Weerbaarheid online criminaliteit

Raadswijzer

Voor u ligt de Raadswijzer Weerbaarheid online criminaliteit. Deze raadswijzer helpt u als raadslid om online criminaliteit en digitale weerbaarheid op de agenda te zetten. Zo wordt het thema beter verankerd in de op te stellen collegeplannen en kan er voldoende budget voor worden vrijgemaakt. De raadswijzer beschrijft de problematiek rond online criminaliteit, de rol die u als raadslid kunt pakken en zet drie stippen op de horizon richting 2030.

Wat verstaan we onder online criminaliteit?

Maar liefst **42% van alle criminaliteits-slachtoffers** in Nederland is het gevolg van **online criminaliteit.**[1] Het aantal mensen dat slachtoffer wordt van online fraude en oplichting stijgt elk jaar. Het onderscheid tussen echt en nep wordt bovendien steeds moeilijker te maken. Criminelen zoeken dagelijks naar nieuwe manieren om mensen online op te lichten of uit te buiten. We zien ook steeds vaker dat traditionele criminaliteit verweven raakt met online criminaliteit.

De digitalisering van de samenleving gaat onverminderd door, maar we zijn nog onvoldoende voorbereid om inwoners en ondernemers weerbaar te maken tegen online criminaliteit. Met alle gevolgen van dien.

Taakvelden van de gemeente bij digitale veiligheid

De **gemeente** heeft in relatie tot digitale veiligheid vier taakvelden waarin zij verantwoordelijk en bevoegd is om op te treden. Deze raadswijzer richt zich op de derde weg van de Cyberwegenkaart:[2]

1. Gemeentelijke organisatie digitaal veilig (eigen huis op orde)
2. Voorbereiding op maatschappelijke ontwrichting, incidenten en crises
3. **Verhogen van de weerbaarheid van inwoners en ondernemers tegen online criminaliteit**
4. Opwerpen van barrières tegen online aangejaagde openbare-ordeverstoringen om de gevolgen ervan te beperken

Begrippen cybercrime, gedigitaliseerde criminaliteit en online schadelijk gedrag

Online criminaliteit is een overkoepelende term voor cybercrime en gedigitaliseerde criminaliteit.

Cybercriminaliteit: delicten waarbij ICT zowel het middel als het doel is. Bijvoorbeeld Ransomware en hacking.

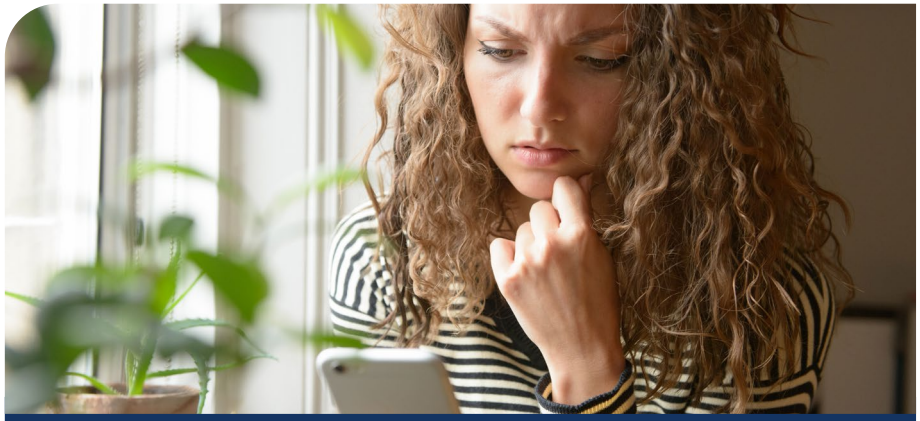
Gedigitaliseerde criminaliteit: traditionele delicten waarbij ICT als middel wordt gebruikt om criminaliteit mogelijk te maken. Bijvoorbeeld phishing en aan- en verkoopfraude.[3]

Naast deze vormen bestaat ook **online schadelijk gedrag**, zoals cyberpesten, online geweld of het verspreiden van desinformatie.

1 Cybercrime, Openbaar Ministerie, 2026.
2 Lokale Cyberwegenkaart, CCV, 2024.
3 Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland, M.G.C.J. Beerthuizen T. Sipma A.M. van der Laan, Cahier 2020-15.

Impact op de samenleving

De leefwereld van mensen speelt zich steeds meer af in de digitale omgeving. Daar ontstaan grote groepen slachtoffers. Daardoor voelen inwoners zich minder veilig en nemen gevoelens van wantrouwen en eenzaamheid toe. Dit is extra zorgelijk omdat de samenleving in toenemende mate afhankelijk is van het internet om te kunnen meedoen. Als het vertrouwen in de onlinewereld afneemt, bestaat het risico dat bepaalde groepen maatschappelijk buiten de boot vallen. Dat kan ook het vertrouwen in de rechtsstaat en de overheid aantasten. De relatief lage pakkans van cybercriminelen zet het vertrouwen van de inwoner in de overheid en politie nog verder onder druk.



De omvang van het probleem

Online criminaliteit groeit sterk. In 2024 gaf **16% van de bevolking van 15 jaar en ouder** (bijna 2,4 miljoen mensen) aan **slachtoffer** te zijn geweest van online criminaliteit.[4] Door de lage meld- en aangiftebereidheid (gemiddeld is de meldingsbereidheid tussen de 15 en 20%), is de werkelijke aard en omvang waarschijnlijk vele malen groter. De inzet van gemeenten, politie en het Openbaar Ministerie is hier onvoldoende in meegegroeid.

4 Online veiligheid en criminaliteit, CBS, 2024.

Gevolgen voor inwoners en ondernemers

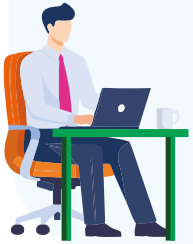
De persoonlijke impact van online criminaliteit is vaak even groot of groter dan bij traditionele delicten. Veel slachtoffers van online criminaliteit krijgen minder vertrouwen in mensen (37%) en voelen zich minder veilig (30%).[5]

Daarnaast ervaart 5 tot 7% van de slachtoffers klachten zoals slaapproblemen, depressieve klachten, angstklachten of het herbeleven van het voorval. Deze klachten komen het vaakst voor bij slachtoffers van online bedreiging en intimidatie. Online oplichting en fraude hebben de grootste impact op het vertrouwen dat mensen in anderen hebben.

Doelgroepen met extra risico:[6]

Senioren: zijn vaak kwetsbaar door beperkte digitale kennis en de financiële impact is vaak groter doordat ze doorgaans meer vermogen hebben.

Jongeren: zijn veel online, zien risico's niet altijd en hebben soms niet door dat ze strafbare feiten plegen.



Ondernemers: zijn kwetsbaar door steeds gerichtere Ransomware-aanvallen. Zij hebben soms onvoldoende kennis, tijd en middelen om de digitale veiligheid van hun bedrijf goed te borgen.

5 Online veiligheid en criminaliteit, CBS, 2024.

6 Cyberweerbaarheid: Resultaten van studentonderzoek naar het vergroten van de weerbaarheid van diverse doelgroepen tegen verschillende vormen van cybercriminaliteit, Hogeschool Saxion, 2020.

Rol van de gemeente

Gemeenten hebben met veel veiligheidsvraagstukken te maken. Veel delicten vinden (deels) online plaats, als overheid zien we dit onvoldoende terug omdat we dit cijfermatig niet (kunnen) onderbouwen. Denk aan woonoverlast, jeugdcriminaliteit, maatschappelijke onrust en huiselijk geweld: vaak hebben deze een online component en worden vuurtjes online aangewakkerd.[7]

Idealiter zijn gemeenten bij online criminaliteit actief in de hele **veiligheidsketen**. Dit wordt geïllustreerd in onderstaand schema.[8] Het lichtblauwe blok verwijst naar de rechtstreekse wettelijke taak en de donkerblauwe blokken naar taken die voortvloeien uit meer algemene wettelijke taken.[9]

Bij een integrale aanpak van online criminaliteit pakt de gemeente, samen met interne en externe partners, haar verantwoordelijkheid in de hele veiligheidsketen. Daarvoor is samenwerking nodig. Binnen de gemeente zelf, tussen onder andere de afdelingen veiligheid, het sociaal domein en wijkteams, én daarbuiten, tussen gemeenten, politie, veiligheidsnetwerken, het Openbaar Ministerie en andere partners.

Welke beleidsdoelen kan de gemeente stellen?[10]

Overheden en partners bundelen hun krachten rond een aantal centrale doelen bij de aanpak van online criminaliteit. Op hoofdlijnen:

- **Proactie** via beleid, kaders en planvorming meer regie op een veilige woon- en leefomgeving
- **Preventie** door het vergroten van awareness over risico's en het herkennen van signalen
- **Vergroten** van meld- en aangiftebereidheid
- **Verstoren** van criminele processen en netwerken

7 Kernbeleid Veiligheid 2021: Handreiking voor gemeenten, VNG, 2021.
8 Cyberweerbaarheid binnen gemeentegrenzen: Uitwerking van het bestuurlijk convenant digitale veiligheid gemeenten en het rijk, Oldengarm P. & Van Summeren, F., 2025.
9 Cyberweerbaarheid binnen gemeentegrenzen, 2025.
10 Kernbeleid Veiligheid 2021, 2021.

Het Integraal Veiligheidsplan (IVP)[11]

Het lokale integrale veiligheidsbeleid is één van de aangewezen bestuurlijke kaders om de taak van gemeente en partners bij de aanpak van online criminaliteit verder uit te werken en te borgen. De gemeenteraad stelt het IVP elke vier jaar vast.

Online criminaliteit kan op verschillende manieren in het IVP worden ingebed. Het is aan te bevelen om dit in elk geval op **drie manieren** te doen:

1. Digitale veiligheid is één van de prioritaire beleidsthema's binnen het IVP
2. Introductie en uitwerking als doorsnijdend, overkoepelend veiligheidsthema
3. Consequente uitwerking van het digitale facet bij zowel de prioritaire als de going concern-thema's

Uw rol als raadslid

Als raadslid heeft u een belangrijke rol in de aanpak van online criminaliteit binnen uw gemeente. U kunt duidelijke kaders stellen, het onderwerp regelmatig op de agenda zetten, het college actief controleren en zorgen voor voldoende budget. Tijdens de begrotings- en verantwoordingsbesprekingen is het verstandig hier structureel tijd voor vrij te maken.[12]

11 Kernbeleid Veiligheid 2021, 2021.

12 Raadgever Digitale veiligheid, VNG, 2025.

Als **raadslid** kunt u vanuit uw **drie rollen** bijdragen aan het verhogen van de online veiligheid:[13]

Volksvertegenwoordigend
- Organiseer een maatschappelijk debat met inwoners en ondernemers over hun ervaringen met online criminaliteit.
- Overweeg een commissie Digitale zaken die zich richt op het versterken van de online weerbaarheid van inwoners en ondernemers.

Kaderstellend
- Neem online weerbaarheid en online criminaliteit op in het IVP van de gemeente.
- Stel geld beschikbaar voor de aanpak van online criminaliteit.
- Stel een raadsbrief op, bijvoorbeeld:
  - Raadsinformatiebrief Digitale criminaliteit, Gemeente Amsterdam
  - Raadsbrief Uitvoeringsprogramma Vergroten digitale weerbaarheid, Gemeente Utrecht
- Dien een motie in, bijvoorbeeld:
  - Grip op digitale zaken, Gemeente Enschede
  - Digitale weerbaarheid en inzet studenten, Gemeente 's-Hertogenbosch
  - Voorkomen digitale criminaliteit, Gemeente Gooise Meren
  - Digitale weerbaarheid vergroten, Gemeente Leiden

Controlerend
- Wordt het IVP voldoende uitgevoerd, is er genoeg inzet op het versterken van de online weerbaarheid en de bestrijding van online criminaliteit?
- Worden alle relevante domeinen betrokken bij een integrale aanpak van online criminaliteit?
- Wordt er goed samengewerkt binnen de driehoek? Wordt er gekeken hoe andere gemeenten het doen?
- Wordt er goed gemonitord?
  - Heeft de raad zicht op cijfers over gedigitaliseerde criminaliteit, zoals diverse vormen van online fraude?
  - Heeft de raad zicht op de relatie met andere thema's zoals ondermijning en maatschappelijke onrust?
  - Welke gegevens over digitale veiligheid staan in de bestuursrapportages?
  - Welke informatie ontbreekt in de periodieke P&C stukken?

13 Checklist Digitale veiligheid voor Raadsleden, VNG, 2023.

Vragen om uw gemeentelijke inzet op online criminaliteit scherp te krijgen

1. Hoeveel fte en middelen zet onze gemeente in voor het tegengaan van online criminaliteit?
2. In welke mate communiceert onze gemeente over online criminaliteit?
3. In hoeverre zijn we bekend met de verschillende vormen van online criminaliteit die er zijn?
4. Hebben we in beeld in hoeverre online criminaliteit binnen onze gemeente een probleem vormt?
   a. Hebben we het aantal daders en slachtoffers binnen onze gemeente in beeld?
   b. Hebben we in beeld welke doelgroepen slachtoffer zijn?
   c. In hoeverre doen bewoners aangifte als ze slachtoffer zijn van online criminaliteit? Om welke vorm gaat het dan?
   d. Hebben we in beeld welke vorm(en) van online criminaliteit het meest voorkomen? En wat de schade is van deze verschillende delicten?
   e. Hoe verhouden deze cijfers zich tot andere gemeenten in onze regio?
5. In hoeverre werken we samen met (mede-)overheden om online criminaliteit tegen te gaan? Of met andere partners zoals de veiligheids-netwerken, politie, onderwijs en/of maatschappelijke organisaties?
6. In hoeverre werken we binnen het gemeentehuis met verschillende afdelingen samen aan online weerbaarheid en online criminaliteit?
7. In hoeverre is online criminaliteit geborgd binnen de gemeentelijke organisatie? Is het een opzichzelfstaand beleidsthema, of ook geborgd binnen andere afdelingen en programma's?
8. Hoe is de samenwerking met de driehoek op het gebied van online weerbaarheid en online criminaliteit?
   a. Geeft de driehoek hier prioriteit aan, en zo ja: hoe?
   b. Worden de doelstelling van politie en OM behaald?
9. In hoeverre zijn we bekend met projecten, programma's, beleid en/of best practices van andere gemeenten tegen online criminaliteit? Of met tools vanuit de rijksoverheid die ons kunnen helpen?
10. Welk beleid hebben we om online criminaliteit tegen te gaan? Welke projecten en/of programma's lopen er binnen onze gemeente om online criminaliteit tegen te gaan?
11. Waar kunnen we als gemeente extra capaciteit of beleid op inzetten? Waar willen we prioriteit aan geven?

Wat heeft u in 2030 als raadslid bereikt?

In het ideaalbeeld heeft u in 2030 **drie mijlpalen** gerealiseerd:

1 In 2030 werken in uw gemeente alle betrokken beleidsdomeinen samen aan weerbaarheid tegen online criminaliteit

Digitale veiligheid raakt alle gemeentelijke beleidsterreinen: van jeugdbeleid en onderwijs tot zorg, economie en het sociaal domein. In 2030 werken deze domeinen integraal, vanuit een gezamenlijke visie, samen aan het vergroten van de online veiligheid van inwoners en ondernemers.

2 In 2030 is er structurele financiering beschikbaar voor het tegengaan van online criminaliteit

Waar structurele financiering voor “traditionele” en ondermijnende criminaliteit vaak vanzelfsprekend is, geldt dat voor online criminaliteit nog onvoldoende. Gemeenten werken hier vaak met incidentele projectgelden, terwijl de opgave structureel is. In 2030 is er binnen uw gemeente structurele financiering beschikbaar voor de aanpak van online criminaliteit.

3 In 2030 beschikt uw gemeente over periodieke cyberbeelden

Om informatiegestuurd te werken zijn actuele en betrouwbare data noodzakelijk. In 2030 beschikt uw gemeente over periodieke cyberbeelden, zodat de benodigde inzet kan worden bepaald en er zicht is op de snel veranderende werkwijze van cybercriminelen.[14]

14 Agenda digitale veiligheid, VNG, 2025.

Vereniging van
Nederlandse Gemeenten

Nassaulaan 12
2514 JS Den Haag
+31 70 373 83 93

info@vng.nl

april 2026