Cybercrime en jongeren: wat moet je als ouder weten?

1. Introductie

Het leven speelt zich meer en meer online af, en dat zien we terug in de criminaliteitscijfers. Traditionele criminaliteit neemt af en online criminaliteit neemt sterk toe.

Preventie
Net zoals dat er regels zijn in het verkeer, zijn er ook regels in de digitale wereld. Mensen moeten hierover leren zodat ze weten wat wel en niet mag in het digitale domein. Zo vroeg mogelijk voorlichting krijgen over dit brede onderwerp, verkleint de kans dat iemand later de criminele digitale wereld betreedt. Daarom is het belangrijk dat jongeren, hun ouders, de school maar ook de politie hiermee aan de slag gaan.

Dit boekje dient als ondersteuning om te leren over de regels en wetgeving van de online wereld en draagt mogelijkheden aan om digitale vaardigheden binnen een veilige, legale haven door te ontwikkelen.

Vragen over het jongeren en cybercrime?
Neem contact op met je wijkagent. De contactgegevens zijn te vinden op https://www.politie.nl/mijn-buurt/wijkagenten

Opmerkingen over de inhoud van dit boek?
Mail dan naar daderpreventie@politie.nl

2. Cybercrime

Je hoort het steeds vaker: servers worden platgelegd, burgers die slachtoffer zijn van phishing en bedrijven die te maken krijgen met DDoS-aanvallen. Cybercrime komt steeds meer voor. Overal hoor je verschillende termen, maar wat verstaan we nou eigenlijk precies onder cybercrime?

Het verschil tussen gedigitaliseerde criminaliteit en cybercriminaliteit
Online criminaliteit kan onderverdeeld worden in gedigitaliseerde criminaliteit en cybercriminaliteit. Als we het over 'cybercrime' hebben, gaat het dus over cybercriminaliteit en niet gedigitaliseerde criminaliteit.

Gedigitaliseerde criminaliteit
Met gedigitaliseerde criminaliteit bedoelen we traditionele delicten waarbij gebruik wordt gemaakt van ICT. Denk bijvoorbeeld aan het:

- voordoen als iemand anders op het internet
- bedreigen van personen via sociale media of andere digitale kanalen
- verspreiden van seksueel beeldmateriaal van minderjarigen
- kopen via internet maar het geld niet overmaken, of iets verkopen via internet en het artikel niet opsturen

Cybercriminaliteit
Met cybercriminaliteit bedoelen we delicten waarbij ICT zowel het doel als het middel is. Denk aan het:

- inloggen op een computer of website zonder toestemming of kennisgeving
- wachtwoorden veranderen
- misbruik maken van gehackte accounts van webshops of sociale media kanalen
- DDoS-aanvallen uitvoeren
- virussen versturen

Strafbaarheid van cybercrime
In Nederland is cybercrime vastgelegd in het Wetboek van Strafrecht. Bekijk het overzicht voor de meest voorkomende cybercrimedelicten en de straffen die opgelegd kunnen worden.

Delict	Betekenis	Hoogst mogelijke straf
DDoS-aanval *artikel 138b*	Een DDoS-aanval is een digitale aanval waarbij de digitale infrastructuur van een bedrijf wordt platgelegd door de servers met grote hoeveelheden data te bestoken.	Vijf jaar gevangenisstraf of een geldboete tot € 22.500)
Hacken *artikel 138ab*	Hacken is het toegang verschaffen tot systemen waartoe de gebruiker niet gemachtigd is, bijvoorbeeld door het kraken van wachtwoorden.	Vier jaar gevangenisstraf of een geldboete tot € 22.500
Phishing *artikel 326*	Phishing is een vorm van online fraude waarbij slachtoffers criminelen toegang geven tot hun persoonlijke informatie of bankrekening.	Vier jaar gevangenisstraf of een geldboete tot € 90.000
Ransomware *artikel 317*	Ransomware is Engels voor gijzelsoftware. Hiermee blokkeren criminelen jouw computer of versleutelen zij een of meerdere bestanden op uw computer. Vaak moet je een bedrag in virtuele valuta, zoals bitcoins, betalen om de computer of bestanden weer terug te krijgen.	Negen jaar gevangenisstraf of een geldboete tot € 90.000
Malware *artikel 350a-3*	Malware is Engels voor kwaadaardige software en is schadelijk voor je computer. Het wordt gebruikt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot computersystemen. Er zijn verschillende soorten malware, waarvan virussen de bekendste zijn.	Vier jaar gevangenisstraf of een geldboete tot € 90.000

Wie pleegt cybercrime?
Plegers van cyberdelicten zijn vaak jong. In veel gevallen zijn daders jonger dan 23 jaar. Daarom is het belangrijk om jongeren al vroeg voorlichting te geven, zodat ze minder vatbaar zijn voor de verleidingen van digitale criminaliteit.

Wat maakt cybercrime verleidelijk?
Is geld de ultieme motivatie om een cyberdelict te plegen? Wanneer het om traditionele delicten in een nieuw jasje gaat waarschijnlijk wel. Gedigitaliseerde vormen van oplichting en fraude worden vaak gepleegd vanuit financieel gewin. Maar, gaat het om cyberdelicten zoals hacken of het ontwikkelen van malware, dan zijn de motieven vaak complexer. Aanzien speelt dan ook een rol. Denk aan complimenten krijgen op een bepaald forum. Of je skills die erkend worden door hoogstaande IT'ers? Daar doe je het voor. Status en populariteit in de onlinewereld zijn verleidelijk voor jongeren die in het offline leven minder aandacht krijgen. Net een stap te ver gaan omdat dat meer respect oplevert, is voor veel jongeren dan geen grote stap meer.

Maatschappelijke gevolgen
De (potentiële) gevolgen van cybercrime kan ongekend groot zijn. Ziekenhuizen waarvan de beademingsapparatuur het niet meer doet, familiebedrijven die miljoenen euro's zien verdwijnen, of een leven aan herinneringen dat door een hack niet meer terug te vinden is. Zijn plegers zich hiervan bewust? Weet iemand van 14 jaar wat voor gevolgen een DDoS-experiment heeft op slachtoffers? Bewustzijn creëren dat één persoon online grote maatschappelijke schade aan kan richten, is daarom noodzakelijk.

3. Positieve alternatieven voor jongeren

De digitale skills van de jongeren kunnen veel potentie hebben. Het zijn skills waarmee ze later de wereld een stukje veiliger kunnen maken. Maar het zijn ook skills die de deuren openen naar de donkere kanten van het internet. Door jongeren zo vroeg mogelijk een goed alternatief te bieden, kun je voorkomen dat jongeren het verkeerde (digitale) pad kiezen.

Van bedreiging naar kans
Een digitale grens is makkelijk overschreden. In andere woorden: als je bezit over technische en digitale kennis geeft dat verantwoordelijkheid. Verantwoordelijkheid dat je jouw skills op een verantwoorde en legale manier inzet. Daar zijn ook volop mogelijkheden voor. Denk alleen al aan het tekort aan mensen met cyberskills, bijvoorbeeld bij de politie. Niet alleen in Nederland maar ook in het buitenland. Je kunt jongeren op allerlei manieren inzicht geven in hun (potentiële) cyberskills en ze wijzen op manieren om die skills verantwoord te verbeteren. Bekijk hier per leeftijdsgroep waar je jongeren op kunt wijzen.

Kinderen(van 8 tot en met 16 jaar)

- **Codecademy -** www.codecademy.com
  Voor kinderen die geïnteresseerd zijn in het leren coderen, is dit de perfecte plek om te beginnen.

- **Hackshield -** nl.joinhackshield.com/nl
  Game voor kinderen waarbij ze in verschillende levels leren om zichzelf online te beveiligen. Er is ook een quest waarin ze leren over online grenzen.

- **Scratch** - https://scratch.mit.edu/studios/158335
  Website waar kinderen de basis van het programmeren kunnen leren.

Jongvolwassenen (vanaf 16 jaar)

- **Inspired Careers -** https://careers.inspirededu.com/
  Een innovatieve hub die alle baanmogelijkheden en carrièrepaden laat zien als het gaat om cybersecurity.

- **Bug bounties**
  Veel bedrijven bieden tegenwoordig bug bounty programma's aan. Dat zijn programma's waarbij hackers wordt gevraagd om kwetsbaarheden in hun systemen op te sporen en dit door te geven aan het bedrijf voor verbetering. Zo kunnen hackers hun talenten inzetten voor een goed doel en daar geld mee verdienen.

- **Opleidingen en banen in de IT, cybersecurity en gaming industrie -**
  https://www.studentum.nl/zoeken/it-opleidingen
  https://blog.andwork.com/ict-opleiding-overzicht-opleidingen/
  https://www.carrierebeurs.nl/de-nationale-carrierebeurs/item508
  https://www.crimediggers.nl/

Overige training

- **Hack the box -** www.hackthebox.eu
  Een online trainingsplatform waarbij je cybervaardigheden op het gebied van beveiliging kunt leren en verbeteren via games.

- **Vulnhub -** www.vulnhub.com
  Biedt online materiaal aan waarmee praktische ervaring kan worden opgedaan op het gebied van digitale beveiliging, computerapplicaties en netwerkbeheertaken.

- **Cybrary -** www.cybrary.it
  Een online trainingsplatform dat zich focust op IT en cyberbeveiliging.

- **SANS Cyber Aces -** www.cyberaces.org
  Gratis online cursus die je de basisconcepten leert die nodig zijn om informatiebeveiligingssystemen te beoordelen en te beschermen.

- **CoderDojo -** www.coderdojo.com
  Communitygebaseerde programmeerclubs voor jongeren. Op deze website zijn de diverse CoderDojo's in Nederland te vinden en wordt aangegeven waar en wanneer de CoderDojo's plaatsvinden.

- **Free Code Camp** - www.freecodecamp.org
  Hier kun je vele video's, artikelen en interactieve lessen over codering vinden.

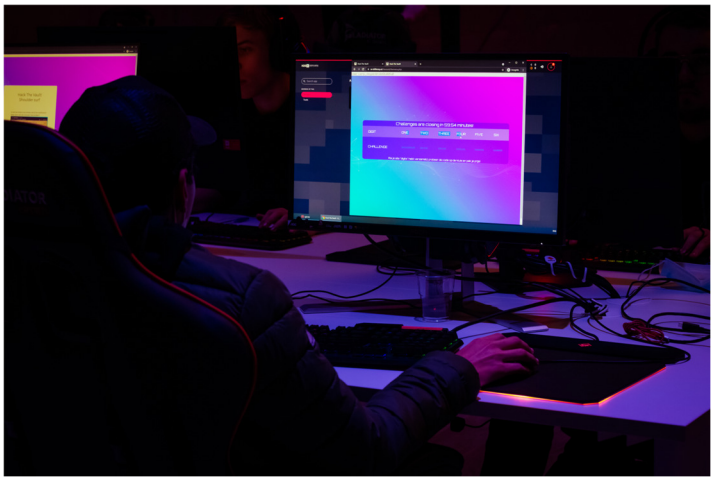
- **Cyber security challenge -** www.cybersecuritychallenge.org.uk
  Op dit platform kunnen jongeren meedoen aan online challenges waarmee ze hun cyberskills testen en verbeteren.

4. Initiatieven

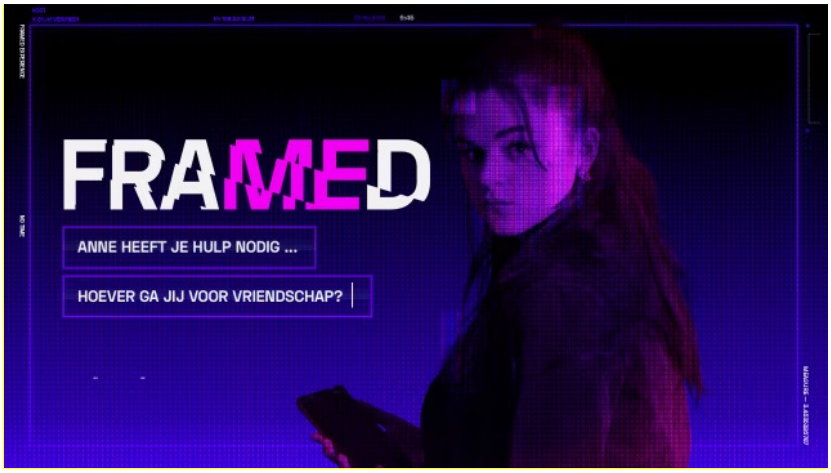
Jongeren zijn zich vaak niet bewust van de mogelijke gevaren van hun online gedrag. Voor jongeren die zich bevinden in het grijze gebied van legale en illegale online activiteiten zijn er passende initiatieven. Daarmee kunnen ze in gaan zien welke gevaren ze lopen en welke positieve alternatieven er ook zijn. Bekijk hier welke initiatieven er zijn waar je jongeren op kunt wijzen.

re_B00TCMP
Een samenwerking tussen gemeenten, politie en scholen: dat is re_B00TCMP. re_B00TCMP is een dagevent voor jongeren tussen 12 en 25 jaar met skills en interesse op het gebied van IT. Op deze dag geven toonaangevende IT'ers presentaties. Jongeren krijgen hierdoor een inkijkje in het toekomstperspectief dat de IT-industrie biedt als ze hun talenten juist inzetten. Ook leren ze over de grenzen van de wet. Het is niet alleen een informatieve dag: ze kunnen een potje gamen met de politie en aan het eind van de dag meedoen aan een challenge waarmee ze een prijs kunnen winnen. Ouders en docenten zijn ook welkom, voor hen is er een speciaal programma ontwikkeld. Zo krijgen ze tijdens re_BTCMP meer informatie over hacken en tips om het gesprek aan te gaan met jongeren.

- Jongeren kunnen niet zomaar deelnemen aan re_B00TCMP. Ze worden eerst geselecteerd via een assessment in de vorm van een game. De game is te vinden op www.re-B00TCMP.nl.
- Om als ouder te kunnen deelnemen aan re_B00TCMP in je regio, kun je een mail sturen naar info@re-B00TCMP.nl



Framed
Framed is een cybergame die zich afspeelt op school. Om te testen hoever leerlingen gaan voor vriendschap, krijgen ze een aantal keuzes voorgelegd. Keuzes zoals het wel of niet doorsturen van inloggegevens om cijfers te veranderen in het schoolsysteem. Door met zulke dilemma's aan de slag te gaan, ontdekken ze welke gevolgen hun online gedrag kan hebben. En dat ook zij op een gewone schooldag slechts één klik verwijderd zijn van het plegen van cybercrime. Na het spelen van Framed is er een klassikaal nagesprek.



HackShield
HackShield is een cybersecuritygame waarin kinderen tussen 8 en 12 jaar opgeleid worden tot ‘junior cyber agent’. De game maakt kinderen via verhalen bewust van de gevaren die ze online lopen. Kinderen leren tijdens tientallen levels alles over onder meer het maken van sterke wachtwoorden, omgaan met online pesten en phishing. Ze leren online gevaar herkennen en voorkomen. Daarnaast kunnen kinderen quests doen zelfs eigen levels maken.

- Hackshield kun je spelen via https://nl.joinhackshield.com/nl
- HackShield heeft ook een variant die bedoeld is voor volwassenen. Ga hiervoor naar: https://hackshield.herocenter.com/

5. Wat als mijn kind cybercrime pleegt?

Stel je voor, de schoolwebsite ligt eruit en de kans is groot dat dit komt door een DDoS-aanval van een leerling. Vervolgens word je gebeld door de school: het blijkt om jouw kind te gaan. Wat kun je doen?

We hebben twee scenario's uitwerkt: een scenario waarin je kind zich al schuldig heeft gemaakt aan het plegen van cybercrime en het tweede wanneer je het preventieve gesprek aan wilt gaan.

Goed om te weten: scholen hebben vaak geen CVD-beleid
In een CVD-beleid staan afspraken over hoe kwetsbaarheden in het digitale netwerk van een organisatie gemeld kunnen worden en hoe deze vervolgens afgehandeld worden. In het kort komt het erop neer dat mensen die zo'n lek of kwetsbaarheid vinden, daar niet meteen voor gestraft zullen worden maar eerder gewaardeerd. Het verantwoord doorgeven van deze informatie, draagt namelijk bij aan de veiligheid van het netwerk.

Scholen hebben vaak geen CVD-beleid. Een CVD-beleid hebben is juist belangrijk, want scholen zijn bij uitstek een veilige plek voor jongeren om te experimenteren en grenzen op te zoeken. Dat maakt de kans ook groter dat het plegen van cybercrime binnen een schoolomgeving gebeurt. De aanwezigheid van een CVD-beleid beschermt een jongere in zekere zin, mits de jongere eerlijk en tijdig melding doet van het gevonden lek.

Scenario 1 - Dader is bekend
Heeft jouw kind cybercrime gepleegd? Dan is het belangrijk om het gesprek aan te gaan. Bekijk hiervoor het hoofdstuk 'Tips om het gesprek aan te gaan'. Bespreek met je kind welke ethische kwesties komen kijken bij het plegen van cybercrime, wat de grenzen van de wet zijn en wat de gevolgen voor het kind zelf kunnen zijn. Denk bijvoorbeeld aan een strafblad en het risico dat het van kwaad tot erger gaat. Wijs je kind ook op de voordelen van het CVD-beleid, zoals het op een veilige manier zoeken naar kwetsbaarheden in het schoolsysteem en eventueel daarvoor beloond worden. Tot slot kun je contact zoeken met Halt. Halt is een instantie die interventies biedt om jeugdcriminaliteit te voorkomen en om jongeren te stimuleren hun talenten en interesses op een constructieve manier in te zetten.

Scenario 2 - Preventief
Voorkomen is beter dan genezen. Daarom is het verstandig om in te zetten op preventie. Ook hierbij speelt het CVD-beleid een rol. Daarnaast zijn er zoveel kansen voor jongeren om hun vaardigheden op een goede manier in te zetten. Vaak zijn jongeren zich niet bewust van deze mogelijkheden. Denk je dat jouw kind goede online vaardigheden heeft? Wijs je kind dan op de kansen die je kind daar later mee heeft: denk aan studierichtingen en baanperspectief. Ook zijn er allerlei manieren voor je kind om vaardigheden te testen en te verbeteren. Een overzicht hiervan vind je in het hoofdstuk 'Positieve alternatieven voor jongeren'.

Vragen aan de politie?
Wil je graag meer weten over wat te doen als je kind cybercrime pleegt, of als je je hier zorgen om maakt? Neem dan contact met ons op via daderpreventie@politie.nl.

6. Casus - Maar één klik verwijderd van cybercrime

Het verhaal van Jesse*
Jesse is 18 jaar en een gamer in hart en nieren. Een van zijn favoriete games is Runscape. Tijdens dit spel wordt hij vaak ge-DDoSt. Jesse doet wat onderzoek naar DDoS-aanvallen en komt daarbij op verschillende sites terecht waaronder een hackforum. Op dit forum vindt hij informatie over hoe je zo'n aanval uit kunt voeren. Uit nieuwsgierigheid wil hij dat een keer proberen. Verrassend makkelijk, ervaart hij. Ineens realiseert hij zich dat hij wel een goed doelwit weet voor zo'n aanval: twee docenten van zijn middelbare school. Dat was een succes, Jesse had flink wat lol met zijn vrienden om het ongemak dat de docenten ondervonden van Jesses actie. Ook merkt hij dat hij meer respect kreeg van vrienden vanwege zijn skills.

Jesse leert steeds meer op de hackforums en gaat telkens een stapje verder. Samen met een vriend van het hackforum bouwt hij een webstresser. Deze verkoopt hij voor een vast bedrag per maand. Uiteindelijk bouwt Jesse een botnet, zodat hij ook zelf krachtige DDoS-aanvallen kan aanbieden. Hij wordt ook ingehuurd door partijen om het hun concurrenten digitaal moeilijk te maken. Zo heeft hij onder andere de Britse nieuwszender BBC, Yahoo en enkele Nederlandse banken aangevallen.

Op zijn 18e wordt Jesse aangehouden door de politie. Hij zit een maand lang in jeugddetentie en krijgt daarna Hack_Right opgelegd. Tijdens dit traject leert hij voor het eerst over de wettelijke online grenzen. Ook ontdekt hij dat er positieve alternatieven voor zijn IT-talenten zoals hij. Na Hack_Right heeft Jesse zijn IT-talent over een andere boeg gegooid: hij is nu ethisch hacker en heeft een aantal ondernemingen opgericht in cybersecurity opgericht. Ook zet hij zich in om jongeren te waarschuwen voor de gevaren van cybercrime door zijn eigen verhaal te delen.

Gebruik deze casus als voorbeeld
Het verhaal van Jesse laat zien dat jongeren maar één klik verwijderd zijn van cybercrime. Daarom is preventie en voorlichting zo'n belangrijk onderdeel in de aanpak van cybercrime, zeker bij jongeren. Want voorkomen is beter dan genezen. Je kunt deze fictieve casus van Jesse gebruiken als voorbeeld om jongeren in te laten zien wat de gevaren van cybercrime zijn. Het schetst een goed beeld van hoe het onschuldig lijkt te beginnen, maar hoe het uiteindelijk ernstige gevolgen heeft.

*Vanwege privacy redenen is Jesse een fictieve naam.

7. Tips om het gesprek aan te gaan

Je kind is ongetwijfeld online actief. Misschien meer dan je zou willen. Heb je het gevoel dat je kind er online een leven op nahoudt waar je geen idee van hebt? Of maak je je zorgen om het onlinegedrag van je kind? Dan is het goed om het gesprek aan te gaan.

Offline versus online
Jongeren hebben van nature de neiging om grenzen op te zoeken. Dit is volkomen normaal en hoort bij de ontwikkeling die zij doormaken tot volwassene. Het is natuurlijk wel belangrijk dat ze de regels kennen en zich bewust zijn van wanneer ze te ver gaan. In de offlinewereld is dit vrij duidelijk: als iemand een steen door een ruit gooit, dan wordt diegene gelijk gewezen op de strafbaarheid daarvan. In de onlinewereld gebeurt dit veel minder snel. Dat komt omdat het van buitenaf niet te zien is dat iemand een grens overgaat. Vaak wordt het pas zichtbaar als het te laat is, bijvoorbeeld als iemand een zwaar cyberdelict heeft gepleegd. Met niet alleen een strafblad tot gevolg, maar soms ook een gevangenisstraf. Daarom is het zo belangrijk om bij de eerste signalen het gesprek met je kind aan te gaan. Ook als er geen signalen of vermoedens van cybercrime zijn, is het goed om het gesprek aan te gaan.

Maak de regels bespreekbaar
Het zal niet zo zijn dat de politie gelijk op de stoep staat op het moment dat je kind de computer van een broertje of zusje heeft gehackt. Maar zolang het thuis niet duidelijk is welke regels er zijn, zal een kind eerder geneigd zijn de grens over te gaan. Zo kan iets relatief onschuldigs leiden tot het plegen van een serieus cyberdelict. En dan zal de politie wel op de stoep staan. Bespreek daarom goed welke afspraken er online gelden. Het lijkt logisch dat je iemand niet mag hacken, maar als je kind van jou nooit hoort dat dit strafbaar is en wat daar de gevolgen van zijn, zal je kind sneller de grenzen opzoeken. Ook kun je meer grip krijgen op het online leven van je kind als je erover praat thuis: wat doet je kind online? Met wie heeft je kind contact en waarover? En zijn er grenzen aan de tijd die je kind online besteedt? Onderzoek hierin wat passend is bij jouw opvoedstijl. Laat ook zien dat je oprecht geïnteresseerd bent. Dat creëert een veilige setting om samen het gesprek aan te gaan. En hoe veiliger en vertrouwder je kind zich voelt om zaken met jou te bespreken, hoe kleiner de kans dat je kind het verkeerde pad op gaat.

Benadruk de kansen
Het is absoluut niet alleen maar zorgelijk als jouw kind interesse heeft in alles wat met cyber te maken heeft. Sterker nog: het biedt je kind veel kansen voor later. De samenleving heeft mensen met cybertalent hard nodig, bijvoorbeeld in cybersecuritybedrijven of bij de politie. Bespreek dit ook met je kind. Want goed geïnformeerde jongeren maken vaker verstandige keuzes.

Benieuwd naar meer tips?
Kijk voor meer tips op deze site: www.gameninfo.nl/opvoeding/tips-voor-ouders