DE ONTWIKKELPADEN VAN JONGE HACKERS: EEN EERSTE VERKENNING

In opdracht van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV)

Auteurs:

Dr. Luuk Bekkers

Prof. dr. Rutger Leukfeldt

Augustus 2026

1. Inleiding

1.1. Achtergrond

De aard en omvang van criminaliteit is fundamenteel veranderd door de bredere technologische ontwikkelingen in de maatschappij. Er zijn nieuwe vormen van crimineel gedrag ontstaan die gedeeltelijk of volledig berusten op het gebruik van computers en internet, ook wel online criminaliteit genoemd (Holt & Bossler, 2014; McGuire & Dowling, 2013; Phillips et al., 2022). Online criminaliteit omvat 'alle misdrijven waarbij informatie- en communicatietechnologie (ICT) van wezenlijk belang is voor de realisatie van het delict' (zie ook Phillips et al., 2022). Ze behoren tegenwoordig tot de meest voorkomende vormen van criminaliteit onder burgers en bedrijven, zowel wat betreft slachtofferschap als daderschap (Akkermans et al., 2024; Eurobarometer, 2022). Daarbij is ook de zelf-gerapporteerde impact even groot of zelfs groter dan bij offline criminaliteit (Borwell et al., 2025).

Deze ontwikkelingen roepen vragen op de toepasbaarheid van bestaande criminologische inzichten. Dat geldt in het bijzonder voor plegers van cybercriminaliteit. Deze groep delictplegers zijn betrokken bij vormen van online criminaliteit die volledig berusten op het gebruik van computers en technologie, zoals website defacement en malware. Voor de leesbaarheid verwijzen we naar deze groep als "hackers". De term hacking wordt dus als synoniem voor cybercriminaliteit gebruikt. Hebben we daarbij te maken met een nieuwe dadergroep? Of reflecteert hacken simpelweg een ander medium voor mensen die net zo goed offline delicten plegen? Het antwoord op dit soort vragen is niet alleen theoretisch relevant maar heeft ook verregaande implicaties voor de praktijk. Interventie kan namelijk alleen effectief zijn als maatregelen zijn afgestemd op de doelgroep en diens kenmerken (Bonta & Andrews, 2023; Hendriks & Stams, 2024). Het is daarom belangrijk dat er wetenschappelijk onderzoek wordt gedaan naar hackers en andere type daders van online criminaliteit.

Het beperkte onderzoek dat tot nu toe is gedaan laat zien dat hackers mogelijk vrij unieke ontwikkelpaden en risicofactoren hebben. Verkennend onderzoek maakt bijvoorbeeld duidelijk dat deze doelgroep wordt gekenmerkt door een hogere mate van zelfcontrole (Bekkers et al., 2025a). Ze spenderen tijd aan programmeren en zijn intrinsiek gemotiveerd om vaardigheden te verbeteren (Loggen et al., 2024; Martineau et al., 2024). In andere woorden, jongeren met vaardigheden en interesses op het gebied van informatie technologie (IT) lopen risico om betrokken te raken bij cybercriminaliteit (Bekkers et al., 2026b; Weulen-Kranenbarg et al., 2018; Paquet-Clouston, 2021). Sommige jongeren zijn geïnteresseerd in het hacken van games en escaleren in delictgedrag nadat ze worden aangemoedigd door vrienden, terwijl andere jongeren experimenteren op internet en eigenlijk zonder intentie veel schade aanrichten (Leukfeldt & Bekkers, 2026).

Wat studies laten zien is dat het hebben van interesses en vaardigheden op het gebied van IT, en bijvoorbeeld een opleiding volgen of werk hebben in de IT-sector, een risico kan zijn voor online delictgedrag (Weulen Kranenbarg et al., 2019; Bekkers et al., 2025a). Het beperkte onderzoek dat is gedaan naar deze doelgroep richt zich echter vaak op delictplegers (e.g., Fox & Holt, 2021; Martineau et al., 2024); het is ook relevant om de ontwikkelpaden en kenmerken van jongeren in kaart te brengen die wel affiniteit hebben voor IT maar nog niet persé delicten hebben gepleegd. Die kennis kan helpen om vroegtijdig in te grijpen: preventie is essentieel.

1.2. Het huidige onderzoek

Het doel van dit onderzoek is om meer zicht te krijgen op de ontwikkelpaden en kenmerken van jongeren (i.e., 12 tot 25 jaar) met een hoge affiniteit en interesse voor computers en technologie. Dit betreft een risicogroep voor betrokkenheid bij cybercriminaliteit. Kennis over deze doelgroep is nodig voor het ontwikkelen en implementeren van effectieve interventies, in lijn met het landelijk kwaliteitskader effectieve jeugdinterventies voor de preventie van jeugdcriminaliteit (Hendriks & Stams, 2024). Het onderzoek kan daarmee ondersteunen bij het ingrijpen in een vroeg stadium en voorkomen dat jongeren – soms onbedoeld – een delict plegen en slachtoffers maken. We maken hierbij gebruik van twee dataverzamelingsmethoden: interviews en vragenlijstonderzoek. De interviews zijn gevoerd met jongeren die affiniteit en interesse hebben op het gebied van computers en technologie en daarmee risico lopen om betrokken te raken bij cybercriminaliteit, maar verder nog geen delicten hebben gepleegd. De vragenlijst brengt risicofactoren in kaart en is afgenomen onder de algemene populatie jongeren (controlegroep) en opnieuw ook onder jongeren met affiniteit en interesse op het gebied van computers en technologie (de risicogroep). De volgende onderzoeksvragen staan centraal in dit onderzoek:

1. Wat zijn de demografische en psychologische kenmerken van jongeren met een hoge affiniteit voor IT?

2. Hoe ontwikkelen jongeren met affiniteit voor IT vaardigheden en interesses voor hacken?

3. Op welke manier wordt het online gedrag van jongeren met een hoge affiniteit voor IT beïnvloed door hun sociale omgeving?

4. In hoeverre en op welke manier is er een link tussen daderschap van cybercriminaliteit en daderschap van offline criminaliteit?

5. Wat zijn de overeenkomsten en verschillen tussen jongeren die risico lopen op online daderschap en jongeren die daadwerkelijk delicten hebben gepleegd?

6. Wat zijn beschermende factoren die kunnen voorkomen dat jongeren met een hoge affiniteit voor IT betrokken raken bij hacken?

1.3. Afbakening

Online criminaliteit omvat ‘alle misdrijven waarbij informatie- en communicatietechnologie (IT) van wezenlijk belang is voor de realisatie van het delict’ (zie ook Phillips et al., 2022). Daarbij worden vaak twee categorieën onderscheiden (McGuire & Dowling, 2013): misdrijven waarbij IT zowel het middel als het doel en misdrijven waarbij IT uitsluitend het middel is. De eerste categorie is ‘cybercriminaliteit’. Hieronder vallen delicten zoals website defacement (i.e., het aanpassen van het tekstuele of visuele uiterlijk van een website zonder toestemming) en betrokkenheid bij DDoS aanvallen (i.e., het overspoelen van een website, server of online dienst met informatie waardoor deze traag wordt of helemaal onbereikbaar). De tweede categorie wordt veelal ‘cybercriminaliteit in ruime zin’ of ‘gedigitaliseerde criminaliteit’ genoemd. De meest voorkomende type delicten in deze categorie zijn financieel-economische delicten, voornamelijk phishing, bankhelpdeskfraude, aan- en verkoopfraude en hulpvraagfraude/Whatsappfraude. Dit onderzoek richt zich dus op jongeren die risico lopen op betrokkenheid bij cybercriminaliteit, ook wel hackers genoemd.

1.4. Leeswijzer

Het rapport bestaat uit een aantal hoofdstukken. Hierna volgt eerst een uiteenzetting van bestaande literatuur omtrent risicofactoren van cybercriminaliteit en de ontwikkelpaden van hackers in hoofdstuk 2. De focus daarbij is op criminele hackers. Daarna beschrijven we de methode in hoofdstuk 3, waarbij een onderscheid wordt gemaakt tussen interviews en vragenlijstonderzoek. Hoofdstuk 4 draait om de resultaten van deze twee dataverzamelingsmethoden. In hoofdstuk 5 volgt een algemene conclusie.

2. Inzichten uit eerder onderzoek

2.1. Ontwikkelpaden van criminele hackers

Het huidig onderzoek richt zich op jongeren die wel interesse en affiniteit hebben met IT en nog geen delicten hebben gepleegd, maar in de afgelopen jaren zijn er door de onderzoekers ook interviews gevoerd met 22 criminele hackers (Leukfeldt & Bekkers, 2026). De bevindingen van dat onderzoek zijn ook relevant voor de huidige studie. Op basis van die interviews is daarbij een ontwikkelpad geschetst van criminele hackers, weergegeven in Figuur 1. In deze sectie beschrijven we de belangrijkste bevindingen van dat onderzoek in de vorm van een samenvatting. Voor methodologische kwesties en aanvullende informatie verwijzen we door naar Leukfeldt en Bekkers (2026).

Respondenten uit de studie van Leukfeldt en Bekkers (2026) geven vaak een vroege interesse in informatietechnologie aan. Ze herinneren zich levendig hun eerste ontmoetingen met computers of gamen en beschrijven dat ze gefascineerd waren door hoe technologie werkte, vaak al vóór hun tiende. Dit wordt ook herkend in ander onderzoek (Martineau et al., 2024; Noordegraaf & Weulen Kranenbarg, 2023). Martineau en collega's hebben bijvoorbeeld ook hackers geïnterviewd en daar specifiek aandacht besteed aan persoonlijkheidstrekken op jonge leeftijd. Respondenten beschrijven zichzelf daarbij vroeger als stille en verlegen kinderen die liever zelfstandige activiteiten ondernamen dan betrokken te zijn bij sociale interacties. Ze spendeerden tijd aan Lego, puzzels of bordspellen, en herkennen zich eerder in een introverte persoonlijkheid waarbij sprake was van angstklachten.

Opvallend is dat de interesse in IT in de loop van de tijd lijkt aan te houden en dat respondenten een soort preoccupatie met computers ervaren die tot ver in de adolescentie doorgaat, maar zich anders uit naarmate ze ouder worden. Zo waren vrijwel alle respondenten op latere leeftijd actief als ethisch hacker of bezig met een opleiding in IT. Dit beeld ontstaat ook in ander onderzoek, zoals die van Noordegraaf en Weulen Kranenbarg (2023). De auteurs hebben 15 ethische hackers geïnterviewd om de carrière over de tijd heen beter te begrijpen. Ze zijn begonnen met hacken vooral vanwege de kick en de uitdaging en zijn zich langzaam steeds meer bezig gaan houden met de ethische kant, zoals het rapporteren van kwetsbaarheden.

Vanuit de vroege interesses en ervaringen onthult de analyse van criminele hackers door Leukfeldt en Bekkers (2026) twee duidelijk verschillende paden: 1) jongeren die worden blootgesteld aan online leeftijdsgenoten die ze via gaming ontmoeten en die hun initiële interesse aanwakkeren, en 2) jongeren die computervaardigheden ontwikkelen en interesses zelfstandig verkennen in relatieve sociale isolatie van leeftijdsgenoten.

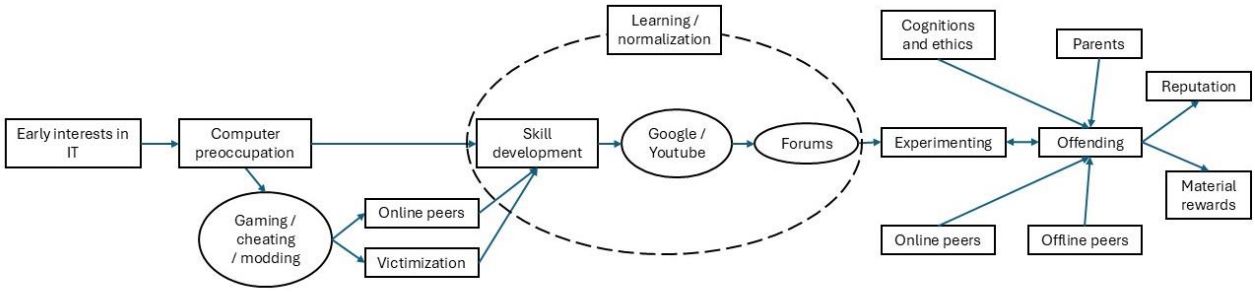
Individuen die worden gekenmerkt door het eerste traject besteden veel tijd aan online gamen, tot op het punt dat sommigen professionele hulp nodig hadden voor gameverslaving (zie ook NCA, 2017). Tijdens het gamen ervaren respondenten slachtofferschap in de vorm van DDoS-aanvallen of worden ze blootgesteld aan andere hackers die valsspelen in het spel. Dit kan een keerpunt vormen waardoor jongeren op een later moment zelf betrokken raken bij valsspelen of cybercriminaliteit, bijvoorbeeld uit nieuwsgierigheid naar hoe het werkt of als een vorm van vergelding. Online gamingplatforms bieden ook toegang tot online peers die valsspelen of ernstigere cybercriminaliteit aanmoedigen. Zij verschaffen de nodige kennis om dergelijke handelingen te plegen of stellen jonge hackers in staat toegang te krijgen tot gesloten hackomgevingen. Via gaming komen jongeren terecht op externe hackingfora of cheatfora waar zij hun vaardigheden verder ontwikkelen en mogelijk escaleren in criminele activiteiten. Respondenten varieerden in de mate waarin zij deelnamen aan online fora, waarbij sommigen als lurkers werden omschreven en anderen actief deelnamen aan discussies.

Andere hackers volgen niet het gamingtraject. Gedreven door de motivatie om algemene vaardigheden te ontwikkelen op het gebied van informatietechnologie, zoals verschillende programmeertalen, besteden jongeren tijd op internet om hun capaciteiten te verbeteren zonder dat zij in eerste instantie noodzakelijk worden aangemoedigd door online peers. Ze willen vooruitlopen op medestudenten of leeftijdsgenoten en oplossingen vinden voor problemen die ze tegenkomen bij het werken met computers en technologie. Anderen zoeken wel specifiek kennis over crimineel hacken; de grenzen tussen ethisch en onethisch computergebruik zijn soms vaag. Jongeren dwalen over fora of vergelijkbare chatrooms om bestaande threads te lezen of actief te vragen naar specifieke informatie. Het is niet eens nodig om met online peers in gesprek te gaan om vaardigheden te verbeteren: respondenten gebruiken simpelweg Google of YouTube om te leren hoe ze een DDoS-aanval kunnen uitvoeren of een SQL-injectie kunnen doen. Dergelijke informatie is toegankelijk op openbare platforms, wat de drempel om betrokken te raken bij cybercriminaliteit verlaagt. Tegenwoordig vormen deze platforms een belangrijk element in de ontwikkelingsfasen van jonge criminele hackers.

Door middel van experimenteren en trial-and-error proberen jonge hackers nieuw opgedane kennis in de praktijk uit. Op dit punt kunnen sommigen al betrokken zijn bij cybercriminaliteit, soms zonder het te beseffen. Zo kunnen jongeren in de veronderstelling zijn dat ze enkel de beveiliging van het schoolnetwerk testen. Scholen bieden in het bijzonder gelegenheid voor cybercriminaliteit omdat scholen deel uitmaken van het dagelijkse leven van jongeren en een geschikt doelwit vormen met soms een gebrek aan adequate beveiligingsmaatregelen. Hieruit blijkt dat het strafbare gedrag van de meeste jonge hackers vaak werd gedreven door nieuwsgierigheid, plezier of spanning. Ze beschouwen hacken als een persoonlijke uitdaging om hun vaardigheden te testen en worden niet per se gedreven door materiële doelen, althans niet in de vroege ontwikkelingsstadia. Andere jongeren zijn bewuster betrokken bij crimineel hacken omdat het hen of hun vrienden bepaalde voordelen oplevert. In

dergelijke gevallen veranderden respondenten bijvoorbeeld cijfers op school of hacken ze gameservers om een voordeel op tegenstanders te krijgen. Dergelijk strafbaar gedrag lijkt in de loop van de tijd te kunnen escaleren, waarbij eenvoudige vormen van hacken fungeren als opstapjes naar misdrijven met grotere financiële, organisatorische of psychologische impact.

Figuur 1. Schematische weergave ontwikkelpaden jonge hackers (Leukfeldt & Bekkers, 2026)



2.2. Risicofactoren

Een ander lijn in wetenschappelijk onderzoek naar online criminaliteit richt zich op het in kaart brengen van risicofactoren. Over het algemeen blijkt dat online criminaliteit gedeeltelijk kan worden verklaard door criminogene factoren die ook traditionele criminaliteit kunnen verklaren. Wat daarbij vooral lijkt te gelden is dat daders van financiële cybercriminaliteit meer op traditionele delictplegers lijken terwijl daders van cybercriminaliteit een unieke dadergroep vormt. Zo hadden zelf-gerapporteerde hackers een significant hogere zelfcontrole dan non-offenders en traditionele delictplegers in vragenlijstonderzoek onder Nederlandse jongeren (Bekkers et al., 2025a). Dit lijkt vooral te gelden voor daders die het delict alleen plegen (Bekkers et al., 2025b) en zou komen omdat een hoge mate van zelfcontrole jongeren beter in staat zou stellen om de kennis op te doen die nodig is voor complex delictgedrag. Het zou immers niet realistisch zijn voor iemand met een lage zelfcontrole om systematisch tijd te steken in het leren van computervaardigheden. Zo lijkt ook het volgen van een opleiding op het gebied van technologie en computers juist het risico op cybercriminaliteit te vergroten, mogelijk omdat daders daar de vaardigheden leren of met leeftijdsgenoten in aanraking komen die ook cybercriminaliteit plegen (Weulen Kranenbarg et al., 2018; Bekkers et al., 2025a,b).

Daders van financiële cybercriminaliteit werden juist gekenmerkt door traditionele risicofactoren, zoals antisociale persoonlijkheidskenmerken (Bekkers et al., 2025b). Dit komt ook terug in delictgedrag zelf, aangezien daders van financiële cybercriminaliteit vaker ook traditionele criminaliteit plegen (Bekkers & Leukfeldt, 2025). Meer technisch onderlegde daders waren juist vaker gespecialiseerd in enkel cybercrime delicten. Hierbij is overlap gevonden tussen specifieke vormen van online en offline criminaliteit, zoals een correlatie tussen winkeldiefstal en diefstal in games.

Aanvullend bewijs over de persoonlijkheidskenmerken van daders van cybercriminaliteit komt uit kwalitatief onderzoek. Zo interviewden Martineau en collega's (2024) tien criminele hackers uit Noord-Amerika. Veel respondenten gaven aan dat zij zich in hun jeugd kenmerkten als stille en verlegen kinderen, die de voorkeur gaven aan solitaire activiteiten boven sociale interacties. Zij besteedden hun tijd aan bezigheden zoals Lego, puzzels en bordspellen, en herkenden zich in een overwegend introverte persoonlijkheid, vaak gepaard gaand met angstklachten. Daarnaast lijken personen die betrokken zijn bij hacking vaker over een sterk oog voor detail te beschikken en systematisch te werk te gaan (Harvey et al., 2016), terwijl er ook aanwijzingen zijn dat hun communicatieve en sociale vaardigheden relatief minder ontwikkeld zijn (Schell & Melnychuk, 2011). Tot slot speelt moraliteit een belangrijke rol: naarmate iemand sterker gelooft dat hacken moreel verwerpelijk is, neemt de kans af dat diegene zich met hackactiviteiten bezighoudt (Hu et al., 2012, 2013; Young et al., 2007).

Naast persoonlijkheid spelen ook vrienden en kennissen een belangrijke rol, waarbij eigenlijk voor alle vormen van cybercriminaliteit wordt geobserveerd dat antisociale vrienden een risicofactor vormen. Studies uitgevoerd in onder andere Israël, de Verenigde Staten, China, Australië, en het Verenigd Koninkrijk naar hacken vinden inderdaad een positieve relatie gevonden tussen deviante leeftijdsgenoten en betrokkenheid bij hacking: jongeren met vrienden die cybercriminaliteit plegen, zijn zelf vaak ook betrokkenheid bij dat soort gedrag (Bossler & Burruss, 2011; Fox & Holt, 2021; Holt et al., 2012; Hutchings, 2013, 2014; Marcum et al., 2014).

Verder blijkt uit het onderzoek dat hoe meer tijd jongeren spenderen aan online gamen, hoe lager de kans is dat zij betrokken zijn bij cybercrime in enge zin (Bekkers et al., 2025c). Gamers leken zelfs minder vaak betrokken bij dat soort delicten dan niet-gamers. Dit wijst op een beschermend effect. Risico's zijn vooral geobserveerd voor in-game deviant gedrag, zoals stelen van tegenstanders. Het is nog de vraag in hoeverre en in welke omstandigheden dit een steppingstone is naar meer serieus delictgedrag. Gamers waren namelijk wel vaker blootgesteld aan deviante invloeden van online vrienden en hadden meer skills op het gebied van computers en technologie, wat risicofactoren kunnen zijn voor betrokkenheid bij cybercriminaliteit.

Gamingsplatformen en de sociale structuren daaromheen vormen dus een potentiële gelegenheidsstructuur voor cybercriminaliteit. Zo kunnen jongeren ook simpelweg Googelen of YouTube video's kijken over hoe ze een DDoS-aanval moeten uitvoeren (Moneva & Leukfeldt, 2024). Kennis, vaardigheden en skills op het gebied van programmeren en computers biedt vervolgens gelegenheid voor crimineel gedrag online. Een hoog niveau van computervaardigheden is bijvoorbeeld gerelateerd aan daderschap van cybercriminaliteit maar niet aan traditionele criminaliteit (Weulen-Kranenbarg et al., 2019).

3. Methode

In dit hoofdstuk beschrijven we de dataverzameling voor het huidige onderzoek. We maken daarbij onderscheid in 1) de interviews met jonge hackers en 2) de vragenlijst die is afgenomen onder de algemene populatie en onder de risicogroep.

3.1. Interviews

3.1.1. Procedure

Voor dit onderzoek zijn 17 respondenten geïnterviewd tussen april 2025 en december 2025. Om te beginnen is een informatiebrief over het onderzoek opgesteld om daarmee potentiële respondenten te kunnen informeren. Respondenten zijn benaderd via drie lijnen: een stichting dat jongeren met interesses in IT begeleidt (n=4), een Hackaton georganiseerd door de politie in Amsterdam (n=4) en scholen die IT-onderwijs aanbieden (n=8). Eén overige respondent is daarnaast benaderd op een cybersecurity conferentie. In dat eerste geval zijn respondenten aangedragen door de voorzitter van de stichting. Die voorzitter heeft de informatiebrief persoonlijk overhandigd aan jongeren en daarna met toestemming contactgegevens gedeeld met de onderzoekers. De onderzoekers hebben contact opgenomen met die respondenten per mail of per Whatsapp. Bij minderjarige respondenten is daarbij eerst contact gelegd met ouders voor toestemming. Binnen de tweede lijn zijn de onderzoekers naar een Hackaton gegaan in Amsterdam op 10 oktober 2025. Daar is contact gelegd met twee vaders die met hun kinderen aanwezig waren en is op een later tijdstip een interview gepland. Binnen de derde lijn is contact gelegd met potentiële respondenten via een “gatekeeper” die op zzp-basis lesgeeft op verschillende middelbare scholen. Op uitnodiging van die docent zijn de onderzoekers naar school gegaan om de informatiebrief te overhandigen aan studenten die vanuit interesse een keuzevak over cyberveiligheid volgde. Bij interesse hebben ouders eerst toestemming gegeven voor deelname voordat de onderzoekers het interview plande met respondenten. Alle respondenten hebben een informed consent formulier ondertekend, wat in het geval van minderjarige respondenten is gedaan door ouders. De interviews zijn met toestemming opgenomen op een versleutelde recorder en naderhand uitgewerkt tot een geanonimiseerd transcript. De opnames zijn verwijderd van de recorder en samen met de transcripten en informed consent formulieren opgeslagen op de beveiligde server van de Haagse Hogeschool.

3.1.2. Respondenten

Tabel 1 bevat een overzicht van de respondenten en diens kenmerken. De respondenten betreffen 15 jongeren (2v/13m) tussen de 9 en 22 jaar en twee vaders van respondenten die aanwezig waren bij het interview. We verwijzen naar deze respondenten als R1, R2, etc. De respondenten zijn geselecteerd op basis van zelf-gerapporteerde interesse en affiniteit met computers en informatietechnologie.

Sommigen hebben daarbij een voorkeur voor hardware terwijl anderen tijd spenderen aan programmeren of design. Er is verder niet specifiek geselecteerd op delictgedrag, maar een aantal respondenten gaven aan wel ooit de wet te hebben overtreden. De gesprekken zijn online gevoerd via Teams (n=11) of fysiek (n=6), in dat laatste geval meestal op school van respondent. De interviews duurde tussen de 25 en 90 minuten.

Tabel 1

Overzicht respondenten

Code	**Leeftijd**	**Opleiding of werk in IT**	**Vaardigheden en interesses**	**Duur interview**	**Locatie**
R01	20	X	Werkzaam als software developer	1:12	Teams
R02	18	X	Opleiding tot applicatiebeheerder	47 minuten	Teams
R03	14	X	Ethisch hacker (vrijwilliger)	36 minuten	Teams
R04	20	X	Werkzaam als software developer	1:16	Teams
R05	16	-	Programmeren en AI	56 minuten	Teams
R06	18	-	Cybersecurity	47 minuten	Teams
R07	15	X	Opleiding in media, vormgeving en ICT	32 minuten	School
R08	15	-	Grafische vormgeving	28 minuten	School
R09	9	-	Hacking	35 minuten	Teams (samen met vader R10)
R11	12	-	Hardware	50 minuten	Restaurant (samen met vader R12)
R13	19	X	Werkzaam als ethisch hacker	1:14	Teams
R14	17	X	Opleiding medewerker ICT	30 minuten	School

R15	16	X	Opleiding medewerker ICT	27 minuten	School
R16	17	X	Opleiding medewerker ICT	22 minuten	School
R17[1]	22	X	Opleiding medeweker ICT	55 minuten	School

3.1.3. Analyse

Data is geanalyseerd in Atlas.Ti. Om de data systematisch te organiseren en interpreteren, hebben we de stappen gevolgd zoals beschreven door Clarke en Braun (2014) en Vaismoradi et al. (2013). Thematische analyse biedt een framework om kwalitatieve data te verkennen en verhoogt de betrouwbaarheid van inzichten verkregen uit interviews, etnografische studies en soortgelijk onderzoek. Het doel van de analyse was om zicht te krijgen op de mechanismen, processen en factoren die een rol spelen bij online gedrag van jonge hackers en de ontwikkeling van vaardigheden op het gebied van computers en technologie. Door de data te coderen en overlappende codes te groeperen zijn zes overkoepelende thema's geïdentificeerd: 1) vroege ervaringen en computer preoccupatie, 2) leren van vaardigheden, 3) ouderlijk toezicht en transparantie, 4) ethiek en morele grenzen, 5) risicoperceptie en 6) sociaal netwerk.

3.2. Vragenlijst

We hebben een vragenlijst afgenomen onder jongeren uit de algemene populatie (de controlegroep) en onder jongeren met affiniteit en interesse voor computers en technologie (de risicogroep) om die twee groepen te kunnen vergelijken op individuele kenmerken. In deze sectie beschrijven we hoe de dataverzameling heeft plaatsgevonden, afzonderlijk voor de controlegroep en de risicogroep.

3.2.1. Procedure

Controlegroep

De controlegroep heeft betrekking op jongeren tussen de 16 en 25 jaar die een vertegenwoordig zijn van de algemene populatie. Ze zijn geworven via I&O Ipsos, een onderzoeksbureau in Nederland dat een jongerenpanel beheert. De dataverzameling vond plaats in augustus 2023. In totaal zijn via het panel 3.419 Nederlandse jongeren tussen de 16 en 25 jaar per e-mail geïnformeerd over de studie,

[1] Deze respondent is opgepakt door de politie vanwege betrokkenheid bij cybercriminaliteit en vormt daarmee een uitzondering op de overige respondenten. We hebben ervoor gekozen dit perspectief ook mee te nemen in het onderzoek.

inclusief informatie over het onderzoek en het doel ervan, en een link naar een online vragenlijst. De vragenlijst begon met een toestemmingsformulier, waarin werd uitgelegd wat het doel van het onderzoek is en op welke manier de gegevens zouden worden verwerkt. De panelleden ontvingen na één week een herinnering om deel te nemen en nog een herinnering na twee weken. Deelnemers aan het onderzoek ontvingen punten van het onderzoeksbureau, die zij konden omzetten in financiële beloningen of producten. Respondenten konden op elk moment de vragenlijst pauzeren en later hervatten, wat resulteerde in invultijden variërend van twee minuten tot 31.257 minuten (M=1291,85; SD=4203,42; Mdn=20). Het onderzoeksbureau verzamelde en bewaarde de gegevens in overeenstemming met de Nederlandse regelgeving omtrent data, en verstrekte de onderzoekers een geanonimiseerde dataset zonder persoonlijke identificeerbare informatie.

Risicogroep

Een deel van dezelfde vragenlijst is vervolgens in precies dezelfde vorm ook afgenomen onder een risicogroep. Daarbij zijn ook een aantal aanvullende factoren gemeten die nog geen onderdeel waren van de eerdere versie van de vragenlijst die is afgenomen onder de controlegroep. De risicogroep heeft betrekking op jongeren van 16 tot 25 jaar die affiniteit hebben met en interesse hebben in computers en technologie en vanuit die hoedanigheid risico lopen om cybercriminaliteit te plegen. In eerste instantie zijn jongeren geworven die actief zijn op Discord in een groep over Reb00t_camp (n=6). Dit betreffen jongeren met interesses en affiniteit voor IT en daarmee dus risico lopen op betrokkenheid bij hacking. De onderzoekers zijn door de beheerders van de groep toegelaten en hebben zichzelf en het onderzoek daar geïntroduceerd in de algemene groep chat in juli 2025. Op dat moment zaten er meer dan 300 leden in de groep. Via een link zijn deelnemers op vrijwillige basis doorverwezen naar de online vragenlijst. De vragenlijst begon met een toestemmingsformulier waarbij het doel en de procedure van het onderzoek nogmaals is toegelicht. De onderzoekers hebben in totaal twee reminders gestuurd in een periode van vier weken. Op deze manier hebben in totaal zes jongeren de vragenlijst ingevuld.

Respondenten in de risicogroep zijn verder geworven via IT-gerelateerd onderwijs (n=74). Meer specifiek betreffen dit jongeren van middelbare scholen die deelnamen aan een vak over IT en studenten van de opleiding Information Security Management (ISM) aan de Haagse Hogeschool. Het uitgangspunt is dat deze jongeren risico lopen om betrokken te raken bij cybercriminaliteit. Om de data te verzamelen zijn de onderzoekers fysiek naar de onderwijslocatie gegaan waar studenten op dat moment les kregen. Daar is het onderzoek geïntroduceerd en zijn studenten in de gelegenheid gesteld om via een QR-code de vragenlijst in te vullen op vrijwillige basis. Er zijn vier verschillende dataverzamelingsmomenten geweest: 3 november 2025, 26 november 2025, 28 november 2025 en 24 februari 2026.

3.2.2. Respondenten

Controlegroep

Na de twee herinneringen hebben in totaal 1.240 unieke personen in de leeftijd van 16 tot 25 jaar deelgenomen aan de vragenlijst, wat neerkomt op een responspercentage van 36,3%. We hebben zogenaamde “speeders” eruit gefilterd, dat wil zeggen respondenten die de vragenlijst in minder dan vijf minuten invulden (n=17). Daardoor bleven er 1,223 respondenten over. In deze steekproef waren er meer vrouwen (n=837; 67,9%) dan mannen (n=396; 32,1%), terwijl in de bredere jeugdbevolking (16 tot 25 jaar) 50,8% mannelijk en 49,2% vrouwelijk is (CBS, 2023b), wat betekent dat vrouwen in onze steekproef oververtegenwoordigd waren. Hetzelfde geldt voor opleidingsniveau, aangezien de meerderheid van de respondenten momenteel een studie volgde of had afgerond aan een universiteit of hoger beroepsonderwijs in Nederland (n=805; 65,3%), in tegenstelling tot de bredere Nederlandse bevolking van 15- tot 25-jarigen, waar ongeveer 14% een hoog opleidingsniveau heeft (CBS, 2023c).

Deze sample is vervolgens gebruikt om “healthy controls” te selecteren, ofwel de controlegroep waarmee de risicogroep wordt vergeleken. Dat wil zeggen dat deze groep juist niet voldoet aan het criterium waarop de risicogroep is geselecteerd, namelijk interesse en affiniteit voor computers en technologie. Daarom zijn binnen de sample van 1.223 respondenten eerst alle jongeren eruit gefilterd die 1) een opleiding volgen of werk hebben op het gebied van technologie en computers en 2) jongeren die ooit betrokken zijn geweest bij een vorm van cybercriminaliteit. Dat betreffen in totaal 161 personen. Daarmee bleef een steekproef van 1.079 respondenten over. Vervolgens is uit deze groep met behulp van SPSS een willekeurige steekproef getrokken van 80 respondenten om het aantal gelijk te trekken met de risicogroep. Binnen die controlegroep waren er 63 vrouwen (78.8%) en 17 mannen (21.3%). Wat betreft opleidingsniveau volgde iets meer dan de helft een opleiding afgerond aan een universiteit of hoger beroepsonderwijs in Nederland en was daarmee hoogopgeleid (n=48; 60.1%). Wat betreft leeftijd waren 10 respondenten in de categorie 16-17 jaar (12.5%), 26 respondenten in de categorie 17-20 jaar (32.5%), 17 respondenten in de categorie 21-23 jaar (21.3%) en 27 respondenten in de categorie 24-25 jaar (33.8%) De verhoudingen van de demografische kenmerken zijn ongeveer gelijk aan de bredere sample van de algemene populatie.

Risicogroep

In totaal hebben 80 respondenten de vragenlijst ingevuld. Het overgrote merendeel daarvan betroffen mannen (n=72; 90%) en bijna alle respondenten waren nog thuiswonend bij ouders of verzorgers (n=73; 91.3%). Dat betekent dat de controlegroep vooral bestond uit vrouwen en de risicogroep vooral uit mannen. De respondenten waren als volgt verdeeld in de verschillende leeftijdscategorieën: 13 respondenten waren 16 of 17 jaar (16.3%), 27 respondenten waren 18 of 19 jaar (33.8%), 29 respondenten waren 20 of 21 jaar (36.3%), 9 respondenten waren 22 of 23 jaar (11.3%) en 2

respondenten waren 24 of 25 jaar (2.5%). Leeftijd is op een andere manier gemeten in de controlegroep maar over het algemeen lijken respondenten in de risicogroep jonger. Verder volgde drie respondenten een opleiding op basisonderwijs (3.3%), twee respondenten op vmbo of mbo-1 (2.2%), twee respondenten op havo/vwo-onderbouw (2.2%), 27 respondenten op mbo-2, mbo-3 of mbo-4 (30%), 10 respondenten op havo/vwo-bovenbouw (11.1%), 42 respondenten op hbo/wo-bachelor (46.7%) en één respondent op hbo/wo-master (1.1%). Dat betekent dat 43 respondent hoogopgeleid waren (47.8%), iets minder dan bij de controlegroep.

3.2.3. Meetinstrumenten

De online vragenlijst bestond uit gevalideerde meetinstrumenten en items afkomstig uit bestaande literatuur. Het doel van de vragenlijst was het in kaart brengen van online en offline delictgedrag en het screenen op de belangrijkste risicofactoren voor crimineel gedrag. De vragenlijst is eerst afgenomen onder de algemene populatie jongeren via het panelbureau. Later zijn delen van die vragenlijst in precies dezelfde vorm afgenomen onder de risicogroep, waardoor we de data kunnen vergelijken. Over het algemeen zijn constructen berekend als een somscore van de corresponderende items.

Delictgedrag

Respondenten is gevraagd of ze ooit betrokken zijn geweest bij de volgende vormen van cybercriminaliteit: afkijken/raden van wachtwoorden, hacken met technische middelen, DoS/DDoS aanvallen, website defacement en malware. Dit onderzoek richt zich op deze daders. Daarnaast is ook gevraagd naar betrokkenheid bij financiële cybercrime, namelijk virtueel diefstal, phishing en online identiteitsfraude. Ten slotte is offline delictgedrag in kaart gebracht. Meer specifiek betreffen dat graffiti, openbare geweldpleging, winkeldiefstal, fietsendiefstal, vandalisme en brandstichting.

Risicofactoren

***Lage zelfcontrole*.** De Brief Self-Control Scale (BSCS; Tangney et al., 2004) meet algemene zelfcontrole. Op een 5-puntsschaal, variërend van ‘1 = sterk mee oneens tot ‘5 = sterk mee eens’, gaven respondenten aan in hoeverre 13 stellingen op hen van toepassing waren (bijv. “Ik ben lui”). De BSCS heeft eerder een Cronbach’s alpha van .85 of hoger laten zien in steekproeven van delinquenten en scholierende jongeren (Malouf et al., 2014; Pechorro et al., 2021). Items werden zodanig gecodeerd dat een hogere score wees op lagere niveaus van zelfcontrole.

***Delinquente vrienden*.** Delinquent gedrag van leeftijdsgenoten werd gemeten met de Criminal Attitudes and Associates (MCAA)-schaal (Mills et al., 2002). Deze schaal liet een zeer hoge betrouwbaarheid zien in een steekproef van jongeren ($\alpha > .90$; O’Hagan et al., 2019). Eerst werd

respondenten gevraagd om na te denken over de vier belangrijkste personen in hun leven, waarna zij voor elk van deze personen vier stellingen beantwoordden met ‘ja’ of ‘nee’ (bijv. “Heeft persoon #1 ooit in de gevangenis gezeten?”). Het tweede deel van de MCAA bestaat uit 46 items (‘eens’ of ‘oneens’), verdeeld over vier subschalen, maar voor de doeleinden van deze studie gebruikten wij acht items die specifiek betrekking hadden op het domein van criminele vrienden (bijv. “Ik voel me altijd welkom in de buurt van criminele vrienden”). Hoe hoger de score, hoe meer werd geacht dat respondenten werden blootgesteld aan delinquent gedrag van leeftijdsgenoten.

Antisociale attitudes. Deze variabele is toegevoegd aan de vragenlijst voor de risicogroep en was dus geen onderdeel van de meting onder de controlegroep. Antisociale attitudes zijn gemeten met vijf items, waaronder “Hoe verkeerd is het volgens jou om iets te stelen van iemand anders?”. Respondenten konden antwoord geven op een 4-puntschaal, variërend van ‘1 = helemaal niet verkeerd’ tot ‘5 = heel verkeerd’. Hoe hoger de score, hoe meer antisociale attitudes aanwezig zijn.

Offline ouderlijk toezicht. Ook deze variabele was alleen onderdeel van de vragenlijst die onder de risicogroep is afgenomen. De mate waarin ouders zicht hebben op de offline activiteiten van respondenten is gemeten met twee items: “Hoe vaak weten je ouders of verzorgers waar je bent gedurende de dag?” en “Hoe vaak weten je ouders of verzorgers met wie je bent wanneer je weg bent van huis?”. Antwoord was mogelijk op een 4-puntschaal, van ‘1 = nooit’ tot ‘4 = vaak’. Deze items zijn afkomstig van Kerr en Stattin (2000).

Schoolfactoren. De vragenlijst bevatte twee dichotoom beantwoordde vragen over schoolbetrokkenheid: “Ben je ooit geschorst van school?” en “Ben je ooit blijven zitten?”. Deze items zijn afkomstig van Fox en Holt (2021) en de YDS (Van der Laan & Beerthuizen, 2021; Tollenaar et al., 2024). Daarnaast vroegen wij respondenten of zij momenteel of in het verleden in IT hebben gewerkt of een opleiding in IT hebben gevolgd.

Familiefactoren. De vragenlijst bevatte twee dichotoom beantwoordde items die betrekking hadden op de gezinssituatie van de respondent (bijv. “Heb je ooit een ernstig conflict of fysieke ruzie tussen je ouders gezien?”). Deze items zijn afkomstig van de YDS (Van der Laan & Beerthuizen, 2021; Tollenaar et al., 2024) en Fox en Holt (2021).

Online deviante invloeden. Daarnaast vroegen we respondenten specifiek naar online deviante invloeden van online leeftijdsgenoten met drie items gebaseerd op Yoon (2011), waaronder: “Mijn online vrienden en kennissen zouden op mij neerkijken als ik cybercriminaliteit pleeg.” Het construct is zo gecodeerd dat hogere scores duidden op een grotere blootstelling aan online leeftijdsgenoten die cybercriminaliteit ondersteunen of aanmoedigen.

Online disinhibitie. Dit construct werd gemeten met drie items van Kerstens en Jansen (2016), zoals "Het is makkelijker om mezelf te uiten op internet dan in het echte leven". Antwoordopties liepen op een 7-punt Likertschaal van '1 = helemaal mee oneens' tot '7 = helemaal mee eens'. De oorspronkelijke studie bestond uit zes items en liet een goede betrouwbaarheid zien onder jongeren (α = 0,85; Kerstens & Jansen, 2016), maar vanwege de lengte van de vragenlijst hebben wij slechts drie items gebruikt. Een hogere score correspondeerde met hogere niveaus van online disinhibitie.

Online routineactiviteiten. Respondenten werd gevraagd hoeveel tijd zij in een gemiddelde week besteden aan bepaalde activiteiten op internet (Weulen Kranenbarg et al., 2019), namelijk gamen, programmeren en online communiceren. Items werden beantwoord op een 5-puntsschaal: '1 = 0 uur' tot '5 = 21 uur of meer'.

Online ouderlijk toezicht. Met drie items op een 5-punt Likertschaal ('1 = sterk mee oneens' tot '5 = sterk mee eens') afkomstig uit Weulen Kranenbarg et al. (2022) en één item uit de ISRD4 (Marshall et al., 2022) vroegen wij respondenten naar de mate waarin hun ouders toezicht houden op hun activiteiten op internet en op computers, bijvoorbeeld: "Mijn ouders weten welke websites en apps ik gebruik." Hoe hoger de score, hoe meer respondenten ouderlijk toezicht op online activiteiten ervoeren.

IT-skills. We hebben het subjectieve niveau van IT-vaardigheden van de respondenten gemeten met één item, afkomstig van Weulen Kranenbarg et al. (2019) en Holt et al. (2012). Dit betreft een ordinale maat, een zogenoemde Guttman-schaal, waarin respondenten aangeven welke stelling het beste op hen van toepassing is: '1 = Ik hou niet van het gebruik van computers en gebruik ze alleen als dat echt nodig is.' tot '5 = Ik kan verschillende programmeertalen gebruiken en ben in staat programmeerfouten te ontdekken'. Hoewel deze maat gebaseerd is op zelfrapportage, bleek in eerder onderzoek dat deze schaal sterk correleert met objectieve metingen van IT-vaardigheden (Weulen Kranenbarg et al., 2019).

3.2.4. Analyse

Alle data is geanalyseerd in SPSS versie 28. Het doel van de analyse was om meer zicht te krijgen op de individuele kenmerken van jongeren die risico lopen om betrokken te raken bij cybercriminaliteit. De analyse bestond uit twee delen. Het eerste deel van de analyse had betrekking op het vergelijken van de risicogroep met de controlegroep om factoren te identificeren die deze twee groepen kunnen onderscheiden. Daarvoor zijn uit de hele dataset van jongeren uit de algemene populatie 80 willekeurige respondenten geselecteerd die zijn aan te merken als "healthy controls". Het selectiecriterium daarbij was dat deze respondenten geen IT-opleiding/IT-werk hebben en niet eerder

betrokken zijn geweest bij cybercriminaliteit, om daarmee te fungeren als controlegroep. Deze 80 respondenten uit de algemene populatie zijn samengevoegd in het databestand met de 80 respondenten uit de risicopopulatie. Vervolgens zijn de gemiddelde scores van deze twee groepen op de risicofactoren die op continue schaal zijn gemeten met elkaar vergeleken met behulp van one-way Analysis of Variance (ANOVA). Voor dichotome variabelen is gebruik gemaakt van chi-kwadraattoetsen. Het tweede deel van de analyse had betrekking op het vergelijken van daders van cybercriminaliteit in de risicogroep met niet-daders in de risicogroep. Dit geeft meer inzicht in de factoren die ervoor kunnen zorgen dat iemand wel of geen delicten pleegt. Het gaat daarbij om technische vormen van hacking, DoS/DDoS aanvallen, website defacement en het verspreiden van malware. Ook hierbij is gebruik gemaakt van ANOVA voor continue variabelen en chi-kwadraattoets voor dichotome variabelen. We rapporteren eta-kwadraat (η^2) als een maat voor effectgrootte, waarbij waardes van 0.10, 0.25 en 0.40 corresponderen met kleine, middelgrote en grote effecten.

4. Resultaten

In dit hoofdstuk beschrijven we de resultaten van het onderzoek. Ook hierbij maken we een onderscheid tussen de interviews en de vragenlijst.

4.1. Interviews

4.1.1. Vroege ervaringen

De respondenten rapporteren over het algemeen vroege ervaringen met computers en technologie, vaak in de context van gaming en hardware. “Ik kon eigenlijk al eerder typen dan dat ik kon schrijven. Dus ik heb altijd al liefde voor computers gehad”, zo beschrijft R01. De respondent vertelt dat leraren naar hem toe kwamen om problemen met een telefoon, laptop of printer op te lossen. R03 was toen hij negen jaar was al bezig met het testen van broncodes. R17 haalde toen hij 10 jaar was computers uit elkaar, en R13 was al op de basisschool aan het programmeren in Python. Ook R11 was acht jaar toen hij voor de eerste keer een computer heeft gebouwd. De vader van deze respondent (R12) legt uit dat R11 sinds hij kon lopen geïnteresseerd was in hoe dingen werken, zoals een draaimolen. “Gewoon even kijken, hoe zit dat in elkaar, hoe alles moet draaien of tandwielen of wat dan ook, daar was hij eigenlijk al mee bezig vanaf hij klein was.” Sommige respondenten zijn door ouders geïntroduceerd in de wereld van IT (R04, R06, R11, R15, R16). R16 heeft via de vriend van zijn moeder een knutsel-PC gekregen, wat zijn interesses verder heeft aangewakkerd. “Mijn vader werkt zelf ook al in de ICT. Ja. Dus dat is ook een beetje waar ik mijn ICT vandaan heb”, zo stelt R15. Ook R04 is ooit in aanraking gekomen met programmeren via zijn vader en heeft dat toegepast in de context van het bouwen van games.

> R15: Als ik thuiskwam, kwam ik dan zijn werkkamer binnen en dan zag ik allemaal code op zijn monitor staan. Allemaal dingen in een soort website waarvan ik op dat moment nog niks van wist. Van wat het allemaal precies inhoudt en wat het doet. Maar het leek me wel interessant om het allemaal te leren.

> R05: Qua procenten. Ik denk dat het op dit moment zo'n één vierde van de dag is. En vroeger was het denk ik wel echt drie/vierde van de dag. Echt grotendeels ja. Nu ben ik minder bezig met gamen.

> R04: En het begon in eerste instantie gewoon met dat ik een server wilde maken een Minecraft server waar mensen dan dingen konden doen. Ik wilde daar dingen aan toevoegen waarvan ik niet weet hoe dat moest. En om dat wel te doen moest je programmeren.

Sommige respondenten hebben wel affiniteit met IT maar bevinden zich nog in een vroeg stadium en hebben nog weinig tijd geïnvesteerd in het opdoen van vaardigheden (R06, R07, R08, R09, R16). Zo heeft R06 wel eens filmpjes gekeken over programmeren maar dat nooit zelf geprobeerd. R07 en R08 geven ook aan dat ze technische aspecten zoals programmeren nog te ingewikkeld vinden om zelf te leren. R16 vind programmeren ook ingewikkeld, maar heeft daar wel een boek over gelezen.

Opvallend is dat interesses op dit gebied zich veelal manifesteren in de context van Roblox[2]. Vrijwel alle respondenten waren in het verleden of nog steeds actief op Roblox en dat lijkt interesse in computers en technologie ook verder aan te wakkeren, mogelijk omdat de aard van Roblox goed aansluit op nieuwsgierigheid die aanwezig is. “Dat was meestal doordat Roblox echt zo interessant leek voor mij. Dan was ik van: nou weet je wat, ik ga het gewoon even uitproberen. Sindsdien vind ik het helemaal geweldig”, zo benoemt R07. R05 was vanaf zeven jaar veel bezig met gamen en dat heeft zich ontwikkeld tot het maken van Mincecraft plugins en bouwen van websites voor Roblox.

> R02: Ja ik hou van videogames. Ik wou eigenlijk programmeur worden voor videogames te maken. Toen had ik dat geprobeerd, maar daar vond ik niet zoveel aan. Toen ben ik maar gewoon aan oude computers gaan kopen en dat gaan fixen.
>
> R06: En toen ik in de zevende klas was, wilde ik dan echt mijn spelletjes programmeren. En daardoor ben ik begonnen beetje programmeren te leren,

Duidelijk is dat respondenten gedreven zijn vanuit intrinsieke motivatie. Ze willen graag mensen helpen en met computers bezig zijn in plaats van geld verdienen. R04 werd benaderd door iemand die zijn video’s over programmeren had gekeken met de vraag om een tool te maken waarmee mensen makkelijk advertenties op Marktplaats kunnen ophalen. Dat heeft hij gratis gedaan voor die persoon. Ook respondenten die in het verleden wel eens een delict hebben gepleegd, zoals R17, geven aan dat ze het zagen als een uitdaging en vooral nieuwsgierig waren. Deze respondent is opgepakt voor het hacken van een database: “Gewoon proberen voor de leuk. Gewoon die simpele dingetjes die af en toe wel eens probeert te doen.” De politie heeft nog onderzocht of hij de data had gedeeld maar dat was niet zo. “Dat was ook al verwijderd toen ze binnen stonden. Had het al niet meer. Ik had er geen interesse in. Nee, ik was gewoon benieuwd hoe groot het was.”

> R01: Nee, ik heb eigenlijk nooit over financiële plaatje nagedacht. Hetzelfde ook met die Minecraft servers. Dingen onderhouden, repareren. Ik heb nooit aan de financiële kant

[2] Een platform waarbij gebruikers games kunnen programmeren en games kunnen spelen die door andere gebruikers zijn gemaakt.

gedacht. Al blij dat ik mensen kan helpen. Blij dat ik met mijn kennis anderen kan helpen om verder te komen.

R04: Ik heb nu een website gemaakt waarvan je dan kan doneren als ik je heb geholpen. Ja, maar dat wordt eigenlijk ook nooit gebruikt. Aan de andere kant, ik vind het ook niet erg, maar voor kleine dingen vind ik het meer moeite om er geld voor te vragen dan om het gewoon te doen.

R03: Nou ja, ik ben vooral eigenlijk overal naar nieuwsgierig. Stel voor je hebt iets gekraakt. Als ik bijvoorbeeld nu voor school een website platleg en ik kan het melden, of bij een bepaalde bounty ik het meld en een vrij grote beloning krijg. Dan is het wel zo van oh ik heb dit gedaan.

4.1.2. Leren van vaardigheden

Respondenten lijken op verschillende manieren kennis op te doen over IT: 1) YouTube, 2) op forums zoals Discord, Reddit en StockOverflow, 3) via vrienden, 4) met behulp van AI en 5) op school. YouTube wordt daarbij het vaakst genoemd als bron van kennis. R15 heeft bijvoorbeeld veel video's gekeken over hardware: "Ik was een keer benieuwd naar hoe je een pc moet bouwen. En toen dacht ik van nou zullen we kijken of er YouTube video's van zijn. En zo kwam ik bij echt een heleboel video's." R13 herkent zicht daarin. De respondent beschrijft dat plekken zoals YouTube de enige manier zijn om programmeren en hacken te leren, waar veel tutorials te vinden zijn. R04 maakte zelf ook tutorials op YouTube, en R11 geeft aan een specifieke YouTuber te volgen die filmpjes maakt over Python.

R03: Toen ik negen was, broncodes testen, dat soort dingen een beetje. Dus ik had allemaal filmpjes uitgezocht en toen wist ik dat een beetje. En toen ben ik dus eigenlijk steeds verder gaan leren.

Naast YouTube noemen respondenten ook verschillende forums en andere communicatieplatformen waarop zij actief zijn, vooral Discord. "Als je me op Discord een berichtje stuurt en ik slaap niet, dan reageer ik heel snel", zo zegt R04. Er zijn volgens R05 honderden discussiegroepen op Discord die draaien om computers, technologie en gaming. Volgens R16 gaat dit vaak wel over vrij gespecialiseerde en technisch complexe onderwerpen, bijvoorbeeld over Python. R13 gebruikte Discord ook om specifieke programmeertalen te leren, maar wel alleen als de respondent er zelf niet uitkwam. Deze respondent is actief in groepen over legaal hacken. R02 is verder actief op Reddit. De kanalen op dat platform die draaien om computers zijn volgens de respondent vooral bedoeld voor cybersecurity experts en daar leer je dus vooral over "white hat hacking". StackOverflow en Try Hack

Me worden ook genoemd. Die eerste lijkt op Reddit en is bedoeld voor technisch onderlegde mensen (R01). Op Try Hack Me kunnen gebruikers oefenen met legaal hacken en wordt in stappen uitgelegd hoe en waarom dat zo werkt (R13).

Respondenten benoemen verder dat vrienden of kennissen een belangrijke bron zijn van kennis. “Vooral als je fysiek samenkomt kan je echt wat van elkaar leren”, zo beschrijft R13. Deze respondent is ethisch hacker op een relatief hoog niveau. Hij kent verschillende mensen in de hackerswereld die goed zijn in bepaalde onderwerpen, zoals specifieke exploits, en daarmee helpen ze elkaar. Ook R05 stelt dat hij iemand in de vriendengroep heeft die beter is in programmeren dan hij zelf: “Van hem leer ik weer nieuwe dingen. En hij leert ook weer nieuwe dingen van mij.” R15 herkent zich daarin: “Er zijn niet zo heel veel in de vrienden die echt iets met ICT doen, maar wel een paar. En dan kan ik af en toe aan hun vragen van hey, weet jij hoe dat zit?”. Ook ouders kunnen daarbij optreden als een mentor, zoals bij R11 het geval is:

> R12 (vader van R11): .. toen zei hij mag ik mijn eigen computer samenstellen, toen zei ik ja is goed maar je zet hem wel zelf in elkaar. Als hij er niet helemaal uitkwam was het wel even met papa bellen, en soms wist ik het zelf ook niet en moest ik het even opzoeken. Ik vertel wel wat ik doe zodat hij daar ook van kan leren.”

> R13: Voor de rest van mijn sociale netwerk is het heel veel hackers vooral. Van de challenge the cyber organisatie waar ik veel mee spreek. Dus ja, een redelijk hoog niveau hackers die er heel veel mee bezig zijn. Die zijn ook sociaal een stuk actiever met andere hackers. En dat is ook ja, daar kan je goed wat van leren. Gewoon over het een en ander hebben is altijd leuk om samen te komen en een beetje te hacken of dat soort dingetjes.

Respondenten investeren dus vooral in het opdoen van algemene vaardigheden en zijn niet zozeer bezig met illegale toepassingen van hacken. Ze willen bijvoorbeeld meer weten over gamen, over programmeren of over hardware. Het gebrek aan blootstelling aan omgevingen om het Internet die draaien om het leren van illegaal hacken lijkt iets waarmee deze respondenten zich van criminele hackers onderscheiden. Volgens R01 zou je specifiek moeten zoeken naar informatie over illegaal hacken en naar personen die je daarbij zouden kunnen helpen om terecht te komen in dat soort omgevingen.

Echter gebruiken sommige respondenten informatiebronnen ook in de context van illegaal hacken. Zo heeft R15 wel eens gezocht naar video’s over gamen en kwam op die manier terecht bij video’s over cheaten en hacken in games. R01 was vroeger ook wel eens actief op chatrooms die draaien om crimineel hacken. Het is volgens R01 makkelijk om in contact te komen met illegale hackers: “Negen

van de tien keer als je op die dingen gaat zoeken, vinden ze jou wel." Deze respondent heeft ook wel eens het wifinetwerk van school gehackt.

> R01: Je kan het niet direct vinden, maar als je echt specifiek gaat zoeken dan kom je ook bepaalde gebruikers tegen. Ja en die zullen jou dan helpen van hey, wij zagen of ik zag dat je dat zocht. Heb je hulp nodig en dat soort dingen?

R02 is vroeger via een link op 4chan terecht gekomen op een crimineel hackforum, die later ook offline is gehaald door de FBI: "Ik weet dat het niet mag, maar het was best wel interessant eigenlijk. Want je zag het vanaf een kant waar je normaal niet zo snel ziet en waar je normaal ook niet snel in komt". Juist ook op die manier heeft de respondent geleerd over scripts, exploits en programmeren. Hij heeft daar wat meegelezen over bijvoorbeeld het maken van exploits en heeft die kennis later gebruikt om zijn schoolnetwerk te hacken. Eenmaal in dit soort omgevingen "blijft het zo door pingpongen totdat je uiteindelijk op één van die chatrooms terecht komt waar ze dan praten over bepaalde [strafbare] dingen", aldus respondent R02.

Ook R05 is via-via terecht gekomen in de wereld van cheaten en hacken. Deze respondent was een paar jaar geleden betrokken bij het maken en verkopen van scripts voor cheats. "Ik had destijds een vriend die deed het al een tijdje. Ik was een jaartje of elf ofzo en door hem ben ik het een beetje gaan leren", zo stelt de respondent. Hij is dus geïntroduceerd in de wereld van cheaten via iemand die hij kent van Minecraft. Hij werd zelf benaderd met de vraag om scripts voor cheating te maken.

> R15: Ja, ik heb wel eens video's gezien over hoe dat hacken dan in elkaar zit, maar zelf heb ik voor het meeste eigenlijk gewoon een beetje gedacht van oh, nou die video's…. Interessant. Nu weet ik hoe dat zou moeten. Maar ja ik pas het niet zelf toe.

Het leren van vaardigheden gaat hand-in-hand met experimenteren in de praktijk. "Gewoon doen en kijken waar het schip strandt", zoals R01 beschrijft. Respondenten handelen immers veelal uit nieuwsgierigheid, waarbij ze soms grenzen overgaan. Zo hebben R02 en R03 wel eens het schoolnetwerk gehackt. R09 is pas negen jaar oud maar benoemt een situatie waarbij ze de tekst in haar spellingtoets kon veranderen: "Ik heb gewoon een keer dubbel geklikt en toen kon ik gewoon zelf intypen wat ik wou intypen." Dit weerspiegelt de nieuwsgierige en verkennende aard van het gedrag van deze jongeren. Ook R12, de vader van R11, herkent zich daarin: "Maar eigenlijk gaat dan vanzelf bij hem. Hij zoekt het gewoon uit. Als hij het wil weten dan gaat hij door tot hij weet hoe het gaat. Ja, zelf ook een beetje experimenteren, gewoon uit eigen kennis."

> R04: Gewoon een beetje experimenteren denk ik. Gewoon om te kijken. Het is niet eens echt een uitdaging denk ik, maar gewoon om te kijken. Want ik zat dan thuis even op de computer. Ja, dan kijk je: werkt het op school hetzelfde bijvoorbeeld?
>
> R05: Ik leerde vooral door te kijken naar andere mensen en hoe hun het deden en dan ging ik het een beetje nadoen en uiteindelijk leer je dan dus hoe je iets moet doen. En dan wou ik bijvoorbeeld iets specifieks bereiken, dan zocht ik dat op en dan kijk ik hoe het moest.

Wat voor R13 belangrijk is geweest is dat hij heeft kunnen experimenteren met vaardigheden binnen de context van websites zoals Try Hack Me. Die geven toestemming om in hun systemen te hacken en leggen uit hoe dat moet. “Ja, en dan kom je eigenlijk direct op redelijk hoog niveau.” Volgens deze respondent lopen vooral jongeren risico op het plegen van cybercriminaliteit die nog op een laag vaardigheidsniveau zitten, wat dus voorkomen kan worden door jongeren binnen een gecontroleerde setting vaardigheden te verhogen.

4.1.3. Ouderlijk toezicht en transparantie

Een centraal thema in de interviews is de rol van ouders en openheid over de online activiteiten van respondenten. Een aantal respondenten geeft aan dat ze het goed kunnen hebben met ouders over wat ze leuk vinden om te doen met computers, zoals programmeren en spellen bouwen in Roblox, en laten dat ook graag zien. “Ik vertel dat gewoon tijdens het avondeten, omdat ik het ook cool vond. Als ik iets had gemaakt, dan wil ik dat ook laten zien”, zoals R04 beschrijft. Deze respondent werd aangespoord door zijn ouders om te vertellen over Minecraft en wat hij had gebouwd, dan mocht hij langer op de computer. R10 is de vader van R09 en herkent het belang van een open en transparant gesprek. Bij het ontbijt en het avondeten bespreken ze thuis hoe dag is verlopen, wat ook kan gaan over bijvoorbeeld Roblox. De ouders van R03 wisten ook wat hij deed online: “Het is niet zo dat ze mijn browser helemaal gingen nachecken. Ik heb ook geen regels daarover of zoiets, maar het was wel zo van als ik iets had gedaan, dan vertelde ik gewoon wat ik had gedaan.”

Het is daarbij belangrijk dat ouders vanuit verbinding handelen en dat er balans is tussen toezicht en monitoring enerzijds en vertrouwen en interesse anderzijds. R03 had bijvoorbeeld ingelogd op het account van zijn docent in groep acht van de basisschool. Dat vertelde hij aan zijn ouders omdat hij daar trots op was. Zijn ouders hebben toen duidelijk gemaakt dat het niet mag en dat hij dat moest melden bij de school. Zo heeft respondent geleerd over grenzen en ethisch gedrag. R01 heeft ook wel eens het computernetwerk gehackt en zo zijn cijfers van wiskunde aangepast omdat hij anders niet over zou gaan. De school heeft dat ontdekt. De respondent benoemt dat zijn ouders erg waren geschrokken en hij twee maanden de computer niet meer mocht gebruiken. Hij heeft het vertrouwen weer moeten opbouwen, en sindsdien weten zijn ouders ook meer over wat hij doet op het gebied van

hacking. Jongeren zouden zich dus begrepen moeten voelen in hun affiniteit met IT en daarbij de ruimte krijgen om die interesses te verkennen in een omgeving met voldoende uitdaging, waarbij ook aandacht is voor ethische grenzen. Mocht er toch een incident optreden, is het volgens R10 (de vader van R09) belangrijk om rustig te blijven en het bespreek te maken: “En gewoon vragen van hey, waarom heb je dat gedaan? En weet je nu wat het gevolg is?.”

> R03: En mijn ouders vertelde gelukkig van dit moet je wel melden he, en niet op een boze manier maar gewoon op een normale manier van een beetje uitleg geven. Ja, toen wist ik dat nog niet, maar het is wel zo van als je die uitleg misschien niet krijgt of je mist het dan en je doet het een keer iets illegaals. Oh, ik kan vier menu's bestellen. Je weet niet dat het illegaal is. Ja, dan ga je ook door, want het geeft een kick.

> R04: Ze zeiden ja, als je als jij iets leuks bouwt in Minecraft, dan mag je twee keer zo lang op de computer dan als jij mensen neerschieten. En dan werd ik aangespoord om mijn ouders te vertellen kijk wat voor moois ik heb gebouwd, want dan mocht ik lekker lang op de computer. En zo zijn we er ook altijd wel over blijven praten en zo.

Wat helpt daarbij is als ouders zelf ook kennis hebben van computers en technologie en daarin een mentorrol aannemen. Dat biedt raakvlakken en kan kinderen stimuleren tot openheid. In twee gevallen zijn vaders geïnterviewd (R10 en R12) die allebei ook werkzaam waren in IT, en die lijken vrij betrokken bij de online activiteiten van hun kinderen. Deze respondenten geven aan dat ouders ook met de school van jongeren zouden moeten schakelen om jongeren op het juiste pad te houden en incidenten te voorkomen. Volgens R03 raken jongeren vooral betrokken bij crimineel hacken vanuit een slechte thuissituatie of band met ouders waarbij er geen openheid is en waarbij ouders snel boos worden, want dat zou jongeren ervan weerhouden om eerlijk te zijn. R15 ervaart ook een goede band met zijn vader op dit gebied. Hij kijkt samen met zijn vader video’s over het bouwen van computers: “want mijn vader, die vindt dat ook heel interessant om te zien.”

> R14: Mijn ouders begrijpen niet heel erg goed van als ik ga praten over oh ja, ik heb vandaag Linux OS op mijn op mijn knutsel-PC gezet en ik heb het toen met Rufus bla bla... Dat begrijpt ze allemaal niet. Ze vraagt natuurlijk wel hoe mijn dag op school is gegaan en dan zeg ik van oh ja, goed, maar voor de rest..

R13 is ethisch hacker op jonge leeftijd en herkent het belang van ouders. Volgens deze respondent worden kinderen in hoge mate blootgesteld aan risicovolle situaties op internet. Ouders zouden op de hoogte moeten zijn van die risico’s en weten waar kinderen mee bezig zijn. R16 is al bijna 18 jaar en daarom is er beperkt toezicht vanuit zijn ouders op internetgebruik, maar zijn broertje heeft dat wel.

Die mag een uur per dag op een beeldscherm en mag ook alleen Minecraft spelen. Ook R10 hanteert een schermtijd voor zijn dochter (R09), die ook eerst moet inloggen met een persoonlijke code. Andere respondenten schatten zelf in of ze te lang op de computer hebben gezeten (R07, R14).

> R12 (vader van R11): Ik denk dat in groep 3 of groep 4 één keer geld van mijn rekening werd afgeschreven. Ik vroeg het aan hem, van ja heb je iets gedaan? Hij zei in eerste instantie nee, nee, dat snap ik ook wel, is een logische reactie. Toen zei ik: ja ik vind het niet erg, maar als het zo is, laat me dat even weten. Ja, en toen heeft ie denk ik een uurtje later bekend dat hij het wachtwoord inderdaad gezien had en dat onthouden heeft. Daar hebben we gewoon goede afspraken overgemaakt.

> R03: Ja, ze wisten zeker wel wat ik gewoon deed online. Het is niet zo dat ze mijn browser helemaal gingen nachecken. Ik heb ook geen regels daarover of zoiets, maar het was wel zo van als ik iets had gedaan, dan vertelde ik gewoon wat ik had gedaan. Ik was er zelf ook gewoon trots op.

4.1.4. Risicoperceptie

Het valt op dat de jongeren die zijn geïnterviewd relatief bewust lijken van de mogelijke gevolgen van crimineel hacken voor zichzelf en ook wat betreft de impact ervan op slachtoffers. Volgens R01 loop je het risico op boetes, gevangenisstraf en ook op consequenties vanuit het criminele circuit. R15 bevestigd dat en geeft aan dat het lastiger zal worden om aan een baan te komen. Andere respondenten benoemen dat ook apparaten in beslag genomen kunnen worden (R14). R02 wil een hbo-opleiding in cybersecurity doen: “Illegaal kan het ook, maar dan is het alleen een kwestie van tijd voor wanneer ze je oppakken of niet. En ja ik wil gewoon een goede toekomst hebben.”.

Ook R14 en R15 benadrukt de potentiële financiële schade voor slachtoffers, bijvoorbeeld na een DDoS-aanval. R13 heeft ooit een kwetsbaarheid gevonden in een overheidswebsite en had daarmee toegang tot persoonlijke gegevens van burgers. Hij zou veel geld kunnen verdienen als hij dat voor illegale doeleinden had gebruikt, aldus de respondent: “Dus ja dit is een kwetsbaarheid en hier kunnen enorme gevolgen aan zitten”. Gevraagd wat er zou kunnen gebeuren bij het plegen van een DDoS-aanval, geeft R07 aan dat je gearresteerd kan worden. “Als ze je tracken naar je computer kunnen ze je wel vinden. Waarschijnlijk dan de gevangenis of moet je veel geld betalen.” R08 zou niet eens weten hoe hij überhaupt een DDoS-aanval zou moeten plegen: “Er was ooit een grote DDoS-aanval en dan is het van dat is alleen maar omdat een 15 jarig kind op zijn kamer daar zijn ding zit te doen. Dan denk ik hoe? Dat het hele internet uitvalt door iemand die 15 jaar is. Zou echt niet weten hoe ik dat zelf zou moeten doen.”

> R05: Ik heb er ooit wel een keer over nagedacht. Alleen ik snap het nut er niet helemaal van, want in 99% van de gevallen gaan ze er toch wel achter komen en dan ben je gewoon de lul. Je leert er wel wat door, maar alles wat je leert kan je niet echt toe gaan passen zonder de wet te overtreden.

> R04: Ik wist wel dat een DDoS dat dat niet mag. Ik denk eigenlijk dat iedereen dat wel wist, maar dat dat andere mensen het gewoon of een smoesje voor zichzelf bedachten. Van daar kom ik wel mee weg of zoiets. Ik denk eigenlijk dat iedereen wel wist dat dat niet mocht.

R16 geeft aan nooit te hebben gecheat in games omdat dat illegaal is en er ook het risico is om gebanned te worden uit het spel. Bovendien heeft hij wel eens video's gekeken over hacken maar daar nooit iets mee gedaan: "Dat is meer omdat ik natuurlijk ook heel erg moet oppassen met dat gebruiken natuurlijk. Als je één commend prompt en dan op enter klik en opeens doe je een DDoS-attack voer je uit dan heb je natuurlijk problemen met de politie. Dat wil je natuurlijk niet." Deze respondent heeft ook wel eens gezocht naar wachtwoordkrakers op Google en hoe dat werkt in Python: "Maar ik dacht al bij mezelf van oei, dat is misschien niet helemaal de bedoeling. Ik dacht van ja, dit voelt raar ja. Het voelt niet goed om dat te doen. Ik had het ook niet eens gevonden. En dat zegt ook wel genoeg." Een vriend van R06 wilde een keer iets hacken maar dat niet was gelukt: "Ik zei ook tegen hem daar krijg je echt straf voor wat je daar doet. En ik ben ook heel blij dat het niet lukte dat hij iets kon hacken." Deze respondent was zelf ook wel benieuwd maar wist dat het strafbaar was en wat de gevolgen zouden kunnen zijn.

> R06: De eigenaar van de website kan het misschien beseffen dat je er iets fout hebt gedaan. En ja die hebben er meer belang van dan jou en kunnen ook zien misschien waar je woont of zo. Via je IP adres of zo. Dus ja, ik zou ermee echt voorzichtig zijn.

R01 heeft ooit zijn schoolnetwerk gehackt en cijfers voor wiskunde aangepast. De school heeft dat ontdekt, maar hebben de politie niet ingeschakeld. Volgens de respondent had hij nooit de intentie om grootschalige fraude te plegen. "Dat heb je dan gewoon niet door", aldus R01. "Je denkt weet je, het is een website. Ik ben er door. Klaar. Ja, en niet echt met de achterliggende gedachte van hey, dit kon nog wel eens grote gevolgen hebben." Dit voorbeeld maakt duidelijk dat ook bij deze groep respondenten een lage risicoperceptie een rol kan spelen bij delictgedrag. Dat geldt ook voor R17. Dat is de enige respondent die in aanraking is gekomen met de politie vanwege cybercriminaliteit, namelijk het hacken van een database. "Ik wist wel dat het fout is, maar niet wat de consequenties zijn. Wat het voor de slachtoffers doet.". Wat bij deze respondent ook een rol speelde waren depressieve gevoelens. "Ik denk dat de gedachte wel ergens in m'n achterhoofd zat, maar ik zat op dat

moment ook zo slecht in m'n vel dat het me niet heel veel interesseerde."

Respondenten leren op verschillende manieren over de risico's van cybercriminaliteit. R02 noemt daarbij YouTube: "Op YouTube zie je ook best wel vaak mensen die bijvoorbeeld over grote exploits bezig zijn die erover praten en ook over dat diegene bijvoorbeeld is opgepakt en wat de gevolgen daarvan zijn". Voor R17 is het met de leeftijd gekomen: "Niet dat ik daar een heel duidelijk gesprek met iemand over heb gehad of wat dan ook. Ik denk ook wel een heel stuk aan mijn toekomst. Wil toch echt wat bereiken in mijn leven. Dan ga je toch wel dingen veranderen." Ook R13 beargumenteert dat het vooral een kwestie is van common sense: "Er is niemand die vertelt dit moet je wel doen, dit moet je niet doen. Het is eigenlijk zo simpel als je kan krijgen." Video's en tutorials over hacken hebben wel disclaimer maar die leest niemand volgens de respondent. Andere respondenten benoemen dat ze hebben geleerd over wetgeving op school, waarbij het tijdens een les over cybersecurity aan bod is gekomen (R07, R08, R16). Zo heeft R16 geleerd over phishing en dat het illegaal is. Ook R07 heeft op school geleerd over wat wel en niet mag online.

> R08: Dat hebben we vorig jaar gehad. Hadden we geleerd over black hat grey hat hacken. Dat was meneer [naam]. Hij had een soort van spelletje gemaakt waarbij je mensen kon hacken. Daar heb ik van geleerd dat er verschillende soorten hackers zijn, sommigen doen het ook om slechte dingen te doen.

> R16: Maar hoe meer je moet opzoeken, des te illegaler hoe minder makkelijker het te vinden is. Want je hebt verschillende kanalen op het internet de dark web. Als je het makkelijk kan vinden ben je bij de bovengrond. Dat is over het algemeen legaal. Maar als je echt helemaal in het deep web moet zoeken dan weet je eigenlijk al dat het niet mag.

> R13: Weet je, als je een breekijzer koopt, dan gaan ze niet zeggen gebruik je niet om een fietsslot te slopen. Want dat komt gewoon uit je common sense.

R15 heeft wel eens opgezocht of hacken strafbaar is: "En dan kreeg ik allemaal verschillende bronnen om te kijken van ja, nou is het strafbaar, ja of nee. En nou zo niet, zijn er bepaalde vormen van hacken die dan wel strafbaar zijn." Voor R15 waren zijn ouders belangrijk: "Wat mij tegenhoudt om dat zelf te doen is eigenlijk vooral nadenken over wat mijn ouders me altijd vertellen. Om het gewoon dus niet te doen." Zijn vader heeft hem veel uitgelegd over strafbaarheid van hacken en dat hij vaardigheden op het gebied van coderen alleen voor legale doeleinden zou moeten gebruiken.

4.1.5. Ethiek en morele grenzen

> R04: Ik ben nooit naar die kant gegaan, zeg maar, naar de Darkside gegaan omdat ik dat ook gewoon niet leuk vond. (…). Ik wil helemaal niet een hacker zijn, want ik weet hoe vervelend het is als je iets maakt en het wordt weer gesloopt. Maar het is ook gewoon dat je denkt ja, zo wil ik toch helemaal niet zijn? Ja, ik heb ook best wel een rechtvaardigheidsgevoel, zeg maar. Ik kan ook niet meer slapen als ik dat doe.

Een belangrijk thema in de interviews heeft betrekking op ethische en morele grenzen online. Gevraagd naar wat precies de grenzen van online gedrag definieert, gaat het respondenten er vooral om of ergens toestemming voor is verleend en afspraken over zijn gemaakt, in hoeverre het schadelijk is voor andere mensen en in hoeverre er openheid is over het online gedrag. “Dan spreek je af van oké, ik ga bijvoorbeeld tot daar. Als ik daar dan ben, ga ik niet verder. Dat is het stukje ethiek”, zo benoemt R01. Zo geeft R16 aan dat hacken toegestaan is op servers die van hunzelf zijn, maar dat in andere gevallen toestemming nodig is.

Ook R11, een jonge respondent van 12 jaar, geeft aan dat een white hat hacker dingen met toestemming doet en een black hat hacker “doet het gewoon”. R13 was nooit geïnteresseerd in illegale vormen van hacken, ondanks dat het volgens respondent makkelijk is om op illegale omgevingen te komen. Hij was zich bewust van de risico’s en wilde gewoon legitiem werk krijgen later. Het melden van eventuele incidenten is ook belangrijk. Zo had R02 geen toegang tot het wifinetwerk van school en daar was hij niet mee eens: “Ja dus toen dacht ik van oh weet je wat, ik ga gewoon dat wifi wachtwoord hacken en dan gewoon ja mezelf toegang geven tot de wifi en dat heb ik ook aangegeven aan het IT team.” Hij heeft dat dus gemeld intern. In dit geval vond de directie van de school het incident geen probleem.

> R16: Ethisch is als je het met beleid doet en goed nadenkt en ook de regels weet. En onethisch is als je over die regels heengaat en dingen uitprobeert en weet dat het niet mag. Je kan natuurlijk heel goed zelf kijken van oké mag dit of mag dat niet? En als niet mag, dan stop ik gewoon direct mee.

> R13: En als ik wel het idee heb dat ik het heb, dus als ik er wel doorheen kunnen komen, zou ik liever gewoon naar de administratie gaan van hey, zou ik even kijken hoe het bij jullie zit. Ja, en dan weet je eigenlijk altijd wel dat ze het daar wel mee eens zullen kunnen zijn. Dat je dus gewoon ja, precies hetzelfde mag doen, maar dan riskeer je geen computervredebreuk.

Een aantal respondenten heeft wel eens gecheat tijdens het gamen, maar meestal in de context van single player of enkel gericht op vrienden. R16 geeft aan wel games te modden om het spel wat makkelijker te maken voor hemzelf. R05 heeft met toestemming een DDoS-aanval gepleegd op een

computersysteem van zijn vriend. R04 heeft wel eens cheats geïnstalleerd voor Minecraft, maar “dat voelt gewoon helemaal niet fijn”, aldus R04. Ook R08 benoemt dat het “gewoon fijn is als iedereen eerlijk doet”. R04 benoemt verder dat hij het zelf ook niet leuk vindt als hij te maken krijgt met hackers tijdens het gamen en daar zelf ook nare ervaringen mee heeft. Slachtofferschap kan dus enerzijds daderschap aanwakkeren zoals bij de criminele hackers maar kan mogelijk ook het moreel kompas versterken in andere gevallen. R14 krijgt ook te maken met hackers bij het spelen van Roblox en meld dat altijd. Respondenten zijn dus over het algemeen van mening dat cheaten in games morele grenzen voorbij gaat.

R17 is juist een voorbeeld van een criminele hacker waarbij betrokkenheid bij cheaten en slachtofferschap in gamen een opstapje was naar zwaardere delicten. “Dan zie je iemand vals spelen, dan denk je dat wil ik ook”, zo stelt R17. Hij ging zich verdiepen in cheaten en kwam terecht op een forum met een sectie voor game cheats maar ook met secties voor bredere cybercriminaliteit. Eerst was de respondent vooral mee aan het lezen maar op een gegeven moment werd zijn betrokkenheid groter en ging ook zelf informatie posten. Hij had geleerd op configuraties voor penetratie testing tools te coderen en verkocht dat later ook zelf.

> R04: Vroeger had ik ook wel eens mensen die dan zeggen ‘oh, als je mij nou toegang geeft als je mij ook admin maakt, dan fix ik wel even dit en dit.’ En dan ging ik even avondeten en dan kwam ik terug boven en was alles kapot gemaakt. Dat is ook gewoon een hele nare ervaring.”

> R14: Ik heb een morele objectie tegen cheaten en hacken. Want word gewoon beter in dit spel om speel een ander spel, kom op. Verspil een ander spel maar he. Het is oneerlijk en ongeskilled.

Het is soms nog wel zoeken waar de grenzen precies liggen. Volgens R01 is de “lijn tussen ethisch en niet ethisch heel dun. Bij twijfel moet je al nee zeggen”. R05 benoemt dat hij enerzijds wel begrijpt dat iemand zijn cijfers zou veranderen als diegene daardoor het schooljaar zou halen, maar dat het voor slachtoffers juist vervelend is: “Tuurlijk, het is strafbaar, maar het is ook gewoon naar voor die persoon die al die shit mag gaan oplossen.” Volgens R15 is het aanpassen van cijfers ook verkeerd: “Die cijfers bepalen eigenlijk zeg maar van hoe goed je het doet en wat voor soort werk je dan zou kunnen doen.” Tegelijkertijd is ook wel de verantwoordelijkheid van de school om het wifi-netwerk goed te beveiligen, aldus R15. Dat wijst weer op het gebruik van neutralisatietechnieken, iets dat ook bij criminele hackers wordt geobserveerd.

R04 stelt ook dat het weinig impact zou hebben als het schoolnetwerk een paar minuten niet zou werken of als je de internetsnelheid van andere mensen zou aanpassen. “Ja, dat is grappig, maar ik

wilde wel altijd dingen doen die ik weer terug kon draaien. Ik was gewoon vooral een beetje aan het klooien." Deze respondent geeft aan steeds eerlijk te zijn geweest over dit soort handelingen. R08 herkent zich daarin: "Als je het 10 minuten doet en dat uitloggen oke. Maar als je het meerdere dagen doet en die man/vrouw wordt daar helemaal gek van. En als je dat gaat gebruiken om dingen te stelen zoals wachtwoorden van e-mails enzo dat gaat ook te ver." Gevraagd wat respondent zou zeggen als een klasgenoot zoiets zou doen: "Ik zou het zeggen dat het niet tof is dat hij zo zou doen. En zeggen ja als je zo doorgaat ga ik geen vrienden meer met je zijn."

> R14: Als ik denk aan cybercriminaliteit. Zijn er hoogtes. Het laagste is van oh ik download even dit mp3tje illegaal of ik download deze show. (…). Middelmatig online criminaliteit is misschien een stad bijna platleggen of een of een DDoS aanval.

R03 heeft vooral over die grenzen geleerd van ouders maar ook via een stichting die jongeren begeleidt en via presentaties van de politie. Respondenten leren ook van incidenten. Zo heeft R03 ooit het systeem gehackt dat scholen gebruiken voor administratie en kon op die manier zijn cijfers inzien tijdens de toetsweek. Hij wist niet dat dit niet mocht. In dit geval kreeg respondent geen straf omdat hij eerder al had gemeld dat hij toegang had tot het magister. R02 geeft aan dat hij met name via YouTube heeft geleerd over online ethiek. Ook voor R11 was zijn vader (R12) daarbij belangrijk. Deze respondent mocht met toestemming de website van het werk van zijn moeder proberen te hacken in ruil voor een beloning, en dat was ook gelukt.

> R02: Ja, vooral eigenlijk YouTube ook natuurlijk. Heel simpel gezegd als je een script van GitHub heb en dat kan bijvoorbeeld internal blue zijn of internal sky zijn. Dan staat er altijd documentatie bij genaamd read me en daar staat altijd eigenlijk in wat gegevens wat je wel mag niet mag.

> R01: Je spreekt gewoon regels af. Van tevoren zeggen ja, ja, maar zover ga ik, dat kan ik zien. En als ik verder kom dan ben ik gewoon in overtreding. Maar bijvoorbeeld ook als je er per ongeluk komt. Je gaat linksom en je bent in één keer alsnog in. Dan moet je dat sowieso aangeven van hey, er is iets gebeurd. Ik weet van mezelf als ik er een keer over heen ben, dan blijf je het doen.

> R13: Ik hou van programmeren, ik hou van hacken en wil er gewoon baan in hebben. Dus voor mij is er heel weinig punt in het illegaal doen.

4.1.6. Sociaal netwerk

Het valt op dat de respondenten over het algemeen geen offline kennissen of vrienden hebben die wel eens betrokken zijn bij cybercriminaliteit. “Die hebben al moeite om zelf een website in elkaar te zetten”, zegt R01 over zijn vrienden. Via een stichting voor jongeren kent deze respondent nu wel leeftijdsgenoten die ook goed zijn met computers, maar daarbuiten niet. “Zijn misschien een enkeling of twee die wat weten, maar die komen ze al gauw naar mij toe van hey hoe doe ik dit.” Dit geldt ook voor R04: “Ik heb allemaal mensen die we gewoon al heel lang kennen, die eigenlijk niks met programmeren te maken hebben”. R05, R06 en R07 kennen ook geen mensen uit de fysieke wereld die goed zijn in programmeren. In andere gevallen benoemen respondenten daarbij dat ze juist worden geholpen door kennissen om beter te worden op een legale manier. R03 is samen met vrienden bezig om een lesmethode te ontwikkelen om jongeren te leren over cybersecurity. Ook R16 heeft samen met een klasgenoot een computer in elkaar gezet.

Naast het fysieke sociale netwerk is duidelijk dat veel van het sociale leven van jongeren met affiniteit voor computers en technologie zich afspeelt in de online wereld, vooral op Discord. Dat merkt R12 bijvoorbeeld ook bij zijn zoon: “Je merkt dat hij in zijn contact met mensen en kinderen goed gaat, maar het ook fijn vindt om zichzelf terug te trekken en digitaal met mensen te spreken of via de telefoon bijvoorbeeld een whatsappgroepje heeft. Of online het gesprek aangaat.” R17 heeft nooit echt vrienden gehad in de fysieke wereld, zo geeft hij aan: “Online wel een aantal die ik nog wel regelmatig spreek.” R14 herkent dit: “Persoonlijk wil ik natuurlijk meer met echt fysiek mensen praten. Maar ja, wat mijn ervaring daarop is, is dat het heel lastig is om contact te maken. En meestal ga ik dan online contact op zoeken met leeftijdsgenoten.”

> R08: Ik heb wel vrienden gehad buiten de Discord, maar daar praat ik niet meer mee.

Over het algemeen gaat het daarbij over prosociale invloeden. Die vrienden hebben ze bijvoorbeeld leren kennen via Discord, Roblox of andere games, of uit de fysieke wereld waarbij ze online communiceren. Ze praten daarbij over allerlei onderwerpen. “De meeste van mijn online vrienden weten überhaupt niks [van hacken]”, zoals de respondent aangeeft. R13 is ethisch hacker en is op Discord actief in allerlei groepen die draaien om ethisch hacken, wat veel van zijn sociale leven beslaat. R15 geeft aan zeer actief te zijn op Discord om contact te onderhouden met vrienden die hij heeft leren kennen via gamen: “Want in heel veel games die ik speel, ontmoet ik mensen en worden we redelijk snel vrienden.” Ook R07 geeft aan vrienden te hebben die hij heeft leren kennen via Discord of via Roblox, met wie hij wel “een uurtje of twee per dag” praat.

> R02: Via online fora natuurlijk. Dat ik denk dat iedereen dat wel van mijn leeftijd op dit moment wel heeft. Ja ja, vooral veel forums op Discord of op private chatrooms.

> R05: Ik heb een hele vriendengroep erdoor opgebouwd, die ik ook al ontmoet heb in het echt, een paar keer al. Er komen echt wel lange contacten uit. Ja, gewoon vrienden, soort vrienden.

> R05: Maar als iemand mij bericht dan reageer ik wel gewoon binnen 1 uur of zo. Ik ben best wel veel online.

Soms kennen respondenten via online platformen leeftijdsgenoten die wel eens betrokken zijn geweest bij hacking. R04 geeft aan mensen te kennen die “dingen hebben gedaan die niet mogen”, maar daar probeert hij afstand van te houden. Vrienden die hij kent via Discord hebben bijvoorbeeld Minecraft-servers gehackt en andere spelers benadeeld. “Daarvan zei ik ook altijd gewoon: nou, het is een beetje wel onaardig dit, man. Niet van ik ga de politie bellen, maar dit is best wel onaardig”, zoals de respondent aangeeft. R01 is meerdere keren benaderd door willekeurige mensen online die vragen om iets te hacken.

> R01: Je krijgt een berichtje van hey kan je die en die van mij hacken, als je deze website plat legt dan krijg je € 10.000 of 50.000 afhankelijk van welke website. Op Instagram, Reddit, Facebook, Discord, het kan gewoon overal wel. Het gebeurt in flows. Eén moment is het heel veel. Of drie maanden niks en dan heb je weer een paar erbij.

Ook R05 kent mensen via Discord die wel eens betrokken waren bij een DDoS-aanval. Zij vertellen daar dan trots over maar worden daarna vaak al snel gekickt uit die groepen. Deze respondent heeft toen hij 11 jaar was iemand ontmoet via Minecraft die de respondent heeft leren cheaten. Door zelf te zoeken naar meer informatie kwam de respondent terecht in groepen op Discord waarin bijvoorbeeld scripts werden gedeeld voor het cheaten. “Als je het opzoekt heb je binnen een seconde een stuk of honderd van die Discord groepen”, aldus R05. Deze respondent gebruikte die groepen dus om andermans scrips te testen maar ook om te socialiseren: “Maar soms ga je daar ook gewoon bellen. Gewoon, het is gezellig. Hoe je ook met een normale vriend zou doen.”

> R05: Ik weet het nog een hele community die erachter stond, dus dat is gewoon ja, het was gewoon gezellig op dat moment. Iedereen deed het. Het was ook gewoon grappig. Want natuurlijk, het is niet fijn voor de ander, maar het is wel heel grappig als je iemand bijvoorbeeld heel boos ziet worden. Tenminste, zo dacht ik op dat moment.

Een ander duidelijk voorbeeld van een respondent die is blootgesteld aan antisociale invloeden online is R17. Hij is via het cheaten in games terecht gekomen op een forum waar hij heeft geleerd om cybercriminele tools te gebruiken, zelf te coderen en daar ook te verkopen. “Op de website is ingebouwd dat je mensen reputatie kan geven. Dat is ook het gevaar. Je blijft erin betrokken”, zo stelt

R17. Hij geeft aan “verkeerde vrienden” te hebben gemaakt op Minecraft en via-via steeds verder het wereldje in is gerold. Zo heeft hij iemand via Minecraft iemand ontmoet uit het buitenland die ook actief was in de cybercriminaliteit en later ook is opgepakt. Dit wijst erop dat “online peers” potentieel een rol kunnen spelen bij escalatie in online crimineel gedrag.

4.2. Vragenlijst

4.2.1. Beschrijvende statistiek

Tabel 2 beschrijft de psychometrische waardes van de onafhankelijke variabele in gecombineerde steekproef en de waardes afzonderlijk voor de risicogroep, aangezien deze twee datasets de basis vormen voor de verdere analyse. Bij de risicogroep zijn twee aanvullende factoren gemeten die nog geen onderdeel waren van de oorspronkelijke vragenlijst die is afgenomen bij de controlegroep, namelijk offline ouderlijk toezicht en antisociale attitudes. In beide datasets hadden alle variabelen een Cronbach’s alpha hoger dan .60 en daarmee een acceptabele interne consistentie (Nunnally & Bernstein, 1994).

Tabel 2

Psychometrische waardes in de gecombineerde steekproef en de risicogroep

Variabele	Steekproef	Min	Max	M	SD	Aantal items	Alpha
Continue variabelen							
Online deviante invloeden	Gecombineerd	3	15	5.06	3.13	3	.904
	Risicogroep	3	15	6.63	3.50	3	.870
Delinquente vrienden	Gecombineerd	0	7	1.28	1.64	8	.724
	Risicogroep	0	7	1.8	1.88	8	.718
Lage zelfcontrole	Gecombineerd	13	53	34.96	8.58	13	.809
	Risicogroep	15	53	35.86	7.95	13	.770
Online disinhibitie	Gecombineerd	3	15	7	3.62	3	.847
	Risicogroep	3	15	8.56	3.65	3	.845
IT-skills	Gecombineerd	1	5	3.07	.99	1	-
	Risicogroep	1	5	3.55	.99	1	-
Online ouderlijk toezicht	Gecombineerd	4	20	9.37	3.78	4	.627
	Risicogroep	4	19	8.88	3.74	4	.741
Gaming	Gecombineerd	1	5	2.46	1.23	1	-
	Risicogroep	1	5	3.13	1.11	1	-

Programmeren	Gecombineerd	1	5	1.46	.84	1	-
	Risicogroep	1	5	1.86	1.02	1	-
Online communicatie	Gecombineerd	2	5	3.26	1.08	1	-
	Risicogroep	1	5	1.86	1.02	1	-
Offline ouderlijk toezicht	Gecombineerd	-	-	-	-	-	-
	Risicogroep	3	8	7.17	7.16	2	.732
Antisociale attitudes	Gecombineerd	-	-	-	-	-	
	Risicogroep	5	20	16.34	2.52	5	.780
Dichotome variabelen							
Schooljaar overdoen	Gecombineerd	0	1	.34	.47	1	-
	Risicogroep	0	1	.45	.500	1	-
Geschorst van school	Gecombineerd	0	1	.09	.28	1	-
	Risicogroep	0	1	.15	.36	1	-
Onder toezicht van jeugdzorg	Gecombineerd	0	1	.04	.21	1	-
	Risicogroep	0	1	.06	.25	1	-
Ouderlijk geweld	Gecombineerd	0	1	.19	.40	1	-
	Risicogroep	0	1	.24	.43	1	-

In Tabel 3 is de prevalentie weergegeven van de verschillende vormen van crimineel gedrag onder de risicogroep en de controlegroep. Cybercriminaliteit is alleen gemeten bij de risicogroep aangezien dit een exclusiecriteria was voor de controlegroep. Alle vormen van delictgedrag komen vaker voor bij de risicogroep, zowel wat betreft het afkijken/raden van wachtwoorden als financiële cybercrime en traditionele offline criminaliteit. Zo was 37.5% van de risicogroep betrokken bij een vorm van offline criminaliteit tegenover 31.3% van de controlegroep. Verschillen zijn ook groot wat betreft financiële cybercrime, met name wat betreft virtueel diefstal: 28.8% van de risicogroep geeft aan wel eens iets te hebben gestolen van tegenstanders in games terwijl dat niet mag, tegenover 3% van de controlegroep. Dit verschil is ook significant (X^2=18.370***). Het meest voorkomende delict was het afkijken of raden van wachtwoorden, zowel binnen de risicogroep (n=29; 36.3%) als de controlegroep (n=18; 22.5%). De risicogroep scoort daarbij hoger dan de controlegroep.

Wat betreft de meer technische vormen van online criminaliteit kwam het plegen van een DoS/DDos aanval relatief veel voor (n=9; 11.3%). In totaal gaven 15 respondenten aan betrokken te zijn geweest bij een vorm van cybercriminaliteit (18.8%). Deze groep is de focus van de verdere analyse. Verder hebben 30 respondenten wel eens offline criminaliteit gepleegd (37.5%). Hoewel het aantal daders van offline criminaliteit in de risicogroep niet veel verschil met het aantal daders van offline

criminaliteit in de controlegroep, is de prevalentie van elk afzonderlijk delict wel hoger in de risicogroep. Zo waren 12 respondenten uit de risicogroep (15%) betrokken bij geweld tegen personen, tegenover 0 respondenten in de controlegroep. Dat betekent dat jongeren in de risicogroep meer verschillende offline delicten plegen.

Tabel 3

Prevalentie van delictgedrag in controlegroep en risicogroep

	Risicogroep		**Controlegroep**	
Delict	**N**	**%**	**N**	**%**
Cybercriminaliteit				
Afkijken/raden van wachtwoorden	29	36.3	18	22.5
Hacken met technische middelen	6	7.5	-	-
DoS/DDoS aanvallen	9	11.3	-	-
Website defacement	5	6.3	-	-
Malware	6	7.5	-	-
Totaal	15	18.8	-	-
Financiële cybercrime				
Virtueel diefstal	23	28.8	3	3.8
Phishing	5	6.3	0	-
Online identiteitsfraude	9	11.3	3	3.8
Totaal	26	32.5	5	6.3
Traditionele offline criminaliteit				
Graffiti	9	11.3	5	6.3
Geweld tegen personen	12	15	0	0
Winkeldiefstal	18	22.5	14	17.5
Fietsendiefstal	3	3.8	1	1.3
Vandalisme	6	7.5	1	1.3
Brandstichting	18	22.5	7	8.8
Totaal	30	37.5	25	31.3

4.2.2. Vergelijking van risicogroep met controlegroep

Tabel 4 beschrijft de resultaten van de ANOVA analyse, waarbij de risicogroep is vergeleken met de controlegroep op de belangrijkste risicofactoren. Hieruit bleek dat de risicogroep significant hoger scoorde op online deviante invloeden ($F(1,158)=53.414$, $p<.001$), delinquente vrienden ($F(1,158)=18.061$, $p<.001$) en IT-skills ($F(1,158)=49.962$, $p<.001$). Ook spenderen ze meer tijd aan gaming ($F(1,158)=65.441$, $p<.001$) en programmeren (($F(1,158)=46.937$, $p<.001$). Middelgrote effecten zijn gevonden voor online deviante invloeden en gaming.

Tabel 4

Resultaten ANOVA

Kenmerk	**Groep**	**M**	**SD**	**F**	**Eta**
Online deviante invloeden	Controle	3.49	1.59	53.414***	.253
	Risicogroep	6.63	3.50		
Delinquente vrienden	Controle	.75	1.16	18.061***	.103
	Risicogroep	1.80	1.88		
Lage zelfcontrole	Controle	34.05	9.13	1.792	.011
	Risicogroep	35.86	7.95		
Online disinhibitie	Controle	5.44	2.85	36.447***	.187
	Risicogroep	8.56	3.65		
IT-skills	Controle	2.59	.71	49.962***	.240
	Risicogroep	3.55	.99		
Online ouderlijk toezicht	Controle	9.86	3.77	2.768	.017
	Risicogroep	8.86	3.74		
Gaming	Controle	1.80	.96	65.441***	.293
	Risicogroep	3.13	1.11		
Programmeren	Controle	1.06	.24	46.937***	.229
	Risicogroep	1.86	1.02		
Online communicatie	Controle	3.15	1.03	1.562	.010
	Risicogroep	3.36	1.12		

Uitkomstvariabele: cybercriminaliteit
**=p<.05, **=p<.01, ***=p<.001*

Tabel 5 beschrijft de resultaten van verschillende chi-kwadraattoetsen voor het vergelijken van de risicogroep met de controlegroep op de categorische variabelen. Daaruit bleek dat jongeren in de risicogroep significant vaker betrokken zijn bij financiële cybercrime (X^2=17.644***), vaker zijn geschorst van school (X^2=7.828**) en vaker zijn blijven zitten op school (X^2=9.057**).

Tabel 5

Resultaten chi-kwadraattoetsen

Variabele	**Groep**	**N**	**%**	X^2
Ouderlijk geweld	Controlegroep	12	15	1.960
	Risicogroep	19	23.75	
Onder toezicht van jeugdzorg	Controlegroep	2	2.5	1.345
	Risicogroep	5	6.25	
Blijven zitten op school	Controlegroep	18	22.5	9.057**
	Risicogroep	36	45	
Geschorst van school	Controlegroep	2	2.5	7.828**
	Risicogroep	12	15	
Traditionele criminaliteit	Controlegroep	25	31.25	.693
	Risicogroep	30	37.5	
Financiële cybercrime	Controlegroep	5	6.25	17.644***
	Risicogroep	26	32.5	

**=p<.05, **=p<.01, ***=p<.001*

4.2.3. Vergelijking van daders met niet-daders in de risicogroep

Tabel 6 beschrijft de resultaten van de ANOVA waarbij daders van cybercriminaliteit binnen de risicogroep (n=15) zijn vergeleken met niet-daders in de risicogroep (n=65). Hieruit bleek dat daders significant hoger scoorde op IT-skills (F(1,78)=19.426, p<.001), online ouderlijk toezicht (F(1,78)=8.372, p<.01), programmeren (F(1,78)=8.855, p<.01) en delinquente vrienden (F(1,78)=5.531, p<.05). Dit waren allemaal kleine effectgroottes. Het is belangrijk om te benoemen dat het kleine aantal daders mogelijk in de hand werkt dat de sterkte van verbanden zijn onderschat. Met meer respondenten waren andere factoren zoals online deviante invloeden mogelijk ook significant.

Tabel 6

Resultaten ANOVA

Kenmerk	Groep	M	SD	F	Eta
Online deviante invloeden	Niet-daders	6.28	3.50	3.550	.044
	Daders	8.13	3.16		
Delinquente vrienden	Niet-daders	1.57	1.78	5.531*	.066
	Daders	2.80	2.04		
Lage zelfcontrole	Niet-daders	35.06	7.66	3.63	.045
	Daders	39.33	8.52		
Antisociale attitudes	Niet-daders	16.26	2.68	.313	.004
	Daders	16.67	1.68		
Offline ouderlijk toezicht	Niet-daders	7.05	1.27	5.531	.047
	Daders	7.75	.45		
Online disinhibitie	Niet-daders	8.54	3.64	.015	.000
	Daders	8.67	3.81		
IT-skills	Niet-daders	3.34	.92	19.426***	.199
	Daders	4.47	.74		
Online ouderlijk toezicht	Niet-daders	9.43	3.74	8.372**	.097
	Daders	6.47	2.72		
Gaming	Niet-daders	3.15	1.11	.233	.003
	Daders	3.00	1.14		
Programmeren	Niet-daders	1.71	.93	8.855**	.090
	Daders	2.53	1.13		
Online communicatie	Niet-daders	3.29	1.14	1.377	.017
	Daders	3.67	.98		

Uitkomstvariabele: cybercriminaliteit

**=p<.05, **=p<.01, ***=p<.001*

Tabel 7 beschrijft de resultaten van de chi-kwadraattoetsen waarbij daders van cybercriminaliteit in de risicogroep zijn vergeleken met risicojongeren die geen cybercriminaliteit hebben gepleegd op de dichotome variabelen. Daaruit kwam naar voren dat daders significant vaker fysiek geweld tussen ouders hebben meegemaakt (X^2=5.354*). Het ging daarbij om bijna de helft van de daders, in vergelijking met nog geen 20% van de niet-daders. Ook hadden daders significant vaker werk in IT (X^2=5.280*), namelijk 60% tegenover ongeveer 30%. Ten slotte hadden daders van cybercriminaliteit significant meer kans om ook offline delicten te plegen.

Tabel 7

Resultaten chi-kwadraattoetsen

Variabele	**Groep**	**N**	**%**	X^2
Ouderlijk geweld	Niet-daders	12	18.46	5.354*
	Daders	7	46.67	
Onder toezicht van jeugdzorg	Niet-daders	5	7.69	1.231
	Daders	0	-	
Blijven zitten op school	Niet-daders	30	46.15	.186
	Daders	6	40	
Geschorst van school	Niet-daders	9	13.85	.362
	Daders	3	20	
Werk in IT	Niet-daders	19	29.23	5.280*
	Daders	9	60	
Traditionele criminaliteit	Niet-daders	19	29.2	10.114**
	Daders	11	73.3	

**=p<.05, **=p<.01, ***=p<.001*

5. Discussie

Het doel van dit verkennende onderzoek was om meer zicht te krijgen op de ontwikkelpaden en kenmerken van jongeren met een hoge affiniteit en interesse voor computers en technologie. Dit betreft een risicogroep voor betrokkenheid bij cybercriminaliteit. Kennis over deze doelgroep is nodig voor het ontwikkelen en implementeren van effectieve interventies, in lijn met het landelijk kwaliteitskader effectieve jeugdinterventies voor de preventie van jeugdcriminaliteit (Hendriks & Stams, 2024). Het onderzoek kan daarmee ondersteunen bij het ingrijpen in een vroeg stadium en voorkomen dat jongeren – soms onbedoeld – een delict plegen en slachtoffers maken. We hebben gebruik gemaakt van twee dataverzamelingsmethoden: interviews en vragenlijstonderzoek. De interviews zijn gevoerd met jongeren die risico lopen om betrokken te raken bij hacking. De vragenlijst was gericht op het in kaart brengen van risicofactoren en is afgenomen onder een algemene populatie jongeren (controlegroep) en opnieuw ook onder jongeren met affiniteit en interesse op het gebied van computers en technologie (de risicogroep).

5.1. Wat zijn de demografische en psychologische kenmerken van jongeren met een hoge affiniteit voor IT?

Uit het onderzoek komt naar voren dat jongeren die risico lopen op cybercriminaliteit vooral worden gekenmerkt door factoren die zich manifesteren in de online omgeving. Ze spenderen veel tijd aan gaming en programmeren, hebben vaardigheden op het gebied van computers en zijn meer ontremd wanneer ze online zijn, zo blijkt uit de resultaten van de vragenlijst. Dat waren allemaal factoren die de risicogroep konden onderscheiden van de controlegroep en zijn grotendeels in lijn met eerder onderzoek (Bekkers et al., 2025; Kerstens & Jansen, 2016). Dat betekent dat potentiële hackers een preoccupatie vertonen richting de digitale omgeving. Jongeren zonder die interesses zijn simpelweg minder vaak online en worden minder blootgesteld aan gelegenheden voor het plegen van delicten. Het risico van online omgevingen is dat jongeren te maken krijgen met deviante invloeden die cybercriminaliteit verheerlijken of anderzijds stimuleren (Holt, 2007; Bossler, 2021). Uit de interviews kwam bijvoorbeeld naar voren dat een deel van de respondenten via de online wereld socialiseert met mensen van wie ze leren hacken en cheaten in games (Leukfeldt & Bekkers, 2026). Ook uit de vragenlijst bleek dat de risicogroep inderdaad vaker te maken krijgt met online deviante invloeden vergeleken met de controlegroep. Opvallend is verder dat de risicogroep het slechter doet op school vergeleken met de normale populatie jongeren: ze blijven vaker zitten en zijn vaker geschorst. Op die manier kunnen jonge potentiële hackers mogelijk vroegtijdig gesignaleerd worden. Het is voor nu onduidelijk hoe de mindere schoolprestaties verklaard kunnen worden. Eerder onderzoek vond gemixte resultaten wat betreft schoolprestaties van hackers (Rokven et al., 2018; Fox & Holt, 2021). Wat betreft demografische kenmerken blijkt dat de risicogroep vrijwel altijd mannen betreffen, maar dat kan ook te maken hebben met de manier van dataverzameling, waarbij de focus

lag op IT-studenten. Dat kan mogelijk ook verklaren waarom de risicogroep jonger was.

5.2. Hoe ontwikkelen jongeren met een hoge affiniteit voor IT hun vaardigheden en interesses?

Veel respondenten beschrijven in de interviews dat hun interesse in computers en technologie al op jonge leeftijd begon, vaak in de context van gamen, hardware en programmeren (Fox & Holt, 2021; Leukfeldt & Bekkers, 2021). Hoewel sommige respondenten nog weinig vaardigheden hadden ontwikkeld op het moment van dataverzameling, waren andere respondenten al bezig met complexe activiteiten voordat ze 10 jaar oud waren, zoals het bouwen van computers, het testen van broncodes of het programmeren van software. Voor een deel van de respondenten werd deze interesse gestimuleerd door ouders of andere familieleden die in de ICT werken, waardoor zij al vroeg in aanraking kwamen met technologie. Opvallend in het bijzonder is de rol van gaming, waarbij Roblox en Minecraft vaak worden genoemd. Jongeren willen bijvoorbeeld hun eigen servers maken, plugins ontwikkelen of aanpassingen doen aan games. Hierdoor komen zij in aanraking met programmeren en worden ze gemotiveerd om technische vaardigheden op te doen. Zo kan die initiële interesse in gamen uitgroeien tot het bouwen van websites, het maken van scripts of het ontwikkelen van tools (NCA, 2017).

Respondenten leren die vaardigheden via verschillende bronnen. YouTube wordt het vaakst genoemd, omdat daar veel tutorials te vinden zijn over programmeren, hardware en hacking. Daarnaast maken jongeren gebruik van online communities en forums, zoals Discord, Reddit, StackOverflow en platforms zoals TryHackMe. Dat komt overeen met eerder onderzoek naar criminele hackers (Leukfeldt & Bekkers, 2026). Naast die online bronnen spelen vrienden en sociale netwerken een belangrijke rol in het leerproces. Jongeren leren van elkaar door samen te experimenteren, kennis uit te wisselen of elkaar te helpen bij technische problemen. In sommige gevallen fungeren ouders of andere familieleden als mentor, bijvoorbeeld door te helpen bij het bouwen van een computer of door uitleg te geven over technische concepten. Het ontwikkelen van vaardigheden gaat samen met experimenteren in de praktijk. Respondenten geven aan dat zij vooral leren door dingen zelf uit te proberen en te kijken wat er gebeurt. Dit experimentele leerproces kan soms leiden tot delictgedrag. Dit gedrag weerspiegelt een verkennende houding, waarbij jongeren willen begrijpen hoe systemen werken en niet zozeer hoe ze die systemen kunnen verstoren.

5.3. Op welke manier wordt het gedrag van jongeren met een hoge affiniteit voor IT beïnvloed door hun sociale omgeving?

Uit de interviews komt naar voren dat leeftijdsgenoten zowel een positieve als negatieve invloed kunnen hebben. Over het algemeen hebben respondenten nauwelijks offline vrienden die ooit betrokken zijn geweest bij cybercriminaliteit, voor zover respondenten dat weten. In een aantal

gevallen geven respondenten aan dat ze juist prosociale activiteiten ondernemen met klasgenoten of andere vrienden, zoals het bouwen van een computer, en daarmee positief gedrag bekrachtigen. In andere gevallen hebben vrienden van respondenten in de fysieke wereld überhaupt weinig technische kennis. De vraag is nog in hoeverre dat positief of negatief is. Duidelijk is ook dat jongeren beïnvloed kunnen worden door rolmodellen in de fysieke wereld die meer ervaring hebben en positief gedrag stimuleren, zoals ethisch hackers en ouders die werken in de IT. Die personen hebben een taak in het overbrengen van moreel gedrag. Over het algemeen lijkt de online omgeving wel meer centraal te staan in het sociale leven van respondenten. Respondenten zijn dagelijks online en socialiseren daar met leeftijdsgenoten, momenteel met name op Discord. Voor sommige jongeren zijn online contacten zelfs belangrijker dan offline vriendschappen. Ze voelen zich prettiger om via digitale omgevingen te communiceren en dat gaat vooral ook over alledaagse onderwerpen. Deze online vriendschappen geven betekenis en lijken daarmee een positieve invloed te hebben. Tegelijkertijd komen jongeren online soms in aanraking met deviant gedrag. Zo kwamen enkele respondenten in de interviews via games, fora of Discord-groepen in contact met communities waar scripts, cheats of cybercriminele tools werden gedeeld. Dit kan ertoe leiden dat jongeren aan de hand van online contacten steeds verder in de cybercriminele wereld terechtkomen. Uit de vragenlijst komen soortgelijke resultaten, waarbij de risicogroep hoger scoorde dan de controlegroep op online deviante invloeden.

5.4. In hoeverre en op welke manier is er een link tussen daderschap van cybercriminaliteit en daderschap van offline criminaliteit?

Er lijkt enige overlap tussen daderschap van cybercriminaliteit en daderschap van offline criminaliteit (zie ook Bekkers & Leukfeldt, 2025). Er waren weinig verschillen tussen de risicogroep en de controlegroep wat betreft de totale prevalentie van offline delictgedrag: in beide groepen pleegt ongeveer één op de drie een offline delict. Echter was de prevalentie van elk afzonder delict (veel) hoger in de risicogroep. Mogelijk is dat deels te wijten aan het feit dat de risicogroep jonger was dan de controlegroep en jonge mensen vaker delicten plegen. Daarnaast kan het ook zo zijn dat de risicogroep in het algemeen vaker regels overtreedt, online dan wel offline. Ook wat betreft het afkijken/raden van wachtwoorden en financiële cybercriminaliteit scoorde de risicogroep hoger dan de controlegroep, vooral wat betreft diefstal in games. Het feit dat de risicogroep vaker andere vormen van online criminaliteit pleegt kan verklaard worden door een hogere blootstelling aan risicovolle situaties online en de aanwezigheid van meer online risicofactoren. Wanneer verder ingezoomd op de risicogroep, waren daders van cybercriminaliteit significant vaker betrokken bij offline criminaliteit dan niet-daders in de risicogroep.

5.5. Wat zijn de overeenkomsten en verschillen tussen jongeren die risico lopen op daderschap en jongeren die daadwerkelijk delicten hebben gepleegd?

In het huidige onderzoek stond een risicogroep centraal en in eerder onderzoek zijn ook interviews gevoerd met criminele hackers (Leukfeldt & Bekkers, 2026; Martineau et al., 2024). Beide groepen jongeren lijken voornamelijk intrinsiek gemotiveerd en handelen vanuit nieuwsgierigheid, plezier en de wens om de techniek te begrijpen of anderen te helpen. Financiële beloningen spelen meestal geen rol in eerste instantie. Respondenten in het huidige onderzoek zijn niet geselecteerd op het plegen van delicten maar een klein aantal gaf wel aan ooit betrokken te zijn geweest bij relatief milde vormen van hacking, zoals cheaten in games of het hacken van het wifi-netwerk op school. Ook die incidenten komen meestal voort uit nieuwsgierigheid, waarbij respondenten het gedrag beschouwen als een persoonlijke uitdaging. Ze vertellen dit bijvoorbeeld ook aan ouders zonder zich daarbij bewust te zijn van mogelijke schade. Wat criminele hackers en de jongere risicogroep ook gemeen hebben is hoe ze vaardigheden leren, namelijk op het reguliere web via hulpbronnen als YouTube, en ook via vrienden die meer kennis hebben.

Er zijn ook een aantal verschillen. Uit de interviews blijkt dat jongeren die (nog) geen delicten hebben gepleegd vooral te onderscheiden van criminele hackers wat betreft 1) een sterker gevoel voor ethische grenzen met meer oog voor slachtoffers en risico's, 2) meer transparantie en controle vanuit ouders en 3) een gebrek aan antisociale invloeden online en offline. Zo lijken niet-delictplegers zich beter te kunnen navigeren in de grenzen van online gedrag, waarbij aandacht is voor toestemming, schadelijkheid en openheid. Veel respondenten kunnen benoemen wat de mogelijke consequenties zijn van het plegen van delicten en schatten de kans dat ze gepakt worden door de politie hoog in. Daarnaast valt het op dat ouders betrokken zijn bij de online activiteiten van respondenten, waarbij sprake is van een connectie dat berust op vertrouwen enerzijds en toezicht anderzijds. Bij criminele hackers is er juist een gebrek aan ouderlijke betrokkenheid, zo blijkt uit eerder onderzoek. Daarnaast lijken jongeren die geen delicten plegen minder vaak te socialiseren met delinquente vrienden of mensen die delictgedrag goedkeuren.

De vragenlijst biedt verder inzicht in factoren die delictplegers in de risicogroep kunnen onderscheiden van jongeren in de risicogroep die nog geen delicten hebben gepleegd. Wat opvalt is dat deze jongeren in veel opzichten op elkaar lijken, maar dat delictplegers in het algemeen meer vaardigheden hebben en een nog sterkere interesse vertonen voor computers. Zo scoren ze hoger op IT-skills, spenderen meer tijd aan programmeren en hebben veel vaker werk in IT. In andere woorden, hoe meer jongeren zich bezighouden met computers en technologie in de levensloop, hoe groter de kans dat zij ooit strafbaar gedrag vertonen. Wat daarnaast ook in het bijzonder een risico lijkt te vormen zijn factoren die zich manifesteren in de familiesfeer. Zo hebben daders een gebrek aan ouderlijk toezicht online en zijn ze vaker getuige geweest van geweld tussen ouders. Ten slotte onderscheiden delictplegers in de risicogroep zich door meer blootstelling aan offline en online

antisociale invloeden vergeleken met jongeren die geen delicten hebben gepleegd.

5.6. Wat zijn beschermende factoren die kunnen voorkomen dat jongeren met een hoge affiniteit voor IT betrokken raken bij cybercriminaliteit?

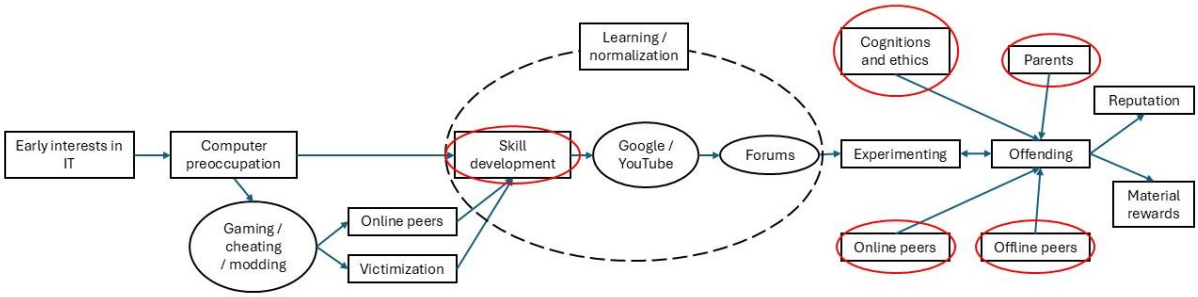
Er is nog weinig bekend over beschermende factoren voor het plegen van online criminaliteit. In het algemeen geldt dat determinanten die een rol spelen bij delictgedrag bipolaire effecten laten zien met zowel een risicofunctie als beschermende functie afhankelijk van de plek op de schaal (Loeber et al., 2016). Dat betekent dan het andere uiterste van een risicofactor mogelijk beschouwd kan worden als een beschermende factor. Uit de verkennende interviews die zijn gevoerd voor dit onderzoek komen een aantal mogelijke factoren aan bod. Ten eerste lijken ouders een beschermende rol te spelen. Respondenten geven aan dat ze thuis open kunnen praten over programmeren, Minecraft of Roblox. Ouders van respondenten tonen interesse en stimuleren hun kinderen om laten zien wat ze online doen, wat de band kan versterken en gesprekken over online activiteiten kan bevorderen. Een goede balans tussen toezicht en vertrouwen lijkt daarbij belangrijk, waarbij jongeren voldoende uitgedaagd worden in een gecontroleerde omgeving. Wanneer jongeren toch grenzen overschrijden, is het belangrijk dat ouders dat gedrag begrenzen en de redenatie daarachter uitleggen. Ten tweede kunnen ook leeftijdsgenoten een bron zijn van prosociale normen en waarden met een mogelijk beschermende invloed. Zo lijken jongeren die geen delicten plegen over het algemeen weinig vrienden te hebben die betrokken zijn bij (cyber)criminaliteit, of delen überhaupt geen interesse in computers. Duidelijk is dat het sociale leven van deze jongeren zich grotendeels online afspeelt, met name op Discord, waar ze vriendschappen onderhouden en contact hebben met leeftijdsgenoten. Dat gaat over het algemeen over dagelijkse onderwerpen. Ook uit de vragenlijst blijkt dat blootstelling aan antisociale vrienden een onderscheidende factor is tussen daders en niet-daders in de risicogroep.

5.7. Conclusie

Op basis van het onderzoek kan geconcludeerd worden dat de ontwikkelpaden van jonge potentiële hackers worden gekenmerkt door een sterke inbedding in de digitale omgeving. Vroege interesses en ervaringen manifesteren zich vaak in de context van gaming en programmeren, waarbij jongeren vaardigheden leren via platformen zoals Discord en YouTube en daar ook socialiseren met leeftijdsgenoten. Enerzijds is dat een bron van prosociale invloeden, maar jongeren lopen ook het risico op blootstelling aan meer deviante online omgevingen die delictgedrag kunnen aanwakkeren. Het is de vraag waarom sommige risicojongeren delicten plegen en anderen niet. Als we de interviews met de risicogroep vergelijken met de resultaten van de interviews met criminele hackers lijken niet-criminele hackers zich met name op drie manieren te onderscheiden: 1) een sterker gevoel voor ethische grenzen en hogere risicoperceptie, 2) meer transparantie en controle vanuit ouders, 3) in sommige gevallen een gebrek aan antisociale invloeden online en offline. Uit dit onderzoek blijkt

verder dat jongeren die later risico lopen om betrokken te raken bij cybercriminaliteit mogelijk herkend kunnen worden door hoge IT-vaardigheden, meer online ontremming, slechtere schoolprestaties, minder betrokkenheid, openheid en toezicht vanuit ouders en meer blootstelling aan risicovolle omgevingen op internet. Wat daarbij ook een rol lijkt te spelen is moraliteit en hoe jongeren denken over online gedrag. Dit proces kan beïnvloed worden door rolmodellen, ouders, op scholen en via platformen zoals YouTube. Technische interesse op zichzelf vormt dus niet persé een risico, maar is vooral afhankelijk van individuele kenmerken in combinatie met de context waarin vaardigheden worden ontwikkeld. Wel lijkt het zo dat hoe sterker de preoccupatie met computers is, hoe hoger het risico op delictgedrag; jongeren die initiële interesses bijvoorbeeld omzetten in een (bij)baan zijn ook vaker betrokken bij cybercriminaliteit, mogelijk als onderdeel van een experimentele fase. De voornaamste punten waarop criminele hackers verschillen van niet-criminele hackers zijn weergegeven in het schematische ontwikkelpad van Leukfeldt en Bekkers (2026).

Figuur 2. Voornaamste gebieden waarop niet-criminele hackers verschillen van criminele hackers



Daderpreventie en vroegsignalering vraagt daarmee om een multidisciplinaire benadering met betrokkenheid van bijvoorbeeld scholen, ouders en politie, waarbij aandacht is voor ethiek en positieve begeleiding. Een aantal punten vragen ook om vervolgonderzoek. Om te beginnen is dat de rol van YouTube en andere online platformen: enerzijds leren jongeren via YouTube illegale toepassingen van hacken, anderzijds leren ze ook over ethische grenzen en regels met betrekking tot online gedrag. Het is daarom de vraag hoe dat samengaat en hoe YouTube en andere platformen ingezet kunnen worden in het kader van preventie en voorlichting. Een andere kwestie is de rol van initiatieven die zijn gericht op de begeleiding van jongeren met talent op het gebied van IT. Bij adequate begeleiding door een prosociale mentor zijn dit soort initiatieven mogelijk beschermend en kan het jongeren helpen op het rechte pad te blijven. Er is echter ook sprake van een potentieel risico, aangezien jongeren elkaar ook negatief kunnen beïnvloeden. Er is daarom meer onderzoek nodig naar de uitkomsten van omgevingen die functioneren als een soort “learning communities” voor jonge hackers en de randvoorwaarden voor positieve effecten.

Referenties

Akkermans, M., Derksen, E., Kennis, M., Kloosterman, R., & Moons, E. (2024). *Veiligheidsmonitor 2023*. Statistics Netherlands. https://www.cbs.nl/nl-nl/longread/rapportages/2024/veiligheidsmonitor-2023/5-online-criminaliteit

Bekkers, L. M. J., Holt, T. J., & Leukfeldt, E. R. (2025b). Exploring the factors that differentiate individual and group offenders in cyber-dependent crime. *Journal of Criminal Justice*, *101*, 102522.

Bekkers, L., Holt, T., & Leukfeldt, R. (2025c). Online gaming as a criminological environment: exploring criminogenic needs and offending behaviors of gamers. *Journal of Criminal Psychology*.

Bekkers, L., & Leukfeldt, R. (2025). Specialization in cybercrime and offense versatility during early adolescence and the role of criminogenic needs. *Crime, Law and Social Change*, *83*(1), 1-21.

Bekkers, L. M., Moneva, A., & Leukfeldt, E. R. (2025a). Distinct group, distinct traits? A comparison of risk factors across cybercrime offenders, traditional offenders and non-offenders. *Psychiatry, Psychology and Law*, 1-25.

Bonta, J., & Andrews, D. A. (2023). *The psychology of criminal conduct* (6th ed.). Taylor & Francis.

Borwell, J., Jansen, J., & Stol, W. (2025). Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. *International Review of Victimology*, *31*(1), 156-181.

Bossler, A. M., & Burruss, G. (2011). The general theory of crime and computer hacking: Low self control hackers? In T. J. Holt & B. H. Schell (Red.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 38-67). IGI Global

Eurobarometer. (2022). *SMEs and Cybercrime.* https://europa.eu/eurobarometer/surveys/detail/2280

Fox, B., & Holt, T. J. (2021). Use of a multitheoretic model to understand and classify juvenile computer hacking behavior. *Criminal Justice and Behavior*, *48*(7), 943-963.

Harvey, I., Bolgan, S., Mosca, D., McLean, C., & Rusconi, E. (2016). Systemizers are better code breakers: Self-reported systemizing predicts code-breaking performance in expert hackers and naïve participants. *Frontiers in Human Neuroscience*.

Hendriks, J., & Stam, G. J. (2024). Landelijk Kwaliteitskader Effectieve Jeugdinterventies voor Preventie van Jeugdcriminaliteit.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant behavior*, *35*(1), 20-40.

Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice*, *37*(3), 378-395.

Hu, Q., Xu, Z., & Yayla, A. A. (2013). Why college students commit computer hacks: Insights from a cross culture analysis. *Pacific Asia Conference on Information Systems (PACIS) 2013 Proceedings. 104*. https://aisel.aisnet.org/pacis2013/104

Hu, Q., Zhang, C., & Xu, Z. (2012). Moral beliefs, self-control, and sports: Effective antidotes to the youth computer hacking epidemic. *2012 45th Hawaii International Conference on System Sciences*, 3061-3070.

Hutchings, A. (2013). *Theory and crime: Does it compute?* [PhD Thesis, Griffith University]. https://research-repository.griffith.edu.au/handle/10072/365227

Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, *62*(1), 1-20.

Leukfeldt, E. R., & Bekkers, L. M. J. (2026). From curiosity to crime: Exploring pathways into criminal hacking. *Computers in Human Behavior*, 108996.

Loggen, J., Moneva, A., & Leukfeldt, R. (2024). Pathways into, desistance from, and risk factors related to cyber-dependent crime: A systematic narrative review. *Victims & Offenders*, 1-32.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behavior*, *35*(7), 581-591.

Martineau, M., Spiridon, E., & Aiken, M. (2024). Pathways to criminal hacking: Connecting lived experiences with theoretical explanations. *Forensic Sciences*, *4*(4), 647-668.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*, 1-35.

National Crime Agency. (2017). *Pathways into cyber crime*. National Crime Agency.

Noordegraaf, J. E., & Weulen Kranenbarg, M. (2023). Why do young people start and continue with ethical hacking? A qualitative study on individual and social aspects in the lives of ethical hackers. Criminology & Public Policy, 22(4), 803-824.

Paquet-Clouston, M. C. (2021). The role of informal workers in online economic crime[PhD Thesis]. Simon Fraser University.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, *2*(2), 379-398.

Schell, B. H., & Melnychuk, J. (2011). Female and male hacker conferences attendees: Their autism spectrum quotient (aq) scores and self-reported adulthood experiences. In T. J. Holt &

B. H. Schell (Red.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 144-169). Business Science Reference.

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J. L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, *40*(1), 40-55.

Weulen Kranenbarg, M., Ruiter, S., Van Gelder, J. L., & Bernasco, W. (2018). Cyber-offending and traditional offending over the life-course: An empirical comparison. *Journal of developmental and life-course criminology*, *4*(3), 343-364.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management*, *24*(4), 281-287.