

Digitaal gevaar in beeld



Analyserapport Digitale criminaliteit in Rotterdam



Gemeente
Rotterdam



Inhoudsopgave

1	Introductie	2
2	Prevalentie van slachtofferschap van digitale criminaliteit	2
2.1	Zelfgerapporteerd slachtofferschap	2
2.2	Officiële registraties	4
2.3	Zelfgerapporteerd daderschap	5
2.4	Conclusie	5
3	Impact van slachtofferschap van digitale criminaliteit	6
4	De ervaren digitale veiligheid	7



1 Introductie

Digitale criminaliteit omvat gedigitaliseerde criminaliteit (zoals online aan- en verkoopfraude en helpdeskfraude waarbij ICT onderdeel is van de modus operandi maar niet het doelwit) en cybercriminaliteit (zoals hacken en DDos-aanvallen waarbij ICT zowel het middel als het doel is). Tot aan 2021 tonen cijfers een toename aan slachtofferschap van digitale criminaliteit, zowel landelijk als onder Rotterdammers. Slachtofferschap van digitale criminaliteit kan zorgen voor financiële, emotionele en psychische gevolgen. Onderzoek toont dat deze impact niet onder doet aan de impact van traditionele delicten. Rotterdammers maken zich wel zorgen over deze risico's maar voelen zich desondanks niet onveilig online.

De stijgende lijn in de cijfers over slachtofferschap van digitale criminaliteit komt niet terug in 2022. Toekomstige cijfers zijn nodig om te bepalen of de stijgende trend afremt of verandert in een daling. Het is van belang om deze cijfers met enige voorzichtigheid te bekijken, aangezien deze cijfers gepaard gaan met diverse beperkingen. Deze worden in het rapport benoemd.

In dit rapport wordt allereerst een overzicht gegeven van de omvang van slachtofferschap van digitale criminaliteit. Hierbij is een onderscheid gemaakt tussen zelfgerapporteerd slachtofferschap en slachtofferschap geregistreerd door de politie. Vervolgens wordt de impact van slachtofferschap benoemd. Tot slot wordt ingegaan op de digitale veiligheid ervaren door Rotterdammers.

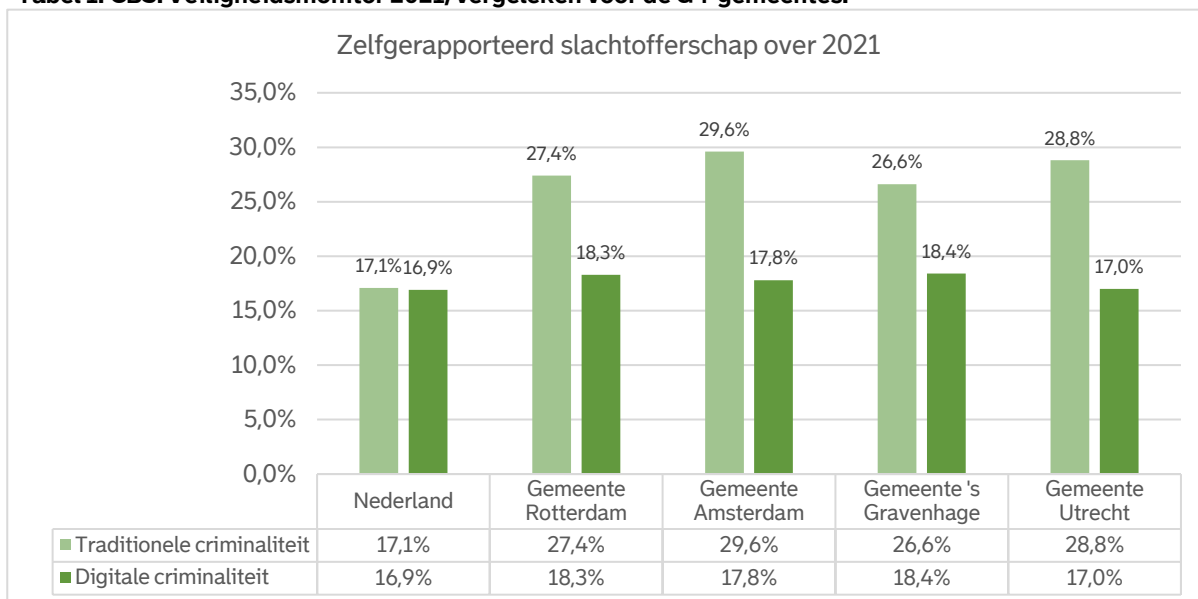
2 Prevalentie van slachtofferschap van digitale criminaliteit

2.1 Zelfgerapporteerd slachtofferschap

Volgens het CBS steeg het aantal *Nederlanders* dat naar eigen zeggen slachtoffer werd van digitale criminaliteit tussen 2012-2021 met 22%¹. In 2021 zijn meer vragen over digitale criminaliteit opgenomen in de Veiligheidsmonitor van het CBS. Daarom zijn enkel over dit jaar openbare cijfers bekend voor de *G4-gemeentes* (zie tabel 1).

¹ Akkermans, M., Kloosterman, R., Moons, E., Reep, C., & Tummers-van der Aa, M. (2022). [Veiligheidsmonitor 2021](#). CBS.

Tabel 1: CBS. Veiligheidsmonitor 2021, vergeleken voor de G4-gemeentes.



Het valt op dat het percentage aan zelfgerapporteerd slachtofferschap voor traditionele criminaliteit en digitale criminaliteit nagenoeg gelijk is op landelijk niveau (resp. 17,1% en 16,9%). Ook is te zien dat het percentage van slachtofferschap van digitale criminaliteit in de gemeente Rotterdam hoger ligt dan het landelijke percentage (18,3% in de gemeente Rotterdam ten opzichte van 16,9% in Nederland). De tabel toont dat slachtofferschap van digitale criminaliteit vaker gerapporteerd is door inwoners van de gemeente Rotterdam dan inwoners van de gemeente Utrecht en de gemeente Amsterdam. De bevroagde Rotterdammers geven aan in 2021 voornamelijk slachtoffer te zijn van online oplichting en fraude (11,1%) en hacken (7,3%). Bij online oplichting en fraude geven vooral 25-65 jarigen slachtofferschap aan², terwijl bij hacken vooral 15-45 jarigen slachtoffer lijken te worden³.

Inwoners van de *gemeente Rotterdam* zijn ook met de Veiligheidsmonitor 2021 van de gemeente Rotterdam bevroagd over slachtofferschap van digitale criminaliteitsvormen (aantal respondenten = 13.820). Bijna 26% van de respondenten was in 2021 naar eigen zegge slachtoffer van minimaal één van de bevroagde digitale criminaliteitsvormen. De respondenten hebben aangegeven vooral slachtoffer te zijn geworden van aankoopfraude (12%) en helpdeskfraude (7%)⁴. Dit zijn vormen die onder de categorie 'online oplichting en fraude' vallen van het CBS (zie bovenstaande alinea). In 2022 is de eerdergenoemde stijging

² Op 1 jan 2022 waren er 362.000 Rotterdammers die in de leeftijdsgroep 25-65 jaar vallen, dit is 55% van het totaal aantal Rotterdammers (653.093).

³ Op 1 jan 2022 waren er 292.812 Rotterdammers die in de leeftijdsgroep 15-45 jaar vallen, dit is 45% van het totaal aantal Rotterdammers (653.093).

⁴ Deze analyse is niet uitgevoerd door OBI, waardoor deze percentages in bepaalde mate kunnen afwijken van de daadwerkelijke percentages.

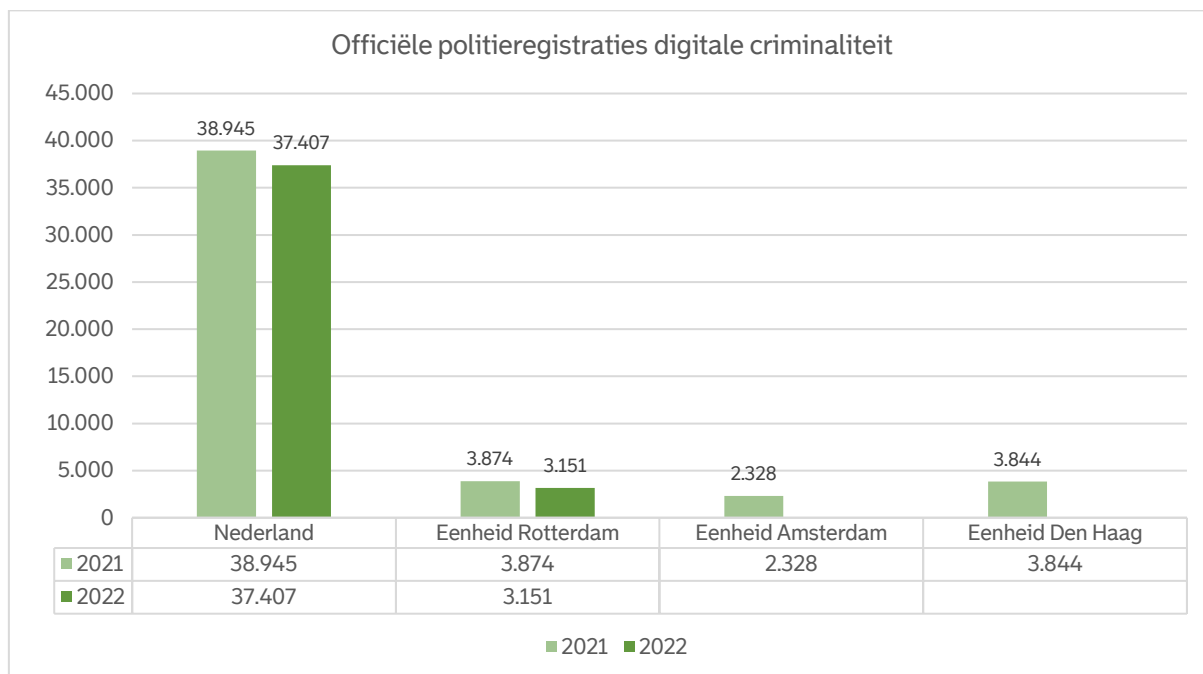


niet duidelijk terug te zien in de cijfers. Nederlanders rapporteren minder slachtofferschap bij het CBS in 2022 dan in 2021 (15% in 2022 ten opzichte van 16.9% in 2021).

2.2 Officiële registraties

In politieregistraties is te zien dat het aantal registraties van digitale criminaliteit in 2022 is afgenomen ten opzichte van 2021 (zie tabel 2). De top drie van de meest voorkomende digitale criminaliteitsvormen, is voor Nederland, de eenheid Rotterdam, de eenheid Amsterdam en de eenheid Den Haag gelijk (zie tabel 3⁶).

Tabel 2: Politie. Jaarbeelden 2021 en 2022.



Tabel 3: Politie. Jaarbeelden 2021 en 2022. Veelvoorkomende digitale criminaliteitsvormen.

	Nederland	Eenheid Rotterdam	Eenheid Amsterdam	Eenheid Den Haag
2021	1. Phishing 2. Betaalverzoekfraude 3. Bankhelpdeskfraude	1. Betaalverzoekfraude 2. Phishing 3. Bankhelpdeskfraude	-	-
2022	1. Bankhelpdeskfraude 2. Account take-over 3. Betaalverzoekfraude	1. Bankhelpdeskfraude 2. Account take-over 3. Betaalverzoekfraude	1. Bankhelpdeskfraude 2. Account take-over 3. Betaalverzoekfraude	1. Bankhelpdeskfraude 2. Account take-over 3. Betaalverzoekfraude
Phishing	Het verkrijgen van (e-banking) gegevens door middel van het verleiden van mensen (phishing) ten behoeve van geldelijk gewin of indirect via goederen (webwinkels).			

⁵ Aan- en verkoopfraude en vriend-in-nood fraude ontbreken in deze cijfers.

⁶ Aan- en verkoopfraude en vriend-in-nood fraude ontbreken in deze cijfers.



Betaalverzoekfraude	Het overmaken van een bedrag via een phishing site gelijkend op de digitale betaalomgeving van de bank in de vorm van een betaalverzoek. Voorheen beter bekend als 1 cent fraude, betaallinkfraude of tikkiefraude.
Bankhelpdeskfraude	Fraude waarbij de dader zich voordoeft als een nepmedewerker van een bank en of het slachtoffer beweegt tot afgifte van geld en/of een bankpas.
Account take-over	Een account van de aangever is gehackt. Deze kan misbruikt worden om allerlei producten te bestellen op naam van de aangever. Het kan ook gaan accounts waar geen bestellingen mee worden gedaan. Vaak zijn dit sociale media accounts of cryptovaluta accounts.

Het halfjaarbeeld (jan-jun) 2022 van de politie omvat registraties van de twee veelvoorkomende criminaliteitsvormen aan- en verkoopfraude en vriend-in-nood fraude. Het biedt daardoor een meer volledig beeld dan de eerdergenoemde jaarbeelden van de politie.

In de periode jan-jun 2022 zijn 3.420 politieregistraties van slachtofferschap van digitale criminaliteit in de *regionale eenheid Rotterdam* bekend. In deze cijfers is te zien dat in de regio Rotterdam voornamelijk sprake is van slachtofferschap van aan- en verkoopfraude en helpdeskfraude. Uit deze registraties volgt dat het bij aan- en verkoopfraude (1.750) om 9.2% van het landelijke aantal politieregistraties in deze periode gaat. Bij helpdeskfraude (498) betreft dit 8.1%. De politie meldt dat slachtofferschap van aan- en verkoopfraude vooral gemeld wordt door 25-65 jarigen⁷. Bij helpdeskfraude hangt het af van de modus operandi die is gebruikt. Zo volgt dat bij bankhelpdeskfraude vooral ouderen (60-plussers⁸) melding doen van slachtofferschap bij de politie⁹.

2.3 Zelfgerapporteerd daderschap

Niet alleen cijfers over slachtofferschap geven inzicht in de omvang van criminaliteit. Ook cijfers over daderschap worden hiervoor gebruikt. Echter, de registratiebronnen van de politie en justitie bieden weinig inzicht in de aard en omvang van daderschap. Er is sprake van een aanzienlijk gat tussen geregistreerd (vermoedelijk) daderschap en zelfgerapporteerd slachtofferschap¹⁰.

2.4 Conclusie

Kortom, omvangschattingen van digitale criminaliteit (volgend uit zowel zelfrapportages van slachtofferschap als politieregistraties) hebben tot aan 2021 een stijgende trend weergegeven.

⁷ Op 1 jan 2022 waren er 362.000 Rotterdammers die in de leeftijdsgroep 25-65 jaar vallen, dit is 55% van het totaal aantal Rotterdammers (653.093).

⁸ Op 1 jan 2022 waren er 136.473 Rotterdammers die in de leeftijdsgroep 60+ vallen, dit is 21% van het totaal aantal Rotterdammers (653.093).

⁹ Halfjaarbeeld Politie 2022. Jaarbeeld Politie 2022.

¹⁰ Beerthuizen, M.G.C.J., Sipma, T., & Van der Laan, A.M. (2020). [Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland](#). WODC.



In 2022 tonen de cijfers van zowel zelfgerapporteerd slachtofferschap als officiële politieregistraties een zeer lichte afname ten opzichte van 2021. Er valt niet te spreken van een 'daling'. Daar zijn meer toekomstige meetpunten voor nodig. Het is afwachten of het gaat om een daadwerkelijke trendbreuk. De voorspelling is namelijk dat de stijgende trend doorzet (CBS, 2022; DRIO, 2022). Deze voorspelling gaat, op basis van onderzoek van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) in 2020, gepaard met de verwachting dat digitale criminaliteit ook zal toenemen in ernst¹¹.

Harde uitspraken op basis van de cijfers over de prevalentie van digitale criminaliteit zijn niet mogelijk. De cijfers worden namelijk sterk beïnvloed door diverse factoren. Er valt te denken aan een toename in aandacht voor de risico's van cybercriminaliteit (en meer genomen preventieve maatregelen), een veranderde modus operandi van daders waardoor slachtoffers minder vaak weten dat ze slachtoffer zijn of wijzigingen in gehanteerde definities van digitale criminaliteitsvormen. De zeer lage aangiftebereidheid bij slachtofferschap van digitale criminaliteit speelt ook een rol¹². Zo volgt uit onderzoek van het CBS in 2021 dat 32% van de zelfgerapporteerde slachtoffers van traditionele criminaliteit aangifte gedaan zou hebben, terwijl dat maar 19% is onder de slachtoffers van digitale criminaliteit (zowel landelijk als in de gemeente Rotterdam). Slechts een klein deel van de slachtoffers is dus bekend bij de politie.

3 Impact van slachtofferschap van digitale criminaliteit

Slachtoffers van digitale criminaliteit ondervinden net als slachtoffers van traditionele criminaliteit financiële, emotionele en psychische gevolgen. Uit cijfers volgt het beeld dat deze schadelijke gevolgen door ongeveer een kwart van de slachtoffers wordt ervaren¹³.

De financiële schade die slachtoffers binnen de *regionale eenheid Rotterdam* hebben ondervonden, wordt door de politie over de periode jan-jun 2022 ingeschat op een schadebedrag van €8,7 miljoen. Dit omvat bijna 11% van de ingeschatte financiële schade voor Nederland (€88,9 miljoen) in deze periode.

¹¹ Dit volgt uit strafrechtelijke indicatoren (hogere strafdreiging en zwaardere straffen) die spelen bij de behandeling van strafzaken gerelateerd aan digitale criminaliteit. Beerthuisen, M.G.C.J., Sipma, T., & Van der Laan, A.M. (2020). [Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland](#). WODC.

¹² Van de Wijer, S.G.A., Leukfeld, E.R., Van de Zee, S. (2020). [Slachtoffer van onlinecriminaliteit, wat nu? Een onderzoek naar aangiftebereidheid onder burgers en ondernemers](#). Politie & Wetenschap, NSCR.

¹³ Veiligheidsmonitor 2021, Gemeente Rotterdam.
Akkermans, M., Arends, J., Derksen, E., & Reep, C. (2023). [Online Veiligheid en Criminaliteit 2022](#). CBS.



Daarnaast blijkt de emotionele en psychische schade ook niet gering. Uit onderzoek van het CBS volgt zelfs dat slachtofferschap vaker leidde tot emotionele of psychische problemen dan financiële problemen. Dit ondersteunt de conclusie uit eerder onderzoek dat de impact van de gevolgen van (vormen van) digitale criminaliteit niet onder doet aan de impact van traditionele delicten. Bij digitale criminaliteit is de schaal waarop slachtoffers worden gemaakt vaak groot, brengen sommige delictsvormen permanente schade met zich mee (bijv. online verspreide beelden) en is er sprake van een hoge mate van 'victim blaming'¹⁴. In onderzoek van het CBS benoemden slachtoffers voornamelijk minder vertrouwen te hebben in mensen en zich minder veilig te voelen. Ook emotionele en psychische gevolgen zoals slaapproblemen, angstklachten en het voorval telkens opnieuw beleven worden door slachtoffers benoemd¹⁵.

De financiële, emotionele en psychische gevolgen worden ook aangekaart door Rotterdamse slachtoffers van digitale criminaliteit. Zij kunnen sinds eind vorig jaar met hun verhaal terecht bij de Cybercrime Nazorg Pilot (CCN). Het CCN volgt uit een samenwerkingsverband tussen Slachtofferhulp Nederland en de gemeente Rotterdam. Vanaf september 2022 tot en met april 2023 heeft CCN 209 slachtoffers kunnen helpen met diverse gevolgen, zoals:

'Slachtoffer geeft aan emotioneel veel last te hebben. Ontdaan, onzeker, vindt alles eng en zit hoog in de emotie. Schaamt zich en is boos op zichzelf'.

'Slachtoffer heeft circa €50.000 overgemaakt naar een kluisrekening, omdat de bankrekening zogenaamd gevaar zou lopen. Tijdens de aangifte geeft slachtoffer aan niet meer te kunnen slapen, hartkloppingen heeft en erg in paniek is.'

4 De ervaren digitale veiligheid

Het CBS heeft in de Veiligheidsmonitor 2021 gevraagd naar de 'kans op slachtofferschap van oplichting via het internet'. Deze kans wordt hoger ingeschat door Nederlanders (17.1%) én Rotterdammers (19.3%) dan de kans op slachtofferschap van enkele traditionele criminaliteitsvormen zoals zakkenrollerij, beroving op straat, inbraak in woning en mishandeling (resp. 2.0-6.4% en 4.9-10.9%). Aanvullend onderzoek van het CBS weergeeft

¹⁴ Borwell, J., Jansen, J., & Stol, W. (2021). [The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory](#). Social Science Computer Review, p. 1-22.

¹⁵ Akkermans, M., Arends, J., Derksen, E., & Reep, C. (2023). [Online Veiligheid en Criminaliteit 2022](#). CBS.



dat veel Nederlanders zich in 2022 ook zorgen maken over misbruik van bankgegevens, persoonsgegevens, accounts en het risico om gehackt te worden. Desondanks geven de meeste van deze respondenten uit ditzelfde onderzoek aan zich (heel) veilig te voelen als ze het internet gebruiken (44%). Maar 4% voelt zich (heel) onveilig als ze het internet gebruiken¹⁶. Ook uit de Rotterdamse veiligheidsmonitor 2019 en 2021 volgt dat Rotterdammers zich vaker nooit of zelden onveilig voelen online (ongeveer 73% t.o.v. de 28% die weleens onveiligheidsgevoelens ervaart).

Het lijkt erop dat burgers zich wel zorgen maken over de risico's van het internet, maar dat deze zorgen geen weerslag vinden in onveiligheidsgevoelens online. Dit kan wijzen op een '*optimistic bias*'. Deze '*bias*' houdt in dat men het risico ziet en zich ervan bewust is, maar het niet ziet als iets dat hen persoonlijk snel zal overkomen. Onderzoek geeft weer dat deze '*bias*' een rol speelt bij digitale criminaliteit. Het kan ervoor zorgen dat mensen minder geneigd zijn om preventief gedrag te tonen ten aanzien van digitale criminaliteit¹⁷. Dit maakt hen kwetsbaarder voor slachtofferschap van digitale criminaliteit.

¹⁶ Akkermans, M., Arends, J., Derksen, E., & Reep, C. (2023). [Online Veiligheid en Criminaliteit 2022](#). CBS.

¹⁷ Misana-ter Huurne, E., Houten, Y. van, Spithoven, R., Notté, R., & Leukfeldt, R., (2020). [Cyberweerbaarheid. Risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb'ers](#). Hogeschool Saxion & De Haagse Hogeschool.

