

# Monitor Identiteit 2023

Bezit, gebruik en misbruik van identiteitsmiddelen



**Guido Brummelkamp**  
**Ruud Hoevenagel**  
met medewerking van  
**Nicole Nibbering (Ipsos I&O)**  
Januari 2024

# Monitor Identiteit 2023

Bezit, gebruik en misbruik van identiteitsmiddelen



# Inhoud

<b>Inleiding</b>	<b>4</b>	<b>Deel 3: Kengetallen uit het stelsel</b>	<b>55</b>
Waarom is er een monitor identiteit?	5	Rijksdienst voor Identiteitsgegevens	56
Hoe wordt de monitor uitgevoerd?	6	Centraal Meldpunt Identiteitsfraude	58
Ontwikkelingen sinds de vorige editie	7	Meldpunt Fouten in Overheidsregistraties (MFO)	60
Identificatie, authenticatie en legitimatie	9	Logius	62
Leeswijzer	10	Centraal Bureau voor de Statistiek	64
		Expertisecentrum Identiteitsfraude & Documenten	67
		Methodische verantwoording	69
<b>Deel 1: Bezit en gebruik identiteitsmiddelen</b>	<b>11</b>	<b>Colofon</b>	<b>71</b>
Bezit van identiteitsmiddelen	12		
Gebruik van identiteitsmiddelen	19		
Kopiëren van identiteitsbewijzen	26		
Risicovol gebruik	30		
Verlies en diefstal	32		
Fouten in registratie bij gemeenten	34		
Biometrische identificatie	35		
<b>Deel 2: Misbruik en fraude</b>	<b>37</b>		
Omvang van het probleem	38		
Kwalitatieve ordening	40		
Indeling identiteitsfraude op basis van dader, middel en doel	42		
Schade en hinder	50		
Ontvangen hulp bij het oplossen van het probleem	52		

# Inleiding



# Waarom is er een monitor identiteit?

Ten behoeve van onze privacy, veiligheid en zekerheid kent Nederland een omvattend identiteitsstelsel. We kunnen hierdoor altijd aantonen dat we zijn die we zeggen te zijn, bijvoorbeeld als we inloggen bij de Belastingdienst, een online aankoop afhalen bij een supermarkt, of een stem uitbrengen bij verkiezingen. Het stelsel is zo omvattend en vanzelfsprekend dat we ons er doorgaans amper van bewust zijn. Om dat zo te houden en tegelijk de risico's op identiteitsfraude te beperken, is het stelsel voortdurend in ontwikkeling. Als eindverantwoordelijke volgt het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) daarom voortdurend gebruik, behoeften, risico's en technische mogelijkheden. Met betrekking tot de ontwikkelingen in gebruik en behoeften, doet het dat onder andere met de monitor identiteit.

De monitor identiteit volgt sinds 2013 tweejaarlijks het bezit en gebruik van identiteitsmiddelen. De monitor houdt bij hoe vaak, in welke situaties en op welke manieren mensen zich identificeren en hoe vaak en in welke omstandigheden het niet goed gaat en mensen bijvoorbeeld slachtoffer worden van identiteitsfraude. De monitor is opgezet om antwoord te geven op de volgende drie centrale vragen:

- Welke identiteitsmiddelen bezitten mensen?
- Hoe vaak, in welke situaties en op welke manier identificeren zij zich?
- Hoe vaak en op welke manier wordt misbruik gemaakt van identiteitsmiddelen?

# Hoe wordt de monitor uitgevoerd?

Bij de beantwoording van deze vragen baseert de monitor zich steeds op twee enquêtes en registraties van partijen uit het stelsel. De ene enquête heeft betrekking op het bezit en gebruik van identiteitsmiddelen. Deze enquête wordt tweejaarlijks online uitgezet onder een steekproef van mensen in de leeftijd van 16 jaar en ouder. De andere enquête wordt uitgezet onder mensen die in de eerste enquête hebben aangegeven te maken te hebben gehad met misbruik van hun identiteit, identiteitsgegevens of identiteitsmiddel. Aan hen wordt gevraagd wat het misbruik precies inhield, welke schade of ongemak het bij hen veroorzaakte en hoe zij zijn geholpen om het misbruik te stoppen.

In de bijlage van dit rapport zijn de methoden verder beschreven en wordt onder meer ingegaan op de representativiteit van de uitkomsten. Naast de enquêtes zijn gegevens verzameld bij partijen die een rol hebben in het identiteitsstelsel. Het betreffen onder meer gegevens van de Rijksdienst voor Identiteitsgegevens (RviG) met betrekking tot het bezit van fysieke identiteitsmiddelen, gegevens van Logius met betrekking tot identificatie aan de hand van DigiD en het CBS met betrekking tot misbruik en identiteitsfraude.

# Ontwikkelingen sinds de vorige editie

Sinds de eerste editie van de monitor in 2013 loopt de digitalisering van identificatie als rode lijn door de resultaten heen. Over een periode van tien jaar is het bezit en gebruik van DigiD steeds toegenomen en benaderde het in 2021 een maximum. Uit zowel enquête als cijfers van Logius kwam naar voren dat vrijwel iedereen inmiddels DigiD bezit en gebruikt. Tegelijk is over dezelfde periode het bezit en gebruik van fysieke identiteitsmiddelen – paspoort, Nederlandse identiteitskaart en rijbewijs – redelijk stabiel gebleven. Tot 2021. De bevindingen van de monitor over dat jaar onderscheidden zich nadrukkelijk van alle voorgaande jaren vanwege het hoge aantal malen dat mensen hun identiteitsmiddel (zowel digitaal als fysiek) gebruikten. Deze stijging kwam volledig voort uit de maatregelen die toen werden genomen om de coronapandemie te bestrijden. Er kwamen immers drie nieuwe veel voorkomende situaties bij waarin mensen zich moesten identificeren, namelijk: het laten testen op corona, het laten vaccineren daartegen, en het gebruik van het coronatoegangsbewijs (Coronacheckapp). De maatregelen leidden ertoe dat mensen in 2021 gemiddeld 10,6 keer een fysiek identiteitsmiddel gebruikten. Hoger dan in 2019 toen ze dat 8,2 keer deden, terwijl er toen nog aanzienlijk meer werd gereisd en er in dat jaar twee verkiezingen werden gehouden. Ook Logius, de partij die in Nederland verantwoordelijk is voor het beheer van DigiD, registreerde een piek en zag in het post-coronajaar van 2022, dat het gebruik van DigiD weer terugzakte. Dit laatste neemt niet weg dat wanneer het effect

van de coronamaatregelen op identificatie buiten beschouwing wordt gelaten de trend van het gebruik van DigiD nog altijd duidelijk stijgend is. Verder waren er in de afgelopen twee jaar de volgende ontwikkelingen:

- Uitrol van een Europees identificatiestandaard (eIDAS): afgelopen twee jaar zijn opnieuw de mogelijkheden uitgebreid voor EU-burgers om zich over de grens (in de Europese ruimte) met hun digitale identiteitsmiddel (zoals DigiD) te identificeren bij overheden. Voor mensen met DigiD geldt dat zij sinds mei 2022 online zaken kunnen regelen met overheidsorganisaties in Europa die zijn aangesloten op Europees inloggen (eIDAS).
- Toegang tot MijnOverheid: Vanaf oktober 2022 is MijnOverheid volledig toegankelijk voor burgers uit de Europese Economische Ruimte (EER), indien zij beschikken over een Europees erkend inlogmiddel (eIDAS). Hiermee is de berichtenbox ook in het buitenland benaderbaar en kunnen mensen gebruik maken van hun berichtenbox en hun persoonlijke gegevens inzien.

- Per 1 juli 2023 is de Wet digitale overheid (Wdo) ingegaan. De wet stelt met name voorwaarden aan overheden ten aanzien van digitale toegankelijkheid, veiligheid en betrouwbaarheid van identificatie. Onder meer zijn voorwaarden gesteld ten aanzien van veilig inloggen op dienstverlening bij (semi-) overheidsinstanties, en toepassing van standaarden zoals informatieveiligheidsstandaarden. Voor gebruikers betekent dit dat inloggen met alleen een DigiD-gebruikersnaam en -wachtwoord kan bij veel organisaties niet meer kan.
- Berichten over identiteitsfraude: in de afgelopen twee jaar bereikten verschillende berichten over (nieuwe vormen van) identiteitsfraude de media. De misdrijven liepen uiteen van het verspreiden van deepfake-video's tot aan de grootschalige handel in persoonsgegevens. Naar aanleiding van een groot onderzoek naar handel in persoonsgegevens, waarschuwde de politie in maart 2023 dat deze (soms gedetailleerde) gegevens door criminelen worden gebruikt om zich als de betrokken burgers voor te doen en daarmee cryptomunten te stelen, bankrekeningen te plunderen of mensen via een gekaapt social media-account af te persen<sup>4</sup>.

In maart 2023 overzag de Algemene rekenkamer de ontwikkelingen<sup>5</sup> en concludeerde op basis daarvan dat de doelen die het ministerie zich oorspronkelijk stelde met betrekking tot digitale authenticatie zijn bereikt. 'Burgers en bedrijven gebruiken massaal DigiD en eHerkenning. Het doel 'voorkomen van fraude' is gedeeltelijk bereikt.' Ook constateert de rekenkamer dat de digitale authenticatie ons veel oplevert in termen van gemak en tijdswinst. Een belangrijk aandachtspunt is evenwel de toegankelijkheid van digitale identificatie voor mensen die minder digitaal vaardig zijn. Voor deze groep wordt het lastiger naarmate de beveiliging zwaarder wordt en zich zij bijvoorbeeld alleen nog met DigiD kunnen identificeren met behulp van een app.<sup>6</sup>

4 NOS, Wereldwijde cybercrimezaak: 50.000 gedupeerden in Nederland, 17 arrestaties, 5 april 2023;  
 NOS, Nederlandse verdachte in cybercrimezaak met tienduizenden slachtoffers aangehouden, 25 juli 2023;  
 NU.nl, Oplichters zetten AI in als levensrecht lokaas, 27 mei 2023

5 Algemene rekenkamer, Digitale identiteit vraagt veel van DigiD en eHerkenning, 29 maart 2023.

6 Algemene rekenkamer, Digitale identiteit vraagt veel van DigiD en eHerkenning, 29 maart 2023.



# Identificatie, authenticatie en legitimatie

Burgers, bedrijven en overheden kunnen om verschillende redenen iemand vragen om een identiteitsbewijs te tonen. Vaak doet men dat om er zeker van te zijn dat iemand daadwerkelijk degene is die hij zegt te zijn. Men doet dat – met andere woorden – om iemand te identificeren. Identificatie vindt bijvoorbeeld veel plaats bij afhaalpunten waar klanten hun online bestelling afhalen. In sommige situaties is identiteitsverificatie wettelijk voorgeschreven zoals bijvoorbeeld in het geval dat iemand iets wil laten vastleggen in een notariële akte, of wanneer iemand aan boord gaat van een vliegtuig.

Vaak ook wordt mensen gevraagd om een identiteitsbewijs te tonen met als doel om na te gaan of iemand gemachtigd is om iets te doen. Er wordt dan gesproken van authenticatie. Authenticatie gebeurt vaak met een afgeleid identiteitsmiddel, zoals een toegangspas, username of token. Door een toegangspas te tonen, laat je niet zozeer zien wie je bent maar vooral dat je gemachtigd bent je ergens te begeven. Van authenticatie is bijvoorbeeld sprake wanneer iemand met DigiD inlogt op de site van de Belastingdienst om aangifte voor de inkomstenbelasting te doen.

Tenslotte wordt burgers regelmatig om een identiteitsbewijs gevraagd om te bepalen of zij bevoegd zijn om iets te doen. In deze situaties wordt gesproken van legitimatie. Legitimatie vindt veelvuldig plaats in supermarkten om te bepalen of iemand ouder is dan achttien jaar (en

daarmee bevoegd is om alcohol of tabak te kopen). Ook ten aanzien van legitimatie geldt dat het onderscheid met identificatie en authenticatie in de praktijk niet altijd duidelijk is. Denk bijvoorbeeld aan het huren van een auto waarbij het tonen van het rijbewijs zowel tot doel heeft om iemands identiteit te bewijzen als iemands rijvaardigheid.

Kijkend naar het onderscheid tussen identificatie, authenticatie en legitimatie, dan wordt duidelijk dat we onze wettige fysieke identiteitsmiddelen in veruit de meeste gevallen gebruiken voor identificatie. Ook het rijbewijs dat formeel in de eerste plaats een legitimatiebewijs is, wordt in de praktijk voornamelijk gebruikt als identiteitsbewijs. Dat we onze identiteitsmiddelen vooral gebruiken voor identificatie komt vooral voort uit wetgeving. De meeste situaties waarin het gebruik van een ID-middel wettelijk is voorgeschreven, hebben betrekking op identificatie. Omdat burgers zich doorgaans niet bewust zijn van het verschil tussen identificatie, authenticatie en legitimatie is in de vragenlijsten die voor dit onderzoek zijn gebruikt steeds één term gebruikt, namelijk identificatie. Ook in voorliggend rapport is er voor gekozen steeds deze term te gebruiken.

# Leeswijzer

Dit rapport bestaat uit drie delen. Het eerste deel bevat cijfers over het bezit en gebruik van vooral fysieke identiteitsmiddelen. Het tweede gaat in op de mate en manier waarop mensen slachtoffer zijn geworden van misbruik van hun identiteit of identiteitsmiddel. Het derde deel geeft een overzicht van gegevens zoals die door verschillende partijen uit het identiteitsstelsel worden bijgehouden.

De eerste twee delen zijn gebaseerd op enquêtes, dat betekent dat de gepresenteerde cijfers schattingen zijn. Hoewel bij de samenstelling van het panel en de analyse van de resultaten geprobeerd is om tot een zo representatief beeld te komen, zijn er groepen die met dit onderzoek onderbelicht zijn gebleven. Dat komt met name doordat de vragenlijst online is afgenomen, waardoor mensen die beperkt digitaal vaardig of beperkt leesvaardig zijn, ondervertegenwoordigd zijn. Voor de onderdelen in dit rapport waar dit een vertekend beeld kan opleveren is dat steeds aangegeven.

# Deel 1

## Bezit en gebruik identiteitsmiddelen



# Bezit van identiteitsmiddelen

Vrijwel iedereen die deelnam aan de enquête bezit een identiteitsmiddel. 67% bezit een paspoort. Een meerderheid van 57% bezit twee middelen waarmee hij zich kan identificeren.

Naast paspoort of identiteitskaart is dat meestal het rijbewijs. Gemiddeld bezit een Nederlander 1,8 identiteitsmiddelen, dit aantal is sinds 2015 niet veranderd.

TABEL 1: **Bezit van identiteitsmiddelen**

	2015 (n=4.854)	2017 (n=4.789)	2019 (n=4.994)	2021 (n=2.473)	2023 (n=2.473)
<b>Nederlands paspoort</b>	60%	59%	62%	63%	67%
<b>Nederlands identiteitskaart</b>	47%	51%	49%	44%	45%
<b>Nederlands rijbewijs</b>	66%	71%	71%	71%	66%
<b>Nederlands verblijfsdocument</b>	1%	1%	2%	1%	2%
<b>Buitenlands verblijfsdocument</b>	1%	1%	2%	2%	2%
<b>Geen</b>	0%	0%	0%	0%	0%

*Bron: enquête onder bevolking*

Ten opzichte van 2015 is het bezit van paspoorten iets toegenomen. Een verklaring daarvoor is dat sinds 2014 paspoorten 10 jaar geldig zijn in plaats van 5 jaar, en over deze periode het aantal reizen naar landen buiten het Schengengebied is toegenomen (op een kortstondige dip na vanwege de Coronamaatregelen).

Tegelijk is het aantal mensen met een rijbewijs iets afgenomen. Deze daling komt vooral door afname van het bezit ervan onder jongvolwassenen (16 - 30 jaar). Het is een daling die het CBR ook constateerde en toeschreef aan de coronamaatregelen waardoor

rijlessen niet konden doorgaan<sup>4</sup>. Hoewel het bezit sinds het einde van de coronamaatregelen volgens gegevens van het CBR weer aantrekt, ligt het aantal nieuw afgegeven rijbewijzen nog steeds onder het niveau van 2019.<sup>5</sup>

TABEL 2: Aantal identiteitsmiddelen in bezit

	2015 (n = 4.854)	2017 (n = 4.790)	2019 (n=4.994)	2021 (n=2.473)	2023 (n=2.473)
<b>1 identiteitsmiddel</b>	33%	28%	27%	27%	31%
<b>2 identiteitsmiddelen</b>	59%	63%	62%	64%	57%
<b>3 of meer identiteitsmiddelen</b>	8%	9%	11%	9%	12%
<b>Geen</b>	0%	0%	0%	0%	0%
Totaal	100%	100%	100%	100%	100%

*Bron: enquête onder bevolking*

<sup>4</sup> RTL Nieuws, Nog altijd minder jongeren met rijbewijs dan voor Corona, 24 februari 2023.

<sup>5</sup> CBS, Statline, Personen met een rijbewijs; rijbewijscategorie, leeftijd, regio

TABEL 3: Welke combinatie van identiteitsmiddelen heeft men?

	2015 (n = 4.853)	2017 (n = 4.789)	2019 (n=4.994)	2021 (n=2.473)	2023 (n=2.473)
<b>Nederlands Paspoort en Nederlands Rijbewijs</b>	33%	35%	35%	38%	34%
<b>Nederlandse ID-kaart en Nederlands Rijbewijs</b>	23%	25%	23%	22%	18%
<b>Alleen Nederlands Paspoort</b>	17%	12%	13%	14%	16%
<b>Alleen Nederlandse ID-kaart</b>	14%	14%	12%	11%	11%
<b>Alleen Nederlands Rijbewijs</b>	2%	1%	1%	1%	2%
<b>Nederlands Paspoort, Nederlands ID-kaart en Nederlands Rijbewijs</b>	7%	8%	9%	8%	11%
<b>Nederlands Paspoort en Nederlandse ID-kaart</b>	3%	2%	3%	2%	4%

*Bron: enquête onder bevolking*

Het bezit van identiteitsbewijzen hangt op onderdelen licht samen met een aantal persoonskenmerken. Dit is in eerdere edities van de monitor ook al geconstateerd. Zo is het bezit van een paspoort onder

hoogopgeleide mensen wat hoger; en is het bezit van de identiteitskaart leeftijdsafhankelijk: jongere mensen bezitten vaker een identiteitskaart dan ouderen.

TABEL 4: **Bezit van fysieke identiteitsmiddelen: verschillen tussen mannen en vrouwen; ouderen en jongeren; lager en hoger opgeleiden**

	Geslacht	Leeftijd	Opleiding
<b>Nederlands paspoort</b>	Geen significante verschillen	Geen significante verschillen	Het bezit van een paspoort ligt onder hoger opgeleiden hoger
<b>Nederlandse identiteitskaart</b>	Geen significante verschillen	Het bezit van een Nederlandse identiteitskaart ligt onder jongeren (30-) hoger	Het bezit van een Nederlandse identiteitskaart ligt onder lager opgeleiden hoger
<b>Nederlands rijbewijs</b>	Het bezit van een rijbewijs is hoger onder mannen	Het bezit van een rijbewijs ligt onder ouderen (30+) hoger	Het bezit van een rijbewijs ligt onder hoger opgeleiden hoger
<b>Nederlands verblijfsdocument</b>	Geen significante verschillen	Het bezit van een Nederlands verblijfsdocument ligt onder jongeren (20-) hoger	Geen significante verschillen
<b>Buitenlands identiteitskaart</b>	Geen significante verschillen	Geen significante verschillen	Geen significante verschillen

*Bron: enquête onder bevolking*

Naast het bezit van de fysieke identiteitsmiddelen is het bezit en gebruik van DigiD verder toegenomen. Logius zag het aantal actieve DigiD-

accounts in 2022 toenemen tot ruim 17 miljoen (op een bevolking van 17,6 miljoen).

TABEL 5: **Aantal actieve DigiD-accounts (in miljoenen)**

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
<b>Aantal actieve DigiD-accounts</b>	11,0	11,8	12,7	13,5	13,5	13,8	15,0	<sup>6</sup>	16,5	17,0

*Bron: Monitor Generieke Digitale Infrastructuur, 2018 & Monitor Digitale Overheid, 2021*

<sup>6</sup> Door een herziening van de berekening van de DigiD-accounts is voor 2020 geen aantal gegeven

Dat inmiddels veruit de meeste mensen DigiD hebben en gebruiken, komt ook uit de enquête naar voren. Van de ongeveer 2.500 mensen die deelnamen, gaven slechts 35 aan geen DigiD te bezitten. Gevraagd naar de reden, geeft ruim een derde aan DigiD niet nodig te hebben.

TABEL 7: Waarom heeft u geen DigiD?	
	2023 (n=34)
Ik weet niet wat een DigiD is	20%
Ik heb DigiD niet nodig	34%
Het lukt mij niet om DigiD te krijgen	6%
Ik wil geen DigiD	20%
Weet niet	23%

Bron: enquête onder bevolking

Driekwart van de geënquêteerden heeft de DigiD-app geïnstalleerd op zijn telefoon, iPad of computer. De meeste mensen hebben inmiddels ook een voorkeur voor het gebruik van deze app boven het inloggen met gebruikersnaam en wachtwoord of het gebruik van SMS-controle.

BRON: ENQ: Op welke manieren heeft u weleens ingelogd met uw DigiD?	
	2023 (n=2.441)
Inloggen met gebruikersnaam en wachtwoord	61%
Inloggen met de DigiD-app	64%
Inloggen met een sms-controle	55%
Door de chip in mijn paspoort, rijbewijs of identiteitskaart met mijn telefoon uit te lezen	6%
Met een digitaal identiteitsmiddel dat in een ander Europees land is uitgegeven	1%

Bron: enquête onder bevolking

TABEL 9: Welke manier van inloggen heeft uw voorkeur?	
	2023 (n=2.441)
Inloggen met gebruikersnaam en wachtwoord	19%
Inloggen met de DigiD-app	54%
Inloggen met een sms-controle	21%
Door de chip in mijn paspoort, rijbewijs of identiteitskaart met mijn telefoon uit te lezen	1%
Ik heb geen voorkeur	3%

Bron: enquête onder bevolking



De toename van het gebruik van DigiD en het gemak dat mensen daarbij ervaren, zoals dat door de Algemene Rekenkamer al eerder is geconstateerd, wordt met de enquête bevestigd. De meeste mensen hebben geen moeite om DigiD te gebruiken. Maar de groep die wel moeite heeft en hulp nodig heeft, is een aandachtspunt. Uit de enquête komt naar voren dat 11% het lastig vindt om DigiD te gebruiken en dat 5% hulp nodig heeft. Het is hoogstwaarschijnlijk een onderschatting omdat de enquête online is afgenomen waardoor de groep niet-digivaardigen ondervertegenwoordigd zal zijn.

TABEL 10: Heeft u moeite om DigiD te gebruiken?

	2023 (n=2.473)		
	Eens	Oneens	Geen antwoord
<b>Ik vind het lastig om DigiD te gebruiken</b>	9%	90%	1%
<b>Ik heb hulp nodig om DigiD te gebruiken</b>	5%	94%	1%

*Bron: enquête onder bevolking*

Naast het publieke DigiD bezit vrijwel iedereen ook meerdere private digitale middelen voor online identificatie. Hierbij moet worden opgemerkt dat identificatie via DigiD van een andere orde is dan identificatie met de meeste private middelen. Daar waar de identiteit bij DigiD altijd is gecontroleerd en voorbehouden is aan één uniek persoon, staat het bij de meeste private identiteitsmiddelen de gebruiker vrij om zelf een naam of identiteit te kiezen (de meeste platforms staan het gebruik van aliassen toe). Meestal kan één en dezelfde persoon bovendien met verschillende identiteiten naar buiten treden. Het bezit van private accounts geeft vooral een beeld van hoe digitale identificatie zich door de tijd heen ontwikkelt. Kijkend naar de afgelopen acht jaar dan is het beeld redelijk constant, op een daling van Facebookgebruikers na.

TABEL 11: **Bezit van online identiteitsmiddelen/accounts**

	2015 (n = 4.853)	2019 (n=4.994)	2021 (n=2.473)	2023 (n=2.473)
<b>DigiD</b>	87%	91%	98%	98%
<b>Facebook</b>	64%	64%	67%	61%
<b>Google</b>	48%	59%	61%	59%
<b>Instagram</b>	*	34%	44%	43%
<b>Microsoft</b>	44%	40%	44%	42%
<b>LinkedIn</b>	23%	26%	36%	34%
<b>Apple</b>	23%	29%	31%	32%
<b>Pinterest</b>	*	21%	25%	24%
<b>X /Twitter</b>	19%	17%	22%	19%
<b>Snapchat</b>	*	15%	15%	16%
<b>Tiktok</b>				16%
<b>eHerkenning</b>	1%	3%	5%	6%
<b>Itsme</b>	*	0,3%	0,1%	0,3%
<b>Irma</b>	*	0,2%	0,3%	0,4%
<b>Anders</b>	1%	1%	1%	1%

*Bron: enquête onder bevolking*

# Gebruik van identiteitsmiddelen

Het gemiddelde gebruik van fysieke identiteitsmiddelen lag in 2023 op 7,0. Dit aantal ligt aanmerkelijk lager dan dat van 2021. In dat jaar identificeerde men zich gemiddeld 10,6 keer. 2021 was wat identificatie betreft een buitengewoon jaar vanwege de verschillende

coronamaatregelen waarbij mensen zich massaal identificeerden, zoals in het kader van de vaccinatiecampagnes, het laten testen op corona en het gebruik van de Coronacheckapp.

TABEL 12: Aantal keer dat men zich in een jaar identificeert

	2015 (n = 4.853)	2017 (n = 4.789)	2019 (n=4.994)	2021 (n = 2.473)	2023 (n=2.473)
<b>Aantal keer geïdentificeerd met wettig fysiek ID-middel</b>	5,7	7,7	8,2	10,6	7,0

Bron: enquête onder bevolking

In tabel 13 is het gebruik van fysieke ID-middelen uitgesplitst. Van de drie middelen worden de identiteitskaart en het rijbewijs het meest gebruikt. Deze worden met name gebruikt voor vaak voorkomende dagelijkse identificatie zoals identificatie bij het ophalen van een online bestelling

bij een afhaalpunt. Het paspoort wordt vooral gebruikt als reisdocument en in meer formele situaties zoals identificatie bij het aanvaarden van een nieuwe baan of bij het bezoek aan een notaris (zie ook tabel 16).

TABEL 13: Gemiddeld gebruik uitgesplitst naar identiteitsmiddel

	2015	2017	2019	2021	2023
<b>Paspoort</b>	3,1	4,1	3,4	2,5	2,7
<b>Identiteitskaart</b>	4,1	4,9	5,4	4,9	4,7
<b>Rijbewijs</b>	2,9	3,9	4,8	4,3	3,1

Bron: enquête onder bevolking

Driekwart van de geënquêteerden heeft altijd een ID-middel bij zich. Dit beeld is constant over de jaren. In tabel 14 is een overzicht gegeven. Voor zover daar tussen jaren verschillen zijn gemeten, zijn deze niet significant. Over het algemeen geldt dat men vaker een identiteitsbewijs bij zich

heeft naarmate men ouder is. Mogelijk komt dat door het rijbewijs dat men vaker op zak heeft en waarvan het bezit hoger is, naarmate men ouder is.

**TABEL 14: Wanneer heeft u een identiteitsbewijs bij u?**

	2015 (n = 4.853)	2017 (n = 4.789)	2019 (n=4.994)	2021 (n=2.473)	2023 (n=2.469)
<b>Altijd</b>	77%	76%	76%	75%	73%
<b>Vaak</b>	15%	16%	16%	16%	16%
<b>Soms</b>	6%	6%	6%	7%	9%
<b>Nooit</b>	2%	2%	2%	2%	3%
Totaal	100%	100%	100%	100%	100%

*Bron: enquête onder bevolking*

De twee landelijke verkiezingen die afgelopen jaar zijn gehouden (voor de Provinciale Staten in maart en voor de Tweede Kamer in november) hebben een belangrijk aandeel gehad in het gebruik van fysieke identiteitsmiddelen. Daarnaast werden fysieke identiteitsmiddelen vaak gebruikt om een pakje op te halen bij een afhaalpunt en ten behoeve van een verblijf in een hotel, pension of op een camping.

TABEL 15: Top-12 van meest voorkomende activiteiten die mensen de afgelopen 12 maanden hebben ondernomen waarbij men zich heeft moeten identificeren (\*)

	2019 (n=4.994)	2021 (n=2.468)	2023 (n=2.469)
1 Gestemd bij Tweede Kamerverkiezingen	-	68%	78% <sup>7</sup>
2 Gestemd bij Provinciale Statenverkiezingen	48%	-	58% <sup>8</sup>
- Gestemd bij Gemeenteraadsverkiezingen	-	-	-
- Gestemd bij verkiezingen Europees Parlement	45%	-	-
3 Pakje in ontvangst genomen bij een afhaalpunt	42%	47%	49%
4 In een hotel, pension, camping of particuliere huurwoning overnacht	39%	35%	41%
5 Vliegreis gemaakt	39%	16%	35%
6 Geregistreerd bij een ziekenhuis/ zorginstelling/ dokter/ therapeut	30%	25%	33%
7 Iets gekocht of verkocht op een online marktplaats	23%	31%	31%
8 Alcohol of sigaretten gekocht	4%	22%	20%
9 (Nieuw) telefoonabonnement afgesloten	19%	14%	15%
10 Een bankrekening geopend	12%	9%	13%
11 Internationale reis per trein, boot of bus gemaakt	9%	4%	12%
12 Een identiteitsbewijs aangevraagd (paspoort, Nederlandse identiteitskaart, rijbewijs, verblijfsdocument)	12%	11%	12%
- Laten vaccineren tegen Covid	-	77%	-
- Corona check app of het papieren bewijs gebruikt om ergens toegang te krijgen of te reizen	-	58%	-
- Laten testen op Covid 19	-	50%	-

Bron: enquête onder bevolking

<sup>7</sup> Dit percentage is niet ontleend aan de enquête maar gebaseerd op het opkomstcijfer, zoals gepubliceerd door de Kiesraad.

<sup>8</sup> Gebaseerd op enquête, werkelijke opkomst was 56%.

Er zijn veel situaties waarbij identificatie aan de hand van een wettig fysiek identiteitsmiddel verplicht of gangbaar is. Bijvoorbeeld bij het openen van een bankrekening, het uitbrengen van een stem bij verkiezingen of bij het aan boord gaan van een vliegtuig. In de enquête zijn 38 van dergelijke situaties onderscheiden, waarbij de deelnemers is gevraagd of zij daar het afgelopen jaar mee te maken hebben gehad en hoe zij zich toen hebben geïdentificeerd. In bijlage 2 is daarvan een overzicht opgenomen. In tabel 16 zijn de 38 situaties gegroepeerd tot zeven domeinen. De uitkomsten van de enquête leren dat de manier waarop mensen zich identificeren per domein verschilt. Bij reizen en het regelen van financiële zaken wordt meestal een paspoort gebruikt, bij het doen van aankopen (bijvoorbeeld bij het kopen van alcohol of het afhalen van een pakketje) vooral een identiteitskaart of rijbewijs. Bij het doen van zaken met de overheid en bij het bezoek van zorginstellingen geldt een sterke toename van het gebruik van DigiD.

TABEL 16: **Identificatie met een wettig fysiek identiteitsmiddel in zeven domeinen**

Kenmerken van identificatie

**Reis en verblijf**

(o.a. vliegreizen, verblijf in hotel, camping)

- 28% van alle identificaties
- Vooral vanwege Vreemdelingenwet bij het maken van vliegreizen
- Voornamelijk face to face
- Paspoort wordt meest gebruikt
- Soms moet kopie overhandigd worden (bij huur auto, camping, hotel)

**Gezondheid**

(o.a. bezoek aan zorginstelling)

- 26% van alle identificaties
- Vooral voor ophalen online aankopen bij afhaalpunt
- Veel identificatie vanwege Alcoholwet en Tabakswet (identificatieplicht bij aanschaf alcohol en tabak)
- Rijbewijs en Nederlandse identiteitskaart worden het meest gebruikt
- Weinig gebruik van kopieën (behalve bij aangaan telefoonabonnement)

**Kopen en verkopen**

(o.a. pakketje afhalen, telefoonabonnement)

- 26% van alle identificaties
- Vooral voor ophalen online aankopen bij afhaalpunt
- Veel identificatie vanwege Alcoholwet en Tabakswet (identificatieplicht bij aanschaf alcohol en tabak)
- Rijbewijs en Nederlandse identiteitskaart worden het meest gebruikt
- Weinig gebruik van kopieën (behalve bij aangaan telefoonabonnement)

**Financiën**

(o.a. bankrekening openen, notarisbezoek)

- 5% van alle identificaties
- Vooral voor zaken met banken, wettelijk voorgeschreven met Wet ter voorkoming van witwassen en financieren terrorisme
- Toename van identificatie op afstand
- Paspoort meest gebruikt
- Veel gebruik van kopieën en scans

TABEL LOOPT DOOR OP VOLGENDE PAGINA >>

<b>Werk en opleiding</b> (o.a. nieuwe baan, inschrijven bij uitzendbureau)	<ul style="list-style-type: none"> <li>• 3% van alle identificaties</li> <li>• Vooral vanwege Wet arbeid vreemdelingen</li> <li>• Voornamelijk face to face</li> <li>• Paspoort en Identiteitskaart het meest gebruikt</li> <li>• Veel gebruik van kopieën en scans</li> </ul>
<b>Wonen</b> (o.a. huren woning, zaken doen met makelaar)	<ul style="list-style-type: none"> <li>• 1% van alle identificaties</li> <li>• Geen wettelijke grondslag</li> <li>• Voornamelijk face to face</li> <li>• Paspoort en identiteitskaart meest gebruikt</li> <li>• Veel gebruik van kopieën en scans</li> </ul>
<b>Zaken met de overheid</b> (o.a. verkiezingen, subsidie aanvragen, aangifte)	<ul style="list-style-type: none"> <li>• 26 % van alle identificaties</li> <li>• Vooral door Tweede Kamerverkiezingen van november 2023.</li> <li>• Voornamelijk face to face.</li> <li>• Wisselend gebruik van paspoort, identiteitskaart en rijbewijs.</li> <li>• Op onderdelen sterke stijging DigiD (aanvragen subsidies, en aangifte bij politie)</li> <li>• Weinig gebruik van kopieën of scans</li> </ul>

Bron: enquête onder bevolking

Paspoorten en identiteitskaarten hebben een chip waarop de gegevens van het document zijn opgeslagen. Op de documenten is dat aangegeven met een logo. 71% van de geënquêteerden is bekend met deze chip. Het is een stijging ten opzichte van 2019 en 2021.

TABEL 17: Paspoorten en identiteitskaarten hebben een chip waarop de gegevens van het document zijn opgeslagen. Wist u dat?			
	2019 (n=4.994)	2021 (n=2.473)	2023 (n=2.473)
<b>Ja</b>	59%	66%	71%
<b>Nee</b>	41%	34%	29%
<b>Totaal</b>	100%	100%	100%

Bron: enquête onder bevolking



Er zijn verschillende instanties en apps die deze digitaal opgeslagen gegevens kunnen uitlezen. In 2023 gaf 18% van de deelnemers aan de enquête aan gegevens wel eens te hebben (laten) uitlezen. Veruit de meeste van hen deden dat met hun eigen telefoon. Meestal deden ze dat door gebruik te maken van de DigiD-app. Enkele andere situaties waarin de chip werd uitgelezen, is het bezoek aan een ziekenhuis en het reizen via Schiphol.

TABEL 18: Heeft u de gegevens die op deze chip zijn opgeslagen zelf wel eens uitgelezen met een app of apparaat?

	2019 (n =2.936 )	2021 (n=1.633)	2023 (n=1.744)
<b>Ja</b>	8%	12%	18%
<b>Nee</b>	92%	88%	82%
Totaal	100%	100%	100%

*Bron: enquête onder bevolking*

# Kopiëren van identiteitsbewijzen

Het komt regelmatig voor dat mensen gevraagd worden om een kopie of scan van hun identiteitsmiddel te overhandigen of op te sturen. Het afgelopen jaar heeft 51 % dat tenminste één keer gedaan. Kopieën en

scans werden met name gemaakt van paspoorten en identiteitskaarten. De mate waarin daarvan kopieën worden verstrekt is over de jaren heen redelijk stabiel.

TABEL 19: Heeft u in de afgelopen 12 maanden wel eens een kopie van uw identiteitsbewijs gemaakt of laten maken?

	Paspoort			Identiteitskaart			Rijbewijs			Nederlands verblijfsdoc.		
	2019 (n = 3.110)	2021 (n=1.567)	2023 (n=1.656)	2019 (n = 2.431)	2021 (n=1.093)	2023 (n=1.567)	2019 (n = 3.520)	2021 (n=1.763)	2023 (n=1.656)	2019 (n = 83)	2021 (n=30)	2023 (n=54)
<b>Een kopie of scan opgestuurd, gemaïld of overhandigd</b>	41%	36%	39%	36%	35%	35%	17%	18%	21%	31%	40%	48%
<b>Een kopie of scan laten maken bij een identiteitscontrole (waar uzelf fysiek bij aanwezig was)</b>	30%	18%	24%	23%	18%	20%	14%	11%	15%	29%	23%	43%

Bron: enquête onder bevolking

Er zijn een aantal situaties waarin het bij identificatie meestal ook voorkomt dat er om een kopie van een identiteitsmiddel wordt gevraagd. Dat gebeurt bijvoorbeeld vrijwel altijd op het moment dat iemand in dienst gaat bij een werkgever.

Ook wordt vaak om kopieën gevraagd met betrekking tot financiële dienstverlening, bijvoorbeeld wanneer iemand een account opent om te handelen in cryptovaluta of wanneer iemand een hypotheek afsluit.

TABEL 20: **Top-10 van situaties waarin mensen het vaakst een kopie van hun identiteitsmiddel moeten overhandigen of opsturen**

% dat aangeeft een kopie te hebben overhandigd of opgestuurd

2023  
(n=2.473)

Een nieuwe werkgever gekregen	81%
Cryptovaluta aangeschaft	74%
Een hypotheek, lening, krediet of credit card afgesloten	66%
Een bankrekening geopend	66%
Gebruik gemaakt van een makelaar	66%
Ingeschreven bij een uitzendbureau	64%
Verhuisd naar een andere huurwoning	64%
Beleggingsrekening geopend	64%
Zaken geregeld bij de notaris	58%
Telefoonabonnement afgesloten	54%

*Bron: enquête onder bevolking*

Het ministerie van BZK heeft door de jaren heen verschillende publiekscampagnes gevoerd om mensen te wijzen op de risico's die het kopiëren met zich mee kan brengen. Onder meer wordt geadviseerd gegevens die niet direct nodig zijn voor identificatie onleesbaar te maken. Over de afgelopen jaren is een daling te zien in het aantal mensen dat dit ooit doet.

TABEL 21:  
Heeft u de kopie bewerkt om misbruik te voorkomen? (% dat aangeeft dit nooit gedaan te hebben)

	2015 (n=2.717)	2017 (n= 2.681)	2019 (n=2.779)	2021 (n=1.169)	2023 (n=1.624)
Ik heb op de kopie of scan vermeld voor welk doel die precies gebruikt mag worden	66 %	59 %	56 %	56%	53%
Ik heb het Burgerservicenummer doorgestreept	73 %	61 %	55 %	49%	48%
Ik heb de pasfoto onherkenbaar gemaakt	85 %	80 %	78 %	74%	73%
Ik heb andere gegevens die de vragende partij niet nodig had doorgestreept	72 %	64 %	58 %	57%	54%

Bron: enquête onder bevolking

Om het makkelijker te maken om gegevens die niet nodig zijn voor identificatie op een kopie van een identiteitsbewijs onleesbaar te maken, bestaat de KopieID app. Deze is uitgegeven door het ministerie van BZK. Sinds 2017 is de bekendheid van de app steeds iets toegenomen. Dit jaar geeft 29% van de geënquêteerden aan de app te kennen.

TABEL 22: Kent u de KopieID app?

	2017 (n = 4.789)	2019 (n=4.994)	2021 (n=2.473)	2023 (n=2.473)
	14%	17%	24%	29%
	86%	83%	76%	71%
	100%	100%	100%	100%

Bron: enquête onder bevolking

Ook het gebruik van de app is sinds 2017 steeds iets toegenomen. Ook afgelopen jaar. Op dit moment heeft 19% van de geënquêteerden de KopieID-app wel eens gebruikt.

TABEL 23: Heeft u de KopieID-app wel eens gebruikt?

	2017 (n = 4.789)	2019 (n=4.994)	2021 (n=2.473)	2023 (n= 2.473)
<b>Ja</b>	7%	10%	14%	19%
<b>Nee</b>	93%	90%	86%	81%
Totaal	100%	100%	100%	100%

*Bron: enquête onder bevolking*

# Risicovol gebruik

Aan het gebruik van identiteitsmiddelen zijn risico's verbonden. Naast de risico's die verbonden zijn aan het vertrekken van kopieën van een identiteitsmiddel ontstaan die risico's wanneer iemand zijn identiteitsmiddel ergens achterlaat (bijvoorbeeld als onderpand) of uitleent. Afgelopen jaar heeft 9% van de geënquêteerden zijn identiteitsmiddel wel eens ergens achtergelaten.

TABEL 24: Heeft u uw identiteitsbewijs wel eens ergens achtergelaten?

	2015 (n = 4.853)	2017 (n = 4.789)	2019 (n = 4.994)	2021 (n=2.445)	2023 (n=2.441)
<b>Ja</b>	5%	10%	9%	5%	9%
<b>Nee</b>	95%	90%	91%	95%	91%
Totaal	100%	100%	100%	100%	100%

Bron: enquête onder bevolking

Voor zover mensen hun identiteitsbewijs ergens achterlaten, is dat meestal in een hotel of bij een camping. Ook - maar minder vaak - gebeurt dat bij benzinestations of winkels, bij de werkgever, een cruisemaatschappij of een bezoek aan een overheidsgebouw (genoemd werden een gevangenis, ambassade en asielzoekerscentrum).

TABEL 25: Waar heeft u uw identiteitsbewijs achtergelaten?

	2021 (n=118)	2023 (n=240)
<b>Hotel/camping</b>	60%	51%
<b>Benzinestation</b>	19%	17%
<b>Winkel</b>	15%	15%
<b>Verhuurbedrijf</b>	6%	6%
<b>Ergens anders</b>	14%	11%

Bron: enquête onder bevolking

In 2023 leende 12% van de geënquêteerden zijn identiteitsmiddel wel eens uit. Meestal was dat in het kader van een machtiging om iemand anders een stem te laten uitbrengen bij landelijke verkiezingen. Het uitlenen van een identiteitsbewijs komt vaker voor onder jongeren en onder mannen. Voor zover mensen hun identiteitsmiddel uitlenen is dat in de meeste gevallen aan een gezins- of familielid.

TABEL 26: Heeft u uw identiteitsbewijs wel eens uitgeleend aan iemand?<sup>9</sup>

	2021 (n=2.468)	2023 (n=2.469)
<b>Ja</b>	9%	12%
<b>Nee</b>	91%	88%
<b>Totaal</b>	100%	100%

Bron: enquête onder bevolking

TABEL 27: Waarom leende u uw identiteitsbewijs uit? (meerdere antwoorden mogelijk)

	2021 (n=222)	2023 (n= 306)
<b>Om namens mij te stemmen</b>	49%	44%
<b>Om toegang te krijgen tot medische zorg</b>	30%	32%
<b>Om diensten af te nemen namens mij</b>	23%	31%
<b>Om sigaretten of alcohol te kopen</b>	9%	14%
<b>Om toegang te krijgen tot een gebouw of terrein</b>	14%	12%
<b>Anders, namelijk</b>	11%	12%

Bron: enquête onder bevolking

TABEL 28: Aan wie heeft u uw identiteitsbewijs uitgeleend?

	2021 (n=203)	2023 (n=342)
<b>Gezins- of familielid</b>	77%	61%
<b>Vriend/kennis</b>	13%	14%
<b>Buur of buurtgenoot</b>	7%	7%
<b>Collega</b>	5%	7%
<b>Klas- /studiegenoot</b>	1%	2%
<b>Iemand anders</b>	5%	10%

Bron: enquête onder bevolking

<sup>9</sup> De vraagstelling in 2021 was anders dan in eerdere versies van deze monitor, cijfers zijn daardoor niet vergelijkbaar.

# Verlies en diefstal

In 2022 werden er 57.500 paspoorten en 138.200 identiteitsbewijzen als vermist opgegeven (RvIG, zie ook Tabel 55). Het is een forse stijging ten opzichte van het jaar ervoor. Het aantal als vermist opgegeven identiteitsbewijzen steeg met 14%, voor paspoorten was dat 28%. Uit

de enquête komt ook een stijging naar voren, al was de stijging het sterkst voor identiteitskaarten. Van de geënquêteerden gaf 4,3% aan zijn identiteitskaart te zijn kwijtgeraakt; 2,7% gaf aan zijn paspoort te zijn kwijtgeraakt (al dan niet door diefstal).

TABEL 29: **Bent u in de afgelopen 12 maanden wel eens een identiteitsdocument kwijtgeraakt of is zo'n document van u gestolen?**

		2017	2019	2021	2023
<b>Paspoort</b>	Kwijtgeraakt	1,9%	1,7%	1,5%	2,0%
	Gestolen	1,4%	0,7%	0,4%	0,7%
<b>Identiteitskaart</b>	Kwijtgeraakt	3,8%	3,2%	1,9%	3,4%
	Gestolen	2,2%	1,1%	0,3%	0,9%
<b>Rijbewijs</b>	Kwijtgeraakt	1,4%	1,4%	1,3%	2,3%
	Gestolen	0,9%	0,7%	0,5%	1,0%

*Bron: enquête onder bevolking*

Driekwart van de mensen die hun identiteitsmiddel kwijtraakten, gaven dat binnen een week door. De meesten gingen daar voor naar de gemeente, wat formeel ook het geëigende loket is. 21% ging daarvoor naar de politie.



TABEL 30: Wanneer heeft u de diefstal of het verlies doorgegeven?

	2023 (n=157)
Binnen 24 uur	36%
Binnen 48 uur	20%
Binnen een week	20%
Binnen een maand	8%
Pas toen ik een nieuw id-bewijs nodig had (na meer dan een maand)	5%
Nog niet	11%
Totaal	100%

Bron: enquête onder bevolking

TABEL 31: Waar heeft u de diefstal of het verlies doorgegeven?

	2023 (n=157)
Ik heb de vermissing niet doorgegeven	23%
Gemeente	53%
Politie	21%
Ergens anders	3%
Totaal	100%

Bron: enquête onder bevolking

# Fouten in registratie bij gemeenten

Met de enquête over bezit en gebruik van identiteitsmiddelen is tevens nagegaan of het bij de deelnemers wel eens is voorgekomen dat gegevens niet goed stonden geregistreerd bij hun gemeente. Zes procent bevestigt dat, dit wel eens is gebeurd. Dit beeld is over de afgelopen jaren constant. Gevraagd naar wat er niet goed stond geregistreerd geven de meeste mensen aan dat het om fouten in adresgegevens gaat, onder andere ontstaan na een verhuizing. Verder komt het voor dat voor- of achternamen niet goed zijn gespeld. Ook geven mensen aan dat contactgegevens die betrekking hebben op digitale communicatie zoals een e-mailadres niet klopten.

TABEL 32: Is het bij u wel eens voorgekomen dat uw gegevens niet goed geregistreerd stonden bij de gemeente?

	2017 (n=4.790)	2019 (n=4.994)	2021 (n=2.298)	2023 (n=2.299)
<b>Ja</b>	8%	6%	7%	6%
<b>Nee</b>	92%	94%	94%	94%
<b>Totaal</b>	100%	100%	100%	100%

Bron: enquête onder bevolking

In 80% van de gevallen was het mogelijk de fout te laten corrigeren. Dit duurde gemiddeld zes weken. Ook dit beeld is over de afgelopen jaren stabiel.

TABEL 33: Was het mogelijk om de fout(en) te corrigeren, en hoeveel tijd kostte dat?

	2019 (n=316)	2021 (n=145)	2023 (n=152)
<b>Ja</b>	77%	77%	79%
<b>Nee</b>	17%	13%	16%
<b>Ik ben er nog mee bezig</b>	6%	10%	5%
<b>Totaal</b>	100%	100%	100%
	(n=242)	(n=111)	(n=120)
<b>Aantal weken (gemiddelde)</b>	6	5	6
<b>Aantal weken (5% trimmed)</b>	4	3	4

Bron: enquête onder bevolking

# Biometrische identificatie

Mensen identificeren zich dit jaar opnieuw weer iets meer aan de hand van gedigitaliseerde biometrische kenmerken. Deze toename komt

vrijwel geheel voort uit het gegeven dat steeds meer mensen hun telefoon ontgrendelen met gezichts- of vingerafdrukherkenning.

TABEL 34: Waarvoor identificeerde u zich met behulp van biometrie?

	2015 (n=4.853)	2017 (n=4.789)	2019 (n=4.994)	2021 (n=1.492)	2023 (n= 2.354)
Vingerafdrukherkenning	11%	20%	33%	35%	37%
Iris/oogherkenning	2%	3%	5%	4%	7%
Stemherkenning	1%	2%	2%	2%	3%
Automatische gezichtsherkenning	2%	3%	10%	19%	25%
Andere vormen van biometrische herkenning	0%	0%	0%	1%	1%
Geen van bovenstaande	81%	72%	56%	51%	48%

*Bron: enquête onder bevolking*

TABEL 35: Waarvoor identificeerde u zich met behulp van biometrie?

	2023 (n=1.705)
Ontgrendelen computer	19%
Ontgrendelen telefoon of tablet	81%
Voor het maken van een vliegreis	10%
Om toegang te krijgen tot een site of app	21%
Om toegang te krijgen tot een kantoor of bedrijventerrein	2%

*Bron: enquête onder bevolking*

Deel 2

Misbruik en fraude



# Omvang van het probleem

Hoewel identiteitsfraude een delict is dat voornamelijk online wordt gepleegd, houdt de ontwikkeling ervan geen gelijke tred met de toename van het online maatschappelijk verkeer. Het aantal mensen dat aangeeft er slachtoffer van te zijn geweest schommelt sinds 2014 tussen de 2,1%

en 5,7%. Dit jaar ligt het percentage op 3,9%. Het betreffen mensen die in de enquête hebben aangegeven in de afgelopen 24 maanden te maken hebben gehad met iemand die zich zonder toestemming voor hem/haar heeft voorgedaan.

TABEL 36: **omvang identiteitsfraude en -misbruik**

**‘Heeft iemand, voor zover u weet, zich in de afgelopen twee jaar (24 maanden) wel eens zonder uw toestemming als u voorgedaan?’**

	2014 (n=1.987)	2015 (n=4.853)	2017 (n=4.789)	2019 (n=4.994)	2021 (n=2.473)	2023 (n=2.473)
<b>Identiteitsfraude en -misbruik</b>	2,1%	3,4%	5,7%	4,1%	3,0%	3,9%

*Bron: enquête onder bevolking*

Wat ten opzichte van 2021 ook stabiel is gebleven, is het gevoel van kwetsbaarheid voor misbruik van persoonsgegevens. Veruit de meeste mensen gaan ervan uit dat hun gegevens tot dusver niet zijn misbruikt. Het neemt niet weg dat een aanzienlijk deel – ongeveer 30% - wel risico's ervaart. Het zijn mensen die hebben aangegeven dat zij wel eens bang zijn dat een van hun accounts wordt misbruikt.

TABEL 37: **Zijn er in het afgelopen jaar persoonsgegevens van u zonder uw toestemming doorverkocht, gelekt of gestolen?**<sup>10</sup>

	2021 (n=2.473)	2023 (n=2.473)
<b>Ja, zeker wel</b>	2%	3%
<b>Waarschijnlijk wel</b>	7%	6%
<b>Waarschijnlijk niet</b>	21%	21%
<b>Nee, zeker niet</b>	36%	37%
<b>Weet niet</b>	33%	33%
<b>Wil niet zeggen</b>	1%	1%
Totaal	100%	100%

Bron: enquête onder bevolking

Mensen die hebben aangegeven dat hun gegevens (waarschijnlijk) wel eens zijn doorverkocht, is gevraagd de situatie te beschrijven. Hieruit komt het beeld naar voren dat mensen sterke vermoedens hebben dat dat is gebeurd op basis van ongevraagde telefoontjes en mails die zij krijgen waarmee wordt geprobeerd producten of diensten aan de man te brengen. Uit de reacties op deze praktijken spreekt veelal een zekere gelatenheid. Voorbeelden daarvan zijn: ‘Ik denk dat er meerdere websites zijn die hengelen naar gegevens’, ‘Het is algemeen bekend dat Apple, Google en Facebook het niet zo nauw nemen’ en; ‘Het zou mij verbazen als het niet is gebeurd’. Verder zijn er meerdere respondenten

<sup>10</sup> Deze vraag is in 2021 voor het eerst opgenomen in de enquête.

die aangeven door een bedrijf of instelling gewaarschuwd te zijn voor een lek. Zo waren er onder andere waarschuwingen van een gemeente, een telecomprovider, een vervoersmaatschappij en een sportschool.

TABEL 38: **Bent u wel eens bang dat iemand misbruik maakt van uw social media-/e-mail- of webwinkelaccount account. door zich voor u uit te geven? (2023)**

	Social media (n=2.101)	E-mail (n=2.473)	Webwinkel (n=2.293)
<b>Ja</b>	30%	27%	26%
<b>Nee</b>	68%	70%	71%
<b>Wil niet zeggen</b>	2%	3%	3%
Totaal	99%	100%	100%

Bron: enquête onder bevolking

# Kwalitatieve ordening

Identiteitsfraude komt sinds de eerste meting van de monitor identiteit steeds opnieuw als een veelomvattend begrip naar voren. Mensen kunnen op uiteenlopende manieren last hebben van iemand die zich ongevraagd voor hen uitgeeft. Achter het slachtofferpercentage van 3,9% gaan dermate verschillende verhalen schuil, dat onduidelijk is wat er precies mee wordt gemeten. Om daar toch een beeld van te krijgen, wordt in de enquête daarom doorgevraagd. Dat is ook dit jaar weer op twee manieren gedaan. Allereerst zijn de geënquêteerden aan de hand van enkele gesloten vragen bevraagd over de aard van de schade, het ervaren ongemak, de manier waarop gegevens zijn misbruikt, of zij de dader (inmiddels) kennen, en welke motieven eventueel achter het misbruik zaten. Ten tweede is aan de deelnemers van de enquête gevraagd in eigen woorden te beschrijven wat er is gebeurd. Op basis hiervan is gekomen tot een kwalitatieve ordening waarin 13 typen van misbruik/fraude worden onderscheiden. Deze ordening is vergelijkbaar

met de ordening uit 2021. Veruit het meeste misbruik vindt online plaats, veel misbruik heeft betrekking op social media-accounts, berichtendiensten en webshops. Dit jaar beschreven respondenten evenwel twee situaties die twee jaar geleden niet naar voren kwamen, namelijk: een fraudeur die bij een werkgever een wijziging van een bankrekeningnummer doorgaf van een werknemer en zo salaris probeerde te stelen; en iemand met een bedrijf die te maken kreeg met iemand die namens hem producten verkocht zonder deze te leveren. Een type van identiteitsfraude dat tot dusver niet door de deelnemers aan de enquête naar voren is gebracht, maar wel in de publiciteit is gekomen, is de overname van iemands identiteit door middel van kunstmatige intelligentie (deep fake video en audio).



TABEL 39: Indeling van identiteitsfraude op basis van open antwoorden

Wat is er gebeurd?<sup>11</sup>

<b>Webwinkelen op andermans rekening</b>	‘Kreeg een raar mailtje van een webwinkel dat mijn bestelde product onderweg was. Ik had helemaal niks besteld. Ik heb toen ingelogd op mijn account. Toen zag ik dat iemand via mijn account iets besteld had en een afleveradres in Limburg had vermeld, terwijl ik in Overijssel woon. Direct telefonisch contact met de webwinkel gezocht. Ook zij zagen dat er gerommeld was. We hebben toen mijn account aangepast.’
<b>Overname van een social media-account</b>	‘Mijn account was gehackt en iemand stuurde via messenger een filmpje naar al mijn vrienden.’
<b>Aanmaken van account op iemands naam</b>	‘Er is voor mij een account aangemaakt op een datingapp.’
<b>Whatsapp hulpvraagfraude</b>	‘Iemand heeft zich voorgedaan als mij in een Whatsapp-bericht aan mijn moeder. Daarin werd om geld gevraagd.’
<b>Aquisitiefraude</b>	‘Ik kreeg een Sms-bericht waarin stond dat ik geld moest overmaken om een pakketje in ontvangst te kunnen nemen.’
<b>Creditcardfraude</b>	‘Na afsluiten abonnement voor een tijdschrift heeft iemand mijn creditcardaccount gebruikt. Na melding is het vergoed door creditcardmaatschappij.’
<b>Phishing</b>	‘Via een online marktplaats werd ik gevraagd om een €0,01 betaling goed te keuren, zogenaamd om mijn identiteit te kunnen controleren. In het proces bleek dat ik goedkeuring had gegeven aan een apparaat om beschikking te krijgen over mijn bankrekening. Binnen een half uur werd ik gebeld door mijn bank of dit klopte en door mij was toegestaan. Dit was uiteraard niet zo en is onmiddellijk door de bank ongedaan gemaakt. Uit coulance heb ik het geld dat van mijn rekening was afgeschreven vergoed gekregen.’
<b>Fraude op online marktplaats</b>	‘Op Marktplaats heeft iemand op mijn naam iets proberen te verkopen.’
<b>Stalking</b>	Ik wordt gestalked door mijn ex. Hij heeft meerdere accounts van mij gehackt. Ik heb daarvoor enkele keren mijn wachtwoord moeten aanpassen.’
<b>Bankfraude</b>	‘Lening afgesloten op mijn naam zonder dat ik dat wist of er toestemming voor gegeven had.’
<b>Misbruik fysiek ID-middel</b>	‘Iemand heeft mij ID gebruikt om toegang te krijgen tot een casino’ ‘Met mijn identificatiedocumenten is een telefoon met abonnement gekocht.’
<b>Commerciële fraude</b>	‘Iemand heeft zich voorgedaan als mijn bedrijf, heeft spullen aangeboden en klanten laten betalen. Kreeg daardoor klachten en bedreigingen van mensen die waren opgelicht.’
<b>Misleiding werkgever</b>	‘Mijn werkgever ontving per e-mail een verzoek om het rekeningnummer voor overmaken van mijn salaris te wijzigen.’

Bron: Slachtofferenquête

11 De respondenten zijn geparafraseerd. Spelfouten zijn gecorrigeerd, ook zijn merknamen achterwege gelaten, zoals de namen van social media-accounts, banken, telecomproviders en webwinkels.

# Indeling identiteitsfraude op basis van dader, middel en doel

Naast de kwalitatieve indeling zoals gegeven in tabel 37 is met de enquête geprobeerd te komen tot een kwantitatief beeld: een beeld van de mate waarin de verschillende typen van identiteitsfraude voorkomen. Omdat mensen de terminologie zoals in bovenstaand overzicht mogelijk niet kennen of herkennen is geprobeerd aan de hand van drie elementen datgene wat mensen is overkomen eenduidig in te delen. In de enquête is dit aan de hand van de volgende elementen nagegaan.

- **Kent u de dader?**

Uit eerdere metingen werd al duidelijk dat identiteitsfraude lang niet altijd wordt gepleegd door onzichtbare of abstracte daders. Het vindt soms ook plaats in familieverband of onder vrienden/kennissen. Regelmatig dekt de term ‘identiteitsfraude’ in die gevallen niet de gevoelsmatige lading van datgene wat er is voorgevallen. Dat geldt bijvoorbeeld voor de mensen die de persoon die zich voor hen uitgaf, hebben kunnen aanspreken. Een voorbeeld daarvan is de moeder die constateerde dat haar zoon ongevraagd van haar rekening iets had gekocht bij een webwinkel.

- **Welk identiteitsmiddel is misbruikt?**

Zoals uit de kwalitatieve indeling al duidelijk werd, is identiteitsfraude bij uitstek een online verschijnsel. Slechts een handvol deelnemers aan de enquête geeft aan dat misbruik is gemaakt van een fysiek identiteitsmiddel zoals een paspoort of rijbewijs. Het gaat veelal om online accounts bij private bedrijven, zoals bij sociale mediaplatforms, berichtendiensten en banken.

- **Welk doel had de dader?**

De veelvormigheid van identiteitsfraude komt verder voort uit de verschillende achterliggende motieven. Soms wordt het gepleegd om er financieel beter van te worden, zoals de veelvoorkomende pogingen om persoons- en inloggegevens te bemachtigen om toegang te krijgen tot iemands bankrekening. Soms handelt een dader uit rancune of frustratie, zoals de situaties waarin slachtoffers geconfronteerd werden met berichten en beelden die via sociale media uit hun naam werden verspreid.

## Dader

Een wezenlijk onderscheid tussen typen van identiteitsfraude, is fraude waarbij het slachtoffer de dader kent en fraude waarbij dat niet het geval is. 14% van de geënquêteerden geeft aan de dader te kennen. In de meeste gevallen is dat iemand die dichtbij staat. Vaak betreft het een (ex) partner of naast familielid. Casussen die uit de enquête naar voren kwamen, betreffen onder andere een ex-partner die op een account aankopen deed bij een webwinkel, en een zoon die inlogde bij een bank en zo geld stal van één van zijn ouders.

TABEL 40: Kent u de persoon die zich voor u heeft voorgedaan?

	2019 (n=437)	2021 (n=459)	2023 (n=367)
<b>Ja</b>	23%	12%	14%
<b>Nee</b>	77%	89%	86%
Totaal	100%	100%	100%

Bron: Slachtofferenquête

TABEL 41: Wie was deze persoon?

	(n=50)
<b>(ex) Partner</b>	34%
<b>Gezins- of familielid (niet zijnde een (ex) partner)</b>	24%
<b>Vriend of kennis</b>	12%
<b>Buur of buurtgenoot</b>	10%
<b>Collega</b>	2%
<b>Klas- of studiegenoot</b>	2%
<b>Iemand anders</b>	16%
Totaal	100%

Bron: Slachtofferenquête

## Middel

Misbruik van iemands identiteit kan plaatsvinden op basis van uiteenlopende identiteitsmiddelen en accounts. Identiteitsfraude- en misbruik waarover de geënuquêteerden rapporteren, is bij uitstek een delict dat plaatsvindt met accounts in het digitale domein. Gevallen waarbij de dader zich in het fysieke domein identificeerde aan de hand van een fysiek identiteitsmiddel dat niet van hem was maar van iemand anders, komen relatief weinig voor. Verder zijn er meerdere gevallen waarbij sprake is van een ‘hybride domein’, waarbij een dader weliswaar gebruik maakte van een fysieke (kopie) van een identiteitsmiddel, maar zich digitaal (op afstand) tot het slachtoffer of een instantie verhiel. Een voorbeeld hiervan is de man op wiens naam een lening werd afgesloten waarbij onder andere een kopie van zijn identiteitsbewijs is gebruikt.

Wat ook dit jaar – net als voorgaande jaren – duidelijk naar voren komt, is dat voor zover er kwetsbaarheden zijn, die vooral zitten bij de private platforms en accounts. Zoals weergegeven in tabel 42 vond 24% van de identiteitsfraude plaats met social media-accounts en 13% met webwinkelaccounts. Misbruik van publieke authenticatie- of identiteitsmiddelen – digitaal dan wel fysiek – komt minder voor. Hierbij moet worden opgemerkt dat misbruik van publieke middelen waarschijnlijk ook een vorm van identiteitsfraude is die met een slachtofferenquête niet altijd naar voren komt, omdat burgers er niet altijd direct zelf slachtoffer van zijn. Te denken valt bijvoorbeeld aan de fraude waarnaar de Koninklijke Marechaussee onderzoek doet: fraude met reisdocumenten in het kader van illegale immigratie.

TABEL 42: Welk middel is misbruikt?

	2021	2023
Inloggegevens social media account	18%	24%
Inloggegevens van een online winkel of online marktplaats	17%	13%
Inloggegevens van mijn bank of andere financiële instelling	14%	13%
Mijn telefoonnummer	11%	10%
Mijn computer, tablet of lap top	5%	5%
Telefoonnummers van bekenden die op mijn telefoon stonden	3%	3%
Een kopie van mijn paspoort, rijbewijs, Nederlandse identiteitskaart of verblijfsdocument	2%	4%
DigiD	2%	2%
Paspoort, rijbewijs of Nederlandse Identiteitskaart of verblijfsdocument	1%	2%
Mijn simkaart	1%	2%
Inloggegevens van mijn cryptocurrency account	0%	1%
Een ander middel	20%	17%
Weet ik niet	7%	5%
Totaal	100%	100%

Bron: Slachtofferenquête

## Doel

Achter identiteitsfraude kunnen uiteenlopen de motieven schuil gaan. Voor zover slachtoffers daar een idee van hebben, ligt er meestal een financieel motief aan ten grondslag. Er wordt een aankoop gedaan bij een webwinkel of een poging gedaan in te breken op een bankrekening.

Maar het komt ook voor dat de dader meer persoonlijke motieven heeft en bijvoorbeeld uit rancune iemand zwart maakt of pest door zijn/haar social media account over te nemen.

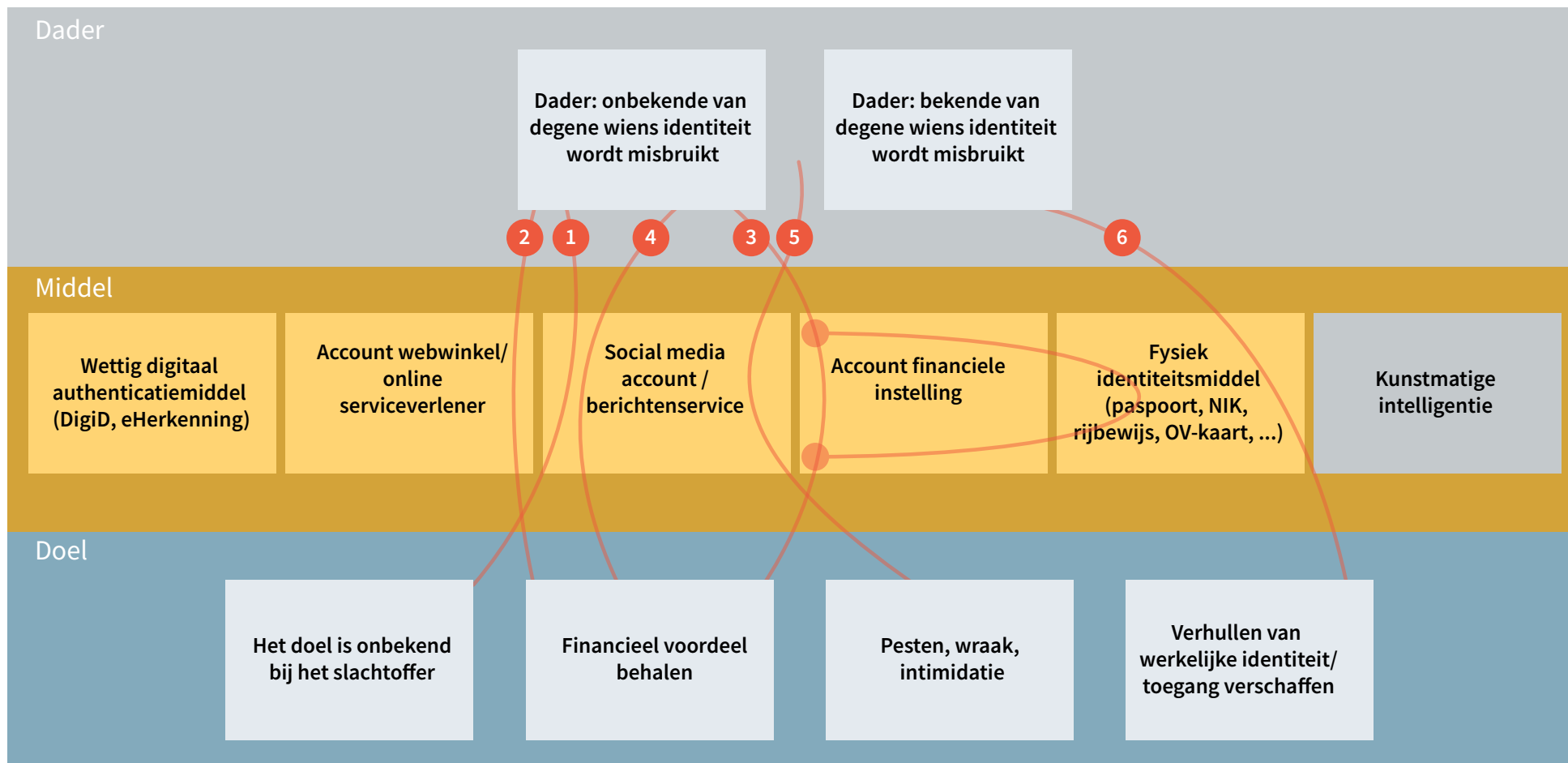
TABEL 43: Wat was de reden voor de fraude? (meerdere antwoorden mogelijk)

	2021	2023
Om een aankoop te doen	36%	28%
Om toegang te krijgen tot mijn bankrekening	19%	16%
Om diensten af te nemen	5%	7%
Om in mijn naam geld van mijn bekenden te vragen	6%	6%
Om een lening aan te vragen	2%	3%
Om toegang tot medische zorg te krijgen	0%	2%
Om een toeslag te ontvangen	1%	1%
Om een uitkering te krijgen	0%	1%
Om toegang tot bepaalde websites/apps te krijgen	5%	9%
Om mijn naam zwart te maken	4%	5%
Om zijn eigen identiteit te verhullen	2%	2%
Om toegang tot specifieke gebouwen te krijgen	0%	1%
Om toegang tot arbeid te krijgen	0%	1%
Dat weet ik niet	26%	31%
Anders	9%	8%

Bron: Slachtofferenquête

Met de drie elementen ‘dader’, ‘middel’ en ‘doel’ zijn er theoretisch heel veel combinaties te maken en daarmee heel veel verschillende vormen van identiteitsfraude te onderscheiden. Ten behoeve van het overzicht onderscheiden wij hier zes ‘typische’ vormen van identiteitsfraude (onder andere op basis van prevalentie): het hacken van een social media account zonder dat duidelijk is wat het doel van de dader is; misbruik van een account van een webwinkel of serviceprovider (zoals een telecombedrijf of energieleverancier) door een onbekende; misbruik van een bankrekening door een onbekende (vaak betreft het een poging daartoe); geld vragen uit naam van iemand zonder diens medeweten; online pesten of intimideren; misbruik maken van iemands fysieke identiteitsmiddel om toegang tot iets te krijgen of om een aankoop te doen.

Een vorm die zich minder duidelijk onderscheidt omdat het weinig voorkomt en de achterliggende motivatie minder eenduidig is, betreft misbruik van DigiD. Een vorm die niet uit de enquête naar voren is gekomen maar wel relevant is vanwege recente publiciteit erover, betreft misbruik door middel van kunstmatige intelligentie. Ten behoeve van de volledigheid heeft dit ook een plaats gekregen in onderstaand figuur.





TABEL 44: Hoe vaak komen de zes typen voor?

	2021 (n=459)	2023 (n=367)
1. Hacken van social media-account door een onbekende met een onduidelijk doel	20%	28%
2. Misbruik van een webwinkelaccount door een onbekende	19%	14%
3. Misbruik van een financieel account, of poging daartoe door een onbekende (evt met behulp van kopie van identiteitsdocument)	14%	15%
4. Misbruik van een social media account om geld te vragen uit naam van iemand	6%	5%
5. Misbruik van een social media account door een (on)bekende om iemand zwart te maken/ dwars te zitten	5%	6%
6. Misbruik van een (kopie van een) identiteitsdocument door een bekende om toegang te krijgen/ een aankoop te doen	2%	3%

Bron: slachtofferenquête

# Schade en hinder

Van alle mensen die te maken hebben gehad met iemand die zich ongevraagd voor hen heeft voorgedaan, geeft 19% aan daar financieel door benadeeld te zijn. Er zijn met name drie vormen van identiteitsfraude die leiden tot financiële schade: oplichting via webwinkels, misbruik maken van inloggegevens van een bank of creditcardgegevens en WhatsApp-hulpvraagfraude. Het gemiddelde schadebedrag is € 1.295. Hierbij moet worden opgemerkt dat dit bedrag een beperkte zeggingskracht heeft omdat de schadebedragen sterk uiteenlopen: van enkele euro's tot meer dan 10.000 euro. Een beeld van de mate van deze spreiding is weergegeven in tabel 46

TABEL 45: Heeft u financiële schade geleden?

	2015 (n=552)	2017 (n=460)	2019 (n=438)	2021 (n=459)	2023 (n=367)
<b>Ja</b>	19%	23%	21%	18%	19%
<b>Nee</b>	79%	75%	78%	82%	80%
<b>Geen antwoord</b>	2%	2%	1%	0%	1%
Totaal	100%	100%	100%	100%	100%

Bron: Slachtofferenquête

<sup>12</sup> Dit is al een 5%-trimmed gemiddelde

TABEL 46: Hoe hoog was de schade?

	2023 (n=63)
Gemiddeld schadebedrag <sup>12</sup>	€ 1.295
<b>Minder dan € 25</b>	3%
<b>€ 25 - € 50</b>	10%
<b>€ 50 - € 100</b>	5%
<b>€ 100 - € 250</b>	18%
<b>€ 250 - € 500</b>	19%
<b>€ 500 - € 1.000</b>	11%
<b>€ 1.000 - € 1.500</b>	8%
<b>€ 1.500 - € 2.500</b>	6%
<b>€ 2.500 - € 10.000</b>	14%
<b>meer dan € 10.000</b>	6%
Totaal	100%

Bron: Slachtofferenquête

Voor zover mensen direct geld zijn verloren, bijvoorbeeld door een onrechtmatige afschrijving van een bankrekening, is deze meestal gecompenseerd: 67% geeft aan volledig te zijn gecompenseerd, 11% is

gedeeltelijk gecompenseerd. Schade als gevolg van misbruik van een account van een webwinkel of online dienst wordt in mindere mate gecompenseerd, namelijk in ongeveer de helft van de gevallen.

TABEL 47: Aard van de schade en compensatie

	2023 (n=69)	Is de schade gecompenseerd?		
		ja	nee	gedeeltelijk
Er is geld van mij gestolen	26%	67%	22%	11%
Ik heb moeten betalen voor producten of diensten die ik niet heb besteld of afgenomen	48%	21%	52%	27%
Kosten voor juridische bijstand	16%	27%	64%	9%
Aanschaf van een nieuw identiteitsbewijs	7%	0%	80%	20%
Telefoonkosten, postzegels, etc.	15%	10%	90%	0%
Anders	22%	20%	73%	7%

Bron: Slachtofferenquête

43% van de geënquêteerden geeft aan naast eventuele financiële schade ook nog andere hinder te hebben ondervonden. In de enquête is aan de deelnemers gevraagd te beschrijven wat die hinder inhield. Uit de antwoorden leiden wij af dat de impact van identiteitsfraude groot kan zijn. Er wordt regelmatig gesproken van stress en verlies van vertrouwen in zichzelf en in anderen. In veel gevallen komt de fraude over als een gebeurtenis waar mensen weinig of helemaal geen grip op hebben.

TABEL 48: Heeft u (naast eventuele financiële schade) nog op andere wijze hinder gehad van de fraude?

	2015 (n=552)	2017 (n=461)	2019 (n=438)	2021 (n=459)	2023 (n=367)
Ja	32%	31%	40%	36%	43%
Nee	65%	67%	58%	62%	55%
Geen antwoord	3%	2%	2%	2%	2%
Totaal	100%	100%	100%	100%	100%

Bron: Slachtofferenquête

# Ontvangen hulp bij het oplossen van het probleem

69% van de mensen die hebben aangegeven last te hebben gehad van iemand die zich ongevraagd voor hem/haar heeft voorgedaan, heeft met tenminste één instantie contact gezocht om (eventuele) schade te

voorkomen of te herstellen. Regelmatig wordt melding gedaan bij politie en financiële instellingen. Degene die een melding doen bij de politie doen in de meeste gevallen ook aangifte.

TABEL 49: Met welke instantie(s) heeft u contact gezocht (meerdere antwoorden mogelijk)

	2015 (n=283)	2017 (n=215)	2019 (n=250)	2021 (n=158)	2023 (n=125)
Politie	25%	34%	32%	53%	54%
Bank	38%	32%	32%	44%	44%
Fraudehelpdesk	9%	14%	10%	22%	18%
Bedrijf waar men zich voor mij heeft uitgegeven	9%	7%	22%	17%	8%
Centraal Meldpunt Identiteitsfouten en -fraude (CMI)	5%	12%	12%	16%	14%
Provider van social media en/of e-mail	18%	33%	21%	15%	16%
Internetprovider	10%	17%	10%	11%	17%
Gemeente	5%	7%	5%	6%	8%
Zorgaanbieder	4%	4%	3%	3%	6%
UWV	1%	1%	0%	1%	0%
Belastingdienst	1%	3%	2%	1%	3%
Anders	25%	17%	11%	23%	25%

Bron: Slachtofferenquête

Net als bij voorgaande metingen scoren banken goed als het gaat over het oordeel over de dienstverlening naar aanleiding van een incident. Voor zover mensen zich tot een bank richtten beoordelen ze de afhandeling met een 8,1. Uit de open antwoorden komen banken regelmatig als pro-actief naar voren. Regelmatig zijn het banken die betrokkenen hebben gewezen op het misbruik.

TABEL 50: Hoe beoordeelt u de wijze waarop u bent geholpen? (rapportcijfer)	
	2023
Bank (n=55)	8,1
Centraal Meldpunt Fraude en Fouten (CMI) (n=17)	6,8
Fraudehelpdesk (n=22)	7,6
Politie (n=67)	6,7
Provicier/host/webwinkel/platform (n=20)	5,1

Bron: Slachtofferenquête

Voor zover het probleem is opgelost, kostte dat in 60% van de gevallen niet meer dan een week. 40% van de ondervraagden geeft aan dat het hen weinig tot geen moeite kostte.

TABEL 51: Binnen welke termijn was het probleem opgelost?					
	2015 (n=397)	2017 (n=331)	2019 (n=318)	2021 (n=285)	2023 (n=222)
Binnen een dag	24%	20%	23%	30%	28%
Binnen een week	30%	35%	33%	33%	32%
Binnen een maand	30%	29%	30%	22%	30%
Binnen een half jaar	12%	15%	11%	13%	7%
Langer dan een half jaar	4%	1%	2%	1%	3%
Totaal	100%	100%	100%	100%	100%

Bron: Slachtofferenquête

TABEL 52: Hoeveel moeite heeft het u gekost om het probleem op te lossen?

	2015 (n=475)	2017 (n=384)	2019 (n=369)	2021 (n=351)	2023 (n=273)
Weinig tot geen moeite	49%	45%	48%	48%	40%
Redelijk wat moeite	41%	45%	44%	44%	48%
Heel veel moeite	9%	0%	8%	8%	12%
Weet niet	1%	10%	0%	0%	0%
Totaal	100%	100%	100%	100%	100%

Bron: Slachtofferenquête

# Deel 3

## Kengetallen uit het stelsel



# Rijksdienst voor Identiteitsgegevens

De Rijksdienst voor Identiteitsgegevens (RvIG) is verantwoordelijk voor het beheer van de Basisregistratie Personen (BRP), het stelsel van reisdocumenten en het beheer en de uitgifte van Burgerservicenummers (BSN) aan gemeenten. Daarmee neemt RvIG een centrale plaats in het Nederlandse identiteitsstelsel in. Ook valt het Centraal Meldpunt

Identiteitsfraude (CMI) onder RvIG, evenals sinds 1 januari 2021 het Meldpunt Fouten in Overheidsregistraties (MFO).

TABEL 53: Aantal paspoorten en identiteitskaarten in omloop (x 1.000.000)

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
<b>Paspoorten</b>	10,1	10,1	10,2	8,7	8,8	8,4	8,0	9,3	9,6	9,6	9,7
<b>Identiteitskaarten</b>	7,8	7,8	8,0	7,2	7,1	6,4	5,9	7,3	7,4	7,4	7,4

Bron: RvIG

TABEL 54: Uitgegeven paspoorten en identiteitskaarten

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
<b>Aantal uitgegeven paspoorten</b>	2.158.965	1.852.789	1.921.886	1.792.056	1.893.174	2.169.638	1.886.703	769.662	392.843	700.358	1.061.472
<b>Aantal uitgegeven identiteitskaarten</b>	1.497.960	1.215.549	1.348.180	1.805.762	1.805.762	1.725.632	1.333.337	694.062	543.714	799.807	808.696

Bron: RvIG



TABEL 55: Vermissingen (x 1.000)

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Aantal paspoorten gestolen/vermist	49,2	48,6	54,6	54,9	58,8	62,7	59,4	52,6	33,2	44,9	57,5
Aantal identiteitskaarten gestolen/ vermist	129,9	135,0	148,1	148,3	152,9	157,4	162,9	134,4	97,0	120,9	138,2
Aantal personen met 3 of meer vermissingen van paspoorten en/of identiteitskaarten		8,0	8,1	12,9	13,6	14,7	10,5				

Bron: RvIG

# Centraal Meldpunt Identiteitsfraude

Bij het Centraal Meldpunt Identiteitsfraude (CMI) kunnen burgers zich melden die (mogelijk) slachtoffer zijn van identiteitsfraude. Het CMI geeft advies en ondersteuning om het misbruik te stoppen, de gevolgen te herstellen en (verdere) identiteitsfraude te voorkomen. Daarnaast levert het meldpunt een bijdrage aan de bewustwording en preventie

en houdt zicht op de kwetsbaarheden in het identiteitsstelsel. Indien nodig schakelt het CMI andere organisaties in zoals de Belastingdienst, politie of RDW. Tabel 56 geeft een overzicht, in tabel 57 zijn de meldingen gespecificeerd.

TABEL 56: Aantal meldingen bij het Centraal Meldpunt Identiteitsfraude en -fouten (CMI)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
<b>Meldingen van ID-fraude</b>	152	209	266	583	793	769	1.677	2.915	3.249	4.142	6.795	6.397	6.151	7.115

*Bron: Centraal Meldpunt Identiteitsfraude, 2024*

TABEL 57: Middel dat volgens het slachtoffer is misbruikt/ontfutseld

	2016	2017	2018	2019	2020	2021	2022	2023
Bankgegevens	2%	3%	3%	2%	2%	2%	1%	2%
Beeldmateriaal	-	4%	5%	7%	8%	5%	3%	4%
BSN	4%	2%	1%	1%	1%	2%	1%	1%
Creditcard	2%	2%	2%	1%	1%	0%	0%	0%
DigiD	4%	2%	4%	2%	2%	4%	2%	1%
Gehackt account	-	7%	7%	10%	17%	7%	7%	7%
Gestolen documenten	1%	0	0%	0%	1%	1%	0%	0%
Identiteitsbewijs vermist/ gestolen	6%	4%	3%	3%	4%	4%	5%	4%
Identiteitsbewijs kopie	40%	41%	45%	43%	30%	38%	49%	55%
Mailadres	7%	4%	3%	3%	3%	2%	3%	2%
Onbekend	4%	2%	2%	2%	1%	1%	1%	1%
Openbare gegevens zoals NAW	26%	23%	22%	23%	28%	32%	25%	20%
Overige	5%	5%	3%	3%	1%	1%	3%	1%
Totaal	100%	100%	100%	100%	100%	100%	100%	100%

Bron: Centraal Meldpunt Identiteitsfraude, 2024

# Meldpunt Fouten in Overheidsregistraties (MFO)

Het MFO is op 1 januari 2021 van start gegaan. De overheid heeft het MFO opgericht om burgers te helpen die tussen wal en schip dreigen te vallen bij het gecorrigeerd willen krijgen van hun gegevens in registraties bij de overheid.

Het MFO kan niet zelfstandig overheidsregistraties corrigeren en heeft nog geen inzage in niet-openbare overheidsregistraties. Daarom werkt het MFO intensief samen met bronhouders en bijhouders van de overheidsregistraties. Het MFO heeft in de afgelopen jaren veel aandacht besteed aan het leggen en onderhouden van contacten met deze zogeheten ketenpartners. Het aantal meldingen dat het MFO ontving is sinds de oprichting ieder jaar toegenomen. Onderstaande tabel toont de groei van het aantal door MFO ontvangen meldingen:

MFO-meldingen	2021	2022	2023
Totaal	504	749	1115

Bron: RvIG

Bij een deel van de meldingen gaat het daadwerkelijk om een fout in een overheidsregistratie. Het MFO hanteert als definitie van fout: 'Wanneer de overheidsregistratie waar de melding betrekking op heeft niet overeenkomt met de werkelijke situatie.'

Door het wijdverbreide gebruik van de Basisregistratie Personen (BRP), kan een relatief kleine fout verstrekkende gevolgen hebben. Wanneer het bijvoorbeeld de IND niet lukt om de verblijfstitel in de BRP zichtbaar te maken, dan kan dat ertoe leiden dat de zorgverzekeraar een zorgverzekering beëindigt. Omdat een geldige verblijfstitel een voorwaarde is om in aanmerking te komen voor een zorgverzekering. Het MFO schakelt in die situaties tussen alle partijen en gaat door totdat zo mogelijk ook de gevolgen van een fout in een registratie zijn rechtgezet.

In 2023 was bij ongeveer 40% van de meldingen sprake van een fout in een overheidsregistratie. Bij ongeveer 30% van de fouten heeft het MFO samengewerkt met de verantwoordelijke overheidsinstantie om de fout en de eventuele gevolgen te herstellen. Bij ongeveer 40% heeft het MFO de melder op weg geholpen door hem of haar in contact te brengen met de verantwoordelijke instantie.

Het komt ook geregeld voor dat registraties in overeenstemming met wet- en regelgeving zijn, maar geen recht doen aan de feitelijke situatie. Dit kan bij burgers tot verwarring leiden. Dit doet zich vooral voor bij de Registratie Niet-Ingezetenen (RNI) waarin burgers die emigreren sinds 2014 terechtkomen. Gegevens over huwelijk en kinderen bijvoorbeeld, worden dan niet meer geactualiseerd. Zo kan het voorkomen dat iemand in het buitenland gescheiden is, maar op MijnOverheid nog ziet staan dat hij/zij gehuwd is. Dit leidt tot ergernis en fouten, vooral wanneer

afnemers (gebruikers) van die registraties details over het hoofd zien en ervan uitgaan dat de getoonde gegevens nog actueel zijn. Dit kan ongewenste gevolgen hebben voor de melder. De overheid kan de registratie in dit geval niet veranderen, maar kan de gevolgen van het onjuiste gebruik van de gegevens wel herstellen.

Niet alle meldingen betreffen daadwerkelijk fouten in registraties bij de overheid. In iets meer dan de helft van de gevallen gaat het om administratieve verzoeken die nog moeten worden verwerkt of om wijzigingen die de melder zelf nog had moeten doorgeven. In dat geval wijst het MFO de melder de juiste weg of geeft het een toelichting op een correctieprocedure.

# Logius

Logius is onderdeel van het ministerie van Binnenlandse Zaken en faciliteert rijksbreed de ontwikkeling van digitale diensten. Zelf omschrijft het zijn dienstverlening als ‘het verbinden van overheid, burgers

en bedrijven’. Belangrijke diensten betreffen het beheer van DigiD, MijnOverheid en Digipoort. In het kader van de monitor identiteit zijn vooral de activiteiten met betrekking tot DigiD relevant.

TABEL 61: Aantal actieve DigiD-accounts (in miljoenen)

	2013	2014	2015	2016	2017	2018	2019	<sup>13</sup>	2021	2022
<b>Aantal actieve DigiD-accounts</b>	11,0	11,8	12,7	13,5	13,5	13,8	15,0	-	16,5	17,0

Bron: Monitor Generieke Digitale Infrastructuur, 2018 & Monitor Digitale Overheid, 2021

TABEL 62: Gebruik DigiD (x 1.000.000)

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
<b>Totaal aantal authenticaties</b>	117,0	158,3	206,0	258,5	280,2	308,0	340,8	402,5	557	514
<b>Aantal authenticaties op basis</b>			184,8	231,3	251,5	260,1	223,9	161,2	121,5	88,3
<b>Aantal authenticaties op midden</b>			21,2	27,1	28,7	36,8	64,6	99,6	149,8	133,7
<b>Aantal authenticaties op Midden (app)</b>					2,6	10,9	46,8	95,6	132	106
<b>Aantal authenticaties op Substantieel</b>					0,01	0,2	5,4	46,1	153,6	186

Bron: Monitor Generieke Digitale Infrastructuur, 2018 & Monitor Digitale Overheid, 2021

<sup>13</sup> Door een herziening van de berekening van de DigiD-accounts is voor 2020 geen aantal gegeven.

TABEL 63: Gebruik DigiD app

	2022
Aantal downloads	2.082.889
Aantal inlogs	292.076.995

*Bron: Logius*

# Centraal Bureau voor de Statistiek

Sinds 2005 voert CBS periodiek onderzoek uit naar slachtofferschap van diverse vormen van criminaliteit. Dit gebeurt met een grootschalige enquête. Sinds 2012 wordt ook gekeken naar identiteitsfraude.

Identiteitsfraude wordt door CBS opgevat als een vorm van digitale

criminaliteit die gepleegd wordt ten behoeve van financieel gewin. Een nadere beschouwing leert dat CBS drie vormen van fraude onder het begrip schaaft: skimming, phishing en pharming.

TABEL 64: Identiteitsfraude								
	2012	2013	2014	2015	2016	2017	2019	2021
<b>Identiteitsfraude totaal</b>	1,5%	1,3%	0,8%	0,6%	0,4%	0,4%	0,5%	0,8%
<b>Skimming</b>	1,1%	0,8%	0,4%	0,2%	0,1%	0,1%	0,1%	-
<b>Pharming/Phishing</b>	0,4%	0,4%	0,4%	0,3%	0,3%	0,3%	0,4%	0,8%

Bron: Veiligheidsmonitor 2019, CBS

Naast slachtofferschap van identiteitsfraude (zijnde skimming, phishing en pharming) worden door CBS ook nog andere vormen van digitale

criminaliteit gemeten. Voor zover daarbij ook regelmatig de identiteit van slachtoffers wordt misbruikt, zijn ze opgenomen in onderstaande tabel.



TABEL 65: vormen van digitale criminaliteit waarbij ook sprake kan zijn van misbruik van persoonsgegevens

	2012	2013	2014	2015	2016	2017	2019	2021
Koop- en verkoopfraude	2,9%	3,3%	3,5%	3,5%	3,4%	3,9%	4,6%	-
Aankoopfraude	6,9%							
Verkoopfraude	1,5%							
Hacken totaal	6%	6,2%	5,2%	5,1%	4,9%	4,9%	5,5%	6,9%
- Ingebroken op computer	1%	1%	0,7%	0,7%	0,7%	0,6%	0,5%	-
- Ingebroken op e-mailaccount	2,7%	2,4%	2,1%	1,8%	1,5%	1,5%	1,7%	-
- Ingebroken op website	1,4%	1,7%	1,4%	1,6%	1,7%	1,7%	2,2%	-
- Anders	2,2%	1,6%	1,3%	1,3%	1,3%	1,4%	1,4%	-
Hack van apparaat	2,9%							
Hack van account	5,7%							
Cyberpesten	3,1%	3,3%	3,1%	3,2%	3,2%	3,1%	4,2%	-
- Laster	1%	1,1%	0,9%	1%	1%	1%	1%	-
- Chantage	0,3%	0,2%	0,2%	0,3%	0,3%	0,3%	1%	-
- Stalken	0,7%	0,7%	0,7%	0,8%	0,8%	0,8%	0,8%	-
- Bedreiging met geweld	0,6%	0,6%	0,6%	0,5%	0,6%	0,6%	0,6%	-
- Anders	1,1%	1,2%	1,1%	1,1%	1,1%	1,1%	1,3%	-
Online bedreiging en intimidatie								0,9%
Online pesten								0,8%
Online stalking								0,8%
Shamesexting								0,4%

Bron: Veiligheidsmonitor 2019, CBS

TABEL 66: Vormen van aan identiteit gerelateerde fraude geregistreerd door Fraudehelpdesk  
(aantal meldingen)

	2017	2018	2019	2020	2021	2022
<b>Acquisitiefraude</b>	3.587	3.245	1.886	1.514	1.139	1.042
card fraude	27	37	31	52	65	77
cyber crime	6.360	6.253	14.237	8.982	9.933	4.471
Identiteitsfraude natuurlijke personen	443	1.024	2.672	12.602	6.066	4.035
Identiteitsfraude rechtspersonen	586	662	908	1.985	9.113	2.366
Marktplaats/ webwinkel fraude	1.909	1.454	2.371	4.827	2.270	5.241

Bron: Fraudehelpdesk, 2021

TABEL 67: Meldingen die specifiek betrekking hebben op  
Whatsapp-hulpvraagfraude

	2020	2021	2022
<b>Aantal meldingen</b>	12.133	8.449	7.448
<b>Slachtoffers</b>	1.340	635	162
<b>Totaal schadebedrag 2020</b>	€ 3.863.056	€ 2.477.041	€ 467.882

Bron: Fraudehelpdesk, 2021

TABEL 68: Vormen van aan identiteit gerelateerde fraude  
geregistreerd door Fraudehelpdesk (aantal slachtoffers)

	2017	2018	2019	2020	2021	2022
<b>Acquisitiefraude</b>	132	129	99	67	49	70
card fraude	15	26	16	31	41	50
cyber crime	344	416	922	668	566	361
identiteitsfraude natuurlijke personen	53	156	387	1.390	675	341
identiteitsfraude rechtspersonen	149	152	129	347	265	345
Marktplaats/ webwinkel fraude	1.277	987	1.570	3.782	5.038	4.326

Bron: Fraudehelpdesk, 2021

# Expertisecentrum Identiteitsfraude & Documenten

Het Expertisecentrum Identiteitsfraude & Documenten (ECID) is een landelijk aanspreekpunt voor (vermoedens) van identiteitsfraude. ECID is onderdeel van de Koninklijke Marechaussee en bedient naast de eigen organisatie ook andere publieke en private instanties met vragen over identiteit en identiteitsdocumenten. Het ondersteunt onder

andere politie, bedrijven, Belastingdienst, gemeenten, en IND. ECID rapporteert jaarlijks over zijn bevindingen in een statistisch jaaroverzicht. Het maakt daarbij onderscheid tussen fraude geconstateerd aan de grens en gevallen van fraude die via andere partijen bij de helpdesk zijn binnengekomen.

TABEL 69: Aantal zaken met betrekking tot identiteits- en documentfraude gemeld bij ECID

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
<b>Aantal zaken identiteits- en/of documentfraude aangetroffen op de Nederlandse grenzen</b>	1034	979	1015	841	868	1053	989	883	947	950	1036	878	969	1146
<b>Aantal documenten waarmee identiteits- en/of documentfraude werd gepleegd op de Nederlandse grenzen.</b>	1392	1308	1394	1172	1163	1567	1446	1256	1435	1436	1487	1153	1397	1216
<b>Aantal zaken identiteits- en/of documentfraude in het Nederlandse binnenland (aangedragen bij ID-Desken)</b>	995	702	811	745	722	904	870	919	1048	1260	1135	939	1032	985

Bron: Expertisecentrum Identiteitsfraude en documenten (ECID), KMar, 2020

TABEL 70: Aantal zaken met betrekking tot  
identiteitsfraude naar segment

	2019	2020	2021	2022
<b>Segment lucht</b>	792	600	691	793
<b>Segment land</b>	171	234	262	338
<b>Segment maritiem</b>	73	44	16	15
Totaal	1.036	878	969	1146

*Bron: Expertisecentrum Identiteitsfraude en documenten (ECID), KMar, 2021*

# Methodische verantwoording

De resultaten van de monitor identiteit zijn gebaseerd op twee enquêtes. De eerste enquête heeft betrekking op het bezit en gebruik van identiteitsmiddelen en is online uitgezet onder een steekproef die is getrokken door marktonderzoeksbureau Ipsos. Deze steekproef is wat betreft leeftijd, geslacht, opleidingsniveau en woonplaats representatief is voor de Nederlandse bevolking ouder dan 16 jaar. 2.473 mensen hebben de vragenlijst ingevuld. Ten aanzien van de representativiteit van de steekproef gelden twee belangrijke beperkingen:

- In de eerste plaats zijn Nederlanders met beperkte digivaardigheid en/of een beperkt computer-/internetgebruik niet in de steekproef vertegenwoordigd.
- Verder is er een ondervertegenwoordiging van mensen die de Nederlandse taal niet of beperkt machtig zijn.

De tweede enquête over misbruik van identiteitsmiddelen is uitgezet onder dezelfde steekproef. Deze enquête is alleen afgenomen onder degenen die aangaven in de afgelopen twee jaar te maken te hebben gehad met iemand die zich ongevraagd voor hem/haar heeft voorgedaan. Aan deze tweede enquête hebben 367 mensen deelgenomen.

	(n=2.473)	(n=13.754.000)	
GESLACHT (16-80 jaar)	steekproef	populatie	verschil
<b>Man</b>	48,1%	49,9%	1,8%
<b>Vrouw</b>	51,9%	50,1%	-1,8%

*Bron: enquête onder bevolking*

	(n=2.473)	(n=13.754.000)	
LEEFTIJD (16-80 jaar)	steekproef	populatie	verschil
<b>16 tot 20 jaar</b>	3,2%	6,0%	-2,8%
<b>20 tot 30 jaar</b>	12,6%	16,2%	-3,6%
<b>30 tot 40 jaar</b>	18,9%	15,9%	3,0%
<b>40 tot 50 jaar</b>	14,2%	15,3%	-1,1%
<b>50 tot 60 jaar</b>	21,9%	18,3%	3,6%
<b>60 tot 70 jaar</b>	16,8%	15,6%	1,2%
<b>70 t/m 80 jaar</b>	12,4%	12,5%	-0,1%

*Bron: enquête onder bevolking*

	(n=2.473)	(n=13.754.000)	
HOOGSTE OPLEIDING DIE IS AFGEMAAKT (16-80).	steekproef	populatie	verschil
Geen onderwijs / basisonderwijs	0,6%	7,6%	-7,0%
LBO / VBO / VMBO (kader- of beroepsgericht) / MBO1	6,9%	11,1%	-4,2%
MAVO / HAVO of VWO (overgegaan naar 4e klas) / (M)ULO / VMBO (theoretische of gemengd) / voortgezet speciaal onderwijs	9,4%	7,5%	1,9%
MBO 2, 3, 4 of MBO voor 1998	30,5%	32,5%	-2,0%
HAVO of VWO (met diploma afgerond) / HBS / MMS	11,0%	9,4%	1,6%
HBO of universitair propedeuse / HBO of universitair bachelor/kandidaats	30,1%	20,1%	10,0%
HBO of universitair master/doctoraal/postdoctoraal	11,5%	11,7%	-0,2%

*Bron: enquête onder bevolking*

# Colofon

De Monitor Identiteit wordt uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Auteurs:

Guido Brummelkamp en Ruud Hoevenagel  
met medewerking van

Nicole Nibbering (Ipsos I&O)

Januari 2024

Grafisch ontwerp: [Streeff.nl](https://streeff.nl)

Iconen gebaseerd op NounProject  
Lieuchien/ Tulpahn/Lakenbrink/Vectors Point/Millenials/Lil Squid



Brummelkamp  
beleidsonderzoek

