City Deal
Lokale Weerbaarheid Cybercrime

Een onderzoek naar het effect van HackShield op de cyberweerbaarheid en agency van kinderen in de bovenbouw van de basisschool.

SAXION HOGESCHOOL

CYBER WEERBAAR NL

Colofon

Dit onderzoek is uitgevoerd door onderzoekers van het lectoraat Online Weerbaarheid van Hogeschool Saxion, aangesloten bij het Expertisenetwerk Cyberweerbaar NL:

Dr. Milou Kievik, senior onderzoeker;

Dr. Ynze van Houten, senior onderzoeker;

Lotte Kloosterhof, MSc., onderzoeker;

& Dr. Remco Spithoven, lector.

Daarbij is dit onderzoeksrapport van feedback voorzien door dr. Susanne van 't Hoff-de Goede, associate lector Cybercrime & Cybersecurity van de Haagse Hogeschool, eveneens aangesloten bij Cyberweerbaar NL.

Dit effectonderzoek is uitgevoerd in opdracht van de ministeries van Justitie & Veiligheid en Binnenlandse Zaken in het kader van de evaluaties van interventies binnen de Citydeal Lokale Weerbaarheid Cybercrime, onder procesregie van het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV).

City Deal
Lokale Weerbaarheid Cybercrime

Samenvatting

Cyberweerbaar NL – een expertisenetwerk van samenwerkende lectoraten met expertise op het gebied van cyberweerbaarheid van de Haagse Hogeschool, Hogeschool Saxion, NHL Stenden Hogeschool en Avans Hogeschool – ondersteunt de City Deal Lokale Weerbaarheid Cybercrime met een onderzoeksprogramma waarin de projecten uit deze City Deal worden geëvalueerd. Met een effectevaluatie wordt inzicht verworven in de daadwerkelijke effectiviteit van interventies en worden aanknopingspunten gezocht om het effect van de interventies te versterken. Dit betreft evaluatieonderzoek op basis van experimenteel onderzoek - met voormeting, de uitvoer van de interventie en nameting - om bestaande interventies te verbeteren (De Lange et al., 2011; Berding & Witte, 2013). Een van de interventies die veel door Nederlandse gemeenten is ingezet ter versterking van de cyberweerbaarheid van jonge kinderen (en hun omgeving) is Hackshield en HackShield in de Klas (Flavour, z.d.).

Op het moment van schrijven van het onderzoeksvoorstel bij dit onderzoek, vermeldde de website van dit platform dat Hackshield Cyber Heroes is gespeeld door 154.926 spelers in 187 Nederlandse gemeenten en dat het platform tevens actief is in Curaçao, Brazilië, België, Duitsland en Zweden (d.d. 19 februari 2024). HackShield is een cybersecurityspel voor kinderen tussen de 8 en 12 jaar en heeft als doel om een cyberveilige generatie kinderen te creëren. In de samenwerking met gemeenten roepen burgemeesters en politieagenten kinderen in hun gemeente op om HackShield te spelen en zo ‘cyber-agent’ in de gemeente te worden. Spelers met de meeste punten in het spel worden gehuldigd door de gemeenten. HackShield kent de volgende doelstellingen: 1) De eigen cyberweerbaarheid van de deelnemers (tussen de 8 en 12 jaar) vergroten; 2) Volwassenen in de omgeving van de deelnemers via de deelnemende kinderen cyberweerbaar maken (*agency*).

In opdracht van de Citydeal Lokale Weerbaarheid Cybercrime (Ministeries van Justitie & Veiligheid & Binnenlandse Zaken), luidt de hoofdvraag van dit onderzoek:

“*In hoeverre vertonen deelnemers van HackShield een toename in (1) de eigen cyberweerbaarheid en (2) agency ten aanzien van cyberweerbaarheid naar volwassenen in hun omgeving?”*

In dit onderzoek richten we ons – op basis van wetenschappelijke literatuur over gedragsverandering en weerbaarheid en gesprekken met de ontwikkelaars van HackShield – op de volgende constructen: (1) kennis; (2) risicoperceptie; (3) zelfeffectiviteit; (4) responseffectiviteit; (5)

subjectieve normen; (6) gedragsintentie; (7) agency, (8) verantwoordelijkheid en (9) verminderde impulsiviteit.

HackShield bestaat uit een individueel spel en “HackShield in de Klas”. Bij HackShield in de Klas spelen leerlingen op hun basisschool – begeleid door hun leerkracht of een gastdocent – gezamenlijk een quest. Omdat het binnen de tijdsspanne en het beschikbare budget voor dit onderzoek niet mogelijk was om alle onderdelen van HackShield en HackShield in de Klas op effect te evalueren, is er in overleg met de opdrachtgevende ministeries en HackShield voor gekozen om een exemplarisch onderdeel te selecteren voor de effectevaluatie. Daarmee is de meest gespeelde klassenquest op effect geëvalueerd. Dit onderzoek richt zich dan ook op de evaluatie van het effect van de klassenquest ‘Online grenzen’, waarin zowel de thema’s ‘online pesten’ als ‘hacken’ aan bod komen. Om de hoofdvraag van dit onderzoek te beantwoorden zijn de onderstaande onderzoeksactiviteiten uitgevoerd:

Literatuurstudie en interviews met de ontwikkelaars van HackShield – Er is literatuuronderzoek uitgevoerd naar o.a. cyberweerbaarheid, cyberweerbaarheid van jonge kinderen (8 tot 12 jaar); *agency* en gedragsverandering van kinderen. Dit resulteerde in een onderbouwde lijst van elementen die van invloed zijn op de cyberweerbaarheid van jonge kinderen en een onderbouwde lijst met criteria om *agency* door kinderen mee vast te kunnen stellen. Tevens is er op basis van interviews met tien oprichters en ontwikkelaars van HackShield in kaart gebracht wat de specifieke doelen van HackShield zijn en op welke wijze zij deze beoogde doelen in de klassenquest ‘Online grenzen’ proberen te realiseren. Deze beoogde doelen van HackShield – naast de variabelen afgeleid uit het literatuuronderzoek – vormden de basis voor dit onderzoek.

Methode van onderzoek – kwalitatieve inhoudsanalyse - Op basis van de literatuurstudie is gekeken naar de mate waarin de inhoud van de klassenquest ‘Online grenzen' resoneert met de in de literatuur aangetroffen voorspellers voor cyberweerbaarheid. Ook is er gekeken naar de wijze waarop hier in deze quest door HackShield invulling aan is gegeven. Het doel hiervan is om – samen met de effectmeting die in dit onderzoek wordt gedaan – inzicht te geven in de eventuele werkzame aspecten, evenals aanknopingspunten te vinden voor toekomstige optimalisering van deze quest. Middels deze kwalitatieve analyse zijn de in de quest ‘Online grenzen’ aan de deelnemers geboden handelingsperspectieven expliciet gemaakt. Daarbij is eveneens gekeken naar de elementen die van invloed zijn op weerbaar gedrag onder de deelnemers van de quest.

Methode van onderzoek – kwantitatieve effectmeting - Op basis van het literatuuronderzoek, en de interviews met de oprichters en ontwikkelaars van HackShield is vervolgens door de onderzoekers een kwantitatief meetinstrument ontwikkeld om de kennis, cyberweerbaarheid en *agency* onder de

deelnemers in kaart te kunnen brengen. Dit betrof een vragenlijst, speciaal ontwikkeld en vooraf getest onder kinderen tussen de 8 en 12 jaar. Door deze, op basis van wetenschappelijke theorie ontwikkelde en zorgvuldig geteste, vragenlijst te laten invullen *voordat* kinderen de quest 'Online grenzen' speelden, en nogmaals *nadat* kinderen deze quest hadden gespeeld, kunnen eventuele verschillen die tussen deze metingen optreden, aan het spelen van de klassenquest worden toegeschreven. Daarmee volgen wij voor deze effectevaluatie een experimenteel onderzoeksdesign (De Vaus, 2021) en meer specifiek het zogenaamde 'één-groep-voormeting-nameting-ontwerp' (Quené & van den Bergh, 2026).

Resultaten kwalitatieve inhoudsanalyse – Uit de kwalitatieve inhoudsanalyse kwam naar voren dat in de klassenquest 'Online grenzen' de onderdelen van cyberweerbaarheid volgens de wetenschappelijke literatuur slechts gedeeltelijk terugkomen. Voor het thema 'hacken' werd vastgesteld dat er duidelijke handelingsperspectieven aan de deelnemende kinderen werden gegeven over hoe kinderen het risico op slachtofferschap van hacken kunnen verminderen. Voor het thema 'online pesten' werden vrijwel geen – en bij nadere analyse soms tegenstrijdige – handelingsperspectieven gegeven hoe online pesten te voorkomen. Deze resultaten hebben aanleiding gegeven te veronderstellen dat het effect van de quest op de weerbaarheid van deelnemer verschillend kan zijn voor de thema's 'hacken' en 'online pesten'.

Kwantitatieve voormeting – In totaal zijn in de voormeting van dit onderzoek de resultaten van 368 kinderen meegenomen. Het gaat om kinderen in groepen 6, 7 en 8 (of een combinatie daarvan) van negen basisscholen verspreid over heel Nederland, die nog *geen* eerdere ervaring hadden met het spelen van HackShield of HackShield in de Klas.

Kwantitatieve nameting – Na deelname van de kinderen aan de klassenquest 'Online grenzen' is hen gevraagd om nogmaals de vragenlijst in te vullen. Daarnaast is gevraagd naar hun mening over de inhoud en vormgeving van de quest zelf. In totaal hebben 295 kinderen deze vragenlijst volledig ingevuld. Deze afname in het totaal aantal ingevulde vragenlijsten is mogelijk te verklaren doordat het voor leerkrachten moeilijk was de drie onderdelen van dit onderzoek - de voormeting, het spelen van de quest en de nameting - in te passen in het hun drukke onderwijsschema, waardoor enkele docenten de nameting niet met hun klas hebben ingevuld.

Resultaten kwantitatieve effectmeting – In de vergelijking van de resultaten van de voor- en nametingen is er allereerst gekeken naar de *overall* waardering van de deelnemers voor de klassenquest 'Online grenzen'. Gemiddeld gaven de deelnemers de quest een 7,1; een ruime voldoende. Deelnemende leerlingen waarderen het spelelement en vinden de quest grotendeels interessant en leerzaam.

Door de scores op de vragenlijst in de voor- en nameting met elkaar te vergelijken is vervolgens een uitspraak gedaan over het effect van het spelen van HackShield – specifiek de klassenquest 'Online grenzen'- op de twee doelstellingen van HackShield: (1) vergroten van de cyberweerbaarheid van deelnemers en (2) vergroten van de *agency* van de deelnemers richting de volwassenen in hun omgeving. Voor het thema 'online pesten' zijn tussen de resultaten van de voor- en nameting *nagenoeg geen effecten* gevonden van het spelen van de quest op de weerbaarheid tegen online pesten of onderdelen van weerbaarheid rond dat thema. Na het spelen van de quest hadden kinderen ook niet meer kennis over online pesten dan voor het spelen van de quest. Wel was een kleine afname zichtbaar in de ervaren zelfeffectiviteit van kinderen: het vertrouwen dat kinderen hebben om zelf iets tegen dit risico te kunnen doen. Eveneens was er een significante afname zichtbaar in de risicoperceptie van kinderen ten aanzien van online pesten: zij schatten het risico op online pesten als kleiner in na het spelen van het spel. Ook wat betreft de intentie tot weerbaar gedrag tegen online pesten waren *overall geen verschillen* tussen de voor- en nameting zichtbaar, met een *kleine significante toename* van de intentie van kinderen om zelf over te gaan tot online pesten. Hierbij moet echter worden opgemerkt dat de kinderen in zowel de voor- als de nameting een hele lage intentie tot pestgedrag lieten zien. Het spelen van de klassenquest 'Online grenzen' blijkt daarmee dus nagenoeg geen effect te hebben op de weerbaarheid van de deelnemende leerlingen tegen online pesten.

Voor het thema 'hacken' vonden we *positieve effecten* van het spelen van de quest op de (onderdelen van) weerbaarheid tegen dit risico. Deelnemers lieten een *significante toename* zien in hun zelfeffectiviteit ten aanzien van dit risico: zij hadden meer vertrouwen in zichzelf om zich te kunnen beschermen tegen hacken. Ook hun responseffectiviteit ten opzichte van hacken *nam significant toe:* de in de quest voorgestelde handelingsperspectieven om hacken tegen te gaan werden na het spelen van deze quest door de deelnemende leerlingen als significant nuttiger en zinvoller ingeschat, dan voor het spelen van de quest. Kinderen hadden tevens *significant positievere subjectieve normen* na het spelen van de quest dan voor het spelen van de quest: zij hadden na het spelen van de quest meer het idee dat hun vrienden geneigd waren om zichzelf tegen hacken te beschermen. Tussen de voor- en nameting werd echter geen significant verschil waargenomen voor de door de deelnemende leerlingen gerapporteerde intentie om zichzelf tegen hacken te beschermen. Het is dus niet zo dat de deelnemende kinderen rapporteerden dat zij na het spelen van de quest 'Online grenzen' zich voor hebben genomen om zichzelf meer tegen hacken te beschermen.

Vervolgens is in kaart gebracht of het spelen van de klassenquest 'Online grenzen' bijdraagt aan de *agency* van kinderen richting hun omgeving. *Agency* is hier – op basis van de gesprekken met de

ontwikkelaars van HackShield - geoperationaliseerd als de intentie van kinderen om het tijdens de quest geleerde actief uit te dragen naar volwassen in hun omgeving en gesprekken met hen te voeren over het thema 'veilig internetten'. Het spelen van de quest 'Online grenzen' had *een beperkt effect* op de agency van de deelnemende kinderen. Kinderen gaven überhaupt aan vrijwel niet met hun ouders of verzorgers te spreken over veiligheid op het internet en hierin was na het spelen van de klassenquest ook geen toename zichtbaar. Wel zagen we een *kleine, significante toename* in de mate waarin kinderen het gevoel hadden dat ze hun ouders of verzorgers iets zouden kunnen leren over online veiligheid.

Conclusies – Op basis van dit onderzoek kan geconcludeerd worden dat het spelen van de quest 'Online grenzen' niet leidt tot een hogere intentie tot weerbaar gedrag tegen hacken en online pesten onder de deelnemende leerlingen. Voor de weerbaarheid tegen online pesten waren er na het spelen van de quest ook *geen effecten* zichtbaar op onderdelen van weerbaar gedrag. Voor de weerbaarheid tegen hacken waren *wel significante, positieve effecten* zichtbaar op de onderdelen van weerbaar gedrag, te weten zelfeffectiviteit, responseffectiviteit en subjectieve normen. Er was na het spelen van de quest 'Online grenzen' onder de deelnemers aan dit onderzoek *weinig tot geen toename van agency* zichtbaar richting volwassenen in hun omgeving.

De resultaten voor de thema's 'online pesten' en 'hacken' waren verschillend van elkaar. Dit kunnen we verklaren met behulp van de uitgevoerde inhoudsanalyse van de quest 'Online grenzen', omdat er voor het thema 'online pesten' geen eenduidige – soms tegenstrijdige – handelingsperspectieven in de quest zijn verwerkt. Hierdoor hebben kinderen wellicht na het spelen van het spel het gevoel dat zij zelf niet in staat zijn om iets tegen online pestgedrag te doen (afname zelfeffectiviteit) en dat er eigenlijk geen zinvolle maatregelen zijn om pestgedrag tegen te gaan. Hierdoor zullen zij mogelijk ook niet geneigd zijn om zelf weerbaar gedrag ten aanzien van online pesten te gaan vertonen. Voor het thema 'hacken' zagen we daarentegen dat er duidelijke handelingsperspectieven in de quest aanwezig waren, bijvoorbeeld het kiezen van verschillende wachtwoorden voor verschillende accounts. Dit onderwerp werd ook actief besproken tijdens het klassikaal spelen van de quest, wat een positieve impact kan hebben gehad op het gevoel van deelnemende leerlingen dat zij in staat zijn om zich te beschermen tegen hacken (toename zelfeffectiviteit) en dat deze maatregelen ook daadwerkelijk zinvol zijn in het verminderen van het risico op hacken (responseffectiviteit).

Aanbevelingen – Effectieve interventies met als doel om de cyberweerbaarheid van deelnemende leerlingen te vergroten zouden – op basis van wetenschappelijke inzichten – idealiter voldoen aan verschillende voorwaarden (Leukfeldt, 2024). Zo zouden deelnemers zich allereerst bewust moeten zijn van het risico en dat dit risico ook voor henzelf een potentiële dreiging zou kunnen zijn.

Vervolgens hebben deelnemers concrete en actuele handelingsperspectieven nodig; maatregelen die hen kunnen helpen bij het verminderen van het risico of de dreiging. Deze handelingsperspectieven moeten zo zijn opgesteld dat deelnemers (1) er vertrouwen in hebben dat ze deze maatregelen zelf kunnen uitvoeren en (2) het gevoel hebben dat deze maatregelen nuttig en zinvol zijn in het verminderen van het risico. Op basis van de kwalitatieve inhoudsanalyse komt naar voren dat deze onderdelen onvoldoende verweven zijn in de klassenquest 'Online grenzen' voor het thema 'online pesten'. Voor het onderdeel 'hacken' komen deze onderdelen duidelijker naar voren. Wel is hier nog winst te behalen ten aanzien van de gedragsintentie: de neiging om jezelf meer tegen het risico te beschermen. Het verdient de aanbeveling voor de ontwikkelaars van HackShield om te overwegen voor online pesten een zelfstandige klassenquest te ontwikkelen en *overall* het aantal doelstellingen en thema's per quest naar beneden te brengen: elk thema binnen het programma bevat immers een complex thema en gedragsverandering heeft, gezien de complexiteit van dit proces, focus nodig.

Het beoogde aspect van *'agency'* in de inhoud van klassenquest 'Online Grenzen' komt op basis van zowel de kwalitatieve inhoudsanalyse als de effectmeting onvoldoende uit de verf om effect van te verwachten. Hierop zou – indien men aan dit doel wil vasthouden – meer gerichte aanpassing van de quest nodig zijn, waarmee deelnemende leerlingen hier meer toe worden aangezet. Het zou voor de ontwikkelaars van HackShield in de Klas aan te bevelen zijn om alle klassenquests inhoudelijk langs het in dit effectonderzoek uiteengezette theoretische kader en de ontwikkelde (of aangevulde) meetlat van cyberweerbaarheid, onderdelen daarvan en *agency* te leggen, om deze aspecten gestructureerd in de verschillende klassenquests van HackShield in de Klas te integreren. Daarnaast sterkt het de aanbeveling om de handelingsadviezen in samenwerking met experts op de specifieke thema's te ontwikkelen, bij hen te toetsen en deze in samenwerking met hen actueel te houden. Tevens zou aanvullend advies of begeleiding door experts op het gebied van gedragsverandering (onder kinderen) kunnen bijdragen aan het realiseren van meer cyberweerbaar gedrag onder deelnemende leerlingen.

Inhoudsopgave

1. Introductie

1.1 Inleiding: noodzaak voor effectevaluaties

Cyberweerbaar NL – een expertisenetwerk van samenwerkende lectoraten met expertise op het gebied van cyberweerbaarheid van de Haagse Hogeschool, Hogeschool Saxion, NHL Stenden Hogeschool en Avans Hogeschool – ondersteunt de City Deal Lokale Weerbaarheid Cybercrime al vanaf de start met een onderzoeksprogramma waarin de projecten uit deze City Deal op proces en effect worden geëvalueerd. Zodoende kunnen andere organisaties die deze interventies willen inzetten hun voordeel doen met de onderzochte succesfactoren bij de implementatie van de interventie. Ook worden de meest veelbelovende en vaakst geïmplementeerde interventies ter versterking van de cyberweerbaarheid van inwoners en ondernemers voorzien van een effectevaluatie. Met deze effectevaluatie wordt inzicht verworven op de daadwerkelijke effectiviteit van de interventie en worden aanknopingspunten gezocht om het effect van de interventie te versterken.

De winst van dit onderzoeksprogramma zit in het geprogrammeerd en gestandaardiseerd vergroten van de algehele effectiviteit van interventies in de City Deal Lokale Cyberweerbaarheid. Daarmee weten lokale partners dat de interventies uit deze City Deal hun effectiviteit hebben bewezen en daarmee *evidence-based* bijdragen aan de lokale cyberweerbaarheid. Een aanvullende meerwaarde is dat het project de evaluatiemethodiek via de City Deal ter beschikking stelt, waarmee gemeenten en partners eigen toekomstige projecten dusdanig kunnen inrichten dat deze in theorie goed geëvalueerd kunnen worden. Daarnaast wordt met de inzet van kwalitatieve methoden het effect voor individuele deelnemers geverifieerd en het zicht op de achtergronden van het effect vergroot. Daarmee wordt in het totale onderzoek zicht verworven op oorzaken van positieve en eventuele negatieve effecten om hier tevens in soortgelijke interventies van te kunnen profiteren.

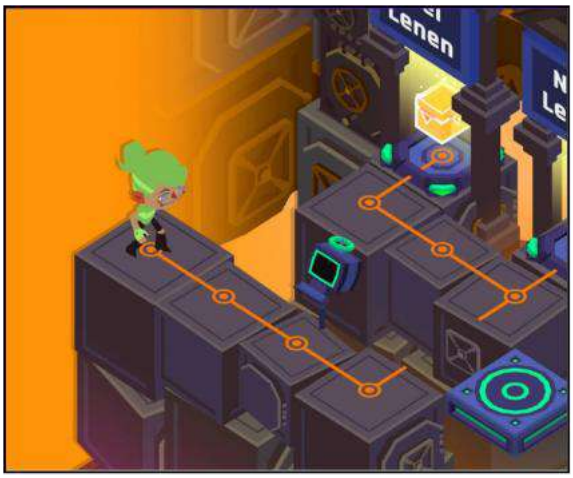
Deze eerder op proces geëvalueerde interventies brengen wij in het kader van *practice* en *evidence-based* onderzoek met effectevaluaties naar de volgende stap. Dit betreft evaluatieonderzoek op basis van experimenteel onderzoek om bestaande interventies te verbeteren en daarmee te innoveren (De Lange et al., 2011; Berding & Witte, 2013). Daarbij wordt gebruik gemaakt van experimenteel onderzoek met voor- en nametingen en een controlegroep om de inhoudelijke effectiviteit van de interventie te kunnen meten.

1.2 Selectie Hackshield Future Cyber Heroes voor een effectevaluatie

Een van de interventies die veel door Nederlandse gemeenten is ingezet ter versterking van de cyberweerbaarheid van jonge kinderen en hun omgeving is Hackshield Future Cyber Heroes (hierna HackShield). Op het moment van schrijven van de onderzoeksopzet bij dit onderzoek vermeldde de website van dit platform dat Hackshield is gespeeld door 154.926 spelers in 187 Nederlandse gemeenten en dat het platform tevens actief is in Curaçao, Brazilië, België, Duitsland en Zweden (d.d. 19 februari 2024). HackShield is een cybersecurity spel voor kinderen tussen de 8 en 12 jaar en heeft naar eigen zeggen tot doel om een cyberveilige generatie kinderen te creëren. In de samenwerking met gemeenten roepen burgemeesters en politieagenten kinderen op om het spel te spelen en 'cyber-agent' van de gemeente te worden. Spelers met de meeste punten worden gehuldigd door de gemeenten. Figuur 1 geeft een sfeerimpressie van HackShield weer.

Figuur 1.

Sfeerimpressie van Hackshield (Hackshield, z.d.)



In een eerdere, beknopte plan- en procesevaluatie uitgevoerd door onderzoekers van de Haagse Hogeschool en Hogeschool Saxion (Schiks et al., 2021) zijn de beleidstheorie, uitvoering en ervaringen van de implementatie van HackShield in gemeenten in Noord-Holland in kaart gebracht. Uit deze plan- en procesevaluatie kwam naar voren dat deelnemers, ouders en uitvoerders tevreden waren over het verloop van de uitrol over de Noord-Hollandse gemeenten. De achttien geïnterviewde spelers (de helft van hen betrof 'testers' en daarmee de meest fanatieke spelers van het spel) gaven aan enthousiast te zijn en het spel als leuk en leerzaam te ervaren. Ook ouders gaven aan het spel aan te bevelen aan andere

ouders. Wel viel het bereik met maximaal 9% van de kinderen in de gemeente wat tegen. Daarom werd geadviseerd om scholen meer bij HackShield te betrekken.

In deze plan- en procesevaluatie bleef het daadwerkelijke effect van het spelen van HackShield onder de deelnemers echter onduidelijk. Hierbij werd het volgende geadviseerd: 'Toekomstig evaluatieonderzoek in de vorm van (kwantitatieve) effectevaluaties kan aantonen wat de daadwerkelijke effecten zijn van het initiatief. Zo kan er een voor- en nameting plaatsvinden met betrekking tot de kennis die deelnemers en ouders daadwerkelijk opdoen, door vragenlijsten op te stellen die deze kennis toetsen. Verder verdient het de aanbeveling om ook kwalitatief onderzoek te blijven uitvoeren, zodat zowel positieve effecten als mogelijke ongewenste consequenties van het initiatief in kaart kunnen worden gebracht. Interviews met deelnemers en ouders zijn hiervoor geschikt, mits de steekproeven representatief zijn voor alle deelnemers' (Schiks et al., 2021).

1.2.1 Doelstellingen en achtergrond van HackShield

HackShield wordt omschreven als een cybersecurity-spel voor kinderen tussen de 8 en 12 jaar oud. In plaats van als potentiële slachtoffers, benadert HackShield de spelers als *future cyber heroes*: de digitale helden van morgen. Het doel van HackShield is om een cyberveilige generatie kinderen te creëren. Om dit doel te bereiken krijgen kinderen tijdens het spel een reeks opdrachten – ook wel 'quests' genoemd – aangeboden. In de opdrachten maken deelnemers eerst kennis met thema's zoals 'phishing' en vervolgens worden de kinderen gestimuleerd om de door hen opgedane kennis over te dragen aan hun omgeving, bijvoorbeeld aan hun (groot)ouders. Kinderen worden door HackShield actief opgeroepen om deel te nemen aan HackShield (Figuur 2).

Figuur 2.

Oproep van Kinderen om Hackshield te gaan spelen (Hackshield, z.d.)

Hieruit kunnen de volgende doelstellingen van HackShield worden afgeleid:

1. De eigen cyberweerbaarheid van de deelnemers (tussen de 8 en 12 jaar) vergroten;
2. Volwassenen in de omgeving van de deelnemers cyberweerbaar maken (*agency*).

HackShield is ontwikkeld aan de hand van 'Hero Centered Design', een design waarbij het publiek een belangrijke taak toebedeeld krijgt. Het Hero Centered Design is gebaseerd op de overtuiging en ervaring van de makers van HackShield dat publiek pas in beweging komt wanneer zij zelf de hoofdrol spelen in hun eigen verhaal. Dit dient te resulteren in een trans mediale productie: een productie waarbij verhalen zich over verschillende media (spellen, sociale-media en andere platformen) heen bewegen en het publiek meeneemt in een multimediale verhaalwereld waar het invloed kan uitoefenen op de uitkomst van het verhaal (Flavour, z.d.).

1.3 Doelstelling van dit onderzoek

Het doel van dit onderzoek is om de effectiviteit van het spelen van HackShield op de *online weerbaarheid* en *agency* van kinderen van groep 7 en 8 van de basisschool in kaart te brengen. We kijken in dit onderzoek naar het effect van het spelen van HackShield op de kennis, weerbaarheid en *agency* van kinderen van basisscholen verspreid over Nederland.

1.4 Hoofdvraag en deelvragen

De hoofdvraag van dit effectonderzoek is:

In hoeverre vertonen deelnemers van HackShield een toename in (1) de eigen cyberweerbaarheid en (2) agency ten aanzien van cyberweerbaarheid naar volwassenen in hun omgeving?

Deze hoofdvraag is opgedeeld in de volgende drie deelvragen:

1. In hoeverre draagt het spelen van HackShield bij aan het vergroten van kennis van deelnemers ten aanzien van cyberrisico's?
2. In hoeverre draagt het spelen van HackShield bij aan het versterken van de cyberweerbaarheid van deelnemers ten aanzien van cyberrisico's?
3. In hoeverre draagt het spelen van HackShield bij aan het vergroten van de *agency* van deelnemers ten aanzien van cyberweerbaarheid naar volwassenen in hun omgeving?

2. Beschrijving van de interventie

2.1 Hackshield

HackShield is een educatief platform in de vorm van online spellen (zogenaamde quests) die kinderen leren hoe ze veilig kunnen omgaan met het internet en hoe ze zich kunnen beschermen tegen cybercrime. Binnen HackShield wordt er aandacht besteed aan een verscheidenheid aan thema's rondom cybercrime, zoals hacking, phishing, online pesten en nepnieuws. HackShield richt zich op kinderen tussen de 8 en 12 jaar (HackShield, z.d.).

HackShield bestaat uit twee onderdelen: een individuele quest en HackShield in de Klas. De individuele quest kan door ieder kind worden gespeeld en wordt niet gestuurd vanaf school. Kinderen kunnen een account aanmaken en het individuele spel op eigen tempo doorlopen. HackShield in de Klas bestaat inmiddels uit zo'n twaalf quests met verschillende thema's (zoals cyberpesten, hacken, phishing et cetera) die kinderen gezamenlijk spelen in de klas met een (gast)docent (HackShield, z.d.).

Het doel van HackShield is om kinderen bewust en weerbaar te maken in de digitale wereld zodat ze online gevaren kunnen herkennen, voorkomen en veilig kunnen kijken naar hun eigen internetgebruik en dat van anderen (HackShield, z.d.). Ook zet HackShield in op het vergroten van de impact van het spel door kinderen te benoemen als zogenaamde "Cyber Agents". Als *cyber agent* is een kind niet alleen verantwoordelijk voor het vergroten van de eigen cyberweerbaarheid, maar ook voor het uitdragen van deze boodschap naar anderen (zoals ouders, verzorgers en grootouders). Ze leren daarmee niet alleen hoe ze zichzelf veilig kunnen houden online, maar ook hoe ze anderen – bijvoorbeeld ouders – kunnen helpen. Dit principe wordt door HackShield het "Hero Centered Design" genoemd (Flavour, z.d.). Het idee is dat HackShield een succes is als kinderen hetgeen ze hebben geleerd binnen het spel gaan uitdragen in de samenleging (HackShield, z.d.).

HackShield heeft bij het opzetten van de verschillende quests samengewerkt met wetenschappers en kennisexperts om tot inhoudelijk zinvolle en relevante quests te komen. Tot op heden is HackShield echter nog niet wetenschappelijk onderzocht. Er is nog geen wetenschappelijk bewijs dat het spelen van HackShield zorgt voor meer cyberweerbaarheid onder kinderen (en hun omgeving). In dit onderzoek wordt daarom gekeken naar de effectiviteit van HackShield op de cyberweerbaarheid van kinderen.

Aangezien HackShield op dit moment bestaat uit een individuele game en twaalf klassenquests, is het te veel om HackShield als geheel op effect te evalueren. We hebben daarom voor dit onderzoek gekozen om een steekproef te trekken uit de quests die op dit moment worden gespeeld en specifiek deze quest te gaan evalueren.

2.2 Keuze voor HackShield in de Klas, klassenquest 'Online grenzen'

Om een betrouwbare effectmeting uit te voeren en inzicht te krijgen in het effect van HackShield op de cyberweerbaarheid van kinderen, is het belangrijk om data te verzamelen bij kinderen die nog *niet* eerder met HackShield in aanraking zijn gekomen. Daarom is ervoor gekozen om respondenten te werven via basisscholen. Via scholen kunnen in één keer veel kinderen worden bereikt en kan bovendien worden vastgesteld of en in hoeverre HackShield eerder in de klas is ingezet. Omdat het moeilijk te controleren is of kinderen het individuele spel zelfstandig hebben gespeeld en afgerond, richt dit onderzoek zich op een klassenquest. Deze quest wordt gezamenlijk met de leerkracht (of een gastdocent) uitgevoerd, waardoor de dataverzameling gecontroleerd en uniform binnen de schoolcontext kan plaatsvinden.

HackShield houdt een overzicht bij van het aantal keer dat hun quests door kinderen worden gespeeld. Op basis van de data aangeleverd door HackShield (maart 2026) blijkt dat de klassenquest 'Online grenzen' het meest wordt gespeeld. In totaal was deze quest toen 2952 keer gespeeld, wat goed is voor meer dan 30% van het totaal aantal gespeelde klassenquests (interne documententatie HackShield, 2026). De Het gaat in dit geval om een klassenquest waarbij de docent (of een gastdocent) samen met de leerlingen de thema's 'online pesten' en 'hacken' bespreekt. De docent (of gastdocent) begeleidt de klassenquest en de discussies die op basis van de quest worden gevoerd. Aangezien de klassenquest 'Online grenzen' veruit het meest wordt gespeeld van alle klassenquests die HackShield heeft ontwikkeld, is de keuze gemaakt om deze klassenquest als exemplarisch gaan gebruiken voor HackShield als geheel. De keuze om deze klassenquest als exemplarisch te gaan gebruiken werd ondersteund door medewerkers en het management van HackShield zelf. Tijdens de interviews met medewerkers van HackShield is onze keuze voor deze klassenquest voorgelegd aan de respondenten. Zij bevestigden eenduidig dat deze quest representatief is voor HackShield als geheel.

2.3 Interviews met medewerkers van HackShield

HackShield is als creatieve, dynamische interventie continu in beweging. Met veel inspanning en betrokkenheid worden quests ontwikkeld met als doel om kinderen meer cyberweerbaar te maken. Bij de start van dit onderzoek (maart 2025) kon HackShield ons voorzien van een aantal interne documenten die uitleg gaven over de rol van *gamification* binnen de quests en hun *Hero Centered Design* (Flavour, z.d.). Een theoretische onderbouwing van waarom de verschillende quests volgens HackShield zouden bijdragen aan de cyberweerbaarheid van kinderen was echter niet voorhanden. Op basis daarvan is er besloten om interviews te houden met in totaal tien medewerkers achter HackShield (verdeeld over vijf online interviews in de tijdsperiode juli-september 2025). Het doel van deze interviews was om samen

met de ontwikkelaars van HackShield de beleidstheorie achter de quest te expliciteren, dat wil zeggen; het geheel aan veronderstellingen over hoe de quest kan bijdragen aan cyberweerbaarheid van kinderen (zie ook Pawson & Klein Haarhuis, 2005). De selectie van medewerkers van HackShield is gedaan door HackShield zelf, waarbij deelnemers zijn geselecteerd op basis van hun bijdrage aan het opzetten van – onderdelen van – HackShield.

Deze interviews waren zeer betekenisvol volgens de onderzoekers. Uit de gesprekken kwam immers naar voren dat HackShield een aantal elementen kent, die volgens de medewerkers zouden moeten leiden tot meer cyberweerbaarheid, namelijk:

1. **Het vergroten van het risicobewustzijn**

   In de interviews kwam naar voren dat een belangrijk doel van HackShield is om kinderen te laten zien dat er gevaren zijn in de onlinewereld die ook op hen van toepassing zijn. Ontwikkelaars gaven aan dat zij kinderen niet zo zeer willen opleggen wat zij moeten doen en waar zij zich aan moeten houden online, maar dat zij wel als doel hebben om kinderen te leren tegen welke risico's zij kunnen aanlopen op het Internet. Zo gaf een ontwikkelaar aan: *"We willen kinderen niet leren wat ze moeten doen, maar wel dat ze slachtoffer kunnen worden en dat dit ook ernstig is".* Het bewust maken van cyberrisico's, het stimuleren van het kritisch denken onder kinderen en het bewustmaken van consequenties van keuzes die online worden gemaakt, zijn volgens HackShield belangrijke doelen die zij willen behalen met hun quests: *"We willen stimuleren dat kinderen kritisch denken en consequenties van keuzes laten zien".*

2. **Het vergroten van de zelfeffectiviteit en responseffectiviteit**

   Tevens kwam in de interviews naar voren dat HackShield kinderen wil leren dat zij zelf iets kunnen doen om cyberrisico's te verkleinen. Medewerkers gaven aan dat kinderen tijdens de quests leren dat zij zelf in staat zijn om zichzelf te beschermen, dat zij maatregelen kunnen treffen om risico's te verkleinen en dat het belangrijk is dat kinderen na het spelen van een quest het gevoel hebben zichzelf te kunnen beschermen tegen risico's op het Internet. Zo gaven medewerkers aan: *"De kinderen moeten leren hoe ze zichzelf kunnen beschermen en dat dat helpt"* en *"Kinderen moeten het gevoel hebben dat ze zelf iets kunnen doen en dat dat dan ook echt helpt".*

3. **Het versterken van de subjectieve normen**

   Daarnaast werd tijdens de interviews duidelijk dat – specifiek voor HackShield in de Klas – de rol van *peers* heel belangrijk is. HackShield in de Klas is zo opgezet, dat er veel gesprekken en discussies over cyber-gerelateerde thema's worden gevoerd in de klas. Het idee hierachter is volgens HackShield: *"Door in de klas de quests samen te spelen leren ze ook hoe andere kinderen*

naar dit thema kijken". Dit werd aangevuld met: *"Door hier samen over te praten in de klas, ontwikkelen kinderen meer begrip voor elkaar en de thema's die worden besproken".*

4. **Het versterken van *agency***

   Een belangrijk doel van HackShield is het vergroten van *agency*. Het idee hierachter is volgens HackShield dat kinderen door deelname aan HackShield worden uitgedaagd en uitgenodigd om met volwassen in hun omgeving over de thema's te spreken die behandeld zijn tijdens HackShield in de Klas. Zo werd door meerdere medewerkers aangegeven: *"Het belangrijkste doel van HackShield is dat kinderen het geleerde uitdragen en gedrag en kennis delen met anderen".* De gedachte hierachter is volgens HackShield dat we veel meer onthouden van een bepaald thema als we dit zelf aan een ander kunnen uitleggen. *"Het idee achter agency/HackShield is ze 95% onthouden van wat we uitleggen. Door kinderen te motiveren de thema's te bespreken met bijvoorbeeld ouders/grootouders, zullen ze meer onthouden van wat ze in de klassenquests hebben geleerd".* HackShield heeft dus als doel om kinderen niet alleen iets te leren van een bepaald thema, maar ook om hen te motiveren het geleerde aan een ander uit te leggen in zijn of haar directe omgeving.

5. **Het creëren van trots en engagement**

   Ook stelt HackShield zichzelf als doel om kinderen het gevoel te geven onderdeel uit te maken van een unieke beweging die zorgt voor een veiligere digitale wereld. Ze willen kinderen enthousiasmeren en voor de langere termijn binden aan HackShield. Zo werd door medewerkers gezegd: *"We willen dat kinderen trots zijn om onderdeel uit te maken van deze beweging en met trots over dit thema vertellen", "We willen dat kinderen zich onderdeel voelen van HackShield en dat ze het spel willen blijven spelen"* en *"We willen de aandacht vasthouden door bijvoorbeeld het bieden van een goed verhaal (storytelling)".*

6. **Het vergroten van de ervaren verantwoordelijkheid**

   De quests van HackShield hebben volgens medewerkers ook als doel om kinderen meer verantwoordelijkheid te laten ervaren voor veilig online gedrag. Het idee is dat kinderen door het spelen van de verschillende quests leren dat zij zelf verantwoordelijk zijn voor hun gedrag op het internet en dat ze zelf goede keuzes kunnen maken. Zo gaf een medewerker aan: *"Door met kinderen te werken aan deze thema's, willen we ze een gevoel van verantwoordelijkheid meegeven. Zij kunnen hier iets tegen doen/hier iets aan veranderen".*

7. **Het tegengaan van impulsiviteit en impulsieve online gedragingen**

Als laatste, belangrijke punt werd genoemd dat HackShield met de verschillende quests de impulsiviteit van kinderen op het internet wil tegengaan. Veel onveilig online gedrag komt volgens HackShield voort uit snel en impulsief handelen. Door het spelen van de quests zouden kinderen gestimuleerd moeten worden om minder impulsief te handelen. Zo werd aangegeven: *"Kinderen reageren over het algemeen heel impulsief. Het doel van HackShield is om deze impulsiviteit tegen te gaan. Eerst denken, dan doen".*

2.4 Beschrijving van HackShield in de klas

Voor dit effectonderzoek richten we ons – zoals eerder toegelicht - op de klassenquest 'Online Grenzen'. Deze klassenquest richt zich op twee verschillende thema's, namelijk (I) online pesten en (II) hacken. In deze klassenquest komen leerlingen erachter wat hacken is, wat de gevolgen kunnen zijn van cyberpesten en welke keuzes je kunt maken (HackShield, z.d.). De klassenquest draait om Sanne. Sanne gaat op oorlogspad, want ze wordt gepest en zet hacken in om de pesters terug te pakken. Ze komt er gedurende de quest samen met de klas achter dat dit niet de beste manier is om pesten tegen te gaan, maar dat ze haar vaardigheden als hacker wel op een goede manier zou kunnen gebruiken (HackShield, z.d.).

De lesdoelen van deze quest die door HackShield zijn geformuleerd zijn als volgt:

Cyberpesten[1]

Leerlingen weten…

- Wat ze zelf kunnen doen wanneer ze online gepest worden.
- Dat online pesten, net als offline pesten, grote gevolgen kan hebben.
- Dat de rol van toeschouwers heel belangrijk is als het gaat om online pesten, en dat je daarin ook een verantwoordelijkheid hebt.

Hacken

Leerlingen weten…

- Dat je als hacker kunt besluiten om je het goede of slechte pad op te gaan.
- Welke gevolgen/consequenties hacken kan hebben voor henzelf en voor slachtoffers.
- Hoe ze hun digitale skills veilig en op een goede manier kunnen inzetten.
- Wat cybercrime inhoudt.

De volledige beschrijving van lesdoelen van deze klassenquest is terug te vinden in Bijlage 1.

[1] Cyberpesten en online pesten worden beide gebruikt door HackShield. In dit rapport wordt online pesten gebruikt.

De klassenquest is een interactieve game. De klas kan zelf kiezen welk antwoord wordt gegeven op de vragen van Sanne over online pesten en hacken. De keuzes die de kinderen hierin maken hebben echter geen invloed op het verloop van het spel. Een letterlijk voorbeeld uit de quest:

Sanne vraagt om hulp, omdat een klasgenoot 'nare berichten' naar haar stuurt.

Sanne wordt online gepest, ze vraagt de klas wat ze moet doen. De klas kan kiezen uit 2 antwoordmogelijkheden, namelijk 1) laat het gaan en 2) reageren! Wanneer de klas kiest voor antwoord 1 (laat het gaan), dan zegt Sanne: "Jullie hebben gelijk… denk ik." En dan zegt ze: "Nee, ik laat niet over mij heenlopen en ik weet hoe we hem gaan aanpakken, kom mee!" Wanneer de klas dit geval kiest voor antwoord 2 (reageren!), dan is de reactie van Sanne: "Goed idee! Wat zullen we terugzeggen?".

In de klassenquest 'Online grenzen' staat de uitkomst en het verloop van het spel dus vooraf vast. De antwoorden die leerlingen geven op de verschillende vragen zijn daarmee *niet* van invloed op het spelverloop. Het doorlopen van de klassenquest duurt ongeveer 45 minuten, waarbij verschillende vragen worden gesteld aan de klas en er stellingen worden behandeld die gaan over zowel cyberpesten als hacken. De klassenquest wordt begeleid door de leerkracht zelf of door een gastdocent die via HackShield door leerkrachten kunnen worden aangevraagd. Zie Bijlage 1 voor de volledige uitwerking van de klassenquest.

3. Literatuurstudie

In deze literatuurstudie is gekeken naar theoretische modellen die zich richten op het verklaren van zogenaamd weerbaar gedrag. Er zijn in de afgelopen tientallen jaren verschillende theoretische modellen ontwikkeld die antwoord proberen te geven op de vraag: “Waarom vertonen mensen in bepaalde situaties al dan niet weerbaar (of zelfredzaam) gedrag” (Rogers, 1975; Witte & Allen, 2000). Bijvoorbeeld in de onderzoeksagenda van het expertisenetwerk Cyberweerbaar NL (CWNL) wordt verwezen naar de volgende theorieën (Leukfeldt et al., 2025): Protection Motivation Theory (Rogers, 1975); Theory of Planned Behavior (Ajzen, 1991); Health Belief Model (Maiman & Becker, 1974); Extended Parallel Processing Model (Witte, 1992) en het Risk Information Seeking & Processing Model (Griffin et al., 1994) en meer recentelijk het COM-B-model (Michie et al., 2011).

Inzicht in factoren die bijdragen aan het vergroten van weerbaarheid (zowel in het algemeen als specifiek gericht op de online context), kan ons helpen bij het verklaren waarom bepaalde interventies die als doel hebben de (online) weerbaarheid te vergroten succesvol zijn (of niet). Door in kaart te brengen welke variabelen in de literatuur worden beschreven als belangrijke voorspellers voor (online) weerbaarheid, kan enerzijds gekeken worden in hoeverre deze variabelen terugkomen in interventies en kunnen deze variabelen anderzijds gebruikt worden voor het opstellen van een valide meetinstrument.

In deze literatuurstudie zal allereerst worden gekeken naar theoretische modellen die inzicht geven in weerbaarheid in de brede zin van het woord. Daarna wordt gekeken naar modellen en variabelen zie zich specifiek richten op de online context. Tenslotte wordt er gekeken naar de variabelen *agency*, verantwoordelijkheid en impulsiviteit, aangezien deze variabelen in de interviews met HackShield werden genoemd als belangrijk onderdelen van de interventie.

Deze literatuurstudie wordt tot slot gebruikt voor het uitvoeren van een gedegen kwalitatieve inhoudsanalyse van de klassenquest ‘Online Grenzen' en voor het opzetten van een meetinstrument om het effect van deze klassenquest te meten in deze effectmeting.

3.1 Gedragsverandering

In de afgelopen decennia is er veel onderzoek gedaan naar redenen voor risicovol gedrag vertoont door mensen en onder welke voorwaarden zij zich beschermen tegen dreigingen en risicovolle situaties. In de jaren ‘70 van de vorige eeuw is hiermee een start gemaakt binnen de communicatiewetenschappen waarin gedacht werd dat angst- en dreigingscommunicatie (bijvoorbeeld in voorlichtingscampagnes over roken) zou leiden tot gezonder en veiliger gedrag. Maar de uitkomsten van deze onderzoeken lieten zien

dat juist het tegenovergestelde werd bereikt. In plaats van hun gedrag te veranderen, werd gezien dat mensen juist de waarschuwingen negeerden, de risico's bagatelliseerden of zich juist heel machteloos gingen voelen en hun gedrag niet veranderden (Ruiter, Kessels, Peters & Kok, 2024).

Als reactie hierop werd in 1975 de Protection Motivation Theory (PMT) ontwikkeld (Rogers, 1975). Deze theorie is ontwikkeld om te verklaren waarom mensen beschermend gedrag vertonen in reactie op dreiging, en waarom zij dat juist niet doen, zelfs wanneer zij weten dat er risico's zijn. De theorie stelt dat de motivatie om beschermend gedrag te vertonen voortkomt uit twee cognitieve beoordelingsprocessen: dreigingsinschatting en copinginschatting. Dreigingsinschatting (risicoperceptie) omvat de waargenomen ernst van een dreiging en de waargenomen persoonlijke kwetsbaarheid. Hier wordt een eerste inschatting gemaakt van het gevaar waarmee iemand te maken krijgt door te beoordelen of de dreiging ernstig is voor de persoon in kwestie (waargenomen ernst) en of diegene ook denkt zelf kwetsbaar te zijn voor dit risico (waargenomen kwetsbaarheid). De copinginschatting heeft betrekking op de verwachte effectiviteit van beschermende maatregelen (responseffectiviteit) en het vertrouwen in het eigen vermogen om deze maatregelen toe te passen (zelfeffectiviteit). Beschermend gedrag is volgens de PMT het meest waarschijnlijk wanneer individuen een dreiging als ernstig en persoonlijk relevant beschouwen, geloven dat beschikbare maatregelen effectief zijn en zichzelf in staat achten deze uit te voeren.

Volgens de PMT (Rogers, 1975) moet een effectieve interventie om risicovol gedrag te veranderen dus bestaan uit *zowel* het verduidelijken van het risico/de dreiging *alsmede* het geven van heldere handelingsperspectieven waarin duidelijk wordt geschetst wat iemand kan doen om de dreiging te verminderen. Het vergroten van de risicoperceptie van een individu en het vergroten van hun verwachting iets aan deze dreiging te kunnen doen (in de vorm van handelingsperspectieven), zorgt voor meer zelfbeschermend en weerbaar gedrag (Rogers, 1975; Kievik, 2017). Deze bevindingen zijn in veel verschillende studies naar een verscheidenheid aan risico-onderwerpen bevestigd (Kievik, 2017; Misana-ter Huurne et al., 2020; Witte & Allen, 2000).

3.2 Gedragsverandering cyberweerbaarheid

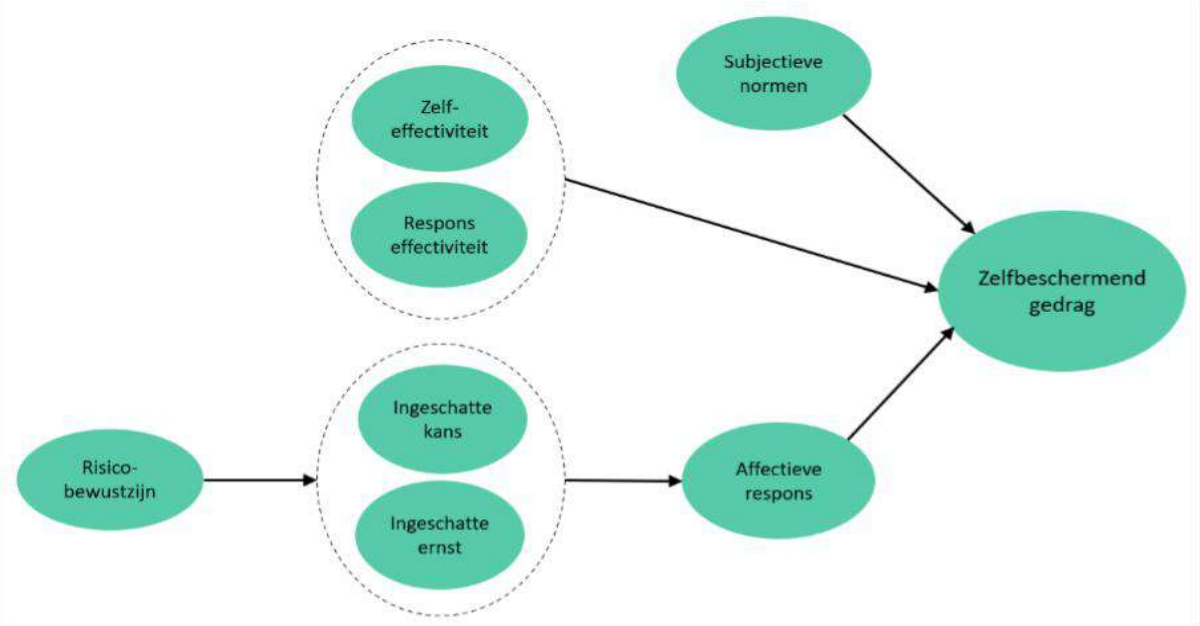
De afgelopen jaren is meer onderzoek gedaan naar cyberweerbaarheid, waarin ook steeds meer aandacht komt voor cyberweerbaarheid onder kinderen (Vissenberg & d'Haenens, 2020). De toenemende digitalisering van de samenleving heeft ertoe geleid dat kinderen steeds vaker online actief zijn, zowel voor school en sociale interacties als voor ontspanning. Hierdoor worden zij op jonge leeftijd blootgesteld aan diverse cyberdreigingen, zoals phishing, online pesten, identiteitsfraude en desinformatie (Vissenberg

et al., 2022). Hoewel technologische beveiligingsmaatregelen zoals firewalls en filters belangrijk zijn, zijn deze alleen niet voldoende om kinderen effectief te beschermen. Menselijk gedrag speelt een cruciale rol: kinderen moeten niet alleen risico's herkennen, maar ook leren hoe ze veilig en verantwoordelijk online kunnen handelen. Daarom is er groeiende wetenschappelijke aandacht voor het vergroten van cyberweerbaarheid bij kinderen, dat wil zeggen het vermogen om digitale dreigingen te signaleren, erop te reageren en veilig gedrag te vertonen (Kievik, 2017; Hammond, Polizzi & Bartholomew, 2022).

Spithoven (2020) heeft als reactie op de toename van cyberdreiging een raamwerk ontwikkeld voor het begrijpen, meten en vergroten van cyberweerbaarheid onder mensen: het *cyberweerbaarheidsmodel* (Spithoven, Misana-ter Huurne & van Houten, 2022). Dit model dient als (wetenschappelijke) basis en als leidraad voor het inzichtelijk maken van de factoren die een rol spelen bij de (intenties tot) zelfbeschermend gedrag met betrekking tot cyberweerbaarheid (Figuur 3). Dit model is afgeleid van de PMT van Rogers (1975) en richt zich specifiek op cyberweerbaar gedrag met als doel een handreiking te bieden voor het effectief ontwikkelen van interventies om de weerbaarheid (van onder meer kinderen) te vergroten.

Figuur 3

Cyberweerbaarheidsmodel



Noot. Afgeleid van Spithoven, Misana-ter Huurne & Van Houten, 2022 en Spithoven 2020, p. 65

Volgens Spithoven (2020) en Misana-ter Huurne e.a. (2020) kan cyberweerbaarheid worden gedefinieerd als “De combinatie van een voldoende hoge mate van risicobewustzijn en zelfbeschermend gedrag onder burgers en ondernemers om slachtofferschap van cybercriminaliteit te voorkomen en/of mogelijke impact te voorkomen of verkleinen” (p. 65).

De uitdaging bij het ontwerpen van effectieve interventies is het bevorderen van het risicobewustzijn en het preventief gedrag om zowel slachtofferschap als daderschap onder de doelgroep te voorkomen. Het doel hierbij is om kinderen daadwerkelijk in staat te stellen en te stimuleren om zichzelf (beter) te beschermen. Hiervoor zijn een aantal aspecten belangrijk, in lijn met de voorspellers uit de PMT. Zij moeten: (1) weten (risicobewustzijn); (2) willen (perceptie eigen verantwoordelijkheid); (3) kunnen (zelfeffectiviteit) en (4) doen (gedrag). Hierbij doorlopen individuen vier inschattingsstadia: (1) Inschatting van de eigen kwetsbaarheid ten opzichte van het gevaar; (2) Inschatting van de ernst van de dreiging en gevolgen daarvan; (3) Inschatting van de effectiviteit van het aanbevolen gedrag; (4) Inschatting van de eigen effectiviteit (de mate waarin een persoon zichzelf in staat acht het aanbevolen gedrag uit te kunnen voeren).

Stadia 1 en 2 vormen samen de waargenomen dreiging of risicoperceptie. Stadia 3 en 4 vormen samen de effectiviteitsverwachting. Volgens verschillende theorieën zijn mensen geneigd het preventieve gedrag uit te voeren wanneer *zowel* de waargenomen dreiging *als* de effectiviteitsverwachting als hoog worden ingeschat. Met andere woorden: een individu moet het idee hebben dat hij/zij vatbaar is voor het risico en dit risico als ernstig inschatten. Daar komt nog bij dat het individu het idee moet hebben dat hij/zij het aanbevolen gedrag kan uitvoeren en dat het nuttig is dit gedrag te gaan uitvoeren. Wanneer één van deze factoren door het individu als (te) laag wordt ingeschat, dan is de kans klein(er) dat het individu over zal gaan tot het uitvoeren van preventief gedrag dat wordt geadviseerd.

Als aanvulling op PMT, richt het cyberweerbaarheidsmodel zich ook op de variabelen affectieve respons en subjectieve normen. Uit onderzoek blijkt dat – specifiek voor het thema cyberweerbaarheid en de doelgroep kinderen in het primair onderwijs – aanvullende variabelen een rol spelen in het verklaren van zelfbeschermend gedrag (Bekkers et al., 2023; De Kimpe et al., 2022; Kievik, 2017).

Affectieve respons is de emotionele reactie die iemand ervaart op een bepaalde risicovolle gebeurtenis. Waar risicoperceptie voornamelijk draait om een meer rationele afweging van kansen en gevolgen, richt affectieve respons zich op de emoties die iemand voelt bij een bepaald risico, nog voordat er een rationele afweging kan worden gemaakt (Bekkers et al., 2023; Slovic, 2004; Slovic & Peters, 2006). Wanneer iemand veel angst ervaart rondom een bepaald risico maar niet goed weet wat hij of zij hiertegen kan doen, dan is diegene minder snel geneigd om zichzelf actief te gaan beschermen tegen dit

risico (Witte, 1992). De ervaren angst zonder concreet handelingsperspectief leidt tot vermijdend gedrag in plaats van weerbaar gedrag. Ander emotionele reacties kunnen juist leiden tot meer zelfbeschermend gedrag. Uit een onderzoek van Farshadkhah et al. (2021) bleek dat schaamte ervoor kan zorgen dat meer werknemers zich houden aan cybermaatregelen binnen organisaties en uit onderzoek van Jenkins et al. (2014) kwam naar voren dat het regelmatig waarschuwen van werknemers helpt bij het voorkomen van cyberincidenten op de werkvloer. Deze onderzoeken laten zien dat de emotionele reactie van iemand op een bepaald risico van invloed is op het uiteindelijke gedrag.

Subjectieve normen worden in de literatuur omschreven als de mate waarin iemand het gevoel heeft dat belangrijke anderen verwachten dat hij of zij bepaald gedrag vertoont (Ajzen, 1991; Bandura, 1977). Subjectieve normen blijken een belangrijke rol te spelen in het verklaren van verschillende type gedragingen, zoals roken (Sunstein, 1996) en alcoholgebruik (Neighbors et al., 2007). Meer recent onderzoek laat zien dat subjectieve normen ook een belangrijke voorspeller zijn van cyberweerbaarheid (Bekkers et al., 2023). Vooral onder kinderen is de invloed van leeftijdsgenoten groot. In een onderzoek onder basisschoolkinderen van groep 7 en 8 in Oost-Nederland naar de (cyber)weerbaarheid van kinderen bleek dat de subjectieve normen de belangrijkste voorspellers zijn voor hun eigen (cyber)weerbare gedrag. Kinderen die het gevoel hadden dat hun *peers* het belangrijk vinden om veilig en zelfbeschermend gedrag te vertonen, zijn significant vaker geneigd dit zelf ook te doen (Kievik, 2017). De subjectieve normen lijken daarmee een belangrijke voorspeller voor cyberweerbaargedrag onder kinderen.

3.3 *Agency* en verantwoordelijkheid

HackShield heeft als doel om kinderen die onderdeel worden van de HackShield community niet alleen meer cyberweerbaar te maken, maar ook om ze op te laten treden als ‘cyber agents’. Daarmee wordt bedoeld dat de kinderen die deelnemen aan HackShield worden gestimuleerd om hun ervaringen en kennis over cyberveiligheid te delen met volwassenen in hun directe omgeving, zoals ouders, grootouders en leerkrachten. Dit noemen zij *agency.* Een belangrijk doel van HackShield is om deze *agency* te vergroten en kinderen dus het idee achter HackShield verder te laten uitdragen binnen de samenleving (HackShield, z.d.).

Agency verwijst volgens de wetenschappelijke literatuur naar het vermogen van een kind om actief keuzes te maken, controle uit te oefenen over zijn of haar handelen, en invloed uit te oefenen op de omgeving. Het gaat dus om het besef dat je zelf kunt handelen om iets te bereiken of te veranderen (Bandura, 1997, 2001; Paris & Lung, 2008), in plaats van dat alles je overkomt (Deci & Ryan, 1995). De rol van het individu in het creëren van zijn of haar eigen ervaringen in de wereld is een actief proces, waarin

mensen *'agents of experiences rather than simply undergoers of experiences'* zijn (Bandura, 2001, p. 4). De insteek van *agency* van de ontwikkelaars van HackShield wijkt dus iets af van hoe hier in wetenschappelijke zin over wordt geschreven, maar de kern zit in de activatie voor het uitdragen van urgentie en kennis.

Er bestaat een zekere onzekerheid over de mate waarin jonge kinderen *agency* zouden kunnen hebben. In het bijzonder is er wetenschappelijke scepsis over hun vermogen tot zelfregulatie en zelfreflectie (Mullin, 2007; Paris & Lung, 2008). Dit perspectief sluit aan bij traditionele discoursen die kinderen zien als onbekwaam en onvolwassen (Woodhead, 2006), of als 'human becomings, not human beings' (Coady, 2008, p. 4). De afgelopen jaren wint een meer hedendaagse, sociaal-constructivistische visie op het kind als een zeer bekwame mede-constructeur van zijn eigen leeromgeving en omgeving echter ook wetenschappelijk aan momentum (bijv. Ahn, 2011; Arthur et al, 2008). Duidelijk is wel dat om *agency* te hebben, kinderen een bepaalde mate van ervaren verantwoordelijkheid nodig hebben.

3.4 Impulsiviteit

Er zijn verschillende variabelen gerelateerd aan slachtofferschap van vormen van cybercriminaliteit, zoals hacking, phishing, online oplichting en identiteitsfraude. Onderzoek laat zien dat vooral jonge mensen die veel tijd spenderen op het internet en impulsief handelen sneller slachtoffer worden van cybercriminaliteit (Van de Weijer & Leukfeldt, 2017). Ander onderzoek laat zien dat er verschillende karaktereigenschappen zijn die positief samenhangen met het risico om slachtoffer te worden van cybercriminaliteit, zoals openheid, extraversie, een gebrek aan zelfcontrole, impulsiviteit en neuroticisme (Halevi, Lewis & Memon, 2013). Vooral kinderen handelen vaak snel, zonder goed na te denken over de gevolgen hiervan (Vannucci et al., 2020; Roozendaal, 2026). Daardoor klikken zij sneller op een link, delen zij vaker (en vaak onbewust) persoonlijke informatie en doen zij sneller mee aan risicovolle gedragingen zoals het downloaden van illegale bestanden. Zij lopen dus meer gevaar online (Vannucci et al., 2020). Het tegengaan van impulsief handelen onder kinderen kan dus zorgen voor minder risicovol gedrag.

3.5 Conceptuele afbakening 'cyberweerbaarheid'

Er bestaat in de wetenschappelijke literatuur geen eenduidige definitie van wat cyberweerbaarheid is. Wel zien we dat er overeenstemming is dat dit concept verder gaat dan enkel de reactie op een online incident, maar ook een preventieve kant kent: weten welke risico's er spelen en hoe je daartegen te beschermen (zie ook Leukfeldt et al., 2025). Het Nationaal Cyber Security Center definieerde

cyberweerbaarheid als (NCSC, 2022, p. 9) ‘het vermogen om (relevante) risico’s tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken’.

Weerbaarheid is duidelijk een holistisch begrip (Hillmann & Guenther, 2021). Alle stappen van de veiligheidsketen worden in het concept van weerbaarheid met elkaar verbonden: proactie, preventie, preparatie, repressie en herstel (De Pauw, Deprins & Spithoven, 2022). Daarbij beweegt cyberweerbaarheid als concept ook weg van de klassieke opvatting dat de mens de zwakste schakel is in cybersecurity en wordt de mens juist als de cruciale, sterke schakel in cybersecurity gezien. Deze positieve benadering (Zimmermann & Renaud, 2019; Spithoven et al., 2024) sluit aan op de insteek van HackShield in de Klas richting de kinderen die hun quest spelen, zij zijn de cyberhelden van morgen.

Op basis van de voorgaande theoretische verkenning en de doelstellingen van HackShield ten aanzien van cyberweerbaarheid, vatten wij ‘cyberweerbaarheid’ in dit onderzoek op als het samenkomen van de volgende kenmerken om slachtofferschap van cyberincidenten te kunnen voorkomen en de schade daarvan te kunnen beperken:

1. kennis;
2. risicoperceptie;
3. zelfeffectiviteit;
4. responseffectiviteit;
5. subjectieve normen;
6. gedragsintentie;
7. agency;
8. verantwoordelijkheid;
9. impulsiviteit.

4. Methode van onderzoek

In dit hoofdstuk beschrijven we de methoden waarmee de effectiviteit van de quest 'Online grenzen' van HackShield in de Klas door de onderzoekers is vastgesteld. Er is hierbij gekozen voor zowel een kwalitatieve als een kwantitatieve onderzoeksmethode. Enerzijds is er op basis van de literatuurstudie gekeken naar de wijze waarop HackShield invulling heeft gegeven aan de quest 'Online Grenzen' en op welke wijze de in de literatuur beschreven onderdelen van cyberweerbaarheid terugkomen. Anderzijds is door middel van vragenlijstonderzoek – middels een voor- en nameting - geëvalueerd in hoeverre de quest 'Online grenzen' bijdraagt aan de online weerbaarheid en *agency* van de onderzochte deelnemers.

4.1 Kwalitatieve inhoudsanalyse 'Online grenzen'

Op basis van de variabelen uit de literatuurstudie (zie Hoofdstuk 3) die hiervoor zijn beschreven wordt gekeken naar de mate waarin de inhoud van de quest 'Online grenzen' resoneert met belangrijke onderdelen van cyberweerbaarheid. Ook wordt er gekeken naar de wijze waarop er door HackShield in deze klassenquest invulling is gegeven aan deze variabelen. Het doel hiervan is om – samen met de effectmeting die in dit onderzoek wordt gedaan – inzicht te geven in de sterke kanten van deze quest alsmede het identificeren van eventuele verbeterpunten.

Voor de kwalitatieve analyse is er gekeken naar onderdelen van cyberweerbaarheid op basis van de geraadpleegde, wetenschappelijke literatuur (risicoperceptie, zelfeffectiviteit, responseffectiviteit, subjectieve normen). Dit is aangevuld met de variabelen die terugkwamen in de interviews met de ontwikkelaars van HackShield in de Klas (*agency*, verantwoordelijkheid en impulsiviteit). Ook is gekeken naar de mate waarin de kennis over de twee onderwerpen (online pesten en hacken) werd vergroot in deze quest.

4.1.1 Operationalisering en werkwijze

De kwalitatieve analyse is onafhankelijk van elkaar door drie onderzoekers van het lectoraat Online Weerbaarheid van Hogeschool Saxion uitgevoerd. Deze keuze is gemaakt om de betrouwbaarheid van deze inhoudsanalyse te vergroten. Voor deze kwalitatieve analyse is er allereerst een volledig transcript gemaakt van de klassenquest (zie Bijlage 4). In dit transcript is woord voor woord uitgeschreven welke stappen deelnemers doorlopen tijdens de quest en welke feedback zij krijgen op keuzes die zij tijdens de quest maken. Naast de tekst zijn - gezien de interactieve aard van de quest - ook de visuele stimuli (Rose,

2001) die terugkomen in de quest door de onderzoekers meegenomen in het codeerproces (Saldana, 2012). Er is onderscheid gemaakt tussen delen van de quest die specifiek ingaan op online pesten en delen van de quest die zich richten op hacken. Dit transcript werd door de onderzoekers onafhankelijk van elkaar geanalyseerd en gecodeerd, waarbij de onderstaande operationalisering van begrippen als codes werden aangehouden (Tabel 1), om zo de validiteit van de inhoudsanalyse te waarborgen.

Tabel 1.

Operationalisering begrippen voor de kwalitatieve analyse

Begrip	**Definitie ***
Kennis	Specifieke onderdelen in de quest die bijdragen aan het vergroten van kennis over online pesten en hacken.
Risicoperceptie	De gepercipieerde ernst van en vatbaarheid voor een bepaald risico.
Zelfeffectiviteit	De mate waarin iemand het gevoel heeft zelf in staat om zichzelf te beschermen tegen een bepaald risico.
Responseffectiviteit	De mate waarin iemand het gevoel heeft dat aangedragen handelingsperspectieven nuttig zijn in het verminderen van een risico.
Subjectieve normen	De perceptie van een individu over wat een ander van hem/haar verwacht ten aanzien van zelfbeschermend gedrag.
Agency	De mate waarin iemand keuzes maakt en doelgericht handelt (bijvoorbeeld in het uitdragen van cyberweerbaarheid).
Verantwoordelijkheid	De mate waarin iemand zichzelf verantwoordelijk acht in het nemen van zelfbeschermende maatregelen.
Impulsiviteit	De mate waarin iemand nadenkt voordat hij/zij een besluit neemt.

Noot: *Definities op basis van literatuur beschreven in de literatuurstudie in hoofdstuk 3. Gedragsintenties worden besproken onder zelfeffectiviteit en responseffectiviteit in deze inhoudsanalyse.

Na het afzonderlijk doorlopen van de klassenquest door de drie onderzoekers, zijn hun coderingen in een gezamenlijke sessie met elkaar vergeleken. Onderdelen die door hen verschillend waren gecodeerd, zijn nogmaals gezamenlijk beoordeeld, totdat er consensus was over de inhoud van de quest. Hierbij zijn de richtlijnen voor gezamenlijk coderen van Saldana (2012) aangehouden.

4.2 Vragenlijsten

Er zijn twee vragenlijsten gebruikt om de effectiviteit van de interventie te kunnen onderzoeken: (1) een vragenlijst die *voor* het spelen van de klassenquest 'Online grenzen' is afgenomen en (2) een vragenlijst die *daarna* is afgenomen. Oorspronkelijk was het idee om daarbij ook te werken met een controleconditie;

volgens het zogenaamde 'voormeting-nameting-controlegroep-ontwerp' (Quené & van den Bergh, 2026). Gezien de grote uitdaging die er gedurende dit project was om voldoende respondenten te werven en de lange doorlooptijd van het onderzoek (start dataverzameling 10 november 2025; einde dataverzameling 20 maart 2026), bleek het niet haalbaar om een controleconditie in te zetten. Dit was enerzijds omdat simpelweg alle respondenten nodig waren voor de effectmeting en anderzijds omdat een controleconditie alleen zinvol is als de voor- en nameting doorgevoerd kan worden op *hetzelfde* moment als de voor- en nameting van de experimentele conditie. Die controle hadden wij niet door onze afhankelijkheid van leerkrachten. Daarom is er door de onderzoekers voor gekozen om te werken met enkel een voor- en nameting bij de conditie die tevens de interventie (het spelen van de klassenquest 'Online grenzen') heeft ondergaan; hierbij is concreet teruggevallen op het zogenaamde 'één-groep-voormeting-nameting-ontwerp' (Quené & van den Bergh, 2026).

4.2.1. Vragenlijst voor effectiviteitsmeting

Voorafgaand aan en ongeveer twee weken na het spelen van de quest 'Online grenzen' is een online vragenlijst met behulp van Qualtrics[2] onder de deelnemende leerlingen afgenomen (zie Bijlage 3). De deelnemende leerlingen konden deze via een link of QR-code openen en op hun telefoon of laptop invullen. Mede vanwege de potentiële gevoeligheid van de onderwerpen 'online pesten' en 'hacken' is op uitdrukkelijk advies van de Saxion Ethische Advies Commissie (SEAC) de deelnemers *volledige anonimiteit gewaarborgd*. Hierom is door de onderzoekers *niet* gewerkt met een extra registratie om de voor- en nameting van een deelnemer aan elkaar te kunnen koppelen. Voor de voor- en nameting zijn twee verschillende vragenlijsten ontwikkeld, die inhoudelijk nagenoeg identiek waren. In de nameting zijn een aantal vragen toegevoegd om te kijken of leerlingen de klassenquest inderdaad hadden gespeeld, of ze zich dit nog goed konden herinneren en wat hun mening over deze quest was.

De instructie aan de docenten was om de vragenlijst ongeveer een week voor het spelen van de quest 'Online grenzen' in te laten vullen door de leerlingen op school. Voor de nameting gold een soortgelijke instructie: ongeveer een tot twee weken na het spelen van de quest werd de vragenlijst voor de nameting afgenomen op school in de klas. Vanwege de potentiële gevoeligheid van de vragen en de jonge doelgroep is er – wederom op advies van de Saxion Ethische Advies Commissie (SEAC) - voor gekozen om bij elke vraag de deelnemers meerdere, zogenaamde uitvluchtopties te geven ("weet ik niet", "zeg ik liever niet", "niet van toepassing").

[2] www.qualtrics.com

De vragenlijst is gebaseerd op de constructen uit het theoretisch kader (zie paragraaf 3.2), en afgeleid van de vragenlijst gebruikt in een eerder onderzoek naar weerbaarheid onder basisschoolleerlingen (zie ook: Kievik, 2017). Gezien de doelgroep van dit onderzoek (9 - 12 jaar) is het aantal vragen om de constructen te meten tot een minimum ingeperkt, en is het taalgebruik voor zover mogelijk aangepast aan de doelgroep. De eindversie van de vragenlijst is uitvoerig getest onder kinderen die tot de doelgroep behoren, om zo de begrijpelijkheid van de vragen te borgen.

4.2.2. Variabelen

Op basis van het theoretisch kader zijn de volgende concepten in het onderzoek gemeten:

1. Kennis;
2. Risicoperceptie;
3. Behavioral beliefs:
    a. zelfeffectiviteit (uitvoerbaarheid) en
    b. responseffectiviteit (beoordeeld nut).
4. Subjectieve normen ten aanzien van zelfbeschermend gedrag;
5. Gedragsintenties.

Op basis van de interviews met leden van HackShield zijn hieraan nog een aantal variabelen toegevoegd:

6. *Agency*;
7. Verantwoordelijkheid;
8. Impulsiviteit.

In de nameting is vervolgens gemeten hoe de klassenquest ‘Online grenzen’ door de deelnemers is ervaren:

9. Subjectief effect van de interventie: hoe de interventie is ervaren.

De vragenlijst bestond voornamelijk uit Likert-type schalen met items (stellingen en vragen) die de onderzoeksconcepten meten. De schalen zijn getoetst op hun betrouwbaarheid, berekend met Cronbachs alpha.

1. Kennis

Kennis is gemeten aan de hand van vijf waar/niet waar vragen over cyberpesten (bijvoorbeeld: *"Als je online gepest wordt, dan kun je daar niks tegen doen")* en zes waar/niet waar vragen over hacken (bijvoorbeeld: *"Wanneer je inlogt op het account van iemand anders, dan ben je aan het hacken").* Kinderen hadden hierbij steeds de mogelijkheid om 'weet ik niet' in te vullen als zij bepaalde begrippen niet kenden.

2. Risicoperceptie

De inschatting van het effect van het risico van online pesten en hacken is gemeten aan de hand van vier stellingen. Voor online pesten is aan deelnemers de volgende fictieve situatie voorgelegd: *"Sam zit in een groepsapp met de hele klas. Er worden nare dingen over Sam gezegd in de app en sommige kinderen lachen daarom [let op: Sam is een verzonnen persoon]".* Vervolgens is gevraagd hoe kinderen zich in deze situatie zouden voelen in vier verschillende stellingen (gespannen, veilig, bang, verdrietig), gemeten op een vijfpuntsschaal met antwoordcategorieën van 'helemaal niet (1) tot 'heel erg' (5). Voor hacken zijn dezelfde vragen gesteld aan de hand van de volgende fictieve situatie: *"Bo is aan het hacken. Bo gebruikt stiekem het Instagram- en TikTok-account van andere kinderen. Bo plaatst daar zelf berichten (bv. teksten, plaatjes, filmpjes), en verwijdert daar ook berichten. [Let op: Bo is een verzonnen persoon]".*

De inschatting van de kans van het risico op online pesten en hacken is gemeten aan de hand van de stelling: *"Wat er met Sam gebeurt in dit voorbeeld, zou ook kinderen in mijn klas kunnen overkomen"* (voor online pesten) en *"Wat er met Bo gebeurt in dit voorbeeld, zou ook kinderen in mijn klas kunnen overkomen*" (voor hacken). Dit is gemeten op een vijfpuntsschaal met antwoordcategorieën van 'helemaal mee oneens' (1) tot 'helemaal mee eens' (5). Een aparte categorie 'weet ik niet' was hieraan toegevoegd.

3. Behavioral beliefs

Zelfeffectiviteit

Zelfeffectiviteit is gemeten met behulp van vier stellingen voor online pesten en drie stellingen voor hacken. Voor online pesten werden de volgende casus voorgelegd: *"Stel: jij zit in de groepsapp van de klas van Sam en je ziet dat er nare berichten over Sam worden verstuurd. Geef aan in hoeverre je het eens bent met de volgende stellingen."* Vervolgens is in vier verschillende stellingen gevraagd in hoeverre deelnemers er vertrouwen in hebben dat ze in dit geval om hulp kunnen vragen of dit gedrag een halt kunnen toeroepen. Voor hacken werden de volgende stellingen voorgelegd:

- *"Ik heb er vertrouwen in dat ik een goed wachtwoord kan bedenken"*
- *"Ik heb er vertrouwen in dat ik voor verschillende accounts verschillende wachtwoorden kan aanmaken"*
- *"Ik heb er vertrouwen in dat ik mijn wachtwoorden voor mijzelf kan houden (mijn wachtwoorden dus nooit met iemand anders deel)".*

Antwoordcategorieën varieerden voor zowel online pesten als hacken van 'helemaal mee oneens' (1) tot 'helemaal mee eens' (5) op een vijfpuntsschaal. Een aparte categorie 'weet ik niet' was hieraan toegevoegd.

Responseffectiviteit

Responseffectiviteit is gemeten aan de hand van zes stellingen voor online pesten en drie stellingen voor hacken. Voor online pesten is wederom de casus van Sam voorgelegd: *"Stel: jij zit in de groepsapp van de klas van Sam en je ziet dat er nare berichten over Sam worden verstuurd".* Vervolgens is voor zes verschillende gedragingen (bijvoorbeeld *"tegen de juf of meester zeggen dat er nare dingen over Sam worden gedeeld"*) gemeten in hoeverre deelnemers het gevoel hebben dat dit zinvol zou kunnen zijn om het gedrag van Sam halt toe te roepen op een vijfpuntsschaal van (1) helemaal niet tot (5) heel erg veel. Voor hacken is de volgende casus voorgelegd: *"Stel, je wilt je goed beschermen tegen hackers."*. Vervolgens is voor drie verschillende gedragingen (bijvoorbeeld *"meerdere wachtwoorden bedenken voor verschillende accounts"*) gemeten in hoeverre deelnemers het gevoel hebben dat dit zinvol zou kunnen zijn om slachtofferschap van hacken tegen te gaan op een vijfpuntsschaal van (1) 'helemaal niet' tot (5) 'heel erg veel'.

4. Subjectieve normen

Subjectieve normen zijn gemeten met zes items voor online pesten en drie items voor hacken. De voorgelegde casus voor het meten van subjectieve normen was vergelijkbaar met de casus van responseffectiviteit, waarbij ditmaal gevraagd werd naar de inschatting van deelnemers van het gedrag van hun beste vrienden. Voor online pesten werd de vraag gesteld: *"Wat denk je dat jouw beste vrienden zouden doen als zij in een groepsapp zitten waarin nare dingen over Sam worden gedeeld".* Vervolgens werd voor dezelfde zes gedragingen als bij respons effectiviteit gemeten in hoeverre deelnemers dachten dat hun vrienden dit gedrag zouden vertonen. Voor hacken werd de vraag gesteld: *"Wat denk je dat jouw beste vrienden zouden doen om zichzelf te beschermen tegen hackers?".* Vervolgens werd voor dezelfde

drie gedragingen als bij respons effectiviteit gemeten in hoeverre deelnemers dachten dat hun vrienden dit gedrag zouden vertonen. Voor zowel online pesten als hacken werd dit gemeten op een vijfpuntsschaal van (1) 'zeker niet' tot (5) 'zeker wel'.

5. Gedragsintentie

Gedragsintentie is gemeten met vijf items voor online pesten en drie items voor hacken. Voor online pesten werd gevraagd: *"De volgende keer als er iemand in onze groepsapp nare dingen zegt over iemand anders, dan…."* met vijf stellingen over het eigen gedrag zoals: *"zeg ik tegen mijn ouders/verzorgers dat er nare dingen over een klasgenoot worden verstuurd in de groepsapp"* en *"verwijder ik de nare berichten over deze klasgenoot".* Voor hacken werd gevraagd: *"Wat denk je dat jijzelf zou doen om je te beschermen tegen hackers?"* met drie stellingen over het eigen gedrag zoals: *"Ik zou mijn wachtwoord altijd voor mijzelf houden (en dus nooit delen met een ander)".* De stellingen voor zowel online pesten als hacken werden gemeten op een vijfpuntsschaal met antwoordcategorieën van (1) 'zeker niet' tot (5) 'zeker wel'.

6. Agency

Agency is gemeten aan de hand van drie verschillende items. Deze items meten verschillende onderdelen van *agency* en worden daarom apart van elkaar geanalyseerd. De volgende twee stellingen zijn gemeten op een vijfpuntsschaal van (1) 'helemaal mee oneens' tot (5) 'helemaal mee eens':

- *"Ik kan mijn ouders/verzorgen iets leren over veilig internetten"*
- *"Ik kan een gesprek aangaan met volwassenen over veilig internetten"*

De laatste vraag die voorgelegd is aan de deelnemers is: *"Hoe vaak praat je met volwassen in jouw omgeving over veiligheid op het internet*". Deze vraag is gemeten op een vijfpuntsschaal van (1) 'heel weinig' tot (5) 'heel vaak'.

7. Verantwoordelijkheid

Verantwoordelijkheid is gemeten aan de hand van vijf items. Allereerst is gekeken naar de mate waarin deelnemers zichzelf verantwoordelijk houden voor hun eigen veiligheid op het internet. De volgende stelling is aan deelnemers voorgelegd: *"Het is mijn eigen verantwoordelijkheid om mijzelf te beschermen tegen gevaren op het internet".* Daarnaast is deelnemers gevraagd naar de mate waarin zij vinden dat anderen verantwoordelijk zijn voor hun eigen online veiligheid aan de hand van de volgende stellingen:

- *"Mijn ouders/verzorgen zijn ervoor verantwoordelijk om mij te beschermen tegen gevaren op het internet"*

- *"Mijn juf/meester is ervoor verantwoordelijk om mij te beschermen tegen gevaren op het internet"*
- *"De overheid/politie is ervoor verantwoordelijk om mij te beschermen tegen gevaren op het internet"*
- *"Instagram, Tiktok en andere sociale media zijn ervoor verantwoordelijk om mij te beschermen tegen gevaren op het internet".*

Alle items zijn gemeten op een vijfpuntsschaal van (1) 'helemaal mee oneens' tot (5) 'helemaal mee eens'.

8. Impulsiviteit

Impulsiviteit is gemeten aan de hand van zes stellingen. Deelnemers is de volgende casus voorgelegd: *"Als je online bent, moet je vaak keuzes maken, bijvoorbeeld of je wel of niet op een link klikt, of dat je wel of niet ergens op reageert, of dat je wel of niet gegevens over jezelf deelt. In hoeverre ben je het met de volgende stellingen eens?".* Vervolgens zijn de volgende stellingen voorgelegd, allemaal gemeten op een vijfpuntsschaal van (1) 'helemaal mee oneens' tot (5) 'helemaal mee eens':

- *"Als ik online keuzes maak, dan denk ik daar altijd goed over na"*
- *"Als ik online keuzes maak, dan bespreek ik dat eerst met mijn ouders/verzorgers"*
- *"Als ik online keuzes maak, dan doe ik dat snel en zonder na te denken"*
- *"Ik heb wel eens te snel op een link geklikt waardoor ik een probleem kreeg"*
- *"Ik heb wel eens een bericht gestuurd waar ik snel spijt van kreeg"*
- *"Ik heb wel eens persoonlijke gegevens (bijv. foto's, adresgegevens) gestuurd naar iemand die ik helemaal niet (goed) ken.".*

9. Subjectief effect van de interventie

Als extra check zijn er in de nameting vier vragen voorgelegd over hoe de interventie ervaren is. Allereerst is gevraagd: *"Kun je je nog herinneren dat je dit spel in jouw klas hebt gespeeld",* met antwoordmogelijkheden (1) 'ja, heel goed' (2) 'ja, een beetje' (3) 'Ja, maar niet zo goed' en (4) 'Nee, ik was er toen niet bij'. Daarna is gevraagd hoe deelnemers HackShield in de klas beoordelen, door te vragen naar de mate waarin ze de quest '*interessant', 'moeilijk', 'lang', 'leuk', 'kinderachtig' en 'spannend'* konden vinden met als antwoordmogelijkheden 'Ja', 'Nee' en 'Weet ik niet'. Ook is aan de deelnemers gevraagd in hoeverre ze het spel geschikt vinden om iets te leren over online pesten en hacken met als antwoordmogelijkheden 'Ja', 'Een beetje' en 'Nee'. Tenslotte is gevraagd om een rapportcijfer te geven aan de quest 'Online Grenzen'. Ook zijn in de vragenlijst demografische gegevens (leeftijd, geslacht en de naam van de basisschool) uitgevraagd.

In Tabel 2 zijn de Cronbachs alfa's als indicatie van interne consistentie en betrouwbaarheid weergegeven voor de gemeten constructen. Voor het vaststellen van de interne consistentie is zowel gekeken naar de voor- als naar de nameting. De variabelen kennis, gedragsintenties en *agency* worden per item geanalyseerd en zijn daarom niet meegenomen in deze tabel. Voor verantwoordelijkheid en impulsiviteit is er geen onderscheid gemaakt tussen online pesten en hacken. Daarom is hier alleen een Cronbachs alfa zichtbaar voor de voor- en nameting

Tabel 2

Interne consistentie gebruikte constructen effectmeting

	Voormeting online pesten	**Nameting online pesten**	**Voormeting hacken**	**Nameting hacken**
Risicoperceptie	α = ,79	α = ,80	α = ,57	α = ,62
Zelfeffectiviteit	α = ,67	α = ,80	α = ,54	α = ,74
Respons effectiviteit	α = ,72	α = ,79	α = ,63	α = ,82
Subjectieve normen	α = ,75	α =,70	α = ,67	α = ,81
	Voormeting		Nameting	
Verantwoordelijkheid	α = ,60		α = ,72	
Impulsiviteit	α = ,66		α = ,71	

Noot: kennis, gedragsintenties en agency zijn per item geanalyseerd omdat het construct niet intern consistent was en komen niet terug in deze tabel.

4.3 Procedure

4.3.1. Werving en deelnemers

In de periode van november 2025 tot en met maart 2026 is de klassenquest 'Online grenzen' van HackShield in de Klas geëvalueerd op negen basisscholen verspreid over Nederland. De scholen zijn in eerste instantie benaderd door HackShield zelf. Na het achterblijven van de respons zijn er tevens scholen via het netwerk van het lectoraat Online Weerbaarheid benaderd om aan deze effectevaluatie deel te nemen. Via contactpersonen binnen de basisschool zijn leerkrachten benaderd van wie de klas de klassenquest 'Online grenzen' zou spelen. Deze leerkrachten is vervolgens gevraagd om zelf de quest 'Online grenzen' met de kinderen te spelen. Van de negen basisscholen die hebben deelgenomen aan dit onderzoek, voelden slechts twee scholen voldoende zelfvertrouwen om de klassenquest zelf uit te voeren. De overige scholen wilden enkel deelnemen aan het onderzoek wanneer zij een gastles verzorgd door

HackShield zouden ontvangen. HackShield heeft bij daardoor bij zeven scholen een gastles laten verzorgen of zelf verzorgd.

De scholen ontvingen voorafgaand aan het spelen van de klassenquest een email van de onderzoekers met daarin de link en QR-code naar de vragenlijst van de voormeting. Tevens ontvingen zij een voorbeeld van een informatiebrief die zij vooraf naar de ouders van de leerlingen konden sturen (zie Bijlage 2). Ouders werd hierin de gelegenheid geboden aan te geven dat zij niet wilden dat hun kind deelnam aan de effectevaluatie. Voor de inhoud van de brief, alsmede andere zaken met betrekking tot de uitvoering van de evaluatie is vooraf door de onderzoekers in contact getreden met de Saxion Ethische Advies Commissie (SEAC). Ongeveer een week na het spelen van de quest kregen de leerkrachten een email met een link en QR-code naar de vragenlijst van de nameting.

In totaal hebben, zoals gesteld, negen basisscholen deelgenomen aan het onderzoek, met per school tussen de een en vier klassen. Alle klassen betroffen groepen 6, 7 of 8 of een combinatie daarvan. De scholen waren afkomstig uit de provincies Noord-Holland (4), Overijssel (2), Utrecht (1), Gelderland (1) en Drenthe (1). De lessen vonden plaats in november 2025 (een school), januari 2026 (twee scholen), februari 2026 (een school), en maart 2026 (vijf scholen). De tijd tussen het invullen van de voor- en nameting varieerde tussen de twee en zeven weken (en bevatte in sommige gevallen een vakantieperiode).

Het aantal respondenten in de voormeting lag iets hoger dan in de nameting (zie Tabel 3). Aan het begin van de vragenlijst gaven de deelnemers hun eigen akkoord voor deelname. Bij de nameting volgde eerst een controlevraag of men deel had genomen aan de les ‘Hackshield in de Klas’. Als dit niet het geval was, dan werd de vragenlijst afgebroken. Alleen volledig ingevulde vragenlijsten werden meegenomen in de analyses (ook vanwege relevante vragen aan het einde van de vragenlijst). Dit zorgde voor uitval van respondenten: 24% (n = 118) in de voormeting en 24% (n = 91) in de nameting. Dit gebeurde ook enkele malen voor een hele klas tegelijk, wat de suggestie wekt dat er door de leerkrachten ondanks de instructie in de praktijk te weinig tijd voor was gereserveerd en bv. een pauze of het einde van de schooldag was bereikt. Van alle volledige ingevulde vragenlijsten zijn de vragenlijsten die ‘onwaarschijnlijk snel’ waren ingevuld verwijderd. Dit is aan de hand van een visueel criterium gedaan: van de invultijd is (apart voor de voor- en nameting) een frequentieverdeling gemaakt. Hierbij werden twee pieken zichtbaar: een normale verdeling van deelnemers die de vragenlijst serieus hadden ingevuld, met links daarvan een piek van de zogenaamde *speeders*. In het dal tussen de twee pieken werd de grens getrokken: bij de voormeting bij 450 seconden (7’30’’), bij de nameting bij 360s (6’0’’). De vragenlijst was in de nameting – logischerwijs - sneller ingevuld dan in de voormeting (de mediane invultijd ging van

17’43’’ terug naar 13’46’’, wat een significante afname is (Mann–Whitney U=38233.5, z=–6.55, p<.001). Dit verschil is te verklaren door een leereffect dat optrad, omdat deelnemers de vragenlijst al eens eerder gelezen en ingevuld hebben. Door deze wijze van selecteren bleven uiteindelijk 368 deelnemers in de voormeting, en 295 deelnemers in de nameting over.

Tabel 3

Aantal respondenten in de voor- en nameting

	Voormeting	**Nameting**
Respons (vragenlijst gestart)	486	386
Akkoord gegeven (eigen consent)	466	368
Herinnert zich het spel gespeeld te hebben (alleen bij nameting)	-	356
100% ingevuld	377	310
Niet te snel ingevuld	368	295

Zoals te zien is in Tabel 3 verschilden de steekproeven wat betreft omvang: bij de nameting waren 73 minder deelnemers dan bij de voormeting. Hiervoor is geen duidelijke verklaring, het is echter denkbaar dat de deelname aan het onderzoek (voormeting – les – nameting, verdeeld over drie verschillende dagen) een te grote inspanning was voor klassen en/of docenten. Het aantal deelnemers aan de nameting is echter wel van voldoende omvang om betrouwbare uitspraken te kunnen doen.

4.4 Data-analyse

De data die verzameld zijn door middel van Qualtrics zijn geëxporteerd naar SPSS[3]. Voor de data-analyse zijn beschrijvende statistieken gebruikt en zijn – afhankelijk van het variabele type - verschillen tussen voor- en nameting getoetst met een t-toets.

[3] Statistical Package for the Social Sciences; https://www.ibm.com/analytics/nl/nl/technology/spss/index.html

5. Resultaten inhoudsanalyse klassenquest 'Online Grenzen'

In dit hoofdstuk wordt – op basis van variabelen die zijn gedestilleerd uit de literatuurstudie en de interviews met de ontwikkelaars van HackShield in de Klas – een kwalitatieve inhoudsanalyse gemaakt van de klassenquest 'Online Grenzen'. Er wordt gekeken naar de mate waarin de beschreven onderdelen (zowel uit de literatuurstudie als uit de interviews met HackShield) van cyberweerbaarheid terugkomen in de klassenquest en de manier waarop hier invulling aan is gegeven. Het doel van deze inhoudsanalyse is om vast te stellen in hoeverre wetenschappelijk onderbouwde werkzame mechanismen voor cyberweerbaar gedrag resoneren met de inhoud van de quest en welke aanbevelingen – op basis van de theorie – kunnen worden gedaan om deze klassenquest eventueel te versterken.

In dit hoofdstuk staat de evaluatie van twee onderdelen uit de quest centraal: de evaluatie van de onderdelen in deze quest die gaan over (1) het thema 'Online pesten' en (2) het thema 'Hacken'. Het volledige transcript van de quest 'Online grenzen' is te vinden in Bijlage 4.

5.1 Online pesten

5.1.1. Kennis

In de klassenquest wordt ingezet op het vergroten van de kennis van deelnemers rondom 'online pesten'. Er wordt aan leerlingen geleerd dat iedereen in principe slachtoffer zou kunnen worden van online pesten. Daarnaast wordt aangegeven dat er dingen zijn die je zou kunnen doen om online pesten tegen te gaan, bijvoorbeeld door het te melden aan iemand die je vertrouwt (een ouder of leerkracht). Zo wordt in de lesbrief de volgende vraag gesteld: *Wat kun je doen als je online gepest wordt?* Hierbij wordt het volgende antwoord gegeven: *Hoe graag je het ook wilt, het is niet de beste optie om iemand terug te pakken, uiteindelijk wordt de ruzie zo juist groter en voel je je ook niet beter. Dit zijn dingen die je wel kunt doen:*

- *Het vertellen aan je vrienden of/en je ouders; iemand die je vertrouwt. Dan kunnen zij jou steunen en helpen.*
- *Het vertellen aan de docent/vertrouwenspersoon op school, die kan je verder helpen.*
- *Met iemand praten over hoe je je voelt, dat lucht op.*

Deze elementen kunnen ervoor zorgen dat leerlingen meer kennis hebben over het onderwerp 'online pesten'.

5.1.2. Risicoperceptie

In de quest zijn elementen toegevoegd die de risicoperceptie van kinderen rondom online pesten kunnen vergroten. Dit zijn elementen die inspelen op de ernst van online pesten en die de nadruk leggen op de vatbaarheid voor online pesten onder kinderen. Bijvoorbeeld:

- Sanne zegt: *"Er is een klasgenoot die echt rot berichten naar me stuurt".* Ze vindt dit dus vervelend en wordt in dit voorbeeld gepest.
- Sanne: *"Wat… Nou… ik… Hoe bedoelt hij… Ik ben helemaal niet…"* is de reactie van Sanne op een pestbericht van Crummit. Deze quote illustreert gevoelens van angst voor vernedering en boosheid. Dit kan bijdragen aan meer angst bij de leerlingen om hetzelfde te ervaren als Sanne.
- Sanne zegt: *"School doet toch ook niks tegen die pesters! Wat nou? Als ik het niet zelf regel, dan gebeurt er NIETS!"* Deze uitspraak kan bijdragen aan een gevoel van angst omdat het pesten dus niet zal ophouden zolang Sanne zelf geen actie onderneemt. Dit kan leerlingen het gevoel geven dat als zij gepest worden dit niet snel zal ophouden en ze er zelf niets aan kunnen doen, wat inspeelt op gevoelens van onmacht en frustratie.

Deze elementen kunnen de ervaren ernst van online pesten vergroten en kunnen kinderen ook het gevoel geven dat ze vatbaar zijn voor online pestgedrag, wanneer kinderen zich met Sanne kunnen identificeren.

5.1.3. Zelfeffectiviteit

Om de zelfeffectiviteit te vergroten moeten in de quest duidelijke handelingsperspectieven worden gegeven. Deze handelingsperspectieven – een beschrijving van adequaat gedrag om het risico te verminderen – moeten inspelen op wat je zelf kunt doen om je te beschermen tegen (in dit geval) online pesten. Door concrete handelingsperspectieven aan te dragen waarvan leerlingen het gevoel hebben dat zij die zelf zouden kunnen inzetten wanneer zij online gepest worden, kan de zelfeffectiviteit worden vergroot. In de quest komt zelfeffectiviteit op de volgende manier terug:

- *Sanne: "En ik weet precies 'hoe' we hem gaan terugpakken*." Dit veronderstelt dat 'terugpakken' passend gedrag zou kunnen zijn in het geval van online pesten. Doordat het Sanne ook lukt om dat te doen gedurende de quest, kan dit zorgen voor het gevoel dat het relatief gemakkelijk is om terug te pesten op het moment dat je gepest wordt.
- *Sanne: "School doet toch ook niks tegen die pesters! / Precies, school doet ook niets tegen die pesters!"* Deze uitspraak kan een negatieve invloed hebben op de zelfeffectiviteit van leerlingen,

aangezien hier wordt gesuggereerd dat je zelf niet in staat bent om het verloop van het pestgedrag te veranderen. Hulp vragen lijkt te worden weggezet als “niet zinvol”.

In deze voorbeelden wordt niet duidelijk gemaakt wat een leerling zou kunnen doen om online pesten tegen te gaan en er wordt niet geoefend met het uitvoeren van positieve gedragingen (bijvoorbeeld het vragen om hulp of het inschakelen van een volwassene). Aan het eind van de quest wordt wel duidelijk gemaakt dat ‘terugpakken’ geen zinvol gedrag is en dat om hulp vragen een goed alternatief zou kunnen zijn. Hierbij wordt echter niet ingegaan op de wijze waarop leerlingen dit zelf zouden kunnen doen. Dit lijkt erop te wijzen dat deze quest waarschijnlijk niet bijdraagt aan het vergroten van de zelfeffectiviteit.

5.1.4. Responseffectiviteit

Om kinderen meer cyberweerbaar gedrag te laten vertonen, is het belangrijk om in een interventie handelingsperspectieven op te nemen die als nuttig en zinvol worden ervaren door de deelnemers. In de volgende fragmenten wordt ingespeeld op responseffectiviteit:

- *Wanneer Sanne de malware op de server van de school wil installeren zegt ze: “Jullie vinden dit toch ook een onschuldig grapje? We lossen samen de puzzel op en dan installeer ik de malware.”* Het installeren van malware wordt hier gepresenteerd als een handelingsperspectief om online pesten tegen te gaan. Wanneer je als leerling Sanne probeert te stoppen met dit gedrag, dan lukt dat niet. Sanne is vastbesloten om degene die haar pest ‘terug te pakken’.
- *Sanne: “School doet toch ook niks tegen die pesters! / Precies, school doet ook niets tegen die pesters!”* Met deze uitspraak wordt gesuggereerd dat het niet zinvol of nuttig is om hulp vanuit school in te schakelen. Dat komt tevens terug in het volgende voorbeeld: *Wanneer Sanne uit de klassenapp is gegooid vanwege haar pestgedrag vraagt ze aan de leerlingen wat zij zouden doen. Als je antwoordt: “vertel het aan de leerkracht”, dan word je teruggezet in de klassenapp, maar krijg je ook het bericht “Ben je daar weer loser? Kon je het niet zonder die leerkracht*?”.

Aan het eind van de quest worden er een aantal handelingsperspectieven aangedragen die positief inspelen op de responseffectiviteit en die laten zien dat het zinvol en nuttig is om hulp te vragen aan volwassenen:

- *“Voor leerkrachten en voor ouders is het moeilijk om te weten als je online gepest wordt. Daarom is het belangrijk om ze op de hoogte te brengen, zodat ze je kunnen helpen.”*

- "*Wat kun je doen als je online gepest wordt? Antwoord: hoe graag je het ook wilt, het is niet de beste optie om iemand terug te pakken, uiteindelijk wordt de ruzie zo juist groter en voel je je ook niet beter. Dit zijn dingen die je wel kunt doen:*
    - *Het vertellen aan je vrienden of/en je ouders; iemand die je vertrouwt. Dan kunnen zij jou steunen en helpen.*
    - *Het vertellen aan de docent/vertrouwenspersoon op school, die kan je verder helpen.*
    - *Met iemand praten over hoe je je voelt, dat lucht op*".

Deze laatste handelingsperspectieven zijn nuttig en zinvol. De wijze waarop dit leerlingen zou kunnen helpen – anders dan 'dat het oplucht' – wordt in de quest echter niet verduidelijkt. Er wordt niet uitgelegd waarom het bijvoorbeeld nuttig is om een volwassene op hulp te vragen. De tegenstrijdigheid van geboden handelingsperspectieven kan verwarrend werken en werpt de vraag op wat kinderen onthouden als (1) niet expliciet wordt gemaakt waarom 'het terugpakken' uiteindelijk niet helpend is, en (2) niet duidelijk wordt wat het alternatief – er met iemand over praten – oplevert. Door deze tegenstrijdigheid is het vermoeden dat deze quest niet bij zal dragen aan het vergroten van de responseffectiviteit.

5.1.5. Subjectieve normen

Positieve subjectieve normen kunnen bijdragen aan de eigen cyberweerbaarheid van individuen. Om de subjectieve normen te vergroten moet in de quest duidelijk worden welk gedrag anderen van een leerling verwachten ten aanzien van zelfbeschermend gedrag tegen online pesten. In de volgende fragmenten van de quest wordt ingespeeld op dit begrip:

- Er zijn een aantal opmerkingen van Sanne die de subjectieve normen illustreren dat Sanne niet te stoppen is, ook als anderen haar tegen proberen te houden. Dit kan leiden tot de subjectieve norm dat luisteren naar anderen niet zinvol is. Daarnaast laten de volgende opmerkingen zien dat je op online pesten kan reageren door iemand 'terug te pakken':
    - *"Nee, nee, NEE! Ik laat niet over me heen lopen, klas."*
    - *"Haha dat zal hem leren!"*
    - *"En ik weet precies 'hoe' we hem gaan terugpakken."*

Deze quotes schetsen het beeld dat 'terugpakken' een passende reactie is op gepest worden in de online omgeving. Aan het einde van de quest wordt dit aspect echter genuanceerd en benadrukt dat het niet goed is om iemand terug te pakken. Als alternatief wordt voorgesteld om de hulp in te roepen van een

volwassene. Door de verschillen in normen die worden gesteld in deze quest, is het niet goed te voorspellen wat dit doet met de subjectieve normen van deelnemers.

5.1.6. *Agency*

In de quest zitten geen duidelijke voorbeelden waaruit blijkt dat *agency* wordt gestimuleerd. Er wordt niet verwezen naar het bespreekbaar maken van het thema 'online pesten' in bijvoorbeeld de thuissituatie of het uitdragen van de handelingsperspectieven in de directe omgeving.

5.1.7.Verantwoordelijkheid

In deze klassenquest wordt ingespeeld op het nemen van eigen verantwoordelijkheid in situaties waarin online wordt gepest. Zo wordt er aangegeven:

- *Peter: "Je moet beter zijn dan de pesters, Sanne."*
- *Uit de lesbrief: Wat kun je doen als je online gepest wordt?*
  Antwoord: hoe graag je het ook wilt, het is niet de beste optie om iemand terug te pakken, uiteindelijk wordt de ruzie zo juist groter en voel je je ook niet beter. Dit zijn dingen die je wel kunt doen:
    - *Het vertellen aan je vrienden of/en je ouders; iemand die je vertrouwt. Dan kunnen zij jou steunen en helpen.*
    - *Het vertellen aan de docent/vertrouwenspersoon op school, die kan je verder helpen.*
    - *Met iemand praten over hoe je je voelt, dat lucht op.*

Leerlingen worden in de quest dus gestimuleerd om zelf verantwoordelijkheid te nemen wanneer zij online gepest worden (of in situaties waarin zij weten dat er online gepest wordt), door het te vertellen aan iemand die zij vertrouwen. Wat niet wordt beschreven in de quest, is dat je ook verantwoordelijkheden kunt hebben als je ziet dat er gepest wordt, bijvoorbeeld door de pester tegen te houden of de gepeste te verdedigen (Salmivalli et al., 2010; Van Houten en Spithoven, 2026). Dit werpt de vraag op of er voldoende elementen in de quest zijn verwerkt om de ervaren eigen verantwoordelijkheid van kinderen daadwerkelijk te vergroten.

5.1.8. Impulsiviteit

In de quest wordt impulsiviteit rondom online pesten niet tegengegaan. Integendeel, Sanne laat (herhaaldelijk) impulsiviteit zien; ze denkt niet na voordat ze gaat hacken. Wanneer Sanne zich afvraagt

wat ze moet doen met een klasgenoot “die echt rot berichten naar me stuurt”, resulteren alle drie de antwoordopties in dat Sanne de pester gaat terugpakken. Dit lijkt impulsiviteit van kinderen eerder te stimuleren dan te remmen.

5.2. Hacken

5.2.1. Kennis

In de quest wordt veel aandacht besteed aan het vergroten van de kennis over hacken en gerelateerde onderwerpen, bijvoorbeeld:

- Er wordt een aantal kennisvragen gesteld over hacken, wachtwoorden, DDoS-aanval, cybercrime, firewall, virusscanner. Deze dragen allemaal bij aan het vergroten van de kennis van leerlingen over de respectievelijke onderwerpen. Daarnaast zijn er aan het einde van de quest stellingen die de leerlingen kunnen beantwoorden om hun kennis te testen. Hier wordt de kennis over firewall en virusscanner herhaald.
    - *“Wat zouden de meest voorkomende wachtwoorden zijn?”*
    - *“Wat is een firewall?”*
    - *“Wat is een DDoS-aanval?”*
    - *“Wat is cybercrime?”*
    - *“Kan je een straf krijgen voor het uitvoeren van een DDoS-aanval?”*
    - *“Wat is een virusscanner?”*
    - *Vraag 4: Een firewall zorgt ervoor dat virussen op je computer gevonden en verwijderd worden.*
    - *Vraag 5: Met een virusscanner kun je een computer beveiligen.*
- *Wat mag je wel doen als je goed bent in hacken? Wat kun je met die vaardigheden? Antwoord:*
    - *Ethisch hacker / White hat hacker worden om ervoor te zorgen dat bedrijven of personen weten waar ze niet goed beschermd zijn en daar iets aan kunnen doen.*
    - *Bij HackShield een account aanmaken.*

De deelnemer wordt in het spel al met al op diverse plekken met feitelijke kennis over hacken en cyberweerbaarheid in contact gebracht, wat de kennis over hacken (en aanverwante thema's) kan vergroten.

5.2.2. Risicoperceptie

Om de risicoperceptie te vergroten moet in de quest bij de leerlingen bewustzijn worden gecreëerd over de ernst van en de vatbaarheid voor slachtofferschap van hacken enerzijds, en de risico's die je loopt als je zelf zou gaan hacken anderzijds. In de volgende fragmenten wordt er ingespeeld op dit begrip:

- *Sanne gaat het profiel van haar pester hacken.* Dit draagt bij aan het vergroten van de risicoperceptie rondom slachtofferschap en daderschap van hacken.
- Vervolgens wordt de vraag gesteld: *"Wat zouden de gevolgen van hacken kunnen zijn?"* Hier wordt ingespeeld op de risico's die je hebt als dader van hacken. De volgende antwoordsuggesties worden gegeven:
    - *Halt / taakstraf*
    - *Van school gestuurd*
    - *Geen zakgeld*
    - *Vrienden kwijtraken*
    - *Huisarrest*
    - *Iemand verdrietig hebben gemaakt*
    - *Een slecht geweten*
    - *Account banned op Xbox/PlayStation/Steam etc*
    - *Schadevergoeding betalen*
    - *Excuus aanbieden aan slachtoffer*
- *Na het beantwoorden van de vraag: "Kan je een straf krijgen voor het uitvoeren van een DDoS-aanval?" Krijg je één van de volgende reacties te zien: "Een DDoS kan veel (financiële) schade aanbrengen, bij scholen of bedrijven bijvoorbeeld" of "Je krijgt een boete, taakstraf of zelfs een gevangenisstraf".* Hierin wordt wederom de ernst van daderschap van hacken benadrukt.
- Aan het eind van de quest komt Peter van het COPS-team (iemand van de Cyber Offender Prevention Squad van de Politie) in beeld. Hij benadrukt dat je als dader niet ongezien weg kunt komen wanneer je besluit over te gaan tot hacken.

Deze elementen van de quest kunnen bijdragen aan het vergroten van de risicoperceptie rondom hacken, waarbij er in de quest voornamelijk de focus ligt op het vergroten van de risicoperceptie over daderschap.

5.2.3. Zelfeffectiviteit

Om de zelfeffectiviteit te vergroten is het van belang om duidelijke handelingsperspectieven te geven waarvan deelnemers het gevoel hebben dat zij deze zelf kunnen uitvoeren. Zij moeten er na afloop van

de quest vertrouwen in hebben dat zij dit gedrag kunnen vertonen. In de quest wordt hier op de volgende manier vorm aan gegeven:

- *Wat kun je doen om te zorgen dat je niet makkelijk gehackt kunt worden? Antwoord:*
    - *Zorgen voor een goed wachtwoord, of beter nog, een wachtZIN!*
    - *Zorgen voor verschillende wachtwoorden bij verschillende accounts*
    - *Zorgen voor tweestapsverificatie*
    - *Je wachtwoord nooit met iemand delen!*
    - *Gebruikmaken van een virusscanner*
    - *Gebruikmaken van een firewall*

Er wordt duidelijk gemaakt dat deze handelingsperspectieven eenvoudig uit te voeren zijn. De handelingsperspectieven worden in de lesbrief behorende bij deze quest duidelijk uitgelegd en er wordt bijvoorbeeld benadrukt dat iedereen een goed wachtwoord kan maken. Hierbij is het wel van belang om op te merken dat het afhankelijk is van de manier waarop de begeleider van het spel deze vragen met de leerlingen bespreekt, en of deze handelingsperspectieven goed overgebracht worden op de leerlingen. Afhankelijk van de wijze waarop dit besproken wordt in de klas kan het bijdragen aan het vergroten van de zelfeffectiviteit.

5.2.4. Responseffectiviteit

Voor het verhogen van de responseffectiviteit is het van belang dat de handelingsperspectieven die worden aangereikt, worden ervaren als nuttig en zinvol in het tegengaan van het risico (in dit geval hacken). Zoals hierboven beschreven worden de volgende handelingsperspectieven aangedragen in deze quest:

- *Wat kun je doen om te zorgen dat je niet makkelijk gehackt kunt worden? Antwoord:*
    - *Zorgen voor een goed wachtwoord, of beter nog, een wachtZIN!*
    - *Zorgen voor verschillende wachtwoorden bij verschillende accounts*
    - *Zorgen voor tweestapsverificatie*
    - *Je wachtwoord nooit met iemand delen!*
    - *Gebruikmaken van een virusscanner*
    - *Gebruikmaken van een firewall*
- *Peter: "Wacht even klas, het is niet goed om te hacken met slechte bedoelingen / Inderdaad klas, het is niet goed om te hacken met slechte bedoelingen. Als je weet of ziet dat iemand dit doet,*

moet je in actie komen!" Hierbij geeft Peter niet aan wat je precies moet doen in zo'n geval en wat het betekent 'om in actie te komen'.

In de quest wordt duidelijk gemaakt dat je iets moet doen om slachtofferschap te voorkomen. Deze handelingsperspectieven worden duidelijk uitgelegd en er wordt tevens aangegeven waarom het bijvoorbeeld nuttig is om verschillende wachtwoorden te kiezen bij verschillende accounts. Hiermee wordt duidelijke gemaakt op welke wijze leerlingen zichzelf kunnen beschermen tegen hacken (en gerelateerde risico's), wat kan bijdragen aan het vergroten van de responseffectiviteit. In het geval van het aanspreken van leeftijdsgenoten die overgaan tot hacken (zoals in het voorbeeld van Peter), wordt echter niet duidelijk gemaakt hoe je dat kunt doen en waarom het zinvol is om mensen aan te spreken op dit gedrag. Voor dit specifieke onderdeel lijkt de responseffectiviteit niet te worden vergroot.

5.2.5. Subjectieve normen

Om de subjectieve normen te vergroten moet in de quest duidelijk worden welk gedrag leeftijdsgenoten van een leerling verwachten ten aanzien van zelfbeschermend gedrag tegen hacken. In de volgende fragmenten van de quest wordt ingespeeld op deze elementen:

- *Koi vraagt: "Wat zouden jullie een goede reden vinden om te gaan hacken?".* Door dit in de klas te bespreken krijgen kinderen een beeld van wat leeftijdsgenoten een goede reden vinden om te gaan hacken. De volgende suggesties worden gegeven:
    - *Om te kijken of een website wel veilig is.*
    - *Om geld te jatten*
    - *Nieuwsgierigheid*
    - *Erkenning of waardering*
    - *Gewoon heel tof*
    - *"Hij heeft vast ook wel eens iemand gehackt"*
    - *"Hij had een slecht wachtwoord"*
    - *"Het is niet onze schuld dat hij zijn computer/account niet beveiligt"*
    - *"Er zijn toch geen slachtoffers"*
    - *"Er is toch geen (financiële) schade"*
    - *"Het is niet alsof we iets kapot maken"*
    - *"Hier leert hij weer van"*
    - *"Het is maar een geintje"*

    - *“Ik doe niks fout”*
    - *“De hele klas doet mee” (groepsdruk)*
- *Sanne zegt voordat ze malware op de computer van school wil zetten: “Jullie vinden dit toch ook een onschuldige grap?”.*
- Peter (van het COPS-team) vertelt aan het einde van de quest dat je als hacker jouw krachten voor goed of kwaad kan gebruiken en dat: *“als het niet jouw server of computer is, blijf je er vanaf!”.*
- *Peter: “Door ‘terug’ te hacken, ben je zelf niet beter dan de pesters.”*

Gedurende de quest lijkt er allereerst een norm te worden gesteld dat je kunt gaan hacken als je wordt gepest en dat je iemand ‘terug mag pakken’ door bijvoorbeeld zijn of haar account te hacken. Dit wordt aan het einde van de quest omgebogen door het verschijnen van iemand van het COPS-team die duidelijk maakt dat je hiermee niet ongezien weg kunt komen. Hij geeft aan dat je niet aan iemands server of computer mag zitten en dat dit gevolgen kan hebben voor degene die overgaat tot hacken. Door de verschillende normen die worden geschetst in de quest is het vooralsnog onduidelijk of deze aanpak leidt tot subjectieve normen die bijdragen aan het vergroten van de eigen online weerbaarheid van leerlingen.

5.2.6. *Agency*

In de quest wordt niet ingespeeld op het versterken van de *agency* van deelnemers. Er wordt niet gestimuleerd om het geleerde tijdens de quest te bespreken of uit te dragen in de directe omgeving - zoals ouders/verzorgers - van de leerlingen.

5.2.7. Verantwoordelijkheid

In de quest wordt ingespeeld op het vergroten van de eigen verantwoordelijkheid door te benadrukken dat kinderen zichzelf kunnen beschermen tegen hacken. Zo wordt er gevraagd:

- *“Heb jij al een virusscanner op jouw computer?”*

Deze vraag illustreert de verantwoordelijkheid die kinderen zelf kunnen nemen om zich te beschermen tegen gevaren op de computer. Bovendien kan het bijdragen aan het vergroten van het verantwoordelijkheidsgevoel van leerlingen om zelf maatregelen te nemen tegen de risico’s die gerelateerd zijn aan hacken.

5.2.8. Impulsiviteit

In de quest wordt niet veel aandacht besteed aan het tegengaan van impulsief handelen onder de leerlingen. Wel wordt er in het volgende fragment getracht leerlingen ervan bewust te maken dat het belangrijk is om bij grote beslissingen eerst goed na te denken:

- *"Wacht even, klas. Sanne staat op het punt een grote beslissing te maken. Ze gaat de school hacken!" "Ik ben heel benieuwd wat jullie daarvan vinden?"*.

In dit voorbeeld wordt er vervolgens met de klas besproken wat zij ervan vinden dat Sanne de keuze maakt om te gaan hacken wanneer zij wordt gepest. Dit kan duidelijk maken dat het belangrijk is om bij grote beslissingen eerst goed na te denken en dan pas te handelen. Dit zou invloed kunnen hebben op de impulsiviteit van deelnemers.

5.3 Samenvatting resultaten inhoudsanalyse

De resultaten van de inhoudsanalyse worden samengevat in Tabel 4. In deze tabel wordt aangegeven of de constructen die meegenomen zijn in dit onderzoek – en die bijdragen aan cyberweerbaarheid – terugkomen in de quest op basis van de inhoudsanalyse. Dit is zowel gedaan voor online pesten als voor hacken.

Tabel 4

Samenvatting van de resultaten van de inhoudsanalyse.

Kenmerk	**Online Pesten**	**Hacken**
Kennis	✓	✓
Risicoperceptie	✓	✓
Zelfeffectiviteit	X	✓
Responseffectiviteit	X	✓/X
Subjectieve normen	X	✓/X
Agency	X	X
Verantwoordelijkheid	✓/X	✓
Impulsiviteit	X	✓

Noot: Als een kenmerk aanwezig is, wordt dit aangegeven met een ✓; als het kenmerk afwezig is of tegenstrijdige boodschappen afgeeft met een X; als het deels aanwezig is maar m.b.t. belangrijke aspecten ook afwezig met ✓/X

6. Resultaten vragenlijstonderzoek

In dit hoofdstuk worden de resultaten van het vragenlijstonderzoek besproken. Allereerst worden de beschrijvende statistieken weergegeven over de deelnemers aan dit onderzoek. Vervolgens wordt er gekeken naar het effect van de quest 'Online grenzen' op de (onderdelen van) cyberweerbaarheid. Dit wordt apart in kaart gebracht voor de thema's 'online pesten' en 'hacken'. Tenslotte wordt er gekeken wat het effect van het spelen van de quest is op de variabelen *agency*, verantwoordelijkheid en impulsiviteit.

Tabel 5

Kenmerken van de steekproeven in de voor- en nameting

	Voormeting	Nameting	Verschil
Respons (gefilterd)	n = 368	n = 295	73
Invultijd (mediaan*)	17'43''	13'46''	U = 38 233.50, z = –6.55, p < .001
Geslacht			Niet significant
Jongen	46,5%	45,1%	
Meisje	49,7%	49,5%	
Wil niet zegggen	3,0%	4,4%	
Anders	0,8%	1,0%	
Leeftijd	m = 10,79 jaar (sd = 0,82)	m = 10,80 jaar (sd = 0,90)	Niet significant
Leeftijdsverdeling			Niet significant
8 jaar	0,3%	1,0%	
9 jaar	6,3%	5,8%	
10 jaar	25,3%	26,4%	
11 jaar	49,5%	43,1%	
12 jaar	17,7%	20,7%	
13 jaar	0%	0%	
14 jaar	0%	0,3%	
ontbreekt	1,1%	2,7%	
Groepsverdeling			Niet significant
Groep 6	7,9%	9,2%	
Groep 7	31,0%	29,5%	
Groep 8	61,1%	61,4%	

Noot: *De mediaan wordt gebruikt omdat in een aantal gevallen de vragenlijst lange tijd open is blijven staan. Door deze uitschieters geeft een gemiddelde een vertekend beeld.

6.1 Beschrijvende statistieken

In totaal hebben 368 kinderen deelgenomen aan de voormeting en 295 kinderen aan de nameting van dit onderzoek. Wat betreft de samenstelling van de steekproef waren de voor- en nameting goed

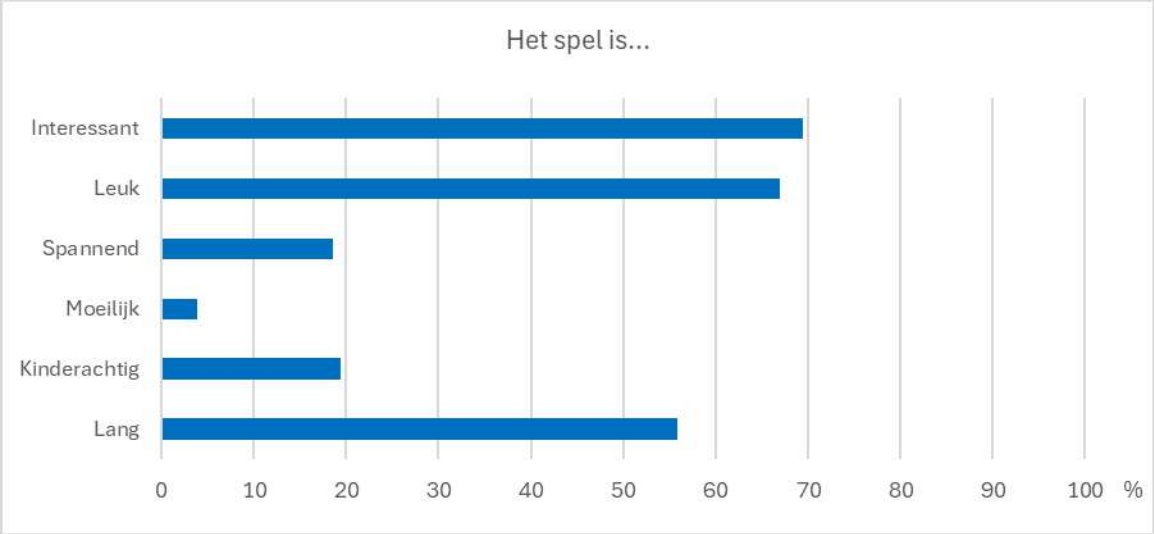
vergelijkbaar (Tabel 5). Er waren *geen* significante verschillen wat betreft indeling op basis van geslacht, leeftijd en groep. Eventuele verschillen tussen de voor- en nameting op relevante variabelen kunnen daarmee niet worden verklaard door een verschillende samenstelling van de meetmomenten.

6.2 Evaluatie spel door deelnemers

In de nameting is de klassenquest 'Online grenzen' geëvalueerd door leerlingen te vragen wat ze van het spel vonden (Figuur 4). Ongeveer twee derde van de kinderen vond het spel interessant en leuk. Het spel werd niet moeilijk gevonden maar ook niet echt spannend. Een vijfde van de kinderen gaf aan het spel kinderachtig te vinden en iets meer dan de helft vond het spel lang duren. Het spel kreeg gemiddeld als rapportcijfer een 7,1 (17,6% gaf het spel een onvoldoende; 21,5% gaf een 9 of een 10).

Figuur 4

Mening over "Hackshield in de Klas" (percentage dat het eens was met de kwalificatie)



De leerlingen werd tevens gevraagd of ze een spel zoals "Hackshield in de klas" geschikt vinden om over onderwerpen zoals online pesten en hacken te leren. Hiermee was 57,7% het eens en 30,1% een beetje. Een kleine groep (12,2%) vond het niet geschikt. Hierbij werden onder andere de volgende redenen aangegeven (noot: de onderstaande teksten zijn *niet* door de onderzoekers aangepast):

- **Het spel leidt af van het onderwerp**
    - *"nee want je bent meer gefocust in het spel dan het onderwerp zelf"*

- *“Als het als ´spel´ word gezien, word het NIET serieus genomen omdat spellen vaak als ´relax´ middel gebruikt worden.”*
- *“want dan doe je het niet echt sirieus”*

- **Het spel is niet aantrekkelijk**
  - *“Het is geen echt spel. Kinderachtig”*
  - *“ik vind het te kinderachtig uit gelegd en miss volgende keer met echte mensen maar dan na gespeeld”*
  - *“ik zegmaar weet alles al en het is wel goed alleen super saai en daardoor letten kinderen niet op en dat leren ze niet”*
- **Het spel zit niet goed in elkaar**
  - *“want als je een slechte keus wilt maken dan zegt die niet bijvoorbeeld weet je het zeker”*
  - *“het ging meer over hacken dan over pesten alleen ope het begin ging het over pestem verder niet”*
  - *“want je kon niet echt veel doen eigelijk alleen maar kijken”*

Positieve reacties benadrukten het **belang** van het behandelen van het onderwerp:

- *“ja wat je kan doen als je gepest word”*
- *“ja want het is goed om dat soort dingen te leren”*
- *“zo dat het minder vaak gebeurt”*
- *“zodat mensen in de klas minder gaan pesten maar in onse klas doen ze dat echt oprocent”*
- *“omdat je moet weten wat er online kan gebeuren”*
- *“want anders gaat iedereen lachen en nu niet dankzij het spel”*

Deze resultaten laten zien dat het de quest ‘Online grenzen’ een ruime voldoende krijgt van de deelnemers. Er was een mix van positieve beoordelingen (interessant, leuk), neutrale beoordelingen (niet moeilijk, niet kinderachtig) en meer negatieve beoordelingen (te lang, niet spannend). Een meerderheid van de deelnemende kinderen vond de klassenquest een geschikte lesmethode.

6.3 Resultaten online pesten

6.3.1. Kennis

In de vragenlijst kregen de deelnemers vijf situaties/stellingen voorgelegd met kennisvragen over online pesten. Aan hen werd gevraagd om aan te geven of deze stelling in hun ogen waar of niet waar is, of dat ze dat niet wisten. In Tabel 6 zijn de scores weergegeven van de leerlingen in de voor- en nameting.

Tabel 6

Scores respondenten op de kennisvragen over online pesten uitgedrukt in percentages.

Stelling	Voormeting	Nameting	Verschil
Als je online gepest wordt, dan kun je daar niets tegen doen.	Waar 14,1% Niet waar 68,8% Weet ik niet 17,1%	Waar 15,3% Niet waar 72,9% Weet ik niet 11,9%	Niet significant
Als iemand online gepest wordt, dan kan dat voor het slachtoffer grote gevolgen hebben.	Waar 70,4% Niet waar 6,0% Weet ik niet 23,6%	Waar 66,8% Niet waar 6,1% Weet ik niet 27,1%	Niet significant
Online pesten is net zo erg als offline pesten (in de klas of op het schoolplein).	Waar 54,1% Niet waar 29,6% Weet ik niet 16,3%	Waar 52,5% Niet waar 27,1% Weet ik niet 20,3%	Niet significant
Als je weet dat iemand online wordt gepest, dan moet je het slachtoffer helpen.	Waar 64,1% Niet waar 10,1% Weet ik niet 25,8%	Waar 63,7% Niet waar 12,2% Weet ik niet 24,1%	Niet significant
Als je weet dat iemand online wordt gepest, dan is het verstandig dit aan een volwassene (bijvoorbeeld de juf of meester of je ouders) te vertellen.	Waar 84,5% Niet waar 6,0% Weet ik niet 9,5%	Waar 80,3% Niet waar 5,8% Weet ik niet 13,9%	Niet significant

Iets meer dan twee derde van de leerlingen dacht dat je iets tegen online pesten kunt doen. Meer dan tachtig procent vond het verstandig het aan een volwassene te vertellen, en weer twee derde vond dat je het slachtoffer moet helpen. Iets meer dan de helft vond online pesten net zo erg als offline pesten, en twee derde dacht dat het grote gevolgen kan hebben voor het slachtoffer. In alle gevallen geldt dat er *geen* significante verschillen zijn gevonden tussen de voor- en nameting. De kennis van deelnemers over online pesten is dus niet veranderd door het spelen van de quest.

6.3.2. Risicoperceptie

Om risicoperceptie te meten is er een onderscheid gemaakt tussen de ervaren kans dat deelnemers slachtoffer kunnen worden van online pesten (de vatbaarheid) en de ervaren ernst van online pesten onder deelnemers. Deelnemers kregen de volgende stelling voorgelegd: “Sam zit in een groepsapp met de hele klas. Er worden *nare dingen* over Sam gezegd in de app en sommige kinderen *lachen* daarom.”

Kans

Om de ervaren kans te meten is deelnemers gevraagd op de volgende stelling te reageren: “Wat er met Sam gebeurt in dit voorbeeld, zou ook kinderen in mijn klas kunnen overkomen”. In de voormeting scoorden de leerlingen gemiddeld een 3,22 op een schaal van (1) helemaal mee oneens tot (5) helemaal mee eens. In de nameting was deze score significant lager, namelijk gemiddeld een 2,84. Deze afname in ervaren kans om slachtoffer te kunnen worden van online pesten is significant ($t(661) = 3.827$; $p<.001$). Dit betekent dat kinderen na het spelen van de quest de kans *kleiner* achten dat een klasgenoot slachtoffer zou kunnen worden van online pesten.

Ernst

Vervolgens is ook de ervaren ernst van online pesten gemeten aan de hand van vier stellingen (gevoelens van gespannenheid, veiligheid, boosheid, verdriet) die zijn samengevoegd tot één construct. In de voormeting scoorden leerlingen gemiddeld een 3,44 op dit construct, in de nameting was dit gemiddelde bijna hetzelfde met een gemiddelde score van 3,32. Dit verschil is niet significant. Dit betekent dat de ervaren ernst van online pesten niet is veranderd door het spelen van de quest.

6.3.3 Zelfeffectiviteit

Om zelfeffectiviteit te meten kregen leerlingen de volgende situatie voorgelegd: “Stel: jij zit in de groepsapp van de klas van Sam en je ziet dat er nare berichten over Sam worden verstuurd.” Aan de hand van vijf stellingen over de mate waarin respondenten het gevoel hebben zelf iets te kunnen doen tegen online pesten is de mate van zelfeffectiviteit gemeten op een schaal van (1) helemaal niet tot (5) heel erg veel. Deze stellingen zijn samen als één construct getoetst. In de voormeting was de gemiddelde score op zelfeffectiviteit 3,87; in de nameting scoorden leerlingen *significant lager* op zelfeffectiviteit met een gemiddelde score van 3,68 ($t(661)=2.935$; $p=.0003$). Kinderen hebben er dus na het spelen van de quest ‘Online grenzen’ minder vertrouwen in dat zij iets tegen online pesten kunnen doen, dan voor het spelen van de klassenquest.

6.3.4. Responseffectiviteit

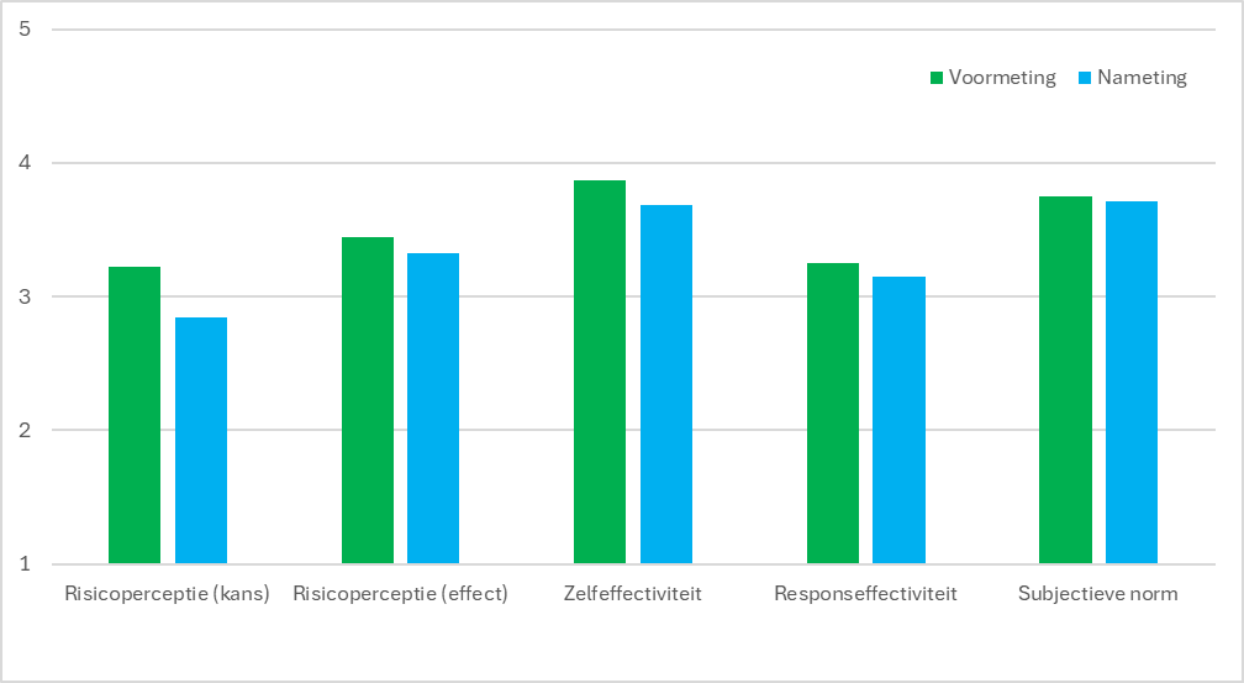
Om responseffectiviteit te meten kregen leerlingen wederom de volgende situatie voorgelegd: “Stel: jij zit in de groepsapp van de klas van Sam en je ziet dat er nare berichten over Sam worden verstuurd.” Vervolgens is aan de hand van zes stellingen gemeten in hoeverre leerlingen bepaalde handelingsperspectieven (zoals het online pestgedrag melden bij een volwassene) als nuttig en zinvol ervaren op een schaal van (1) helemaal niet tot (5) heel erg. Deze stellingen zijn samen als één construct getoetst. In de voormeting scoorden leerlingen iets bovengemiddeld (m = 3,25). In de nameting scoorden leerlingen heel iets lager op dit construct met een gemiddelde van 3,15. Dit verschil was *niet* significant. Het spelen van de klassenquest heeft daarmee geen invloed gehad op de gerapporteerde responseffectiviteit van deelnemers.

6.3.5. Subjectieve norm

De subjectieve normen zijn gemeten aan de hand van zes stellingen waarbij leerlingen wederom dezelfde situatie voorgelegd kregen als bij de hierboven genoemde variabelen. Vervolgens is aan leerlingen gevraagd in hoeverre zij denken dat hun vrienden deze handelingsperspectieven (zoals het online pestgedrag melden bij een volwassene) zouden uitvoeren op een schaal van (1) zeker niet tot 5 (zeker wel). Deze stellingen zijn samen als één construct getoetst. In de voormeting scoorden leerlingen ruim boven gemiddeld (m = 3,75). In de nameting scoorden leerlingen heel iets lager op dit construct met een gemiddelde van 3,71. Dit verschil was *niet* significant. Het spelen van de quest heeft dan ook geen invloed gehad op de gerapporteerde subjectieve normen van kinderen die deel hebben genomen aan dit onderzoek.

Figuur 5

Gemiddelde scores van constructen (op Likert-schaal van 1 tot 5) in de voor-en nameting (online pesten)



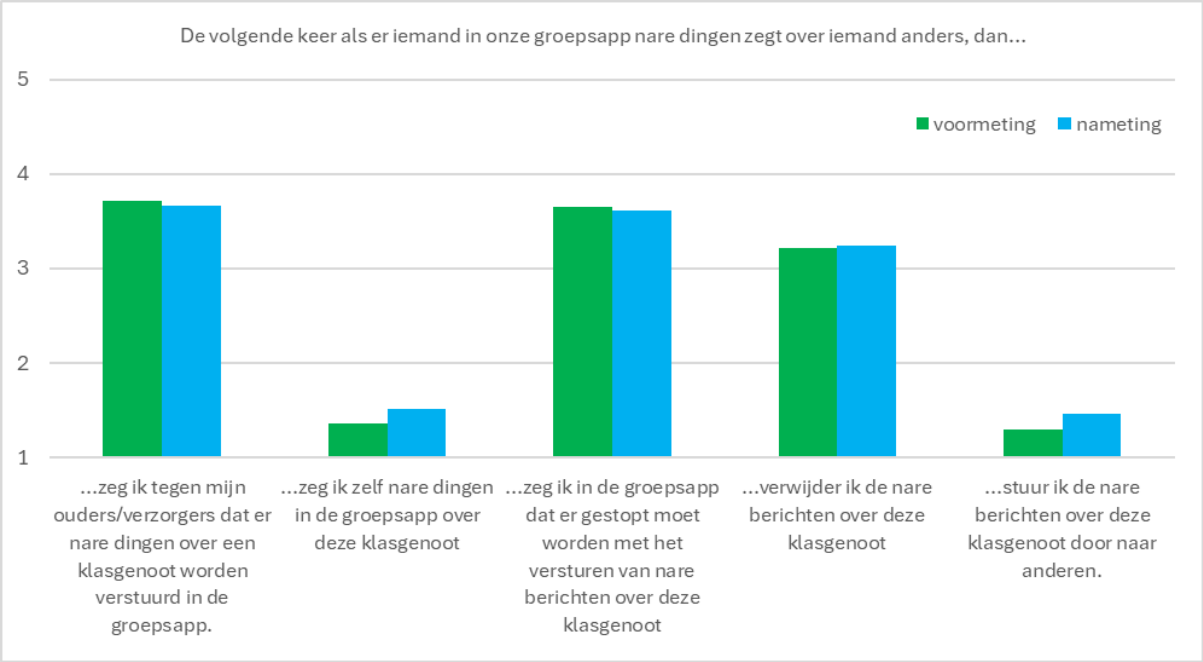
Noot: de verschillen bij Risicoperceptie (kans) en Zelfeffectiviteit zijn significant bij p<0.01.

6.3.6. Gedragsintentie

Vanwege de lage Cronbachs alfa voor het construct 'intentie tot gedrag' is ervoor gekozen om de verschillende items behorende bij dit construct apart te meten. Om de gedragsintentie van deelnemers te meten zijn vijf verschillende stellingen voorgelegd rondom de volgende situatiebeschrijving: *"De volgende keer als er iemand in onze groepsapp nare dingen zegt over iemand anders, dan…"* op een schaal van (1) zeker niet tot (5) zeker wel. Voor de positief geformuleerde gedragingen (stellingen 1, 3 en 4) zagen we geen significante toename van dit gedrag (Figuur 6). Voor de negatief geformuleerde gedragen (stellingen 2 en 5), zagen we wel een significante toename van pestgedrag. Na het spelen van de quest 'Online grenzen' geven kinderen aan dus eerder geneigd te zijn om zelf pestgedrag te vertonen dan vóór het spelen van het spel. Wel moet worden opgemerkt dat ook in de nameting de gemiddelde scores nog steeds laag zijn (1,51 en 1,46), wat betekent dat na het spelen van de klassenquest de meeste kinderen gemiddeld 'zeker niet' tot 'waarschijnlijk niet' overgaan tot pestgedrag.

Figuur 6

Gemiddelde scores (op Likert-schaal van 1 tot 5) op gedragsintentie bij online pesten



Noot: de verschillen bij item 2 en item 5 zijn significant.

6.4 Resultaten Hacken

6.4.1. Kennis

In de vragenlijst kregen de deelnemers zes stellingen voorgelegd met kennisvragen over hacken. Aan hen werd gevraagd om aan te geven of deze stelling in hun ogen waar of niet waar is, of dat ze dat niet wisten. In Tabel 7 zijn de scores weergegeven van de leerlingen in de voor- en nameting. Voor *alle stellingen* geldt dat er een *significant* verschil is tussen de voor- en nameting. Leerlingen waren na het spelen van het spel duidelijk beter op de hoogte van wat hacken is (35,1% > 52,5%), wat een goed wachtwoord is (75,3 > 83,7%), waartoe een firewall dient (53,8% > 76,3%), hoe je het een hacker moeilijk kunt maken met een ingewikkeld wachtwoord (76,9% > 84,1%), en dat er ook *white hat hackers* bestaan (62,2% > 72,2%). Dat hackers vaak geld of informatie proberen te stelen door in te breken op apparaten en netwerken van anderen, werd minder vaak als waar gezien (83,7% > 76,3%). De kennis van deelnemers over hacken en aanverwante thema's is dus grotendeels significant toegenomen.

Tabel 7

Scores respondenten op de kennisvragen over hacken uitgedrukt in percentages.

Stelling	Voormeting	Nameting	Verschil
Wanneer je inlogt op het account van iemand anders, dan ben je aan het hacken.	Waar 35,1% Niet waar 33,7% Weet ik niet 31,3%	Waar 52,5% Niet waar 23,1% Weet ik niet 24,4%	$X^2(2)=20,816$ p<.001
Een goed wachtwoord bestaat uit heel veel verschillende letters, cijfers en tekens.	Waar 75,3% Niet waar 12,8% Weet ik niet 12,0%	Waar 83,7% Niet waar 4,7% Weet ik niet 11,5%	$X^2(2)=12,972$ p=.002
Een firewall maakt het moeilijker voor een hacker om in jouw computer te komen.	Waar 53,8% Niet waar 5,2% Weet ik niet 41,0%	Waar 76,3% Niet waar 4,4% Weet ik niet 19,3%	$X^2(2)=37,749$ p<.001
Hackers proberen vaak geld of informatie te stelen door in te breken op apparaten en netwerken van anderen.	Waar 83,7% Niet waar 3,3% Weet ik niet 13,0%	Waar 76,3% Niet waar 7,1% Weet ik niet 16,6%	$X^2(2)=7,442$ p=.024
Hoe ingewikkelder jouw wachtwoord is, hoe moeilijker het voor een hacker is om het wachtwoord te kraken.	Waar 76,9% Niet waar 7,6% Weet ik niet 15,5%	Waar 84,1% Niet waar 4,1% Weet ik niet 11,9%	$X^2(2)=6,003$ p=.050
Er zijn ook hackers die hun kennis en talenten gebruiken voor goede dingen.	Waar 62,2% Niet waar 8,2% Weet ik niet 29,6%	Waar 72,2% Niet waar 7,5% Weet ik niet 20,3%	$X^2(2)=8,077$ p=.018

6.4.2. Risicoperceptie

Om risicoperceptie te meten is er een onderscheid gemaakt tussen de ervaren kans dat deelnemers slachtoffer kunnen worden van hacken (de vatbaarheid) en de ervaren ernst van slachtofferschap van hacken. Deelnemers kregen de volgende stelling voorgelegd: *"Bo is aan het hacken. Bo gebruikt stiekem het Instagram- en TikTok-account van andere kinderen. Bo plaatst daar zelf berichten (bv. teksten, plaatjes, filmpjes), en verwijdert daar ook berichten."*

Kans

Op de stelling "Het kan ieder kind overkomen dat zijn of haar sociale media gehackt wordt." – gemeten op een vijfpuntsschaal van (1) 'helemaal mee oneens' tot (5) helemaal mee eens – scoorden kinderen in de voormeting een 3,89. Ze zijn het er dus gemiddeld over eens dat het een kind kan overkomen om gehackt te worden. In de nameting is deze gemiddelde score nagenoeg hetzelfde (m = 3,80). Dit verschil is *niet* significant.

Ernst

Om de ervaren ernst te meten van slachtofferschap van hacken, zijn vier stellingen geformuleerd die ingaan op gevoelens van gespannenheid, veiligheid, boosheid en verdriet ten aanzien van potentieel slachtofferschap van hacken. Deze stellingen zijn samen als construct geanalyseerd. In de voormeting scoorden de deelnemers gemiddeld een 3,63 op een schaal van (1) helemaal niet tot (5) heel erg. In de nameting is deze score nagenoeg gelijk gebleven met een gemiddelde score van 3,61. In zowel de voormeting als de nameting gaven leerlingen aan dat het worden van slachtoffer van hacken een behoorlijke impact heeft. Het verschil tussen voor- en nameting is *niet* significant. De risicoperceptie rondom het thema hacken – zowel voor kans als ernst – is dan ook niet veranderd na het spelen van de klassenquest 'Online grenzen'.

6.4.3. Zelfeffectiviteit

Om zelfeffectiviteit te meten kregen leerlingen de volgende stellingen voorgelegd, gemeten op een schaal van (1) helemaal niet tot (5) heel erg veel: *"Ik heb er vertrouwen in dat ik een goed wachtwoord kan bedenken", "Ik heb er vertrouwen in dat ik voor verschillende accounts verschillende wachtwoorden kan aanmaken" en "Ik heb er vertrouwen in dat ik mijn wachtwoorden voor mijzelf kan houden (mijn wachtwoorden dus nooit met iemand anders deel)."* Deze stellingen zijn samen als één construct getoetst. In de voormeting was de gemiddelde score op zelfeffectiviteit 3,93; in de nameting scoorden leerlingen *significant* hoger op zelfeffectiviteit met een gemiddelde score van 4,11 ($t(602)=-2.814$; $p=.005$). Kinderen hebben er dus na het spelen van de quest 'Online grenzen' meer vertrouwen in dat zij in staat zijn om iets tegen hacken te doen dan voor het spelen van de quest. De gerapporteerde zelfeffectiviteit neemt dan ook toe.

6.4.4. Responseffectiviteit

Om responseffectiviteit te meten kregen leerlingen wederom de volgende situatie voorgelegd: *"Stel: Jij wilt je goed beschermen tegen hackers. Denk je…"*. Vervolgens is aan de hand van drie vragen in kaart gebracht in hoeverre kinderen de beschreven handelingsperspectieven (het gebruiken van een goed wachtwoord, meerdere wachtwoorden gebruiken voor meerdere accounts en je wachtwoord nooit met iemand delen) als nuttig en zinvol inschatten op een schaal van (1) helemaal niet tot (5) heel erg. Deze stellingen zijn samen als één construct getoetst. In de voormeting scoorden leerlingen gemiddeld een 4,19. Zij gaven aan dat ze deze maatregelen als erg nuttig en zinvol inschatten. In de nameting waren ze nog positiever over deze maatregelen met een gemiddelde score van 4,40. Dit verschil was significant

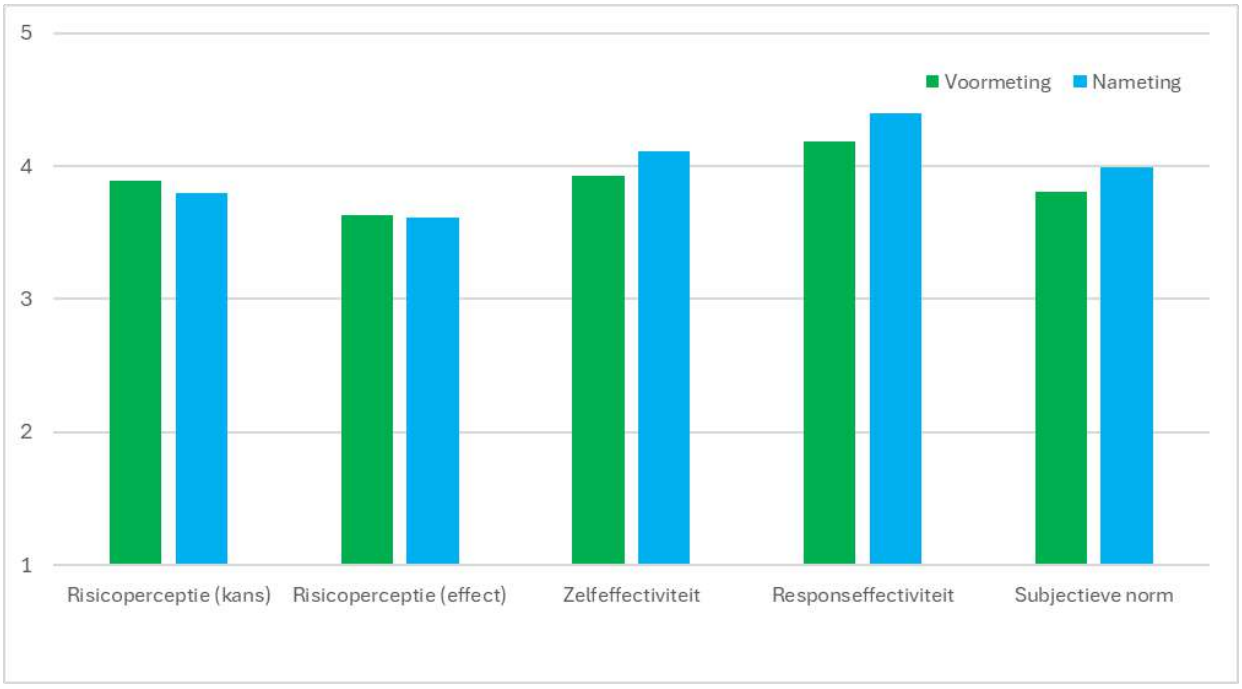
(t(610)=-3.407; p<.001). Het spelen van de klassenquest heeft een positieve invloed gehad op de gerapporteerde responseffectiviteit van deelnemers. Maatregelen die je beschermen tegen hackers werden als nuttiger gezien na het spelen van de quest.

6.4.5. Subjectieve normen

De subjectieve normen zijn gemeten aan de hand van drie stellingen waarbij leerlingen wederom dezelfde situatie voorgelegd kregen als bij de hierboven genoemde variabelen. Vervolgens is aan leerlingen gevraagd in hoeverre zij denken dat hun vrienden deze handelingsperspectieven (zoals het gebruiken van goede wachtwoorden) zouden uitvoeren op een schaal van (1) zeker niet tot (5) zeker wel. Deze stellingen zijn samen als één construct getoetst. In de voormeting scoorden leerlingen ruim boven gemiddeld (m = 3,81). In de nameting scoorden leerlingen gemiddeld nog hoger met een gemiddelde score van 3,99. Deze toename is *significant* (t(461)=-2.395; p=.017). Het spelen van de quest heeft dan ook een positieve invloed gehad op de gerapporteerde subjectieve normen van kinderen. Kinderen verwachten na het spelen van de quest nog meer weerbaar gedrag van vrienden dan voor het spelen van de quest. De gevonden resultaten voor het thema hacken zijn weergegeven in Figuur 7.

Figuur 7

Gemiddelde scores op constructen (Likert-schaal van 1 tot 5) in de voor-en nameting (hacken)



Noot: de verschillen bij zelfeffectiviteit, responseffectiviteit en subjectieve normen zijn significant.

6.4.6. Gedragsintentie

Aan de hand van drie items is de intentie tot cyberweerbaar gedrag rondom hacken gemeten. Deelnemers is gevraagd in hoeverre zij zelf (1) een goed wachtwoord gaan gebruiken, (2) meerdere wachtwoorden gaan gebruiken voor meerdere accounts en (3) wachtwoorden nooit met andere mensen zouden delen. Deze intenties tot cyberweerbaargedrag zijn gemeten op een schaal van (1) zeker niet tot (5) zeker wel. In de voormeting scoorden respondenten gemiddeld een 4,22. In de nameting was de gemiddelde score een 4,33. Ondanks deze kleine toename, was dit verschil *niet* significant. Dit zou verklaard kunnen worden doordat hier sprake is van een zogenaamd *plafondeffect:* De scores in de voormeting waren al dusdanig hoog dat een verdere toename niet aannemelijk is. Wel wordt duidelijk dat leerlingen dus sterk geneigd zijn om maatregelen te nemen om zichzelf te beschermen tegen hacken.

6.5 Resultaten van *agency*, verantwoordelijkheid en impulsiviteit

6.5.1. *Agency*

Om de variabele *agency* te meten zijn er drie stellingen voorgelegd aan de deelnemers. Deze items gaan allemaal over onderdelen van *agency*. Aangezien er geen interne consistentie was tussen de verschillende items, worden de items afzonderlijk van elkaar geanalyseerd.

Zoals in Tabel 8 te zien is, hebben leerlingen na het spelen van de quest het gevoel dat ze hun ouders/verzorgers meer kunnen leren over veilig internetten. In de voormeting scoorden leerlingen gemiddeld een 3,05. In de nameting was een *significante* toename zichtbaar en scoorden leerlingen gemiddeld een 3,25 ($t(661)=-2.378$; $p=.018$). Op de vraag of leerlingen het gevoel hebben dat ze het gesprek aan kunnen gaan met volwassenen over veilig internetten, scoorden leerlingen in de voormeting een 3,44. In de nameting was een kleine afname zichtbaar (m = 3,37). Dit verschil is echter *niet* significant. Leerlingen hebben dus zowel in de voor- als de nameting het gevoel dat ze redelijk in staat zijn om een gesprek over veilig internetten aan te gaan met een volwassene. Tenslotte is aan leerlingen gevraagd hoe vaak ze met een volwassene in hun omgeving praten over veiligheid op het internet. Deze vraag is gemeten op een schaal van (1) heel weinig tot (5) heel vaak. In de voormeting scoorden leerlingen gemiddeld een 2,50. Ze praten dus relatief weinig met een volwassene over dit thema. In de nameting is een kleine toename zichtbaar (m = 2,57). Dit verschil is echter *niet* significant. Het spelen van de quest 'Online grenzen' zorgt dus niet voor een toename in het praten over dit onderwerp met volwassenen. De *agency* is dus voor de meeste items niet toegenomen na het spelen van de quest. Alleen voor het item *"Ik kan mijn ouders/verzorgers iets leren over veilig internetten"* is een *significante* toename te zien.

Tabel 8

Gemiddelde scores voor agency in de voor- en nameting op een vijfpuntsschaal.

Stellingen	Gemiddelde score voormeting	Gemiddelde score nameting
Ik kan mijn ouders/verzorgers iets leren over veilig internetten.	3,05	3,25*
Ik kan een gesprek aangaan met volwassen over veilig internetten.	3,44	3,37
Hoe vaak praat je met volwassenen in jouw omgeving over veiligheid op het internet?	2,50	2,57

Noot: Items zijn apart getoetst (geen schaal met interne consistentie). * is significant bij p<0.05

6.5.2 Verantwoordelijkheid

Om in kaart te brengen wie – volgens de deelnemers – verantwoordelijk is voor hun veiligheid op het internet, zijn vijf vragen gesteld op een schaal van (1) helemaal mee oneens tot (5) helemaal mee eens. Hierbij is onderscheid gemaakt tussen de mate waarin kinderen vinden dat zij zelf verantwoordelijk zijn: *"Het is mijn eigen verantwoordelijkheid om mijzelf te beschermen tegen gevaren op het internet"* en de mate waarin zij vinden dat anderen (*ouders/verzorgen, juf/meester, overheidsinstellingen zoals de Politie en socialmediaplatforms zoals Instagram*) verantwoordelijk zijn voor hun veiligheid op het internet.

Allereerst is er gekeken naar de mate waarin kinderen vinden dat zij zelf verantwoordelijk zijn voor hun eigen veiligheid op het internet. Deelnemers scoren gemiddeld een 3,74 in de voormeting en vinden dus dat zij zelf behoorlijk verantwoordelijk zijn voor hun eigen veiligheid. In de nameting is een kleine afname te zien (m = 3,65), maar dit verschil is *niet* significant. Er verandert na het spelen van de quest dus niets in de mate waarin kinderen zichzelf verantwoordelijk houden voor hun veiligheid op het internet na het spelen van de quest.

Vervolgens is er gekeken naar de mate waarin kinderen anderen verantwoordelijk achten voor hun eigen veiligheid op het internet. De vier items die gaan over de verantwoordelijkheid van anderen (ouders/verzorgen, juf/meester, overheidsinstellingen zoals de Politie en socialmediaplatforms zoals Instagram) is als construct getoetst. In de voormeting scoorden leerlingen gemiddeld een 2,99. In de nameting was deze score vrijwel gelijk en dus *niet* significant (m = 3,00). Zij zijn dus neutraal als het gaat over de verantwoordelijkheid die anderen dragen voor hun eigen veiligheid en leggen de verantwoordelijkheid voor hun eigen online veiligheid voornamelijk bij zichzelf neer. Het spelen van de quest heeft geen invloed gehad op hun idee over wie verantwoordelijk is voor de veiligheid op het internet.

6.5.3. Impulsiviteit

Impulsiviteit werd gemeten aan de hand van een construct opgebouwd uit zes items op een schaal van (1) helemaal mee oneens tot (5) helemaal mee eens. De items waren:

1. Als ik online keuzes maak, dan denk ik daar altijd goed over na.
2. Als ik online keuzes maak, dan bespreek ik dat eerst met mijn ouders/verzorgers.
3. Als ik online keuzes maak, dan doe ik dat snel en zonder na te denken.
4. Ik heb wel eens te snel op een link geklikt waardoor ik een probleem kreeg.
5. Ik heb wel eens een bericht gestuurd waar ik snel spijt van kreeg.
6. Ik heb wel eens persoonlijke gegevens (bijv. foto's, adresgegevens) gestuurd naar iemand die ik helemaal niet (goed) ken.

Een hogere score op het construct betekent meer impulsief gedrag (voor de samenstelling van het construct zijn item 1 en 2 gespiegeld). Gemiddeld scoorden respondenten in de voormeting een 2,21. In de nameting scoorden zij gemiddeld een 2,18. Dit verschil is *niet* significant. Er is dus na het spelen van de klassenquest 'Online grenzen' *geen* afname in impulsiviteit zichtbaar.

6.6 Samenvatting resultaten vragenlijstonderzoek

De resultaten van het vragenlijstonderzoek worden samengevat in Tabel 9.

Tabel 9

Samenvatting van de resultaten van het vragenlijstonderzoek.

Kenmerk	**Online Pesten**	**Hacken**
Kennis	X	✓/X
Risicoperceptie	*Kans:* ✓(negatief) *Ernst:* X	*Kans:* X *Ernst:* X
Zelfeffectiviteit	✓(negatief)	✓
Responseffectiviteit	X	✓
Subjectieve normen	X	✓
Gedragsintenties	X/✓(negatief)	X
Agency	✓/X	
Verantwoordelijkheid	X	
Impulsiviteit	X	

Noot: Als een kenmerk significant is veranderd, wordt dit aangegeven met een ✓; als het kenmerk niet significant is veranderd met een X; als het significant is veranderd maar in de verkeerde richting met ✓(negatief)

7. Conclusie, discussie en aanbevelingen

In dit hoofdstuk geven we eerst antwoord op de onderzoeksvragen, om vervolgens af te sluiten met het antwoord op de hoofdvraag. Daarna behandelen wij de beperkingen van dit onderzoek en brengen wij op basis van de literatuur, de resultaten en onze observaties advies uit aan de ontwikkelaars van HackShield in de Klas.

7.1 Antwoorden op de onderzoeksvragen

Onderzoeksvraag 1: ***"In hoeverre draagt het spelen van HackShield bij aan het vergroten van kennis van deelnemers ten aanzien van cyberrisico's?"***

Een belangrijk doel van HackShield is om de kennis van kinderen (groep 5 t/m 8 in het basisonderwijs) over cybergerelateerde thema's te vergroten. In dit onderzoek is gekeken naar de mate van kennis van deelnemers over de thema's 'online pesten' en 'hacken'. Voor het thema 'online pesten' zagen we geen verandering in kennis onder de leerlingen. Zij hadden na afloop van de interventie vrijwel evenveel kennis als voorafgaand aan de interventie. Voor het thema 'hacken' zagen we wel een significante toename in kennisniveau; kinderen wisten na het spelen van de klassenquest 'Online grenzen' meer over hacken en aanverwante thema's dan voor het spelen van de quest. De quest 'Online grenzen' draagt dus gedeeltelijk bij aan het vergroten van kennis van deelnemers ten aanzien van cyberrisico's. Dit verschil in de mate van kennistoename komt wellicht doordat er in de quest meer aandacht is besteed aan kennis over 'hacken' dan kennis over 'online pesten'.

Onderzoeksvraag 2*: "In hoeverre draagt het spelen van HackShield bij aan het versterken van de cyberweerbaarheid van deelnemers ten aanzien van cyberrisico's?"*

Om een eventuele toename in cyberweerbaarheid te kunnen meten onder leerlingen in het basisonderwijs, is er gekeken naar onderdelen van cyberweerbaargedrag en de intentie van kinderen om cyberweerbaar gedrag te vertonen. Hierbij hebben we ons gericht op de twee thema's die aan bod komen in de klassenquest 'Online grenzen', namelijk 'online pesten' en 'hacken'.

Voor online pesten vonden we dat er geen positieve veranderingen optraden na het spelen van de quest 'Online grenzen' op zowel de onderdeln van cyberweerbaarheid als de gerapporteerde intentie

tot cyberweerbaar gedrag. De resultaten laten zien dat er geen verandering zichtbaar is voor responseffectiviteit (het ervaren nut van handelingsperspectieven) en subjectieve normen. Wel was er een kleine significante negatieve verandering zichtbaar in risicoperceptie en zelfeffectiviteit. Leerlingen schatten de kans kleiner in dat iemand online gepest zou kunnen worden na het spelen van de quest. Ook hadden zij er na het spelen van het spel significant *minder* vertrouwen in dat zij maatregelen zouden kunnen treffen om het risico op online pesten te verminderen dan voor het spelen van de quest.

Wat betreft de gerapporteerde intentie van leerlingen om cyberweerbaargedrag te vertonen kwam naar voren dat ook hier geen positieve effecten zichtbaar waren binnen het thema 'online pesten'. Leerlingen waren na het spelen van de quest niet meer geneigd om maatregelen te treffen om zichzelf te beschermen tegen online pesten dan voor het spelen van de quest. De intentie van leerlingen om zelf over te gaat tot pestgedrag was na de interventie iets toegenomen. Er was echter in zowel de voor- als de nameting een hele lage intentie tot pestgedrag zichtbaar. Ondanks een kleine significante toename, laten kinderen over het algemeen weinig intentie tot pestgedrag zien.

Voor het thema hacken zijn wel positieve effecten gevonden van het spelen van de quest 'Online grenzen' op de onderdelen van cyberweerbaar gedrag. De kennis over het onderwerp hacken en aanverwante thema's nam significant toe na het spelen van het spel. Ook de zelfeffectiviteit van leerlingen nam significant toe. Zij hadden er na het spelen van de quest meer vertrouwen in dat zij zichzelf zouden kunnen beschermen tegen hacken. Ook was er een significante toename in responseffectiviteit zichtbaar. De voorgestelde handelingsperspectieven werden na het spelen van de quest als nuttiger en zinvoller ingeschat dan voor het spelen van de quest. Ook verwachtten leerlingen na het spelen van het spel dat hun vrienden meer cyberweerbaar gedrag zouden vertonen; zij rapporteerden significant positievere subjectieve normen na het spelen van de quest. Alleen voor risicoperceptie was geen verschil zichtbaar voor- en na het spelen van de quest.

Wanneer vervolgens gekeken wordt naar de intentie tot cyberweerbaar gedrag werd voor het thema 'hacken' geen verschil gevonden in de voor- en de nameting. Er lijkt geen effect te zijn van het spelen van de quest 'Online grenzen' op de gerapporteerde intentie om maatregelen te treffen om je te beschermen tegen hacken en gerelateerde risico's. Dit kan mogelijk verklaard worden doordat er sprake was van een zogenaamd plafondeffect. In de voormeting scoorden leerlingen ver boven gemiddeld op de intentie tot cyberweerbaargedrag. Een verdere toename is daardoor eerder onwaarschijnlijk.

Onderzoeksvraag 3: ***"In hoeverre draagt het spelen van HackShield bij aan het vergroten van de agency van deelnemers ten aanzien van cyberweerbaarheid naar volwassenen in hun omgeving?"***

Ten slotte is in dit onderzoek gekeken naar de variabelen die uit de interviews met HackShield naar voren kwamen als belangrijke doelen van deelname aan HackShield. Er is hierbij gekeken naar de variabelen *agency*, verantwoordelijkheid en impulsiviteit.

Voor *agency* vonden we alleen een significante toename in de mate waarin deelnemers denken hun ouders iets te kunnen leren over veilig internetten. Voor de andere onderwerpen rondom *agency* werd geen verschil gevonden in de voor- en nameting. Ze praten relatief weinig met hun ouders/verzorgers over veiligheid op het internet en het spelen van de quest had hier geen invloed op. Wel hebben leerlingen het gevoel dat ze een gesprek aan kunnen gaan met hun ouders over veilig internetten. Dit nam echter niet (verder) toe door het spelen van het spel.

Aan de hand van de interviews met medewerkers van HackShield kwam naar voren dat er nog twee relevante variabelen zijn waar HackShield op probeert in te spelen met de klassenquests, namelijk verantwoordelijkheid en impulsiviteit. Deze variabelen zijn daarom ook meegenomen in dit onderzoek.
Voor verantwoordelijkheid vonden we geen effect van de interventie op de mate waarin kinderen zichzelf of anderen verantwoordelijk achten voor hun eigen online veiligheid. Zij vinden dat zijzelf grotendeels verantwoordelijk zijn voor veiligheid op het internet. Zij leggen deze verantwoordelijkheid meer bij zichzelf neer dan bij anderen. Dit is niet verandert na het spelen van de quest.

Tenslotte is gekeken naar de mate van impulsiviteit die leerlingen laten zien bij het maken van keuzes op het internet, bijvoorbeeld in hoeverre ze bij online keuzes goed nadenken of het eerst met hun ouders bespreken. Over het algemeen geven de leerlingen aan niet te impulsief keuzes te maken op het internet. Hierbij was geen verschil zichtbaar tussen de voor- en nameting.

Hoofdvraag: ***"In hoeverre vertonen deelnemers van HackShield een toename in (1) de eigen cyberweerbaarheid en (2) agency ten aanzien van cyberweerbaarheid naar volwassenen in hun omgeving?"***

De onderzochte klassenquest is representatief voor het aanbod van Hackshield en bestaat uit twee thema's: online pesten en hacken. De resultaten zijn duidelijk verschillend voor de twee thema's. Voor het thema 'online pesten' is er geen positieve verandering gemeten voor wat betreft de onderdelen die samenhangen met de cyberweerbaarheid van leerlingen. Ook lieten leerlingen na het spelen van de quest

geen verandering zien in de intentie om maatregelen te treffen tegen online pesten. In enkele gevallen zijn contraproductieve effecten vastgesteld. Voor het thema 'hacken' is een gedeeltelijke toename te zien op de onderdelen die samenhangen met de cyberweerbaarheid van leerlingen. Voor dit thema was geen toename te zien in de mate waarin leerlingen aangeven maatregelen te willen gaan treffen tegen hacken.

Het spelen van de quest leidt niet direct tot een verandering in '*agency*'. Kinderen zijn op basis van deze quest niet meer geneigd om het gesprek aan te gaan over cyberweerbaarheid met volwassenen in hun omgeving en vertonen niet de intentie om het geleerde binnen de quest uit te dragen in de maatschappij. Ook op de overige variabelen die voor HackShield van belang zijn (dragen van verantwoordelijkheid en tegengaan van impulsiviteit), is geen verschil gemeten. Een samenvatting van alle resultaten in dit onderzoek is te vinden in Tabel 10.

Tabel 10

Samenvatting van alle resultaten

	Online pesten		**Hacken**	
	Inhoudsanalyse	*Vragenlijstonderzoek*	*Inhoudsanalyse*	*Vragenlijstonderzoek*
	Component aanwezig?	Significant verschil?	Component aanwezig?	Significant verschil?
Kennis	✓	X	✓	✓/X
Risicoperceptie	✓	✓(negatief)/X	✓	X
Zelfeffectiviteit	X	✓(negatief)	✓	✓
Responseffectiviteit	X	X	✓/X	✓
Subjectieve normen	X	X	✓/X	✓
Gedragsintentie	n.v.t.	✓(negatief)/X	n.v.t.	X
Verantwoordelijkheid	X	✓/X	X	✓/X
Verminderde impulsiviteit	✓/X	X	✓	X
Agency	X	X	✓	X

Noot: een ✓ duidt op aanwezigheid van het kenmerk (inhoudsanalyse) of een significante verandering (vragenlijst). De toevoeging 'negatief' duidt op een effect in de verkeerde richting. Een X duidt op afwezigheid of geen significante verandering.

7.2 Discussie

In dit onderzoek is gekeken naar het effect van het spelen van de klassenquest 'Online grenzen' op de onderdelen van – en gerapporteerde intentie van kinderen tot - cyberweerbaargedrag. Ondanks dat dit onderzoek zeer zorgvuldig is uitgevoerd, zijn er een aantal limitaties aan te wijzen.

HackShield bestaat uit een individueel spel en (op dit moment) twaalf klassenquests. Gezien de duur van dit onderzoek was het niet mogelijk om alle onderdelen van HackShield te evalueren. Er is

daarom gekozen om in dit onderzoek te kijken naar een specifieke klassenquest, namelijk ‘Online grenzen’. Deze specifieke klassenquest is in overleg met de ontwikkelaars van HackShield als representatief aangemerkt voor HackShield in de Klas en wordt volgens hen veruit het meest gespeeld van alle ontwikkelde klassenquests. Er kan in dit onderzoek daardoor enkel een uitspraak worden gedaan over het effect van deze specifieke klassenquest ‘Online Grenzen’, en niet voor HackShield in de Klas als geheel.

Daarnaast bleek het lastig om scholen te motiveren om deel te nemen. Leerkrachten zagen vaak weinig ruimte om de klassenquest te spelen met hun leerlingen en voelden zich grotendeels onvoldoende geëquipeerd om de les zelf te verzorgen. Dit maakte het uitdagend om voldoende scholen te vinden voor het onderzoek. De uiteindelijk geselecteerde scholen kunnen als bovengemiddeld gemotiveerd worden beschouwd. Doordat leerkrachten in de meeste gevallen niet zelf de les hebben verzorgd – en een groot deel van de interventie valt of staat met de wijze waarop invulling wordt gegeven aan de groepsdiscussies – kan het zijn dat de gastdocenten die de lessen hebben verzorgd invloed hebben gehad op de uitkomsten van dit onderzoek. Er kan worden verwacht dat medewerkers van HackShield beter op de hoogte zijn van de inhoud en de doelen van het spel. Daardoor kunnen de lessen minder representatief zijn geweest dan wanneer alleen eigen docenten de begeleiding op zich hadden genomen.

Tevens moest een controleconditie worden losgelaten vanwege de problemen met het werven van deelnemers en het lange tijdspad waarin de data zijn verzameld. Door de lange doorlooptijd van het onderzoek was het niet meer mogelijk om een zuivere controleconditie in te zetten. We hebben daardoor in plaats van het beoogde 'voormeting-nameting-controlegroep-ontwerp' (Quené & van den Bergh, 2026) moeten terugvallen op het 'één-groep-voormeting-nameting-ontwerp' (Quené & van den Bergh, 2026), waardoor een eventueel verschil tussen de voor- en nameting niet uitsluitend kan worden toegeschreven aan het spelen van de klassenquest 'Online grenzen', maar ook het gevolg zou kunnen zijn van het herhaald invullen van de vragenlijst of anderszins leren rondom cyberweerbaarheid. Hierdoor is het lastig om bijvoorbeeld een *history effect* vast te stellen dat mogelijk een bedreiging voor de validiteit van het onderzoek zou kunnen vormen. Echter, aangezien bij dit veldonderzoek de metingen uitgesmeerd zijn over een lange tijd, en er nametingen op sommige scholen plaats hebben gevonden vóór voormetingen op andere scholen, zal een dergelijk eventueel effect onderdrukt zijn. Er is ook geen aanleiding geweest te denken dat er tijdens het onderzoek op de onderzochte thema’s maatschappelijke veranderingen zijn geweest die effect zouden kunnen hebben op meerdere scholen tegelijkertijd in Nederland, en zo de nameting hebben beïnvloed.

Een laatste aandachtspunt van dit onderzoek gaat over de wijze van dataverzameling. Er is voor gekozen om te werken met vragenlijstenonderzoek. Een nadeel hiervan is dat het om zelfgerapporteerd gedrag gaat; er wordt geen daadwerkelijk gedrag gemeten. Ondanks dat onderzoek laat zien dat intentie tot gedrag een belangrijke graadmeter is voor daadwerkelijk gedrag, kan niet met zekerheid worden vastgesteld dat de gerapporteerde gedragsintenties van de leerlingen ook overeenkomen met hun daadwerkelijke gedrag (zie ook Van 't Hoff- de Goede et al., 2025). Oorspronkelijk was het idee om naast een kwantitatieve analyse ook een kwalitatieve analyse ter verificatie van resultaten uit te voeren. Het was van meerwaarde geweest om leerlingen na het spelen van de quest ook te spreken, om verklaringen voor gevonden verschillen beter te kunnen duiden. Er was echter meer tijd nodig om voor deze effectevaluatie voldoende grip te krijgen op de doelstellingen, werkwijze en veronderstelde effecten van HacksShield in de klas. Omdat deze niet in detail beschikbaar waren, moesten deze via gesprekken met de ontwikkelaars van HackShield in de klas worden opgehaald, gesynthetiseerd en aan hen ter toetsing worden voorgelegd. Omdat het beschikbare budget voor dit evaluatieonderzoek niet kon worden aangepast, was er geen ruimte voor deze kwalitatieve stap.

7.3 Aanbevelingen

De klassenquest 'Online grenzen' wordt door leerlingen *overall* beoordeeld met een ruime voldoende (een 7,1 als rapportcijfer). Het wordt grotendeels gezien als leuk en interessant. De quest trekt daarmee de aandacht en motiveert leerlingen mee te doen.

Toch bleken de resultaten op met name online pesten niet te wijzen op positieve veranderingen in intentie tot gedrag onder deelnemers. Dit is waarschijnlijk te verklaren doordat er onvoldoende elementen in de quest verwerkt zitten die inspelen op het uitdragen van zinvolle en gemakkelijk uit te voeren handelingsperspectieven. Online pesten is een complex thema waarbij ook de sociale omgeving en de dynamieken tussen leeftijdsgenoten een grote rol spelen (Spithoven & van Tuijl, 2024; van Houten en Spithoven, 2026). Het is daardoor niet eenvoudig om een goed werkende interventie te ontwikkelen ten behoeve van het tegengaan van online pestgedrag. Effectieve interventies met als doel om de cyberweerbaarheid van deelnemende leerlingen te vergroten zouden – op basis van wetenschappelijke inzichten – idealiter voldoen aan verschillende voorwaarden. Zo zouden deelnemers zich allereerst bewust moeten zijn van het risico en dat dit risico ook voor henzelf een potentiële dreiging zou kunnen zijn. Vervolgens hebben deelnemers concrete handelingsperspectieven nodig; maatregelen die hen kunnen helpen bij het verminderen van het risico of de dreiging. Deze handelingsperspectieven moeten zo zijn opgesteld dat deelnemers (1) er vertrouwen in hebben dat ze deze maatregelen zelf kunnen

uitvoeren en (2) het gevoel hebben dat deze maatregelen nuttig en zinvol zijn in het verminderen van het risico. Op dit moment zitten deze onderdelen – voor het thema 'online pesten' – onvoldoende verweven in de klassenquest 'Online grenzen'. Voor het onderdeel 'hacken' is duidelijk nog winst te behalen ten aanzien van de gedragsintentie: de neiging om zichzelf meer tegen het risico te beschermen. Het verdient de aanbeveling om te overwegen voor online pesten een zelfstandige klassenquest te ontwikkelen en *overall* het aantal doelstellingen en thema's per quest naar beneden te brengen: elk thema bevat immers een complex thema en gedragsverandering heeft, gezien de complexiteit van dit proces, focus nodig.

Het beoogde aspect van '*agency*' in de inhoud van klassenquest 'Online grenzen' komt op dit moment nog onvoldoende uit de verf om effect van te verwachten. Hierop zou – indien men aan dit doel wil vasthouden – meer gerichte aanpassing van de quest nodig zijn. Het zou aan te bevelen zijn om alle klassenquests van HackShield inhoudelijk langs het in dit effectonderzoek uiteengezette theoretische kader en de ontwikkelde (of aangevulde) meetlat van cyberweerbaarheid, onderdelen daarvan en *agency* te leggen, om deze aspecten gestructureerd te integreren in de verschillende klassenquests van HackShield. Daarnaast sterkt het de aanbeveling om de handelingsadviezen in samenwerking met experts op de specifieke thema's te ontwikkelen, bij hen te toetsen en deze in samenwerking actueel te houden. Tevens zou aanvullend advies of begeleiding door experts op het gebied van gedragsverandering (onder kinderen) kunnen bijdragen aan het realiseren van meer cyberweerbaar gedrag onder deelnemende leerlingen.

Ook wordt Hackshield in de Klas door de makers specifiek aangeduid als een veilige spelomgeving waarbinnen je kunt experimenteren, en waar je de gevolgen van je eigen keuzes kunt ervaren zonder grote consequenties. Bij de onderzochte quest zagen we echter dat er geen alternatieve scenario's worden geboden: elke gemaakte keuze leidt tot hetzelfde gevolg. Hiermee lijkt de potentiële kracht van een *serious game* niet ten volle benut te worden. Het zou zinvol kunnen zijn om in de quest onderdelen toe te voegen waarbij gemaakte keuzes daadwerkelijk leiden tot andere gevolgen. Hierdoor leren kinderen beter wat het gevolg van hun handelen zou kunnen zijn en wat de opbrengsten zijn van cyberweerbaargedrag.

Tenslotte kwam gedurende dit onderzoek naar voren dat leerkrachten zich over het algemeen niet voldoende geëquipeerd voelen om zelfstandig aan de slag te gaan met HackShield in de Klas. Van de negen scholen die hebben deelgenomen aan dit onderzoek, hebben de leerkrachten van slechts twee scholen het spel zelf begeleid. De overige scholen hebben gebruik gemaakt van een gastles van HackShield. Het is aan te bevelen voor HackShield om nog duidelijkere instructies te schrijven voor

leerkrachten – en wellicht instructievideo’s op te nemen - over de wijze waarop zij aan de slag kunnen met HackShield in de Klas.

Literatuur

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, *84*(2), 191-215. https://doi.org/10.1037/0033-295X.84.2.191

Bekkers, L., van't Hoff-De Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers & Security*, *127*, 103099.

Berding, J. & Witte, T. (2013) *Praktijkonderzoek op niveau. Inspelen op onderzoeksdilemma's bij sociale studies*. Coutinho.

Coady, M. (2008). Beings and Becomings: Historical and philosophical considerations of the child as citizen. In G. MacNaughton, P. Hughes & K. Smith (Eds.), Young Children as Active Citizens (pp. 2-14). Newcastle: Cambridge Scholars Publishing.

Deci, E.L., Ryan, R.M. (1995). *Human Autonomy*. In: Kernis, M.H. (eds) Efficacy, Agency, and Self-Esteem. The Springer Series in Social Clinical Psychology. Springer, Boston, MA. https://doi.org/10.1007/978-1-4899-1280-0_3

De Lange, R., Schuman, H. & Montesano Montessiori, N. (2011). *Praktijkgericht onderzoek voor reflectieve professionals*. Garant.

De Pauw, E., De Prins, F. & Spithoven, R. (2022). Samenwerken in de veiligheidsketen. In: R. Spithoven, et al. (red.). *Basisboek integrale veiligheid.* Den Haag: Boom criminologie, p. 147-174.

De Vaus, D. (2001) Research design in social research. Los Angeles : Sage.

Farshadkhak, S., van Slyke, C. & Fuller, B. (2021). Onlooker effect and affective responses in information security violation mitigation. *Computers & Security, 100*, 102082. https://doi.org/10.1016/j.cose.2020.102082

Flavour (z.d.). Hero Centered Design. Via: https://www.flavour.nl/hero-centered-design/.

Griffin, R. J., Dunwoody, S., Dybro, T., & Zabala, F. (1994). The relationship of communication to risk perceptions and preventive behavior related to lead in drinking water. In *Science Communication Interest Group, Association for Education in Journalism and Mass Communication, at the 1994 annual convention.* Atlanta, GA.

HackShield (z.d). HackShield Future Cyber Heroes. Via: https://nl.joinhackshield.com/nl.

Halevi, T., Lewis, J., & Memon, N. (2013, May). A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd international conference on world wide web* (pp. 737-744).

Hammond, S. P., Polizzi, G., & Bartholomew, K. J. (2023). Using a socio-ecological framework to understand how 8–12-year-olds build and show digital resilience: A multi-perspective and multimethod qualitative study. *Education and Information Technologies*, *28*(4), 3681-3709. https://doi.org/10.1007/s10639-022-11240-z

Hillmann, J. & Guenther, E. (2021). Organizational Resilience: A Valuable Construct for Management Research? International Journal of Management Reviews, 23, 7-44. https://doi.org/10.1111/ijmr.12239

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

Leukfeldt, E.R. (2024). Meer dan alleen een goed idee. Naar een empirisch onderbouwde aanpak van cybercrime. Universiteit Leiden (Oratie).

Leukfeldt, E.R., Spithoven, R., Jansen, J. & Van Amersfoort, C. (2025). Een SPRONG naar cyberweerbaarheid: onderzoeksagenda. Cyberweerbaar NL. www.cyberweerbaarnl.nl

Kievik, M. (2017). The time of telling tales: The determinants of effective risk communication. [PhD Thesis - Research UT, graduation UT, University of Twente]. University of Twente. https://doi.org/10.3990/1.9789036544269

Leukfeldt, R. Spithoven, R., Jansen, J., & Van Amersfoort, C. (eds.) (2025). *Een sprong naar cyberweerbaarheid. Onderzoeksagenda.* Boom / CyberweerbaarNL.

Maiman, L. A., & Becker, M. H. (1974). The health belief model: Origins and correlates in psychological theory. *Health education monographs, 2*(4), 336–353.

Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: a new method for characterising and designing behaviour change interventions. *Implementation science, 6*, 1-12.

Misana-ter Huurne, E.F.J., van Houten, Y.A., Spithoven, R., Notté, R.J. & Leukfeldt, E.R. (2020). *Cyberweerbaarheid. Risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb'ers.* Lectoraat Maatschappelijke Veiligheid, Hogeschool Saxion & Lectoraat Cybersecurity in het mkb, De Haagse Hogeschool.

Nationaal Cyber Security Center (NCSC). (2022). NCSC Onderzoeksagenda 2023-2026. Geraadpleegd van www.ncsc.nl/documenten/publicaties/2022/oktober/11/ncsc-onderzoeksagenda-2023---2026

Neighbors, C., Lee, C. M., Lewis, M. A., Fossos, N., & Larimer, M. E. (2007). Are social norms the best predictor of outcomes among heavy-drinking college students?. *Journal of studies on alcohol and drugs*, *68*(4), 556-565.

NWO (2018). Nederlandse gedragscode wetenschappelijke Integriteit. Via: Nederlandse gedragscode wetenschappelijke integriteit | NWO.

Paris, C., & Lung, P. (2008). Agency and child-centered practices in novice teachers: Autonomy, efficacy, intentionality, and reflectivity. *Journal of early childhood teacher education*, *29*(3), 253-268. https://doi.org/10.1080/10901020802275302

Pawson, R., & Haarhuis, C. K. (2005). Evaluatie van complexe programma's: Een theoriegestuurde aanpak. Justitiële verkenningen, 31(8), 42.

Quené H, van den Bergh H. (2026). Kwantitatieve Methoden en Statistiek. GutHub. Via: https://hugoquene.github.io/KMS-NL/ch-ontwerp.html

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

Rose, G. (2001) Visual methodologies. London : Sage publications.

Ruiter, R.A.C., Kessels, L.T.E., Peters, G.Y. & Kok, G. (2024). Sixty years of fear appeal research: Current state of evidence. *International Journal of Psychology*, *49*(2), 63–70.

Saldaña, J. (2012) The Coding Manual for Qualitative Researchers. Second edition. London : SAGE Publications.

Schiks, J., Hansen, S., Foppen, E., Leukfeldt, R. & Spithoven, R. (2021). *HackShield in Noord-Holland - Een evaluatie van de implementatie en resultaten van HackShield in Noord-Hollandse gemeenten.* Haagse Hogeschool / Hogeschool Saxion.

Slovic, P. (2004). What's fear got to do with it - It's affect we need to worry about. *Mo. L. Rev.*, *69*, 971-990.

Slovic, P., & Peters, E. (2006). Risk Perception and Affect. *Current Directions in Psychological Science*, *15*(6), 322-325. https://doi.org/10.1111/j.1467-8721.2006.00461.x

Spithoven, R., Misana-ter Huurne, E., & van Houten, Y. (2022). Towards a holistic theoretical model on the psychological dynamics underlying cyber resilience. *Society For Risk Analysis Benelux Chapter Conference*, 3 oktober 2022.

Spithoven, R. & van Tuijl, C. (2024). Cyberpesten. Theorie over en onderzoek naar de onbegrensde, digitale leefwereld van kinderen en adolescenten in Nederland. Boom

Spithoven, R. (2020). *Verbonden risico's. Maatschappelijke veiligheid in de black box society.* Boom Criminologie.

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

Sunstein, C. R. (1996). Social norms and social roles. *Colum. L. Rev.*, *96*, 903.

Van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407-412.

van Houten, Y., & Spithoven, R. (2026). Results of a Questionnaire on Prevalence, Impact, Roles and Experienced Supervision in Traditional and Online Bullying Situations during Secondary Education among Adolescents in the Netherlands. In *Bullying Today - Power, Pain and Prevention in the Context of the 21st Century* [Working Title]. IntechOpen. https://doi.org/10.5772/intechopen.1013069

Vannucci, A., Simpson, E. G., Gagnon, S., & Ohannessian, C. M. (2020). Social media use and risky behaviors in adolescents: A meta-analysis. *Journal of adolescence*, *79*, 258-274. https://doi.org/10.1016/j.adolescence.2020.01.014

Van 't Hoff-de Goede, M.S., Leukfeldt, E.R., van de Weijer, S.G.A, & van der Kleij, R. (2025). Does protection motivation predict self-protective online behaviour? Comparing self-reported and actual online behaviour using a population-based survey experiment. *Computers in Human Behavior Reports*, 100649. https://doi.org/10.1016/j.chbr.2025.100649

Vissenberg, J. & d'Haenens, L. (2020). Protecting youths' wellbeing online: Studying the association between opportunities, risks and resilience. *Media and communication, 8*(2), 175 – 184. https://doi.org/10.17645/mac.v8i2.2774

Vissenberg, J., d'Haenens, L., & Livingstone, S. (2022). Digital literacy and online resilience as facilitators of young people's well-being? A systematic review. *European Psychologist, 27*(2), 76–85. https://doi.org/10.1027/1016-9040/a000478

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health education & behavior*, *27*(5), 591-615.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329-349. https://doi.org/10.1080/03637759209376276

Woodhead, M. (2006). Changing perspectives on early childhood: theory, research and policy. *Paper commissioned for the EFA Global Monitoring Report 2007, Strong foundations: early childhood care and education* (Vol. 4, No. 2, pp. 1-43).

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. International Journal of Human-Computer Studies, 131, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Bijlage 1: Lesbrief Online Grenzen

Voorbereidingstijd

15 minuten

Lesduur

45 minuten

Welke les wil je doen?

In deze klassenquest worden de onderwerpen 'Hacken' en 'Cyberpesten' besproken. Je kunt zelf kiezen waar je de nadruk op legt. We hebben beide onderwerpen in deze les voor je uitgewerkt. Je kunt deze quest daarom twee keer met jouw klas spelen! De eerste uitwerking gaat over Hacken en de tweede uitwerking gaat over Cyberpesten. Veel plezier!

Doelgroep

Groep 5 t/m 8
Geschikt voor leerlingen tussen de 8 en 12 jaar.

Lesdoelen

Cyberpesten
Leerlingen weten...

- wat ze zelf kunnen doen wanneer ze online gepest worden.
- dat online pesten, net als offline pesten, grote gevolgen kan hebben.
- dat de rol van toeschouwers heel belangrijk is als het gaat om online pesten, en dat je daarin ook een verantwoordelijkheid hebt.

Hacken
Leerlingen weten...

- dat je als hacker kunt besluiten om je het goede of slechte pad op te gaan.
- welke gevolgen/consequenties hacken kan hebben voor henzelf en voor slachtoffers.
- hoe ze hun digitale skills veilig en op een goede manier kunnen inzetten.
- wat cybercrime inhoud.

SLO
Digitale geletterdheid
Kerndoel 3: Veiligheid en privacy
Doelzin: De leerling gaat veilig om met digitale systemen, data en de privacy van zichzelf en anderen. Het gaat hierbij om:

- adequaat omgaan met ongepaste content, ongepast gedrag en veiligheidsrisico's in digitale omgevingen.
- herkennen van veiligheidsrisico's bij het gebruik van digitale systemen en data

Kerndoel 8: Digitale technologie, jezelf en de ander
Doelzin: De leerling maakt weloverwogen keuzes bij het gebruik van digitale technologie en digitale media. Het gaat hierbij om:

- online communiceren en handelen op respectvolle en verantwoorde wijze;

Burgerschap
Kerndoel 1: Schoolcultuur
Doelzin: De school zorgt voor een democratische cultuur. Het gaat hierbij om:

- Stimuleren van kritische denkvaardigheden, morele en ethische oordeelsvorming en het offline en online respectvol communiceren daarover;

Kerndoelen 2: Diversiteit
Doelzin: De leerling handelt respectvol vanuit kennis over diverse samenleving. Het gaat hierbij om:

- in gedrag rekening houden met ervaringen en perspectieven van anderen.

Kerndoel 3: Democratische waarden
Doelzin: De leerling geeft aan hoe diens handelen verbonden is met democratische waarden. Het gaat hierbij om:

- verkennen op basis van morele en ethische perspectieven wat rechtvaardigheid en verantwoordelijk handelen betekent voor
- afwegen hoe het eigen handelen effect heeft op de omgeving en het welzijn van anderen, nu en in de toekomst.

Kerndoel 4: Maatschappelijke betrokkenheid
Doelzin: De leerling verkent verschillende mogelijkheden om bij te dragen aan de samenleving. Het gaat hierbij om:

- verkennen van de eigen mogelijkheden om maatschappelijke betrokkenheid vorm te geven.

Benodigdheden

- Digibord *(te besturen met touch, muis of pijltjes op toetsenbord)*
- Leerkracht account voor HackShield (maak deze hier aan).

Begrippen*:

Trollen:	Nepaccounts die worden ingezet om met heel veel accounts tegelijkertijd één iemand te belagen.
Omstanders:	Mensen die getuige zijn van een situatie waarin iemand gepest wordt en er niet aan meedoen, maar ook niet iemand verdedigen.
White hat hacker:	Als ethisch hacker gebruik je je talent voor goede dingen. Je probeert systemen niet te hacken om geld of gegevens te stelen maar je probeert ze te hacken om te laten zien hoe ze de systemen veiliger kunnen maken.
Black hat hacker:	Een criminele hacker die zijn vaardigheden gebruikt om informatie of geld te stelen.
Firewall:	Een online 'brandmuur' die probeert jouw netwerk en computer virus en spyware vrij te houden.
Malware:	Een samenstelling van 'malicious' en 'software', oftewel kwaadaardige software. Het gaat om een stuk code dat is geschreven met het doel om gegevens, netwerken of hosts te stelen, beschadigen of verstoren.
Virus scanner:	Een programma dat de computer controleert op aanwezigheid van virussen.
Server:	Computer die diensten verleent aan andere computers, zoals berichten versturen, iets opzoeken of gegevens opslaat.

Algemeen

In deze klassenquest komen de leerlingen erachter wat hacken is, wat de gevolgen kunnen zijn van cyberpesten en welke keuzes je kunt maken. Sanne gaat op oorlogspad, want ze wordt gepest, en zet daarvoor hacken in. Ze komt er samen met de klas achter dat dit niet de beste manier is om pesten tegen te gaan, maar dat ze haar vaardigheden als hacker op een goede manier zou kunnen gebruiken.

Handig om te weten

Neem zelf een kijkje op de website van HackShield, zodat je kunt zien hoe HackShield en de klassenquest eruit zien. Dit kost ongeveer een half uur. Vergeet niet dat je een leerkracht account nodig hebt om dit met de klas te spelen. Die kun je hier aanmaken.

Uitwerking - Hacken

Introductie - 10 min
Vertel de leerlingen dat jullie het gaan hebben over hacken. Wat is hacken? Waarom zou je het doen? En mag dat eigenlijk wel?

Introductievragen

- Is het je wel eens overkomen dat jij of iemand die je kent werd gehackt?
- Wat heb je gedaan om dit op te lossen?
- Wat doen jullie om hacken van jullie account tegen te gaan?
- Heb je wel eens ingelogd op een account dat niet van jou was?
- Heb je zelf wel eens gehackt? Waarom deed je dat?

Leuk om samen uit te proberen!

Ga met de klas naar de wachtwoordkraaktest van Veiliginternetten.nl. Laat iemand uit de klas de tekens tellen van zijn of haar meest gebruikte wachtwoord en vul samen de test in. Hoe veilig is dat wachtwoord eigenlijk? Ligt het aan verschillende soorten tekens of juist de hoeveelheid tekens? Vertel dat het gemakkelijk en veilig is een wachtZIN te maken. Deze kun je goed onthouden en er zitten spaties tussen de woorden die bijna niet te kraken zijn!

Kern - 30 min
Start de quest op het digibord. Geef aan dat jullie nu gaan starten met de game en bespreek regels die passen bij jouw klas wanneer jullie klassikaal een spel op het digibord spelen.

Hoe maak ik de les interactiever?

- In de quest vertellen Sanne en André van alles over het internet. Dit is in tekst beschreven. Je kunt ervoor kiezen om kinderen de tekst van een specifiek karakter te laten voorlezen (bijvoorbeeld kind x leest de tekst van André en kind y de tekst van Sanne).
- Tijdens de quest zullen er keuzes gemaakt moeten worden. Je kunt ervoor kiezen om een actieve werkvorm daarbij te gebruiken. Bijvoorbeeld: Als je denkt dat we rechts moeten gaan, mag je gaan staan. Als je denkt dat we rechtdoor moeten, dan mag je blijven zitten op je stoel. En als je denkt dat we links moeten, dan mag je op de grond gaan zitten.
- Doe de klassenactiviteiten! (zie de klassenactiviteiten op de volgende pagina)

Tip

Wil je het geluid uit tijdens de quest? Dat kun je doen in het opties menu van de game voordat je een klassenquest start.

Klassenactiviteiten in de quest

Onderstaande vragen worden als klassenactiviteiten aangeboden door Koi (zie afbeelding) in de quest. Je kunt als leerkracht zelf kiezen of je de activiteiten wilt doen (tijdens de quest). Je kunt de vragen natuurlijk ook op een ander moment nog bespreken!

De klassenactiviteiten met de nadruk op **Hacken** zijn **oranje**:

1. **Wat zouden redenen kunnen zijn voor iemand om te gaan cyberpesten?**
   Suggesties:
   - *Bang om zelf gepest te worden en dus bij het andere 'kamp' aansluiten.*
   - *Boos of verdrietig zijn en zich af willen reageren om beter te voelen.*

2. **Sanne is nu aan het hacken, omdat ze gepest wordt. Maar wat zouden jullie een reden vinden om te gaan hacken?**
   Suggesties:
   - *Om te kijken of een website wel veilig is.*
   - *Om geld te jatten*
   - *Nieuwsgierigheid*
   - *Erkenning of waardering*
   - *Gewoon heel tof*
   - *"Hij heeft vast ook wel eens iemand gehackt"*
   - *"Hij had een slecht wachtwoord"*
   - *"Het is niet onze schuld dat hij zijn computer/account niet beveiligt"*
   - *"Er zijn toch geen slachtoffers"*
   - *"Er is toch geen (financiële) schade"*
   - *"Het is niet alsof we iets kapot maken"*
   - *"Hier leert hij weer van"*
   - *"Het is maar een geintje"*
   - *"Ik doe niks fout"*
   - *"De hele klas doet mee" (groepsdruk)*

3. **Wat zouden de gevolgen van hacken kunnen zijn?**
   - Halt / taakstraf
   - Schadevergoeding betalen
   - Boete! Kan behoorlijk oplopen..
   - Van school gestuurd worden
   - Naar de rechter
   - Aangifte tegen jou bij politie: strafblad

- Geen zakgeld krijgen
- Vrienden kwijtraken
- Huisarrest
- Iemand verdrietig hebben gemaakt
- Een slecht geweten
- Account verbannen op xbox/PS/steam etc.
- Excuus aanbieden aan slachtoffer

Puzzels en energizers

Naast klassenactiviteiten zitten er in iedere klassenquest ook minimaal 1 puzzel en energizer. De puzzel en de oplossing kun je terugvinden in bijlage 1.

De energizer in deze quest is "Ga staan als...". In de quest worden jullie stapje voor stapje meegenomen in de regels van dit spel. Maar je kunt ze hier ook teruglezen:

Ga allemaal zitten en ga staan als: Je vindt dat Sanne de school en haar klas terug mag pakken omdat ze gepest wordt. Bespreek waarom je bent gaan staan of blijven zitten.

Wat valt voor jullie eigenlijk onder online pesten? Ga allemaal weer zitten, en ga staan als: Je wel eens online gepest bent. Bespreek waarom je bent gaan staan of blijven zitten.

Ga daarna weer allemaal zitten, en ga staan als: Jij wel eens iemand online hebt gepest. Dit is echt super belangrijk om met elkaar te bespreken, klas!

Afsluiting - 5 min

Vraag de leerlingen wat ze hebben geleerd. Kunnen ze nu vertellen wat er met Sanne aan de hand was?

Vragen

- **Wat kun je doen om te zorgen dat je niet makkelijk gehackt kunt worden?**
  Antwoord:
  - *Zorgen voor een goed wachtwoord, of beter nog, een wachtZIN!*
  - *Zorgen voor verschillende wachtwoorden bij verschillende accounts*
  - *Zorgen voor tweestapsverificatie*
  - *Je wachtwoord nooit met iemand delen!*
  - *Gebruikmaken van een virusscanner*
  - *Gebruikmaken van een firewall*

- **Wat mag je wel doen als je goed bent in hacken? Wat kun je met die vaardigheden?**
  Antwoord:
  - *Ethisch hacker / White hat hacker worden om ervoor te zorgen dat bedrijven of personen weten waar ze niet goed beschermd zijn en daar iets aan kunnen doen.*
  - *Bij HackShield een account aanmaken.*

Goed om te weten

Een van mijn leerlingen hackt en gaat misschien de grens over, waar kan ik terecht?
Er zijn verschillende initiatieven waar jongeren legaal aan hun digitale vaardigheden kunnen werken. Daar zou je ze naartoe kunnen verwijzen. Laat ze kennismaken en oefenen op bijvoorbeeld deze websites:

- *Gamechangers* https://publicaties.politie.nl/changeyourgame/
- *Crimediggers* https://www.crimediggers.nl
- *Cyber workplace* https://cyberworkplace.tech
- *Hack in the Class* https://hackintheclass.nl
  Bijv: https://lab.hackintheclass.org/

Shield & punten

Wanneer je met de leerlingen de quest uitspeelt, ontvang je aan het einde een code. Wanneer leerlingen op www.hackshieldgame.com een eigen profiel hebben, kunnen zij deze code invullen en een shield en extra punten verdienen.

Schrijf de code op het bord of laat de leerlingen de code zelf opschrijven om mee naar huis te nemen. Zo stimuleer je dat de leerlingen zich thuis ook verder zullen verdiepen in cyberveiligheid. Wat wil je nog meer!?

Wil je de leerlingen helpen deze code in te laten vullen? Volg dan dit stappenplan:

1. Open de game in de HackShield app of via www.hackshieldgame.com
2. Ga naar de instellingen via het tandwieltje linksonder
3. Kies voor "Code invoeren".
4. Vul hier de code in

Account leerlingen aanmaken

Wil je de leerlingen helpen een account aan te maken? Volg dan dit stappenplan met de leerlingen:

1. Ga naar www.hackshieldgame.com of open de game in de HackShield app
2. Kies een regio en spelersnaam (zie screenshot). *Tip: zorg dat dit een andere naam is dan hun eigen voor-/achternaam, dan blijven ze anoniem.*
3. Klik op de knop "Start nieuw avontuur".
4. Klaar! Je kan van start!

Goed om te weten

Bij het maken van een account is het invullen van een e-mailadres niet verplicht. Wil de leerling kans maken op prijzen of uitgenodigd worden voor evenementen? In dat geval is het wel noodzakelijk om een e-mailadres van een ouder / verzorger toe te voegen. Dit kan via het profiel van de leerling door op de spelersnaam te klikken en het e-mailadres in te vullen.

Uitwerking - Cyberpesten

Introductie - 10 min
Vertel de leerlingen dat jullie het gaan hebben over cyberpesten. Hoe verschilt cyberpesten van andere vormen van pesten, welke gevolgen kan het hebben en wat kun je er tegen doen?

Introductievragen

- Hoe verschilt cyberpesten denk je van andere vormen van pesten?
- Op welke soorten sociale media ben je weleens cyberpesten tegengekomen?
- Moet je iets terugdoen als je online gepest wordt?
- Was het vroeger of nu gemakkelijker voor ouders en leerkrachten om te weten wanneer er iemand gepest wordt?
- Wat zou je kunnen doen om cyberpesten te voorkomen?

Optioneel

Laat leerlingen een papier pakken en uitrekenen hoe snel een nare 'meme' over iemand zich kan verspreiden als iedereen in een klas het weer doorstuurt, en die mensen het weer doorsturen, en die mensen het weer doorsturen, etc. Hoe snel gaat dat denk je? Maak het bruggetje naar 'viral' gaan van een bericht, foto of video.

Kern - 30 min
Start de quest op het digibord. Geef aan dat jullie nu gaan starten met de game en bespreek regels die passen bij jouw klas wanneer jullie klassikaal een spel op het digibord spelen.

Hoe maak ik de les interactiever?

- In de quest vertellen Sanne en André van alles over het internet. Dit is in tekst beschreven. Je kunt ervoor kiezen om kinderen de tekst van een specifiek karakter te laten voorlezen (bijvoorbeeld kind x leest de tekst van André en kind y de tekst van Sanne).
- Tijdens de quest zullen er keuzes gemaakt moeten worden. Je kunt ervoor kiezen om een actieve werkvorm daarbij te gebruiken. Bijvoorbeeld: Als je denkt dat we rechts moeten gaan, mag je gaan staan. Als je denkt dat we rechtdoor moeten, dan mag je blijven zitten op je stoel. En als je denkt dat we links moeten, dan mag je op de grond gaan zitten.
- Doe de klassenactiviteiten! (zie de klassenactiviteiten op de volgende pagina)

Tip

Wil je het geluid uit tijdens de quest? Dat kun je doen in het opties menu van de game (zie afbeeldingen hieronder).

Klassenactiviteiten in de quest

Onderstaande vragen worden als klassenactiviteiten aangeboden door Koi (zie afbeelding) in de quest. Je kunt als leerkracht zelf kiezen of je de activiteiten wilt doen (tijdens de quest). Je kunt de vragen natuurlijk ook op een ander moment nog bespreken!

De klassenactiviteiten met de nadruk op **cyberpesten** zijn **oranje**:

1. **Wat zou iemand die cyberpest volgens jou voor redenen kunnen hebben?**
   Suggesties:
   - *Bang om zelf gepest te worden en dus bij het andere 'kamp' aansluiten.*
   - *Boos of verdrietig zijn en zich af willen reageren om beter te voelen.*

2. **Sanne hackt hier omdat ze gepest wordt. Maar wat zouden nog meer redenen kunnen zijn om te gaan hacken?**
   Suggesties:
   - *Om te kijken of een website wel veilig is.*
   - *Om geld te jatten*
   - *Nieuwsgierigheid*
   - *Erkenning of waardering*
   - *Gewoon heel tof*
   - *"Hij heeft vast ook wel eens iemand gehackt"*
   - *"Hij had een slecht wachtwoord"*
   - *"Het is niet onze schuld dat hij zijn computer/account niet beveiligt"*
   - *"Er zijn toch geen slachtoffers"*
   - *"Er is toch geen (financiële) schade"*
   - *"Het is niet alsof we iets kapot maken"*
   - *"Hier leert hij weer van"*
   - *"Het is maar een geintje"*
   - *"Ik kan het"*
   - *"Ik doe niks fout"*
   - *"De hele klas doet mee" (groepsdruk)*

3. **Wat zouden gevolgen zijn van hacken? Wat kan je gebeuren?**
   - Halt / taakstraf
   - Van school gestuurd
   - Geen zakgeld
   - Vrienden kwijtraken
   - Huisarrest
   - Iemand verdrietig hebben gemaakt
   - Een slecht geweten
   - Account banned op xbox/PS/steam etc
   - Schadevergoeding betalen
   - Excuus aanbieden aan slachtoffer

Puzzels en energizers

Naast klassenactiviteiten zitten er in iedere klassenquest ook minimaal 1 puzzel en energizer. De puzzel en de oplossing kun je terugvinden in bijlage 1.

De energizer in deze quest is "Ga staan als...". In de quest worden jullie stapje voor stapje meegenomen in de regels van dit spel. Maar je kunt ze hier ook teruglezen:

Ga allemaal zitten en ga staan als: Je vindt dat Sanne de school en haar klas terug mag pakken omdat ze gepest wordt. Bespreek waarom je bent gaan staan of blijven zitten.

Wat valt voor jullie eigenlijk onder online pesten? Ga allemaal weer zitten, en ga staan als: Je wel eens online gepest bent. Bespreek waarom je bent gaan staan of blijven zitten.

Ga daarna weer allemaal zitten, en ga staan als: Jij wel eens iemand online hebt gepest. Dit is echt super belangrijk om met elkaar te bespreken, klas!

Afsluiting - 5 min

Vraag de leerlingen wat ze hebben geleerd. Kunnen ze vertellen wat er met Sanne aan de hand was?

Vragen

- **Wat kun je doen als je online gepest wordt?**
  Antwoord: hoe graag je het ook wilt, het is niet de beste optie om iemand terug te pakken, uiteindelijk wordt de ruzie zo juist groter en voel je je ook niet beter. Dit zijn dingen die je wel kunt doen:
  - Het vertellen aan je vrienden of/en je ouders; iemand die je vertrouwt. Dan kunnen zij jou steunen en helpen.
  - Het vertellen aan de docent/vertrouwenspersoon op school, die kan je verder helpen.
  - Met iemand praten over hoe je je voelt, dat lucht op.

- **Wat kun je doen als je ziet dat iemand anders online gepest wordt?**
  - Hetzelfde wanneer het bij jou zelf zou gebeuren. Zie de punten hierboven.

Goed om te weten

Waar kun je terecht als je met cyberpesten te maken hebt?

- Iets vervelends (Pesten, seks, oplichting, lastige gevallen) gebeurd op het internet? Meldknop.nl is een initiatief van Veilig internetten en wordt ondersteund door de politie. Let op: het doen van valse aangifte bij de politie is strafbaar.

- Met de Kindertelefoon kun je over alles praten.

- Helpwanted.nl is een website voor kinderen, jongeren en opvoeders die informatie willen of melding willen doen van seksueel misbruik via internet. Helpwanted.nl is een onderdeel van het Expertisebureau Online Kindermisbruik (EOKM). De medewerkers zijn allemaal professionals met kennis over online seksueel misbruik en datgene wat je kunt doen wanneer jij er mee te maken hebt. Natuurlijk behandelen zij alle meldingen vertrouwelijk.

- Pestweb is bedoeld voor iedereen die in Nederland op school zit en op wat voor manier dan ook met pesten te maken heeft. Niet alleen leerlingen die gepest worden, maar ook kinderen en jongeren die iemand kennen die gepest wordt en pesters zelf, zijn welkom bij

Pestweb.

- https://www.vraaghetdepolitie.nl/pesten-en-online
- https://veiliginternetten.nl/veilig-digitaal-opgroeien/#locatie_d
- Op de website van Stop Pesten NU vind je tips over hoe jij kan omgaan met pesten. Of je nu zelf pest of gepest wordt. Ook zijn er veel verhalen van anderen (vaak bekende Nederlanders) die vertellen over gepest worden (of pesten). https://www.stoppestennu.nl/voor-leerlingen

Shield & punten

Wanneer je met de leerlingen de quest uitspeelt, ontvang je aan het einde een code. Wanneer leerlingen op www.hackshieldgame.com een eigen profiel hebben, kunnen zij deze code invullen en een shield en extra punten verdienen.

Schrijf de code op het bord of laat de leerlingen de code zelf opschrijven om mee naar huis te nemen. Zo stimuleer je dat de leerlingen zich thuis ook verder zullen verdiepen in cyberveiligheid. Wat wil je nog meer!?

Wil je de leerlingen helpen deze code in te laten vullen? Volg dan dit stappenplan:

5. Open de game in de HackShield app of via www.hackshieldgame.com
6. Ga naar de instellingen via het tandwieltje linksonder
7. Kies voor "Code invoeren".
8. Vul hier de code in

Account leerlingen aanmaken

Wil je de leerlingen helpen een account aan te maken? Volg dan dit stappenplan met de leerlingen:

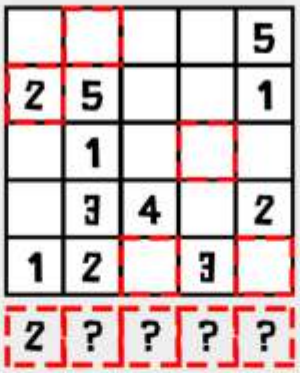
5. Ga naar www.hackshieldgame.com of open de game in de HackShield app
6. Kies een regio en spelersnaam (zie screenshot). *Tip: zorg dat dit een andere naam is dan hun eigen voor-/achternaam, dan blijven ze anoniem.*
7. Klik op de knop "Start nieuw avontuur".
8. Klaar! Je kan van start!

Goed om te weten

Bij het maken van een account is het invullen van een e-mailadres niet verplicht. Wil de leerling kans maken op prijzen of uitgenodigd worden voor evenementen? In dat geval is het wel noodzakelijk om een e-mailadres van een ouder / verzorger toe te voegen. Dit kan via het profiel van de leerling door op de spelersnaam te klikken en het e-mailadres in te vullen.

Bijlage 1

Puzzel



Oplossing

Bijlage 2. Informatiebrief voor ouders

INFORMATIEBRIEF VOOR OUDERS/ VERZORGERS

Beste ouders/verzorgers van leerlingen die binnenkort met de klas een online spel (quest) van HackShield gaan spelen.

HackShield is een online spelomgeving waarin kinderen worden geleerd wat de gevaren zijn in de online wereld en op welke manier ze zich tegen deze gevaren kunnen beschermen. Het doel van de spellen van HackShield is om kinderen weerbaarder te maken tegen mogelijke risico's die zij in hun dagelijks leven online kunnen tegenkomen. Ze leren daarbij hoe hiermee om te gaan door zelf online spellen te spelen en dit in klas met de leerkracht te bespreken.

Hogeschool Saxion doet in opdracht van het CCV (Centrum voor Criminaliteit en Veiligheid) onderzoek naar de effectiviteit van dit online programma. Via deze brief informeren we u over het onderzoek dat gepland is voorafgaand en na het spelen van de online quest van HackShield in de klas. Leest u daarom het onderstaande a.u.b. zorgvuldig door.

Indien u bezwaar heeft tegen deelname van uw kind aan het onderzoek, dan kunt u dat bij de mentor van uw kind aangeven. Uw kind doet dan niet mee.

Doel van het onderzoek

Dit onderzoek heeft tot doel om een wetenschappelijke evaluatie uit te voeren van het online programma van HackShield.

Instructie en procedure

In dit onderzoek wordt er op de volgende manier gegevens verzameld over uw kind:

Ca. een/twee weken voorafgaand aan het spelen van de quest van HackShield in de klas vult uw kind op school een vragenlijst in met vragen over het onderwerp. Deze vragenlijst is anoniem. De ingevulde gegevens kunnen dus niet herleid worden naar uw kind.

De vragen gaan o.a. over kennis van het onderwerp, zelfbeschermend gedrag, ervaringen, en bewustzijn en perceptie van de risico's. Het invullen duurt ca. 15 minuten. Ca. een/twee weken ná het spelen van het spel in de klas vult uw kind de vragenlijst nogmaals in.

Vrijwilligheid

Als uw kind niet wil meedoen aan het onderzoek, of als u daar bezwaar tegen heeft, dan zal uw kind niet meedoen aan het onderzoek. Als uw kind gedurende het onderzoek besluit dat hij/zij wil stoppen, dan kan dat op elk moment, zonder opgaaf van redenen en zonder dat dit op enige wijze gevolgen zal hebben voor u of uw kind.

Ongemak, risico's en verzekering

Voor ieder onderzoek van Hogeschool Saxion geldt een standaard aansprakelijkheidsverzekering.

Privacy is gewaarborgd

De onderzoeksgegevens worden door de onderzoekers nader geanalyseerd. Onderzoeksgegevens die worden gepubliceerd in rapporten en wetenschappelijke tijdschriften zijn anoniem en zijn dus niet tot uw kind te herleiden. Volledig geanonimiseerde onderzoeksgegevens kunnen voor wetenschappelijke doeleinden worden gedeeld met andere onderzoekers. In het onderzoek worden geen persoonsgegevens (over wie uw kind is) vastgelegd.

Nadere inlichtingen

Mocht u vragen hebben over dit onderzoek, vooraf of achteraf, dan kunt u zich wenden tot de verantwoordelijke onderzoeker; dr. Milou Kievik (m.kievik@saxion.nl). Voor formele klachten aangaande het gebruik van persoonsgegevens binnen dit onderzoek kunt u zich wenden tot de Functionaris Gegevensbescherming van Hogeschool Saxion, Monique Witlam (functionarisgegevensbescherming@saxion.nl).

Met vriendelijke groet,

Milou Kievik, senior onderzoeker bij het Lectoraat Online Weerbaarheid

Bijlage 3A. Vragenlijst voormeting

Beste leerling, Binnenkort ga je met je klas "Hackshield in de klas" spelen. Dit spel gaat over dingen die je op het internet mee kunt maken. Wij willen je graag vooraf een aantal vragen stellen. Let op: je kunt geen goede of foute antwoorden geven! Geef het antwoord dat het best past bij wat je vindt of voelt. Je hoeft je naam nergens op te schrijven. Als je je er niet prettig bij voelt om de vragenlijst in te vullen, dan mag je op elk moment stoppen met het invullen van de vragenlijst.

Als je hiermee akkoord gaat, kun je beginnen met het invullen van de vragenlijst.

- ○ Ik ga akkoord
- ○ Ik ga niet akkoord en vul de vragenlijst niet in

Ga naar: Einde enquête Als Als je hiermee akkoord gaat, kun je beginnen met het invullen van de vragenlijst. = Ik ga niet akkoord en vul de vragenlijst niet in

Ben je een jongen of meisje?

- ○ Jongen
- ○ Meisje
- ○ Anders
- ○ Wil ik niet zeggen

Hoe oud ben je? (zelf invullen)

_____

Op welke school zit je? (zelf invullen)

_____

In welke groep zit je? (zelf invullen)

_____

Einde blok: Een paar vragen over jou

Start van blok: Online pesten

De volgende vragen gaan over online pesten (dus pesten via het internet). Bij online pesten worden er nare dingen gezegd over iemand via bijvoorbeeld WhatsApp, Snapchat, Instagram, Youtube of TikTok.

Hieronder wordt een aantal situaties beschreven. Kruis aan of ze volgens jou *waar* of *niet waar* zijn.

	Waar	Niet waar	Weet ik niet
Als je online gepest wordt, dan kun je daar niets tegen doen.	○	○	○
Als iemand online gepest wordt, dan kan dat voor het slachtoffer grote gevolgen hebben.	○	○	○
Online pesten is net zo erg als offline pesten (in de klas of op het schoolplein).	○	○	○
Als je weet dat iemand online wordt gepest, dan moet je het slachtoffer helpen.	○	○	○
Als je weet dat iemand online wordt gepest, dan is het verstandig dit aan een volwassene (bijvoorbeeld de juf of meester of je ouders) te vertellen.	○	○	○

Sam zit in een groepsapp met de hele klas. Er worden *nare dingen* over Sam gezegd in de app en sommige kinderen *lachen* daarom. *[let op: Sam is een verzonnen persoon]*

Als ik Sam zou zijn, dan *voel* ik mij:

- ○ Helemaal niet gespannen
- ○ Niet echt gespannen
- ○ Een beetje gespannen
- ○ Behoorlijk gespannen
- ○ Heel erg gespannen

Als ik Sam zou zijn, dan *voel* ik mij:

- ○ Helemaal niet veilig
- ○ Niet echt veilig
- ○ Een beetje veilig
- ○ Behoorlijk veilig
- ○ Heel erg veilig

Als ik Sam zou zijn, dan *voel* ik mij:

- ○ Helemaal niet bang
- ○ Niet echt bang
- ○ Een beetje bang
- ○ Behoorlijk bang
- ○ Heel erg bang

Als ik Sam zou zijn, dan *voel* ik mij:

- ○ Helemaal niet verdrietig
- ○ Niet echt verdrietig
- ○ Een beetje verdrietig
- ○ Behoorlijk verdrietig
- ○ Heel erg verdrietig

Wat er met Sam gebeurt in dit voorbeeld, zou ook kinderen in mijn klas kunnen overkomen.

- ○ Helemaal mee oneens
- ○ Enigszins mee oneens
- ○ Niet mee eens / niet mee oneens
- ○ Enigszins mee eens
- ○ Helemaal mee eens

Pagina-einde

Stel: jij zit in de groepsapp van de klas van Sam en je ziet dat er nare berichten over Sam worden verstuurd. Geef aan in hoeverre je het eens bent met de volgende stellingen.

	Helemaal niet	Niet echt	Een beetje	Behoorlijk veel	Heel erg veel
Ik heb er vertrouwen in dat ik het mijn juf of meester kan vertellen.	○	○	○	○	○
Ik heb er vertrouwen in dat ik het mijn ouders/verzorgers kan vertellen.	○	○	○	○	○
Ik heb er vertrouwen in dat ik in de groepsapp tegen mijn klasgenoot die de berichten verstuurt kan zeggen dat hij/zij hiermee moet stoppen.	○	○	○	○	○
Ik heb er vertrouwen in dat ik in de groepsapp kan zeggen dat mijn klasgenoot moet stoppen met het versturen van nare berichten over Sam.	○	○	○	○	○

Stel: jij zit in de groepsapp van de klas van Sam en je ziet dat er nare berichten over Sam worden verstuurd.

	Helemaal niet	Niet echt	Een beetje	Behoorlijk veel	Heel erg veel
Denk je dat het helpt om jouw juf of meester te vertellen dat er nare berichten over Sam worden rondgestuurd.	○	○	○	○	○
Denk je dat het helpt om jouw ouders/verzorgers te vertellen dat er nare dingen over Sam worden rondgestuurd.	○	○	○	○	○
Denk je dat het helpt om tegen je klasgenoot die de berichten verstuurt in de groepsapp te zeggen dat hij/zij hiermee moet stoppen.	○	○	○	○	○
Denk je dat het helpt om in de groepsapp te zeggen dat jouw klasgenoot moet stoppen met het versturen van de nare berichten.	○	○	○	○	○
Denk je dat het helpt om de nare berichten over Sam te verwijderen van jouw telefoon.	○	○	○	○	○
Denk je dat het helpt om de groepsapp te verlaten.	○	○	○	○	○

Wat denk je dat jouw beste vrienden zouden doen wanneer zij in een groepsapp zitten waarin nare dingen over Sam worden gedeeld?

	Zeker niet	Waarschijnlijk niet	Soms wel, soms niet	Waarschijnlijk wel	Zeker wel	Dat weet ik niet
Mijn beste vrienden zouden tegen de juf of meester zeggen dat er nare dingen over Sam worden verstuurd in de groepsapp.	○	○	○	○	○	○
Mijn beste vrienden zouden tegen hun ouders/verzorgers zeggen dat er nare dingen over Sam worden verstuurd in de groepsapp.	○	○	○	○	○	○
Mijn beste vrienden zouden zelf ook nare dingen in de groepsapp zetten over Sam.	○	○	○	○	○	○
Mijn beste vrienden zouden in de groepsapp zeggen dat er gestopt moet worden met het versturen van nare berichten over Sam.	○	○	○	○	○	○
Mijn beste vrienden zouden de nare berichten over Sam verwijderen.	○	○	○	○	○	○
Mijn beste vrienden zouden de nare berichten over Sam doorsturen naar anderen.	○	○	○	○	○	○

De volgende keer als er iemand in onze groepsapp nare dingen zegt over iemand anders, dan...

	Zeker niet	Waarschijnlijk niet	Soms wel, soms niet	Waarschijnlijk wel	Zeker wel
...zeg ik tegen mijn ouders/verzorgers dat er nare dingen over een klasgenoot worden verstuurd in de groepsapp.	○	○	○	○	○
...zet ik zelf nare dingen in de groepsapp over deze klasgenoot.	○	○	○	○	○
...zeg ik in de groepsapp dat er gestopt moet worden met het versturen van nare berichten over deze klasgenoot.	○	○	○	○	○
...verwijder ik de nare berichten over deze klasgenoot.	○	○	○	○	○
...stuur ik de nare berichten over deze klasgenoot door naar anderen.	○	○	○	○	○

Einde blok: Online pesten

Start van blok: Hacken

De volgende vragen gaan over het onderwerp 'hacken'. Hacken betekent dat iemand in een computer, telefoon of account (bijv. van Instagram of TikTok) van een ander komt, zodat hij of zij daar gegevens kan weghalen of veranderen.

Hieronder wordt een aantal situaties beschreven. Kruis aan of ze volgens jou waar of niet waar zijn.

	Waar	Niet waar	Weet ik niet
Wanneer je inlogt op het account van iemand anders, dan ben je aan het hacken.	○	○	○
Een goed wachtwoord bestaat uit heel veel verschillende letters, cijfers en tekens.	○	○	○
Een firewall maakt het moeilijker voor een hacker om in jouw computer te komen.	○	○	○
Hackers proberen vaak geld of informatie te stelen door in te breken op apparaten en netwerken van anderen.	○	○	○
Hoe ingewikkelder jouw wachtwoord is, hoe moeilijker het voor een hacker is om het wachtwoord te kraken.	○	○	○
Er zijn ook hackers die hun kennis en talenten gebruiken voor goede dingen.	○	○	○

Pagina-einde

Bo is aan het hacken. Bo gebruikt stiekem het Instagram- en TikTok-account van andere kinderen. Bo plaatst daar zelf berichten (bv. teksten, plaatjes, filmpjes), en verwijdert daar ook berichten. *[Let op: Bo is een verzonnen persoon]*

Als Bo dit op mijn account zou doen, dan *voel* ik mij:

- ○ Helemaal niet gespannen
- ○ Niet echt gespannen
- ○ Een beetje gespannen
- ○ Behoorlijk gespannen
- ○ Heel erg gespannen

Als Bo dit op mijn account zou doen, dan *voel* ik mij:

- ○ Helemaal niet veilig
- ○ Niet echt veilig
- ○ Een beetje veilig
- ○ Behoorlijk veilig
- ○ Heel erg veilig

Als Bo dit op mijn account zou doen, dan *voel* ik mij:

- ○ Helemaal niet boos
- ○ Niet echt boos
- ○ Een beetje boos
- ○ Behoorlijk boos
- ○ Heel erg boos

Als Bo dit op mijn account zou doen, dan *voel* ik mij:

- ○ Helemaal niet verdrietig
- ○ Niet echt verdrietig
- ○ Een beetje verdrietig
- ○ Behoorlijk verdrietig
- ○ Heel erg verdrietig

Het kan ieder kind overkomen dat zijn of haar sociale media gehackt wordt.

- ○ Helemaal mee oneens
- ○ Enigszins mee oneens
- ○ Niet mee eens / niet mee oneens
- ○ Enigszins mee eens
- ○ Helemaal mee eens

Pagina-einde

Geef aan in hoeverre je het eens bent met de volgende stellingen.

	Helemaal niet	Niet echt	Een beetje	Behoorlijk veel	Heel erg veel	Ik weet niet wat dit betekent
Ik heb er vertrouwen in dat ik een goed wachtwoord kan bedenken.	○	○	○	○	○	○
Ik heb er vertrouwen in dat ik voor verschillende accounts verschillende wachtwoorden kan aanmaken.	○	○	○	○	○	○
Ik heb er vertrouwen in dat ik mijn wachtwoorden voor mijzelf kan houden (mijn wachtwoorden dus nooit met iemand anders deel).	○	○	○	○	○	○

Pagina-einde

Stel: jij wilt je goed beschermen tegen hackers. Denk je...

	Helemaal niet	Niet echt	Een beetje	Behoorlijk veel	Heel erg veel	Ik weet niet wat dit betekent
...dat het helpt om gebruik te maken van een goed wachtwoord?	○	○	○	○	○	○
...dat het helpt om meerdere wachtwoorden te bedenken voor verschillende accounts?	○	○	○	○	○	○
...dat het helpt om je wachtwoord nooit met iemand anders te delen?	○	○	○	○	○	○

Pagina-einde

Wat denk je dat jouw beste vrienden zouden doen om zichzelf te beschermen tegen hackers?

	Zeker niet	Waarschijnlijk niet	Soms niet, soms wel	Waarschijnlijk wel	Zeker wel	Dat weet ik niet
Mijn beste vrienden zouden gebruik maken van een goed wachtwoord.	○	○	○	○	○	○
Mijn beste vrienden zouden verschillende wachtwoorden gebruiken voor verschillende accounts.	○	○	○	○	○	○
Mijn beste vrienden zouden hun wachtwoord altijd voor zichzelf houden (en dus nooit delen met een ander).	○	○	○	○	○	○

Pagina-einde

Wat denk je dat jijzelf zou doen om je te beschermen tegen hackers?

	Zeker niet	Waarschijnlijk niet	Soms niet, soms wel	Waarschijnlijk wel	Zeker wel	Dat weet ik niet
Ik zou gebruik maken van een goed wachtwoord.	○	○	○	○	○	○
Ik zou verschillende wachtwoorden gebruiken voor verschillende accounts.	○	○	○	○	○	○
Ik zou mijn wachtwoord altijd voor mijzelf houden (en dus nooit delen met een ander).	○	○	○	○	○	○

Einde blok: Hacken

Start van blok: Overkoepelende vragen

In hoeverre ben je het hier mee eens:

	Helemaal mee oneens	Enigszins mee oneens	Niet mee eens / niet mee oneens	Enigszins mee eens	Helemaal mee eens
Ik vind het internet een onveilige plek.	○	○	○	○	○
Ik weet meer over het internet en de risico's ervan dan mijn ouders/verzorgers.	○	○	○	○	○
Ik kan mijn ouders/verzorgers iets leren over veilig internetten.	○	○	○	○	○
Ik kan een gesprek aangaan met volwassen over veilig internetten.	○	○	○	○	○

Pagina-einde

Hoe vaak praat je met volwassenen in jouw omgeving over veiligheid op het internet?

- ○ Heel weinig
- ○ Weinig
- ○ Niet weinig / niet vaak
- ○ Vaak
- ○ Heel vaak

Pagina-einde

In hoeverre ben je het hier mee eens:

	Helemaal mee oneens	Enigszins mee oneens	Niet mee eens / niet mee oneens	Enigszins mee eens	Helemaal mee eens
Het is mijn eigen verantwoordelijkheid om mijzelf te beschermen tegen gevaren op het internet.	○	○	○	○	○
Mijn ouders/verzorgers zijn ervoor verantwoordelijk om mij te beschermen tegen gevaren op het internet.	○	○	○	○	○
Mijn juf/meester is ervoor verantwoordelijk om mij te beschermen tegen gevaren op het internet.	○	○	○	○	○
De overheid/politie is ervoor verantwoordelijk om mij te beschermen tegen gevaren op het internet.	○	○	○	○	○
Instagram, Tiktok en andere sociale media zijn ervoor verantwoordelijk om mij te beschermen tegen gevaren op het internet.	○	○	○	○	○

Pagina-einde

Als je online bent, moet je vaak keuzes maken, bijvoorbeeld of je wel of niet op een link klikt, of dat je wel of niet ergens op reageert, of dat je wel of niet gegevens over jezelf geeft. In hoeverre ben je het hier mee eens:

	Helemaal mee oneens	Enigszins mee oneens	Niet mee eens / niet mee oneens	Enigszins mee eens	Helemaal mee eens
Als ik online keuzes maak, dan denk ik daar altijd goed over na.	○	○	○	○	○
Als ik online keuzes maak, dan bespreek ik dat eerst met mijn ouders/verzorgers.	○	○	○	○	○
Als ik online keuzes maak, dan doe ik dat snel en zonder na te denken.	○	○	○	○	○
Ik heb wel eens te snel op een link geklikt waardoor ik een probleem kreeg.	○	○	○	○	○
Ik heb wel eens een bericht gestuurd waar ik snel spijt van kreeg.	○	○	○	○	○
Ik heb wel eens persoonlijke gegevens (bijv. foto's, adresgegevens) gestuurd naar iemand die ik helemaal niet (goed) ken.	○	○	○	○	○

Einde blok: Overkoepelende vragen

Start van blok: Blok 4

Dit is het einde van de vragenlijst. Bedankt voor het invullen!

Einde blok: Blok 4

Bijlage 3B. Extra vragen bij de nameting

De vragen bij de nameting waren identiek aan die bij de voormeting. De introductie echter was anders, en er waren een aantal extra vragen aan het begin toegevoegd m.b.t. de evaluatie van de gespeelde game. Er was ook een vraag toegevoegd om te checken of de leerling de game daadwerkelijk had gespeeld.

Start van blok: Een paar vragen over jou

Beste leerling,
Kortgeleden heb je met je klas "Hackshield in de klas" gespeeld. Dit spel gaat over dingen die je op het internet mee kunt maken. Wij willen je hierover graag een aantal vragen stellen.

Als je deze vragen al een keer eerder hebt beantwoord, dan geeft dat niet. Wij willen graag opnieuw jouw reactie weten.

Let op: je kunt geen goede of foute antwoorden geven! Geef het antwoord dat het best past bij wat je vindt of voelt.

Je hoeft je naam nergens op te schrijven.

Als je je er niet prettig bij voelt om de vragenlijst in te vullen, dan mag je op elk moment stoppen met het invullen van de vragenlijst.

Akkoord Als je hiermee akkoord gaat, kun je beginnen met het invullen van de vragenlijst.

- ○ Ik ga akkoord
- ○ Ik ga niet akkoord en vul de vragenlijst niet in

Ga naar: Einde enquête Als Als je hiermee akkoord gaat, kun je beginnen met het invullen van de vragenlijst. = Ik ga niet akkoord en vul de vragenlijst niet in

---

Pagina-einde

Ben je een jongen of meisje?

- ○ Jongen
- ○ Meisje
- ○ Anders
- ○ Wil ik niet zeggen

Hoe oud ben je? (zelf invullen)

_____

Op welke school zit je? (zelf invullen)

_____

In welke groep zit je? (zelf invullen)

_____

Einde blok: Een paar vragen over jou

Start van blok: Evaluatievragen

Het spel "Hackshield in de klas" gaat over dingen die je op het internet mee kunt maken. Het spel dat jullie klas gespeeld heeft ging over pesten op het internet, en over hacken.

Kun je je nog herinneren dat je dit spel in jouw klas gespeeld hebt?

- ○ Ja, heel goed
- ○ Ja, een beetje
- ○ Ja, maar niet zo goed
- ○ Nee, ik was er toen niet bij

Ga naar: Einde enquête Als Kun je je nog herinneren dat je dit spel in jouw klas gespeeld hebt? = Nee, ik was er toen niet bij

Wat vond je van het spel "Hackshield in de klas"?

	Ja	Nee	Weet ik niet
Interessant	○	○	○
Moeilijk	○	○	○
Lang	○	○	○
Leuk	○	○	○
Kinderachtig	○	○	○
Spannend	○	○	○

Vind je een spel zoals "Hackshield in de klas" geschikt om over onderwerpen als pesten en hacken te leren?

- ○ Ja
- ○ Een beetje
- ○ Nee (als je wilt mag je een reden geven) _____

Rapportcijfer Welk rapportcijfer zou je aan dit spel geven?

	0 1 2 3 4 5 6 7 8 9 10
cijfer	

Einde blok: Evaluatievragen

Start van blok: Online pesten

Bijlage 4. Transcript van de klassenquest ‘Online grenzen’.

S: Er is een klasgenoot die echt rot berichten naar me stuurt.

S: Moet je dit zien!

S: Wat moet ik daar nu mee?

Je krijgt 3 opties:

A. Laat het gaan Sanne!

a. S: Jullie hebben gelijk… denk ik.

b. …

c. Nee, nee, NEE! Ik laat niet over me heen lopen, klas.

d. *Vervolg zie beneden*

B. Terugpakken

a. S: Dat dacht ik ook! We zullen hem een lesje leren!

b. *Vervolg zie beneden*

C. Reageren!

a. S: Goed idee! Wat zullen we terugzeggen!

b. *Je krijgt 2 opties:*

c. 1. Je hebt zelf een rotkop!

d. 2. Waarom doe je zo gemeen tegen mij?

e. *Beide geven hetzelfde vervolg*

i. S: Haha dat zal hem leren!

ii. 

iii. S: Wat… Nou… ik… Hoe bedoelt hij… Ik ben helemaal niet…

iv. …

v. Weet je wat? Dan zal ik hem krijgen ook!

Daarna gaan alle opties verder bij

S: En ik weet precies ‘hoe’ we hem gaan terugpakken.

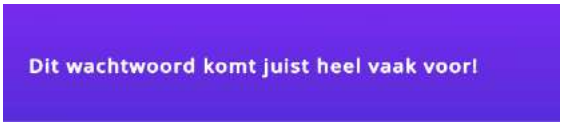
Kom mee! We gaan door de deur, klas.

S: Daarvoor moeten we eerst het wachtwoord van zijn account kraken.

Makkelijk zat! Online staan hele lijsten met de meest gebruikte wachtwoorden.

Wat zouden de meest voorkomende wachtwoorden zijn? Laten we naar de activator gaan!

Slechte antwoorden:



Je moet blijven proberen tot je het goede antwoord kiest.

Goede antwoord links boven:

S: Wow, die zou ik zelfs niet kunnen kraken!

S: Ik heb jullie hulp nodig, klas! Als we deze puzzel oplossen weten we Cummits wachtwoord.

Pak pen en papier en teken de puzzel na. In elke rij en kolom mag maar 1x het cijfer 1 t/m 5 voorkomen.

De cijfers die in de rode vakjes staan zijn Crummit's wachtwoord.

Zijn jullie klaar? Klik dan op volgende.

Wat is het juiste wachtwoord?

Bij het aanklikken van het foute antwoord krijg je:

S: Nee, dat kan niet kloppen! Kijk nog eens goed, klas!

Wat is het juiste wachtwoord?

Bij het aanklikken van het goede antwoord krijg je:

S: Yes, dat is hem! Snel naar zijn profiel.

Koi: Wat zouden redenen kunnen zijn voor iemand om te gaan cyberpesten?

S: Wat dit zwarte scherm is? Ja, het profiel is weg natuurlijk…

Ik breng ons terug naar het startpunt.

S: Dat hebben we echt goed gedaan klas.

Misschien alleen nog even een grappige opmerking in de klassenapp over hem maken.

S: Hèh? Heb ik geen toegang meer tot onze klassenapp?

Maar dat betekent…

Dat ik eruit ben geschopt…

Wat zouden jullie doen als je in deze situatie zou zijn beland?

1. Zeg het tegen de leerkracht!

a. S: Goed idee. Denk ik… Ik zal de leerkracht even appen.

b. 

c. S: Phieww. Ik zit er in weer in.

d. 

e. S: Huh?!

f. Nu ben ik pas echt boos!

2. Hack de groepsapp om jezelf er weer in te laten

a. Nu ben ik pas echt boos!

3. Niks. Lekker laten gaan!

a. S: Goed idee, ik negeer hem gewoon… Of wacht!

Alle drie de opties komen hier weer samen:

S: Ik heb een NOG beter idee!

Door de deur klas!

S: Een firewall is een blokkade die ervoor zorgt dat er geen virussen op een computer binnenkomen.

Gelukkig is de beveiliging van de klassenappserver een stuk slechter.

Koi: Sanne is nu aan het hacken, omdat ze gepest wordt. Wat zouden jullie een goede reden vinden om te gaan hacken?

Optie: Als je de technische afdeling in loopt: (dit zit verder dan de deur die je moet hebben dus het kan goed dat dit wordt overgeslagen)

S: Zo maken ze het ons wel heel makkelijk.

Q: Ik ben heel benieuwd wat jullie daarvan vinden? We spelen “Ga staan als…”. Ga allemaal zitten en ga staan als:

Je vindt dat Sanne de school en haar klas terug mag pakken omdat ze gepest wordt.

Bespreek waarom je bent gaan staan of blijven zitten.

Wat valt voor jullie eigenlijk onder online pesten? Ga allemaal weer zitten, en ga staan als:

Je wel eens online gepest bent.

Bespreek waarom je bent gaan staan of blijven zitten. Ga daarna weer allemaal zitten, en ga staan als:

Jij wel eens iemand online hebt gepest.

Dit is echt super belangrijk om met elkaar te bespreken, klas! Goed gedaan. Laten we snel kijken hoe het met Sanne gaat aflopen.

S: Zo wordt het NOG makkelijker dan ik dacht… hihihihi.

Beide opties geven hetzelfde resultaat.

S: We gaan malware op de server installeren.

Geen firewall en geen virusscanner? Ze vragen er praktisch om!

1. Praat Sanne om

a. S: School doet toch ook niks tegen die pesters!

b. Wat nou? Als ik het niet zelf regel, dan gebeurt er NIETS!

c. …

2. Moedig Sanne aan

a. S: Precies, school doet ook niets tegen die pesters!

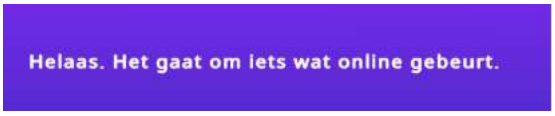
b. We moeten het zelf doen!

Vervolg beide paden

S: Jullie vinden dit toch ook een onschuldig grapje? We lossen samen de puzzel op en dan installeer ik de malware.

Antwoord optie 1:

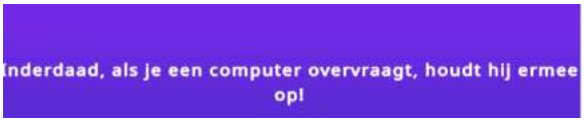
Antwoord optie 2:



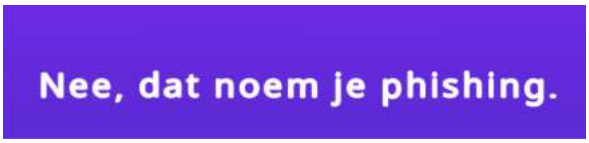
Antwoord optie 1:

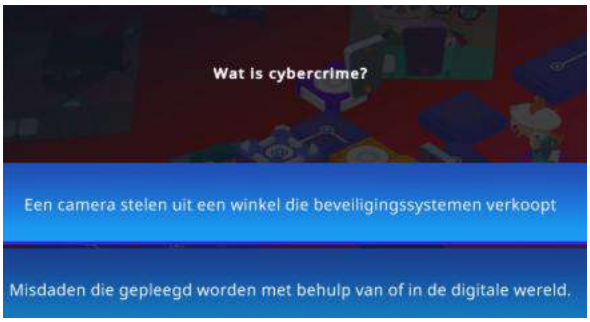
Antwoord optie 2:

Antwoord optie 1:



Antwoord optie 2:





Antwoord optie 1: Nee, dat noem je gewoon stelen. Ook dat is criminaliteit, maar niet online.

Antwoord optie 2: Inderdaad. Online criminaliteit.

Antwoord optie 1: Aii… dat is dan een duur geintje. Een DDoS kan veel (financiële) schade aanbrengen, bij scholen of bedrijven bijvoorbeeld.

Antwoord optie 2: Inderdaad. Je krijgt een boete, taakstraf of zelfs een gevangenisstraf.

Antwoord optie 1: Nee, helaas. Het zou wel makkelijk zijn als je gewoon met een scannertje kan zeggen of je koorts hebt, in plaats van met een thermometer.

Antwoord optie 2: Lekker bezig! Heb jij al een virusscanner op jouw computer?

Koi: Wat zouden de gevolgen van hacken kunnen zijn?

S: De volgende die een berichtje opent in de app, installeert automatisch het virus.

En dan ligt in een keer de hele server plat. HAHAHA!

S: Ja. Als een server 'platligt' kan niemand ermee verbinden. Apps, websites, de hele bende werkt niet meer.

Twee opties

1. Dat zal ze leren!

a. S: Juist! Verdiende loon!

2. Dat klinkt niet als een 'onschuldig' grapje Sanne…

a. S: Nou ik vind dat ze het verdienen!

Laten we teruggaan naar het startpunt.

Pas op wat je doet Sanne. We houden je in de gaten. Groet, P.

S: Wat is dat nu weer!? Ze weten ook niet van ophouden die pestkoppen. DELETE!!

Kom klas, terug naar het startpunt.

1. Heb je die klassenapp niet ‘platgelegd’?
2. Maar Crummit zit toch zelf ook in die klassenapp?

S:Uhh.. ja.. nou.. Dan doe ik het toch lekker zelf!

1. Probeer Sanne te kalmeren
2. Spreek Sanne aan op haar gedrag

S: Gaan jullie nu ook al beginnen!? Zoekt het uit!

Peter: Ach, ik heb zo mijn methodes Sanne. Net als jij, toch?

Ik ben Peter. Ik had je al een bericht gestuurd. Ik werk voor de COPS.

Het COPS-team laat mogelijke daders van cybercrime de gevolgen ervan zien. Maar we kijken ook naar de toffe dingen die ze zouden kunnen doen met hun digitale skills!

Waar kan ik jullie mee helpen?

1. Hulp bij pesten

a. P: Je moet beter zijn dan de pesters, Sanne. Het voelt niet eerlijk en is ontzettend moeilijk.

b. S: Maar ik was gewoon zo boos. Ik kon niets anders.

i. 1. Neem het op voor Sanne

1. P: Wacht even klas, het is niet goed om te pesten. Als je weet of ziet dat iemand dit doet, moet je in actie komen!

ii. 2. Spreek Sanne toe

1. Peter: Inderdaad klas, het is niet goed om te pesten. Als je weet dat iemand dit doet, moet je in actie komen!

c. Peter: Maar geloof me, er zijn altijd mensen die je KUNNEN en WILLEN helpen. Bijvoorbeeld je ouders of volwassenen op school.

d. Ze zullen het pesten misschien niet kunnen voorkomen. Maar ze kunnen je helpen en staan aan JOUW kant.

2. Hulp bij hacken

a. Peter: Als hacker kun je jouw krachten voor goed of kwaad gebruiken… Hoe heb JIJ ze gebruikt, Sanne?

b. Sanne: Ik kon toch niet anders, wat had ik moeten doen dan? Die pestkop houdt niet op!

i. Neem het op voor Sanne

1. Peter: Wacht even klas, het is niet goed om te hacken met slechte bedoelingen. Als je weet of ziet dat iemand dit doet, moet je in actie komen!

ii. Spreek Sanne toe

1. Peter: Inderdaad klas, het is niet goed om te hacken met slechte bedoelingen. Als je weet of ziet dat iemand dit doet, moet je in actie komen!

c. Peter: Bij COPS zeggen we altijd; “If You don’t own it, you won’t pwnt it!”

d. S: Wat betekent dat nu weer?

e. Peter: Als het niet jouw server of computer is blijf je er vanaf!

f. Hacken is cool, maar je kunt niet zo maar anderen aanvallen! Dat is een misdaad en daar kun je voor naar de gevangenis gaan!

Peter: Door ‘terug’ te hacken, ben je zelf niet beter dan de pesters.

S: En nu? Zit ik in de problemen?

P: Nog niet… wees blij dat ik er ben en en dat je nog niet gearresteerd bent. Wij gaan eerst praten.

En klas, jullie hebben vast ook nog een hoop te bespreken met elkaar.

Antwoord Oneens: Inderdaad! Voor de pester voelt het vaak minder erg omdat hij/zij de reactie van het slachtoffer niet kan zien. Voor degene die gepest wordt is het echter net zo erg.

Antwoord Eens: Helaas… Voor de pester voelt het vaak minder erg omdat hij/zij de reactie van het slachtoffer niet kan zien. Voor degene die gepest wordt is het echter net zo erg.

Vraag 2: Terugpesten helpt om minder gepest te worden.

Antwoord Oneens: Inderdaad! De pester vind het vaak alleen maar leuk als je terugpest, omdat de pester je daar dan belachelijk mee kan maken.

Antwoord Eens: Helaas… Als je terugpest ben je niet beter dan de pester. En vaak wordt het pesten hierdoor zelfs erger.

Vraag 3: Als je online gepest wordt is het slim om de leerkracht of je ouders om hulp te vragen.

Antwoord oneens: Helaas… Voor leerkrachten en voor ouders is het moeilijk om te weten als je online gepest wordt. Daarom is het belangrijk om ze op de hoogte te brengen, zodat ze je kunnen helpen.

Antwoord eens: Inderdaad! Voor leerkrachten en voor ouders is het moeilijk om te weten als je online gepest wordt. Daarom is het belangrijk om ze op de hoogte te brengen, zodat ze je kunnen helpen.

Vraag 4: Een firewall zorgt ervoor dat virussen op je computer gevonden en verwijderd worden.

Antwoord oneens: Inderdaad! Een firewall zorgt ervoor dat virussen niet zomaar op de computer kunnen komen.

Antwoord eens: Helaas… Een firewall zorgt ervoor dat virussen niet zomaar op je computer kunnen komen.

Vraag 5: Met een virusscanner kun je een computer beveiligen.

Antwoord oneens: Inderdaad! Een virusscanner zorgt ervoor dat gevaarlijke bestanden op je computer gevonden en verwijderd worden.

Antwoord eens: Helaas… Een virusscanner zorgt ervoor dat gevaarlijke bestanden op je computer gevonden en verwijderd worden.