

POSITION PAPER HACKSHIELD

Online kinderrechten en digitale veiligheid

Inleiding: Kinderrechten en digitalisering

De digitale wereld biedt kansen en risico's voor kinderen. Het beschermen van hun rechten vereist een balans tussen vrijheid en veiligheid. HackShield streeft naar een toekomst waarin kinderen beter beschermd zijn en intrinsiek gemotiveerd worden om nu en in de toekomst bij te dragen aan een veilige digitale samenleving. Via onze game leiden we kinderen op tot Junior Cyber Agents die digitale rechten leren kennen en opkomen voor de rechten van zichzelf en anderen.¹ In plaats van kinderen te beperken door angst voor het onbekende, moedigen we hen aan nieuwsgierig en gezond alert te zijn zodat ze zich positief en zelfbewust ontwikkelen in een steeds digitalere wereld.

1. Vergroten van de online veiligheid van kinderen

De snelle technologische vooruitgang creëert maatschappelijke uitdagingen. Internetcriminelen en bedrijven benutten nieuwe technologieën en spelen in op kwetsbaarheden van onwetende gebruikers. Door het gebrek aan adequate educatie groeit de digitale kenniskloof, wat kinderen blootstelt aan risico's zoals cyberpesten, datadiefstal en schadelijke content. Klassen met grotendeels achterstandsl leerlingen lopen nog meer risico: zij scoren gemiddeld lager op digitale geletterdheid.² Hoewel digitale geletterdheid belangrijker wordt, ontbreekt digitale weerbaarheid in het curriculum. Wij vragen ons af of het huidige onderwijsstelsel snel genoeg kan inspelen op de kansen en gevaren van technologische innovaties, om te voorkomen dat de bescherming van kinderen achterblijft bij de digitale ontwikkelingen.

Kinderen experimenteren thuis en op school onvoldoende onder begeleiding van ouders en leerkrachten in de digitale wereld en krijgen zonder voldoende voorbereiding of begeleiding een smartphone. Uit een onderzoek van onderzoeksinstituut Motivaction blijkt dat bijna de helft van de ondervraagde ouders en kinderen niet weet of zij cybercriminaliteit zouden herkennen, er beschermd tegen zijn, en weten wat ze moeten doen.³ We sturen kinderen geblinddoekt de digitale snelweg op; ze krijgen toegang tot het internet zonder de benodigde vaardigheden om daar veilig te navigeren.

Een ander zorgelijk aandachtspunt is te vinden in het gevoel dat kinderen wordt gegeven wanneer het gaat over cyberveiligheid. Oudere generaties kunnen de digitalisering niet goed volgen, wat kan leiden tot angst voor het onbekende. Er zijn natuurlijk ook dreigingen, zo leert het dagelijkse nieuws ons. Maar krijgen kinderen geen disproportioneel negatief beeld van de werkelijkheid? Dit draagt niet bij aan de nieuwsgierige, gezond alerte en verantwoordelijke houding die we kinderen willen meegeven in hun groei naar volwassenheid. Als we kinderen vragen naar hun visie op technologie, horen we de angstbeelden terug waarmee ze dagelijks geconfronteerd worden. Met HackShield willen we kinderen een reëel beeld schetsen van de online risico's, maar ze ook meenemen in de kansen die de digitale wereld hen biedt en welke positieve rol ze hierin kunnen vervullen.



Een positief voorbeeld van HackShield is Malaika Mughal Uribe (11), die via de game HackShield haar interesse voor ethisch hacken ontwikkelde en nu met trots kinderburgemeester van Alkmaar is. Ze zei: "HackShield veranderde mijn leven, ik weet nu bijna alles over hacken" (De Volkskrant, 29 maart 2024).

Het is belangrijk jong talent te vinden, te enthousiasmeren en op een positieve manier te betrekken bij de digitale toekomst. HackShield leert talent wat wel en niet mag in de digitale wereld om daderschap te voorkomen.⁴ Daarnaast is een essentieel aspect van online veiligheid het ontwikkelen van voldoende IT- en cybersecuritytalent. De tekorten op de cybersecurityarbeidsmarkt vormen een risico voor de digitale weerbaarheid van Nederland en Europa. Recente EU-brede onderzoeken geven aan dat, tenzij jongeren vanaf jonge leeftijd actief betrokken worden bij cybersecurity, het tekort aan gekwalificeerde professionals zal blijven groeien, wat onze digitale weerbaarheid zal beïnvloeden.⁵

Aanbevelingen:

- In plaats van kinderen uit de digitale wereld te weren, moeten we hen voorbereiden met digitale geletterdheid en digitaal burgerschap bijbrengen. Dit betekent praktische educatie, ondersteund door scholen en ouders, waarbij kinderen leren omgaan met de risico's van sociale media en digitale platforms en binnen een veilige omgeving onder begeleiding kunnen experimenteren.
- HackShield zet zich in om een positief verhaal tegenover het angstbeeld te zetten dat overheerst. Door de kansen en mogelijkheden van digitalisering te benadrukken, dragen we bij aan een gevoel van veiligheid, zonder kinderen in onwetendheid te laten. Dit wekt nieuwsgierigheid en een gezond alerte houding op en stimuleert verantwoordelijkheid.
- Technologie biedt kansen voor het ontzorgen van leerkrachten en kan bijdragen aan het oplossen van het lerarentekort.⁶ De onderwijsmaterialen van HackShield kunnen zonder veel kennis en voorbereiding gegeven worden en sluiten aan op de SLO concept kerndoelen.



2. De rol van sociale media in online veiligheid

Online platforms spelen een cruciale, vaak negatieve, rol in het waarborgen van de online veiligheid van kinderen. De huidige pogingen om leeftijdsverificatie in te voeren of schadelijke content te filteren zijn onvoldoende. Dit laat kinderen kwetsbaar achter voor misbruik, terwijl platforms profiteren van hun gegevens en online activiteit.

Aanbevelingen:

- Net zoals in de fysieke wereld, waar identificatieplicht geldt vanaf 14 jaar, moet ook in de digitale wereld de identiteit van gebruikers worden geverifieerd. Voor kinderen onder de 14 moet ouderlijk toezicht en goedkeuring vereist zijn bij het aanmaken van een account. We moeten stoppen met de online- en offlinewereld

als gescheiden te beschouwen.

- Sociale media platforms moeten verantwoordelijker omgaan met de gegevens van kinderen. Er zijn strengere regels nodig om te voorkomen dat kinderen worden geprofileerd of commercieel geëxploiteerd. Dat kinderen vaak niet eens op deze platform mogen is wettelijk (in de AVG) vastgelegd, maar dat betekent in de realiteit weinig.
- Sextortion (versterkt door AI) is een snelgroeiend en veelbeschreven probleem.⁷
- “Stukje Van Mij” van KPN is een sterke campagne, maar we moeten sneller handelen als het aankomt op deze criminele vorm.

3. Flexibiliteit en innovatie in het onderwijs

Het huidige onderwijssysteem is traag in het inspelen op technologische veranderingen, wat resulteert in een groeiende digitale kenniskloof. De innovatiekracht van het onderwijs ligt grotendeels bij uitgeverijen, die achterlopen op inhoud (actualiteit thema's) en op vorm. Meer immersieve lesmethoden, zoals gamification, dragen bij aan een beter leereffect.⁸ Gamification gaat verder dan het leuk maken van lesmateriaal; het creëert een veilige en uitdagende online omgeving waarin leerlingen keuzes kunnen maken, fouten mogen maken, en van de gevolgen leren. Dit stimuleert diepgaander leren en het ontwikkelen van probleemoplossende vaardigheden. HackShield werkt nauw samen met de private sector om nieuwe onderwijsmaterialen te ontwikkelen en te verspreiden. De private sector levert niet alleen expertise, maar ook vrijwilligers die gastlessen verzorgen in het onderwijs. Deze aanpak stelt HackShield in staat om binnen 4 tot maximaal 12 weken een nieuw, actueel thema te vertalen naar kant-en-klaar educatief materiaal.

HackShield is een missiegedreven voorbeeld van een publiek-private samenwerking die succesvol educatieve materialen ontwikkelt, zonder uitgever van onderwijsmaterialen te zijn, zonder geld te vragen van het onderwijs of van kinderen, en zonder kindermarketing toe te passen. HackShield werkt samen met 190 Nederlandse gemeenten, de Nederlandse politie, het ministerie van Justitie en Veiligheid, en bedrijven uit de IT- en securitysector, banken en verzekeraars. Het is essentieel dat de overheid dergelijke private samenwerkingen en maatschappelijk ondernemerschap stimuleert, zodat succesvolle initiatieven kunnen worden opgeschaald in plaats van te verzanden in een eindeloze stroom van pilots.

Het is ook van cruciaal belang om extra aandacht te besteden aan scholen in kwetsbare wijken. Deze scholen lopen vaak achter bij de adoptie van nieuwe lesmaterialen, wat de digitale kenniskloof kan vergroten en daarmee de ongelijkheid in de samenleving verder kan versterken.

HackShield ontwikkelt kant-en-klare lessen die klassikaal op het digibord gespeeld worden en een individueel speelbare game die door kinderen op bijna alle apparaten kunnen spelen. De docent of gastdocent faciliteert, maar de fictieve karakters geven de gastles. Dit zorgt voor een interactieve en aantrekkelijke leerervaring die zowel voor kinderen als leerkrachten van toegevoegde waarde is. Er liggen enorme kansen voor het onderwijs om met digitalisering het lesaanbod te verbeteren voor zowel de leerling als de leerkracht. Hiervoor is echter meer R&D nodig, evenals ruimte in het curriculum, wat gestimuleerd kan worden door bijvoorbeeld OCW.

Aanbevelingen:

- Het onderwijssysteem moet flexibeler worden, zodat scholen sneller kunnen inspelen op technologische ontwikkelingen. Dit kan door een deel van het curriculum open te stellen voor experimentele onderwijsvormen die nog niet volledig door instanties zijn goedgekeurd.
- Er moet meer ruimte komen voor digitale oplossingen die kinderen op een veilige en leuke manier leren omgaan met technologie. Gamification en digitalisering kan het onderwijs interactiever, efficiënter en toegankelijker maken.
- Al vanaf de PABO moeten digitale thema's onderdeel zijn van de opleiding en moet er enthousiasme worden gecreëerd voor nieuwe onderwijsvormen die de mogelijkheden van digitalisering optimaal benutten.

Conclusie: Missiegedreven innovatie voor een veilige digitale toekomst

De toekomstige veiligheid van onze samenleving wordt gecreëerd door voldoende IT- en securitytalent. Om deze talenten te enthousiasmeren, moeten we kinderen en jongeren vanaf jonge leeftijd positief en met nieuwsgierigheid benaderen in plaats van hen bang te maken.

Missiegedreven publiek-private samenwerking is essentieel om de snelheid van digitalisering bij te houden en de kenniskloof te dichten. HackShield is hier een succesvol voorbeeld van. Het huidige systeem moet ruimte creëren voor dergelijke initiatieven en de overheid moet actief stimuleren dat ze worden opgeschaald, om te voorkomen dat ze blijven steken in een eindeloze stroom aan pilots. Alleen zo kunnen we kinderen voorbereiden op een digitale toekomst zonder hen af te sluiten van de technologieën die hun leven onvermijdelijk zullen beïnvloeden.

Wij zullen ons onvermoeid blijven inzetten voor een veilige digitale toekomst met gelijke kansen voor iedereen!

190 Nederlandse gemeenten werken samen met HackShield om cyberveiligheid op lokaal niveau te promoten.



190 Nederlandse gemeenten werken samen met HackShield om cyberveiligheid op lokaal niveau te promoten.



In 2023 won HackShield de **Best Applied Game Award Nederland**, en in 2024 de **IPON Onderwijsinnovatieprijs**.



HackShield werd in 2019 opgericht en heeft meer dan **200.000 kinderen bereikt** in Nederland, waarvan velen actief als **Junior Cyber Agents**.



Voetnoten

1. HackShield Future Cyber Heroes. <https://nl.joinhackshield.com/nl/indeklaas>
 2. DUO Onderwijsonderzoek & Advies. Monitor Digitale Geletterdheid in het PO.
 3. Paloma Bunc en Jorn Lingsma. Onderzoeksrapportage HackShield: Kinderen en cybersecurity. <https://nl.joinhackshield.com/documents/onderzoek.pdf>
 4. <https://nscr.nl/negatief-en-positief-cybergedrag-aagt-vaak-samen-bijjongeren-die-ict-onderwijs-volgen/>
https://nscr.nl/app/uploads/2022/01/NL-Samenvatting_Understandingcybercriminal-behaviour-among-young-people_NSCR-VU_2022-1.pdf
 5. <https://www.rijksoverheid.nl/documenten/kamerstukken/2024/05/15/kamerbrief-human-capital-cybersecurity>
<https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states>
 6. <https://www.rijksoverheid.nl/documenten/rapporten/2023/12/15/biilage-5-factsheet-lerarentekort>
 7. <https://www.rtl.nl/nieuws/artikel/5469589/sextoortion-seksueel-afpersing-nigeriaanse-broers-michigan-vs>
- BBC: 'Tips en handleidingen voor sextortion verkocht op sociale media' | Het Parool
- Federal Bureau of Investigation. Sextortion: A Growing Threat Targeting Minors – FBI. <https://www.fbi.gov/contact-us/field-offices/memphis/news/sextoortion-a-growing-threat-targeting-minors>
8. Gabriela Kiryakova, Nadezhda Angelova & Lina Yordanova. Gamification in Education.

Overige bronnen

[A Systematic Literature Review on Cyber Security Education for Children.](#) - Sağlam, Rahime Belen, Miller, Vincent and Franqueira, Virginia N. L.

[Cybersecurity awareness for children: A systematic literature review](#) - Farzana Quayyum, Daniela S. Cruzes, Letizia Jaccheri