



Digitaal Meedoen: LVB Cyberweerbaar!

Eindrapportage voor subsidieverstrekker
Stichting Achmea Slachtoffer en Samenleving
(SASS) 2025
(Projectnummer 1464)

Datum 31 maart 2025
Titel Digitaal Meedoen: LVB Cyberweerbaar!
Pagina 2 / 94

Colofon

Datum 31 maart 2025

Auteurs Hogeschool Saxion, lectoraat Online Weerbaarheid (Julia Klopman BA., Nick van der Klok MSc., dr. Milou Kievik, dr. Ynze van Houten & dr. Remco Spithoven) en Hogeschool Windesheim, lectoraat Bewegen, Gezondheid en Welzijn (dr. Tina Bellemans)

Met medewerking van Marielle Van der Salm (designer posters), Elsa Foppen (onderzoek), Joyce te Bos (onderzoek), allen van Hogeschool Saxion

Ter nagedachtenis aan Gerard van Egmond.

Inhoudsopgave

Samenvatting	5
1. Inleiding	10
2. Projectdoelstellingen	11
3. Theorie en eerder onderzoek	13
3.1 Online criminaliteit	13
3.2 Weerbaarheid tegen gedigitaliseerde criminaliteit	14
3.3 Licht verstandelijke beperking	16
3.4 Weerbaarheid bij mensen met een LVB	16
3.5 De grootste dreiging van online criminaliteit: <i>social engineering</i>	18
3.6 Interventies gericht op weerbaarheid bij mensen met een LVB	20
4. Onderzoeksmethoden	23
4.1 Onderzoekstas	23
4.2 Vragenlijst	26
4.3 Interviews	27
5. Onderzoeksresultaten	29
5.1 Kwalitatieve analyse: onderzoekstas	29
5.2 Kwalitatieve analyse: interviews	32
5.2 Kwantitatieve analyse: vragenlijst	33
6. Interventie-ontwikkeling	41
6.1 Inventarisatie: shortlist van bestaande interventies	41
6.2 Iteratie ronde 1: ontwerp geldezel interventie	46
6.3 Iteratie ronde 2: verbreding van de interventie naar top vijf vormen van oplichting	47
7. Conclusie/discussie	51
7.1 Projectdoelstellingen	51
7.2 Discussie	54
BIJLAGE 1 - Geraadpleegde literatuur	57
BIJLAGE 2 - Vragenlijst	63
BIJLAGE 3 - Goedkeuring Saxion Ethische Advies Commissie (SEAC)	73
BIJLAGE 4 – Instructie-handleiding begeleiders	74
BIJLAGE 5 – Eerste poster (1^e iteratie ronde)	81
BIJLAGE 6 – Tweede poster (1^e iteratieronde)	82
BIJLAGE 7 – PDF met extra voorlichting informatie voor begeleiders omtrent geldezelen (1^e iteratieronde)	83

Datum 31 maart 2025
Titel Digitaal Meedoen: LVB Cyberweerbaar!
Pagina 4 / 94

BIJLAGE 8 – Poster (2^e iteratieronde)	84
BIJLAGE 9 – Opdrachten onderzoekstas	85
BIJLAGE 10 – Informatiefolder onderzoeksmap	90
BIJLAGE 11 – Toestemmingsformulier onderzoekstas	92

Samenvatting

Inleiding en onderzoeksopzet

Hoewel de digitalisering van de samenleving het dagelijks leven voor veel mensen vereenvoudigt en versnelt, brengt deze ook nieuwe uitdagingen en sterke neveneffecten met zich mee. Zo gaat de digitalisering voor veel mensen te snel waardoor zij moeite hebben met deelname en digitale uitsluiting dreigt (Digitale Overheid, 2018; Mariën et al., 2013). Ook onder mensen met een LVB is een toename te zien in hun digitale participatie (Alfredsson et al., 2019; Chiner, Gómez-Puerta & Cardona-Moltó, 2017), wat het risico op slachtofferschap van cybercriminaliteit met zich meebrengt (Jenaro et al., 2018; Normand & Sallafranque-St-Louis, 2015). Deze ontwikkeling in combinatie met de uitdagingen die mensen met een LVB ervaren rondom de digitalisering, leidt ertoe dat mensen met een LVB vaak door hun omgeving worden beperkt of zelfs helemaal van het internet worden geweerd (Chadwick, 2019; 2022; Chadwick et al., 2022; Chiner, Gómez-Puerta & Cardona-Moltó, 2017; Löfgren-Mårtenson, et al., 2015). Hoewel er een toename zichtbaar is in de omvang en impact van cybercriminaliteit (CBS, 2024) en er voor mensen met een LVB dus digitale uitsluiting dreigt (Chadwick, 2019; 2022; Chadwick et al., 2022; Chiner, Gómez-Puerta & Cardona-Moltó, 2017; Löfgren-Mårtenson, et al., 2015), willen wij met dit project een interventie ontwikkelen voor mensen met een LVB om de cyberweerbaarheid te vergroten.

Het doel van dit project is een bestaande, passende interventie door te ontwikkelen voor zowel de LVB'er als het netwerk rond deze persoon zoals ouders en hulpverleners, zodat de LVB-doelgroep in Nederland op veilige wijze kan deelnemen aan de digitale samenleving. We kiezen daarbij voor doorontwikkeling van een bestaande, passende interventie, omdat er al een rijk aanbod van interventies rond cyberweerbaarheid geboden wordt (Bluhm et al., 2024).

Deze centrale projectdoelstelling is opgedeeld in de volgende subdoelen:

- 1) Het in kaart brengen van het dagelijkse digitale leven van mensen met een LVB en de risico's waarmee zij geconfronteerd worden in de digitale wereld;
- 2) Inzicht krijgen in de factoren die bijdragen aan online weerbaarheid van mensen met een LVB en hierbij passende effectieve interventies voor deze doelgroep;
- 3) Het inzichtelijk maken van potentieel geschikt te maken, bestaande interventies voor mensen met een LVB om de online weerbaarheid te vergroten;
- 4) Het inzichtelijk maken van potentieel geschikt te maken, bestaande interventies voor de schil om de LVB'er heen (ouders/begeleiders), met als doel het signaleren van onveilige online situaties en het adequaat hierop reageren;
- 5) Het ontwikkelen/geschiedt maken en implementeren van een effectieve interventie om de cyberweerbaarheid van mensen met een LVB en de schil hieromheen te verhogen;
- 6) Het evalueren van de effecten van de interventies.

Literatuur en eerder onderzoek

Wanneer er gesproken wordt over **online criminaliteit** gaat het om "het gebruiken van het internet of andere computertechnologie ten behoeve van het faciliteren van criminaliteit of ander norm overschrijdend gedrag" (Spithoven, 2020, p. 48). In dit onderzoek richten wij ons specifiek op *gedigitaliseerde criminaliteit* of *cyber-enabled crime*. Dit betreffen klassieke vormen van criminaliteit, die nu door middel van ICT op een grotere schaal door criminelen worden uitgevoerd. Deze categorie online criminaliteit valt uiteen in verschillende subcategorieën: (I) overtredingen, zoals bijvoorbeeld het forceren van toegang door het raden van wachtwoorden en het downloaden van films en games; (II) bedrog en diefstal, zoals bijvoorbeeld

WhatsAppfraude, aankoopfraude en helpdeskfraude; (III) geweld, zoals online pesten, stalken en laster en (IV) obsceniteit zoals het verspreiden van kinderporno en online kinderlokken.

Wanneer we kijken naar de omvang van het slachtofferschap van online criminaliteit onder de Nederlandse bevolking dan zien we het slachtoffer van online oplichting en fraude met 9,3% verreweg de grootste groep vormen onder slachtoffers van online criminaliteit (Figuur 4) en dit betreft slachtoffers van aankoop-, verkoop- en identiteitsfraude maar ook fraude in het betalingsverkeer en phishing. Naast deze door het CBS gemeten vormen van online oplichting en fraude kan hierbij ook worden gedacht aan datingfraude, afpersmails, (bank)helpdeskfraude, factuur- en vacaturefraude. Online oplichting en fraude kent immers vele verschijningsvormen (FraudeHelpdesk, z.d.).

Onder het slachtofferschap van online oplichting en fraude ligt de algemene aanvalsstrategie van criminelen die in de literatuur *social engineering* of wordt genoemd. Het gaat hierbij concreet om misleiding. Social engineering kan immers beschreven worden als een vorm van gedragsbeïnvloeding waarbij gebruik wordt gemaakt van de psychologische valkuilen in de menselijke natuur (Salahdine & Kaabouch, 2019).

Wanneer er gesproken wordt over een **licht verstandelijke beperking** (LVB), dan zijn er beperkingen wat betreft intelligentie en adaptief gedrag. Dit eerste uit zich in een totale IQ-score tussen de 50 en 70/75. De beperkingen in het adaptief gedrag, ook wel (sociaal) aanpassingsvermogen genoemd, kunnen onderverdeeld worden in (1) conceptuele vaardigheden (zoals taal, tijd-, getal- en geldbegrip), (2) sociale vaardigheden (communicatieve vaardigheden en sociale problemen oplossen) en (3) praktische vaardigheden (zoals persoonlijke verzorging en gebruik van vervoer). Door deze beperkingen in het adaptief functioneren, met name op het gebied van sociale en probleemoplossende vaardigheden, kunnen jongeren met een LVB zich moeilijk staande houden in sociale situaties.

Voor mensen met een LVB zijn fysiologische reacties van het lichaam een bewezen aangrijppingspunt voor bewustwording. Deze reacties, mede gekoppeld aan stress, treden in werking wanneer we ons op één of andere manier bedreigd voelen (Marko & Riecanaky, 2018; Simon et al, 2021). Mensen met een LVB hebben vaker te maken met stressvolle situaties in hun leven; vergeleken met leeftijdsgenoten met een (boven) gemiddeld IQ (Emerson, 2003; Hatton & Emerson, 2004; Schuengel & Jansen, 2006). Ook hebben mensen met een LVB minder bronnen om hiermee om te gaan (o.a. Lunsy & Benson, 2001). Dit maakt het extra belangrijk voor mensen met een LVB om voldoende veerkracht te hebben. Door eerst op het lijf aan te grijpen, kan men tot weloverwogen beslissing komen. Het lijkt dus van belang om fysiologische en emotionele arousalregulatie te stimuleren om verhoging in *arousal* tegen te gaan in stressvolle situaties en als gevolg hiervan ook adequaat gereageerd kan worden (Thayer & Lane, 2009; Weber et al., 2010). Zo kan het onder controle hebben van je ademhaling leiden tot een verminderde stressreacties (o.a. McCraty & Atkinson, 2012) waardoor oplopende emoties (zoals paniek) voorkomen kunnen worden. Naast de rol van het lijfelijke aspect voor het bevorderen van weerbaarheid, speelt een steunend sociaal netwerk een cruciale rol, zoals beschreven door Scheffers en collega's (2020). Begeleiders hebben naast ouders een belangrijke rol in het leven van iemand met een VB. Zo hebben begeleiders vaak veel invloed en zijn zij vaker betrokken in het leven van mensen met een VB vergeleken met leeftijdsgenoten en vrienden (Dew et al., 2006. Starke, 2013).

Uit systematische literatuuronderzoek blijkt dat wanneer interventies voor mensen met een verstandelijke beperking gericht zijn op het verhogen van het bewustzijn van lichamelijke signalen bij stress, dit positieve effecten heeft op het vergroten van zelfvertrouwen, verminderen van angst en vergroten van weerbaarheid. Ook hebben wij verschikende richtlijnen voor effectieve interventies voor deze doelgroep in de literatuur aangetroffen (de Wit, Moonen & Douma, 2011; 2023): eenvoudig taalgebruik; concrete oefenstof; voor-structureren en vereenvoudigen; het netwerk rond de persoon betrekken en een veilige en positieve

leeromgeving bieden. Duidelijk is dat wanneer wij de weerbaarheid van mensen met een lvb tegen gedigitaliseerde criminaliteit - en online fraude en oplichting op basis van social engineering in het bijzonder - er dan moet er in de uiteindelijke interventie een integratie worden gemaakt tussen *kennis* (over gevaren/risico's), *attitude* (*window of tolerance*) en *vaardigheid* (handelingskaders voor zowel deelnemers als begeleiders) nodig om effectieve gedragsverandering bij deze doelgroep te realiseren.

Onderzoeksresultaten

Onderzoekstas

Op basis van de uitwerkingen van de opdrachten in de onderzoekstas onder veertien deelnemers van de Klup met een LVB tussen de 8 en 59 jaar oud, is duidelijk geworden dat de respondenten met een LVB in het online, dagelijks leven daadwerkelijk kwetsbaar zijn voor pogingen van criminelen hen via *social engineering* te misleiden, met name via social media platforms, e-mail, online games en datingapps. Wel was duidelijk dat zij zich redelijk tot goed bewust zijn van het specifieke risico rondom geldezelen, maar dat het handelingsperspectief kan worden vergroot.

Interviews

Uit het interview met de *begeleider-coördinator* van de Klup werd duidelijk dat er op kleine schaal ervaring is met online risico's voor deelnemers met een LVB. Zo gingen eerdere gesprekken tussen begeleiders en deelnemers over onbekende URL-linkjes via Facebook, een deelnemer werd benaderd op een datingsapp door een verdacht figuur en een deelnemer kreeg te maken met een anonieme beller. Daarnaast bleek dat het in het algemeen welkom was als meer vrijwilligers instaat zouden zijn om deelnemers te kalmeren via ademhalingsoefeningen wanneer zij in een hevige, emotionele staat verkeren (boos of verdrietig) om hen terug te brengen naar kalmte. Uit het interview met de *gamification medewerker* van de Klup kwam naar voren dat begeleiders weinig grip ervaren op de thuissituatie en sociale groepen waarin de deelnemers verkeren. Ook is er weinig grip op het sociale mediagebruik. Men spreekt weinig met deelnemers over problemen of vraagstukken in de online levens van deelnemers, wat zij zien van het online leven van deelnemers is dat zij zich graag op hun devices terugtrekken als zij momenten van ontspanning hebben.

Vragenlijsten

Uiteindelijk hebben 60 begeleiders onze vragenlijst over het online leven van zichzelf en deelnemers aan de Klup ingevuld. Voor het eigen digitale leven is men naar eigen inschatting behoorlijk actief en maakt men meerdere keren per dag gebruik van het internet, vooral voor mailen, appen, muziek, nieuws en televisiekijken. De meerderheid van de begeleiders maakt zich gematigd zorgen over de kans op, en mogelijke schade door, online criminaliteit en men schat de zelfeffectiviteit in het beschermen tegen online criminaliteit overwegend positief in. Het slachtofferschap onder de begeleiders bij de Klup is relatief klein: 11,7% geeft aan in aanraking gekomen te zijn met online criminaliteit en 8,3% weet dit niet zeker.

Ten aanzien van de online veiligheid van deelnemers van de Klup bestaat er aanzienlijke onzekerheid onder begeleiders. Dat geldt voor de inschatting van het internetgebruik van de deelnemers van de Klup. De meest ingeschatte activiteiten die deelnemers online uitvoeren zijn social media (53%), Whatsapp (53%), video's bekijken (48%), gamen (47%) en muziek luisteren (35%). Er wordt heel verschillend onder begeleiders gedacht over de kans en gevolgen van slachtofferschap van online criminaliteit onder deelnemers van de Klup: ruim een derde maakt zich er veel zorgen over, terwijl bijna een derde dat nagenoeg niet doet. Rondom slachtofferschap onder de deelnemers van de Klup tast men in het duister:

een grote meerderheid (65%) van de begeleiders geeft aan geen inzicht te hebben in het slachtofferschap van de deelnemers. Ook constateren wij dat er vrijwel *geen* contact is (93,3%) tussen de begeleiders en deelnemers over digitaal veilig gedrag.

Inventarisatie van beschikbare interventies

Op basis van een aantal uitgangspunten is gekeken naar bestaande interventies en beoordeeld in hoeverre deze interventies geschikt zijn om de zelfredzaamheid van mensen met een LVB te vergroten. Interventies zijn beoordeeld op:

- Is de interventie gericht op cyberweerbaarheid?
- Is de interventie gericht op de LVB doelgroep?
- Wordt in de interventie aandacht gegeven aan het vergroten van **kennis, attitude en vaardigheden**?

Interventies die zowel gericht zijn op cyberweerbaarheid als specifiek aansluiten bij de behoeften van de LVB-doelgroep, zijn geselecteerd voor een nadere analyse. Op basis van deze criteria is ervoor gekozen om de interventie *Mediajungle* (gericht op cyberweerbaarheid van het LVB – specifiek op het thema *geldezelen*) te selecteren als basisinterventie. Deze interventie richt zich namelijk op cyberweerbaarheid en de LVB doelgroep, waarbij voornamelijk wordt ingezet op het vergroten van kennis. De interventie zal worden aangevuld met oefeningen die inspelen op attitude en vaardigheden, om de kennis van deelnemers over cybercriminaliteit te vergroten en ze adequate manieren aan te leren om met de gevaren van de online wereld om te gaan.

Interventie-ontwikkeling

Als basis voor de doorontwikkeling van de interventie is *Mediajungle* gebruikt. Deze interventie richt zich specifiek op *geldezelen* en richt zich voornamelijk op het vergroten van de kennis over dit thema onder het LVB. Voor onze specifieke interventie is er voor gekozen om naast kennis ook in te zetten op attitude- en vaardigheidsaspecten. Helaas bleek het na overleg met *Mediajungle* niet mogelijk om deze elementen binnen het spel kosteloos te integreren. Daarom is besloten om de interventie als een aanvullend product te ontwikkelen, dat naast het spel ingezet kan worden.

Voor het vergroten van de kennis over dit thema en het op gang brengen van het gesprek tussen deelnemers en begeleiders is ervoor gekozen om posters te ontwikkelen. Deze posters vergroten enerzijds het risicobewustzijn en bieden anderzijds concrete handvatten voor begeleiders over op welke wijze ze cliënten kunnen helpen bij (een vermoeden van) cybercriminaliteit. Daarnaast zijn voor het aanleren van emotie-regulatie en vaardigheden verschillende instructie-handleidingen ontwikkeld (bijlage 4), waarin deelnemers wordt aangeleerd om 'nee' te zeggen tegen het uitlenen van een pinpas, en twee ademhalingsoefeningen voor het leren rustig worden in spannende situaties.

Na de terugkoppeling van de geldezel interventie bleek de behoefte van de Klup breder te zijn dan het thema geldezelen. Hierdoor is de interventie verbreed naar een top vijf criminaliteitsvormen en is afgeweken van de doorontwikkeling op *Mediajungle* (**2^e iteratie**). De focus van de interventie lag in de 2^e iteratie op (1) het ontwikkelen van voorlichtingsmateriaal rondom de vijf meest gevaarlijke online criminaliteitsvormen voor de LVB-doelgroep (*kennis*; via een poster en kennisfolder) en (2) het bieden van een instructie-handleiding voor begeleiders waarin de deelnemers leren 'nee' zeggen tegen het delen van persoonlijke informatie en waarbij begeleiders ademhalingsoefeningen kunnen toepassen om deelnemers in een hoge arousal te kalmeren (*attitude* en *vaardigheden*).

Conclusies en discussie

In dit onderzoek is gekeken naar de digitale leefwereld van mensen met een LVB. Er is in kaart gebracht op welke wijze zij digitaal actief zijn en welke interventies kunnen bijdragen aan het online weerbaar maken van deze doelgroep. Hierbij is niet alleen gekeken naar de LVB'er zelf, maar is er ook gekeken naar de wijze waarop de schil om deze groep (begeleiders bij de Klup) betrokken kunnen worden bij het vergroten van de digitale vaardigheden en de online weerbaarheid van mensen met een LVB. De focus in dit onderzoek lag daarmee op het vergroten van de *samenredzaamheid*.

Titel Digitaal Meedoen: LVB Cyberweerbaar!

Pagina 9 / 94

Uit het onderzoek kwam naar voren dat begeleiders veel behoefte hebben aan handreikingen om met deelnemers in gesprek te gaan over het thema cybercriminaliteit en dat zij behoefte hebben aan tools om cliënten te helpen bij het trainen van adequate vaardigheden. De doorontwikkelde interventie – waarbij zowel client als begeleider wordt betrokken en die inspeelt op kennis, attitude en vaardigheden – is als (zeer) bruikbaar en zinvol beoordeeld en zal worden geïmplementeerd binnen de Klup.

1. Inleiding

Hoewel de digitalisering van de samenleving het dagelijks leven voor veel mensen vereenvoudigt en versnelt, brengt deze ook nieuwe uitdagingen en sterke neveneffecten met zich mee. Zo gaat de digitalisering voor veel mensen te snel waardoor zij moeite hebben met deelname en digitale uitsluiting dreigt (Digitale Overheid, 2018; Mariën et al., 2013). Verder biedt de digitalisering nieuwe gelegenheid om criminaliteit te plegen (Spithoven, 2020). Inmiddels wordt cybercriminaliteit bestempeld als groot maatschappelijk probleem (Beerhuizen, Sipma & Van der Laan, 2020).

Voor mensen met een licht verstandelijke beperking (LVB) kan de digitalisering extra uitdagend zijn (Nikken, Berns & van Beekhoven, 2018). Het kan voor hen bijvoorbeeld lastiger zijn om de juiste digitale vaardigheden of competenties te ontwikkelen, zodat positieve uitkomsten van de digitalisering worden benut en negatieve effecten zoveel mogelijk worden voorkomen. Als gevolg van hun beperking, hebben mensen met een LVB bijvoorbeeld moeite met het inschatten van risico's en het begrijpen van informatie die zij ontvangen (Amerpoort, *z.d.*). Daarnaast hebben mensen met een LVB meer hulp van ouders of hulpverleners nodig, terwijl hun ouders en hulpverleners vaak ook zelf zoekend zijn in de digitale samenleving en daarmee de benodigde hulp niet kunnen bieden (de Groot, 2021).

Ook onder mensen met een LVB is een toename te zien in hun digitale participatie (Alfredsson et al., 2019; Chiner, Gómez-Puerta & Cardona-Moltó, 2017), wat het risico op slachtofferschap van cybercriminaliteit met zich meebrengt (Jenaro et al., 2018; Normand & Sallafranque-St-Louis, 2015). Deze ontwikkeling in combinatie met de uitdagingen die mensen met een LVB ervaren rondom de digitalisering, leidt ertoe dat mensen met een LVB vaak door hun omgeving worden beperkt of zelfs helemaal van het internet worden geweerd (Chadwick, 2019; 2022; Chadwick et al., 2022; Chiner, Gómez-Puerta & Cardona-Moltó, 2017; Löfgren-Mårtenson, et al., 2015). Hoewel er een toename zichtbaar is in de omvang en impact van cybercriminaliteit (Akkermans et al., 2024) en er voor mensen met een LVB dus digitale uitsluiting dreigt (Chadwick, 2019; 2022; Chadwick et al., 2022; Chiner, Gómez-Puerta & Cardona-Moltó, 2017; Löfgren-Mårtenson, et al., 2015), willen wij met dit project een interventie ontwikkelen voor mensen met een LVB om de cyberweerbaarheid te vergroten.

In de nastreving van een veiligere digitale leefwereld voor mensen met een LVB hebben wij samengewerkt met praktijkpartner de Klup Twente. De Klup Twente is een vrijwilligersorganisatie—actief in Almelo—die activiteiten verzorgt voor kwetsbare doelgroepen (kinderen, senioren en mensen met een LVB+ en autisme). In totaal zijn er 350+ vrijwilligers, 1000+ deelnemers en 50+ activiteiten, reikend van computerles tot bowlen tot dansen en samen koken. Deze activiteiten worden voornamelijk na school uitgevoerd en in de avonden. In het gebouw van de Klup bevindt zich ook een Game- en Sportcentrum genaamd FUN-IE-FIT. Hier kunnen deelnemers met behulp van een gamewand (X-Wall), VR-brillen, diaschermen en de nieuwste spelcomputers (Playstation 5, XBOX Series X) deelnemen aan verschillende games, die naast entertainment ook—via simulaties—inzicht bieden in de belevingswereld van o.a. iemand met dimensie. Aansluitend aan de FUN-IE-FIT bevindt zich een keuken en ontspanningsplaats waar de groepen vaak samenkomen. Gezien het uitgebreide aanbod aan activiteiten en de nauwe verbinding tussen begeleiders en deelnemers is de Klup een ideale plaats om een passende, bestaande interventie door te ontwikkelen en in te zetten om mensen met een LVB weerbaarder te maken in de online wereld.

2. Projectdoelstellingen

Het doel van dit project is een bestaande, passende interventie door te ontwikkelen voor zowel de LVB'er als het netwerk rond deze persoon zoals ouders en hulpverleners, zodat de LVB-doelgroep in Nederland op veilige wijze kan deelnemen aan de digitale samenleving. We kiezen daarbij voor doorontwikkeling van een bestaande, passende interventie, omdat er al een rijk aanbod van interventies rond cyberweerbaarheid geboden wordt (Bluhm et al., 2024).

Deze centrale projectdoelstelling is opgedeeld in de volgende subdoelen:

1. Het in kaart brengen van het dagelijkse digitale leven van mensen met een LVB en de risico's waarmee zij geconfronteerd worden in de digitale wereld;
2. Inzicht krijgen in de factoren die bijdragen aan online weerbaarheid van mensen met een LVB en hierbij passende effectieve interventies voor deze doelgroep;
3. Het inzichtelijk maken van potentieel geschikt te maken, bestaande interventies voor mensen met een LVB om de online weerbaarheid te vergroten;
4. Het inzichtelijk maken van potentieel geschikt te maken, bestaande interventies voor de schil om de LVB'er heen (ouders/begeleiders), met als doel het signaleren van onveilige online situaties en het adequaat hierop reageren;
5. Het ontwikkelen/geschikt maken en implementeren van een effectieve interventie om de cyberweerbaarheid van mensen met een LVB en de schil hieromheen te verhogen;
6. Het evalueren van de effecten van de interventies.

In afstemming met SASS is dit project opgesplitst in werkpakketten, waarin de doelen zijn verdeeld. Zie Tabel 1 voor meer informatie hierover. Gedurende het onderzoek zijn er in totaal 4 voortgangsrapporten gestuurd naar SASS om de progressie van het project te delen.

Tabel 1- Opdeling subdoelen in werkpakketten

Werkpakket	Beschrijving	Tijdslijn
1	Het dagelijkse digitale leven van deelnemers van De Klup met LVB in kaart brengen. De risico's waarmee zij worden geconfronteerd bij deze digitale activiteiten inzichtelijk maken. Kennis, risicobewustzijn, zelfbeschermend gedrag en de verklarende variabelen hiervoor worden bij de doelgroep op passende wijze in kaart gebracht per risico. Dit vormt het fundament voor het geschikt maken van een interventie voor de doelgroep. Dit werkpakket wordt afgerond met een rapportage over de bevindingen.	<i>Februari-juni 2023</i>
2	Uitgangspunten van effectieve interventies voor de doelgroep in kaart brengen op basis van wetenschappelijke theorie en empirisch onderzoek. Dit werkpakket wordt afgerond met een rapportage over de bevindingen en ook wordt er een factsheet gemaakt over de criteria waaraan een geschikte interventie per doelgroep zou moeten voldoen.	<i>Februari-september 2023</i>

3	Bestaande interventies gericht op cyberweerbaarheid in kaart brengen die potentieel voor de specifieke doelgroep geschikt gemaakt zouden kunnen worden. De geschiktheid van deze interventies voor de doelgroep wordt getoetst om te komen tot een shortlist van potentieel geschikte interventies.	<i>Oktober-december 2023</i>
4	De gekozen interventies wordt geschikt gemaakt voor de doelgroep. Dit werkpakket wordt afgerond met de oplevering van ten minste twee aangepaste interventies.	<i>Januari-september 2024</i>
5	De aangepaste interventies worden samen met de deelnemers van De Klup en hun begeleiders geëvalueerd. Vervolgens wordt de aangepaste interventie met evaluatie en daaruit voortkomende aandachtspunten via ons netwerk landelijk beschikbaar gesteld. Dit werkpakket wordt afgerond met een evaluatierapport.	<i>September-december 2024</i>
6	De beschikbaar gekomen interventie(s), de ontwikkelde kennis en het eindrapport van het project worden landelijk beschikbaar gesteld via een afsluitende, landelijke conferentie voor vrijwilligers en professionals die met de doelgroep LVB werken.	<i>Januari-februari 2025*</i>

**Het project heeft een verlenging gehad van één maand: oplevering 31 maart 2025.*

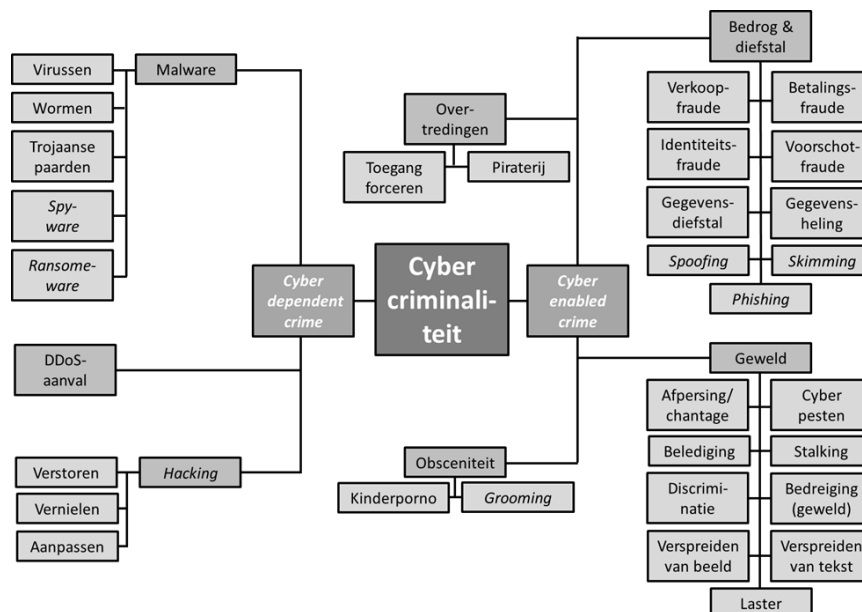
3. Theorie en eerder onderzoek

3.1 Online criminaliteit

Uit cijfers van het Centraal Bureau voor de Statistiek (2023) blijkt dat tegenwoordig bijna iedereen toegang heeft tot het internet. In 2022 had namelijk 97 procent van de Nederlanders ouder dan 12 jaar thuis toegang tot internet. Door 90 procent van de Nederlanders ouder dan 12 jaar werd het internet ook dagelijks gebruikt (CBS, 2023). De komst van het internet heeft onze maatschappij enorm veranderd. Zo sturen we tegenwoordig gemakkelijk berichten naar kennissen of vrienden die aan de andere kant van de wereld zitten, winkelen we online of spreken we de huisarts via beeldbellen. Naast al deze voordelen is het ook van belang om stil te staan bij de neveneffecten die de digitalisering met zich meebrengt.

Berichtgeving over nieuwe risico's als gevolg van de digitalisering laten mensen nog vaak onberoerd, omdat het te abstracte informatie voor hen is (Spithoven, 2020). Dat slachtofferschap van cybercriminaliteit toeneemt, blijkt ook uit onderzoek naar Online Veiligheid en Criminaliteit (CBS, 2023): 15 procent van de Nederlanders (2,2 miljoen mensen) van 15 jaar en ouder werd in 2022 slachtoffer van één of meer vormen van online criminaliteit. Daarnaast zijn “morele en juridische normen in online omgevingen veel onduidelijker dan in offline omgevingen” (Spithoven, 2020, p. 32) waardoor “offline moreel bewuste mensen online binnen *no-time* en op grote schaal overgaan tot immoreel gedrag” (Cocking & Van den Hoven, 2018, in Spithoven, 2020, p. 33). Niet al deze immorele gedragingen zijn strafbaar gesteld en dus is er sprake van een grijs gebied wanneer we het hebben over online dader- en slachtofferschap. Denk hierbij bijvoorbeeld aan cyberpesten (Spithoven & van Tuijl, 2024).

Wanneer er gesproken wordt over online criminaliteit gaat het om “het gebruiken van het internet of andere computertechnologie ten behoeve van het faciliteren van criminaliteit of ander normoverschrijdend gedrag” (Spithoven, 2020, p. 48). Online criminaliteit omvat dus diverse vormen van criminaliteit en normoverschrijdend gedrag (zie hiervoor Figuur 1). In dit het vervolg van dit rapport wordt er ingegaan op *gedigitaliseerde criminaliteit* of *cyber-enabled crime*. Dit betreffen klassieke vormen van criminaliteit, die nu door middel van ICT op een grotere schaal door criminelen worden uitgevoerd. Deze categorie online criminaliteit valt uiteen in verschillende subcategorieën: (I) overtredingen, zoals bijvoorbeeld het forceren van toegang door het raden van wachtwoorden en het downloaden van films en games; (II) bedrog en diefstal, zoals bijvoorbeeld WhatsAppfraude, aankoopfraude en helpdeskfraude; (III) geweld, zoals online pesten, stalken en laster en (IV) obsceniteit zoals het verspreiden van kinderporno en online kinderklokking.

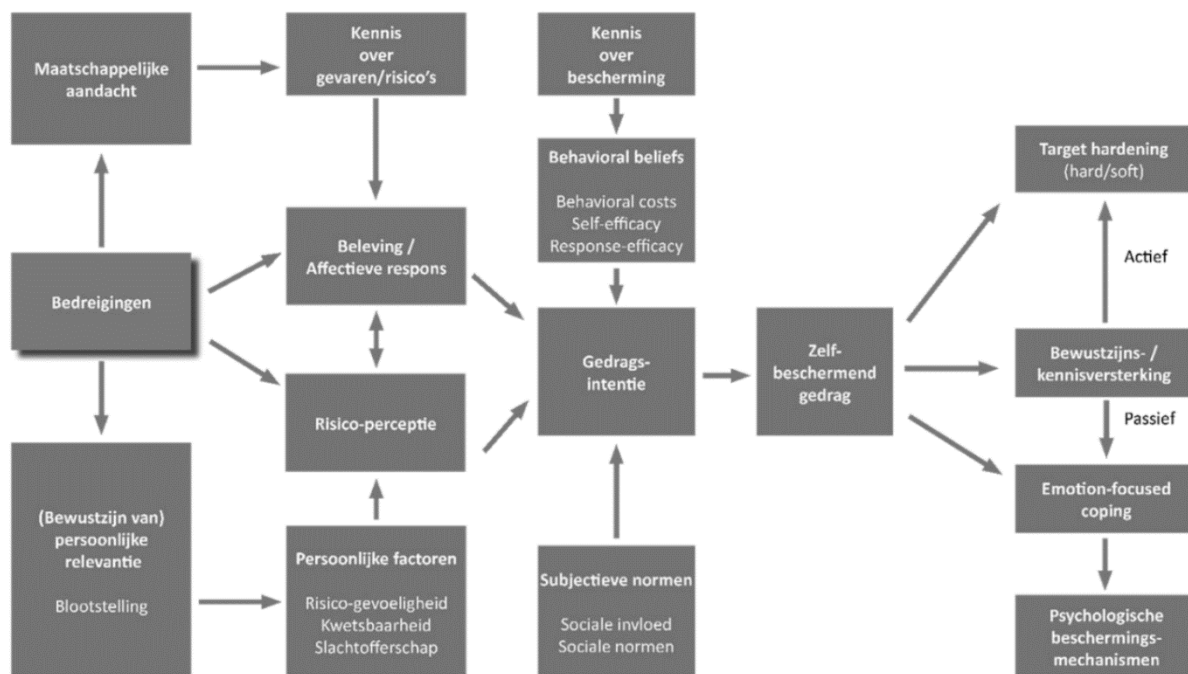


Figuur 1 - Taxonomie Cybercriminaliteit (Spithoven, 2020)

3.2 Weerbaarheid tegen gedigitaliseerde criminaliteit

Een verklaring voor de toename van het aantal slachtoffers van online criminaliteit kan worden gevonden in de kenmerken van slachtoffers. Over het algemeen geloven mensen dat zij zelf niet kwetsbaar zijn voor risico's (van cybercriminaliteit), terwijl zij deze risico's voor anderen overschatten (Misana-ter Huurne, et al., 2020; Weinstein, 1989). Dit verschijnsel, de *optimistic bias* genoemd, weerhoudt mensen ervan om zelfbeschermend gedrag te vertonen. Door de aanwezigheid van de *optimistic bias* en de afwezigheid van voldoende zelfbeschermend gedrag blijven er kansen bestaan voor criminelen op het gebied van cybercriminaliteit.

Om het aantal slachtoffers van cybercriminaliteit terug te dringen is het belangrijk om de cyberweerbaarheid van individuen te vergroten. Het gaat hierbij over de aanwezigheid van risicobewustzijn onder potentiële slachtoffers en het vermogen om zelfbeschermende maatregelen te nemen om het risico op individueel slachtofferschap te verminderen (Spithoven, 2020). Het cyberweerbaarheidsmodel (Spithoven, 2020) is een algemeen, theoretisch model dat inzicht geeft in hoe risicobewustzijn en zelfbeschermend gedrag tot stand komt (zie Figuur 2).



Figuur 2 – Cyberweerbaarheidsmodel (Spithoven, 2020)

Het ontstaan van zelfbeschermend gedrag

De intentie tot het uitvoeren van zelfbeschermend gedrag komt volgens dit model tot stand door 1) de verwachtingen met betrekking tot je eigen gedrag, 2) de risicobeleving, 3) de risico-perceptie en 4) de sociale normen. Ten eerste hebben deze verwachtingen—met betrekking tot het eigen gedrag—een direct effect op de intentie om zelfbeschermend gedrag uit te voeren. Deze verwachtingen omvatten *behavioral costs*, *zelfeffectiviteit* (de overtuiging dat men in staat is om zelfbeschermend gedrag te vertonen) en *responseeffectiviteit* (de overtuiging dat het zelfbeschermende gedrag effectief is om de kans op slachtofferschap te beperken).

Risicobewustzijn en risicoperceptie

Verder wordt er op basis van het risicobewustzijn—dat voortkomt uit factoren zoals kennis en eerdere ervaringen—een bepaald niveau van risicoperceptie ontwikkeld. Het gaat hierbij om het individuele oordeel over risico's. Dit oordeel wordt gevormd op basis van inschattingen van de kans dat een persoon wordt blootgesteld aan risico's en de ernst van de gevolgen. Deze inschatting heeft gevolgen voor de gevoelsmatige beleving van risico's.

Subjectieve normen

Ten slotte hebben subjectieve normen invloed op de mate van zelfbeschermend gedrag. Het gaat hierbij om de sociale aanmoediging van gedrag door de geldende normen op bijvoorbeeld de omgang met cyberrisico's. De risicoperceptie en de risicobeleving worden op hun beurt beïnvloed door de kennis van risico's gebaseerd op de maatschappelijke aandacht voor de risico's en de persoonlijke relevantie van het risico. Deze worden gefilterd door persoonlijke factoren zoals risicogevoeligheid en eerder slachtofferschap.

Het cyberweerbaarheidsmodel geeft dus inzicht in de factoren die risicobewustzijn en zelfbeschermend gedrag kunnen beïnvloeden. Wij nemen daarom dit model als basis voor ons project; waarbij handvatten

worden ontwikkeld om dit model toe te passen op de doelgroep mensen met een licht verstandelijke beperking (LVB).

3.3 Licht verstandelijke beperking

Een verstandelijke beperking (VB) wordt in de DSM 5 omschreven als een ontwikkelingsstoornis welke zichtbaar wordt tijdens de ontwikkelingsperiode. Er zijn beperkingen waar te nemen op cognitief functioneren en op het vlak van adaptieve vaardigheden (Schalock & Luckasson, 2021).

Wanneer er gesproken wordt over een licht verstandelijke beperking (LVB), dan zijn er beperkingen wat betreft intelligentie en adaptief gedrag. Dit eerste uit zich in een totale IQ-score tussen de 50 en 70/75. De beperkingen in het adaptief gedrag, ook wel (sociaal) aanpassingsvermogen genoemd, kunnen onderverdeeld worden in (1) conceptuele vaardigheden (zoals taal, tijd-, getal- en geldebegrip), (2) sociale vaardigheden (communicatieve vaardigheden en sociale problemen oplossen) en (3) praktische vaardigheden (zoals persoonlijke verzorging en gebruik van vervoer). Door deze beperkingen in het adaptief functioneren, met name op het gebied van sociale en probleemoplossende vaardigheden, kunnen jongeren met een LVB zich moeilijk staande houden in sociale situaties. Vanuit het Social Information Processing (SIP)-model van Crick en Dodge (1994) gedacht, is gepast sociaal omgaan in een online setting voor deze doelgroep nog ingewikkelder. Vergeleken met jongeren met een (boven)gemiddeld IQ, begrijpen jongeren met een LVB anderen vaak verkeerd. Jongeren met een LVB schatten emoties (van zichzelf en anderen) en de reacties van anderen vaak niet goed in. Zij interpreteren vaak zaken foutief en hun waarnemingen kunnen vertekend zijn. Verder overschatten zij zich vaak, zeker in een context die minder grijpbaar voor hen is en reageren zij vaker impulsief in plaats van doordacht (van Nieuwenhuijzen et al., 2004; Van Rest et al., 2018).

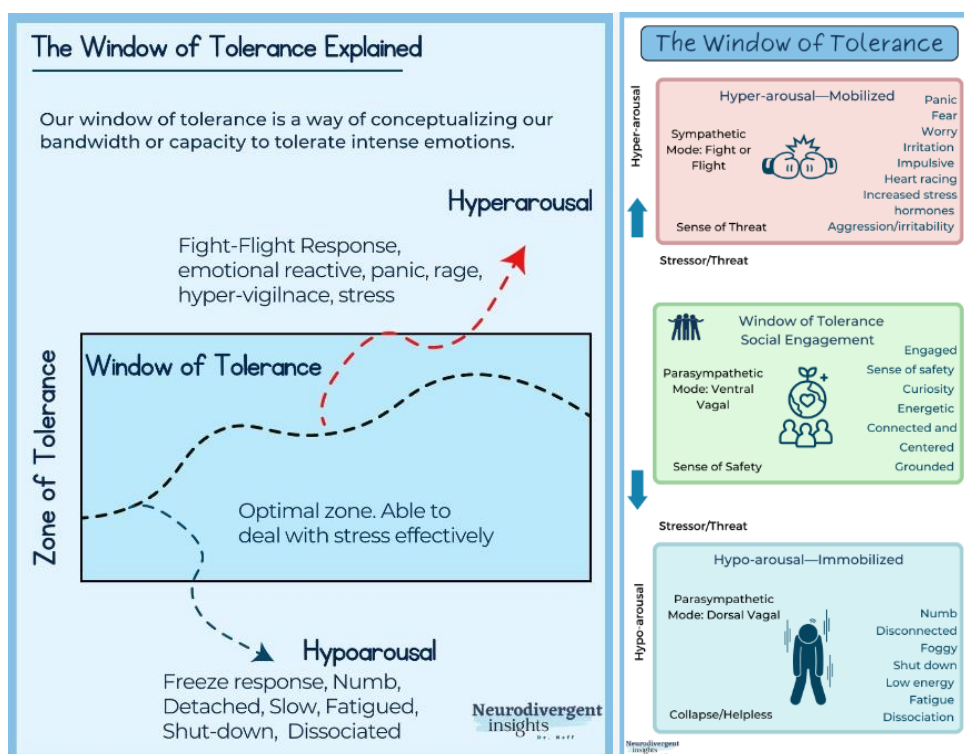
3.4 Weerbaarheid bij mensen met een LVB

Weerbaarheid betreft het adequaat reageren in uitdagende situaties. Deze uitdagende situaties roepen vaak emoties op die bepalend zijn hoe er gereageerd wordt op de situatie. Emoties hebben lichamelijke, cognitieve en gedragsmatige aspecten. Wanneer het gaat om veiligheid worden de primaire overlevingsmechanismen in ons lichaam aangewend via het *fight-flight-freeze* systeem. De *fight* en *flight* mechanismen gaan gepaard met een toename van *arousal*. Het *freeze* mechanisme gaat gepaard met het verlagen van het *arousal* niveau. Deze fysiologische reacties, mede gekoppeld aan stress, treden in werking wanneer we ons op één of andere manier bedreigd voelen. Van oudsher waren dit fysieke levensbedreigende situaties, maar dit stressfenomeen treedt dus bij elke situatie op. We weten dat stress een impact heeft op het maken van beslissingen en dat het vaak leidt tot een verhoogde tendentie om impulsief te reageren (Marko & Riecanaky, 2018; Simon et al, 2021).

Weerbaarheid is nodig om je op een veilige en gezonde manier te begeven in de maatschappij, zowel fysiek als online. Zoals hierboven weergegeven kan dit een uitdaging zijn voor mensen met een LVB, zeker in stressvolle situaties. Bij stressvolle incidenten of stressvolle situaties is bekend dat de hartslag stijgt door de activatie van het autonome zenuwstelsel (o.a. Kim et al., 2018). Wanneer deze stijging hoog is, in tegenstelling tot mild, is men minder goed in staat om mentaal en fysiek te functioneren tijdens stress (Kim et al., 2018). Daarnaast hebben mensen met een LVB vaker te maken met stressvolle situaties in hun leven; vergeleken met leeftijdsgenoten met een (boven) gemiddeld IQ (Emerson, 2003; Hatton & Emerson, 2004; Schuengel & Jansen, 2006). Ook hebben mensen met een LVB minder bronnen om hiermee om te gaan (o.a. Lunsky & Benson, 2001). Dit maakt het extra belangrijk voor mensen met een LVB om voldoende veerkracht te hebben.

Bij het vergroten van de weerbaarheid van mensen met een LVB lijkt een lichamelijke aanvliegroute van meerwaarde omdat er op deze manier minder ingezet wordt op de cognitieve vaardigheden. Zeker voor deze

doelgroep, waar de cognitieve en reflectieve vermogens beperkt zijn. Door de lijfelijke aanpak wordt de fysiologische stressreactie direct beïnvloed (en dus daarmee ook het direct het impulsief handelen), zonder dat er echt begrepen hoeft te worden hoe het werkt (o.a. Bellemans et al., 2022; Currie et al., 2019). Het belang van een optimaal stressniveau is het uitgangspunt bij de Window of Tolerance (WoT) (Siegel, 1999; Ogden & Minton, 2000; zie Figuur 3). Zo kan het stressniveau beïnvloed worden door het verhogen van *arousal* wanneer er sprake is van *hypo-arousal* of net het verlagen wanneer er sprake is van *hyper-arousal*. Wanneer men zich binnen de WoT bevindt, is men in staat om adequate probleemoplossende vaardigheden in te zetten en ook vergroot het de cognitieve responsen.



Figuur 3 – Window of Tolerance

Door eerst op het lijf aan te grijpen, kan men tot weloverwogen beslissing komen. Het lijkt dus van belang om fysiologische en emotionele arousalregulatie te stimuleren om verhoging in *arousal* tegen te gaan in stressvolle situaties en als gevolg hiervan ook adequaat gereageerd kan worden (Thayer & Lane, 2009; Weber et al., 2010). Zo kan het onder controle hebben van je ademhaling leiden tot een verminderde stressreacties (o.a. McCraty & Atkinson, 2012) waardoor oplopende emoties (zoals paniek) voorkomen kunnen worden. Met een stressniveau binnen de WoT is men beter in staat “het geleerde” toe te passen en zal men dus minder impulsief handelen (o.a. Jamieson et al, 2010).

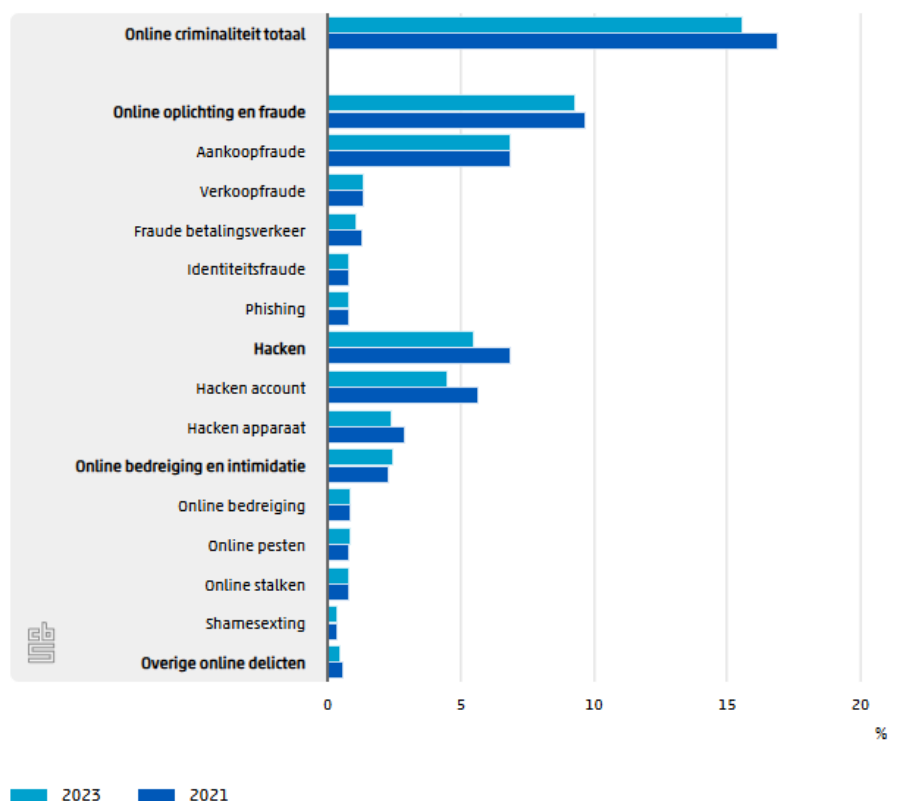
Naast de rol van het lijfelijke aspect voor het bevorderen van weerbaarheid, speelt een steunend sociaal netwerk een cruciale rol, zoals beschreven door Scheffers en collega's (2020). Begeleiders hebben naast ouders een belangrijke rol in het leven van iemand met een verstandelijke beperking (VB). Zo hebben begeleiders vaak veel invloed en zijn zij vaker betrokken in het leven van mensen met een VB vergeleken met leeftijdsgenoten en vrienden (Dew et al., 2006; Starke, 2013). Voor begeleiders is het dus van belang dat zij de jongvolwassenen ondersteunen bij het autonoom functioneren en het ontwikkelen van competenties. Op deze manier kunnen zij helpen bij het ervaren van een zinvol leven en ook draagt dit bij aan het vergroten

van interne motivatie bij het (gezamenlijk) maken van keuzes (Van den Broeck et al., 2016; Elwyn et al., 2012; Elwyn et al., 2010). In de ondersteuning vanuit het netwerk zijn mensen met LVB (en bijkomende problemen) gebaat bij een veilig en ondersteunend leefklimaat, continuïteit in de woonomgeving en behandeling, een duidelijke en voorspelbare begeleidingsstijl, voorspelbaarheid in daginvulling, herkenbare leefregels en de verbondenheid met begeleiders (Embregts et al., 2019; Knotter, 2019; Moonen, 2017). Vandaar dat er in dit project naast het lijfelijke aspect ook aandacht is voor het betrekken van het netwerk van de persoon met een LVB.

3.5 De grootste dreiging van online criminaliteit: *social engineering*

Wanneer we kijken naar de omvang van het slachtofferschap van online criminaliteit onder de Nederlandse bevolking dan zien we het slachtoffer van online oplichting en fraude met 9,3% verreweg de grootste groep vormen onder slachtoffers van online criminaliteit (Figuur 4) en dit betreft slachtoffers van aankoop-, verkoop- en identiteitsfraude maar ook fraude in het betalingsverkeer en phishing. Naast deze door het CBS gemeten vormen van online oplichting en fraude kan hierbij ook worden gedacht aan datingfraude, afpersmails, (bank)helpdeskfraude, factuur- en vacaturefraude. Online oplichting en fraude kent immers vele verschijningsvormen (FraudeHelpdesk, z.d.).

5.1.1 Slachtoffers online criminaliteit



Figuur 4 – Slachtoffers online criminaliteit in 2021 en 2023 (Akkermans et al., 2024)

Onder het slachtofferschap van online oplichting en fraude ligt de algemene aanvalsstrategie van criminelen die in de literatuur *social engineering* of wordt genoemd. Het gaat hierbij concreet om misleiding. Social engineering kan immers beschreven worden als een vorm van gedragsbeïnvloeding waarbij gebruik

wordt gemaakt van de psychologische valkuilen in de menselijke natuur (Salahdine & Kaabouch, 2019). Er wordt—op basis van Cialdini's principes—ingespeeld op zes factoren (zie Tabel 2; Ferreira et al., 2015).

Social engineering is daarmee het misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid. Bij online oplichting en fraude wordt door criminelen veel gebruik gemaakt van social engineering. Volgens Steinmetz et al. (2020) gaat dit fenomeen over het 'sociaal manipuleren' van mensen via frauduleuze handelingen. Hierbij wordt een verhaal gebruikt als psychologisch wapen. Naast psychologische trucs wordt bij social engineering ook gebruikgemaakt van de overvloed aan dagelijkse online sociale en commerciële interactie, waarbij een geloofwaardig verhaal gemakkelijk wordt geloofd en vertrouwd. Volgens Steinmetz et al. (2020) probeert een crimineel middels social engineering vertrouwen van het slachtoffer te wekken, wordt er zoveel mogelijk gebruikgemaakt van interne en openbaar beschikbare kennis, worden berichten professioneel opgemaakt, correct gespeld en worden bekende merken gebruikt met vrijwel identieke details. Zo wordt er door criminelen misbruik gemaakt van de emoties, percepties en gebreken van ontvangers. Met name het oproepen van een sterke, emotionele reactie bij de ontvanger - door vertrouwen, angst, urgentie, opwinding, empathie, hebzucht en nieuwsgierigheid te activeren - vertroebelt het kritisch denken en handelen van de slachtoffers (Steinmetz et al., 2020).

De toenemende digitalisering van de samenleving vraagt veel van zowel het cognitieve als het aanpassingsvermogen van mensen met een LVB. De beperkte cognitieve en adaptieve vaardigheden van mensen met een LVB maken hen extra kwetsbaar, ook in de digitale wereld (Nikken, Berns & van Beekhoven, 2018; Jenaro et al., 2018; Normand & Sallafranque-St-Louis, 2015). Zij kunnen sneller in problematische situaties terecht komen dan anderen. Bijvoorbeeld omdat zij de bedoeling van anderen niet altijd juist kunnen inschatten. Zij zijn vaak beïnvloedbaar, vatbaarder voor verslaving en gevoeliger voor afwijzing of manipulatie. Zij lopen daardoor een groter risico om slachtoffer én dader te worden van cybercrime (Wiltshut, 2020; Pijpers, 2017). Mensen met een LVB zijn daardoor bijzonder vatbaarder om slachtoffer te worden van social engineering.

Er zijn vijf vormen van online criminaliteit waarin criminelen het social engineering mechanisme geïntegreerd hebben—waarbij voornamelijk kwetsbare doelgroepen een hogere kans op slachtofferschap lopen, namelijk (FraudeHelpdesk, z.d.):

- Geldezelen – *oplichting door iemand zijn bankpas te laat gebruiken (bewust of onbewust) voor criminele doeleinden;*
- Sextortion – *oplichting door het gebruik van intieme foto's;*
- Online oplichting – *oplichting door het niet betalen van verkochte producten;*
- Datingfraude – *het aangaan van een online romantisch contact met een man of vrouw, vrijwel altijd in het buitenland, die zich presenteert als iemand anders en vraagt om (grote) financiële steun;*
- Identiteitsfraude – *Van identiteitsfraude is sprake wanneer iemand zich bedient van andermans identiteit of een gecreëerde, fictieve identiteit om daarmee geld en/of goederen te verwerven.*

In de kern zijn deze vijf vormen van gedigitaliseerde criminaliteit gericht op het onthullen van persoonlijke informatie van het slachtoffer door de crimineel, om er vervolgens voor eigen gewin misbruik van te maken. Bijvoorbeeld, bij geldezelen draait het om geld witwassen via de bankrekening van de geldezel. Bij sextortion draait het om beeldmateriaal vast te krijgen en vervolgens via afdwinging geld te ontvangen.

Omdat mensen met een LVB zowel cognitieve als sociale uitdagingen kunnen hebben (Nikken, Berns & van Beekhoven, 2018), zijn zij extra gevoelig voor slachtofferschap van social engineering. Hierdoor is het extra belangrijk dat interventies gericht op gedragsverandering bij deze doelgroep zich niet alleen op kennis, maar ook op attitude en vaardigheden richt. Het is een combinatie van risicobewustzijn, het reguleren van

emoties en het bereik tot concrete handvatten om zelfbeschermend gedrag uit te voeren in samenwerking met het netwerk, dat uiteindelijk zal leiden tot een hogere online weerbaarheid tegen deze vijf online criminaliteitsvormen.

	C	G	S
1	Authority	Authority	Social compliance
2	Social proof	Diffusion responsibility	Herd
3	Linking & Similarity	Deceptive relationship	Deception
4	Commitment & Consistency	Integrity & Consistency	Dishonesty
5	Scarcity	Overloading	Time
6	Reciprocation	Reciprocation	Need & Greed
7	-	Strong Affect	Distraction

Tabel 2 – Cialdini’s principes van psychologische gedragsbeïnvloeding (Ferreira et al., 2015)

3.6 Interventies gericht op weerbaarheid bij mensen met een LVB

Wanneer er op systematische wijze gekeken wordt naar de literatuur (met name Controlled Clinical Trials en Randomised Clinical Trials) over lichaamsgerichte en bewegingsgerichte interventies om weerbaarheid en bewustzijn te vergroten, worden positieve resultaten gezien bij mensen met een verstandelijke beperking (de Rijt, 2023). De geïncludeerde studies bij deze literatuur review zijn weergegeven in Tabel 3.

Tabel 3 - Geïncludeerde studies bij literatuur review

Jaar	Titel	Auteurs	Type onderzoek (effect)
2018	Effects of a Mindfulness-Based Intervention on the Perception of Basic Psychological Need Satisfaction among Special Education Students	Malboeuf-Hurtubise, Catherine; Joussemet, Mireille; Taylor, Geneviève; Lacourse, Eric;	Pre-post: negatief significant
2022	"Mindfulness Matters": A pilot study of a Mindfulness-Based Stress Reduction group for adults with intellectual disabilities	Lake, Sam; MacHale, Rosemary;	Pre-post: geen sign verschil (positieve trend)
2022	Effects of recreational therapy on emotional adjustment of students with intellectual disabilities	ErtÜZÜN, Ezgi; DaŞKiran, Hasan;	Pre-post: geen sign verschil (positieve trend)
2022	Effect of Indoor Climbing on Occupational Self-Efficacy and Employability: Results of a 10-Month Randomised Controlled Study of Persons with Intellectual Disability	Vreuls, Mockenhap; Tillman; Anneken	RCT: sign positief effect

2022	The effect of the adapted soccer programme on motor learning and psychosocial behaviour in adolescents with Down syndrome	Perić, D. B.; Milićević-Marinković, B.; Djurović, D.	Pre-post: positief significant
2015	Relaxation therapy and anxiety, self-esteem, and emotional regulation among adults with intellectual disabilities: A randomized controlled trial	Cyrille Bouvet, Aure ´ lie Coulet	RCT: sign positief effect
2018	Efficacy of Adapted Breathing Exercise on Self-Confidence among Children with Intellectual Disability	Ranjan, Akash;	RCT: sign positief effect

Uit dit systematische literatuuronderzoek blijkt dat wanneer interventies gericht zijn op het verhogen van het bewustzijn van lichamelijke signalen bij stress, dit positieve effecten heeft op het vergroten van zelfvertrouwen, verminderen van angst en vergroten van weerbaarheid bij mensen met een LVB. Bij deze interventies worden ook direct handvatten geboden voor arousalregulatie tijdens het ervaren van een stressreactie. Wanneer het bewegen centraal staat (zonder expliciete aandacht voor de lichaamservaringen) zoals een voetbalinterventie of meer *recreational therapy*, (bij pre-post metingen) zijn er positieve verschillen, echter niet altijd significant. Bij meditatie-interventies zijn er wisselende inzichten: kleine significante verslechtering, of geen significant verschil. Bij deze laatste twee groepen moet ook vermeld worden dat het gaat om quasi-experimentele designs.

Het inzicht vanuit de literatuur pleit voor een ervaringsgerichte, lijfelijke insteek bij de doelgroep LVB. Er wordt verondersteld dat wanneer deelnemers in de ervaring staan, zij meer regie hebben over hun lijf en daarmee ook meer regie hebben over de emoties en dus ook over hun eigen gedrag. Een dergelijke lijfelijke insteek blijkt dus erg waardevol voor mensen met een LVB (Bellemans, 2022; Ter Harmsel, 2022). Verder is bekend, ook voor de normale populatie, dat stress en negatieve emoties kunnen leiden tot impulsiviteit (Herman et al., 2018; Simon et al., 2021). Dus stressverlaging zou op die manier kunnen bijdragen aan het minder impulsief handelen, ook wanneer het cyberactiviteiten betreft.

Ook zijn wij in de literatuur de volgende richtlijnen tegengekomen voor effectieve interventies voor mensen met een LVB. Hieronder zijn de belangrijkste aspecten aangegeven die van belang zijn om interventies te laten aansluiten bij deze doelgroep (de Wit, Moonen & Douma, 2011; 2023):

- I. **Taalgebruik aanpassen:** eenvoudig taalgebruik, controleer of je elkaar begrijpt, visuele ondersteuning; (Doordat de interventie ervaringsgericht is en taal ter ondersteuning wordt gebruikt sluit dit goed aan bij de doelgroep mensen met een LVB. Van belang blijft uiteraard dat taal concreet/ simpel is en aansluit bij de beleving van de deelnemer).
- II. **Concrete oefenstof:** concrete voorbeelden uit hun leven, zichtbaar maken van oefenstof, ervaren staat centraal; (Door hun in een context van bewegen en lijfelijke ervaringen te zetten wordt het lijfelijke aspect van stress maar ook het lichaam als instrument om weer spanning te laten zakken voelbaar voor hen. Zij kunnen ook onmiddellijk ervaren en oefenen in het hier en nu).
- III. **Voorstructureren en vereenvoudigen:** meer externe sturing, meer structuur, vereenvoudigen, doseren en ordenen van de informatie en de oefenstof, herhalen en meer tijd voorzien. (Het helder structureren, het veel herhalen met kleine variaties waarbij kleine stapjes aan bod komen in de ervaring helpt de deelnemer om sneller tot leren te komen).
- IV. **Netwerk en generaliseren:** informeren en betrekken van het netwerk bij de interventie, vergroot het netwerk, aandacht voor generalisering; (De link tussen therapeut en leefomgeving van de deelnemer

is cruciaal, hierbij worden de lijfelijke aspecten centraal gezet waarbij ook aangegrepen kan worden op het dagelijkse leven van de deelnemer zelf en de begeleiding hierin handvatten kan krijgen).

- V. **Veilige en positieve leeromgeving:** motiveren van de deelnemer, zelfvertrouwen vergroten, veilige en positieve leeromgeving (Door het non-verbale/doe-karakter zijn deelnemers vaker gemotiveerd en ervaren zij meer de regie omdat zij door de ervaringen meer lijfelijk ervaren en hier regie over ervaren. Dit maakt dat hun zelfvertrouwen ook groeit. Door de veilige "beweeg"-context staan succeservaringen ook centraal).

Samengevat, als er wordt gekeken naar het grote geheel rond effectieve interventie creatie voor mensen met een LVB, dan is een integratie tussen **kennis** (over gevaren/risico's), **attitude** (*window of tolerance*) en **vaardigheid** (handelingskaders voor zowel deelnemers als begeleiders) nodig om effectieve gedragsverandering bij deze doelgroep te realiseren. Als al deze drie factoren niet meegenomen worden in een interventie voor deze doelgroep, dan is zelfbeschermend gedrag (voor de deelnemer, begeleider en combinatie van die twee) niet mogelijk, en bemoeilijkt dit ook de toepassing op het dagelijks leven. Naast de inhoud —kennis, attitude en vaardigheid— is het belangrijk om de interventie te langs de bovenstaande richtlijnen (eenvoudig, concreet, gestructureerd en geïntegreerd in het netwerk) in te richten.

4. Onderzoeksmethoden

In dit onderdeel beschrijven wij de verschillende onderzoeksmethoden die wij hebben ingezet om de doelstellingen van de werkpakketten en het totale project te realiseren.

Tabel 4 – Onderzoeksmethode per werkpakket (operationalisatie)

Werkpakket	Onderzoeksmethode
1	Onderzoekstas
2	Literatuuronderzoek
3	Interventie-inventarisatielijst
4	Synthese inventarisatie en data (onderzoekstas + vragenlijst)
5	Feedbackgesprekken en evaluatie-vragenlijst
6	Thema-avond op de Klup Wetenschappelijke conferenties: <ul style="list-style-type: none"> • Nederlandse Vereniging voor Criminologie, juni 2024 in Leiden (gepresenteerd) • European Society of Criminology Conference sept 2024 in Boekarest (gepresenteerd) • CWNL/CCV event: Krachten bundelen voor cyberweerbaarheid, sept 2024 (gepresenteerd) • Nederlandse Vereniging voor Criminologie, juni 2025 in Leiden (aankomend)

4.1 Onderzoekstas



Figuur 5 – Ontwikkeling onderzoekstas



Figuur 6 – Inhoud onderzoekstas

Achtergrond

De onderzoekstas hebben wij als methode ontwikkeld om ervaringen, kennis en vaardigheden op het gebied van digitale veiligheid te verzamelen. Deze methode is gebaseerd op het eerder uitgevoerde onderzoek van

Valerie de Groot (2022), waarin zij de onderzoeksbox ontwierp als instrument om technologie-ervaringen op te halen bij mensen met een LVB en niet-aangeboren hersenletsel (NAH).

De onderzoeksbox werd ontwikkeld met als doel een laagdrempelige, toegankelijke en interactieve manier te bieden om inzichten te verkrijgen in hoe mensen met een LVB en NAH technologie ervaren en gebruiken (De Groot, et al., 2022). Hierbij stond een hands-on benadering centraal, waarin deelnemers door middel van tastbare materialen en opdrachten hun ervaringen en perspectieven konden delen. Deze methodologie biedt mogelijkheid om participatief onderzoek te doen, waarbij de doelgroep actief betrokken wordt en hun eigen tempo en manier van communiceren centraal staan.

De onderzoeksbox, zoals beschreven in *durf te experimenteren* (Suijkerbuijk, Hofman & Engels, 2016), is een methode die gebruikmaakt van 'probe kits' pakketten met voorwerpen en opdrachten die deelnemers inspireren om hun waarden, gevoelens en gedachten te verwoorden. Typische items in zo'n kit zijn onder andere een wegwerpcamera, een notitieboekje, kaartjes met prikkelende vragen, een bewaardoosje en een voicerecorder. Deelnemers kunnen zelf kiezen welke voorwerpen ze gebruiken om hun verhaal te vertellen, wat hen de vrijheid geeft om op een voor hen passende manier te communiceren. Deze methode is bijzonder geschikt voor exploratief onderzoek bij mensen die moeite hebben om hun vragen of behoeften te verwoorden, doordat het een creatieve en persoonlijke benadering biedt die aansluit bij de individuele voorkeuren en mogelijkheden van de deelnemers.

Geïnspireerd door deze methodes en aanpak hebben wij de onderzoekstas ontwikkeld, waarin verschillende opdrachten en materialen zijn opgenomen die aansluiten bij het thema van ons onderzoek. De onderzoekstas biedt een praktische en veilige omgeving waarin deelnemers spelenderwijs ons als onderzoekers kunnen meenemen in hun digitale dag. Door middel van gestructureerde, maar flexibele opdrachten krijgen deelnemers de kans om hun online-ervaringen delen, zonder dat dit vraagt om abstracte of schriftelijke verwoordingen, wat vaak een uitdaging is of kan zijn voor mensen met een LVB.

Het gebruik van een fysieke onderzoeksmethode, zoals de onderzoekstas, vergroot de toegankelijkheid en stimuleert actieve participatie, in lijn met de principes van de onderzoeksbox. Bovendien maakt de tastbare aard van de onderzoekstas het mogelijk om niet alleen verbale, maar ook non-verbale en ervaringsgerichte inzichten te verkrijgen.

Operationalisering

Deelnemers kregen de vrijheid om de onderzoekstas op een manier in te vullen die het beste bij hen paste. Ze mochten zelf kiezen of ze de opdrachten wilden maken, en hoe ze hun antwoorden wilden weergeven. Dit kon door te schrijven, tekenen, stickers te plakken, een begeleider hun antwoorden te laten opschrijven of hun reacties in te spreken via een videorecorder. Om deelnemers voldoende tijd en ruimte te geven om op hun eigen tempo te werken, kregen ze twee tot drie weken de tijd om de onderzoekstas in te vullen. De respondenten waren niet verplicht om de opdracht te maken en mochten op elk moment afzien van deelname aan ons onderzoek. De deelnemers werden wel aangemoedigd om elke opdracht minimaal één keer en bij voorkeur twee keer te maken. Indien gewenst, mochten ze een opdracht ook vaker dan twee keer maken.

Elke deelnemer ontving een linnen tas met daarin de onderzoeksmap met de verschillende opdrachten, uitleg over de opdrachten en het onderzoek en een toestemmingsformulier voor deelname aan het onderzoek. Verder zaten er in de onderzoekstas ook de benodigde spullen om de opdrachten te maken zoals stickers, kleurpotloden, pennen en textielstiften om de buitenkant van de tas naar eigen wens te versieren. In elke onderzoekstas zat ook een extra schriftje voor eventuele aanvullende notities. De begeleiders kregen ook een eigenmap met daarin aanvullende informatie en de spraakrecorder voor de deelnemers.

Inhoud onderzoekstas: opdrachten

De onderzoeksmap in de onderzoekstas bevatte vijf verschillende opdrachten (zie Bijlage 9 en 10) die gericht waren op het in kaart brengen van de digitale ervaringen, dag en uitdagingen van de deelnemers.

Opdracht 1, beschrijf je dag

De deelnemers werden gevraagd om op te schrijven, op te nemen, te stickeren of te tekenen welke activiteiten zij die dag hadden uitgevoerd waarbij ze het internet hadden gebruikt. Dit gaf inzicht in hoe en waarvoor zij het internet gebruikte en online actief waren.

Opdracht 2, wat ging er goed?

Vervolgens kregen de deelnemers de vraag om hetzelfde papier als opdracht één voor zich te pakken. Dit papier noemde wij het papier met het zonnetje. De deelnemers konden met een groene of rode duim sticker aangeven wat goed en minder goed ging die dag online. Dit bood een laagdrempelige manier om positieve en negatieve internetervaringen aan te duiden en voor ons in kaart te brengen.

Opdracht 3, mentale belasting door internetgebruik

Deze opdracht richtte zich op de impact van online activiteiten op de mentale belasting van de deelnemers. Ze konden aangeven of ze problemen hadden ervaren bij hun internetgebruik die dag door het probleem in de tekstballon op te schrijven. Vervolgens konden ze met een schuifmechanisme (een rood papier) aangeven hoe vol hun hoofd zat door deze uitdagingen, vervelende situaties of problemen. Dit is dus een visuele opdracht waarbij de respondenten met behulp van een rood papier konden aangeven hoe vol hun hoofd zat door een probleem op het internet.

Opdracht 4, Whatsapp hulpvraag

In deze opdracht stond een casus centraal waarin Charlie via WhatsApp aan Sem vroeg om zijn bankpas te lenen. Deelnemers werd gevraagd welke tip ze Sem zouden geven als hij zijn pas zou uitlenen of had uitgeleend, maar geen beloning had ontvangen. Met deze opdracht wilden wij onderzoeken hoe deelnemers reageren op hulpvragen zoals deze. Inzichtelijk krijgen of en in hoeverre deelnemers zich hiervan bewust waren en of ze deze overweging in hun reactie zouden meenemen is het voornaamste doel van deze opdracht. Daarnaast kan deze opdracht al bijdragen aan de bewustwording rondom online fraude en oplichting, vooral als deze samen met een begeleider werd doorgenomen en ingevuld.

Opdracht 5, versieren van de onderzoekstas

De laatste opdracht betrof het versieren van de linnen onderzoekstas met textielstiften. Deelnemers mochten hun tas decoreren met alles wat zij associeerden met internet. Dit gaf niet alleen inzicht in hun perceptie van het internet, maar bood ook een creatieve afsluiting en van de onderzoeksactiviteiten en een eigen invulling over het onderwerp.

Respondenten

Voor het werven van deelnemers van de Klup met een LVB die de onderzoekstas wilden ontvangen en bijbehorende opdrachten wilden uitvoeren, is door de onderzoekers nauw samengewerkt met de begeleiders van de Klup. Dankzij hun hulp zijn veertien respondenten geïdentificeerd en benaderd voor deelname. De groep respondenten bestond uit veertien personen, variërend in leeftijd van 8 tot 59 jaar. Onder de respondenten waren zes vrouwen en acht mannen. De data is verzameld op verschillende momenten en binnen verschillende groepen, namelijk een volwassengroep, een kinder- en tienergroep en een ouderengroep. Voor de gehele groep geldt dat zij zowel op de Klup als thuis toegang hebben tot een of meerdere device(s) om zich in het digitale verkeer te begeven waarmee zij ook in contact kunnen komen met criminelen.

Het betrekken van begeleiders bij het proces bracht zowel uitdagingen als voordelen met zich mee. Sommige begeleiders namen een actieve rol op zich, terwijl anderen minder betrokken waren dan verwacht. In enkele gevallen werd de afspraak over het aantal uitgezette onderzoekstassen niet nagekomen of bleek het proces intensiever dan vooraf werd ingeschat door de begeleiders. Daarnaast kostte het sommige begeleiders meer energie om collega's aan te sporen om deel te nemen aan het onderzoek. Een-op-een begeleiding bleek lastig te realiseren.

Ondanks deze uitdagingen waren er ook positieve ervaringen. Voornamelijk de jongeren van de Klup vulden de opdrachten uitgebreider in dan verwacht, en de spraakrecorder als methode werd goed ontvangen. Sommige deelnemers, gebruikten de spraakrecorder bijvoorbeeld om hun antwoorden op de WhatsApp-opdracht te geven. Ook werd de onderzoekstas met succes binnen een vrijdagavondgroep geïntroduceerd, waarbij een begeleider in slechts twee avonden zelfstandig vijf tassen uitzette. Deze begeleider was erg enthousiast en dat heeft geleid tot een positief effect als wij kijken naar de invulling van de onderzoekstassen. Dit benadrukt dat de mate van betrokkenheid van begeleiders een belangrijke rol speelde in de uitvoering van het onderzoek.

Daarnaast bleek er soms incongruentie te zijn tussen hoe deelnemers hun kennis verwoordden en hoe zij dit creatief uitten. Bijvoorbeeld, terwijl sommige respondenten op de onderzoekstas tekenden wat ze met het internet associeerden, was er een verschil met de antwoorden die zij gaven in schriftelijke opdrachten uit de onderzoeksmat over hun kennis. Dit biedt interessante inzichten in de manier waarop mensen met een LVB hun begrip van het internet verbeelden versus verwoorden.

Exclusiecriteria. Voor respondenten onder de twaalf jaar oud is aangegeven dat één van de opdrachten genaamd 'Whatsapp hulpvraag' te vervallen komt. De voornaamste reden hiervoor is dat het niet aansluit bij hun levensfase. Deze kinderen hebben vaak geen eigen telefoon waar ze dit soort gesprekken kunnen voeren.

Tijdsduur. De deelnemers van de Klup die als respondent optreden kregen na ontvangst van de onderzoekstassen gemiddeld drie tot vier weken de tijd om de onderzoekstassen en bijbehorende opdrachten in te vullen.

Prevalentie. Enkel deelnemers van de Klup die tot de LVB doelgroep behoren konden participeren in dit onderzoek en de onderzoekstassen invullen.

4.2 Vragenlijst

De vragenlijst is geconstrueerd om de cyberweerbaarheid van de begeleiders bij de Klup te testen, en daarnaast hun perspectief op de cyberweerbaarheid van de deelnemers. Hiervoor zijn een aantal constructen – onder andere vanuit het cyberweerbaarheidsmodel (Spithoven, 2020) – toegepast:

- i. **Internet gebruik** – frequentie waarop iemand dagelijks het internet gebruikt;
- ii. **Activiteiten op het internet** – handelingen die worden uitgevoerd op het internet;
- iii. **Risicoperceptie** – de mate waarin iemand het risico op slachtofferschap inschat;
- iv. **Affectieve response** – zorgen over de kans en schade van slachtofferschap;
- v. **Prevalentie** – frequentie van de daadwerkelijke aanraking met een vorm van online criminaliteit;
- vi. **Slachtofferschap** – schade opgelopen als gevolg van aanraking met online criminaliteit;
- vii. **Zelfbeschermend gedrag** – wijze waarop iemand zichzelf beschermt tegen online criminaliteit;
- viii. **Zelfeffectiviteit** – mate waarin iemand denkt in staat te zijn om zichzelf te beschermen;
- ix. **Contact over online veilig gedrag** – woordvoering deelnemer-begeleider over online veilig gedrag;
- x. **Preventie van online criminaliteit** – inschatting effectieve tools voor preventie slachtofferschap.

Deze constructen zijn door middel van verschillende *items* gemeten via de vragenlijst (zie Bijlage 2). Via een pilot studie (n = 8) met vaste medewerkers van de Klup is deze vragenlijst getest. De lengte werd als goed beschouwd, enkel de vraag kwam terug: “Wanneer ben ik, of een deelnemer van de Klup, slachtoffer?”. Er bleek onduidelijkheid te bestaan wanneer iemand zich aan deze classificatie kon toekennen. Hierdoor is deze vraag aangescherpt; er is een lijst aan opties meegegeven van vormen van slachtofferschap die de begeleider kon aankruisen. Om de vragenlijst nog toegankelijker te maken, zijn een aantal *open-vragen* (die veel cognitieve lading kosten voor een participant) omgezet naar *multiplechoice-vragen*.

Na goedkeuring van de Saxion Ethische Advies Commissie (SEAC; zie bijlage 3) is de vragenlijst uitgezet door een coördinator bij de Klup via de online nieuwsbrief (zie Figuur 7) naar 350 begeleiders/vrijwilligers. Na twee weken is er een reminder gestuurd. In totaal kwam er een response van 90 participanten (response ratio = 25,71%).

Figuur 7 – Email met vragenlijst naar de vrijwilligers van de Klup

Beste vrijwilliger,

U heeft een belangrijke rol in de begeleiding van deelnemers van De Klup. Als onderzoekers van Hogeschool Saxion en Windesheim zijn wij door De Klup gevraagd om inzichtelijk te krijgen waar u mee in aanraking komt tijdens uw werkzaamheden bij De Klup. Het gaat hierbij specifiek om zaken met betrekking tot online veiligheid. Het doel van dit onderzoek is de deelnemers van De Klup helpen in het weerbaarder worden tegen de gevaren van online criminaliteit.

U kunt ons helpen door de bijgevoegde vragenlijst in te vullen.
Dit duurt ongeveer 10 tot 15 minuten om in te vullen en is volledig anoniem.
De vragenlijst kunt u via de onderstaande link zowel op de smartphone, tablet als PC starten.

https://saxion.eu.qualtrics.com/jfe/form/SV_1ZCJ1mpwJWJxno

Alvast ontzettend bedankt voor uw medewerking aan dit onderzoek!

Met vriendelijke groet,
[namen onderzoekers]

4.3 Interviews

Om naar aanleiding van de onderzoekstassen en vragenlijst een verdiepende blik te krijgen van wat er speelt op de Klup zijn er twee interviews uitgevoerd met een begeleider coördinator en ICT/gamification medewerker. Dit was een semi-gestructureerd interview met een aantal vooropgestelde vragen afgestemd op de rol van de geïnterviewde.

De interviewvragen voor de **ICT/gamification medewerker** waren:

1/ In hoeverre gebruiken de deelnemers van de Klup Netflix of YouTube of andere platformen om filmpjes te kijken? Wat zie jij voorbijkomen?

1a/ Zo ja, zoeken zij deze filmpjes dan zelf op?

2/ Wordt er wel eens over de schouders van de deelnemers meegekeken naar digitale activiteiten?

2a/ Zo ja, op welke wijze wordt er meegekeken en op welke wijze wordt het gesprek aangegaan?

3/ Maken de deelnemers zelfstandig gebruik van platformen zoals whatsapp, Youtube, Tinder, Instagram, X (voormalig Twitter), Facebook?

3a/ Zo ja, waar maken de deelnemers dan zoal gebruik van?

4/ Hoe zouden de deelnemers reageren op deze hulpvraag?

Titel Digitaal Meedoen: LVB Cyberweerbaar!
Pagina 28 / 94

5/ Welke actie zouden de deelnemers eventueel ondernemen om een vriend te hulp te schieten als deze blijft doorvragen/smeken en op het gevoel probeert in te praten?

6/ Hoe ziet de digitale dag van een deelnemer eruit?

7/ Met welke digitale verhalen komen deelnemers van de Klup wel eens naar jou toe?

8/ Met welke digitale problemen komen de deelnemers van de Klup in aanraking?

9/ Hoe ervaren mensen met een LVB hun sociale interacties online?

10/ Zijn er bepaalde momenten of situaties waar ze zich bijzonder kwetsbaar voelen, en wat zou hen kunnen helpen om zich dan beter te voelen?

11/ Formuleren de deelnemers dan ook concrete hulpvragen voor jou?

De interviewvragen voor de **begeleider-coördinator** waren:

1/ Welke activiteiten voer jij hier uit op de Klup? (tijdens de avondsessies)

1a/ Hoe ziet de samenstelling van de groepen eruit? (leeftijd, LVB+/autisme?)

2/ Hoe ziet de digitale dag van een deelnemer eruit?

2a/ Kijken de deelnemers van de Klup Twente filmpjes op Netflix of via YouTube? Zoeken zij de filmpjes zelf op?

2b/ Wordt er wel eens over de schouders van de deelnemers meegekeken naar de digitale activiteiten? Op welke wijze wordt er een gesprek aangegaan?

2c/ Maken de deelnemers zelfstandig gebruik van Whatsapp, YouTube, Tinder, Instagram, X (voormalig Twitter) en Facebook? Waar maken zij vooral gebruik van?

3/ Met welke digitale verhalen komen deelnemers van de Klup wel eens naar jou toe?

3a/Waarom denk je dat zij bij jou komen met deze verhalen?

3b/ Met welke digitale problemen komen de deelnemers van de Klup in aanraking?

3c/ Hoe ervaren mensen met een LVB hun sociale interacties online?

3d/ Zijn er bepaalde momenten waar zij zich bijzonder kwetsbaar voelen, en wat zou hen kunnen helpen om zich dan beter te voelen?

4/ Er zijn een aantal specifieke kwesties/risico's die op de loer liggen (sextortion, bankfraude, geldezelen, datingfraude) zie jij dat terug in de Klup? Heb je een vermoeden dat dit bij de cliënten kan spelen?

4a/ Wat zie je dan concreet? Welke vormen zien jij en jouw collega's terug? Zie 2a.

4b/ In hoeverre denk je dat zij de problemen die zij overdag meemaken met jou bespreken? Benoemen zij de problemen die zij overdag hebben meegemaakt?

4c/ Stel een deelnemer heeft iets meegemaakt, zou die dat melden? Zo ja, wat zou jij doen?

4d/ Zie jij de rol van begeleiders als geschikt om begeleiders weerbaarder te maken tegen deze online kwesties?

4e/ Betreft kwestie geldezels: als je een inschatting moest maken, welke actie zouden de deelnemers eventueel ondernemen zodra een 'vriend' blijft doorvragen/smeken om hun pinpas en op het gevoel probeert in te praten.

5. Onderzoeksresultaten

5.1 Kwalitatieve analyse: onderzoekstas

De onderzoekstas

Uiteindelijk hebben 14 respondenten de tas ingevuld. Er is echter variatie in de mate waarop de tas is ingevuld:

- 9 respondenten hebben alle opdrachten twee keer uitgevoerd.
- 1 respondent heeft de opdrachten meer dan twee keer uitgevoerd
- 4 respondenten hebben de opdrachten één keer uitgevoerd
- 5 respondenten hebben de tas niet versiert, 9 deden dat wel
- 3 respondenten hebben gebruik gemaakt van de spraakrecorder, de rest met stickers, tekeningen en schrift (via begeleiders).

Gezien de wisselingen in dataverzameling moeten deze inzichten zorgvuldig worden beoordeeld, en enkel qua inventarisatie worden beschouwd. Hieronder worden de resultaten beschreven die voortkomen uit de opdrachten van de onderzoekstassen.

Opdracht 1 - beschrijf je dag

Uit de ingevulde onderzoekstassen, die zijn verstrekt aan deelnemers van de Klup met een licht verstandelijke beperking (LVB), blijkt hoe hun digitale dag eruitziet. Eén van de opdrachten vroeg de respondenten te beschrijven welke apparaten zij gedurende de dag gebruikten en waarvoor. Uit de resultaten komt naar voren dat de respondenten gebruik maken van diverse apparaten, zoals een Tablet (N=4), telefoon (N=6), televisie (N=7), PlayStation (N=1), laptop (N=3) en een laptop op school (N=1). Deze apparaten worden voor verschillende doeleinden ingezet, variërend van entertainment en communicatie tot educatieve activiteiten en dagelijkse praktische taken.

Niet alle respondenten hebben per activiteit aangegeven op welk apparaat zij dat hebben. Uit de resultaten komt naar voren dat de respondenten zich bezig houden met filmpjes kijken op YouTube (N=8), programma's of films kijken op de televisie (N=7) of de telefoon (N=1), Whatsapp berichten sturen (N=1), video bellen (N=1), bellen (N=1) en bellen met de huisarts (N=1) sportuitslagen bekijken (N=1), gamen (N=7), streamen (N=1) website de dag vandaag bezocht (N=1), muziek luisteren (N=4), op de playroom van school zitten (N=1), informatie opzoeken (op google) (N=3), het weer bekijken (N=3), mailen (N=5), agenda bijhouden (N=1) het nieuws lezen (N=2), geldzaken regelen (N=1), online winkelen (N=1) memes bekijken (N=1), foto's bekijken (N=1) en één van de respondenten geeft aan liturgieën te maken voor de kerkelijke gemeente (N=1).

De programma's en films die de respondenten bekeken waren divers. De respondenten keken naar kerstfilms (N=1), de sinterklaas intocht (N=1), de grote rode hond (N=1), het jachtseizoen (N=1), het jeugdjournaal (N=1), het nieuws (N=2), de film stargate (N=1), diamonds painting filmpjes (N=1) en één van de respondenten geeft aan een 'mooi' programma te hebben gezien (N=1). Niet alle respondenten specificeren wat zij hebben gekeken en omschrijven alleen dat zij bijvoorbeeld televisie of YouTube hebben gekeken. De respondenten speelden ook verschillende game zoals Roblox (N=1) Minecraft (N=1) een game waar je leert omgaan met geld (N=1), Poki (N=1), Starfleet Command (N=1), Startrek (N=1). Niet alle respondenten specificeren wat voor een games zij spelen. Eén van de respondenten geeft ter aanvulling aan dat hij aan het denken is (dagdromen) over de game Roblox overdag.

Opdracht 2 – wat ging er goed?

De tweede opdracht uit de onderzoekstas vroeg de respondenten te omschrijven wat er goed en niet goed ging tijdens hun digitale dag. De ingevulde antwoorden op de vraag wat er goed ging geven een duidelijk

beeld van hun positieve ervaringen: zij konden goed omgaan met hun iPad en andere *devices*, ouders hielpen bij het voor structureren van YouTube op de telefoon door kanalen op te slaan en abonnementen te beheren. Grotere letters hielpen hen beter de tekst te kunnen lezen en zoeken. WhatsAppen met vrienden en leeftijdsgenoten werd als leuk en gezellig ervaren. Ook het opzoeken van informatie en het kijken naar de intocht ging goed. Andere positieve ervaringen waren het kijken van tv, het duidelijk en succesvol versturen van e-mails, het goed functioneren van de telefoon en het verkrijgen van duidelijke antwoorden, evenals het gamen en spelen van spelletjes. De respondenten meldden dat activiteiten goed gingen door een groene sticker met een duimpje om hoog te plakken of op te schrijven 'ging goed' bij de activiteit.

Daarnaast is de respondenten gevraagd te omschrijven wat er niet goed ging tijdens hun digitale dag. Negen van de veertien respondenten meldden geen problemen of dingen die niet goed gingen tijdens hun onlineactiviteiten. De overige respondenten (N=5) gaven aan dat zij hulp nodig hadden met het typen van zoekopdrachten op YouTube en dat laat appen lastig was in verband met het (vroeg) opstaan voor werk, wat zij oplosten door de telefoon op stil te zetten. Daarnaast gaf één van de respondenten het volgende aan: 'Soms zijn sommigen onderwerpen wel wat lastig'. Eén respondent vond de geld game moeilijk. Videobellen verliep niet goed voor een respondent omdat een onbekend persoon belde, die vervolgens geblokkeerd werd. Tot slot gaf één van de respondenten aan dat het opzoeken van informatie niet goed ging omdat hij of zij de gewenste informatie niet kon vinden.

Opdracht 3 – mentale belasting door internetgebruik

De derde opdracht uit de onderzoekstas was een visuele opdracht waarbij de respondenten met behulp van een rood papier konden aangeven hoe vol hun hoofd zat door een probleem op het internet. Negen respondenten hadden geen problemen waardoor hun hoofd ook niet vol zat. Vijf respondenten hadden wel problemen, namelijk: het appen op een laat tijdstip door vrienden werd als vervelend ervaren en scoorde 2/10 rood, omdat het hun slaap verstoortte. Een ander probleem was het praten via sociale media, waarbij een respondent ernstig werd gepest en de situatie als 10/10 rood beoordeelde: "ik werd kankerezel genoemd in de chat van making meme. En dat ik mijn bek moest houden. Dit vond ik niet leuk." (cyberpesten). Verder vond één van de respondenten het slechte internet bij het kijken van YouTube video's en het ontvangen van een telefoontje van een onbekende tijdens videobellen vervelend, beide scoorden 2/10 rood. Tot slot gaf één van de respondenten aan dat hij iets op het internet niet vertrouwde en hierover met de begeleiding van de Klup had gesproken, wat ook 2/10 rood scoorde.

Opdracht 4 – Whatsapp hulpvraag

De vijfde opdracht betrof een WhatsApp-hulpvraag, waarbij een karakter (Charlie) vroeg om de bankpas van het andere karakter (Sem) uit een whatsapp conversatie te lenen. De respondenten moesten hun advies geven over deze situatie aan de zogenaamde 'Sem'. Twee respondenten konden deze vraag niet beantwoorden vanwege hun jonge leeftijd. De overige antwoorden (N=12) waren: nooit de bankpas uitlenen en geen pasje geven; niet doen omdat de vriend je bedriegt en hulp inschakelen van de politie; geen geld geven aan vrienden of vriendinnen; Sem had moeten reageren met "ik wil niet"; de ouders om advies vragen; de politie bellen en melden dat Charlie een oplichter is; het pasje niet uitlenen en eerst bellen om te controleren of het echt Charlie is; opletten op de manier van appen; en als iemand iets nodig heeft, die persoon vragen om langs te komen of te bellen om de echtheid te verifiëren. In het algemeen was het advies om de bankpas niet uit te lenen.

Alle respondenten die deze opdracht konden maken gaven dus aan de bankpas niet uit te lenen (N=12). Twee respondenten gaven als tip aan "Sem" om de politie in te schakelen. Andere respondenten adviseerden helemaal geen geld uit te lenen aan vrienden (N=2) of alleen geld uit te lenen als de desbetreffende persoon fysiek langskomt (N=1). Drie respondenten gaven aan dat zij eerst willen identificeren of "Sem" ook

daadwerkelijk de persoon is die hun via de app bereikt met de hulpvraag en één respondent geeft aan de persoon met de hulpvraag te vragen om langs te komen en er over te praten.

Opdracht 5 – versieren van de onderzoekstas

De vijfde en laatste opdracht van de onderzoekstas vroeg de respondenten om de onderzoekstas te versieren met creatieve elementen die betrekking hadden op digitale apparaten, apps of andere onlineactiviteiten. Negen van de veertien respondenten hebben hun tas versierd, resulterend in diverse en kleurrijke ontwerpen.

Enkele tassen werden door de respondenten in het algemeen mooi versierd met regenbogen, kleuren, namen, hartjes en bloemen. Andere tassen bevatten logo's van populaire platforms zoals TikTok, YouTube, Facebook, PlayStation, Tinder, Netflix, en Instagram. Een tas had met paars de woorden "WhatsApp, YouTube, spelletjes spelen, dingen opzoeken, tv kijken, mailen, online kopen" erop geschreven. Met blauw werden "WhatsApp, tv kijken, spelletjes spelen, Facebook, geldzaken, mailen, muziek luisteren, dingen opzoeken, nieuws kijken" toegevoegd. Een andere tas was versierd met zwart geschreven woorden zoals "Facebook, X, WhatsApp, Instagram, Nintendo, pc, tab7" en een tekening van een computer. Er waren ook tassen met kleurrijke teksten als "whappe: gamen, Facebook, nintenswif, whappe (WhatsApp?), tekening van de Nintendo" en woorden zoals "WhatsApp, Facebook, tv kijken, YouTube, spelletjes, mailen, online kopen."



Figuur 8 – Onderzoekers met de door respondenten ingevulde en versierde onderzoekstassen om inzicht te krijgen in hun digitale leefwereld.

Uit de resultaten van de onderzoekstas komt het volgende beeld over het digitale leven van de respondenten naar voren:

- Men maakt overwegend gebruik van het internet om te *ontspannen* dat wil zeggen series, films en YouTube video's bekijken;
- Ook wordt er gebruik gemaakt van verschillende *sociale media* om contact te leggen en onderhouden met bekenden en leeftijdsgenoten. Hierbij gaat het om platformen als WhatsApp, Instagram en Facebook. Gezien de aard van deze sociale media kan hiermee *door onbekenden contact worden gelegd met de deelnemers*. Zo ontving een deelnemer een videogesprek van een onbekende. Dit hoeft niet te betekenen dat dit direct een crimineel was die deze persoon benaderde, maar geeft aan dat ook deze doelgroep door onbekenden wordt benaderd. Daarnaast is er sprake van *slachtofferschap van online pesten* onder de deelnemers.
- Ook wordt er gebruik gemaakt van *online games* waaronder Roblox. Deze game heeft een chatfunctie waarmee onbekenden met elkaar kunnen chatten en de doelgroep dus in theorie *door onbekenden kunnen worden benaderd*. Criminelen kunnen hier misbruik van maken;
- Verder wordt het platform Tinder genoemd, een dating-platform waardoor deelnemers te maken kunnen krijgen met *dating fraude*;
- Verder noemen respondenten dat zij gebruik maken van e-mail, hierdoor kunnen zij in potentie het slachtoffer worden van *phishing* en andere vormen van fraude en oplichting die gebruik maken van e-mail (o.a. afpersingsmails);
- Tenslotte noemen respondenten ook het gebruikmaken van internet voor bankzaken. Daarmee zouden zij in potentie het slachtoffer kunnen worden van verschillende vormen van fraude die gebruik maken dan online betalingen (o.a. verkoopfraude).

Op basis van deze resultaten is duidelijk dat de respondenten met een LVB in het online, dagelijks leven daadwerkelijk kwetsbaar zijn voor pogingen van criminelen hen via social engineering te misleiden, met name via social media platforms, e-mail, online games en datingapps. Wel was duidelijk dat zij zich redelijk tot goed bewust zijn van het specifieke risico rondom geldezelen, maar dat het handelingsperspectief kan worden vergroot.

5.2 Kwalitatieve analyse: interviews

Hier worden de hoofdinzichten van de interviews met de begeleider-coördinator en gamification-medewerker gesproken.

Inzichten uit interview met de begeleider-coördinator

Allereest, kwam uit het interview met de begeleider-coördinator naar voren dat er zich relevante casuïstieken hebben afgespeeld op de Klup omtrent de onlinewereld. Als vertrouwenspersoon binnen de Klup komen deelnemers regelmatig naar haar toe met hulpvragen. Dit zijn de besproken casuïstieken:

1. Een deelnemer ontving bijvoorbeeld onbekende URL-linkjes en wist niet wat ze moest doen;
2. Een deelnemer werd benaderd op een datingsapp (Tinder) door een verdacht figuur;
3. Een deelnemer had last van hyperactieve groepsapps die "24 uur per dag doorgingen";
4. Een deelnemer werd regelmatig gebeld door een anonieme beller en werd daar onrustig van.

Ten tweede, gaf de geïnterviewde aan dat zij soms ademhalingsoefeningen inzet om verontruste deelnemers te kalmeren en tot een goed gesprek te komen over de problematiek. Hiermee brengt ze deelnemers—na het loskoppelen van de groep—van een hoge emotionele staat (boos of verdrietig) terug naar kalmte. Ze gaf aan behoefte te hebben aan meer vrijwilligers die uitgerust zijn in het toepassen van ademhalingsoefeningen, zodat dit breder ingezet kan worden binnen de Klup.

Als laatste, gaf de geïnterviewde aan dat een recentelijk (in 2024) georganiseerde thema-avond van een bank (gericht op omgang met internetbankieren) positief werd ontvangen voor zowel vrijwilligers als deelnemers (veel interactie, veel vragen). Dit zou een format kunnen zijn om onze interventie in uit te zetten.

Inzichten uit interview met de gamification medewerker

Allereest, kwam uit het interview met de gamification medewerker naar voren dat dat begeleiders en professionals beperkte grip hebben op hoe digitale media in de thuissituatie worden gebruikt. De geïnterviewde gaf aan dat zij wel zicht hebben op het mediagebruik binnen de Klup, maar controle over het gebruik thuis ontbreekt. Dit geldt zowel voor senioren als voor kinderen en jongeren met een specifieke ondersteuningsbehoefte. Ouderen maken bijvoorbeeld vooral gebruik van WhatsApp, YouTube en Facebook, terwijl jongeren zich vaak onderdompelen in TikTok, YouTube Shorts en online gaming volgens de respondent. In de thuisomgeving, waar minder toezicht is, kunnen sociale groepsdynamieken en mediagebruik ongecontroleerd plaatsvinden. Dit kan volgens de geïnterviewde leiden tot vervelende situaties, zoals het ontvangen van ongepaste foto's of het contact met onbekenden via gaming platformen en sociale media.

Ten tweede gaf de geïnterviewde aan dat er weinig zicht is op hoe en in welke mate sociale media worden wordt gebruikt. Hoewel begeleiders binnen de dagbesteding enige controle hebben over het digitale gedrag, verliezen zij dit volledig zodra deelnemers thuis of buiten begeleide omgevingen zijn. Vooral jongeren met autisme zoeken volgens de geïnterviewde vaker hun eigen digitale bubbel op, waarbij ze via hun telefoon of tablet urenlang video's kunnen bekijken of gamen. Hoewel sommige begeleiders volgens hem aangeven dat ze sporadisch meekijken met wat jongeren doen, wordt structureel toezicht nauwelijks toegepast. Dit komt deels doordat sociale media persoonlijk contact vervangen, waardoor het gebruik zich buiten het zicht van begeleiders afspeelt. Daarnaast is de technische toegankelijkheid van sociale media, waarbij leeftijdsrestricties eenvoudig te omzeilen zijn, volgens de geïnterviewde een complicerende factor.

Ten derde gaf de geïnterviewde aan dat er weinig sprake is van een structureel gesprek over de wisselwerking tussen digitale media en sociale interacties. Deelnemers delen zo af en toe ervaringen door bijvoorbeeld foto's te laten zien aan de begeleiders die ze via Facebook of WhatsApp hebben ontvangen, maar diepgaandere gesprekken over de impact van digitale media blijven volgens de geïnterviewde uit. Dit betekent dat begeleiders vooral op vervelende gebeurtenissen of incidenten reageren, zoals wanneer jongeren problematische content tegenkomen of specifieke vragen hebben over sociale media-gebruik.

Als laatste gaf de geïnterviewde aan dat er geen structurele controle is op wanneer en hoe vaak de deelnemers hun devices of sociale media gebruiken, vooral tijdens momenten van isolement of ont prikkeling. Alleen als er een duidelijk probleem ontstaat, zoals het voorbeeld van de geïnterviewde van een jong kind dat een horror game speelt, wordt er ingegrepen. Buiten deze incidenten is het moeilijk om toezicht te houden.

5.3 Kwantitatieve analyse: vragenlijst

Participanten

De coördinator van de vrijwilligers op de Klup (regio Twente) heeft via de nieuwsbrief (zie Figuur 7, Hoofdstuk 4.2) de vragenlijst (zie Bijlage 2) naar 352 vrijwilligers gestuurd. De vragenlijst is goedgekeurd door de Saxion Ethische Advies Commissie (SEAC; zie Bijlage 3). Er zijn twee dataverzameling rondes geweest. Dataverzameling ronde 1 (verzonden op 22 maart 2024) leverde 40 participanten op en ronde 2 (herinneringsmail op 24 april 2024) leverde 50 participanten op; in totaal hebben daarmee 90 begeleiders gereageerd.

Van de 90 participanten zijn 13 participanten verwijderd van de dataset vanwege volledig missende data. Daarnaast zijn er een aantal *cutoff* criteria gesteld voor de variabele “*progressie*” (100 = volledige participatie), “*tijdsduur*” (in minuten) en “*prevalentie met de LVB-doelgroep*”. Om de kwaliteit van participatie te waarborgen zijn alleen participanten met een *progressie-score* van 100 meegenomen in de sample. Er zijn hierdoor 10 participanten ($range_{progress} = 50-75$) uitgesloten van de sample.

De door Qualtrics gecalculerde verwachte tijdsduur van de vragenlijst was 11.6 minuten—de daadwerkelijk gemiddelde tijd is 11.3 minuten ($SD = 5.17$). Dit is berekend zonder drie *outliers* (lengte > 40 minuten). Dit is een gemiddelde waarbij rekening is gehouden met variatie in snelheid. Daarom is de *cutoff* op vier minuten gezet. Voor de mensen die geen open vragen beantwoord hebben werd een minimale duur van vier minuten als realistisch geschat. Hierdoor zijn geen cases op basis van tijd geëxcludeerd van de sample.

Als laatste exclusiecriteria zijn enkel participanten die in aanraking komen met de LVB-doelgroep in de sample meegenomen. Hierdoor zijn 7 participanten uitgesloten. De uiteindelijke sample bevat daarmee in totaal 60 participanten. Dit zijn participanten die volledig hebben geparticipeerd binnen een realistische tijd en in hun werk in aanmerking komen met de LVB-doelgroep.

De vragenlijst is in de analyse opgesplitst in twee delen: (1) gericht op begeleiders op de Klup zelf en (2) hun visie op de online weerbaarheid van deelnemers (met een LVB) bij de Klup.

Deel 1 – Begeleiders van de Klup

Internet gebruik. Een groot deel van de begeleiders is actief op het internet; zij maken meerdere keren per dag (63,3%) tot dagelijks (31,7%) gebruik van het internet. De top vijf meest uitgevoerde activiteiten op het internet zijn: mailen (90%), Whatsappen (87%), legaal video’s of muziek downloaden (82%), nieuwsberichten lezen (75%) en televisie kijken (70%). Opvallend is dat 25% van de participanten aangeeft wel eens illegaal video’s of muziek te downloaden; wat kan leiden tot een hoger risico op slachtofferschap—gezien de circulatie van virussen en malware rond illegale bestanden.

Affectieve respons. De meerderheid van de begeleiders bij de Klup maakt zich gematigd zorgen over de kans op, en mogelijke schade door, online criminaliteit ($M = 3,08$; $SD = 0,77$). In totaal geeft 25% aan dat zij zich (heel) veel zorgen maken over online criminaliteit (zie Tabel 5 en Figuur 9 voor de verdeling). De affectieve respons is met twee items gemeten (en samengevoegd in de analyse).

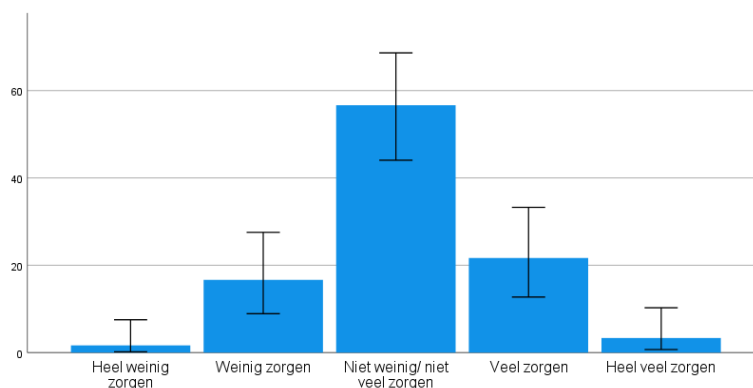
Item 1: *In hoeverre maakt u zich zorgen over de KANS dat u slachtoffer wordt van online criminaliteit?*

Item 2: *In hoeverre maakt u zich zorgen over de mogelijkheid dat u SCHADE oploopt door slachtofferschap van online criminaliteit?*

Tabel 5

Affectieve response: mate waarin begeleiders zich zorgen maken over online criminaliteit

	Frequentie	Percentage
Heel weinig zorgen	1	1,7
Weinig zorgen	10	16,7
Niet weinig/niet veel zorgen	34	56,7
Veel zorgen	13	21,7
Heel veel zorgen	2	3,3

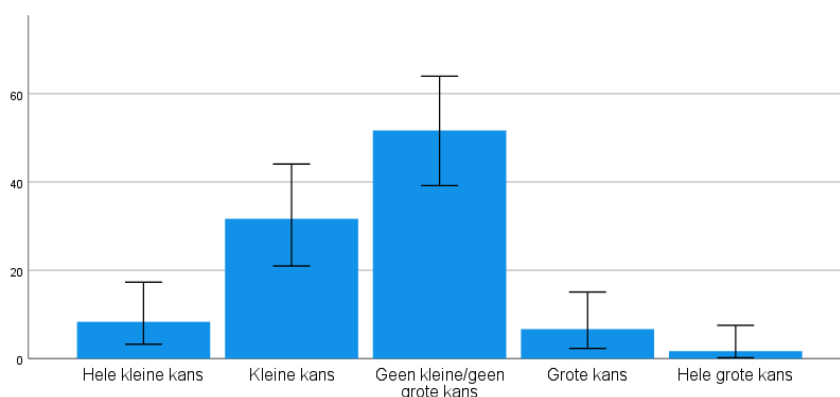


Figuur 9 – Affectieve response¹

Risicoperceptie. De meerderheid van de begeleiders rapporteren een kleine risicoperceptie ($M = 2,62$; $SD = 0,80$). In totaal zegt 8,4% een (zeer) grote kans te lopen om zelf slachtoffer te worden van online criminaliteit (zie Tabel 6 en Figuur 10 voor de verdeling). De begeleiders hebben een inschatting gemaakt over hoe groot zij de kans achten slachtoffer te worden van online criminaliteit in de komende 12 maanden. Deze risicoperceptie is gemeten met het item: *Hoe groot schat u de kans om de komende 12 maanden zelf het slachtoffer te worden van online criminaliteit?*

Tabel 6 – Risicoperceptie van de begeleiders op eigen slachtofferschap

	Frequentie	Percentage
Hele kleine kans	5	8,3
Kleine kans	19	31,7
Geen kleine kans/geen grote kans	31	51,7
Grote kans	4	6,7
Hele grote kans	1	1,7



Figuur 10 – Risicoperceptie van de begeleiders op eigen slachtofferschap

Zelf-effectiviteit. De begeleiders schatten de zelfeffectiviteit in het beschermen van online criminaliteit overwegend positief in ($M = 3,56$; $SD = 0,85$). De meerderheid van de begeleiders (41,7%) gaf aan het enigszins eens te zijn met de onderstaande items, terwijl 33,3% een neutrale positie innam. De kennis over gevaren/risico's van de begeleiders is gemeten door middel van zeven items:

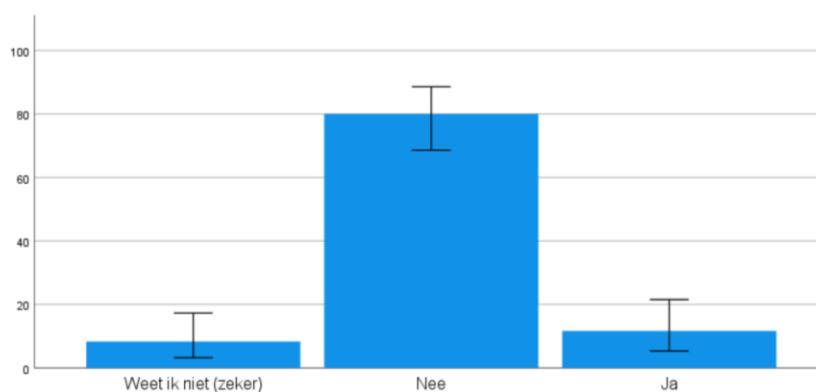
¹ Voor deze—en de volgende figuren—geven de getallen op de Y-as het percentage respondenten weer.

- Item 1: Ik weet hoe daders van online criminaliteit te werk gaan.
- Item 2: Ik ben in staat om in te schatten welke risico's ik loop om slachtoffer te worden van online criminaliteit.
- Item 3: Ik ben in staat mijzelf te beschermen tegen online criminaliteit.
- Item 4: Als ik voorbereidende maatregel tref, verkleint dat mijn kans om slachtoffer te worden van online criminaliteit.
- Item 5: De door mij genomen maatregelen zorgen ervoor dat ik minder kans heb om slachtoffer te worden van online criminaliteit.
- Item 6: Ik ben in staat juist te handelen wanneer ik slachtoffer ben of denk te zijn van online criminaliteit.
- Item 7: Mensen in mijn omgeving verwachten dat ik mijzelf bescherm tegen online criminaliteit.

Slachtofferschap onder begeleiders. Het slachtofferschap onder de begeleiders bij de Klup is relatief klein. Een groot deel van de respondenten (80%) geeft aan in de afgelopen 12 maanden geen aanraking te hebben gehad met een vorm van online criminaliteit, 11,7% geeft aan in aanraking gekomen te zijn met online criminaliteit en 8,3% weet dit niet zeker. Het is belangrijk om dit resultaat met de nodige voorzichtigheid te interpreteren, aangezien de gevoeligheid van deze vraag ertoe kan leiden dat niet alle slachtoffers hun slachtofferschap melden. Het slachtofferschap is gemeten met het item: *“Bent u in de afgelopen 12 maanden zelf in aanraking gekomen met een vorm van online criminaliteit?”* (zie Tabel 7 en Figuur 11 voor de verdeling).

Tabel 7 – Gerapporteerd slachtofferschap onder begeleiders bij de Klup

	Frequentie	Percentage
Weet ik niet (zeker)	5	8,3
Nee	48	80
Ja	7	11,7



Figuur 11 – Gerapporteerd slachtofferschap onder begeleiders bij de Klup

Zelfbeschermend gedrag. De top vijf meest uitgevoerde zelfbeschermende handelingen zijn:

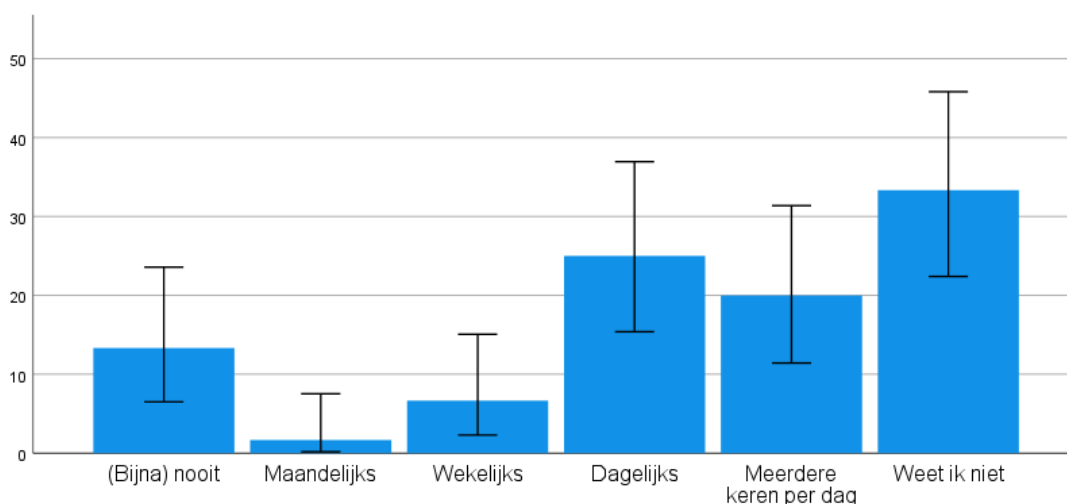
1. Inloggegevens niet delen met anderen (80%)
2. Niet op links/bijlage klikken in e-mails die niet vertrouwd lijken (77%)
3. Niet ingaan op advertenties die te mooi om waar te zijn lijken (77%)
4. Het vermijden/verlaten van websites die niet vertrouwd lijken (72%)
5. Sterke wachtwoorden met meerdere cijfers en tekens gebruiken (72%)

De top vijf *minst* uitgevoerde zelfbeschermende handelingen zijn:

1. Het downloaden van films, muziek en/of games enkel op de legale wijze (8%)
2. Het versleutelen van belangrijke/vertrouwelijke bestanden (15%)
3. Het vermijden van het gebruik van openbare wifi (23%)
4. Het gebruiken van een dubbele verificatie op de accounts (27%)
5. Het Googelen van informatie over onbekenden die contact opnemen (30%)

Deel 2 – deelnemers van de Klup

Internet gebruik. Er is een aanzienlijke onzekerheid en variabiliteit onder begeleiders over hun inschatting van het internetgebruik van de deelnemers van de Klup ($M = 4,37$; $SD = 1,67$). Alhoewel internetgebruik als hoog wordt ingeschat, wijzen de foutbalken in Figuur 12 op een aanzienlijke variabiliteit binnen de gerapporteerde percentages, wat de onzekerheid onder de begeleiders als geheel aangeeft. De data suggereert dat er mogelijk een gebrek aan communicatie of zichtbaarheid is met betrekking tot het internetgebruik van de deelnemers, of dat het internetgebruik zo divers is dat begeleiders geen eenduidig antwoord kunnen geven. De meest ingeschatte activiteiten die deelnemers online uitvoeren zijn social media (53%), Whatsapp (53%), video’s bekijken (48%), gamen (47%) en muziek luisteren (35%).

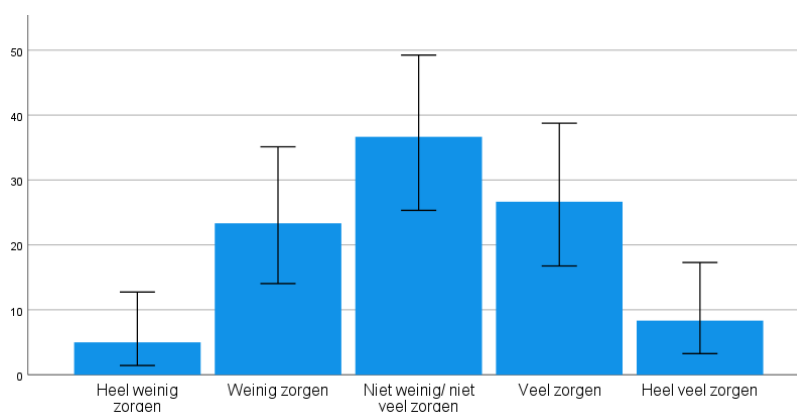


Figuur 12 – Internetgebruik van de deelnemers

Affectieve response. De resultaten tonen een variatie in de mate van zorgen onder de begeleiders over de kans en impact van slachtofferschap bij de deelnemers van de Klup ($M = 3,10$; $SD = 1,02$). Van de begeleiders maakt 35% zich (heel) veel zorgen over de kans op slachtofferschap van deelnemers—en de schade die deelnemers vervolgens oplopen door online criminaliteit. Tegenovergesteld, maakt zich 28,8% juist (heel) weinig zorgen. Er is onder de begeleiders dus geen eenduidige inschatting op zowel de kans als de gevolgen van online criminaliteit voor de deelnemers (zie Tabel 8 en Figuur 13).

Tabel 8 – Affectieve response m.b.t. kans en impact van slachtofferschap onder deelnemers

	Frequentie	Percentage
Heel weinig zorgen	3	5
Weinig zorgen	14	23,3
Niet weinig/niet veel zorgen	22	36,7
Veel zorgen	16	26,7
Heel veel zorgen	5	8,3

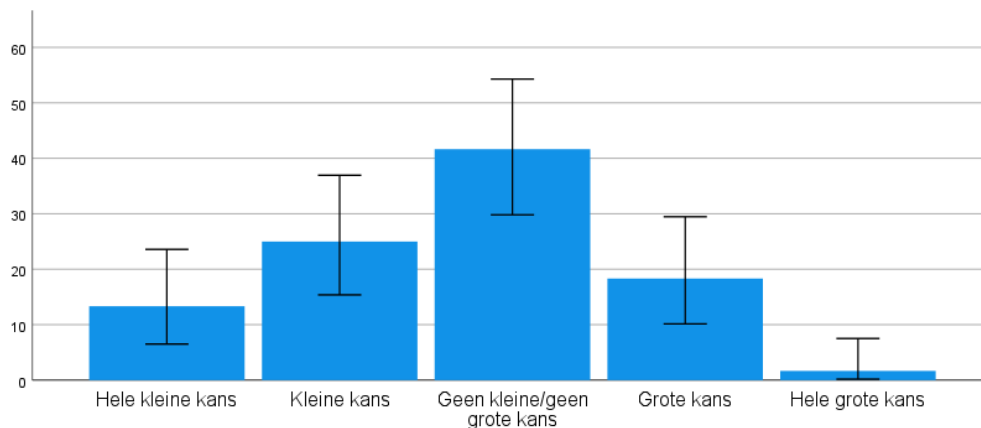


Figuur 13 – Affectieve response m.b.t. kans en impact van slachtofferschap onder deelnemers

Risicoperceptie. De resultaten tonen aan dat de begeleiders' perceptie van het risico op online criminaliteit onder de Klup-deelnemers varieert ($M = 2,7$; $SD = 0,98$), met een meerderheid die een neutrale houding aanneemt (41,7%), maar ook met aanzienlijke onzekerheid en variabiliteit (zie Tabel 9 en Figuur 14).

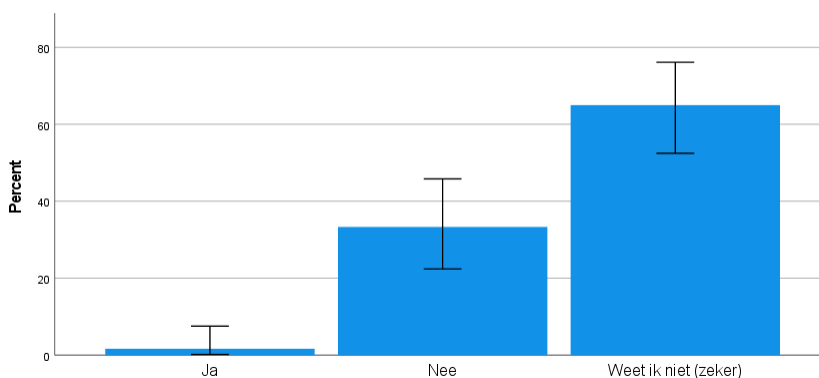
Tabel 9. Risicoperceptie richting deelnemers

	Frequentie	Percentage
Hele kleine kans	8	13,3
Kleine kans	15	25
Geen kleine/geen grote kans	25	41,7
Grote kans	11	18,3
Heel veel zorgen	1	1,7



Figuur 14 – Risicoperceptie richting deelnemers

Slachtofferschap. Een derde van de begeleiders schat in dat er geen sprake is van online criminaliteit onder deelnemers. Echter, een grote meerderheid (65%) geeft aan geen inzicht te hebben in het slachtofferschap van online criminaliteit onder de deelnemers (zie figuur 15).

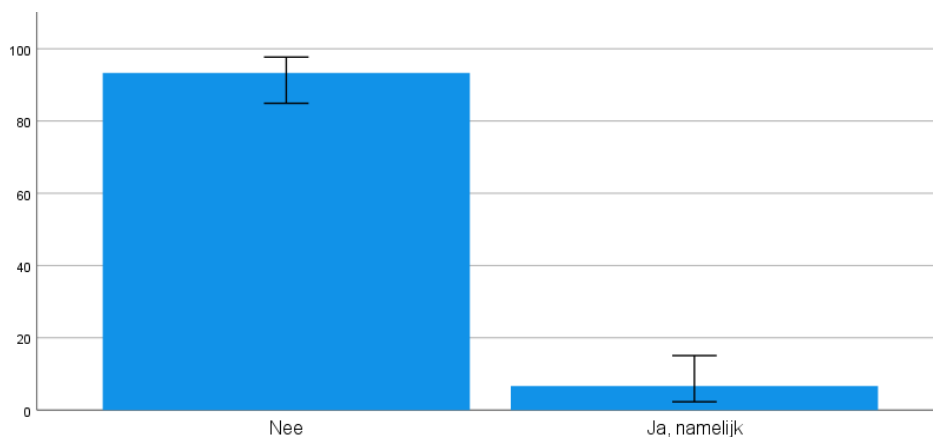


Figuur 15 – Inschatting van slachtofferschap onder deelnemers

Contact over veilig online gedrag. Op basis van de resultaten kunnen we constateren dat er vrijwel geen contact is (93,3%) tussen de begeleiders en deelnemers over digitaal veilig gedrag (zie Figuur 16). Dit is gemeten met het item: “Stellen deelnemer(s) van De Klup u wel eens vragen die te maken hebben met veilig gedrag op het internet?”.

Tabel 10 – Contact over veilig online gedrag tussen begeleiders en deelnemers.

	Frequentie	Percentage
Nee	56	93,3
Ja	4	6,7



Figuur 16 – Contact over veilig online gedrag tussen begeleiders en deelnemers

Preventie slachtofferschap. De top vijf meest voorgestelde interventies van begeleiders om online criminaliteit te voorkomen bij deelnemers zijn:

1. Kennis over contactpunten om hulp te vragen (45%).
2. Kennis over hoe de deelnemer criminele risico's kan herkennen (43%).
3. Kennis over hoe de deelnemer(s) moet reageren wanneer diegene in aanraking komt met online gevaren (43%).
4. Begeleiding omtrent praktische vragen (bv. online bankzaken) (37%)
5. Ervaringsdeskundigen die kunnen vertellen over de risico's van de online gevaren (35%).

6. Interventie-ontwikkeling

6.1 Inventarisatie: shortlist van bestaande interventies

Bij deze interventie-inventarisatie² (zie Tabel 11) is er onderscheid gemaakt tussen vier verschillende criteria, op basis van kleuren (groen, geel, rood, blauw) om het huidige interventie-landschap te filteren. Hieronder is per kleur toegelicht wat onder de categorisatie valt.

Groen: Dit betekent dat de interventie zich richt op cyberweerbaarheid én specifiek geschikt is voor mensen met een licht verstandelijke beperking (LVB) of een ervaringsgerichte aanpak hanteert. Er is ook gekeken naar de toegankelijk van de interventie en of de interventie begrijpelijk is voor deze doelgroep.

Geel: Deze interventies richten zich wél op cyberweerbaarheid, maar zijn niet specifiek ontwikkeld voor mensen met een LVB. Ze kunnen dus geschikt zijn voor een breder publiek, maar mogelijk minder toegankelijk of begrijpelijk voor de LVB-doelgroepen.

Rood: Deze interventies zijn te moeilijk op verschillende aspecten voor mensen met een LVB. Dat kan bijvoorbeeld komen door complexe taal, ingewikkelde opdrachten, of een vorm die veel zelfstandigheid en digitale vaardigheden vereist.

Paars: Deze interventies zijn vooral bedoeld voor begeleiders. Ze geven bijvoorbeeld richtlijnen, methodieken of hulpmiddelen om begeleiders te ondersteunen bij het vergroten van de cyberweerbaarheid van hun doelgroep.

Bij het beoordelen van de interventies hanteren wij naast de kleuren criteria ook een aantal andere criteria om te bepalen in hoeverre de interventies aansluiten bij de doelgroep en hoe deze kunnen worden ingezet. Deze criteria zijn: **betaalbaarheid**, **uitvoerbaarheid**, **(kosten)effectiviteit**, **gepastheid** en mogelijke **beperkingen**.

- **Betalbaarheid** verwijst naar de kosten die verbonden zijn aan de interventie. Dit kan variëren van gratis interventies tot programma's waarvoor een financiële investering nodig is.
- **Uitvoerbaarheid** beoordeelt of de interventie praktisch inzetbaar is, bijvoorbeeld of er specifieke middelen of begeleiding (netwerk) vereist zijn.
- **(Kosten)effectiviteit** kijkt naar de mate waarin een interventie bijdraagt aan het beoogde doel in verhouding tot de kosten.

² Het gehele Excel-bestand met de inventarisatie zal ook via de mail worden doorgestuurd.

- **Gepastheid** verwijst naar de mate waarin de interventie aansluit bij de doelgroep, bijvoorbeeld of deze is ontwikkeld met input van de doelgroep of goed aansluit bij hun belevingswereld.
- **Beperkingen** beschrijven mogelijke beperkingen van de interventie, zoals een sterke nadruk op kennisoverdracht zonder aandacht voor vaardigheden of een complexe aanpak die niet goed aansluit bij bepaalde doelgroepen.

Tabel 11 – Gefilterde interventielijst (shortlist)

Naam van de interventie/organisatie	Product	Thema('s) / Doel
Mediawijsheid	Lesmateriaal	Ondersteuners opleiden in de gevaren en bescherm-methoden
Mediajungle	platform online	geldezelen
Mediajungle	Bordspel + app	Bewustwording en weerbaarheid
Framed	Klassikaal gamen + Discussiëren	Leerlingen online bewuster maken en cybercrime voorkomen
Digitaal veilig op weg naar de brugklas	Laagdrempelig kaartspel	Bewustwording
Online Veiligheid	Voorlichting	Voorlichting
SnAppje, Sexting en Grooming	Voorlichting / lespakket	Voorlichting
Shitzooi	Interactief lesprogramma (video's)	Jongeren weerbaar maken tegen risico's van sexting
Online fraude en cybercriminaliteit	Voorlichting	Preventie slachtoffer / dader internet criminaliteit
Gemeente Breda	Virtuele Escape room	Cybersecurity
Hackhelpdesk: digitale eerstehulpverlening	Hulpplek voor slachtoffers	Snelle hulp (bij paniek)
Cyber24	Serious game met escapekoffer	Bewustwording: Sextortion, ID-fraude, geldezel, fraude, hacken
Het stopt bij jou	Educatieve escape room	Educatieve escape room
#leerlingalert	Voorlichting	Criminele carrière voorkomen
Game changers (via Politie)	Online challenge	Online spellen en uitdagingen
LVB Media Experience	Online tool	Bewustwordingstool voor begeleiders mbt digitale hindernissen LVB
Datadetoxkit (handig voor begeleiders)	Handleiding	Handleiding voor bevordering veiligheid
Leuker online	Gids voor begeleiders	
Groen = wel thema cyberweerbaarheid, wel LVB/ervaringsgericht		
Geel = wel thema cyberweerbaar, geen LVB		
rood = te moeilijk voor LVB		
paars = gericht op begeleiders		
1e beoordeling op kleur: zie legenda onderaan document		
2e beoordeling op kwaliteit: zie punten na link		

Naam van de Interventie/organisatie	Link
Mediawijsheid	https://www.mediawijsheid.nl/beperking/
Mediajungle	Mediajungle - Platform
Mediajungle	https://mediajungle.eu/
Framed	https://www.politie.nl/informatie/framed.html/
Digitaal veilig op weg naar de brugklas	https://hetc.cv.nl/themas/cyberveiligheid/cybercrime/database-lokale-cyberprojecten/digitaal-veilig-op-weg-naar-de-brugklas/
Online Veiligheid	https://www.halt.nl/samenwerken-met-halt/school/voorlichtingen-en-ouderbijeenkomsten
SnAppje, Sexting en Grooming	http://www.qpido.nl/aanbod/lespakket-sexting-grooming
Shitzooi	https://shitzooi.com/
Online fraude en cybercriminaliteit	https://www.halt.nl/halt-op-school/voorlichting-online-fraude-en-cybercriminaliteit
Gemeente Breda	https://gemeente-breda-cybersecurity-webpages.vercel.app
Hackhelpdesk: digitale eerstehulpverlening	https://hetc.cv.nl/themas/cyberveiligheid/cybercrime/database-lokale-cyberprojecten/hackhelpdesk-digitale-eerstehulpverlening/
Cyber24	https://www.voordeklas.com/onderwijsprogramma/cyber24/
Het stopt bij jou	https://hetstoptbijjou.nl/
#leerlingalert	#Leerlingalert PVO Oost Nederland (pvo-oostnederland.nl)
Game changers (via Politie)	https://hackintheClass.nl/legaal-hacken-tijdens-corona/
LVB Media Experience	https://lvmmediaexperience.nl/
Datadetoxkit (handig voor begeleiders)	https://datadetoxkit.org/nl/privacy/essentials
Leuker online	https://www.leukeronline.nl/

De ideeënbox (zie Tabel 12) is een verzameling van (alternatieve) interventies en voorlichtingsmateriaal die wij gedurende het onderzoek verzamelt hebben en mogelijk in de toekomst interessante toevoegingen kunnen zijn. De Ideeënbox biedt dus binnen ons onderzoek een aanvulling op bestaande geïnventariseerde interventies. De ideeën in deze box variëren in vorm en aanpak. Sommige richten zich op voorlichting en bewustwording via storytelling en informatieve campagnes, zoals Storytelling Cybercrime en diverse NOS-informatievideo's. Andere ideeën leggen de nadruk op lichaamsgerichte en ervaringsgerichte methoden, zoals Nextround, dat bokszaktraining combineert met weerbaarheid, of VR-simulaties zoals Flowborne. De ideeënbox fungeert dus als een inspiratiebron en biedt aanvullende, vernieuwende mogelijkheden om cyberweerbaarheid en zelfregulatie op diverse manieren te versterken. Afhankelijk van de doelgroep en context kunnen deze ideeën verder worden uitgewerkt en toegepast binnen bestaande of nieuwe interventies.

Tabel 12 – Ideëenbox

Ideëenbox		
Storytelling cybercrime (via Regiobureau)	Voorlichting (verhalen van slachtoffers)	Bewustwording (via verhalen van slachtoffers)
Labyrinth		
Landelijke campagne senioren en veiligheid	Posters / communicatie	Bewustwording
nextround	bokszak en sportprogramma	feedback over kracht en cardioprogramma; weerbaarheid door martial arts
Breinbijsluiters		
INFORMATIEF NIEUWSITEM:		
kan onderdeel worden van voorlichtingsprogramma of als onderdeel om gesprek verder aan te gaan, dit samen bekijken.		
NOS	Relevant artikel voor bestaande problematiek	
NOS	Voorlichting via Agent Robin	Cyberpesten
NOS	Voorlichting materiaal	Snel rijk worden
NOS	Voorlichting materiaal	Extra info over geldezels
NOS	Voorlichting materiaal	Grooming
NOS	Voorlichting materiaal	Cybercriminelen opgepakt
NOS	Voorlichting materiaal	Risk Factory: Info rond wat te doen bij ontvangst naaktfoto
LIJFELIJKE ASPECTEN / LVB RELEVANT		
Zelfontwikkeling (via CVD / De Klup)	VR simulatie met biofeedback	Aanschaf VR met biofeedback voor signalering stress-stijging / angst
Flowborne	VR simulatie	Stressreductie mbv visuele stimuli reactief obv de ademhaling
Jij en ik	Serious game	Stress-regulatie
X-Wall	Interactieve muur via voorwerpen gooien	
Snoezelen	Snoezelruimte	ontspanning bij mensen met ernstige verstandelijke beperking; beter omgaan met prikkels van buitenaf.

Bij de inventarisatie van interventies is er rekening gehouden met zes kernprincipes die van belang zijn voor effectieve interventies voor mensen met een LVB. Deze principes zijn gebaseerd op de theorie van de Wit, Moonen & Douma (2011; 2023) en vormen een belangrijke leidraad bij de beoordeling van de effectiviteit en toegankelijkheid van interventies binnen deze LVB-doelgroep. Mensen met een LVB hebben specifieke leer- en ondersteuningsbehoeften. Dit betekent dat interventies niet alleen informatief moeten zijn, maar ook afgestemd moeten worden op de manier waarop deze doelgroep informatie opneemt en toepast in de praktijk. De zes elementen van effectieve interventies bieden handvatten om leerprocessen beter aan te laten sluiten bij hun mogelijkheden en behoeften (zie Tabel 13).

Tabel 13 – Selectie op basis van de elementen

Koppeling 6 elementen van effectieve interventie voor LVB (de Witte, Moonen & Douma, 2011; 2023)						
Interventie	Veilige en positieve omgeving	Concrete oefenen	Eenvoudige taal, visueel	Afgestemd individu	Voorgestructureerd en simpel	Netwerk
Mediawijsheid	Is aandacht voor	Nee	Erg verbaal	Niet expliciet door enkel verbaal	Ja	Handvatten voor netwerk, maar niet samen tot oplossing komen en oefenen
Mediajungle (bordspel/app)	Is aandacht voor	Beperkt	Ja	Ja	Ja	Kan samen gespeeld, minder expliciet
Mediajungle (geldezel)	Is aandacht voor; extra benadrukt in aanvulling	Beperkt; extra nadruk op attitude en vaardigheid bij aanpassing	Ja	Ja	Ja	Ja, samen bespreken; in aanpassing ook samen oefenen

6.2 Iteratie ronde 1: ontwerp geldezel interventie

Allereerst, gaven de onderzoekstassen inzicht over de platformen waar deelnemers bij de Klup zich bevinden (YouTube, TikTok, Instagram, Tinder, X, Facebook en Whatsapp). Criminelen gebruiken deze online platformen steeds meer om (voornamelijk) jongeren te ronselen (Wissink & Quint, 2021). Er wordt op deze platformen veel geld beloofd in ruil voor het uitlenen van een pinpas en uiteindelijk worden ze zowel dader als slachtoffer, m.a.w. een geldezel. Ook mensen met een LVB vallen onder deze slachtoffergroep. Zij participeren ook in de onlinewereld, en gezien hun uitdagingen op cognitief en sociaal adaptief niveau van functioneren zijn zij extra kwetsbaar voor deze criminele praktijken omdat ze gevoelig zijn voor direct beloning, de gevolgen niet overzien en snel beïnvloedbaar zijn (Landelijk Kenniscentrum LVB, z.d.).

Ten tweede, de kwantitatieve analyse (vragenlijst) bleek dat het netwerk om de LVB-groep een relatief lage risicoperceptie en affectieve response heeft—en dat er vrijwel geen contact over veilig online gedrag plaatsvindt tussen begeleiders en deelnemers. Gepaard met het feit dat begeleiders vaak *digital immigrants* zijn en zelf al moeite hebben met de verbinding naar de online leefwereld van de LVB'er, ontstaat hier een extra risico.

Ten derde, gaf het interview met de gamification medewerker aan dat er weinig zicht en grip is op de onlinewereld van de deelnemers (waaronder LVB) en dat er ook geen frequente controle is wanneer deelnemers (buitenom de fysieke activiteiten) op de telefoon, tablet of PC zitten.

Als laatste, de interventie-inventarisatie blijkt dat veel interventies gericht zijn op kennisontwikkeling, terwijl deze niet altijd aansluiten op de lijfelijke en ervaringsgerichte behoeften van de LVB-doelgroep, waarbij ook attitude en vaardigheden van belang zijn. Daarnaast is er een opvallend tekort aan interventies rondom cyberweerbaarheid, zowel voor mensen met een LVB als voor hun begeleiders. De bestaande interventies richten zich doorgaans óf op de doelgroep óf op de begeleiders, maar een geïntegreerde aanpak die beide groepen omvat, ontbreekt. Bovendien is er geen enkele interventie die kennis, attitude en vaardigheden combineert.

Vanuit de bovenstaande vier inzichten is ervoor gekozen om de interventie *Mediajungle* verder te ontwikkelen voor de geldezelproblematiek, waarbij naast kennis ook attitude- en vaardigheidsaspecten worden toegevoegd. Helaas bleek het na overleg met *Mediajungle* niet mogelijk om deze elementen binnen het spel kosteloos te integreren. Daarom is besloten om de interventie als een aanvullend product te ontwikkelen, dat naast het spel ingezet kan worden.

Een onderzoeker—gespecialiseerd op psychomotorische therapie met de LVB-doelgroep—heeft vanuit haar expertise in emotie-regulatie en het aanleren van vaardigheden een instructie-handleiding ontwikkeld (zie Bijlage 4). Concreet bestaat dit uit (1) een rollenspel voor het aanleren van 'nee' zeggen tegen het uitlenen van een pinpas, en (2) twee ademhalingsoefeningen (Box-breathing en de Vijf-Vinger-Ademhaling). Aanvullend, zijn er twee posters ontwikkeld met zowel een preventieve als repressieve functie (zie Bijlage 5 en 6). Naast het aanleren van attitude en vaardigheden is het belangrijk dat er ook kennisoverdracht plaatsvindt rond bewustwording van de problematiek en specifieke handelingskaders in het geval van slachtofferschap. Deze posters zijn ontwikkeld volgens de principes besproken in het theoretisch kader (de Wit, Moonen & Douma, 2023): simplistisch taalgebruik, concrete oefenstof, voorgestructureerd en vereenvoudigd, gegeneraliseerd en betrokken bij het netwerk.

De eerste poster is gericht op kennisdeling rondom de geldezel problematiek. Het bespreekt in stappen hoe iemand een geldezel wordt (contact, vriendschap, belofte cadeau, vraag om pinpas, geld kwijt en geen

cadeau) en wat hierin de juiste keuze is (“Nee, je geeft je pinpas niet”). De informatie uit deze poster komt overeen met de informatie die de verkregen wordt wanneer de voorlichting doorlopen wordt van Media Jungle. Deze was eerder gratis toegankelijk, maar werd later toch betalend. Vandaar is er naast het spel ook een poster ontwikkeld om de kennis op eenvoudige manier te delen met zowel deelnemers als ouders/begeleiders.

De tweede poster gaat over de stappen die iemand kan zetten in het geval van slachtofferschap: rustig worden (via ademhaling), met een ouder of begeleider praten (of een hulplijn inschakelen; kindertelefoon, luisterlijn, Helpwanted, Keerpunt) en samen het probleem oplossen (door contact op te nemen met de politie en de bank). Vervolgens zijn deze posters met twee begeleiders geëvalueerd. Waarbij een aantal aanpassingen zijn doorgevoerd. Poster 1: (1) minder woorden, (2) visueler, waarin duidelijker werd wat een goede en slechte keuze was (via duimpjes, kruis, rood/groene kleuren) en (3) een consequentie: geen ontvangst geld of cadeau. Poster 2: telefoonnummers en website naar hulplijnen. Uit deze feedback kwam ook het belang van de begeleider naar voren in het uitleggen van de poster aan deelnemers, gezien de variatie in cognitieve capaciteit onder de LVB doelgroep. Dit sluit aan bij het belang van integratie van de interventie in het netwerk. Er is een aanvullende PDF ontwikkelt met handelingskaders voor begeleiders in het geval van slachtofferschap (zie Bijlage 7).

6.3 Iteratie ronde 2: verbreding van de interventie naar top vijf vormen van oplichting

De ontwikkelde interventie uit iteratie ronde 1 is voorgelegd aan de Klup om feedback op te halen over inhoud, vorm en toepasbaarheid van de ontwikkelde interventie. Op basis van een onlinegesprek op 4 februari 2025 is de conclusie getrokken dat er een aantal aanpassingen gedaan moeten worden aan de ontwikkelde interventie om aan te sluiten op de wensen van de opdrachtgever. De belangrijkste punten die uit het gesprek zijn gekomen:

- De ontwikkelde interventie is gebaseerd op het thema “geldezelen”, omdat dit de meest voorkomende vorm van criminaliteit is onder het LVB (Bekkers et al., 2020). De Klup heeft echter behoefte aan een interventie die te generaliseren is naar meerdere vormen van online criminaliteit en waarbij de focus ligt op zowel de deelnemer als de begeleider. Er is dus behoefte aan verbreding van de interventie, zodat de interventie bruikbaar is voor meerdere vormen van online criminaliteit.
- Op basis van deze feedback hebben we een stappenplan gemaakt om verder aan te sluiten op de wensen van de Klup, te weten:
 1. Het ontwikkelen van een top 5 van belangrijkste vormen van online criminaliteit, gebaseerd op het principe van social engineering;
 2. Een blauwdruk voor een generalistische interventie bruikbaar voor deze top 5 van belangrijkste vormen van online criminaliteit.

Blauwdruk algemene interventie

Om de interventie generalistischer te maken en aan te laten sluiten op verschillende vormen van online criminaliteit passend bij “social engineering” is er gekozen voor een interventie (een poster) waarbij de kernboodschap is: “FF Pauze, ademhalen, hulp vragen”.

De poster die is ontwikkeld richt zich op de vijf meest voorkomende vormen van online criminaliteit onder het LVB, zoals beschreven in het theoretisch kader (geldezelen, sextortion, online oplichting, dating fraude en identiteitsfraude). Daarbij wordt uitgegaan van vragen die online gesteld kunnen worden en die interessant kunnen zijn voor de doelgroep, namelijk: *Iemand stelt jou online de volgende vraag:*

- Wil je jouw bankpas uitlenen?
- Wil je persoonlijke (naakt)foto’s delen?
- Mag ik jouw inloggegevens van de bank?
- Wil je geld overmaken op mijn rekening?

- Mag ik jouw gegevens gebruiken voor het afsluiten van een betaalrekening?

De centrale boodschap voor cliënten is dan altijd: *“Dit zijn **jouw** persoonlijke gegevens. Deze gegevens deel je **niet** met onbekenden. Ook niet als je daarvoor een mooi cadeau, geld of een relatie wordt beloofd. Die krijg je daarna namelijk **nooit**.”*

“Houd persoonlijke informatie altijd voor jezelf”

Wat kun je doen?

Je krijgt een verzoek om iets persoonlijks te delen. Dit voelt niet fijn.
Voel je je gespannen en weet je niet goed wat je moet doen?
Geef je onderbuik je aan dat er iets niet klopt?

“FF PAUZE, RUSTIG WORDEN en dan EERST HULP VRAGEN”

Deze informatie is verwerkt in een poster (zie Bijlage 8).

Nieuwe feedbackronde de Klup

Op 12 maart 2025 zijn de aangepaste interventies nogmaals voorgelegd aan de Klup. Uit dit gesprek kwam naar voren dat de algemene campagne bruikbaar en zinvol is, maar dat er tevens behoefte is aan een specifiekere interventie. Deze interventie was in iteratieronde 1 reeds ontwikkeld (geldezelen). De afspraak is gemaakt om beide interventies te gaan gebruiken en evalueren. Er is voor gekozen om de interventies alleen te evalueren onder de begeleiders bij de Klup en te inventariseren in hoeverre deze interventies bruikbaar en nuttig zijn in de online begeleiding van de deelnemer.

Evaluatie van de interventies

Voor de evaluatie van de interventie zijn de begeleiders van de Klup benaderd door de coördinator van de avondgroep. Alle begeleiders hebben een mail ontvangen met daarin een link naar de online vragenlijst via Qualtrics waar begeleiders werden gevraagd hun reactie te geven op de ontwikkelde interventies. In totaal hebben we vijftien begeleiders bereid gevonden om hun reactie te geven op de interventies en de bruikbaarheid hiervan.

De begeleiders komen binnen de Klup allemaal in aanraking met deelnemers met een LVB, autisme, beginnende dementie, niet aangeboren hersenletsel en/of mensen met een (chronische) fysieke beperking. De leeftijdsgroepen variëren van kinderen tot 18 jaar (N=9), jongvolwassenen van 18 tot 25 jaar (N=9), volwassenen van 25 tot 65 jaar (N=13) en senioren (65+) (N=9).

Kennis

Vervolgens is in kaart gebracht in hoeverre de ontwikkelde interventies als bruikbaar worden gezien door de begeleiders. Allereerst is gevraagd in hoeverre de ontwikkelde tabel (Tabel 14) helpt om inzicht te krijgen in de verschillende criminaliteitsvormen en bijdraagt aan de kennis over criminaliteit. 59% van de respondenten geeft aan op basis van de tabel een redelijk tot zeer goed inzicht te krijgen in de verschillende vormen van online criminaliteit waar cliënten mee te maken kunnen krijgen ($M = 3,67$). Op de vraag in hoeverre respondenten op basis van de tabel weten waar zij terecht kunnen voor hulp, antwoordt 66,7% dat de tabel hierbij behulpzaam is ($M = 3,73$).

Tabel 14 - Top vijf criminaliteitsvormen

Criminaliteitsvorm	Definitie	Voorlichtingsinformatie	Contact slachtofferhulp	Tools voor verdieping
Geldezelen	Personen die hun bankrekening en/of pinpas uittelen aan criminelen om geld wit te wassen. Dit gebeurt vaak in ruil voor een geldbeloning, waarbij ze bijvoorbeeld hun pinpas afstaan voor criminele transacties.	- Politie: Informatie over geldezels - Mediawijsheid: Gesprekstips over online gedrag en cyberweerbaarheid - Veilig Bankieren: Informatie over geldezels - Slachtofferhulp Nederland: Hulp en informatie over geldezels - NOS: Wat is een geldezel? (uitlegvideo)	- Ga naar de bank en meld hier het (vermoeden van) geldezels. - Ga naar de politie om aangifte te doen, dit kan via: - Bel de politie op 0900-8844, of bij spoed op 112. - Anoniem, bel 0800-7000 of via meldmisdaadanoniem.nl	Mediajungle: mediajungle.nl
Sextortion				
Online-oplichting				
Datingfraude				
Identiteitsfraude				

Attitude

Vervolgens is aan respondenten gevraagd naar hun mening over het stappenplan voor de ademhalingsoefeningen (zie Figuur 17). Dit stappenplan wordt als zeer positief beoordeeld. 80% van de respondenten vindt dit stappenplan redelijk goed tot zeer goed ($M = 4,27$). Wel wordt aangegeven dat het ligt aan het type deelnemer. Hoe lager het niveau, hoe moeilijker het wordt. Op de vraag of de instructie (zie Bijlage 4, p. 70 voor Box-Breathing ademhalingsoefening) helpt om deze ademhalingsoefeningen samen uit te voeren, zegt 66,7% dat deze instructies helpend zijn ($M = 3,73$). Hierin geven respondenten aan dat het belangrijk is dat het met regelmaat wordt getraind.

Stappenplan

- 1. Bespreek de situatie**
 - o Vraag wat er is gebeurd en luister actief.
 - o Stimuleer de deelnemer om de hulpvraag te verwoorden.
- 2. Pauzeren en kalmeren**
 - o Help de deelnemer om rustiger te worden via een ademhalingsoefening.
 - o Geef ruimte voor emoties, maar help deze ook te reguleren.
- 3. Samen tot een oplossing komen**
 - o Bespreek mogelijke stappen om de situatie op te lossen.
 - o Ondersteun waar nodig bij het nemen van actie, zoals het melden van het incident.

Figuur 17 – Stappenplan voor emotie-regulatie en oplossing van incident

Vaardigheden

Op de vraag in hoeverre de instructies voor het “leren NEE zeggen” handvatten geeft om deze vaardigheden te oefenen met de deelnemers, zegt 66,7% van de respondenten dat deze instructies redelijk tot zeer goed zijn ($M = 3,80$). Hierbij wordt door de respondenten aangegeven dat de doelgroep duidelijk gewezen moet worden op de werkwijze van criminelen (gebruik van overtuigende argumenten om het slachtoffer over te halen deel te nemen aan criminele activiteiten). Ook wordt er aangegeven dat er veel behoefte is aan het krijgen van trainingen over de toepassing van deze vaardigheden.

Vorm

Op de vraag in welke vorm respondenten de interventie graag zouden willen ontvangen geeft het merendeel aan dit zowel fysiek als online te willen (53,3%). 20% zou het graag willen in fysieke vorm en 26,7% juist in een onlinevorm. Daarnaast wordt aangegeven dat er behoefte is aan voorbeeldvideo's en rollenspellen. Ook geven respondenten aan dat het handig zou zijn om een duidelijk zichtbaar en aanwezig aanspreekpunt of vertrouwenspersoon binnen de Klup te hebben voor zowel personeel, vrijwilligers als deelnemers.

Interactieve informatie-avond

Tenslotte is gevraagd in hoeverre respondenten behoefte hebben aan een interactieve informatiesessie om kennis te krijgen van de interventie en de wijze waarop deze toe te passen is. 46,7% zegt hier geen behoefte aan te hebben. De overige respondenten hebben hier behoefte aan, mits het tijdstip uitkomt.

7. Conclusie/discussie

In dit onderzoek is gekeken naar de digitale leefwereld van mensen met een LVB. Er is in kaart gebracht op welke wijze zij digitaal actief zijn en welke interventies kunnen bijdragen aan het online weerbaar maken van deze doelgroep. Hierbij is niet alleen gekeken naar de LVB'er zelf, maar is er ook gekeken naar de wijze waarop de schil om deze groep (begeleiders bij de Klup) betrokken kunnen worden bij het vergroten van de digitale vaardigheden en de online weerbaarheid van mensen met een LVB.

7.1 Projectdoelstellingen

Voorafgaand aan het onderzoek hebben wij een zestal doelen gesteld, die hieronder behandeld zullen worden.

- 7.1.1. *Het in kaart brengen van het dagelijkse leven van mensen met een LVB en de risico's waarmee zij geconfronteerd worden in de digitale wereld.*

Aan de hand van onderzoekstassen is bevraagd aan de respondenten op welke wijze zij gebruik maken van het Internet. De resultaten laten zien dat de respondenten gebruik maken van diverse apparaten om online te kunnen zijn, zoals tablets en telefoons. Deze apparaten worden voor verschillende doeleinden ingezet, variërend van entertainment en communicatie tot educatieve activiteiten en dagelijkse praktische taken. Respondenten maken hierbij gebruik van verschillende platformen, zoals YouTube, Whatsapp, Facebook, X, Tinder en Instagram. Dit maakt hen vatbaar voor vormen van online criminaliteit waarbij slachtoffers worden gezocht via deze platformen, zoals geldezelen, sextortion en vormen van online fraude en oplichting. De respondenten die de onderzoektas hebben ingevuld geven aan weinig ervaring te hebben met problemen in de digitale wereld. Wel zijn er respondenten die vervelende ervaringen hebben gehad op het internet, zoals online pestgedrag.

- 7.1.2. *Inzicht krijgen in de factoren die bijdragen aan online weerbaarheid van mensen met een LVB en hierbij passende effectieve interventies voor deze doelgroep.*

Uit het literatuuronderzoek komt naar voren dat er verschillende factoren zijn die bijdragen aan de online weerbaarheid van mensen met een LVB. Om potentiële slachtoffers weerbaarder te maken tegen online dreiging is het belangrijk om de cyberweerbaarheid van individuen te verhogen. Hierbij gaat het vooral om de aanwezigheid van risicobewustzijn onder mogelijke slachtoffers en het vermogen om zelfbeschermende maatregelen te nemen om het risico op slachtofferschap te verminderen (Spithoven, 2020).

Daarnaast laat het literatuuronderzoek zien dat mensen met een LVB vaker—in vergelijking met leeftijdsgenoten—te maken krijgen met stressvolle situaties (Emerson, 2003; Hatton & Emerson, 2004; Schuengel & Jansen, 2006) en meer moeite hebben hierop adequaat te reageren. Ze hebben minder bronnen om hiermee om te gaan (o.a. Lunsky & Benson, 2001), wat het extra belangrijk maakt voor mensen met een LVB om voldoende veerkracht te hebben.

Bij het vergroten van de weerbaarheid van mensen met een LVB lijkt een lijfelijke aanvliegroute van meerwaarde omdat er op deze manier minder ingezet wordt op de cognitieve vaardigheden. Zeker voor deze doelgroep, waar de cognitieve en reflectieve vermogens beperkt zijn. Door de lijfelijke aanpak wordt de fysiologische stressreactie direct beïnvloed (en dus daarmee ook het direct het impulsief handelen), zonder dat er echt begrepen hoeft te worden hoe het werkt (o.a. Bellemans et al., 2022; Currie et al., 2019).

Wanneer er wordt gekeken naar het grote geheel rond effectieve interventie creatie voor mensen met een LVB, dan is een integratie tussen **kennis** (over gevaren/risico's), **attitude** (*window of tolerance*) en

vaardigheid (handelingskaders voor zowel deelnemers als begeleiders) nodig om effectieve gedragsverandering bij deze doelgroep te realiseren. Als al deze drie factoren niet meegenomen worden in een interventie voor deze doelgroep, dan is zelfbeschermend gedrag (voor de deelnemer, begeleider en combinatie van die twee) niet mogelijk, en bemoeilijkt dit ook de toepassing op het dagelijks leven. Naast de inhoud—kennis, attitude en vaardigheid—is het belangrijk dat interventies eenvoudig, concreet, gestructureerd en geïntegreerd zijn in het netwerk van iemand met een LVB (de Wit, Moonen & Douma, 2023).

7.1.3. *Het inzichtelijk maken van potentieel geschikt te maken, bestaande interventies voor mensen met een LVB om de online weerbaarheid te vergroten.*

Op basis van een aantal uitgangspunten is gekeken naar bestaande interventies en beoordeeld in hoeverre deze interventies geschikt zijn om de zelfredzaamheid van mensen met een LVB te vergroten. Interventies zijn beoordeeld op:

- Is de interventie gericht op cyberweerbaarheid?
- Is de interventie gericht op de LVB doelgroep?
- Wordt in de interventie aandacht gegeven aan het vergroten van **kennis, attitude en vaardigheden**?

Interventies die zowel gericht zijn op cyberweerbaarheid als specifiek aansluiten bij de behoeften van de LVB-doelgroep, zijn geselecteerd voor een nadere analyse. Uit de interventie-inventarisatie bleek dat veel interventies zich voornamelijk richten op kennisontwikkeling, terwijl deze aanpak niet altijd aansluit op de lijfelijke en ervaringsgerichte behoeften van de LVB-doelgroep, waarbij ook attitude en vaardigheden van belang zijn. Van alle beoordeelde interventies voldeed alleen *Mediajungle* aan veel van de gestelde criteria. *Mediajungle* is een online spel over digitale geletterdheid en online weerbaarheid (waaronder de geldezelproblematiek), waarbij op interactieve wijze wordt ingezet op het vergroten van de kennis van participanten over dit onderwerp. Daarnaast biedt het spel de mogelijkheid om uit te breiden en lijfelijke elementen toe te voegen. Daarom is in dit onderzoek gekozen om deze interventie verder te ontwikkelen, waarbij naast het kennisgedeelte ook attitude- en vaardigheidsaspecten worden geïntegreerd.

Na contact met *Mediajungle* bleek dat het niet mogelijk was om de attitude- en vaardigheidsaspecten binnen het spel te integreren volgens de reeds gemaakte afspraken. Daarom is ervoor gekozen de interventie te ontwikkelen als een aanvullend product dat naast het spel kan worden ingezet (**1^o iteratie**). Hoewel de attitude en vaardigheden-integratie in *Mediajungle* aanvankelijk gratis geïntegreerd kon worden, werd deze later via betalend geëist. Daarom is de aparte handleiding—die tijdens het spel kan worden toegepast—aanvullend een poster ontworpen als een laagdrempelige manier om kennis eenvoudig te delen met zowel deelnemers als ouders en begeleiders.

Na de terugkoppeling van de geldezel interventie bleek de behoefte van de Klup breder te zijn dan het thema geldezelen. Hierdoor is de interventie verbreed naar een top vijf criminaliteitsvormen en is afgeweken van de doorontwikkeling op *Mediajungle* (**2^o iteratie**). De focus van de interventie lag in de 2^o iteratie op (1) het ontwikkelen van voorlichtingsmateriaal rondom de vijf meest gevaarlijke online criminaliteitsvormen voor de LVB-doelgroep (*kennis*; via een poster en kennisfolder) en (2) het bieden van een instructie-handleiding voor begeleiders waarin de deelnemers leren ‘nee’ zeggen tegen het delen van persoonlijke informatie en waarbij begeleiders ademhalingsoefeningen kunnen toepassen om deelnemers in een hoge arousal te kalmeren (*attitude* en *vaardigheden*).

7.1.4. *Het inzichtelijk maken van potentieel geschikt te maken, bestaande interventies voor de schil om de LVB'er heen (ouders/begeleiders), met als doel het signaleren van onveilige online situaties en het adequaat hierop reageren.*

Om interventies geschikt te maken voor begeleiders, is er gekeken naar handvatten voor begeleiders om cliënten te kunnen begeleiden in de online wereld en te helpen wanneer zij potentieel slachtoffer zijn geworden van cybercrime. De geïnventariseerde interventies op cyberweerbaarheid waren allemaal gericht op kennis en slechts beperkt op attitude en vaardigheden. Dit terwijl met name het attitude en vaardighedenaspect – naast het kennisaspect rond cybercriminaliteit - belangrijk zijn om tot juist toepassen van gedrag te komen bij de doelgroep mensen met een LVB. Het generaliseren naar het dagelijks leven kreeg nergens aandacht. Dit is echter van wezenlijk belang voor de doelgroep en zij hebben hierin ondersteuning nodig van hun begeleiders. Zonder hulp van begeleiders zijn zij niet in staat om adequaat te handelen bij potentieel slachtofferschap.

Om adequaat te kunnen handelen in een situatie die stressvol of onveilig is, is het van belang om eerst rustig te worden. Op die manier is men in staat om te komen tot doordacht/adequaat gedrag in plaats van impulsief gedrag. Een voorwaarde hiervoor is om dus lijfelijke rust te kunnen ervaren, of met andere woorden emoties te kunnen reguleren. Dit houdt in dat wanneer een deelnemer gespannen is (te merken aan druk gedrag, gespannen spieren (vaak gespannen kaakspieren, gebalde vuisten, wiebelende benen of vingers) of veranderd ademhalingspatroon (snellere ademhaling of zuchten), lijfelijke ontspanning van belang is om vervolgens het gesprek aan te kunnen gaan en samen tot oplossing te kunnen komen (adequaat gedrag).

Deze aspecten zijn verwerkt in de interventies die zijn ontwikkeld, door 1) begeleiders informatie te geven over cybercrime en daarmee hun kennis te vergroten (voor **iteratieronde 1** ging het hier om *de geldezelproblematiek* en voor **iteratieronde 2** om *social engineering*) en 2) door oefeningen te ontwikkelen die uitgevoerd kunnen worden door begeleiders om ervoor te zorgen dat cliënten rustig worden (de ademhalingsoefeningen – zie bijlage 4) en het leren NEE zeggen. Deze interventies geven begeleiders de nodige tools om cliënten te begeleiden in de online wereld, ze te helpen op het gebied van kennis en ze te begeleiden in het rustig worden en zoeken naar adequate oplossingen wanneer dat nodig is. Dit is zowel helpend in situaties waarin de deelnemer zelf met een vraag komt als deze gespannen is. Dan zijn de ademhalingsoefeningen zinvol in het helpen om eerst rustig te worden en vervolgens samen tot oplossingen te komen. Tevens zijn deze oefeningen zinvol in het geval dat het een deelnemer niet lukt om dit zelf op te merken. In dat geval kan de begeleider vanuit observatie even checken bij de client of er hulp nodig is, de deelnemer even apart nemen en tot rust komen om dan vervolgens ook samen tot een oplossing te komen.

7.1.5. *Het ontwikkelen/geschikt maken en implementeren van een effectieve interventie om de cyberweerbaarheid van mensen met een LVB en de schil hieromheen te verhogen.*

Binnen dit onderzoek zijn een tweetal interventies ontwikkeld die inspelen op kennis, attitude en vaardigheden met als doel om de cyberweerbaarheid van mensen met een LVB en de schil hieromheen te verhogen. Hierbij is de theorie uit het literatuuronderzoek als uitgangspunt genomen en is er – naast het vergroten van de kennis over online criminaliteit – veel aandacht voor de bijbehorende attitude en vaardigheden van deelnemers en hun begeleiders. Deze combinatie aan facetten zorgt niet alleen voor een toename aan risicobewustzijn en kennis over het onderwerp, maar ook voor het leren om adequaat te handelen wanneer er zich een cyberrisico voordoet.

Allereerst zijn posters ontwikkeld om de bewustwording rondom de thema's geldezelen (**iteratieronde 1**) en social engineering (**iteratieronde 2**) te vergroten. De posters helpen tevens om een gezamenlijke taal te

spreken over deze thematiek en de stappen die genomen moeten worden om adequaat te handelen samen te doorlopen. Daarnaast geven de posters ook een ingang om over dit onderwerp met begeleiders in gesprek te gaan.

Daarnaast zijn er oefeningen ontwikkeld die het adequaat handelen (attitude en vaardigheden) stimuleren, namelijk 1) ademhalingsoefeningen en 2) het leren 'nee' zeggen. Om adequaat te leren handelen, is het van belang om de hierbij passende adequate vaardigheden te oefenen: van een geïsoleerde oefening tot het toepassen van deze oefening in de situatie waarin het van belang is. Deze generalisatie is voor mensen met en LVB niet vanzelfsprekend en moet in kleine stapjes met variaties en herhaling geoefend worden. Daarom zijn zowel de ademhalingsoefeningen en de oefeningen om 'nee' te zeggen wanneer persoonlijke informatie wordt gevraagd, belangrijk om te oefenen in combinatie met de kennis over de cybergevaaren die kunnen spelen.

Het oefenen van deze vaardigheden wordt binnen de ontwikkelde interventie gedaan in een steeds moeilijker worden context (meer realistisch – in gespreksvorm), waarbij er veel herhaling is. Hierbij is het ook belangrijk dat de begeleider betrokken is om hierin te ondersteunen. Niet enkel om hen bij de oefening te ondersteunen maar ook om de bewustwording rond het onderwerp scherp te houden en een opening te bieden voor een gesprek rondom dit thema.

7.1.6. Het evalueren van de effecten van de interventies.

Vanwege tijdsgebrek is het helaas niet gelukt om de interventie onder zowel cliënten als begeleiders te evalueren. Wel zijn in totaal vijftien begeleiders bereid gevonden om de ontwikkelde interventies te beoordelen op effectiviteit. Uit deze evaluatie bleek dat de begeleiders grotendeels tevreden tot zeer tevreden zijn over de ontwikkelde interventies. Zij zien een grote meerwaarde in de ontwikkelde ademhalingsoefeningen en het leren 'nee' zeggen en zien beide onderdelen als zeer zinvol en bruikbaar binnen de Klup. Daarnaast beoordelen zij de ontwikkelde posters als zinvol en helder en hebben zij behoefte aan een thema-avond waarin de ontwikkelde interventies worden besproken en de vaardigheden worden geoefend. Zij zien een duidelijke meerwaarde in de koppeling tussen kennis, attitude en vaardigheden in de ontwikkelde interventies.

7.2 Discussie

Dit onderzoek is met veel enthousiasme en zorgvuldigheid uitgevoerd en heeft veel bruikbare informatie opgeleverd over de online weerbaarheid van mensen met een LVB en hun begeleiders. Desondanks zijn er ook een aantal limitaties binnen dit onderzoek die hieronder besproken zullen worden.

We hebben een maand vertraging opgelopen in de afronding van het onderzoek en hebben de effectevaluatie uiteindelijk niet onder cliënten kunnen uitvoeren, maar enkel onder begeleiders. Dit komt enerzijds doordat er een aantal wisselingen zijn geweest in zowel onderzoekers vanuit Saxion alsook aanspreekpunten binnen de Klup. Anderzijds was het contact met de praktijkpartner soms uitdagend. De contactpersonen binnen de Klup hebben te maken met een hoge werkdruk en hadden daardoor niet altijd de mogelijkheid om (snel) te reageren op verzoeken en vragen. Ook was het ontbreken van kennis over en ervaring met online criminaliteit binnen de Klup soms een uitdaging, omdat daarmee de denkkaders vanuit de praktijk niet altijd overeenstemden met de feitelijke risico's van online criminaliteit voor de LVB doelgroep.

Dit laatste punt zorgde ervoor dat we meerdere iteratierondes hebben doorgevoerd in de ontwikkeling van de interventies, waarbij we op verzoek van de Klup van een hele specifieke interventie (*geldzelen*)

teruggegaan zijn naar een hele generalistische benadering (*social engineering*), om vervolgens weer terug te gaan naar het oorspronkelijke idee van een specifieke interventie voor zowel deelnemer als begeleider (*geldeezelen*). Ondanks dat het doorlopen van deze fases zorgde voor wat vertraging, leverde het ook veel op. Het heeft geholpen in het vergroten van de kennis en het risicobewustzijn van de praktijkpartner en heeft daarnaast geresulteerd in een interventie die breed gedragen wordt en uitgezet wordt binnen de Klup.

Een andere limitatie van het onderzoek is het gebruik van onderzoekstassen als meetinstrument. Ondanks dat de vragen gesteld in de onderzoekstas voor alle cliënten hetzelfde waren (en daarmee een constante factor), is de wijze van beantwoording door alle cliënten anders gedaan. Dit maakte de analyse van de verkregen data moeilijk. Het verzamelen van data onder de LVB doelgroep is uitdagend en zeer tijdsintensief doordat alle cliënten verschillend in de exacte aard van hun problematiek. Wel bleek het uitzetten van de onderzoekstassen en het feit dat begeleiders samen met de cliënten aan de slag gingen met deze onderzoekstassen zinvol in het creëren van een eerste bewustwording ten aanzien van online criminaliteit.

Opvallend aan het onderzoek is dat er een duidelijke incongruentie bestaat tussen de eigen inschatting van de online weerbaarheid van cliënten en begeleiders enerzijds en het daadwerkelijk handelen anderzijds. Dit maakt dat begeleiders zichzelf overschatten in de kennis en kunde rondom online veiligheid, zowel voor zichzelf als voor de deelnemers. Tegelijkertijd nemen zij niet de passende zelfbeschermende maatregelen die nodig zijn om de kans op slachtofferschap te minimaliseren. Deze resultaten benadrukken de noodzaak om in te zetten op werkende interventies voor zowel cliënten als hun begeleiders, waarin zowel kennis, attitude als vaardigheden worden vergroot.

Het onderzoek laat zien dat de nadruk binnen interventies om online weerbaarheid onder het LVB te vergroten moet liggen op kennis, attitude en vaardigheden, waarbij vooral het contact met het eigen lichaam en het reguleren en inoefenen van vaardigheden *an sich* cruciaal is. De vraag is in hoeverre begeleiders hiertoe in staat zijn. Wanneer hierop vastgelopen wordt, dan is het wijs om op dat stuk een psychomotorisch therapeut in te zetten en daarop te ondersteunen.

Zoals al aangegeven hebben we een kleine vertraging opgelopen in de afronding van dit onderzoek. Daarom zal voor de Klup nog een tweetal dingen worden gedaan, zodat de interventies goed kunnen landen binnen de organisatie, te weten:

1. Er zal een thema-avond worden georganiseerd. Ondanks enige handelingsverlegenheid zijn mensen op zoek naar het internaliseren van de vaardigheden die nodig zijn om cliënten (beter) te begeleiden in de online wereld. Tijdens de thema-avond zal er ruimte zijn om de vaardigheden te oefenen en te leren toepassen;
2. In de generalistische interventie zijn een vijftal vormen van online criminaliteit genoemd passend bij het construct *social engineering*. Deze vormen van online criminaliteit worden nog verder uitgewerkt, inclusief definities en verwijzingen naar websites voor meer informatie, zodat begeleiders hierin beter in staat zijn cliënten te helpen wanneer nodig.

Slotwoord

Het onderzoek was zeer innovatief en creatief van aard. De ontwikkelde interventies zijn naar ons weten de eerste interventies voor de LVB doelgroep gericht op zowel het vergroten van kennis, het inzetten op attitude alsook het integreren van vaardigheden. De focus op het lijfelijke en ervaringsgerichte is hierbij vernieuwend en blijkt zeer effectief te zijn in het vergroten van de online weerbaarheid van mensen met een LVB. Daarnaast heeft dit onderzoek een positieve bijdrage geleverd aan het gesprek over online criminaliteit. Begeleiders en deelnemers zijn door dit onderzoek met elkaar in gesprek gegaan over de online componenten uit het dagelijks leven van de deelnemers, wat inzicht geeft in waar de risico's in de online wereld voor de specifieke doelgroep zitten. Daarnaast leren begeleiders hoe zij deelnemers tegen deze

Titel Digitaal Meedoen: LVB Cyberweerbaar!

Pagina 56 / 94

risico's kunnen beschermen en zorgt het contact tussen begeleiders en deelnemers ervoor dat deelnemers hulp kunnen vragen aan begeleiders als dat nodig is en kunnen begeleiders op hun beurt weer hulp zoeken bij o.a. sociaal werk, de politie, de bank, etc. als daar een aanleiding voor is. Met andere woorden: het netwerk om het netwerk activeren: samenredzaamheid!

BIJLAGE 1 - Geraadpleegde literatuur

Alfredsson Ågren, K., Kjellberg, A., & Hemmingsson, H. (2019). Digital participation? Internet use among adolescents with and without intellectual disabilities: A comparative study. *New Media & Society*, 22(12), 2128–2145. <https://doi.org/10.1177/1461444819888398>

Akkermans, M., Derksen, E., Kennis, M., Kloosterman, R., & Moons, E. (2024). Veiligheidsmonitor 2023. Ministerie van Justitie en Veiligheid & Centraal Bureau voor de Statistiek. <https://www.cbs.nl/nl-nl/longread/rapportages/2024/veiligheidsmonitor-2023#:~:text=Landelijke%20enqu%C3%AAte%20onder%20Nederlanders%20van%2015%20jaar%20en,burgers%20en%20politie%2C%20preventie%2C%20respectloos%20gedrag%20en%20discriminatie.CBS>

Amerpoort. (z.d.). Meer weten over mensen met een LVB. Geraadpleegd op 4 november 2022, via <https://www.werkenbijamerpoort.nl/doelgroepen/lvb>.

Beerthuisen, M. G. C. J., Sipma, T., & van der Laan, A. M. (2020). *Aard en omvang van dader-en slachtofferschap van cyber-en gedigitaliseerde criminaliteit in Nederland*. WODC. <https://repository.wodc.nl/handle/20.500.12832/253>

Bellemans, T., Peters-Scheffer, N., Didden, R., Traas, R., & van Busschbach, J. T. (2022). Psychomotor therapy for individuals with mild intellectual disabilities or borderline intellectual functioning presenting anger regulation problems and/or aggressive behaviour: A qualitative study on clients' experiences. *Journal of intellectual & developmental disability*, 47(1), 74-86.

Bekkers, L., Schiks, J., & Leukfeldt, E. R. (2020). Naar een interventie tegen geldezels. *Een pilot in de gemeente Haarlem*. Centre of Expertise Cybersecurity, Haagse Hogeschool, Den Haag.

Bluhm, K., Andriessen, M., van de Wal, M., Berkenpas, M., de Boer, D., Leukfeldt, R., Spithoven, R. & Jansen, J. (2024). Een eerste blik op het verloop en de werking van cyberweerbaarheidsprojecten in Nederland: Procevaluaties van CCV City Deal projecten Deelrapport 1: Tranche 1 en 2. *Procevaluatie city deal*. CCV. [2024-03-21-Procevaluaties-CCV-City-Deal-Projecten-Deelrapport-1-v1.0.pdf](https://www.ccv.nl/2024-03-21-Procevaluaties-CCV-City-Deal-Projecten-Deelrapport-1-v1.0.pdf)

Centraal Bureau voor de Statistiek. (2023, 10 mei). 2,2 miljoen Nederlanders slachtoffer online criminaliteit in 2022. *Centraal Bureau voor de Statistiek*. <https://www.cbs.nl/nl-nl/nieuws/2023/19/2-2-miljoen-nederlanders-slachtoffer-online-criminaliteit-in-2022>

Centraal Bureau voor de Statistiek. (2024, 10 mei). 2,2 miljoen Nederlanders slachtoffer online criminaliteit in 2022. *Centraal Bureau voor de Statistiek*.

CBS. (2023, 1 december). *ICT-gebruik bij personen - ICT, kennis en economie 2023*. ICT-gebruik bij personen - ICT, kennis en economie 2023 | CBS. <https://longreads.cbs.nl/ict-kennis-en-economie-2023/ict-gebruik-bij-personen/>

CBS (2022). Cybersecuritymonitor 2021. Geraadpleegd op 18 november 2022, via: <https://www.cbs.nl/nl-nl/longread/rapportages/2022/cybersecuritymonitor-2021>

Chiner, E., Gómez-Puerta, M., & Donohue, D. K. (2017). *Factors associated with access to inclusive education for children with disabilities in southern Europe: The case of Spain*. *British Journal of Learning*

Disabilities, 45(3), 175–181.

https://rua.ua.es/dspace/bitstream/10045/67868/4/2017_Chiner_etal_BritJLearnDisab_revised.pdf

Chadwick, D. D. (2019). Online risk for people with intellectual disabilities. *Tizard Learning Disability Review*, 24(4), 180–187. <https://doi.org/10.1108/tldr-03-2019-0008>

Chadwick, D. D. (2022). “You want to know that you’re safe”: Experiences of risk, restriction and resilience online among people with an intellectual disability. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 16(3). <https://doi.org/10.5817/cp2022-3-8>

Chadwick, D., Ågren, K. A., Caton, S., Chiner, E., Danker, J., Gómez-Puerta, M., Heitplatz, V., Johansson, S., Normand, C. L., Murphy, E., Plichta, P., Strnadová, I., & Wallén, E. F. (2022). Digital inclusion and participation of people with intellectual disabilities during COVID-19: A rapid review and international bricolage. *Journal of Policy and Practice in Intellectual Disabilities*, 19(3), 242–256. Portico. <https://doi.org/10.1111/jppi.12410>

Crick, N. R., & Dodge, K. A. (1994). A review and reformulation of social information-processing mechanisms in children's social adjustment. *Psychological bulletin*, 115(1), 74.

Cocking, D., & Van den Hoven, J. (2018). *Evil online*. John Wiley & Sons.

Currie, T. L., McKenzie, K., & Noone, S. (2019). The experiences of people with an intellectual disability of a mindfulness-based program. *Mindfulness*, 10, 1304-1314.

de Groot. (2021, 19 januari). Digital leven: Jongeren met LVB [PDF]. Kenniscentrum LVB.

<https://www.kenniscentrumlvb.nl/wp-content/uploads/2021/01/De-Groot-Digital-leven-jongeren-met-LVB-2101-01-19.pdf>

de Groot, V., Patel, S., Ter Stal, M., Vos, N., Van der Weegen, S., Buimer, H., & Van der Poel, A. (2022). Totstandkoming en toepassing van de ‘onderzoeksbbox’, als methode om ervaringen met technologie op te halen bij mensen met een licht verstandelijke beperking en niet-aangeboren hersenletsel, LVB Onderzoek & Praktijk Najaar, jaargang 20, nummer 2. <https://www.kenniscentrumlvb.nl/wp-content/uploads/2022/11/de-Groot-et-al-2022-LVB-OenP-jg-20-nr-2.pdf>

Dew, A., Llewellyn, G., & Gorman, J. (2006). “Having the time of my life”: An exploratory study of women with intellectual disability growing older. *Health Care for Women International*, 27(10), 908-929.

Digitale Inclusie: Iedereen moet kunnen meedoen. (2018). *Digitale Overheid*.

<https://www.digitaleoverheid.nl/nieuws/digitale-inclusie-iedereen-moet-kunnen-meedoen/>

Emerson, E. (2003). Prevalence of psychiatric disorders in children and adolescents with and without intellectual disability. *Journal of intellectual disability research*, 47(1), 51-58.

Embregts, P., Didden, R., Moonen, X., Leusink, G., & Schuengel, C. (2023). Kenmerken en ondersteuningsbehoeften van mensen met een licht of ernstig verstandelijke beperking en ernstig probleemgedrag en psychische problematiek. *NTz*, 49(3).

Elwyn, G., Laitner, S., Coulter, A., Walker, E., Watson, P., & Thomson, R. (2010). Implementing shared decision making in the NHS. *Bmj*, 341.

Elwyn, G., Frosch, D., Thomson, R., Joseph-Williams, N., Lloyd, A., Kinnersley, P., ... & Barry, M. (2012). Shared decision making: a model for clinical practice. *Journal of general internal medicine*, 27, 1361-1367.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of Persuasion in Social Engineering and Their Use in Phishing. In Lecture notes in computer science (pp. 36–47). https://doi.org/10.1007/978-3-319-20376-8_4

Fraudehulpdesk. (z.d.). *Fraudevormen en termen*. <https://www.fraudehulpdesk.nl/fraudevormen-en-termen/>

Hatton, C., & Emerson, E. (2004). The relationship between life events and psychopathology amongst children with intellectual disabilities. *Journal of Applied Research in Intellectual Disabilities*, 17(2), 109-117.

ter Harmsel, J. F. (2022). Be aware: biocueing as an addition to aggression regulation therapy in forensic psychiatric outpatients.

Herman, A. M., Critchley, H. D., & Duka, T. (2018). Risk-taking and impulsivity: the role of mood states and interoception. *Frontiers in psychology*, 9, 1625.

Jamieson, J. P., Harkins, S. G., & Williams, K. D. (2010). Need threat can motivate performance after ostracism. *Personality And Social Psychology Bulletin*, 36(5), 690–702.
<https://doi.org/10.1177/0146167209358882>

Jenaro, C. Flores, N., Frías, C. P. (2018) Systematic review of empirical studies on cyberbullying in adults: What we know and what we should investigate, *Aggression and Violent Behavior*, Volume 38, p.113-122, ISSN 1359-1789, <https://doi.org/10.1016/j.avb.2017.12.003>

Knotter, M. H. (2019). *The whole is more: A contextual perspective on attitudes and reactions of staff towards aggressive behaviour of clients with ID in residential institutions*.

Kim, H. G., Cheon, E. J., Bai, D. S., Lee, Y. H., & Koo, B. H. (2018). Stress and heart rate variability: a meta-analysis and review of the literature. *Psychiatry investigation*, 15(3), 235.

Landelijk Kenniscentrum LVB. (z.d.). *LVB & Risico's*. <https://www.kenniscentrumlvb.nl/themas/risicos-lvb/>

Marko, M., & Riečanský, I. (2018). Sympathetic arousal, but not disturbed executive functioning, mediates the impairment of cognitive flexibility under stress. *Cognition*, 174, 94-102.

Mccraty, R., & Atkinson, M. (2012). Resilience Training Program Reduces Physiological and Psychological Stress in Police Officers. *Global Advances in Health And Medicine*, 1(5), 44–66.
<https://doi.org/10.7453/gahmj.2012.1.5.013>

Mariën, I., Baelden, D., Bens, J., Schurmans, D., Van Audenhove, L., Smukste, K., Pierson, J., Lemal, M. and Goubin, E. (2013), “Van digitale naar maatschappelijke participatie: opportuniteiten en uitdagingen”, in Callens, M., Noppe, J. and Vanderleyden, L. (Eds) *De sociale staat van Vlaanderen 2013*, Studiedienst Vlaamse Regering, Brussel, pp. 227-272. <https://researchportal.vub.be/nl/publications/van-digitale-naar-maatschappelijke-participatie-opportuniteiten-e>

Misana-ter Huurne, E., Van Houten, Y., Spithoven, R., Notté, R., & Leukfeldt, R. (2020, februari). Cyberweerbaarheid: risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb-ers. Saxion.
https://www.researchgate.net/publication/340377007_Cyberweerbaarheid_Risicobewustzijn_en_zelfbeschermend_gedrag_rondom_cybercrime Onder_jongeren_en_mkb%27ers

Moonen, X. M. H. (2017). (H) erkennen en waarderen: Over het (h) erkennen van de noden mensen met licht verstandelijke beperkingen en het bieden van passende ondersteuning.

van Nieuwenhuijzen, M., Orobio de Castro, B., Wijnroks, L., Vermeer, A., & Matthys, W. (2004). The relations between intellectual disabilities, social information processing, and behaviour problems. *European Journal of Developmental Psychology*, 1(3), 215-229.

Normand, C. L., & Sallafranke-St-Louis, F. (2016). Cybervictimization of young people with an intellectual or developmental disability: Risks specific to sexual solicitation. *Journal of Applied Research in Intellectual Disabilities*, 29(2), 99-110. <https://doi.org/10.1111/jar.12163>

Nikken, P., Berns, J., & van Beekhoven, E. (2018). Mediawijsheid bij kinderen met een lvb: Een verkenning naar ervaringen in de praktijk. Utrecht: Nederlands Jeugdinstituut. <https://netwerkmediawijsheid.nl/wp-content/uploads/2018/11/Eindrapportage-theorie-en-praktijk-lvb-en-mediawijsheid.pdf>

Ogden, P., & Minton, K. (2000). Sensorimotor psychotherapy: One method for processing traumatic memory. *Traumatology*,

Lunsky, Y., & Benson, B. A. (2001). Association between perceived social support and strain, and positive and negative outcome for adults with mild intellectual disability. *Journal of Intellectual Disability Research*, 45(2), 106-114.

Pijpers, R. (2017). Mediawijsheid voor leerlingen met een licht verstandelijke beperking. Zoetermeer: Mijn kind online. Kennisnet. <https://netwerkmediawijsheid.nl/mediawijsheid-leerlingen-licht-verstandelijke-beperking/>

de Rijt, E. (2023). *Systematic review of psychomotor therapy targeting resilience in people with an intellectual disability: the difference between movement-oriented and body-oriented interventions*. Masterthesis, Windesheim university of applied sciences.

van Rest, M. M., Matthys, W., Van Nieuwenhuijzen, M., De Moor, M. H., Vriens, A., & Schuengel, C. (2019). Social information processing skills link executive functions to aggression in adolescents with mild to borderline intellectual disability. *Child Neuropsychology*, 25(5), 573-598.

Salahdine, F., & Kaabouch, N. (2019). *Social Engineering Attacks: a survey*. *Future Internet*, 11(4), 89. <https://doi.org/10.3390/fi11040089>

Schalock, R. L., Luckasson, R., & Tassé, M. J. (2021). *Intellectual disability: Definition, diagnosis, classification, and systems of supports* (12th ed.).

Scheffers, F., van Vugt, E., & Moonen, X. (2020). Resilience in the face of adversity in adults with an intellectual disability: A literature review. *Journal of Applied Research in Intellectual Disabilities*, 33(5), 828-838.

Schuengel, C., & Janssen, C. G. (2006). People with mental retardation and psychopathology: Stress, affect regulation and attachment: A review. *International review of research in mental retardation*, 32, 229-260.

Simon, L., Jiryis, T., & Admon, R. (2021). Now or later? Stress-induced increase and decrease in choice impulsivity are both associated with elevated affective and endocrine responses. *Brain sciences*, 11(9), 1148.

Siegel, D. J. (1999). *The developing mind: Toward a neurobiology of interpersonal experience*. Guilford Press.

Starke, M. (2013). Everyday Life of Young Adults With Intellectual Disabilities: Inclusionary and Exclusionary Processes Among Young Adults of Parents With Intellectual Disability. *Intellectual And Developmental Disabilities*, 51(3), 164–175. <https://doi.org/10.1352/1934-9556-51.3.164>

Steinmetz, K. F., Pimentel, A., & Goe, W. R. (2020). Decrypting social engineering: An analysis of conceptual ambiguity. *Critical Criminology*, 28, 631-650.

Spithoven, R. & van Tuijl, C. (2024). Cyberpesten. Theorie over en onderzoek naar de onbegrensde, digitale leefwereld van kinderen en adolescenten in Nederland. Boom. https://www.boom.nl/criminologie/100-17005_Cyberpesten

Spithoven, R. (2020). Verbonden Risico's: Maatschappelijke veiligheid in de black box society. Boom. https://www.boom.nl/criminologie/100-12520_Verbonden-risico-s

Suijkerbuijk, S., Hofman, C., & Engels J. (2016). Durf te experimenteren Past je manier van onderzoeken bij de mensen die je onderzoekt? Kwaliteit in zorg, 2016, nummer 5. https://www.overkwaliteitvanzorg.nl/wp-content/uploads/2017/12/012-015_KIZ05_THE-6_Suijkerbuijk.pdf

Thayer, J. F., & Lane, R. D. (2009). Claude Bernard and the heart–brain connection: Further elaboration of a model of neurovisceral integration. *Neuroscience & Biobehavioral*

Vega, V., Cruz, M., Pérez, Ma. C., & Torres, V. A. (2018). Cyberbullying among adults with intellectual disabilities: Some preliminary data. *Research in Developmental Disabilities*, 72, 265–274. <https://doi.org/10.1016/j.ridd.2017.12.006>

Van den Broeck, A., Ferris, D. L., Chang, C. H., & Rosen, C. C. (2016). A review of self-determination theory's basic psychological needs at work. *Journal of management*, 42(5), 1195-1229.

Weinstein, N. D. (1989). Effects of personal experience on self-protective behavior. *Psychological Bulletin*, 105(1), 31–50. <https://pubmed.ncbi.nlm.nih.gov/2648439/>

de Wit, M., Moonen, X., & Douma, J. (2023). Richtlijn Effectieve interventies LVB: Aanbevelingen voor het aanpassen, uitvoeren en ontwikkelen van gedragsveranderende interventies voor personen met een licht verstandelijke beperking. Landelijk kenniscentrum LVB.

Wiltschut, H. (2020). Niet alleen gevaarlijk. LVB en de digitale wereld. Sozio 3. Amsterdam: Uitgeverij SWP BV. <https://www.sociaaldigitaal.nl/p/lvb-en-de-digitale-wereld/4662>

Titel Digitaal Meedoen: LVB Cyberweerbaar!

Pagina 62 / 94

Wissink, I., & Quint, R. (2021). 'If it's too good to be true, it's too good to be true': Een verkenning van de literatuur over de kenmerken van jonge geldezels.

Zorginstituut Nederland (2022). Mensen met een licht verstandelijke beperking gebaat bij meer tijd en aandacht van de huisarts. Geraadpleegd op 4 november 2022, via:

<https://www.zorginstituutnederland.nl/actueel/nieuws/2022/02/23/mensen-met-een-lichte-verstandelijke-beperking-gebaat-bij-meer-tijd-en-aandacht-van-de-huisarts>

BIJLAGE 2 - Vragenlijst

Hartelijk dank dat u deze vragenlijst wilt invullen!

Deze vragenlijst bestaat uit twee delen.

Het eerste deel gaat in op uw kennis over en vaardigheden ten aanzien van online veilig gedrag van u **als begeleider van deelnemer(s) van De Klup**.

Het tweede deel gaat over uw inschatting van de vaardigheden **van deelnemer(s) van De Klup** die u begeleid, ten aanzien van online veilig gedrag én hoe zij hierin geholpen kunnen worden. Met **deelnemer(s)** wordt bedoeld: de mensen die u begeleidt in uw (vrijwilligers)werk bij De Klup.

Het invullen van deze vragenlijst duurt ongeveer 15 minuten.

Het is belangrijk om te weten dat er **geen goede of fouten antwoorden** zijn in deze vragenlijst: we zijn op zoek naar uw ervaring over online veilig gedrag, waaronder in het contact met de deelnemer(s).

Deelname aan deze vragenlijst is volledig anoniem; er wordt nergens gevraagd uw naam op te geven en we kunnen uw antwoorden op geen enkele wijze herleiden naar u als persoon.

Gaat u hiermee akkoord en wilt u de vragenlijst invullen?

- Ja, gelezen en akkoord (1)
- Nee, gelezen maar niet akkoord (2)

Skip To: End of Survey If Hartelijk dank dat u deze vragenlijst wilt invullen! Deze vragenlijst bestaat uit twee delen. Het... = Nee, gelezen maar niet akkoord

End of Block: Blok 1

Start of Block: Blok 2

Display This Question:

If Hartelijk dank dat u deze vragenlijst wilt invullen! Deze vragenlijst bestaat uit twee delen. Het... = Ja, gelezen en akkoord

Deel 1: ervaringen online veilig gedrag begeleiders

De volgende vragen hebben betrekking op uw eigen kennis en vaardigheden op het gebied van online veilig gedrag.

End of Block: Blok 2

Start of Block: DEEL 1: Ervaringen cyberweerbaarheid begeleiders

Q3 Hoe vaak maakt u gemiddeld gebruik van internet?

- (Bijna) nooit (1)
- Maandelijks (2)
- Wekelijks (3)
- Dagelijks (4)
- Meerdere keren per dag (8)

- Weet ik niet (6)

Q4 Wat heeft u in de afgelopen 12 maanden regelmatig online gedaan? Selecteer uit de volgende lijst (meerdere antwoorden mogelijk)

- Versturen/ontvangen e-mails (1)
- Bellen via internet (2)
- Sociale media checken (zoals Instagram, Telegram, Facebook en Snapchat) (3)
- Whatsapp of andere apps om te chatten (4)
- Nieuwsberichten, kranten of nieuwsbladen lezen (5)
- Videobellen via internet (16)
- Informatie zoeken over producten (6)
- Televisie kijken (7)
- Video's of filmpjes kijken (8)
- Legaal video's of muziek downloaden (14)
- Illegaal video's of muziek downloaden (13)
- Muziek luisteren (15)
- Gamers: spelletjes spelen of downloaden (9)
- Internetbankieren of mobiel bankieren (10)
- Producten of diensten kopen en/of verkopen (11)
- Anders, namelijk... (12) _____

End of Block: DEEL 1: Ervaringen cyberweerbaarheid begeleiders

Start of Block: 2DEEL 1: Ervaringen cyberweerbaarheid begeleiders

Q5 **Online criminaliteit** betreft alle vormen van criminaliteit die via het internet worden gepleegd. Dit zijn bijvoorbeeld verschillende vormen van oplichting en fraude, maar ook wanneer u een virus krijgt, uw inloggegevens gestolen worden, of uw apparaat gehackt wordt.

Q6 In hoeverre maakt u zich zorgen over...

	Heel weinig zorgen 1 (1)	Weinig zorgen 2 (2)	Niet weinig / niet veel zorgen 3 (3)	Veel zorgen 4 (4)	Heel veel zorgen 5 (5)
...de KANS dat u slachtoffer wordt van online criminaliteit? (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...de mogelijkheid dat u SCHADE oploopt door slachtofferschap van online criminaliteit? (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Page Break

Q7 Hoe groot schat u de kans om de komende 12 maanden zelf het slachtoffer te worden van online criminaliteit?

	Hele kleine kans (1)	Kleine kans (2)	Geen kleine/geen grote kans (3)	Grote kans (4)	Hele grote kans (5)
1 (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Page Break

End of Block: 2DEEL 1: Ervaringen cyberweerbaarheid begeleiders

Start of Block: 4DEEL 1: Ervaringen cyberweerbaarheid begeleiders

Q8 Bent u in de afgelopen 12 maanden zelf in aanraking gekomen met een vorm van online criminaliteit?

- Ja (1)
- Nee (2)
- Weet ik niet (zeker) (3)

Page Break

End of Block: 4DEEL 1: Ervaringen cyberweerbaarheid begeleiders

Start of Block: Block 15

Display This Question:

If Bent u in de afgelopen 12 maanden zelf in aanraking gekomen met een vorm van online criminaliteit? = Ja

Or Bent u in de afgelopen 12 maanden zelf in aanraking gekomen met een vorm van online criminaliteit? = Weet ik niet (zeker)

Q10 Van welke vorm van online criminaliteit bent u in de afgelopen 12 maanden (vermoedelijk) het **slachtoffer** geworden? **(meerdere antwoorden mogelijk).**

- Ik had een virus of andere malware (1)
- Iemand heeft ingebroken in een apparaat van mij (hacking) (3)
- Mijn foto's/bestanden zijn ongewenst verspreid (17)
- Ik ben opgelicht bij een aankoop/verkoop (4)
- Ik ben opgelicht bij een belegging (5)
- Ik ben opgelicht door een date die ik heb ontmoet via het internet (7)
- Mijn persoonsgegevens (identiteit) zijn gestolen/misbruikt (6)
- Ik heb geld overgemaakt naar aanleiding van een whatsappbericht van iemand die zich voordeed als een vriend/familie (8)
- Ik heb op een link geklikt die niet in orde bleek (11)
- Ik heb een phishing mail ontvangen (maar ben hier niet op ingegaan) (20)
- Ik ben online afgeperst/gechanteerd (12)
- Ik ben online gepest (13)
- Ik ben online gestalkt (14)
- Ik ben online gediscrimineerd (15)
- Ik ben online bedreigd (16)
- Anders, namelijk (19) _____

Page Break

End of Block: Block 15

Start of Block: 5DEEL 1: Ervaringen online veilig gedrag begeleider

Q11 Kruis a.u.b. aan wat u momenteel al doet om uzelf tegen online criminaliteit te beschermen.

Meerdere antwoorden zijn mogelijk.

- Ik installeer updates zodra deze beschikbaar zijn (1)
- Ik let op of er sprake is van een beveiligde verbinding (HTTPS of het "slotje" in de adresbalk) tijdens het internetten of online betalingen (2)
- Ik gebruik sterke wachtwoorden met meerdere cijfers en tekens (3)
- Ik download alleen films, muziek en/of games op legale wijze (4)
- Ik stel mijn apparaten, apps en sociale media-accounts altijd zo in, dat ik zo min mogelijk persoonlijke gegevens blootgeef (5)
- Ik gebruik een virusscanner (6)
- Ik houd mijn inloggegevens voor mijzelf (7)
- Ik klik niet op links en open geen bijlagen van e-mails die ik niet vertrouw (8)
- Ik gebruik dubbele verificatie op mijn accounts (9)
- Ik gebruik een vergrendelingscode of wachtwoord op al mijn apparaten (10)
- Ik gebruik voor ieder account een ander wachtwoord (11)
- Ik maak back-ups (reservekopie) van mijn waardevolle bestanden (12)
- Ik vermijd het gebruik van openbare wifi (13)
- Als ik een website niet vertrouw, vermijd ik die of verlaat ik deze onmiddellijk (14)
- Ik versleutel belangrijke/vertrouwelijke bestanden met een wachtwoord of andere beveiliging (15)
- Als een onbekende online contact met mij zoekt, en ik vertrouw het niet helemaal, google ik die persoon of zoek ik hem op op sociale media (16)
- Als een advertentie te mooi is om waar te zijn ga ik er niet op in (17)
- Ik neem de telefoon niet op als ik het nummer niet ken (19)
- Anders, namelijk..... (18) _____
- Geen van bovengenoemde zaken gebruik ik om mijzelf te beschermen tegen online criminaliteit (20)

Page Break

Q12 In hoeverre bent u het eens met de volgende stellingen?

	Helemaal mee oneens 1 (1)	Enigszins mee oneens 2 (2)	Niet mee oneens / niet mee eens 3 (3)	Enigszins mee eens 4 (4)	Helemaal mee eens 5 (5)
Ik weet hoe daders van online criminaliteit te werk gaan. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ik ben in staat om in te schatten welke risico's ik loop om slachtoffer te worden van online criminaliteit. (8)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Ik ben in staat mijzelf te beschermen tegen online criminaliteit. (9)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Als ik voorbereidende maatregel tref, verkleint dat mijn kans om slachtoffer te worden van online criminaliteit. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
De door mij genomen maatregelen zorgen ervoor dat ik minder kans heb om slachtoffer te worden van online criminaliteit. (6)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ik ben in staat juist te handelen wanneer ik slachtoffer ben of denk te zijn van online criminaliteit. (10)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mensen in mijn omgeving verwachten dat ik mijzelf bescherm tegen online criminaliteit. (7)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

End of Block: 5DEEL 1: Ervaringen online veilig gedrag begeleiders

Start of Block: Block 15

Q13 Komt u tijdens uw (vrijwilligers)werk bij De Klup in aanraking met deelnemer(s) met een licht verstandelijke beperking (LVB)?

- Ja (1)
- Nee (2)

Display This Question:

If Komt u tijdens uw (vrijwilligers)werk bij De Klup in aanraking met deelnemer(s) met een licht ver... = Nee

Q14 Met welke doelgroep komt u bij De Klup wel in aanraking?

- Senioren (2)
- Kinderen (4)
- Beginnend dementerende (5)
- Mensen met niet aangeboren hersenletsel (6)
- Mensen met een (chronisch) fysieke beperking (7)

Titel Digitaal Meedoen: LVB Cyberweerbaar!
Pagina 68 / 94

- Anders, namelijk (3) _____

End of Block: Block 15

Start of Block: Blok 14

Q15 Deel 2: inschatting over online veilig gedrag van deelnemer(s) bij De Klup

De volgende vragen hebben betrekking op uw inschatting van de vaardigheden van deelnemer(s) bij De Klup waarmee u contact heeft ten aanzien van hun online veilig gedrag.

End of Block: Blok 14

Start of Block: 1DEEL 2: Inschatting over cyberweerbaarheid van deelnemers

Q16 Hoe vaak (schat u) dat de deelnemer(s) van De Klup waarmee u contact heeft gemiddeld gebruik maken van internet?

- (Bijna) nooit (1)
- Maandelijks (2)
- Wekelijks (3)
- Dagelijks (4)
- Meerdere keren per dag (5)
- Weet ik niet (6)

Page Break

Q17 Wat doen de meeste van de deelnemer(s) van De Klup waarmee u contact heeft volgens u regelmatig online? Selecteer uit de volgende lijst (**meerdere antwoorden zijn mogelijk**)

- Versturen/ontvangen e-mails (1)
- Bellen via internet (2)
- Sociale media (zoals Instagram, Telegram, Facebook en Snapchat) (3)
- Whatsapp of andere apps om te chatten (4)
- Nieuwsberichten, kranten of nieuwsbladen lezen (5)
- Videobellen via internet (16)
- Informatie zoeken over producten (6)
- Televisie kijken (7)
- Video's of filmpjes kijken (8)
- Legaal video's of muziek downloaden (14)
- Illegaal video's of muziek downloaden (13)
- Muziek luisteren (15)
- Gamen: spelletjes spelen of downloaden (9)
- Internetbankieren of mobiel bankieren (10)
- Producten of diensten kopen en/of verkopen (11)
- Anders, namelijk... (12) _____

Page Break

Q18 In hoeverre maakt u zich zorgen over...

	Heel weinig zorgen 1 (1)	Weinig zorgen 2 (2)	Niet weinig / niet veel zorgen 3 (3)	Veel zorgen 4 (4)	Heel veel zorgen 5 (5)
...de KANS dat de deelnemer(s) waarmee u contact heeft slachtoffer wordt van online criminaliteit? (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...de mogelijkheid dat de deelnemer(s) waarmee u contact heeft SCHADE oploopt door slachtofferschap van online criminaliteit? (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

End of Block: 1DEEL 2: Inschatting over cyberweerbaarheid van deelnemers

Start of Block: 2DEEL 2: Inschatting over cyberweerbaarheid van deelnemers

Q19 Hoe groot schat u de kans dat deelnemer(s) van De Klup waarmee u contact heeft de komende 12 maanden in aanraking komen met een vorm van online criminaliteit?

- Hele kleine kans (1)
- Kleine kans (2)
- Geen kleine/geen grote kans (3)
- Grote kans (4)
- Hele grote kans (5)

Q20 Hieronder kunt u uw antwoord eventueel toelichten:

Page Break



Q21 Als u zou inschatten met welke vormen van online criminaliteit de deelnemer(s) van De Klup het meeste risico lopen om de komende 12 maanden mee in aanraking mee te komen, welke vormen zouden dat zijn? Selecteer a.u.b. **drie** uit de onderstaande lijst.

- Het krijgen van een virus of andere malware (1)
- Iemand die inbreekt op een apparaat of account van de deelnemer (hacking) (3)
- Foto's/bestanden die ongewenst worden verspreid (4)

- Oplichting bij aankoop/verkoop (5)
- Oplichting bij een belegging (6)
- Oplichting door daten (7)
- Persoonsgegevens (identiteit) die wordt gestolen/misbruikt (8)
- Geld overmaken naar aanleiding van een whatsapp bericht van iemand die zich voordoeft als vriend/familie (11)
- Op een link klikken die niet in orde blijkt (12)
- Bankpas en pincode uitlenen in ruil voor geld of een cadeau (19)
- Online afpersing/chantage (13)
- Online pesten (14)
- Online stalking (15)
- Online discriminatie (16)
- Online bedreiging (17)
- Anders, namelijk: (21) _____

End of Block: 2DEEL 2: Inschatting over cyberweerbaarheid van deelnemers

Start of Block: Blok 8

Q23 Zijn één of meerdere van de deelnemer(s) van De Klup waarmee u contact heeft de afgelopen 12 maanden het slachtoffer geworden van een vorm van online criminaliteit?

- Ja (1)
- Nee (2)
- Weet ik niet (zeker) (3)

Page Break

Display This Question:

If Zijn één of meerdere van de deelnemer(s) van De Klup waarmee u contact heeft de afgelopen 12 maanden... = Ja

Or Zijn één of meerdere van de deelnemer(s) van De Klup waarmee u contact heeft de afgelopen 12 maanden... = Weet ik niet (zeker)

Q24 Van welke vorm(en) van online criminaliteit is/zijn deelnemer(s) de afgelopen 12 maanden het slachtoffer geworden?

(meerdere antwoorden zijn mogelijk).

- Deelnemer had een virus of andere malware (1)
- Iemand heeft ingebroken in een apparaat van deelnemer (hacking) (3)
- Foto's/bestanden van deelnemer zijn ongewenst verspreid (4)
- Deelnemer is opgelicht bij een aankoop/verkoop (5)
- Deelnemer is opgelicht bij een belegging (6)
- Deelnemer is opgelicht tijdens het daten (8)
- Deelnemer zijn of haar persoonsgegevens (identiteit) zijn gestolen/misbruikt (7)
- Deelnemer heeft geld overgemaakt naar aanleiding van een whatsapp bericht van iemand die zich voordeed als vriend/familie (11)
- Deelnemer heeft op een link geklikt die niet in orde bleek (12)
- De deelnemer heeft een phishing mail ontvangen (maar is hier niet op ingegaan) (21)
- Deelnemer heeft bankpas en pincode uitgeleend in ruil voor geld of een cadeau (19)
- Deelnemer is online afgeperst/gechanteerd (13)

Titel Digitaal Meedoen: LVB Cyberweerbaar!
Pagina 71 / 94

- Deelnemer is online gepest (14)
- Deelnemer is online gestalkt (15)
- Deelnemer is online gediscrimineerd (16)
- Deelnemer is online bedreigd (17)
- Anders, namelijk: (20) _____

Display This Question:

If Zijn één of meerdere van de deelnemer(s) van De Klup waarmee u contact heeft de afgelopen 12 maanden... = Ja

Or Zijn één of meerdere van de deelnemer(s) van De Klup waarmee u contact heeft de afgelopen 12 maanden... = Weet ik niet (zeker)

Q25 Zou u hieronder kunnen omschrijven wat er precies gebeurd is?

Q28 Stellen deelnemer(s) van De Klup u wel eens vragen die te maken hebben met veilig gedrag op het internet?

- Nee (4)
- Ja, namelijk (5) _____



Q47 Wat hebben deelnemer(s) van De Klup volgens u nodig om te voorkomen dat zij slachtoffer worden van online criminaliteit? **Meerdere antwoorden zijn mogelijk**

- Kennis over hoe criminelen online te werk gaan (1)
- Kennis over hoe de deelnemer criminele risico's kan herkennen (4)
- Kennis over hoe de deelnemer(s) moet reageren wanneer diegene in aanraking komt met online gevaren (6)
- Kennis over contactpunten om hulp te vragen (7)
- Experts binnen De Klup die kunnen helpen met het voorkomen van online risico's/gevaren (bv. virusscanner installeren) (8)
- Contactpunt voor vragen over veilig online gedrag (bv. het wel/niet openen van een bericht/link) (14)
- Cursussen om digitaal vaardiger/weerbaarder te worden (12)
- Begeleiding omtrent praktische vragen (bv. online bankzaken) (13)
- Technische beschermingen tegen online criminaliteit (2)
- Ervaringsdeskundigen die kunnen vertellen over de risico's van de online gevaren (3)
- Anders, namelijk (9) _____
- Ze hebben niets nodig (10)

End of Block: Blok 8

Start of Block: Blok 12

Q30 Hartelijk dank voor het invullen van deze vragenlijst.

Mocht u naar aanleiding van deze vragenlijst nog vragen of opmerkingen hebben, dan kunt u deze hieronder invullen.

Ook kunt u desgewenst contact opnemen met de onderzoekers van Saxion: Nick van der Klok (n.vanderklok@saxion.nl) en Julia Klopman (j.klopman@saxion.nl).

Titel Digitaal Meedoen: LVB Cyberweerbaar!
Pagina 72 / 94

Q31 Heeft u naar aanleiding van deze vragenlijst nog vragen of opmerkingen?

- Ja (1)
- Nee (2)

Display This Question:

If Heeft u naar aanleiding van deze vragenlijst nog vragen of opmerkingen? = Ja

Q32 Laat ons hier uw vragen of opmerkingen weten:

End of Block: Blok 12

BIJLAGE 3 - Goedkeuring Saxion Ethische Advies Commissie (SEAC)



Aan Nick van der Kolk
Lectoraat Maatschappelijke Veiligheid

Saxion
Postbus 70.000
7500 KB Enschede
M.H. Tromplaan 28
7513 AB Enschede
www.saxion.nl

Referentie SEAC-24-03
Datum 14 februari 2024
Pagina 1 / 1
Onderwerp Advies Saxion Ethische Adviescommissie

Saxion Ethische Advies Commissie
seac@saxion.nl

Geachte heer Van der Kolk, beste Nick,

Op 7 februari 2024 ontving de Saxion Ethische Adviescommissie (hierna: SEAC) jouw verzoek voor advies over jullie onderzoek. Samen met onderzoekers streeft onze commissie naar een goede onderbouwing en borging van diverse ethische dilemma's waarmee jullie binnen jullie onderzoeksopzet en onderzoekuitvoering te maken kunnen krijgen.

In haar vergadering op 13 februari 2024 heeft de SEAC het verzoek besproken om te adviseren over het onderzoek "Stichting Achmea Slachtoffer en Samenleving". In dit onderzoek willen jullie met behulp van een vragenlijst de digitale weerbaarheid van begeleiders en vrijwilligers (en indirect mensen met een licht verstandelijke beperking) onderzoeken.

De bespiegeling heeft op de diverse ijkpunten (denk bv. aan: meldingsplichtigheid Medisch Ethische Toetsingscommissie, opdrachtgeverschap en onderzoeksdoel, methodiek, borging privacy onderzoeksgroep en wijze van dataverzameling, dataopslag en databeheer) plaatsgevonden.

Vanuit de bespreking kwam een paar kleine punten naar voren die jullie nog mee kunnen nemen bij de voorbereiding van het onderzoek:

1. Wij kunnen ons voorstellen dat door deelname aan het onderzoek respondenten vragen hebben over een casus die zij zelf hebben meegemaakt. In de vragenlijst staan de contactgegevens van de hoofdonderzoeker. Kunnen respondenten ook bij de onderzoekers terecht voor inhoudelijke vragen/nazorg en/of hebben jullie daar afspraken met De Klup over gemaakt?
2. De vragenlijst kan anoniem worden ingevuld. Echter bij Q20 wordt gevraagd naar een casus van online criminaliteit. Hoe waarborgen jullie ook hier de anonimiteit van de respondenten danwel de doelgroep waar vragen over worden gesteld?
3. De vragenlijst lijkt relatief lang: hebben jullie de vragenlijst getest met de doelgroep en wat zijn hun ervaringen? Of anders, hoe introduceren jullie de vragenlijst zodat de kans op volledige data en een hoge respons worden vergroot?

De commissie concludeert dat zij in de aangeleverde documenten zoals deze aan haar is voorgelegd op dit moment geen bezwaren ziet voor wat betreft uitvoering van het onderzoek. Met het voorleggen van het onderzoeksvoorstel aan onze commissie voldoe je aan de toets die je moet hebben gedaan om in de toekomst te kunnen publiceren over dit onderzoek.

De commissie wenst je bij de uitvoering van het onderzoek, met inachtneming van het hiervoor verstrekte advies, veel succes toe.

Met vriendelijke groet, namens de SEAC,

Dr. Marjolein den Ouden, voorzitter SEAC

BIJLAGE 4 – Instructie-handleiding begeleiders

Instructies voor begeleiders

Aanvullende doe-activiteit bij het geldezel-spel

Doel van de activiteit

Deze oefening is gericht op het versterken van de houding en vaardigheden van mensen met een licht verstandelijke beperking, specifiek gericht op het reguleren van hun gedrag, het stellen van grenzen en het "nee" zeggen. We focussen hierbij op het voorkomen van het ingezet worden als geldezel. Concreet betekent dit dat we hen leren hun pinpas en pincode te beschermen door te oefenen met duidelijke grenzen.

Vorbereiding

Leg aan de deelnemers uit dat we gaan oefenen met het aangeven dat zij hun pinpas en pincode nooit mogen uitlenen of delen. Zorg voor een rustige, veilige omgeving waar deelnemers zich op hun gemak voelen om te oefenen. Deze oefening is geschikt voor maximaal twee deelnemers tegelijkertijd.

Stap 1, hardop lezen van de zinnen

Lees samen met de deelnemers de zinnen hardop voor. Dit helpt hen de belangrijke boodschap in te prenten en geeft hun een gevoel van zekerheid in het gebruiken van deze zinnen.

1. Begin met de eerste set zinnen, die duidelijk maken dat ze hun pinpas niet uitlenen:
 - "Ik leen mijn pinpas niet uit."
 - "Ik geef mijn pinpas aan niemand."
 - "Mijn pinpas is van mij."
 - "Jij krijgt mijn pinpas niet."
 - "Ik deel mijn pinpas nooit."
2. Lees daarna de zinnen die aangeven dat ze hun pincode niet delen:
 - "Mijn code is geheim."
 - "Mijn code deel ik met niemand."
 - "Jij krijgt mijn code niet."
 - "Ik deel mijn code niet."
 - "Ik geef mijn code aan niemand."

Geef elke deelnemer de kans om de zinnen zelf hardop te lezen. (Deze kan ook worden voorgelezen en worden herhaald wanneer de deelnemer niet in staat is om te lezen.) De gelezen zin wordt dan 3x nog een keer hardop herhaald.

Stimuleer hen om dit met overtuiging te doen. Ondersteun waar nodig en complimenteer zelfs als de deelnemers wat onzeker zijn.

Stap 2, oefenen met het weigeren van de pinpas afgeven

Laat de deelnemers in duo's samenwerken. **Persoon A** speelt de rol van degene die vraagt om de pinpas. **Persoon B** oefent met het duidelijk aangeven dat ze hun pinpas niet mogen uitlenen. Gebruik de zinnen die in de vorige opdracht zijn geoefend.

Persoon A vraagt 10 keer op verschillende manieren om de pinpas, bijvoorbeeld met een andere intonatie of door de vraag op een andere manier te stellen.

Persoon B geeft elke keer duidelijk en zelfverzekerd antwoord, met behulp van de zinnen die bij stap 1 zijn besproken. Moedig de deelnemers aan om verschillende zinnen te gebruiken en hun eigen grenzen op een rustige, maar vastberaden manier te bewaken.

Na 10 keer draaien de rollen om. Nu speelt **persoon B** de rol van degene die om de pinpas vraagt, en **persoon A** oefent met het aangeven dat ze hun pinpas niet uitlenen. Ook hier wordt weer 10 keer geoefend, waarbij beide deelnemers de kans krijgen om zowel het vragen als het weigeren te oefenen.

Stap 3, oefenen met het weigeren van delen van de pincode

Laat opnieuw de deelnemers in duo's samenwerken. **Persoon A** vraagt dit keer om de pincode. **Persoon B** oefent met het duidelijk aangeven dat ze hun code niet delen. Gebruik de zinnen die in opdracht 1 zijn geoefend.

Persoon A vraagt 10 keer op verschillende manieren om de code, bijvoorbeeld door te smeken, te dwingen of de vraag op een andere manier te stellen.

Persoon B geeft elke keer zelfverzekerd antwoord, met behulp van de zinnen die aangeven dat ze hun code niet delen. Ook hier is variatie in de zinnen belangrijk, zodat de deelnemer meerdere manieren leert om "nee" te zeggen.

Na 10 keer draaien de rollen om. **Persoon B** vraagt nu om de code en **persoon A** oefent met het weigeren van het delen van de code. Ook hier herhalen ze de oefening 10 keer.

Stap 4, intermezzo ademhalingsoefening

Het doel van deze intermezzo is om de deelnemers een ademhalingstechniek te leren om stress te verminderen en kalmte te bevorderen zodat ze in moeilijke, lastige of spannende situaties het juiste doen.

Leg aan de deelnemers uit dat we even een pauze nemen om ons te richten op onze ademhaling. Vertel hen dat een rustige ademhaling helpt om kalm te blijven en het juiste te doen in spannende situaties, zoals wanneer iemand vraagt om hun pinpas of code.

Box Breathing (Ademen in een vierkant):

Uitleg van de techniek: je ademhaling wordt in vier stukken gehakt, net als de zijden van een vierkant. Je ademt in langs de linkerkant (4 sec), houdt je adem vast langs de bovenkant (4 sec), ademt uit langs de rechterkant (4 sec), en houdt je adem vast langs de onderkant (4 sec).

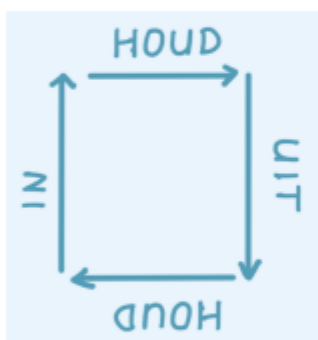
Hulp voor uitleg aan de deelnemer:

Uitleg:

Uitleg: We gaan *de vierkante ademhaling* toepassen. Dit is een techniek van ademen. Je adem splits je op in 4 delen.

- 4) Je ademt 4 tellen in langs je neus.
- 4) Je houdt je adem 4 tellen vast.
- 4) Je ademt 4 tellen uit langs je mond.
- 4) Je houdt je adem 4 tellen vast.

Dit herhaal je dan vijf keer tot je rustiger wordt.



Waarom deze oefening?

Deze oefening helpt goed en snel om te ontspannen. Als je traag ademt, gaat je hart ook langzamer kloppen. Dan wordt je lichaam kalm. En kan je dan ook beter nadenken. Je zal dan bij spannende gebeurtenissen sneller juist beslissingen

Stap voor stap ontspannen via box breathing:

Open de applicatie voor visuele ondersteuning bij de oefening:

1. Zorg dat iedereen rechtop zit: voeten plat op de grond, rug recht (niet tegen de leuning).
2. Adem 4 tellen rustig in door je neus (volg de linkerkant van het vierkant).
3. Houd je adem 4 tellen vast (volg de bovenkant van het vierkant).
4. Adem 4 tellen uit door je neus (volg de rechterkant van het vierkant).

5. Houd je adem 4 tellen vast (volg de onderkant van het vierkant).
6. Herhaal dit 10 keer en laat de deelnemers rustig voelen wat er in hun lichaam verandert. Wat merkt de deelnemer op in zijn of haar lichaam?

Stap 5, oefenen in dialoog, nee zeggen tegen het uitlenen van de pinpas

Deelnemers oefenen in een dialoog om "nee" te zeggen tegen het uitwisselen van hun pinpas.

- De begeleider speelt de rol van iemand die om de pinpas vraagt, door bijvoorbeeld een pet op te zetten.
- De deelnemer oefent met het aangeven dat ze hun pinpas niet uitwisselen, gebruikmakend van de zinnen die eerder zijn geoefend.

Geef complimenten elke keer als de deelnemer hun pinpas niet geeft. Als de deelnemer in de fout gaat, lees dan samen nog een keer de juiste reactie en oefen deze opnieuw.

Stap 6, oefenen in dialoog alleen dan meer druk uitoefenen

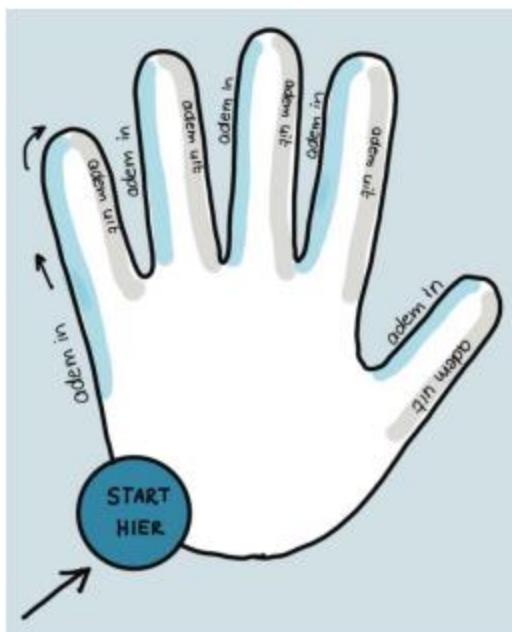
Deelnemers oefenen om "nee" te zeggen wanneer er meer druk wordt uitgeoefend, bijvoorbeeld door te zeuren. De begeleider vraagt opnieuw om de pinpas, maar dit keer met meer nadruk, zoals: "Asjeblijft, alsjeblijft, ik heb hem echt nodig!" De deelnemer oefent weer met het aangeven dat ze hun pinpas niet uitwisselen.

Complimenteer de deelnemer als ze hun grenzen bewaken, ook al wordt er meer druk uitgeoefend. Gaat een deelnemer toch in de fout, lees samen de juiste reactie door en oefen opnieuw.

Stap 7, intermezzo, ademhalingsoefening

Het doel is dat deelnemers een tweede ademhalingsstechniek leren om rustig te worden, zodat ze in stressvolle situaties beter kunnen handelen. Hoe meer manieren inge oefend worden, hoe beter deze ook toegepast kunnen worden. Op deze manier kan ook nagegaan worden welke oefening het best past bij een deelnemer.

Leg aan de deelnemer uit dat dit een techniek is waarbij je **rustig** met je vinger langs je hand heen beweegt. Wanneer je met je vinger omhoog beweegt (richting de vingertop), adem je in. Bij de beweging naar beneden adem je uit. Als je bij de duim bent aangekomen, begin je weer opnieuw bij je pink.



Stap voor stap: vijf-vinger-ademhaling

- Sluit je ogen en zet de wijsvinger van je ene hand aan de basis van de pink van je andere hand.
- Beweeg met je wijsvinger langzaam omhoog richting topje van je pink terwijl je rustig inademt door je neus.
- Als je bij het topje bent, beweeg je je wijsvinger weer naar beneden terwijl je rustig uitademt door je mond.
- Ga door met je ringvinger: beweeg je wijsvinger omhoog tot het topje en adem in door je neus.
- Als je bij het topje bent, beweeg je wijsvinger weer naar beneden terwijl je rustig uitademt door je mond.
- Als je alle vingers hebt gehad, begin je weer bij je pink.

Adem dus tijdens deze oefening in terwijl je met je vinger langs je hand en vingers omhoog beweegt, en adem uit terwijl je met je vinger omlaag beweegt. Herhaal dit 10 keer en merk op hoe je je voelt.

Stap 8 Oefenen met meer emotionele druk

Deelnemers oefenen weer om nee te zeggen. Alleen deze keer doen ze dat wanneer er emotionele druk wordt uitgeoefend, zoals iemand die smeekt om de pinpas. Denk bijvoorbeeld aan zinnen zoals:

- "Ik moet snel nog een cadeautje kopen voor mijn zus, anders is ze teleurgesteld. Please, help me!"

- "Ik moet een kaartje kopen voor de bus, anders ben ik te laat thuis. Je bent toch mijn broer dan kan je mij toch even snel helpen anders kom ik niet thuis!"
- "Alsjeblieft, het duurt maar heel kort, ik moet snel even betalen. Ik beloof dat ik hem meteen teruggeef, ik help jou toch ook altijd?!"
- "Als ik je pinpas even mag lenen dan ben ik echt heel erg blij! Dan krijg jij van mij als beloning 50 euro!"
- "Je ouders (naam ouders) zeiden tegen mij dat ik wel even jouw pinpas kon lenen om boodschappen te doen, ik ben hem vergeten en moet nu eten halen!"

Complimenteer de deelnemer als ze hun grenzen bewaken, ook al wordt er meer druk uitgeoefend. Gaat een deelnemer toch in de fout, lees samen de juiste reactie door en oefen opnieuw.

Stap 9, intermezzo ademhalingsoefening

Het doel is dat de deelnemers leren om hun aandacht te kunnen controleren en richten op de ademhaling door hun hand op hun buik te leggen. Deze oefening is weer een andere manier om jezelf tot rust te brengen. Hoe meer manieren ingeoeft worden, hoe beter deze ook toegepast kunnen worden. Op deze manier kan ook nagegaan worden welke oefening het best past bij een deelnemer.

Stap voor stap:

1. Ga rustig zitten en leg je hand op je buik.
2. Adem 4 tellen in, voel dat je buik je hand wegduwt.
3. Adem 4 tellen uit, voel dat je hand weer terugkomt.
4. Herhaal dit 10 keer.

Dit kan ook worden toegepast terwijl je ligt of staat. Deze oefening kan dus terwijl je zit, ligt of staat.

Stap 10, terugkerende oefening later in de week

De begeleider vraagt later in de week nogmaals om de pinpas of code, en oefent ook met smeken of emotionele druk. Geef complimenten wanneer de deelnemer hun pinpas of code niet geeft. Indien nodig, nogmaals de reactie lezen en samen oefenen.

Deze opdrachten helpen deelnemers bij het ontwikkelen van hun vaardigheden om "nee" te zeggen en om onder druk kalm te blijven, zodat ze zichzelf kunnen beschermen in moeilijke situaties.

Titel Digitaal Meedoen: LVB Cyberweerbaar!

Pagina 80 / 94

Algemene tips voor beide opdrachten:

- **Herhaling is cruciaal:** De kracht van deze opdrachten ligt in de herhaling, zodat deelnemers de vaardigheid om "nee" te zeggen automatiseren.
- **Positieve feedback:** Geef regelmatig positieve feedback en erken de inspanning van de deelnemers, zelfs als ze moeite hebben.
- **Variatie in situaties:** Moedig variatie in het vragen aan, zodat deelnemers leren omgaan met verschillende soorten druk en manipulatie.

BIJLAGE 5 – Eerste poster (1^e iteratie ronde)



BIJLAGE 6 – Tweede poster (1° iteratieronde)

BEN JIJ GELDEZEL? 

JE HEBT JE PINPAS
UITGELEEND.
WAT DOE JE NU ?  

1 WORD RUSTIG, LET OP
JE ADEMHALING 

2 PRAAT MET IEMAND :
JE OUDER(S) OF
BEGELEIDER 

3 PRAAT JE LIEVER
MET IEMAND DIE
JE NIET KENT ?   **KINDERTELEFOON**
0-24 JAAR
0800 - 0432

  **LUISTERLIJN**
VANAF 18 JAAR
088 - 0767 000

OF WIL JE CHATTEN ?  **WWW.HELPWANTED.NL**
WWW.KEERPUNT.CHAT

4 GA SAMEN MET JE OUDER(S)
OF BEGELEIDER NAAR
POLITIE EN BANK   

 hogeschool
Windesheim  STUDIEBUREAU
AANSPRAKELIJK
TOEGEGANEN

BIJLAGE 7 – PDF met extra voorlichting informatie voor begeleiders omtrent geldezelen (1^o iteratieronde)

BEN JIJ GELDEZEL?

JE HEBT JE PINPAS
UITGELEEND.
WAT DOE JE NU?






1) WORD RUSTIG, LET OP
JE ADEMHALING


2) PRAAT MET IEMAND:
JE OUDER(S) OF
BEGELEIDER

3) PRAAT JE LIEVER
MET IEMAND DIE
JE NIET KENT?

OF WIL JE CHATTEN?

4) GA SAMEN MET JE OUDER(S)
OF BEGELEIDER NAAR
POLITIE EN BANK



1) Paniek helpt niet. Probeer rustig te ademen, dan wordt je weer rustig. Daarna kan je pas het gesprek aangaan.

Voor oefeningen om rustig te worden (zie de ademhalingsoefeningen bij de extra opdrachten ([instructies bij spel mediajungle](#)): bijvoorbeeld 5-vinger ademhaling)

2) Ga het gesprek aan als het de cliënt rustig is. Ga het gesprek constructief in, niet belerend en straffend.

Meer info over [hoe een gesprek te voeren over online gedrag en cyberweerbaarheid](https://www.mediawijsheid.nl/veelgestelde-vraag/is-er-materiaal-voor-begeleiders/) (inclusief geldezels): <https://www.mediawijsheid.nl/veelgestelde-vraag/is-er-materiaal-voor-begeleiders/>
Meer info over [geldezels](https://www.veiligbankieren.nl/fraude/geldezels/) voor begeleiders is te vinden bij: <https://www.veiligbankieren.nl/fraude/geldezels/>
<https://www.slachtofferhulp.nl/gebeurtenissen/fraude/geldezels/#:~:text=Een%20geldezels%2C%20money%20mule%20of%20of%20Telegram%2C%20of%20via%20vacatures>
Wil je ook meer [uitleg over geldezels geven aan de doelgroep](#) kan ook voorlichtingsmateriaal gebruikt worden:
• Wat is een geldezels? (NOS) zie link: https://www.youtube.com/watch?v=A9KR_cJ3DsU

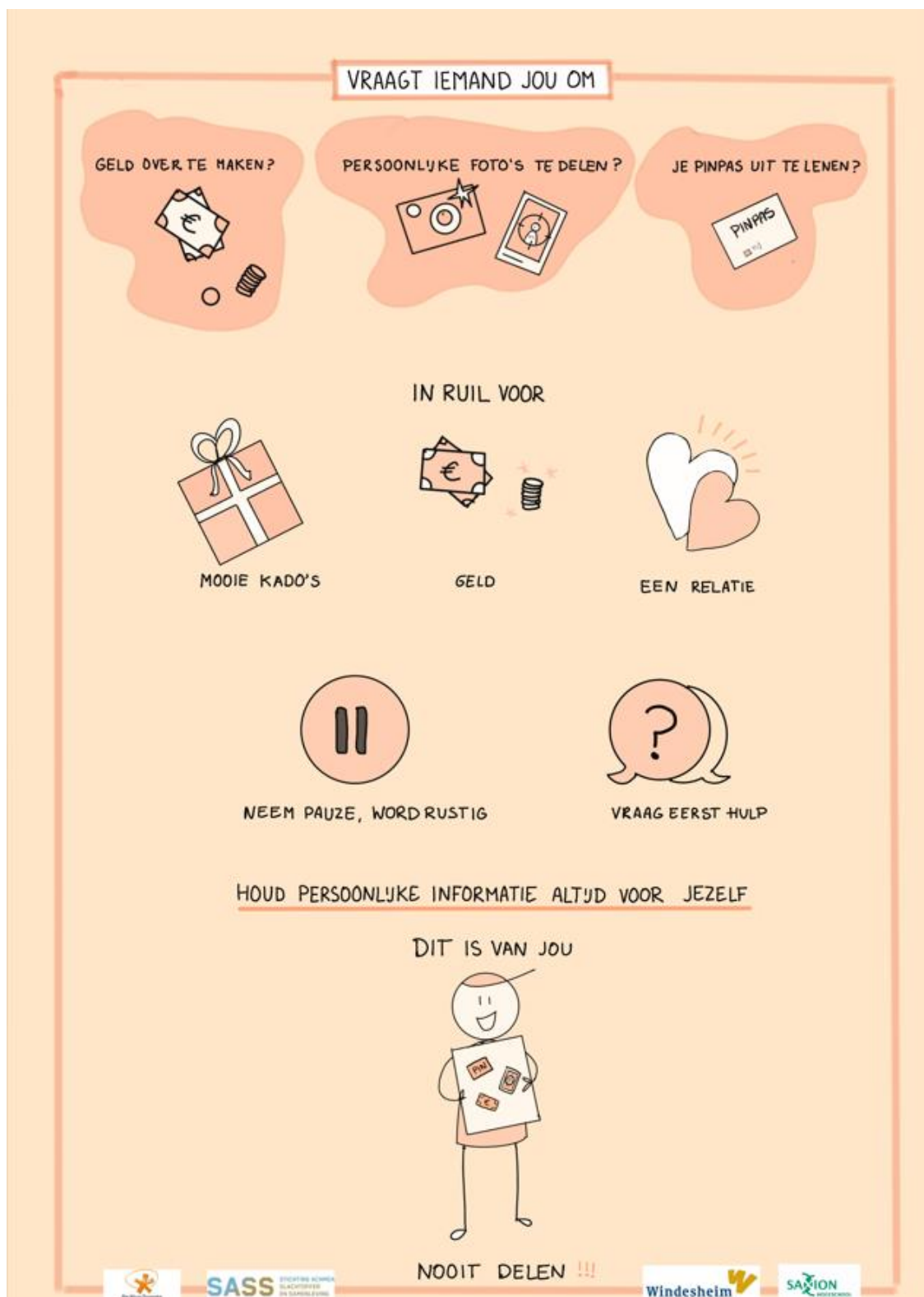
3) In gesprek ook aangeven dat ze ook bij andere instanties (anoniem) terecht kunnen

4) Kijk op volgende website voor tips over wat te doen wanneer jij/je cliënt als geldezels werd ingezet: <https://www.slachtofferhulp.nl/gebeurtenissen/fraude/geldezels/#:~:text=Een%20geldezels%2C%20money%20mule%20of%20of%20Telegram%2C%20of%20via%20vacatures>

Ga naar de **bank** en meld hier het (vermoeden van) geldezels.

Ga naar de **politie** om aangifte te doen, dit kan via:
Bel de politie op 0900-8844, of bij spoed op 112.
Anoniem, bel M. 0800-7000 of Meldmisdaadanoniem.nl

BIJLAGE 8 – Poster (2^e iteratieronde)



BIJLAGE 9 – Opdrachten onderzoekstas

Opdracht 1, beschrijf je dag

We willen graag weten wat jij vandaag hebt gedaan waarbij je internet hebt gebruikt.

Je kunt dit op de volgende manieren duidelijk maken:

Vraag aan je begeleider of je mag vertellen wat je hebt gedaan en neem dit verhaal op.

Vertel hierbij ook of je verteld over een dag in het weekend of door de weeks

Pak het papier met de zon en schrijf wat je hebt gedaan

Pak het papier met de zon en teken wat je hebt gedaan

Pak het papier met de zon en plak er stickers van wat jij hebt gedaan op.

Titel Digitaal Meedoen: LVB Cyberweerbaar!

Pagina 86 / 94

Opdracht 2, Wat ging er goed?



Pak het papier met het zonnetje.

**Geef met de stickers van de duimen aan
wat goed ging en wat niet.**

**Je mag hier iets bij schrijven of tekenen
als je wil.**

Titel Digitaal Meedoen: LVB Cyberweerbaar!

Pagina 87 / 94

Opdracht 3, mentale belasting door internetgebruik

Wat voor probleem heb je vandaag gehad bij de dingen waarbij je internet hebt gebruikt?

Schrijf het probleem in de tekstballon.

Schuif het rode papier omhoog om te laten zien hoe vol jouw hoofd zat door het probleem.



Opdracht 4, Whatsapp hulpvraag

Charlie vraagt Sem om hulp via Whatsapp.

De tekst die Charlie stuurt is groen en de tekst die Sem stuurt is wit.



Wat voor tip zou jij Sem geven als hij wel zijn pasje heeft uitgeleend, maar geen sneakers krijgt?

Schrijf de tip hieronder op.

.....

.....

.....

.....

Titel Digitaal Meedoen: LVB Cyberweerbaar!

Pagina 89 / 94

Opdracht 5, versieren van de onderzoekstas



BIJLAGE 10 – Informatiefolder onderzoeksmap



Informatiefolder Digitaal meedoen!

Je mag hulp vragen bij het lezen.



Julia

Hallo,
Wij zijn Julia, Tina en Nick.
Wij doen onderzoek bij een school.
Wil je meedoen aan ons onderzoek?
Je leest deze folder voor meer informatie.



Tina

Heb je vragen?
Deze kan je stellen aan Nick van der Klok.
Je begeleider kan je hierbij helpen.
Je kan mailen naar n.vanderklok@saxion.nl.
Je kan bellen naar Nick op: 06-41851629.



Nick

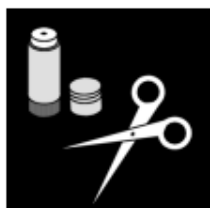
Wil je met iemand anders praten?
Dat kan met Willeke Slingerland.
Je kan mailen naar w.slingerland@saxion.nl.
Je kan bellen naar Willeke op: 06-13959327.



Waar gaat dit onderzoek over?

Dit onderzoek gaat over jou en het internet.
Wij willen weten waar jij aan denkt bij het woord internet.
Wij willen weten welke dingen jij doet op het internet.
Wij willen weten wat goed gaat op het internet.
Wij willen weten wat jij lastig vindt op het internet.

⁴ Deze rechten op inzage, rectificatie en ontvangen van persoonsgegevens staan beschreven in de Algemene verordening gegevensbescherming. Voor meer informatie: <https://www.saxion.nl/over-saxion/privacyverklaring>



Wat gaan we doen?

Je krijgt een tas met opdrachten.
Je kan zelf kiezen wat je gaat doen.
Je mag schrijven, tekenen of stickers plakken.
Je mag hulp vragen.
Je maakt de opdrachten 2 keer.
1 keer in het weekend en 1 keer door de weeks.
Je mag het ook vaker doen.
Niks moet.



Wanneer wordt de tas opgehaald?

Na 2 weken halen Julia en Nick de tas op.
We kijken naar jouw opdrachten.
Julia en Nick komen terug om met jou te praten over de tas.
De tas mag jij dan houden.



Doe je mee met het onderzoek?

Je helpt Julia, Tina en Nick als je meedoet.
Je mag zelf kiezen of je meedoet.
Je mag overleggen met je begeleider of je mee wil doen.



Wat zijn de afspraken als ik meedoe?

Als je meedoet zet je een handtekening op het toestemmingsformulier.

De onderzoeker maakt een verslag van de opdrachten.
Jouw naam staat niet in het verslag.

⁵ Deze rechten op inzage, rectificatie en ontvangen van persoonsgegevens staan beschreven in de Algemene verordening gegevensbescherming. Voor meer informatie: <https://www.saxion.nl/over-saxion/privacyverklaring>

BIJLAGE 11 – Toestemmingsformulier onderzoekstas

Toestemmingsformulier Digitaal meedoen!

Je mag hulp vragen bij het lezen.

Je mag overleggen met je begeleider of je mee wil doen.

Wil je meedoen aan dit onderzoek over gebruik van het internet?

Vul dan de grijze balk onderaan in.

Afspraken:



Als je meedoet:

- 1) Maak je opdrachten uit de tas.
 - 2) Praat je met een onderzoeker over de opdrachten.
 - 3) Je begeleider schrijft je leeftijd, geslacht en diagnose op voor de onderzoeker.
- ! Je naam wordt niet opgeschreven.



Je praat met een onderzoeker over de opdrachten.
Dit wordt opgenomen.
De onderzoeker luistert het gesprek later terug.
De onderzoeker schrijft op wat er is gezegd.
Jouw naam wordt niet genoemd.
Daarna wordt de opname verwijderd.



Je hoeft geen antwoord te geven.
Je mag op elk moment stoppen.
Je hoeft niet te vertellen waarom je stopt.



De onderzoeker bewaart de opdrachten op een veilige plek.
Wie mag de opdrachten bekijken:
- De onderzoekers
- De mensen die nakijken of het onderzoek klopt
Na 10 jaar worden de opdrachten verwijderd.

Heb jij vragen?

Deze kan je stellen aan Nick van der Kloek

Je begeleider kan je hierbij helpen.

Je kan mailen naar n.vanderklok@saxion.nl.

Je kan bellen naar 06-41851629.

Dat mag ook als je na het onderzoek nog vragen hebt.



De onderzoeker maakt een verslag van de opdrachten.
Jouw naam staat niet in het verslag.
Een verslag kan er zo uitzien:

In dit onderzoek deden 10 mensen mee.
Zij gebruiken soms het internet.
Dit doen ze vooral als ze gamen.
Ook spreken ze met vrienden af met whatsapp.
4 mensen geven aan wel eens problemen te ervaren met het internet.
Ze worden online gepest.
Ze willen leren hoe ze veilig kunnen omgaan met het internet.
Begeleiders moeten hierbij kunnen helpen.

Toestemming Digitaal meedoen!

- Ik heb informatie gekregen over het onderzoek.
- Al mijn vragen zijn beantwoord.
- Ik ben het eens met de afspraken op dit formulier.
-
- Ik doe mee aan het onderzoek:
 - Ja
 - Nee
- Ik vind het goed dat de opdrachten die ik maak gebruikt worden in een ander onderzoek:
 - Ja
 - Nee

Heb jij vragen?

Deze kan je stellen aan Nick van der Klok

Je begeleider kan je hierbij helpen.

Je kan mailen naar n.vanderklok@saxion.nl.

Je kan bellen naar 06-41851629.

Dat mag ook als je na het onderzoek nog vragen hebt.

Handtekeningen:

Deelnemer

Datum:

Naam:

Handtekening:

Wettelijk vertegenwoordiger

Datum:

Naam:

Relatie tot deelnemer:

Handtekening:

Onderzoeker

Datum:

Naam:

Handtekening:

Heb jij vragen?

Deze kan je stellen aan Nick van der Klok

Je begeleider kan je hierbij helpen.

Je kan mailen naar n.vanderklok@saxion.nl.

Je kan bellen naar 06-41851629.

Dat mag ook als je na het onderzoek nog vragen hebt.