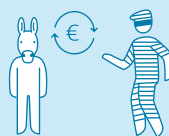


PRAATPLAAT

Ondermijning

Via Instagram krijgt Mees hulp aangeboden voor zijn schulden. Wat een uitweg lijkt, blijkt een val: zijn bankrekening wordt gebruikt voor criminele geldstromen. Mees is nu een zogeheten 'geldezel' en is zo onderdeel van een witwasproces van een criminele organisatie.



Sociaal domein



Milo, met een licht verstandelijke beperking, denkt online een relatie aan te gaan. Hij leent geld uit voor haar auto, maar wordt misleid en financieel uitgebuit. De vrouw blijkt niet te bestaan.

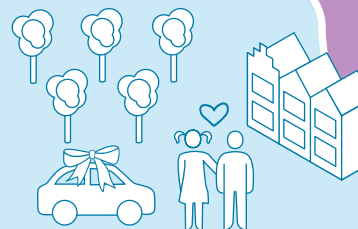
Online criminaliteit raakt iedereen

Online dreigingen hebben impact op inwoners én op het werk van gemeenten. Om te laten zien dat online veiligheid alle domeinen raakt, vind je hier voorbeelden uit de dagelijkse praktijk. Ga aan de hand van deze praatplaat het gesprek met elkaar aan.

Jeugd



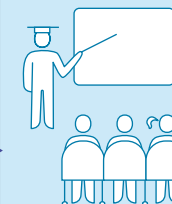
Laura (14) scrollt uren op TikTok en droomt van een luxe leven. Ze ontvangt een bericht over de 'f-game' en gaat online fraude plegen. Het lijkt onschuldig, tot ze bedreigd wordt door het netwerk waar ze in beland is. Ondertussen wordt klasgenoot Yasmine (13) stelselmatig online gepest. Via een groepschat wordt ze uitgescholden en bedreigd. Op school lijkt er niks aan de hand.



Onderwijs



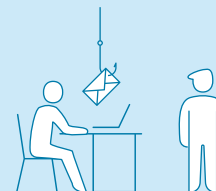
Tijdens een les over digitale vaardigheden leert Ibrahim kritisch kijken naar online informatie. Hij demonstreert trots hoe hij deepfake-video's kan maken en laat zien dat hij toegang kan krijgen tot het schoolsysteem.



Burgercontact



Anne werkt als schuldhelpverlener. Zij ziet steeds meer jongeren met schulden en geblokkeerde rekeningen. Anne begrijpt niet hoe deze toename is ontstaan. Ze belt de gemeente. De balie medewerkers herkennen de signalen van geldezels en schakelen direct met de juiste afdeling.

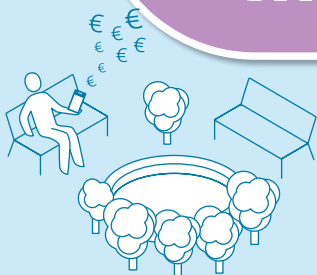


Denk ook aan Communicatie

Digitale veiligheid



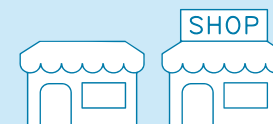
Jan ontvangt een WhatsApp-bericht van zijn 'dochter' die dringend geld nodig heeft. Hij maakt 500 euro over, maar beseft al snel dat het oplichting is. Uit schaamte zwijgt hij. In de gemeente blijken meerdere inwoners slachtoffer van deze vorm van online fraude.



Economie



Lokale ondernemer Ben krijgt een dreigmail: zijn gestolen klantgegevens worden gepubliceerd tenzij hij betaalt. Uit angst voor imago schade houdt hij het stil, maar het risico voor anderen blijft groot.



Ga in gesprek

- Herken jij deze praktijkvoorbeelden ook vanuit je eigen werk?
- Welke verantwoordelijkheid neem jij als je een soortgelijk voorbeeld in de praktijk tegenkomt?
- Welke andere vormen van online criminaliteit kom jij in de praktijk tegen?
- Wat is volgens jou de rol van de gemeente in het voorkomen of aanpakken van online criminaliteit?
- Op welke initiatieven kun je aanhaken om dit praktijkvoorbeeld te signaleren en preventief te handelen?
- Hoe kan de gemeente ervoor zorgen dat alle afdelingen op de hoogte zijn van signalen van online criminaliteit en gezamenlijk actie ondernemen?



Denk ook aan CISO
(Chief Information Security Officer)



“Digitale veiligheid is als een satéprikker die alles met elkaar verbindt. Het moet door alle beleidsterreinen heen zichtbaar en voelbaar zijn.”

Voorwoord →

Digitale veiligheid →

Ondermijning →

Jeugd →

Onderwijs →

Sociaal domein →

Economische zaken →

Overige afdelingen →

Voorwoord

Digitale veiligheid is een thema dat alle gemeentelijke beleidsterreinen raakt – van jeugdbeleid en onderwijs tot zorg, economie en het sociaal domein. Deze praatplaat én de bijbehorende pagina's zijn ontwikkeld om gemeenten te ondersteunen bij het voeren van het gesprek over digitale veiligheid. Ze bieden per afdeling of thema praktische informatie en relevante vragen die helpen om de samenwerking – zowel intern als extern – te verbeteren. Dit document is bedoeld als uitnodiging aan beleidsmedewerkers en samenwerkingspartners: ga met elkaar in gesprek over hoe we digitale veiligheid duurzaam kunnen borgen – voor alle inwoners.

Samen werken aan digitale veiligheid

Onze samenleving digitaliseert in rap tempo. Inwoners doen steeds meer online – van bankzaken tot sociale contacten – en mogen verwachten dat ze zich daarin net zo veilig voelen als in de fysieke wereld. Toch is digitale veiligheid nog niet vanzelfsprekend verankerd in gemeentelijk beleid. Vaak wordt het onderwerp vooral bij de afdeling Openbare Orde en Veiligheid belegd, terwijl het juist een brede aanpak vereist. Om inwoners écht te kunnen beschermen en ondersteunen, is samenwerking nodig. Niet alleen tussen afdelingen binnen de gemeente, maar ook met externe partners. Digitale veiligheid vraagt om een structurele en geïntegreerde aanpak. Dat kan met deze praatplaat.

Werkwijze praatplaat



Achtergrondinformatie: Elk hoofdstuk geeft inzicht in wat er speelt rondom cybercrime en gedigitaliseerde criminaliteit binnen de betreffende afdeling of het thema. Hoewel de informatie niet volledig is, biedt het wel goede handvatten om het gesprek te starten en toe te werken naar een gezamenlijke, integrale aanpak van digitale veiligheid.



Tips: De genoemde tips geven een praktisch handelingsperspectief.



Partners: Bij elk hoofdstuk worden relevante partners genoemd. Zij kunnen een belangrijke rol spelen in het signaleren van problemen en het gezamenlijk uitvoeren van interventies. Ga met hen in gesprek, luister naar hun ervaringen en verken samen de mogelijkheden. Wees nieuwsgierig en kritisch.



Meer informatie: Er wordt verwezen naar websites, onderzoeken en inspirerende praktijkvoorbeelden. Gebruik deze bronnen om je kennis te verdiepen en ideeën op te doen.



Vragen: De vragen zijn bedoeld als gespreksstarter – zowel binnen de gemeente als met externe partners. Ze helpen om het onderwerp op de kaart te zetten en om collega's en partners bewust te maken van de impact van digitalisering. De vragen kunnen ook duidelijk maken wat jij voor anderen kunt betekenen.

Heb je nog vragen over deze praatplaat of dit onderwerp? Neem contact op met CCV-adviseur [Doris van Rooijen](#).





Digitale veiligheid

In een tijd waarin digitale technologieën een integraal onderdeel zijn van ons dagelijks leven, is het versterken van de cyberweerbaarheid essentieel voor het waarborgen van de openbare orde en veiligheid. Als regisseur van lokale veiligheid brengt de afdeling Openbare Orde en Veiligheid verschillende partijen samen om haar inwoners en bedrijven weerbaar te maken tegen online criminaliteit.

Achtergrondinformatie

Online criminaliteit komt voor in verschillende vormen:

- **Cybercrime:** delicten die zich richten op ICT (Informatie- en Communicatie Technologie). Denk hierbij aan het hacken van een account of apparaat of aan het plegen van een DDOS-aanval. Met als doel bijvoorbeeld een computer over te nemen, het netwerk plat te leggen of gegevens te stelen. En het wordt criminelen steeds makkelijker gemaakt met 'cybercrime as a service'. Dit is een model waarbij criminelen digitale tools en diensten aanbieden om cybercriminaliteit te plegen. Het maakt het voor mensen zonder technische kennis mogelijk om aanvallen uit te voeren, zoals malware, ransomware en DDOS-aanvallen. Dit vergroot de toegankelijkheid en het gevaar van cybercriminaliteit.
- **Gedigitaliseerde criminaliteit:** delicten die buiten de digitale wereld ook plaats vinden. Denk bijvoorbeeld aan oplichting door middel van babbeltrucs of verkoopfraude. Voorbeelden hiervan zijn: WhatsApp-fraude, marktplaatsfraude of digitale stalking. Het doel is geld verkrijgen of invloed op mensen uitoefenen.

[Het Cybercrimebeeld 2024](#) geeft een beeld van de wereldwijde omvang van cybercrime:

- Het cybercrimelandschap is complex
- Zorgwekkend aandeel jonge cybercrimeverdachten
- Opkomst van datadiefstal en -handel om tot afpersing over te gaan
- Vermenging van traditionele criminaliteit
- Nederland als host van criminele infrastructuur
- Impact op slachtoffer wordt onderschat
- Brede bestrijding is noodzakelijk voor een effectieve aanpak van cybercrime.

De gemeente heeft een belangrijke taak in het weerbaar maken van haar inwoners en ondernemers. De gemeente kan een goede basis leggen door verschillende dingen te doen:

- **Borging in het gemeentelijk veiligheidsbeleid.** Het is van cruciaal belang om cyberveiligheid als een integraal onderdeel van het gemeentelijke veiligheidsbeleid te beschouwen. Dit zorgt ervoor dat de inspanningen om cybercriminaliteit aan te pakken, geïntegreerd zijn in de bredere strategie van de gemeente.
- **Maak gebruik van bestaande middelen.** Gemeenten kunnen gebruikmaken van de beschikbare tools en hulpmiddelen om hun digitale veiligheid te versterken. Bekijk de [Database Lokale Cyberprojecten](#) op de website van het CCV.
- **Werk samen.** Gebruik hiervoor bestaande samenwerkingsverbanden om het onderwerp aan te jagen, van elkaar te leren en signalen te ontvangen. Binnen de organisatie kan tijdens elk teamoverleg worden aangesloten. Maar ook buiten de organisatie zijn vele kansen. De regioaanjager heeft een goede positie en kan helpen om de juiste partijen te verbinden, het thema aan te jagen en te koppelen aan structurele overleggen (zoals bij de cybersubdriehoek).
- **Blijf op de hoogte.** OOV'ers kunnen zich door zowel het CCV als de VNG geregeld bij laten praten over de laatste ontwikkelingen en bedreigingen in het digitale landschap.

Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein



Economische zaken



Overige afdelingen





Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein



Economische zaken



Overige afdelingen



Cyberwegenkaart

Om gemeenten te helpen, onderscheidt het CCV vier wegen waarop je als gemeente actie moet ondernemen om een cyberweerbare gemeente te worden. De vier wegen zijn:

1. **Eigen huis op orde:** verantwoordelijkheid nemen voor het goed functioneren van de eigen digitale systemen.
2. **Cyberincidenten en cybercrises:** voorbereid zijn.
3. **Cybercrime en gedigitaliseerde criminaliteit:** weerbaar maken van bewoners en ondernemers.
4. **Online aangejaagde ordeverstoring:** goed zicht hebben op onrechtmatige activiteiten die online afspelen en daarmee fysieke ordeverstoringen voorkomen.

In de beschrijvingen van deze vier wegen wordt duidelijk welke rol de gemeente kan nemen, welke gevaren er op de weg zijn en waar de gemeente hulp (de zogenoemde wegwacht) kan invoeren. Er is geen volgorde in het nemen van deze vier wegen. Elke weg kan afzonderlijk en naast elkaar genomen worden.



Partners

- Regioaanjager
- VNG
- CCV
- Regionale samenwerkingsverbanden (vraag hiernaar bij jouw regioaanjager)
- Andere (buur)gemeenten
- Lokale partijen zoals bibliotheken, onderwijs, buurthuizen.



Tips

- Gebruik dit document om de andere afdelingen te betrekken op dit onderwerp; met hun netwerk kan eerder gesignaleerd en preventief gehandeld worden!
- Maak een plan van aanpak om het thema van beleid naar praktijk te brengen: betrek partners, buurgemeenten en bestaande structuren en leg deze afspraken vast.
- Richt een werkgroep binnen de gemeente op met een vertegenwoordiger van (zoveel mogelijk) andere beleidsterreinen.



Meer informatie

- [Beleid cyberweerbaarheid - Het CCV](#)
- [Database Lokale Cyberprojecten - Het CCV](#)
- [Focusblad Digitale Veiligheid - VNG](#)
- [Wegwijzen domeinoverstijgend samenwerken binnen gemeenten - VNG](#)



Vragen

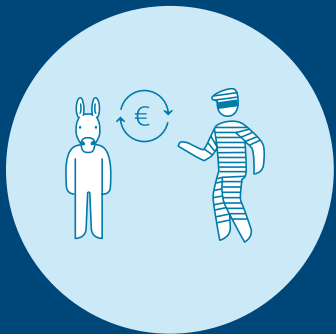
- Op welke manier wordt het onderdeel cyber van het integraal veiligheidsplan uitgevoerd binnen de gemeente?
- Wat heb je nodig om hier betere uitvoering aan te geven?
- Op welke manier kan jij andere afdelingen en partners betrekken om de samenwerking te versterken?
- Welke signalen ontvang je van andere afdelingen en partners op het thema cyberveiligheid?
- Welke acties onderneem je op basis van deze signalen?
- Welke aanvullende handelingsperspectieven en kennis zijn nodig voor professionals, zowel binnen als buiten de organisatie?



1

2





Ondermijning

Voor een succesvol bedrijfsproces en verdienmodel, maken criminelen gebruik van diensten van legale bedrijven en dienstverleners. Zo raken de onder- en bovenwereld met elkaar vermengd. Dat wordt ook wel ondermijning genoemd. Ook binnen het thema ondermijning speelt digitale veiligheid een steeds grotere rol.

Achtergrondinformatie

Uit het [Cybercrimebeeld 2024](#) blijkt dat er een toenemende vermenging is van de online en de fysieke wereld in de criminaliteit, waaronder de vermenging van cybercrime en ondermijning. De online omgeving wordt enerzijds gebruikt als middel voor contacten en verkoop van bijvoorbeeld drugs en tools om online criminaliteit eenvoudig uit te kunnen voeren (cybercrime as a service). Anderzijds plegen veel individuen binnen het criminele netwerk gedigitaliseerde of cybercriminaliteit en is er een toename van wapen- en explosievenbezit onder cybercriminelen.

Zo zijn *phishing* en online fraude manieren om anoniem, snel geld te verdienen. En onder jongeren is vooral de 'fraude-game' erg populair. Deze jongeren zijn vaak onderdeel van een groter crimineel netwerk die deze winsten beheert en de jongeren ook klussen geeft, zoals het leveren van drugspakketten of containers legen in de haven. Tot slot wordt de online omgeving gebruikt voor intimidatie, afpersing en bedreiging, als gevolg van (offline) ondermijnende activiteiten.

Geldezels

Een ander fenomeen dat gelinkt wordt met ondermijning zijn de geldezels. Geldezels laten hun bankrekening gebruiken om geld van criminelen naar iemand anders over te maken of wit te wassen. Op deze manier zijn zij onderdeel van een groter crimineel netwerk en onderdeel van de ondermijning. Geldezels worden vaak geronseld via bijvoorbeeld Snapchat, Telegram of via vacatures. De online omgeving is dus een middel om te communiceren en snel in contact te komen met criminele netwerken.



Tips

- Betrek ook de afdeling digitale veiligheid bij dit fenomeen; welke signalen ontvangen zij en op welke manier kan hier gericht op geacteerd worden?
- Betrek de digitale teams van bijvoorbeeld jongerenwerk en de politie bij dit thema.



Partners

- Zorg: slachtofferhulp, schuldhulpverlening
- Veiligheid: Politie, RIEC, FIOD, OM
- Sociaal: jongerenwerkers, straatcoaches, scholen, sociale dienst
- Bedrijven: DNB, AFM, banken



Meer informatie

- [Online ondermijning - RIEC](#)
- [Geldezels aanpak - Het CCV](#)
- [Het ontrafelen en integraal aanpakken van een cybercrimineel jeugdnetwerk - Boomportaal](#)

Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein

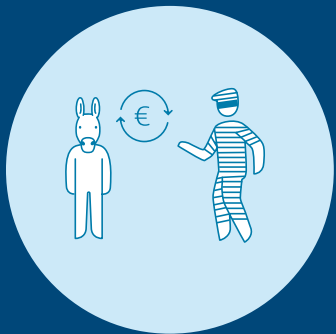


Economische zaken



Overige afdelingen





Ondermijning



Vragen

- Welke concrete signalen van online criminaliteit en ondermijning komen bij jouw afdeling binnen?
- Welke actie onderneem jij op basis van deze signalen?
- In hoeverre betrek je collega's binnen de gemeente bij de signalen die jij ontvangt?
- Welke kwetsbare groepen in jouw werkgebied lopen een verhoogd risico om online betrokken te raken bij ondermijnende criminaliteit?
- In hoeverre hebben jij en je partners zicht op het online gedrag van doelgroepen die vatbaar zijn voor ondermijning?
- In hoeverre zijn partners zich bewust van de rol van de online wereld in ondermijning – en hebben zij handelingsperspectief om daarmee om te gaan?
- In hoeverre zijn partners actief bezig met het risico en de gevolgen van online criminaliteit voor jongeren of andere risicogroepen binnen het thema ondermijning?
- Op welke manier kan jij hen hierin ondersteunen?

Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein



Economische zaken



Overige afdelingen



1

2





Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein



Economische zaken



Overige afdelingen



Jeugd

Bij de afdeling jeugd speelt er veel op het gebied van cyberveiligheid. Aan de hand van de thema's gezondheid en welzijn, slachtofferschap en ouderschap geven we je achtergrondinformatie om goed beslagen het gesprek aan te kunnen gaan met deze afdeling.

Gezondheid en welzijn

Achtergrondinformatie

Aangezien jongeren veel tijd online besteden, is het van belang dat ze ook in deze online leefwereld worden beschermd.

De leefwereld van jongeren speelt zich voor een groot deel af op het internet waardoor het impact heeft op de ontwikkeling. Dit kan positief zijn; jongeren kunnen op een laagdrempelige manier contacten leggen, nieuwe kennis opdoen of nieuwe hobby's ontwikkelen. Zo gebruikt een deel van de jeugd het internet om zichzelf te ontdekken en ontwikkelen. Het is een verlengstuk van hun offline leven.

Aan de andere kant brengt het ook risico's met zich mee.

- Gevolgen kunnen zijn: angst, depressie en slaapproblemen.
- Jongeren kunnen ook slachtoffer worden van verschillende vormen van online ongewenst gedrag (zoals online pesten, sextortion, online bedreigingen en blootstelling aan ongewenste content).

Het is daarom van belang om jongeren te begeleiden in hoe zij veilig en verantwoord internet en sociale media kunnen gebruiken. Behoud de nieuwsgierigheid maar zorg dat zij zich bewust zijn van de risico's, net zoals in de fysieke wereld.



Tips

- Voer gesprekken met partners zoals jeugdwerkers, onderwijs, en buurtcentra om het onderwerp aan te jagen.
- Leg partners uit wat hun rol is: vroegsignalering en schakelen met partners die mogelijk invloed hebben. Denk aan ouders, jeugdwerkers en leraren.
- Haal signalen op waar knelpunten worden ervaren; op welke manier kan de gemeente ondersteuning bieden in de vorm van interventies/voorlichting?
- Bied de partners tools aan: HelpWanted is een Trusted Flagger voor onwenselijke online gedragingen.



Partners

- Sociaal: onderwijs, buurtcentra, BSO, jongerenwerkers
- Veiligheid: wijkagenten, Halt, Zorg- en Veiligheidshuizen, jeugdzorg
- Zorg: jeugdzorginstellingen, centrum seksueel geweld, huisarts, slachtofferhulpNL, instellingen en begeleiders (zoals LVB)
- Bedrijven: HelpWanted, mediawijsheid



Meer informatie

- [Trendanalyse Digitalisering en het welzijn van jonge mensen - VNC](#)
- [Rapport over online gedrag onder jongeren - NHL Stenden](#)
- [Jongeren online: het is net de echte wereld - Sociale stabiliteit](#)
- [Online grensoverschrijdend gedrag - HelpWanted](#)





Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein



Economische zaken



Overige afdelingen



Slachtofferschap en daderschap

Achtergrondinformatie

Slachtofferschap

Jongeren spenderen veel tijd op het internet, waardoor er een grotere kans is dat zij slachtoffer worden van online delicten. Voorbeelden van deze delicten zijn hacken en *phishing*. In recent [onderzoek](#) van Scholieren.com (2024) zijn jongeren door middel van een vragenlijst bevraagd over online oplichting en veiligheid. Uit het onderzoek komt onder andere naar voren dat aan- en verkoopfraude nog steeds de meest voorkomende vorm van online fraude is onder scholieren. Verder vinden veel scholieren dat het niet je eigen schuld is als je slachtoffer wordt van online fraude, maar wanneer zij zelf slachtoffer worden zou een groot deel zich wel schamen.

*20% van de 15- tot 25-jarigen is wel eens
slachtoffer geworden van online criminaliteit.
Daarvan was 8,6% slachtoffer van online
oplichting en fraude en 8,5% van hacken.*

De online wereld biedt kansen, zoals sociale contacten en het verbeteren van digitale vaardigheden, maar er zijn ook risico's (cyberbullying, sextortion, phishing) voor jongeren zo stelt het [NJI](#). De gemeente kan een rol spelen in het cyberweerbaar en digitaal bewust maken van de nieuwe generatie.

Daderschap

Uit de Monitor Zelf gerapporteerde Jeugdcriminaliteit (MZJ) 2020 blijkt dat 19,5% van de jongeren een online delict heeft gepleegd. Jongeren vormen een steeds grotere groep onder de verdachten van online criminaliteit. Meer dan de helft van de cyberverdachten is jonger dan 25 jaar. Dat is deels te verklaren doordat jongeren digitaal vaardig zijn en veel tijd online doorbrengen. Hoe meer tijd online, hoe groter de kans dat ze in aanraking komen met online criminele netwerken – vaak via sociale media of chatgroepen op Telegram of Discord. Dit gebeurt niet alleen wanneer zij online geronseld worden; jongeren bieden zichzelf ook aan voor criminele klussen. In video's op sociale media zien zij veel geld voorbijkomen en lijkt het alsof criminaliteit loont.

Kant-en-klare online tools

Diensten, tools en kennis worden online verkocht; online criminaliteit plegen wordt zo laagdrempelig en door iedereen uitvoerbaar. Dankzij deze opkomende ontwikkeling 'cybercrime as a service', hebben jongeren geen technische kennis meer nodig om online delicten uit te voeren, zoals WhatsApp-fraude, phishing en het gebruik van gestolen bankgegevens.

De 'cyberbreinen': technisch vaardige jongeren met een uitdaging

Er is ook een groep jongeren met een sterke interesse in technologie, ICT of programmeren. Zij worden ook wel de 'cyberbreinen' genoemd. Vanuit nieuwsgierigheid of de drang om zichzelf uit te dagen beginnen zij met hacken of het omzeilen van systemen. Financieel gewin is voor deze groep vaak niet de belangrijkste motivatie. Toch kunnen ook zij – al dan niet onbewust – de grens van legaliteit overschrijden, en zo in het criminele circuit belanden.





Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein



Economische zaken



Overige afdelingen



Jongeren als dader én slachtoffer

Daderschap en slachtofferschap is binnen online criminaliteit niet zwart-wit. Jongeren worden soms geronseld, gemanipuleerd of verleid met beloftes van geld en status. Wanneer zij uit het circuit willen stappen, worden zij soms online bedreigd en onder druk gezet. Daarmee zijn ze niet alleen dader, maar ook slachtoffer. De aanpak vraagt dus niet alleen om repressie, maar juist ook om preventie, educatie en bewustwording – in de klas, op straat en online.



Tips

- **Onderwijs:** ga in gesprek met onderwijsinstellingen en maak duidelijk dat jullie actief zijn op digitale weerbaarheid.
- Haal signalen op over de ervaringen die jongeren online hebben. Neem hierbij ook de basisschool mee; criminaliteit start steeds vroeger.
- Signaleer mogelijkheden voor interventies op risico- en beschermende factoren: wat wordt er al gedaan bij jongeren om gewenst gedrag te stimuleren en op welke wijze kan het online component hier een rol in spelen?
- Benoem in structurele gesprekken met partners op het thema jeugd dat jullie ook bezig zijn met de online wereld. Wat zien zij en welke knelpunten ervaren zij?



Partners

- Sociaal: onderwijs, buurtcentra, BSO
- Veiligheid: wijkagenten, Halt, Zorg- en Veiligheidshuizen, jeugdzorg
- Zorg: jeugdzorginstellingen, huisarts, slachtofferhulpNL, instellingen en begeleiders (zoals LVB)
- Bedrijven: CodeAcademy, DIVD Academy, Stichting Cyberbreinen.nl, HackShield, FreeCodeCamp, VulnHUB, Centrum voor Veiligheid en Digitalisering, HelpWanted/OFFLimits



Meer informatie

- [Tech skills - Code academy](#)
- [Academy cybersecurity - DIVD academy](#)
- [Stichting Cyberbrein - Cyberbrein](#)
- [Routekaart samenwerken bij online jeugdcriminaliteit - Wegwijzer jeugd en veiligheid](#)
- [Onderzoek slachtoffers jeugd van scholieren.com - Slachtofferhulp](#)
- [Lessenreeks digitale weerbaarheid groep 7 en 8 - Mijn cyberrijbewijs](#)
- [Bekijk het kader voor het hoofdstuk Jeugd speciaal voor docenten en ouders](#)



Vragen

- Welke concrete signalen van online ongewenst gedrag/criminaliteit komen bij jouw afdeling binnen?
- Welke actie onderneem jij op basis van deze signalen?
- Waar ervaar jij knelpunten of mis jij handelingsperspectief?
- In hoeverre betrek je collega's binnen de gemeente bij de signalen die jij ontvangt?
- Welke kwetsbare groepen in jouw werkgebied lopen een verhoogd risico om negatieve gevolgen te ervaren door online ervaringen/betrokken te raken bij online criminaliteit?
- In hoeverre hebben jij en je partners zicht op het online gedrag van doelgroepen die vatbaar hiervoor zijn?
- In hoeverre zijn partners zich bewust van de rol van de online wereld op jongeren – en hebben zij handelingsperspectief om daarmee om te gaan?
- In hoeverre zijn partners actief bezig met het risico en de gevolgen van online ongewenst gedrag/criminaliteit voor jongeren?
- Op welke manier kan jij hen hierin ondersteunen?





Onderwijs

Binnen het onderwijs speelt digitale veiligheid een steeds grotere rol. De gemeente kan scholen ondersteunen bij thema's, zoals digitale geletterdheid, talentontwikkeling en het vergroten van het veiligheidsgevoel op school.

Achtergrondinformatie

Digitale geletterdheid onderwijs

Digitale geletterdheid gaat over goed kunnen omgaan met digitale technologie. Het gaat hierbij om verschillende dingen:

- Weten hoe digitale technologie werkt.
- Leren hoe je digitale middelen gebruikt.
- Snappen hoe je deze technologie op een slimme en veilige manier inzet.
- Kansen en risico's herkennen bij het gebruik van digitale middelen.

Leerlingen leren niet alleen wát technologie is, maar ook h^oe ze het gebruiken. Ze leren bijvoorbeeld hoe ze informatie op internet kunnen controleren: is het betrouwbaar of niet? Dit vraagt om kritisch nadenken en omgaan met situaties die niet altijd één duidelijk antwoord hebben. Digitale geletterdheid hoort bij de kerndoelen van het onderwijs. Dat betekent dat scholen verplicht zijn hier aandacht aan te besteden en dat de Inspectie dit controleert. Binnen dit vakgebied kunnen scholen ook lesgeven over digitale weerbaarheid – hoe je jezelf online beschermt tegen gevaren, zoals nepnieuws, online pesten of fraude.

Mediawijsheid

De Week van de Mediawijsheid biedt een uitstekende gelegenheid om extra aandacht te besteden aan online veiligheid. Door een flexibelere benadering van het curriculum te hanteren - waarbij gewerkt wordt met doelstellingen in plaats van een vaststaande methode - ontstaat er ruimte om deze belangrijke onderwerpen te integreren.

Themaweken om aan te sluiten:

- Week van de mediawijsheid
- Week van de veiligheid
- Cybersecuritymaand

Talentontwikkeling

Op school wordt veel aandacht besteed aan de ontwikkeling van kinderen. Er wordt gekeken naar wat een kind goed kan en waar zijn of haar talenten liggen. Daarbij is het belangrijk om ook te kijken naar hun digitale vaardigheden. Sommige kinderen en jongeren zijn geïnteresseerd in computers of programmeren. Hun nieuwsgierigheid kan uitgroeien tot een echt talent voor IT, zoals het bouwen van software of het begrijpen van systemen. Dit is natuurlijk iets positiefs, maar het kan ook risico's met zich meebrengen. Denk bijvoorbeeld aan het hacken van systemen. Deze jongeren – ook wel “cyberbreinen” genoemd – willen zichzelf graag blijven verbeteren en zoeken steeds naar iets nieuws om te leren of op te lossen. Daarom is het belangrijk dat scholen dit soort talenten op tijd herkennen. Als een school deze interesse opmerkt, kan het goede begeleiding bieden. IT-talent is een waardevolle competentie, net als sport, muziek of taal. Het is dus belangrijk dat ook dit talent wordt gezien, gestimuleerd én op een veilige manier wordt ontwikkeld.

Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein



Economische zaken



Overige afdelingen



1

2





Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein



Economische zaken



Overige afdelingen



Partners

- Sociaal: onderwijsinstellingen, scholen, BSO, SLO, PO-Raad
- Veiligheid: politie, OM, Halt
- Bedrijven: cybersecuritybedrijven, Codeacademy, DIVD Academy, Stichting Cyberbreinen.nl, HackShield, FreeCodeCamp, VulnHub.



Tips

- Benoem dat de gemeente ook actief is op digitale weerbaarheid in je gesprekken met partners (zoals onderwijs).
- Zoek bestaande structuren om aan te haken; digitale geletterdheid en themaweken worden uitgevoerd en hier kan het online component een rol spelen.
- Breng in kaart waar knelpunten worden ervaren en welke mogelijke interventies er zijn (vraag dit na bij je OOV'er cybercriminaliteit).
- Door een artikel in de nieuwsbrief voor ouders en informatieavonden kan er al een eerste stap worden gemaakt.



Meer informatie

- [Digitale geletterdheid - SLO](#)
- [Digitalisering in het onderwijs - Rijksoverheid](#)
- [Rapport online gedrag onder jongeren - NHL Stenden](#)
- [Nieuwe cyberbrein projecten - Het CCV](#)
- [Cyberbreinen - Cyberbrein](#)
- [Het herkennen van cyberbreinen - wegwijzer jeugd en veiligheid](#)

Slachtofferschap van online criminaliteit – voor meldingen voor docenten en ouders

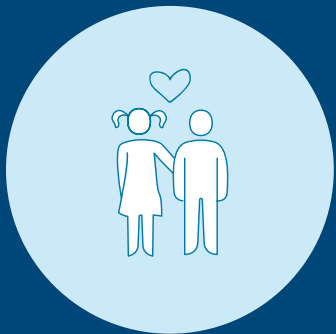
- [hulp of melding maken - www.meldknop.nl](#)
- [brochures veilig internetten - Veiliginternetten](#)
- [mediaopvoeding - Nederlands jeugdinstituut](#)
- [stop online grensoverschrijdend gedrag - offlimits.nl](#)
- [kindermisbruik - stopitnow.nl](#)
- [hulp bij grensoverschrijdend gedrag - helpwanted.nl](#)
- [seksueel kindermisbruik op internet - meldpunt-kinderporno](#)



Vragen

- Op welke manier zie jij online criminaliteit en digitale risico's terug in jouw onderwijsdossiers (bijvoorbeeld via meldingen vanuit scholen, jeugdzorg of politie)? Welke signalen ontvang je?
- Zijn er signalen binnen jouw gemeente dat jongeren digitaal zeer vaardig zijn, en hoe zou je deze groep op een positieve manier kunnen begeleiden of inzetten?
- Welke actie onderneem jij op basis van deze signalen?
- In hoeverre bespreek je bovenstaande signalen met jouw collega's binnen de gemeente?
- In hoeverre zijn jouw onderwijs- of samenwerkingspartners (zoals scholen, GGD, Halt, jongerenwerk) bewust van de risico's van online criminaliteit voor leerlingen?
- Zijn partners binnen het onderwijs voldoende toegerust en handelingsbekwaam om in te grijpen bij signalen van online criminaliteit of cyberonveiligheid bij jongeren?
- Hoe kun jij als gemeenteambtenaar scholen en andere partners ondersteunen in het herkennen én bespreekbaar maken van online risico's in de klas?
- Wordt er binnen jouw gemeente structureel aandacht besteed aan digitalisering, online veiligheid en weerbaarheid in themaweken of schoolcampagnes?





Sociaal domein

De maatschappij verandert door het toenemende gebruik van digitale middelen. Zo worden bankzaken, inschrijvingen voor woningen en belasting online geregeld. Het is dus belangrijk dat elke inwoner mee kan komen met deze digitalisering. De gemeente kan in samenwerking met partners zorgen dat jong, oud, laaggeletterden en mensen met een licht verstandelijke beperking op een veilige manier verder groeien in de digitale ontwikkelingen.

Achtergrondinformatie

Ongelijkheid neemt toe

Internet kan bestaande ongelijkheden versterken, zo blijkt uit het [trendrapport digitale inclusie](#). Ouderen, laagopgeleiden, mensen met een lager inkomen en mensen met een beperkte geletterdheid profiteren minder van de mogelijkheden die de online wereld te bieden heeft en zijn minder goed in staat eventuele gevaren af te wenden. De toenemende digitalisering brengt het risico met zich mee dat ongelijkheid en afstand tot de samenleving toenemen.

Basisvaardigheden

Digitale basisvaardigheden zijn van belang om deel te kunnen nemen aan de maatschappij, maar zijn ook van belang om slachtofferschap te kunnen voorkomen, dat blijkt uit cijfers van [veiliginternetten](#). 11% van de ouderen blijkt gedupeerd te zijn door online oplichting en 81% van de ouderen is bang om slachtoffer te worden van online oplichting. Bovendien blijkt dat een derde last van gevoelens van schaamte heeft als het hen overkomt.

Risico's

Ouderen geven vaak aan dat ze risico's zien in het gebruik van digitale tools, zoals apps. Deze angst kan een drempel vormen, waardoor mensen de tools niet durven of niet meer willen gebruiken. Toch is het belangrijk dat iedereen mee kan doen binnen de samenleving.

Digitale vaardigheden dragen bij aan het vergroten van digitale veerkracht en weerbaarheid bij kwetsbare groepen.

Licht verstandelijk beperkten

In Nederland vallen zo'n één miljoen mensen onder de groep met een licht verstandelijke beperking (LVB), zo blijkt uit [onderzoek](#). Een deel van deze mensen is extra kwetsbaar voor misleiding, uitbuiting en misbruik. Steeds vaker wordt deze doelgroep genoemd als risicogroep binnen de wereld van online criminaliteit. Zo worden mensen met een LVb regelmatig geronseld als geldezel of ingezet bij het plegen van (online) strafbare feiten. Ook lopen zij een verhoogd risico om slachtoffer te worden van bijvoorbeeld online fraude, datingfraude en phishing. Het is daarom van groot belang dat zorg- en veiligheidspartners weten hoe ze signalen kunnen herkennen. Binnen de fysieke grenzen worden mensen met een LVb beschermd of proberen we dat, echter ontbreekt deze bescherming in de online omgeving.

Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein



Economische zaken



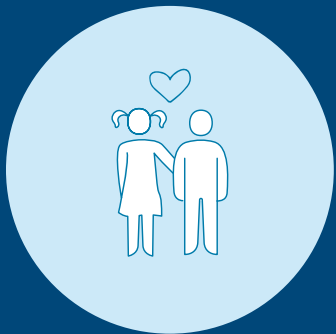
Overige afdelingen



1

2





Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein



Economische zaken



Overige afdelingen



Tips

- Sluit aan bij initiatieven van bibliotheken en buurthuizen, zoals taallessen of mediavaardigheden lessen.
- Praat je partners bij over de mogelijke risico's voor de doelgroep, zoals ouderenzorg of wijkzorg.
- Maak het een vast onderdeel van de vragen die je met je partners bespreekt en koppel dit terug bij je OOV'er die op het thema actief is.
- Er zijn verschillende initiatieven waar digitale vaardigheden kunnen worden geïntegreerd. Denk bijvoorbeeld aan taallessen en bijeenkomsten in de bibliotheek.



Partners

- Zorg: wijkzorg, (LVB)-begeleiders, woonbegeleiders, tehuizen, slachtofferhulp, zorgboerderijen
- Sociaal: ouderenzorg, buurthuizen, bibliotheken, kerken
- Veiligheid: politie, digitaal wijkagent
- Bedrijven: Seniorweb, ouderenbond



Meer informatie

- [Werkagenda waarde gedreven digitaliseren - digitale overheid](#)
- [Herkennen van fraude onder ouderen - veiliginternetten](#)
- [Fraude herkennen en voorkomen - seniorweb](#)



Vragen

- Welke kwetsbare doelgroepen die betrokken kunnen raken bij online criminaliteit identificeer je binnen het sociaal domein?
- Welke concrete signalen ontvang je binnen het sociaal domein over deze betrokkenheid?
- Welke acties onderneem je op basis van deze signalen?
- Hoe betrek je collega's binnen de gemeente bij deze signalen?
- Op welke manier speelt digitale veiligheid een rol in de projecten binnen het sociaal domein (zoals preventie en inclusie)?
- Op welke manier kunnen we toegankelijke informatie over cyberveiligheid aanbieden aan zowel kwetsbare inwoners als externe partners?
- Op welke manier zou digitale veiligheid een vaste plek kunnen krijgen in onderwijsprojecten, preventieprogramma's of educatieve activiteiten binnen het sociaal domein?
- In hoeverre zijn partners bewust dat kwetsbare groepen waarmee zij direct werken een risico lopen om slachtoffer te worden van online criminaliteit?
- In hoeverre hebben partners handelingsperspectief om hiermee om te gaan?
- Wat kan jij doen om hen te ondersteunen wanneer zij knelpunten ervaren?



1

2





Economische zaken

Gemeenten kunnen een belangrijke rol spelen in het versterken van de digitale veiligheid van lokale ondernemers. Door hen te ondersteunen op het gebied van cyberweerbaarheid, helpt de gemeente mee om schade te voorkomen en de lokale economie stabiel en weerbaar te houden.

Achtergrondinformatie

Steeds meer ondernemers krijgen te maken met online criminaliteit. Ongeveer 1 op de 5 ondernemers wordt jaarlijks slachtoffer van cybercrime. Denk aan phishingmails (nepmails die gevoelige informatie proberen te ontfutselen), online oplichting, gijzelsoftware (ransomware) en malware (schadelijke software).

De gevolgen kunnen groot zijn, zoals het verlies van belangrijke data, financiële schade en zelfs schade aan het imago van het bedrijf. Vaak ligt de oorzaak in simpele dingen, zoals:

- Zwakke of hergebruikte wachtwoorden
- Geen goede back-ups
- Slechte beveiliging van websites of e-mail
- Geen duidelijke afspraken over veilig digitaal gedrag binnen het bedrijf

Bovendien is digitale veiligheid voor veel ondernemers geen dagelijkse prioriteit. Ze willen vooral dat hun systemen gewoon werken, zodat zij zich kunnen richten op hun onderneming. Dat is begrijpelijk, maar juist een klein lek in de beveiliging kan grote gevolgen hebben voor de hele bedrijfsvoering.



Tips

- Maak cyberweerbaarheid een vast onderdeel in gesprekken met partners, zoals het Platform Veilig Ondernemen (PVO).
- Organiseer informatiebijeenkomsten of workshops over cyberveiligheid, specifiek gericht op kleine ondernemers.
- Verbind lokale ondernemers met experts of bedrijven die hen kunnen helpen met hun digitale beveiliging.

Partners

- Zorg: slachtofferhulpNL
- Veiligheid: PVO, FraudeHelpDesk, Centraal Meldpunt Identiteitsfraude
- Economie: Consumentenbond, Autoriteit Consument en Markt, Autoriteit Financiële Markten, mkbNL
- Bedrijven: werkgeversorganisaties, HISWA, brancheorganisaties, Nederlandse Verenigingen van Banken



Meer informatie

- [Cyber & het mkb - Het CCV](#)
- [Cybersecurity binnen het mkb - MKB Nederland](#)
- [PVO en cybercrime - PVO](#)

Vragen

- Welke concrete signalen van online criminaliteit zie je binnen de afdeling economische zaken?
- Welke acties onderneem je op basis van de signalen?
- In hoeverre bespreek je deze signalen binnen de gemeente met collega's?
- Op welke manier kan de doelgroep slachtoffer worden van online criminaliteit?
- In hoeverre zijn partners op de hoogte van de risico's die ondernemers lopen om slachtoffer te worden van online criminaliteit?
- In hoeverre hebben partners en de ondernemers een handelings-

Voorwoord →

Digitale veiligheid →

Ondermijning →

Jeugd →

Onderwijs →

Sociaal domein →

Economische zaken →

Overige afdelingen →





Overige afdelingen

Zoals je in voorgaande hoofdstukken hebt kunnen lezen is cyberveiligheid allang niet meer alleen een zaak van de OOV'er. Hieronder lichten we tot slot nog drie belangrijke gemeentemedewerkers en hun rol in het versterken van cyberweerbaarheid uit:

De communicatieadviseur

De communicatieadviseur speelt een cruciale rol in het voorlichten en activeren van inwoners op het gebied van digitale veiligheid. Denk aan:

- Het opzetten van campagnes over veilig internetgebruik, zoals het herkennen van phishing of het gebruik van sterke wachtwoorden.
- Het toegankelijk maken van informatie via de gemeentelijke website, social media of folders bij de balie.
- Het helder en begrijpelijk communiceren over datalekken of andere digitale incidenten, als die zich voordoen.

Een communicatieadviseur zorgt ervoor dat digitale weerbaarheid niet als een “technisch probleem” wordt gezien, maar als iets waar iedereen aan kan bijdragen.

De CISO

De Chief Information Security Officer (CISO) is verantwoordelijk voor de digitale veiligheid binnen de gemeentelijke organisatie. Deze persoon houdt toezicht op:

- De beveiliging van systemen en netwerken.
- Het opstellen van beleid en regels rondom informatiebeveiliging.
- Het voorbereiden en begeleiden van incidenten en datalekken.

Maar de rol van de CISO stopt niet bij techniek en beleid. De CISO werkt ook samen met andere afdelingen om ervoor te zorgen dat digitale veiligheid ingebed raakt in het dagelijks werk – en dus ook dat burgers veilig met de gemeente kunnen communiceren, bijvoorbeeld via online formulieren of DigiD.



Tip: Betrek de afdeling Communicatie op tijd

Het is belangrijk om de communicatieadviseur vroegtijdig aan te haken. Zo kunnen communicatieactiviteiten goed worden afgestemd op landelijke campagnes en initiatieven. Denk bijvoorbeeld aan landelijke themaweken.

Voorbeelden van relevante themaweken:

- **Januari** – Data Privacy Week
- **September** – Week van het Lezen en Schrijven (o.a. digitale geletterdheid)
- **Oktober** – Week van de Veiligheid
- **Oktober (eerste week)** – Week van de Toegankelijkheid (ook online toegankelijkheid)
- **Oktober** – European Cyber Security Month
- **November** – Week van de Mediawijsheid

Burgercontact

De baliemedewerker is vaak het eerste contact dat inwoners met de gemeente hebben. Juist daarom is deze rol belangrijk in het versterken van digitale weerbaarheid. Denk aan:

- Het herkennen van signalen dat een burger slachtoffer is van bijvoorbeeld identiteitsfraude of oplichting.
- Het doorverwijzen naar de juiste hulp binnen de gemeente of naar externe partijen zoals slachtofferhulp of de Fraudehulpdesk.
- Het geven van eenvoudige tips aan inwoners over bijvoorbeeld het veilig omgaan met DigiD of gemeentelijke online diensten.

Een goed geïnformeerde baliemedewerker kan het verschil maken tussen onzekerheid en grip voor een inwoner die met een digitaal probleem zit.

Voorwoord



Digitale veiligheid



Ondermijning



Jeugd



Onderwijs



Sociaal domein



Economische zaken



Overige afdelingen



Colofon

Tekst

Het CCV, Doris van Rooijen

Vormgeving

CO3, Woltera Niemeijer

© het CCV, mei 2025



Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is een onafhankelijke stichting die partijen en veiligheidsprofessionals helpt om Nederland veiliger en leefbaarder te maken.

Centrum voor Criminaliteitspreventie en Veiligheid
Churchilllaan 11, 3527 GV Utrecht
Postbus 14069, 3508 SC Utrecht

T (030) 751 67 00

E info@hetccv.nl

I www.hetccv.nl

