen garantie dat een interventie die aan bovenstaande onderdelen voldoet in de praktijk ook daadwerkelijk effectief is. Er zijn diverse, externe aspecten die invloed kunnen hebben op het verloop van de interventie. Voorbeelden zijn maatschappelijke ontwikkelingen of noodzakelijke wijzigingen tijdens de uitvoering van de interventie, zoals de bijdrage die partners kunnen leveren (Bluhm et al., 2024-b). Ondanks deze mogelijke ontwikkelingen, onderschrijven we het belang om aanvankelijk zoveel mogelijk randvoorwaarden en mogelijke risico's in kaart te brengen om de kans op eventuele wijzigingen te minimaliseren.

Een andere beperking is dat we voor het huidige onderzoek geen systematisch literatuuronderzoek hebben uitgevoerd, maar ons hebben beperkt tot de literatuur die bij ons bekend is, aangevuld met publicaties die met de zoektermen naar voren zijn gekomen en input vanuit de partners. Hierdoor is het mogelijk dat we belangrijke ontwikkelingen die spelen bij andere organisaties en experts die niet bij het huidige project zijn aangesloten, hebben gemist en daardoor niet in deze rapportage hebben opgenomen.

Ten slotte is er relatief weinig (Nederlandstalige) literatuur over de digitale weerbaarheid van ouderen, waardoor de huidige kennisbasis enigszins beperkt is. Om die reden hebben we ook literatuur bestudeerd over ouderen binnen andere thematische contexten, waarbij de onderliggende aanpak (i.e., wat werkt voor de doelgroep) vergelijkbaar of relevant zijn voor het versterken van digitale weerbaarheid in bredere zin. We benadrukken het belang van het rapporteren en verspreiden van ontwikkelingen binnen het huidige thema. Dit stelt ons in staat om hier in de toekomst lering uit te trekken, wat bijdraagt aan het versterken van de digitale weerbaarheid van zowel ouderen als de samenleving als geheel.

Literatuurlijst

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I., & Fishbein, M. (1974). Factors influencing intentions and the intention-behavior Relation. *Human Relations*, *27*(1), 1–15. https://doi.org/10.1177/001872677402700101

Al Shaikh, M., Humza, N., Atif, A., & Maynard, S. B. (2019). Toward sustainable behaviour change: An approach for cyber security education training and awareness. In *Proceedings of the 27th European Conference on Information Systems (ECIS)*.

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

Arends, J., Derksen, E., & Morren, M. (2025). *Online veiligheid en criminaliteit 2024*. Via: https://www.cbs.nl/-/media/_pdf/2025/16/online-veiligheid-en-criminaliteit-2024-_-cbs.pdf

Ashenden, D., & Lawrence, D. (2013). Can we sell security like soap? In *Proceedings of the 2013 New Security Paradigms Workshop*, 87–94. https://doi.org/10.1145/2535813.2535823

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* Via: https://arxiv.org/pdf/1901.02672

Bartholomew Elredge, E. L. K., Markham, C. M., Ruiter, R. A. C., Fernández, M. E., Kok, G., & Parcel, G. S. (2016). *Planning health promotion programs: An Intervention Mapping approach* (4th ed.). Jossey-Bass.

Blatter, B., & Bakhuys Roozeboom, M. (2018). Bewust van onbewust gedrag: Handvatten voor gedragsbeïnvloeding. In F. Guldenmund (Ed.), *Gedrag en Veiligheid* (pp. 93–109). Vakmedianet.

Bluhm, K., Andriessen, M., Klopman, J., Klaver, I., Leukfeldt, R., Spithoven, R., & Jansen, J. (2024a). *Van praktijk naar interventie: Procesevaluaties van CCV City Deal projecten - Deelrapport 2: Vervolg Tranche 2*. CyberweerbaarNL.

Bluhm, K., Andriessen, M., Van De Wal, M., Berkenpas, M., De Boer, D., Leukfeldt, R., Spithoven, R., & Jansen, J. (2024b). *Een eerste blik op het verloop en de werking van cyberweerbaarheidsprojecten in Nederland: Procesevaluaties van CCV City Deal projecten - Deelrapport 1: Tranche 1 en 2*. CyberweerbaarNL.

Bluhm, K., Borwell, J., & Stol, W. (2022). De slachtofferimpact van cybercrime versus traditionele criminaliteit: Aanknopingspunten voor slachtofferzorg en preventieprioriteiten. *Tijdschrift Voor Veiligheid*, *21*(3–4), 13–31. https://doi.org/10.5553/TvV/.000045

Booijink, M. (n.d.). *Bouwstenen voor een effectieve sociale interventie*. Via: https://www.movisie.nl/sites/default/files/publication-attachment/Bouwstenen%20ESI%20%5BMOV-12891374-1.0%5D.pdf

Borwell, J., Jansen, J., & Stol, W. (2021). Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions. *Journal of Digital Social Research*, *3*(3), 85–110.

Borwell, J., Jansen, J., & Stol, W. (2022). The psychological and financial impact of cybercrime victimization: A novel application of the Shattered Assumptions Theory. *Social Science Computer Review*, *40*(4), 933–954. https://doi.org/10.1177/0894439320983828

Borwell, J., Jansen, J., & Stol, W. (2025). Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. *International Review of Victimology*, *31*(1), 156–181. https://doi.org/10.1177/02697580241282782

Boulton-Lewis, G. M. (2010). Education and learning for the elderly: Why, how, what. *Educational Gerontology*, *36*(3), 213–228. https://doi.org/10.1080/03601270903182877

Bullée, J.-W., & Junger, M. (2020). Social engineering: Digitale fraude en misleiding. *Justitiële Verkenningen*, *46*(2), 92–110. https://doi.org/10.5553/JV/016758502020046002009

Burns, A. J., Posey, C., Roberts, T. L., & Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190–209. https://doi.org/10.1016/j.chb.2016.11.018

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology*, *159*, 111678. https://doi.org/10.1016/j.exger.2021.111678

Clubb, A. C., & Hinkle, J. C. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Criminal Justice Studies*, *28*(3), 336–355. https://doi.org/10.1080/1478601X.2015.1050590

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). *Using behavioural insights to improve the public's use of cyber security best practices*. Via: http://dx.doi.org/10.13140/RG.2.1.2387.3761

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Daamen, W. (2015). *Wat werkt bij het implementeren van jeugdinterventies?* Via: https://www.nji.nl/uploads/2021-06/Wat-werkt-bij-het-implementeren-van-jeugdinterventies.pdf

De Bruine, H. (2018). Organiseren van Veiligheid. In F. Guldenmund (Ed.), *Gedrag en Veiligheid* (pp. 153–168). Vakmedianet.

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). 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), 1796–1808. https://doi.org/10.1080/0144929X.2021.1905066

Dijkstra, M. (2009). *Mentaal vermogen: Ouderen*. https://www.trimbos.nl/docs/4d1e7362-7953-4049-ba5f-d27dbf014365.pdf

Durlak, J. A., & DuPre, E. P. (2008). Implementation matters: A review of research on the influence of implementation on program outcomes and the factors affecting implementation. *American Journal of Community Psychology*, *41*(3–4), 327–350. https://doi.org/10.1007/s10464-008-9165-0

ENISA (2019). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. Via: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

Esposito, G., Hernández, P., van Bavel, R., & Vila, J. (2017). Nudging to prevent the purchase of incompatible digital products online: An experimental study. *PLOS ONE*, *12*(3), e0173333. https://doi.org/10.1371/journal.pone.0173333

Fishbein, M., & Ajzen, I. (2010). *Predicting and changing behavior*. Psychology Press. https://doi.org/10.4324/9780203838020

Fisher, T. S. (2024). *Gone smishing: An integration of decision-making and protection motivation in the context of identity theft victimization*. University of South Florida.

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

Fokkema, T., & van Tilburg, T. (2006). *Aanpak van eenzaamheid: Helpt het?* Via: https://research.vu.nl/ws/portalfiles/portal/2173082/2006+Fokkema+vT+nidi-report-69.pdf.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004

Glasgow, R. E., Vogt, T. M., & Boles, S. M. (1999). Evaluating the public health impact of health promotion interventions: the RE-AIM framework. *American Journal of Public Health*, *89*(9), 1322–1327.

Griffin, R. J., Dunwoody, S., & Neuwirth, K. (1999). Proposed model of the relationship of risk information seeking and processing to the development of preventive behaviors. *Environmental Research*, *80*(2), S230–S245. https://doi.org/10.1006/enrs.1998.3940

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. *Information Management & Computer Security*, *17*(3), 276–289. https://doi.org/10.1108/09685220910978112

Hassan, S., Ahmad, R., Katuk, N., Ghazali, N. N., Aripin, J. A., & Ali, F. (2024). Staying one step ahead: Exploring Protection Motivation Theory to combat cyber-fraud among e-services users. *Procedia Computer Science*, *234*, 1364–1371. https://doi.org/10.1016/j.procs.2024.04.011

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

Jansen, J. (2025). *Samen sterker in een digitaliserende samenleving: Van en met elkaar leren*. Boom.

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Janssen, A., Engelaer, M., Kloosterman, A., & Richter, B. (2024). *Het groot interventieboek*. Boom Management.

Joinson, A. N., Dixon, M., Coventry, L., & Briggs, P. (2023). Development of a new 'human cyber-resilience scale.' *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyad007

Kahneman, D. (2011). *Thinking, fast and slow.* Penguin Group.

Kievik, M. (2017). *The time of telling tales: The determinants of effective risk communication.* Universiteit Twente. https://doi.org/10.3990/1.9789036544269

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping* (Vol. 464). Springer.

Leukfeldt, R., Notté, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*. Via: https://repository.wodc.nl/bitstream/handle/20.500.12832/2355/2839_Volledige_Tekst_tcm28-368216.pdf?sequence=1&isAllowed=y

Leventhal, H. (1970). Findings and theory in the study of fear communications. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 5, pp. 119–186). Academic Press.

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, *6*(1), 42. https://doi.org/10.1186/1748-5908-6-42

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-A22. https://www.jstor.org/stable/26635045

NCSC (2022). *Nederlandse Cybersecuritystrategie 2022-2028*. Via: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/nlcs-2022/NLCS_2022_19.pdf

NCSC (2025). *Voorbij de e-learning*. Via: https://www.ncsc.nl/documenten/publicaties/2025/januari/28/voorbij-de-elearning

Nederlands Instituut van psychologen (n.d.). *Principes voor ethisch handelen bij gedragsbeïnvloeding*. Via: https://nip.nl/wp-content/uploads/2022/04/Ethische_handvatten_for_grootschalige_gedragsbeinvloeding_NIP-SEP.pdf

Nicholson, J., Morrison, B., Dixon, M., Holt, J., Coventry, L., & McGlasson, J. (2021). Training and embedding cybersecurity guardians in older communities. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–15. https://doi.org/10.1145/3411764.3445078

Nijland, S., Preller, L., Kalkman, I., & Willemsen, N. (2018). *Werkzame elementen van beweeginterventies voor 55-plussers*. Via: https://www.kennisbanksportenbewegen.nl/?file=9086&m=1536042824&action=file.download

Nouri, M., Ghasemi, S., Dabaghi, S., & Sarbakhsh, P. (2024). The effects of an educational intervention based on the protection motivation theory on the protective behaviors of emergency ward nurses against occupational hazards: A quasi-experimental study. *BMC Nursing*, *23*(1), 409. https://doi.org/10.1186/s12912-024-02053-1

Parry, D. A., Davidson, B. I., Sewall, C. J. R., Fisher, J. T., Mieczkowski, H., & Quintana, D. S. (2021). A systematic review and meta-analysis of discrepancies between logged and self-reported digital media use. *Nature Human Behaviour*, *5*(11), 1535–1547. https://doi.org/10.1038/s41562-021-01117-5

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

Preller, L., & de Zeeuw, J. (2018). *Succesvolle inzet van interventies voor 55-plussers*. Via: https://www.seniorsportiefactiefdrv.nl/sites/default/files/Whitepaper%20Succesvolle%20inzet%20van%20interventies%20voor%2055-plussers_0.pdf

RBPO (2024). *Cyber & 55-plussers: 'Thee, tablets en taartjes' - Cyberweerbaarheid 55-plussers in Noord-Nederland*. Werkgroep cyberveiligheid Noord-Nederland.

Redmiles, E. M., Warford, N., Jayanti, A., Koneru, A., Kross, S., Morales, M., Stevens, R., & Mazurek, M. L. (2020). A comprehensive quality evaluation of security and privacy advice on the web. In *Proceedings of the 29th USENIX Security Symposium* , 89–108.

Reeder, R. W., Ion, I., & Consolvo, S. (2017). 152 Simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy*, *15*(5), 55–64. https://doi.org/10.1109/MSP.2017.3681050

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

Rolandi, E., Sala, E., Colombo, M., Vaccaro, R., & Guaita, A. (2022). *Designing an innovative intergenerational educational program to bridge the digital divide: The Cyber School for Grandparents Initiative* (pp. 398–412). Via: https://doi.org/10.1007/978-3-031-05654-3_28

Rosenstock, I. M. (1974). The Health Belief Model and preventive health behavior. *Health Education Monographs*, *2*(4), 354–386. https://doi.org/10.1177/109019817400200405

Rothrock, R. A. (2022). *Digital resilience: Is your company ready for the next cyber attack*. HarperCollins Leadership.

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied*, *80*(1), 1–28.

Ruer, P., Gouin-Vallerand, C., & Vallières, E. F. (2016). Persuasive strategies to improve driving behaviour of elderly drivers by a feedback approach. In A. Meschtscherjakov, B. De Ruyter, V. Fuchsberger, M. Murer, & M. Tscheligi, M. (Eds.), *Persuasive Technology: PERSUASIVE 2016* (pp. 110–121). Springer. https://doi.org/10.1007/978-3-319-31510-2_10

Sharif, M., Urakawa, J., Christin, N., Kubota, A., & Yamada, A. (2018). Predicting impending exposure to malicious content from user behavior. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 1487–1501. https://doi.org/10.1145/3243734.3243779

Sheeran, P. (2002). Intention—behavior relations: A conceptual and empirical review. *European Review of Social Psychology*, *12*(1), 1–36. https://doi.org/10.1080/14792772143000003

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

Spithoven, R., Jansen, J., Verweijen, B., & Ebbers, S. (2024). *Mensgerichte cyberweerbaarheid: Een praktische uitwerking van het 'human-as-solution'-paradigma*. CyberweerbaarNL.

Spithoven, R., Leukfeldt, R., Misana - ter Huurne, E., van 't Hoff - de Goede, S., van Houten, Y., Bekkers, L., Foppen, E., & te Bos, J. (2022). *Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime*. Via: https://www.saxion.nl/binaries/content/assets/onderzoek/areas--living/maatschappelijke-veiligheid/cyberweerbaarheid---eindrapport---werkpakket-5.pdf

Stals, K. (2012). *De cirkel is rond. Onderzoek naar succesvolle implementatie van interventies in de jeugdzorg*. Via: https://dspace.library.uu.nl/bitstream/handle/1874/242465/stals.pdf?sequence=2&isAllowed=y

Stokkel, M., Pouw, R., van 't Hoff - de Goede, S., & van der Wal, M. (2023). *Sectorrapportage 2023: Over security en privacy awareness in onderwijs en onderzoek*. Via: https://www.surf.nl/files/2023-10/awarenessmeting-onderwijs-onderzoek-2023.pdf

Thaler, R., & Sunstein, C. (2022). *Nudge - de ultieme editie* (Vol. 12). Business Contact.

The Board of Regents of the University of Wisconsin. (2021). *Using the retrospective post-then-pre questionnaire design*. Via: https://fyi.extension.wisc.edu/programdevelopment/files/2021/12/RetrospectivePost-then-Pre.pdf

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376–391. https://doi.org/10.1016/j.cose.2017.07.003

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

van der Kleij, R., van 't Hoff-de Goede, S., van de Weijer, S., & Leukfeldt, R. (2020). Ons cybergedrag is veel onveiliger dan we zelf denken. *Justitiële Verkenningen*, *46*(2), 113–128. https://doi.org/10.5553/JV/016758502020046002011

van der Meer, P., & Lenssink, A. (2019). Onderzoek Cybercrime. *KBO-PCOB Magazine*, 25–31.

van Deursen, A. J. A. M. (2019). *Digitale ongelijkheid in Nederland: Internetgebruik van mensen van 55 jaar en ouder*. Via: https://research.utwente.nl/files/250788789/2019_Digitale_Ongelijkheid_55_vanDeursen.pdf

van Scherpenseel, M., Donné, L., van Veenendaal, L., van den Broeke, J., te Velde, S., & Ronteltap, A. (2022). *Hoe thuiswonende ouderen te bereiken met valpreventie-interventies?* Via: https://www.Pharos.nl/Wp-Content/Uploads/2022/05/van-Scherpenseel-et-al-2022-Hoe-Thuiswonende-Ouderen-Te-Bereiken-Met-Valpreventie-Interventies.Pdf.

van Steen, T. (2024). Developing a behavioural cybersecurity strategy: A five-step approach for organisations. *Computer Standards & Interfaces*, *92*, 103939. https://doi.org/10.1016/j.csi.2024.103939

van Steen, T., & de Busser, E. (2021). *Security by behavioural design: A rapid review.* Institute of Security and Global Affairs.

van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa019

Van ’t Hoff - de Goede, S., Van der Kleij, R., Van der Weijer, S., & Leukfeldt, R. (2019). *Hoe veilig gedragen wij ons online?* Via: https://repository.wodc.nl/bitstream/handle/20.500.12832/2433/2975_Volledige_Tekst_tcm28-421151.pdf?sequence=2&isAllowed=y

Vance, A., Siponen, M. & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*, 190–198.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified View. *MIS Quarterly*, *27*(3), 425–478.

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, *77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191–198. https://doi.org/10.1016/j.cose.2004.01.012

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, 25–35. https://doi.org/10.1016/j.dss.2016.09.013

Witte, K. (1991). The role of threat and efficacy in aids prevention. *International Quarterly of Community Health Education*, *12*(3), 225–249. https://doi.org/10.2190/U43P-9QLX-HJ5P-U2J5

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & 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

Zaid, N. N. M., Rauf, M. F. A., Ahmad, N. A., Zainal, A., Razak, F. H. A., & Shahdan, T. S. T. (2022). Learning Elements for Digital Literacy among Elderly: A Scoping Review. *Journal of Algebraic Statistics*, *13*(3), 2850–2859.

Bijlagen

Bijlage I: Interventie Evaluatie Checklist

Op basis van de bevindingen uit de literatuur is onderstaande checklist opgesteld. Deze checklist kan worden gebruikt om nieuwe en bestaande interventies te beoordelen. Middels deze beoordeling wordt bepaald in hoeverre de interventie voldoet aan succesfactoren die uit de literatuur naar voren zijn gekomen. Deze factoren zijn gecategoriseerd in vier onderdelen en gebaseerd op de Intervention Mapping methodiek van Bartholomew et al. (2016), aangevuld met andere bevindingen vanuit de literatuur.[13]

Wanneer een interventie wordt opgezet, is het van belang dat de ontwikkelingen die per stap plaatsvinden, aansluiten op de eerder gemaakte keuzes. Hiermee wordt voorkomen dat de interventie uit losse onderdelen gaat bestaan, terwijl een samenhangend geheel noodzakelijk is.

Stap en thema	Indicator	Aanwezig	Niet aanwezig	Onduidelijk
Stap 1: Probleem/ thema in kaart brengen	Er is een probleemanalyse uitgevoerd			
	Er is een behoeftepeiling uitgevoerd			
	Relevante partijen zijn in kaart gebracht			

[13] In de checklist wordt uitsluitend gefocust op de invulling van de interventie. Er wordt hier dus geen rekening gehouden met de uitvoering.

Stap en thema	Indicator	Aanwezig	Niet aanwezig	Onduidelijk
Stap 2: Bepaling doelstellingen	De doelgroep is concreet beschreven (incl. aantallen) en de keuze daarvoor is onderbouwd			
	De doelstelling is SMART geformuleerd			
	Er zijn concrete doelgedragingen geformuleerd die mensen moeten volgen om hun cyberhygiëne te verbeteren en/of hun digitale weerbaarheid tegen criminaliteit te vergroten			
Stap 3: Ontwerp interventieprogramma				
Theory-informed	De interventie is theoretisch onderbouwd			
	De interventie gaat in op een of meerdere dreigingen			
	De interventie biedt een of meerdere handelings-perspectieven			
	De interventie maakt gebruik van een of meerdere constructen voor gedragsbeïnvloeding			
Practice-informed	Ervaringen uit de praktijk zijn meegenomen in de interventie			
Ethische richtlijnen	In de interventie wordt rekening gehouden met ethiek, en de privacy van deelnemers wordt gewaarborgd.			

Stap en thema	Indicator	Aanwezig	Niet aanwezig	Onduidelijk
Stap 4: Activiteiten interventieprogramma				
Algemeen	De interventie heeft een interactief karakter (spelelementen)			
	Tijdens de interventie is er contact met de deelnemers			
	De interventie richt zich op concrete onderwerpen binnen een overkoepelend thema			
	De invulling van en materiaal voor de interventie zijn afgestemd op de doelgroep			
Ouderen	De interventie (of het projectteam) biedt nazorg-mogelijkheden			
	De interventie wordt uitgevoerd door gekwalifi-ceerde uitvoerders			
	De interventie biedt sociale voordelen			
	De interventie kent een positieve insteek			
	De interventie bestaat uit verschillende onderdelen			
	De intensiteit van de interventie is aangepast op de doelgroep			
	Tijdens de inter-ventie is er ruimte voor reflectie			

Toelichting checklist

Stap 1: Probleem/thema in kaart brengen

De eerste stap van de checklist is het in kaart brengen van het probleem of thema wat in de interventie centraal staat. Dit fungeert als startpunt van de interventie en deze stap bestaat uit drie indicatoren:

- *Er is een probleemanalyse uitgevoerd*: In de probleemanalyse wordt gekeken naar wat er leeft en speelt bij de doelgroep, bijvoorbeeld door trends en ontwikkelingen in kaart te brengen.
- *Er is een behoeftepeiling uitgevoerd*: De behoeftepeiling wordt uitgevoerd bij de doelgroep om te bepalen in hoeverre het noodzakelijk is om een interventie uit te voeren en op welke aspecten de interventie zich dient te richten.
- *Relevante partijen zijn in kaart gebracht*: Er wordt een overzicht opgesteld van alle stakeholders die een rol spelen in het project.

Stap 2: Bepaling doelstellingen

De tweede stap van de checklist is het bepalen van de verschillende doelstellingen. Hierbij wordt onderscheid gemaakt tussen een doelstelling voor de interventie en de te bereiken doelgroep.

- *De doelgroep is concreet beschreven (incl. aantallen) en de keuze is onderbouwd:* De doelgroep die de betrokkenen/uitvoerders met de interventie willen bereiken. Hierbij is het van belang dat de doelgroep zo concreet mogelijk wordt beschreven, inclusief het aantal te bereiken personen. De volgende opzet kan hiervoor als onderlegger worden gebruikt: “[aantal] senioren in [afgekaderd gebied]”. Door meetbare onderdelen te formuleren kan achteraf worden bepaald in hoeverre de doelgroep is bereikt. Wanneer een doelstelling onhaalbaar wordt geformuleerd, zoals het bereiken van álle ouderen in een provincie of regio, ontbreekt een realistisch kader voor evaluatie achteraf.

- *De doelstelling is SMART geformuleerd:* Het uiteindelijke doel wat met (de uitvoering van) de interventie wordt bereikt. Deze doelstelling dient aan te sluiten bij de risico's of de gewenste ontwikkeling die bij het centrale thema horen. Hierbij is het van belang dat de doelstelling SMART (specifiek, meetbaar, acceptabel, realistisch en tijdsgebonden) wordt geformuleerd. Hierin dienen minimaal de volgende onderdelen terug te komen:
    - Concreet eindresultaat, datgeen dat wordt beoogd om met de interventie te bereiken. Hiervoor is een specifiek en meetbaar eindresultaat nodig, omdat hiermee achteraf kan worden bepaald of dit doel ook is bereikt. Abstracte begrippen zoals 'het verhogen van de digitale weerbaarheid' is lastig te meten. Een betere doelstelling kan bijvoorbeeld zijn 'het aanbieden van kennis [bijvoorbeeld over het herkennen en voorkomen van digitale delicten] en vaardigheden [zoals het uitvoeren van preventieve handelingen] aan [beschrijving doelgroep].
    - In het verlengde van bovenstaande dient de doelstelling acceptabel en realistisch te zijn. Acceptabel betekent dat de doelstelling aansluit bij de verwachtingen en mogelijkheden van zowel de doelgroep als de betrokken uitvoerders, en draagvlak geniet bij alle betrokkenen. Realistisch houdt in dat het doel haalbaar is binnen de beschikbare middelen, tijd en context van de interventie.
    - Het laatste onderdeel van de doelstelling is het tijdsgebonden aspect. Dit is de periode waarin de doelstelling wordt bereikt.
- *Er zijn concrete doelgedragingen geformuleerd in relatie tot cyberhygiëne en/of criminaliteit:* Een interventie richt zich op een bepaalde gedragsverandering die teweeg wordt gebracht. Dit gedrag kan worden geconcretiseerd door een bepaalde doelgedraging te formuleren in relatie tot het gedrag of de omgeving. Deze doelgedragingen kunnen ook worden opgenomen

in de evaluatie van de interventie, omdat hiermee kan worden bepaald in hoeverre het gewenste doelgedrag wordt uitgevoerd. In de literatuur zijn veelgebruikte doelgedragingen gevonden. Deze doelgedragingen focussen zich voornamelijk op de cyberhygiëne van individuen. Ter illustratie:

- [Doelgroep] gebruikt sterke en unieke wachtwoorden voor online accounts.
- [Doelgroep] maakt wachtwoorden aan met en slaat deze op in een wachtwoordmanager.
- [Doelgroep] stelt in dat updates automatisch worden geïnstalleerd.
- [Doelgroep] maakt gebruik van antivirussoftware.
- [Doelgroep] doet aangifte bij de politie in geval van slachtofferschap van online criminaliteit.

Als een interventie zich richt op een specifiek delict kunnen daarvoor doelgedraging worden geformuleerd. Het is belangrijk dat deze gedragingen concreet worden beschreven en bij voorkeur positief. Benoem daarbij dus vooral wat men wél moet doen, in plaats van wat men moet nalaten. Ter illustratie:

- Bankhelpdeskfraude: [Doelgroep] hangt telefoon op wanneer iemand (ogenschijnlijk) van de bank belt.
- Vriend-in-nood-fraude: [Doelgroep] neemt contact op via een ander kanaal/medium of in persoon in geval iemand via een onbekend nummer om geld vraagt.

Stap 3: Ontwerp interventieprogramma

De derde stap betreft het ontwerp van het interventieprogramma en betreft de theoretische onderbouwing van de interventie. In de checklist en verdere toelichting komen onderdelen van de Protection Motivation Theory terug. Er zijn echter meer theorieën/modellen beschikbaar die ook

hiervoor gebruikt kunnen worden. Wij hebben de constructen uit twee aanvullende raamwerken opgenomen in deze toelichting, te weten die van de Reasoned Action Approach en het Capability-Opportunity-Motivation-Behaviour model. Betrokkenen bij een interventie kunnen hier aanvullend rekening mee houden. Vraag, indien mogelijk, ook aan de ontwikkelaar of aanbieder welke werkzame factoren bewust in de interventie zijn opgenomen. Let op dat het aantal factoren beperkt blijft (maximaal drie à vijf), zodat de interventie praktisch uitvoerbaar blijft.

- *De interventie is theoretisch onderbouwd:* Een interventie kan gebaseerd worden op een theorie/model, zoals hierboven beschreven. Een methodiek kan tevens als basis worden gebruikt, bijvoorbeeld Design Thinking. Hierbij kan eventueel lering worden getrokken uit eerdere evaluaties van de theorie/methodiek.
- *De interventie gaat in op een of meerdere dreigingen:* Een interventie gaat in op de waarschijnlijkheid van de dreiging, dus van mogelijk slachtofferschap. Daarnaast is de ernst/impact van de dreiging onderdeel van een interventie.
- *De interventie biedt daarbij een of meerdere handelingsperspectieven.* Een interventie gaat in op het vertrouwen van deelnemers in het zelf kunnen uitvoeren van een maatregel (zelfeffectiviteit), de verwachte effectiviteit van een maatregel en de inschatting van de kosten die met een maatregel zijn gemoeid.
- *De interventie maakt gebruik van een of meerdere theoretische constructen voor gedragsbeïnvloeding.*
    - *Gepercipieerde norm*: De waargenomen norm speelt een belangrijke rol in de sociale invloed die deelnemers tijdens een interventie ervaren. Deze norm bestaat uit twee onderdelen: (1) de perceptie van anderen welk gedrag moet worden vertoond; en (2) de perceptie of anderen het doelgedrag uitvoeren. Voor het thema digitale weerbaarheid in een interventie betekent dit

dat kan worden ingezet op wat peers vinden welk digitaal veilig gedrag moet worden vertoond (bijvoorbeeld het gebruiken van sterke wachtwoorden). Daarnaast kan worden ingezet op in hoeverre peers het gedrag ook daadwerkelijk uitvoeren. Naast peers kunnen bijvoorbeeld ook bekende Nederlanders worden ingezet.

- *Houding*: De houding betreft de positieve of negatieve gevoelens van een individu gericht op het gewenste doelgedrag. Door in een interventie in te zetten op een positieve houding kan dit een positieve invloed hebben op het uiteindelijke doelgedrag. In een interventie kan bijvoorbeeld worden ingezet op het gebruik van sterke wachtwoorden, omdat een individu in de veronderstelling is dat dit een effectieve maatregel is om de eigen gegevens te beschermen.
- *Capaciteiten*: Capaciteiten gaat over het psychologische en fysieke vermogen van een persoon om een bepaald doelgedrag uit te voeren, bijvoorbeeld door de benodigde kennis en vaardigheden te bezitten. In een interventie kunnen deze onderdelen worden aangeboden over een specifiek thema, waardoor deelnemers (in de veronderstelling zijn) deze elementen (te) bezitten.
- *Gelegenheid*: Gelegenheid gaat over de externe factoren om de gewenste doelgedraging al dan niet uit te voeren. Deelnemers van een interventie hebben hier geen invloed op. Wel kunnen de omstandigheden zo worden ingericht, dat dit een positieve invloed heeft op het gedrag, bijvoorbeeld het ontwerp van de digitale omgeving, de fysieke omgeving (posters, flyers), het sociale netwerk van deelnemers (zorgverleners) en nazorg.
- *Motivatie*: Motivatie gaat over de cognitieve processen die het doelgedrag activeren en sturen. In een interventie kan hierop worden ingespeeld door in te spelen op de relevantie van het

erkennen van voordelen. Zie ook de punten in de checklist over de ingeschatte dreigingen en geboden handelingsperspectieven.

- *Ervaringen vanuit de praktijk zijn meegenomen in de interventie*: Bevindingen vanuit de praktijk kunnen waardevolle lessen bevatten. Er kan bijvoorbeeld lering worden getrokken uit de ervaringen van professionals en ontwikkelingen die zichtbaar zijn bij de doelgroep door betrokkenen.
- *In de interventie wordt rekening gehouden met ethiek en de privacy van deelnemers wordt gewaarborgd*: Het ontwerp van de interventie voldoet aan de ethische richtlijnen. Hiervoor worden de vijf richtlijnen voor ethisch handelen gevolgd:
    - *Het nemen van verantwoordelijkheid voor gedragsbeïnvloeding*: De betrokkenen dragen zorg voor het voorkomen en beperken van schade bij deelname aan een interventie. Daarbij attenderen zij ook andere collega's hierop.
    - *De gedragsbeïnvloeding vindt op een integere manier plaats*: De betrokkenen handelen op een betrouwbare manier, zijn open over hun kwalificaties en voorkomen hierdoor misleiding.
    - *De gedragsbeïnvloeding vindt op een respectvolle manier plaats*: Hierbij wordt rekening gehouden met de doelgroep en eventuele kwetsbare leden.
    - *De gedragsbeïnvloeding vindt op een deskundige manier plaats*: De betrokkenen hebben oog voor ontwikkelingen in het vakgebied en bewaken hun eigen professionele grenzen.
    - *Het gebruik van data vindt op een rechtmatige en betrouwbare manier plaats*: De betrokkenen houden rekening met de privacywetgeving en zorgen voor valide/betrouwbare data.

Stap 4: Produceren programma

De vierde stap van de checklist is het geproduceerde programma, waarbij het gaat over de inhoud van de interventie. Hierbij maken we onderscheid tussen interventies in het algemeen en interventies gericht op ouderen.

Algemeen:

- *De interventie heeft een interactief karakter (spelelementen)*: De interventie dient een interactief karakter te hebben, waarbij deelnemers een actieve bijdrage leveren gedurende de interventie. Dit kan op verschillende manieren plaatsvinden, bijvoorbeeld middels een gesprek dat tijdens de interventie ontstaat (zie ook volgende indicator) of spelelementen waardoor deelnemers worden uitgedaagd om zelf na te denken over het thema. Door dit interactieve karakter op te nemen in een interventie wordt voorkomen dat een interventie enkel bestaat uit het zenden van relevante informatie, maar dat deelnemers worden aangespoord om actief met de informatie/thematiek aan de slag te gaan.
- *Tijdens de interventie is er contact met deelnemers*: Als een interventie wordt uitgevoerd, dient er contact te zijn met de deelnemers. Hierdoor worden deelnemers meegenomen in de thematiek en geactiveerd om een bijdrage te leveren. Dit kan op verschillende manieren plaatsvinden, bijvoorbeeld door een gesprek te starten met het publiek of in kleine groepen de thematiek te bespreken. Dit geeft deelnemers tevens de kans om hun kennis/ervaringen over de thematiek te delen.
- *De interventie richt zich op concrete onderwerpen binnen een overkoepelend thema*: De interventie richt zich op een specifiek thema, bijvoorbeeld een bepaald delict, waarbij één of twee concrete onderdelen nader worden toegelicht, bijvoorbeeld twee maatregelen ter bescherming tegen dat delict.

- *De invulling is afgestemd op de doelgroep*: Binnen de doelgroep kunnen verschillen zichtbaar zijn in de kennis en vaardigheden op het thema digitale weerbaarheid. De uitvoerders van de interventie kunnen de inhoud van de interventie aanpassen op de doelgroep, zodat dit aansluit bij hun behoeften en kennis en vaardigheden. Hierbij kan gebruik worden gemaakt van herkenbare situaties voor de doelgroep.

Ouderen:

- *De interventie (of het projectteam) biedt nazorgmogelijkheden*: Een nazorgtraject is onderdeel van een interventie, zodat een duurzame gedragsverandering wordt gecreëerd. Dit nazorgtraject kan op verschillende manieren worden vormgegeven, bijvoorbeeld door een vervolg op de initiële interventie op te zetten of deelnemers door te verwijzen naar relevante partners die deelnemers na afloop van de interventie kunnen ondersteunen, bijvoorbeeld door het beantwoorden van vragen.
- *De interventie wordt uitgevoerd door gekwalificeerde uitvoerders*: De uitvoerders van de interventie zijn gekwalificeerd/getraind/ ervaren om een interventie bij de doelgroep uit te voeren. Hierbij is het van belang dat uitvoerders affiniteit hebben met de doelgroep en in staat zijn om het niveau van de interventie aan te passen aan het individu en/of de groep.
- *De interventie biedt sociale voordelen*: In de interventie komen de sociale voordelen van deelname aan de interventie naar voren, bijvoorbeeld contact met andere deelnemers.
- *De interventie kent een positieve insteek*: De framing van (de informatie in) de interventie is positief en benadrukt de voordelen van deelname, i.e., wat deelnemers met de interventie kunnen bereiken. Voorbeelden zijn het veilig kunnen gebruiken van het internet middels het aanreiken van kennis en vaardigheden, waarbij

wordt voorkomen dat de focus ligt op de negatieve aspecten/het bang maken van de deelnemers. Het is dus van belang om in te zetten op de zelfeffectiviteit van de deelnemers, i.e., vertrouwen opwekken dat zij in staat zijn om een bepaald gedrag te kunnen vertonen.

- *De interventie bestaat uit verschillende onderdelen*: De interventie bestaat uit verschillende onderdelen, zodat afwisseling plaatsvindt. Deze afwisseling werkt mogelijk bevorderlijk, omdat een combinatie van elementen zorgt voor een blijvende deelname/oplettendheid.
- *De intensiteit is aangepast op de doelgroep*: Het is belangrijk om rekening te houden met de cognitieve vaardigheden van de doelgroep. Het kan bij ouderen bijvoorbeeld langer duren om aangereikte informatie te verwerken en onthouden. Het tempo gedurende de interventie is medeafhankelijk van de samenstelling – en leeftijd – van de doelgroep.
- *Tijdens de interventie is er ruimte voor een reflectie:* Het (gezamenlijk) reflecteren op de resultaten met de deelnemers zorgt voor inzichten in en motivatie voor de thematiek.