



KENNIS PROJECT SCHOLEN

Digitale veiligheid is niet vanzelfsprekend!



Ontwikkeld door:
Jeremy Loman

Contact gegevens

www.Cyberburger.nl
Info@CyberBurger.nl
0316-798 000
(nummer van Didev)

INHOUDSOPGAVE

Waarom digitale veiligheid essentieel is voor scholen 02

Over CyberBurger 03

Het CyberScholen project 04

Kennis 09

Implementatie voor scholen 13

Investering 14



WAAROM DIGITALE VEILIGHEID ESSENTIEEL IS VOOR SCHOLEN

De digitale wereld stopt niet bij de schoolpoort. Jouw leerlingen brengen meer dan 6 uur per dag door op school – een substantieel deel van hun leven waarin ze in aanraking komen met digitale risico's. Uit ons onderzoek onder 159 ouders en professionals bleken slechts 4 personen voldoende kennis te hebben van de digitale gevaren die kinderen bedreigen.

Wat veel onderwijsprofessionals nog niet weten:

- **Verborgen inhoud in populaire games:** In spellen als Roblox zijn er componenten met seksuele handelingen en geluiden die niet effectief te blokkeren zijn.
- **Online grooming op school:** Volwassenen benaderen kinderen via schoolnetwerken, via games en social media om hun vertrouwen te winnen.
- **AI-deepfake naaktbeelden:** Leerlingen maken met behulp van AI naaktbeelden van klasgenoten, wat tot ernstige pesterijen en trauma's leidt.
- **Toegang tot drugs en medicijnen:** Kinderen kunnen via digitale kanalen eenvoudig toegang krijgen tot drugs, medicijnen zoals Ritalin, of designer drugs.
- **Zelfexploitatie:** Leerlingen, voornamelijk meisjes vanaf 12 jaar, verkopen zelf intieme foto's online.
- **Sextortion:** Kinderen worden gechanteerd met intieme beelden en zien vaak geen uitweg – soms leidt dit tot zelfdoding.
- **Criminele rekrutering:** Criminele netwerken rekruteren online leerlingen, bijvoorbeeld beginnend met het verkopen van vapes, waarna ze onder druk worden gezet voor zwaardere criminaliteit.

De impact op jouw school is enorm. Zonder adequate kennis en begeleiding kunnen leerlingen in situaties terechtkomen die hun veiligheid, welzijn en schoolprestaties ernstig in gevaar brengen. Als onderwijsprofessional sta je op de voorste linie – jij ziet als eerste wanneer een leerling verandert door online ervaringen.

OVER CYBERBURGER



CyberBurger is een initiatief van Didev, opgezet zonder winstoogmerk. Onze missie is het zo breed mogelijk delen van kennis over digitale veiligheid tegen zo laag mogelijke kosten, zodat deze kennis toegankelijk is voor iedereen. Wij beschikken over diepgaande kennis van de digitale wereld en online veiligheid en weten precies wat er speelt. We hebben veel gezien, herkennen de risico's én weten wat we als maatschappij moeten doen om onszelf te beschermen.

Onze aanpak:

- **Kennisdeling:** We maken complexe digitale veiligheidskennis toegankelijk voor onderwijsprofessionals.
- **Netwerkontwikkeling:** We bouwen netwerken van getrainde professionals die elkaar ondersteunen.
- **Praktische tools:** We bieden concrete stappenplannen, handreikingen en interventiestrategieën.
- **Actuele informatie:** We houden onze kennis up-to-date met de nieuwste digitale ontwikkelingen en risico's.



HET CYBERSCHOLEN PROJECT

CyberScholen zorgt ervoor dat onderwijsprofessionals goed geïnformeerd zijn over de digitale leefwereld van hun leerlingen. Het programma biedt scholen de kennis en tools om digitale veiligheid structureel in te bedden in hun onderwijs en zorgstructuur.

Van leraren en onderwijsondersteunend personeel tot schooldirecteuren – iedereen krijgt inzicht in de digitale leefwereld van hun leerlingen. Het doel is om een veilige digitale leeromgeving te creëren waarin problemen vroegtijdig worden gesignaleerd en aangepakt.

**EEN COMPLEET PROGRAMMA VOOR
DIGITALE VEILIGHEID IN HET
ONDERWIJS**

WAAROM ZIJN CYBERSCHOLEN NODIG?

Kinderen en jongeren brengen een groot deel van hun dag door op school, en de invloed van de digitale wereld stopt niet bij de schoolpoort. Veel onderwijsprofessionals geven aan dat ze:

- Worstelen met het herkennen van signalen van online problematiek
- Onvoldoende kennis hebben van actuele digitale trends en risico's
- Handelingsverlegen zijn bij digitale incidenten zoals sexting of cyberpesten
- Behoeftte hebben aan praktische tools om leerlingen digitaal weerbaar te maken
- Een veilige digitale schoolomgeving willen creëren, maar niet weten hoe

CyberScholen helpt onderwijsinstellingen om deze uitdagingen structureel aan te pakken.



HOE WERKT HET CYBERSCHOLEN-PROJECT?

- 1. Benadering:** Scholen kunnen direct deelnemen of worden aangemoedigd door hun gemeente of schoolbestuur.
- 2. Implementatie:** Scholen krijgen toegang tot het e-learning platform en kunnen bepalen welke personeelsleden welke modules volgen.
- 3. Training:** Maandelijks online trainingen bieden persoonlijke begeleiding en ruimte voor schoolspecifieke vragen.
- 4. Integratie:** De school wordt ondersteund bij het integreren van digitale veiligheid in bestaande protocollen en zorgstructuur.
- 5. Oudervoorlichting:** Deelnemende scholen ontvangen materialen om ouders te informeren en te betrekken bij digitale veiligheid.
- 6. Doorlopende ondersteuning:** Scholen krijgen ondersteuning bij complexe digitale incidenten en blijven op de hoogte van nieuwe ontwikkelingen.

Wat levert het op?

- **Voor de school:** Een coherente aanpak van digitale veiligheid, minder incidenten en betere ondersteuning bij problematiek.
- **Voor onderwijsprofessionals:** Meer vertrouwen in het omgaan met de digitale aspecten van hun werk en concrete handvatten bij incidenten.
- **Voor leerlingen:** Een veiligere digitale schoolomgeving waar problemen vroegtijdig worden gesignaleerd en aangepakt.
- **Voor ouders:** De zekerheid dat de school digitale veiligheid serieus neemt en adequaat kan handelen bij problemen.

INHOUD VAN DE TRAINING

CyberScholen-deelnemers worden getraind in:

De digitale wereld begrijpen

- Werking van games, apps en social media
- Psychologische mechanismen achter online platforms
- Digitale detox en mediabalans
- Privacy en gegevensbescherming

Gevaren en risico's herkennen

- Uitgebreide kennis over 20+ digitale risico's (zie kennisgebieden)
- Signaalherkenning bij leerlingen die in de problemen komen
- Up-to-date blijven met nieuwe trends en risico's

Praktisch handelen

- Stappenplannen voor verschillende incidenten
- Effectieve communicatie met leerlingen en ouders
- Integratie van digitale veiligheid in schoolprotocollen
- Cybersecurity basics voor de school

Wat staat er in het projectplan?

Het CyberScholen-projectplan bevat alles wat jouw school nodig heeft om direct te starten:

- Implementatiehandleiding voor scholen
- Communicatiesjablonen voor ouders en leerlingen
- Lesmateriaal voor in de klas
- Stappenplan voor schoolbrede implementatie
- Evaluatie-instrumenten om impact te meten



DIFFERENTATIE NAAR ONDERWIJSTYPEN

Het CyberScholen-programma is aangepast aan verschillende onderwijsniveaus en -typen:

Basisonderwijs: Focus op vroege bewustwording, veilig internetgebruik en mediawijsheid

Voortgezet onderwijs: Nadruk op sociale media, sexting, cyberpesten en digitale identiteit

Speciaal onderwijs: Toegespitst op specifieke kwetsbaarheden en aangepaste begeleiding

Het programma omvat:

Basiskennis digitale wereld

- Relevante platformen, games en apps voor verschillende leeftijdsgroepen
- Psychologische mechanismen achter online gedrag
- Privacy en gegevensbescherming in onderwijscontext

Herkennen en signaleren

- Signalen van digitale problemen in de klas
- Vroegtijdig herkennen van online pesten, grooming of verslaving
- Signalering van radicalisering of criminele recruitment

Schoolbrede aanpak

- Integratie van digitale veiligheid in schoolbeleid
- Opstellen van protocollen voor digitale incidenten
- Samenwerking met ouders, zorgteam en externe instanties

Materialen voor in de klas

- Lessen over digitale veiligheid voor verschillende leeftijdsgroepen
- Gesprekskaarten en werkvormen voor mentoruren
- Activiteiten voor projectweken rond digitale bewustwording

DE DIGITALE WERELD BEGRIJPEN

Hoe werken games, apps en social media?

Inzicht in de basisprincipes achter populaire digitale platforms, hun verdienmodellen en hoe algoritmes bepalen wat gebruikers te zien krijgen.

Waarom zijn digitale platforms zo verslavend?

Uitleg over de psychologische mechanismen (dopamine, beloningssystemen, sociale validatie) die platforms gebruiken om gebruikers aan zich te binden.

Digitale detox en mediabalans

Strategieën voor het creëren van een gezonde balans tussen online en offline activiteiten, inclusief praktische tips voor schermtijdbeperking.

Privacy en gegevensbescherming

Bewustwording van welke persoonlijke gegevens worden verzameld, hoe deze worden gebruikt en hoe je privacy beter kunt beschermen.

GEVAREN EN RISICO'S

Cyberpesten en online negativiteit

Herkennen van digitaal pestgedrag, de impact ervan en effectieve interventies om dit tegen te gaan.

Social media risico's

Overzicht van de specifieke risico's verbonden aan verschillende social media platforms en hoe deze te beperken.

Foto's/video's plaatsen op social media

Bewustwording van de langetermijengevolgen van gedeelde beelden en hoe veilig te delen zonder privacyrisico's.

Online uitdagingen en challenges

Inzicht in virale challenges, hoe ze zich verspreiden en hoe potentieel gevaarlijke trends te herkennen.

Parasociale relaties met influencers

Begrip van eenzijdige emotionele banden die jongeren ontwikkelen met online persoonlijkheden en de invloed hiervan.

Online gaming

De positieve en negatieve aspecten van gaming, inclusief verslavingsrisico's, in-game aankopen en online interacties.

Sexting, sextortion en online intimiteit

Uitleg over de risico's van het delen van intieme beelden, afpersing hiermee en hoe hierover te communiceren met jongeren.

Online grooming

Herkennen hoe online predatoren vertrouwen winnen van jongeren, waarschuwingssignalen en preventieve maatregelen.

'Hulpverleners' en autoriteitsoplichting

Inzicht in hoe oplichters zich voordoen als hulpverleners of autoriteiten om vertrouwen te winnen en misbruik te maken.

Deepfakeporno en AI-misbruik

Bewustwording van technologieën die gezichten kunnen manipuleren in video's en foto's en de impact hiervan op jongeren.

Moderne oplichting & financiële fraude

Overzicht van hedendaagse oplichtingsmethoden gericht op jongeren, zoals nepaccounts, phishing en betaalfraude.

Fake webshops, dropshipping & online guru's

Herkennen van onbetrouwbare webwinkels en zogenaamde experts die beloven snel rijk te worden met minimale inspanning.

Nepnieuws en desinformatie

Vaardigheden om betrouwbare van onbetrouwbare informatie te onderscheiden en kritisch mediageletterd te zijn.

Online radicalisering & extremisme

Inzicht in hoe extremistische groepen jongeren online rekruteren en radicaliseren, en hoe dit te herkennen.

Online medicijnen en drugs

Bewustwording van de toegankelijkheid van illegale substanties online en de bijbehorende risico's.

Verspreiding van zelfbeschadiging/eetstoornis-content

Herkennen van platforms die zelfbeschadiging of eetstoornissen verheerlijken en hoe hiermee om te gaan.

Gevaarlijke contacten via games, apps en chatplatforms

Inzicht in risicovolle interacties tijdens online games en in chatapps, en hoe deze te vermijden.

Online predatoren en pedofielen

Begrip van tactieken die online predatoren gebruiken en hoe kinderen hiertegen te beschermen.

(Cyber)criminele recruitment

Herkennen hoe criminele netwerken jongeren online rekruteren voor illegale activiteiten en hoe dit te voorkomen.

Verslavingsgevoelige apps

Inzicht in welke apps specifiek ontworpen zijn om verslavend te zijn en hoe gezond gebruik te stimuleren.

Kunstmatige intelligentie

Begrip van AI-toepassingen, de impact op het dagelijks leven van jongeren en zowel de kansen als risico's.

Crypto en online valuta

Basiskennis over cryptocurrencies, NFTs en de risico's van investeringen en oplichting in deze sector.

ACTIEPUNTEN

- **Stappenplannen voor verschillende situaties**
- **Contactgegevens van instanties en hulporganisaties**
- **Communicatie: hoe praat je met kinderen en jongeren?**
- **Toezicht en betrokkenheid: een gezonde balans**
- **Cybersecurity basics**
- **Online reputatie opbouwen**

IMPLEMENTATIE VOOR SCHOLEN

Stappenplan implementatie:

Oriëntatie en besluitvorming

- Kennismakingsgesprek met Didev
- Behoeftenanalyse binnen de school
- Keuze voor modules en deelnemende personeelsleden

Vorbereiding

- Overeenkomst voor licenties (minimaal 20)
- Communicatieplan naar personeel en ouders
- Planning van trainingen

Lancering

- Kick-off bijeenkomst voor deelnemers
- Activatie e-learning platform
- Eerste online training

Uitvoering en verankering

- Integratie in bestaande protocollen
- Materialen inzetten in de klas
- Oudervoorlichting organiseren

Evaluatie en verduurzaming

- Impactmeting
- Plan voor continuering
- Eventuele uitbreiding

Ondersteuning:

- Volledig implementatieplan voor scholen
- Communicatiematerialen voor ouders en leerlingen
- Maandelijkse online trainingen voor startende deelnemers
- Technische ondersteuning bij gebruik van het e-learning platform
- Advies op maat voor specifieke schoolsituaties
- Lesmateriaal voor verschillende leeftijdsgroepen



Resultaten van CyberBurger

INVESTERING

Wij streven ernaar om de kennis zo toegankelijk mogelijk te maken tegen zo laag mogelijke kosten.

Licentiestructuur:

- Basislicentie: €50 per persoon per jaar

Pakketprijzen:

Voor scholen: Minimale afname van 20 licenties - €1.000,- Inclusief toegang tot alle modules, maandelijkse trainingen, oudermateriaal en lesmateriaal

Wat is inbegrepen:

- 24/7 toegang tot alle e-learning modules
- Maandelijkse online trainingen voor deelnemers
- Materialen voor oudervoorlichting
- Lesmateriaal voor in de klas
- Updates bij nieuwe ontwikkelingen
- Technische ondersteuning
- Implementatiebegeleiding

Extra services (optioneel):

- Training op locatie: €1.500,- per dag
- Spreken op evenementen: €1.500,-
- Maatwerk lesmateriaal: op aanvraag

CONTACT GEGEVENS

Telefoon

0316-798 000
(nummer van Didev)

Email

Info@cyberburger.nl

Website

www.CyberBurger.nl

Postadres

Nieuwkamppad 2
6905VD Zevenaar

