Rapport

Online Veiligheid en Criminaliteit 2022

Math Akkermans,
Judit Arends,
Elianne Derksen,
Carin Reep

Mei 2023

Online Veiligheid en Criminaliteit 2022

Over deze publicatie

De twee centrale thema's van deze publicatie zijn online veiligheid en online criminaliteit. Bij online veiligheid gaat het om de veiligheidsbeleving van burgers op internet en de maatregelen die ze nemen om zich te beschermen tegen criminelen. Bij online criminaliteit gaat het vooral om slachtofferschap van online delicten, gevolgen die slachtoffers ervaren van wat hen overkomen is, en hun meldings- en aangiftebereidheid. Naast deze twee centale thema's komen ook online discriminatie en online oproepen tot openbare-ordeverstoring aan de orde.

De cijfers in deze publicatie zijn gebaseerd op het onderzoek *Online Veiligheid en Criminaliteit 2022*. Dit onderzoek heeft plaatsgevonden van augustus-oktober 2022. In totaal hebben 32 861 personen van 15 jaar of ouder meegedaan, het responspercentage bedroeg daarmee bijna 32,9 procent. Aanvullend is ook gebruik gemaakt van data van andere CBS-onderzoeken: de ICT-enquête Personen en Huishoudens, de Veiligheidsmonitor, en de Prevalentiemonitor Huiselijk Geweld en Seksueel Grensoverschrijdend gedrag.

1. Inleiding

Hoe veilig voelen Nederlanders zich als ze online zijn? Zijn ze bang om slachtoffer te worden van criminelen? Weten ze hoe ze zich kunnen beschermen op internet en welke concrete maatregelen nemen ze? En hoeveel Nederlanders worden slachtoffer van online criminaliteit? In hoeverre hebben ze te maken met online discriminatie en online oproepen tot openbare-ordeverstoring? Al deze vragen, en nog meer, worden in deze publicatie *Online Veiligheid en Criminaliteit 2022* (afgekort *OVeC 2022*) beantwoord.

Dit is niet het eerste onderzoek over deze thematiek dat het CBS heeft uitgevoerd. In de jaarlijkse ICT-enquête Internetgebruik Huishoudens en Personen is eerder onderzoek gedaan naar online veiligheid en in de tweejaarlijkse Veiligheidsmonitor wordt online criminaliteit onderzocht. Uit deze monitor bleek dat in 2021 ongeveer 1 op de 6 Nederlanders van 15 jaar of ouder (dat zijn 2,5 miljoen mensen) slachtoffer waren van online criminaliteit (Akkermans, Kloosterman, Moons, Reep en Tummers-van der AA, 2022). Op verzoek van het ministerie van Justitie en Veiligheid (J&V) heeft het CBS de stand van zaken anno 2022 op het terrein van online veiligheid en criminaliteit onderzocht. Het is de eerste keer dat het CBS beide thema's, online veiligheid en online criminaliteit, in één onderzoek heeft gecombineerd[1)]. De intentie bestaat om het onderzoek in de even jaren, de jaren waarin geen Veiligheidsmonitor wordt gehouden, te herhalen zodat het ook een monitorfunctie krijgt. De eerste vervolgmeting zal dan dus plaatsvinden in 2024.

Het onderzoek richt zich op inwoners van Nederland van 15 jaar of ouder[2)]. Het verslagjaar is 2022[3)]. Centraal staan de volgende onderzoeksvragen:

Online veiligheid

- Hoe gaan Nederlanders om met privacy en het beschermen van persoonlijke gegevens op internet?
- In welke mate zijn Nederlanders bekend met begrippen op het terrein van internetveiligheid?
- In welke mate maken Nederlanders zich zorgen over internetveiligheid?
- Welke maatregelen nemen Nederlanders om te voorkomen dat ze slachtoffer worden van online criminaliteit?
- Hoe veilig voelen Nederlanders zich op internet en hoe schatten ze de kans in om slachtoffer te worden van online criminaliteit?

Online criminaliteit

- Wat is de aard en omvang van het slachtofferschap van online criminaliteit?
- Wie zijn de daders van online criminaliteit?
- Wat zijn de gevolgen van online criminaliteit voor de slachtoffers?
- In welke mate vindt melding en aangifte van online criminaliteit plaats?

Online discriminatie

- In welke mate voelen Nederlanders zich online gediscrimineerd?
- Op welke gronden en op welke manieren voelen de slachtoffers zich online gediscrimineerd?
- Wat zijn de gevolgen van online discriminatie voor de slachtoffers?
- In welke mate vinden melding en aangifte plaats van online discriminatie?

Online oproepen tot openbare-ordeverstoring

- Hoe vaak zien Nederlanders online oproepen tot openbare-ordeverstoring?
- Om welke soorten verstoring van de openbare orde gaat het?
- Hoe vaak vindt er een openbare-ordeverstoring plaats in de eigen buurt?
- Om welke soorten verstoring van de openbare orde in de buurt gaat het?
- In welke mate ervaart men zelf overlast van openbare-ordeverstoring in de eigen buurt?

Beide laatste thema's met de bijbehorende onderzoeksvragen (online discriminatie en online oproepen tot openbare-ordeverstoring) vallen buiten de scope van online criminaliteit, maar zijn op verzoek van het ministerie van J&V toegevoegd.

Opzet van het onderzoek

De cijfers in dit onderzoek zijn gebaseerd op een internetenquête onder de Nederlandse bevolking van 15 jaar en ouder (ruim 14,7 miljoen personen). Het onderzoek heeft plaatsgevonden van augustus tot en met oktober 2022. Voor het onderzoek zijn honderdduizend personen benaderd. Bijna 33 duizend personen hebben de vragenlijst ingevuld, een respons van 32,9 procent. Dit grote aantal respondenten maakt het mogelijk om niet alleen voor de totale 15-plus bevolking maar ook voor groepen daarbinnen betrouwbare uitspraken te doen over online veiligheid en criminaliteit in Nederland.

Vragenlijst

De vragen die online veiligheid en criminaliteit meten zijn door het CBS opgesteld in overleg met het ministerie van J&V. Met name voor online criminaliteit is daarbij zoveel mogelijk aangesloten bij de vraagstellingen in de Veiligheidsmonitor (zie ook hieronder).

De publicatie wordt uitgebracht als webpublicatie en is beschikbaar via de website van het CBS.

Extra informatiebronnen: ICT-enquête, Veiligheidsmonitor en Prevalentiemonitor

In deze publicatie is aanvullend gebruik gemaakt van informatie uit de volgende bronnen:

ICT-enquête huishoudens en personen
Dit onderzoek verzamelt informatie over de toegang en het gebruik van ICT-apparatuur en internet onder huishoudens en personen. De enquête wordt jaarlijks in de periode april-juli door het CBS uitgevoerd onder personen van 12 jaar of ouder. Ook wordt het onderzoek onder 16- tot 75-jarigen door alle lidstaten van de EU uitgevoerd in opdracht van de Europese Commissie. In 2022 hebben ongeveer 6 duizend Nederlanders deelgenomen aan het onderzoek.

Veiligheidsmonitor
De Veiligheidsmonitor is een tweejaarlijkse veiligheids- en slachtofferenquête van het CBS en het ministerie van Justitie en Veiligheid. Een van de thema's is online criminaliteit. In 2021 hebben ongeveer 172 duizend mensen van 15 jaar of ouder aan het onderzoek deelgenomen.

Prevalentiemonitor Huiselijk Geweld en Seksueel Grensoverschrijdend gedrag
De Prevalentiemonitor is een tweejaarlijkse enquête die het CBS op verzoek van het WODC uitvoert. Een van de thema's is online seksuele intimidatie. In 2022 hebben ongeveer 24 duizend personen van 16 jaar of ouder aan het onderzoek deelgenomen.

Wanneer in deze publicatie gebruik wordt gemaakt van data uit bovenstaande bronnen wordt dit expliciet vermeld.

1.1 Samenvatting

De antwoorden op de centrale onderzoekvragen worden hieronder samengevat. Eerst volgt nog beknopte informatie over de opzet van het onderzoek Online Veiligheid en Criminaliteit (OVeC) 2022.

Opzet van het onderzoek

OVeC 2022 is uitgevoerd door het CBS op verzoek van het ministerie van J&V. De cijfers zijn gebaseerd op een internetenquête onder de Nederlandse bevolking van 15 jaar en ouder (ruim 14,7 miljoen personen). Het onderzoek heeft plaatsgevonden van augustus tot en met oktober 2022. Voor het onderzoek zijn honderdduizend personen benaderd. Bijna 33 duizend personen hebben de vragenlijst ingevuld, een respons van 32,9 procent. De vragenlijst is opgesteld door het CBS in overleg met het ministerie van J&V. Het gaat om zelfrapportage, dus om opvattingen, percepties en ervaringen van respondenten. En het is een steekproefonderzoek. Dit betekent dat de weergegeven cijfers schattingen zijn waarvoor betrouwbaarheidsintervallen gelden. In de tabellenset die bij deze publicatie hoort zijn deze betrouwbaarheidsintervallen opgenomen in de vorm van boven- en ondergrenzen behorende bij deze schattingen.

Antwoorden op de onderzoeksvragen

Online veiligheid

Hoe gaan Nederlanders om met privacy en het beschermen van persoonlijke gegevens op internet?

Nederlanders zijn relatief terughoudend om privacygevoelige persoonlijke informatie online door te geven zoals een kopie van de bankpas, van een paspoort, ID-kaart of rijbewijs, of het Burgerservicenummer (BSN). Drie kwart gaf aan dat ze een kopie van de bankpas niet online doorgeven; 1 op de 5 doet het alleen als het moet. Ruim de helft deelt geen kopie van het paspoort, ID-kaart, rijbewijs of van het BSN via internet. Ruim een derde doet dit alleen als het moet.

Bijna alle Nederlanders (95 procent) nemen een of meerdere maatregelen om hun persoonlijke gegevens op internet te beschermen. Van de acht in het onderzoek voorgelegde beschermingsmaatregelen heeft in 2022 60 procent van de Nederlanders 5 of meer maatregelen genomen, 25 procent 3 of 4 maatregelen, en 11 procent 1 of 2.

In welke mate zijn Nederlanders bekend met begrippen op het terrein van internetveiligheid?

Nederlanders zijn het meest bekend met de begrippen spam, hacken, identiteitsfraude en back-ups maken: van elk van deze begrippen zegt ongeveer 90 procent van de 15-plussers te weten wat het betekent. 80 procent weet wat phishing is en eenzelfde deel weet wat met WhatsApp-fraude wordt bedoeld. Het minst bekend zijn Nederlanders met het relatief nieuwe begrip social engineering[4)]: 23 procent weet wat dit is. Ook de begrippen VPN-verbinding, Dos- of DDos-aanval, en ransomware zijn minder bekend: ongeveer de helft weet wat hiermee bedoeld wordt.

In welke mate maken Nederlanders zich zorgen over internetveiligheid?

De meeste zorgen als het gaat om internetveiligheid hebben Nederlanders over misbruik van bankgegevens en misbruik van persoonsgegevens: ruim een kwart maakt zich veel zorgen over deze veiligheidsaspecten. Over het misbruik van accounts en hacken van een apparaat of account maakt ongeveer 20 procent zich veel zorgen. Het laagst is de bezorgdheid om online gediscrimineerd te worden: 8 procent maakt zich hierover veel zorgen en meer dan 70 procent geen zorgen.

Welke maatregelen nemen Nederlanders om te voorkomen dat ze slachtoffer worden van online criminaliteit?

De meest gebruikte maatregelen om apparatuur en/of accounts met persoonlijke informatie te beveiligen tegen misbruik door anderen zijn het vergrendelen van apparaten en het controleren van bijlages in e-mails vóór het openen ervan: de eerste maatregel werd door 8 op de 10 Nederlanders vaak genomen, de tweede door drie kwart. Bijna 6 op de 10 zeiden updates van apparatuur of apps direct of zo snel mogelijk uit te voeren. Het gebruik van tweetrapsverificatie en vooral het gebruik van wachtwoorden van minimaal 16 tekens zijn maatregelen die het minst vaak worden genomen. Wel gaven relatief veel Nederlanders aan voor sommige (maar niet voor alle) accounts een ander wachtwoord te gebruiken.

Hoe veilig voelen Nederlanders zich op internet en hoe schatten ze de kans in om slachtoffer te worden van online criminaliteit?

In 2022 gaf de helft van de Nederlanders aan zich veilig of heel veilig te voelen als ze internet gebruiken. 4 procent voelde zich onveilig of heel onveilig. De rest (44 procent) voelde zich veilig noch onveilig.

Vooral 15- tot 18-jarigen en mannen voelden zich (heel) veilig op internet. Vrouwen en 75-plussers voelden zich er het vaakst (heel) onveilig. De veiligheidsbeleving op internet verschilt niet naar opleidingsniveau.

Vooral als het gaat om voorvallen die te maken hebben met online bedreiging en intimidatie schatten Nederlanders de kans om zelf hiervan slachtoffer te worden relatief laag in: grofweg 10 procent acht de kans aanwezig om zelf slachtoffer te worden van online pesten, bedreiging of discriminatie. Bijna de helft van de bevolking acht de kans aanwezig om slachtoffer te worden van aankoop- of verkoopfraude. Ook de kans om gehackt te worden wordt vrij hoog ingeschat.

Online criminaliteit

Wat is aard en omvang van het slachtofferschap van online criminaliteit?

In 2022 gaf 15 procent van de Nederlanders van 15 jaar of ouder aan in de afgelopen 12 maanden slachtoffer te zijn geweest van online criminaliteit. Dit zijn 2,2 miljoen mensen. De meesten, 8 procent, waren slachtoffer van oplichting en fraude, vooral van aankoopfraude. 5 procent had te maken met hacken en 4 procent met bedreiging of intimidatie. Een half procent werd slachtoffer van andere online delicten.

Jongeren werden relatief vaak slachtoffer van online criminaliteit. Zo werd 21 procent van de 15- tot 25-jarigen slachtoffer, jonge vrouwen iets vaker dan jonge mannen. Vooral bij het slachtofferschap van online bedreiging en intimidatie is er een groot verschil tussen jongeren en oudere leeftijdsgroepen. Verder hadden biseksuele vrouwen en aseksuelen vaker met online criminaliteit te maken dan anderen. Dit komt door hun hoge slachtofferschap van online bedreiging en intimidatie.

Wie zijn de daders van online criminaliteit?

Vragen over de bekendheid met dader(s) van online criminaliteit zijn alleen gesteld voor online bedreiging en intimidatie omdat het hierbij (in tegenstelling tot bij online oplichting en hacken) gaat om interpersoonlijke voorvallen die vaak gericht zijn op het veroorzaken van negatieve emoties bij het slachtoffer en waarbij het slachtoffer bekend kan zijn met de dader(s). Ruim 4 op de 10 slachtoffers van voorvallen op het terrein van online bedreiging en intimidatie kende de dader(s). Bij pesten en stalken was dit het vaakst het geval. De meest genoemde daders van online bedreiging en intimidatie zijn de ex-partner, een vriend/vriendin of een medestudent/-scholier. De ex-partner wordt bij online stalken en shamesexting het vaakst als dader genoemd, respectievelijk door 18 en 14 procent van de slachtoffers. Bij online pesten, waarvan jongeren het vaakst slachtoffer zijn, wordt een medestudent/-scholier (15 procent) of een vriend/vriendin (12 procent) het vaakst als dader genoemd.

Wat zijn de gevolgen van online criminaliteit voor de slachtoffers?

Voor de meeste slachtoffers van online criminaliteit heeft of had het voorval tot gevolg dat men minder vertrouwen had in mensen (37 procent) en dat men zich minder veilig voelde (30 procent).

Slaapproblemen, depressieve klachten, angstklachten en het voorval steeds opnieuw beleven werden elk door 7 á 8 procent van de slachtoffers genoemd. Het telkens opnieuw beleven van het voorval, slaapproblemen, depressieve klachten en angstklachten worden door slachtoffers van online bedreiging en intimidatie vaker gerapporteerd dan door slachtoffers van de andere online delicten.

In welke mate vindt melding en aangifte van online criminaliteit plaats?

Ruim 2 op de 10 slachtoffers van online criminaliteit hebben bij de politie gemeld wat hen overkomen is, en bijna 5 op de 10 slachtoffers hebben dit bij een andere instantie of persoon gedaan. Bijna alle meldingen van online criminaliteit bij de politie resulteerden in een aangifte (21 procent maakte een melding; 19 procent deed aangifte). De meest genoemde reden om het voorval niet bij de politie te melden of aangifte te doen is dat er niet aan wordt gedacht of dat men het niet zo belangrijk vindt, gevolgd door 'het helpt toch niets'.

Online discriminatie

In welke mate voelen Nederlanders zich online gediscrimineerd?

2 procent van de Nederlanders voelden zich in 2022 weleens online gediscrimineerd. Dat zijn bijna 340 duizend mensen. Jongeren van 15 tot 25 jaar gaven dit met 5 procent relatief vaak aan. Biseksuele vrouwen (9 procent) en homoseksuele mannen (7 procent) hadden er vaker mee te maken dan personen met een andere seksuele oriëntatie. Personen geboren in Nederland met herkomst buiten Europa (tweede generatie) ervoeren met 7 procent het vaakst online discriminatie. Personen geboren in het buitenland voelden zich met 4 procent vaker gediscrimineerd dan personen geboren in Nederland (2 procent).

Op welke gronden en op welke manieren voelen de slachtoffers zich online gediscrimineerd?

Van degenen die online discriminatie ervoeren ging het bij 40 procent om discriminatie op grond van ras of huidskleur, gevolgd door discriminatie op grond van nationaliteit (34 procent) en godsdienst of levensbeschouwing (29 procent).

7 op de 10 personen die discriminatie ervoeren, gaven aan dat dit kwam door discriminerende opmerkingen. Grofweg 5 op de 10 zeiden dat dit kwam door een negatief beeld/stigmatisering, door ongelijke behandeling/benadeling/het voortrekken van bepaalde groepen, of door agressief taalgebruik. Andere manieren van discriminatie zoals negeren/uitsluiten, roddels of bedreiging werden minder vaak genoemd.

Wat zijn de gevolgen van online discriminatie voor de slachtoffers?

Als het gaat om emotionele of psychische gevolgen gaf meer dan de helft (55 procent) van degenen die online discriminatie ervoeren aan dat zij daardoor minder vertrouwen in mensen hebben. Iets meer dan 30 procent voelt/voelde zich minder veilig en 20 procent heeft/had depressieve klachten. Angstklachten en/of paniekaanvallen, slaapproblemen en het voorval telkens opnieuw beleven werden door ongeveer 1 op de 10 genoemd.

In welke mate vindt melding en aangifte plaats van online discriminatie?

Bijna een kwart (23 procent) van de mensen die zich in de afgelopen 12 maanden online gediscrimineerd voelden, heeft dit ergens gemeld. De meesten meldden het direct bij de website (12 procent); 6 procent meldde het bij de politie, 4 procent op het werk en 3 procent op school. Minder dan 1 procent meldde het bij het Meldpunt voor Internetdiscriminatie, bij het College voor de Rechten van de Mens of bij een gemeentelijke antidiscriminatievoorziening.

5 procent van degenen die online discriminatie ervoeren, deden hiervan aangifte bij de politie. De meest genoemde reden om geen melding of aangifte bij de politie te doen is dat het toch niet helpt, gevolgd door dat er niet aan is gedacht/dat het niet zo belangrijk was.

Online oproepen tot openbare-ordeverstoring

Hoe vaak zien Nederlanders online oproepen tot openbare-ordeverstoring?

In 2022 gaf 9 procent van de Nederlanders aan in de afgelopen 12 maanden weleens online berichten, bijvoorbeeld via sociale media of in app-groepen, gezien te hebben waarin opgeroepen werd tot openbare-ordeverstoring of activiteiten die vaak daartoe leiden, zoals demonstraties, rellen of illegale feesten. Dat zijn 1,4 miljoen mensen.

Om welke soorten verstoring van de openbare orde gaat het?

Verreweg de meesten die berichten zagen waarin werd opgeroepen tot openbare-ordeverstoring, gaven aan dat het (laatste) bericht ging om een oproep tot demonstratie (59 procent). Berichten die oproepen tot illegale feesten of evenementen werden door 15 procent genoemd en berichten die oproepen tot rellen door 10 procent. 6 procent zei dat het bericht opriep tot het bedreigen van bekende personen of politici. 3 procent noemde berichten met een andere inhoud, waaronder oproepen tot burgerlijke ongehoorzaamheid, ageren tegen politiek beleid, boycotten van producten, pesterijen, niet laten vaccineren, onwaarheden of complottheorieën verspreiden, of onrust veroorzaken bij de werkgever.

Hoe vaak vindt er openbare-ordeverstoring plaats in de eigen buurt?

In 2022 gaf 5 procent van de Nederlanders aan dat er in de afgelopen 12 maanden in hun eigen buurt weleens een evenement heeft plaatsgevonden waarbij de openbare orde werd verstoord. Openbare-ordeverstoring in de eigen buurt vindt in de stad vaker plaats dan op het platteland. Zo maakte 7 procent van de inwoners van zeer sterk stedelijke gemeenten dit mee, tegen 3 procent van de inwoners van niet-stedelijke gemeenten. In de G4, de vier grote steden samen, werd dit door 9 procent van de bewoners meegemaakt.

Om welke soorten verstoring van de openbare orde in de buurt gaat het?

De meesten (41 procent) zeiden dat het bij de openbare-ordeverstoring in de buurt ging om demonstraties. Daarna volgden rellen (27 procent), illegale feesten of evenementen (12 procent), straatraces (5 procent) en bedreiging van bekende personen of politie (2 procent). Ruim 10 procent noemde iets anders, bijvoorbeeld bedreiging en vernieling, hangjongeren, boerenprotesten/blokkades door boeren met trekkers, brandstichting, corona-ongeregeldheden en lockdownprotesten, samenscholingen tijdens corona, ordeverstoring vanwege vuurwerkverbod/illegaal vuurwerk afsteken, oudejaarsongeregeldheden, of feestjes waar mensen kwamen die niet welkom waren.

In welke mate ervaart men zelf overlast van openbare-ordeverstoring in de eigen buurt?

Van de mensen die aangaven dat openbare-ordeverstoring in de eigen buurt in de afgelopen 12 maanden weleens is voorgekomen, zei 11 procent hier zelf veel overlast van te hebben ervaren. 36 procent ervoer een beetje overlast. Ruim de helft had er zelf geen overlast van.

Inwoners van zeer sterk stedelijke gemeenten en sterk stedelijke gemeenten die openbare-ordeverstoring meemaakten ervoeren met respectievelijk 14 en 12 procent daar vaker veel overlast van dan inwoners van minder stedelijke gemeenten (grofweg 6 procent). In de vier grote steden (G4) zei 15 procent van de inwoners die weleens openbare-ordeverstoring in de buurt hebben gezien, dat ze hier veel overlast van hebben ervaren.

1.2 Leeswijzer

Eerst wordt in hoofdstuk 2 een beeld geschetst van het internetgebruik van Nederlanders en van hun online activiteiten. Dit als introductie op hoofdstuk 3 waarin het thema internetveiligheid centraal staat. In de hoofstukken 4 tot en met 7 worden de verschillende vormen van online criminaliteit inclusief een totaalbeeld beschreven. Daarna komen de thema's online discriminatie (hoofdstuk 8) en online oproepen tot openbare-ordeverstoring (hoofdstuk 9) aan de orde. Afgesloten wordt met conclusies en aanbevelingen (hoofdstuk 10).

De bijlagen bevatten tabellen met achterliggend cijfermateriaal, een onderzoeksverantwoording, referenties, een verwijzing naar meer cijfers, en een overzicht van medewerkers die aan deze publicatie hebben bijgedragen.

[1)] In het onderzoek Digitale Veiligheid en Criminaliteit (Akkermans et al., 2018) zijn de thema's digitale veiligheid en criminaliteit weliswaar ook onderzocht, maar dit was een pilotonderzoek dat primair als doelstelling had vraagstellingen over beide thema's te testen.
[2)] In dit rapport wordt vanwege het leesgemak gesproken over 'Nederlanders', waar het eigenlijk gaat om inwoners van Nederland, ongeacht hun nationaliteit.
[3)] De cijfers over (slachtofferschap van) online criminaliteit hebben betrekking op de periode van 12 maanden voorafgaand aan het onderzoek. De enquêtering heeft plaatsgevonden van augustus tot en met oktober 2022. Dit betekent dat de cijfers over online criminaliteit betrekking hebben op de periode augustus/oktober 2021 – augustus/oktober 2022.
[4)] Social engineering is het misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid. Criminelen (social engineers) proberen vertrouwelijke informatie van iemand los te krijgen. Ze willen bijvoorbeeld persoonlijke gegevens (phishing) en beveiligingscodes te weten komen of malware installeren (bron: Veiligbankieren.nl).

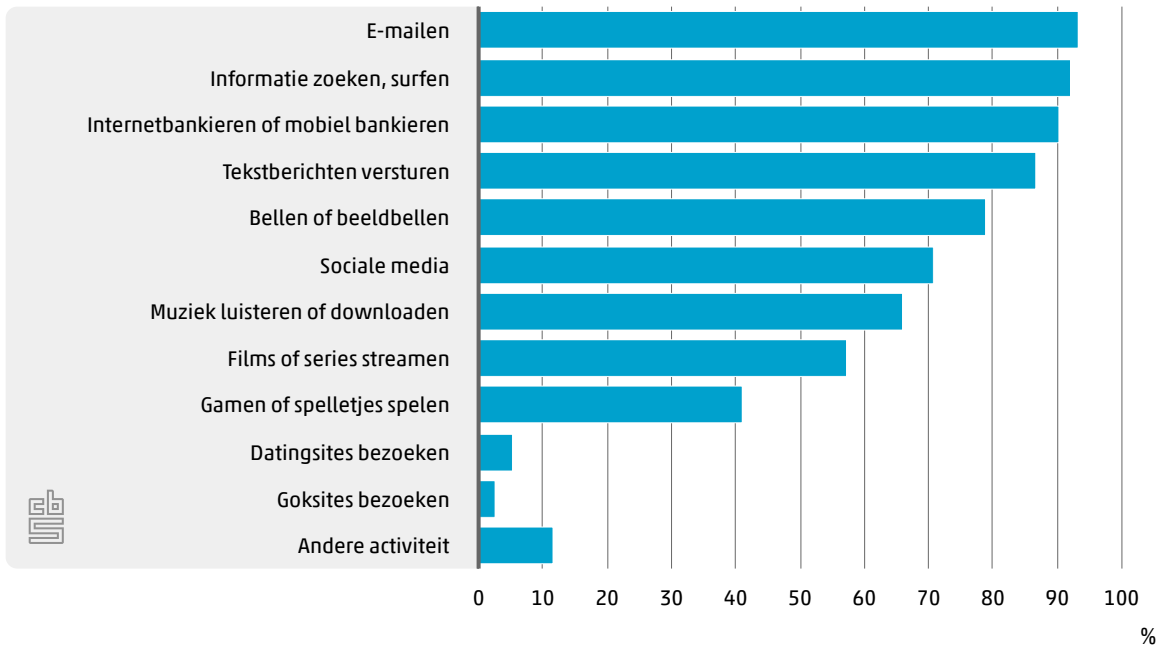
2. Internetgebruik

In de periode dat het onderzoek is uitgevoerd (augustus – oktober 2022) telde Nederland 14,7 miljoen mensen van 15 jaar of ouder. Bijna iedereen van hen (99 procent) gaf aan in de afgelopen 12 maanden internet te hebben gebruikt. In dit hoofdstuk wordt als introductie op de volgende hoofdstukken over online veiligheid en criminaliteit, kort beschreven waarvoor Nederlanders internet gebruiken.

2.1 Activiteiten op internet

Nederlanders gebruiken het internet het vaakst om te e-mailen: in 2022 gaf 94 procent aan dit te hebben gedaan in de afgelopen 12 maanden. Ook voor het opzoeken van informatie/surfen op internet en voor internet- of mobiel bankieren werd het internet door ruim 90 procent gebruikt. Andere veelvoorkomende online activiteiten waren (WhatsApp)berichten versturen (87 procent), bellen of beeldbellen (79 procent) en socialemediagebruik (71 procent). Grofweg de helft gebruikte internet voor ontspanning, zoals het streamen van films of series (57 procent) of gamen/spelletjes spelen (41 procent). Van de onderzochte activiteiten was het percentage het laagst bij het bezoek van datingsites (5 procent) en goksites (3 procent).

2.1.1 Activiteiten op internet[1) 2)], 2022

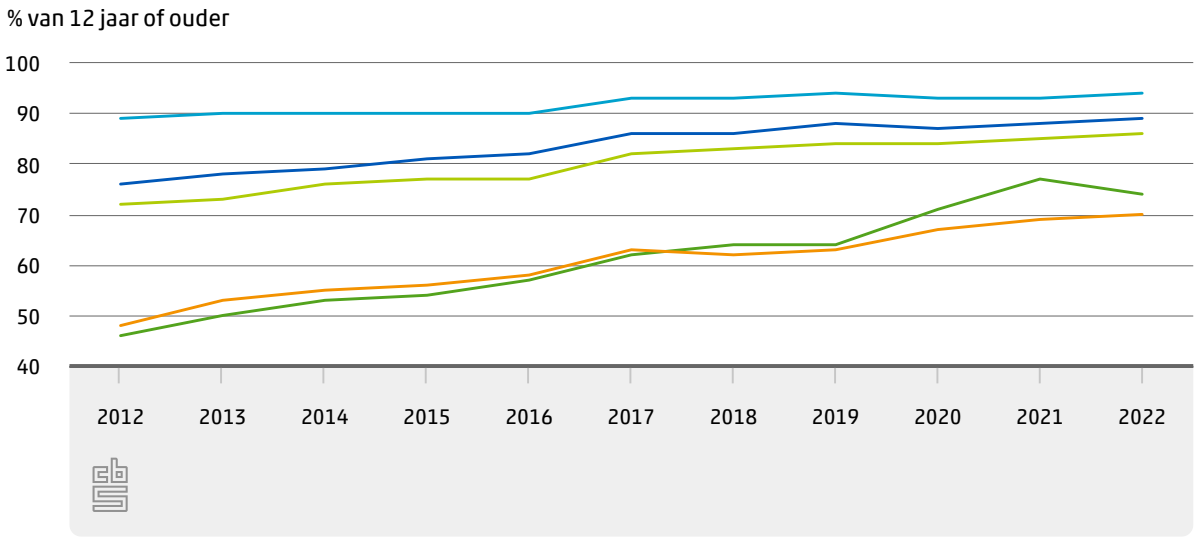


[1)] Het gaat om activiteiten in de periode van 12 maanden voorafgaand aan het onderzoek.
[2)] Meerdere antwoorden mogelijk.

Trend internetgebruik en online activiteiten

Uit de ICT-enquête huishoudens en personen, waarmee sinds 2012 informatie wordt verzameld over het gebruik van ICT-apparatuur en internet door Nederlanders van 12 jaar of ouder, blijkt dat internet niet meer weg te denken is uit het dagelijks leven van de meeste Nederlanders. In 2022 gebruikten vrijwel alle 12-plussers (94 procent) het internet. In 2012 was het internetgebruik met 89 procent ook al hoog. Het *dagelijkse* internetgebruik is sterk toegenomen van 76 procent in 2012 tot 90 procent in 2022. Online activiteiten zoals internetbankieren en socialemediagebruik zijn in de afgelopen tien jaar gestaag gestegen. Het aandeel Nederlanders dat online aankopen doet nam toe in 2021, het tweede jaar waarin door de coronapandemie mensen door lockdowns en andere beperkingen vaak aan huis waren gebonden. In 2022, het jaar waarin de coronamaatregelen werden versoepeld en deels opgeheven, nam het percentage online kopers iets af.

Internetgebruik en online activiteiten



Bron: CBS, ICT-enquête personen en huishoudens

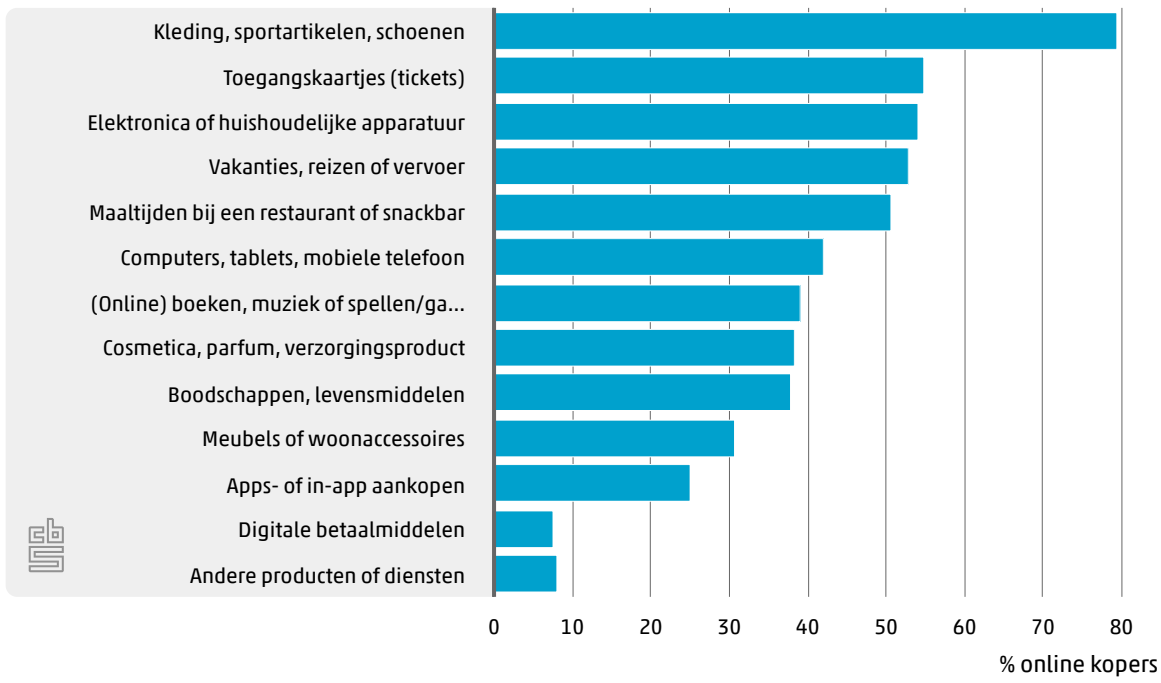
* Het gaat om internetgebruik in de periode van 12 maanden voorafgaand aan het onderzoek.
** Het gaat om activiteiten in de periode van 3 maanden voorafgaand aan het onderzoek.

2.2 Online kopen

Het online bestellen van producten of diensten is wijdverbreid in Nederland. In 2022 gaf 86 procent van de mensen van 15 jaar of ouder aan online aankopen te hebben gedaan in de afgelopen 12 maanden.

Kleding, sportartikelen of schoenen werden in 2022 het meest online gekocht, 80 procent van de online kopers deed dit. Daarna volgden toegangskaartjes, elektronica/huishoudelijke apparatuur, vakanties/reizen, en maaltijden bij een restaurant of snackbar met elk ruim 50 procent. Computers, mobiele telefoons en dergelijke werden door ruim 40 procent online gekocht, en (online) boeken, muziek, spellen of games, cosmetica of verzorgingsproducten, en boodschappen of levensmiddelen elk door bijna 40 procent.

2.2.1 Online gekochte producten of diensten[1)], 2022



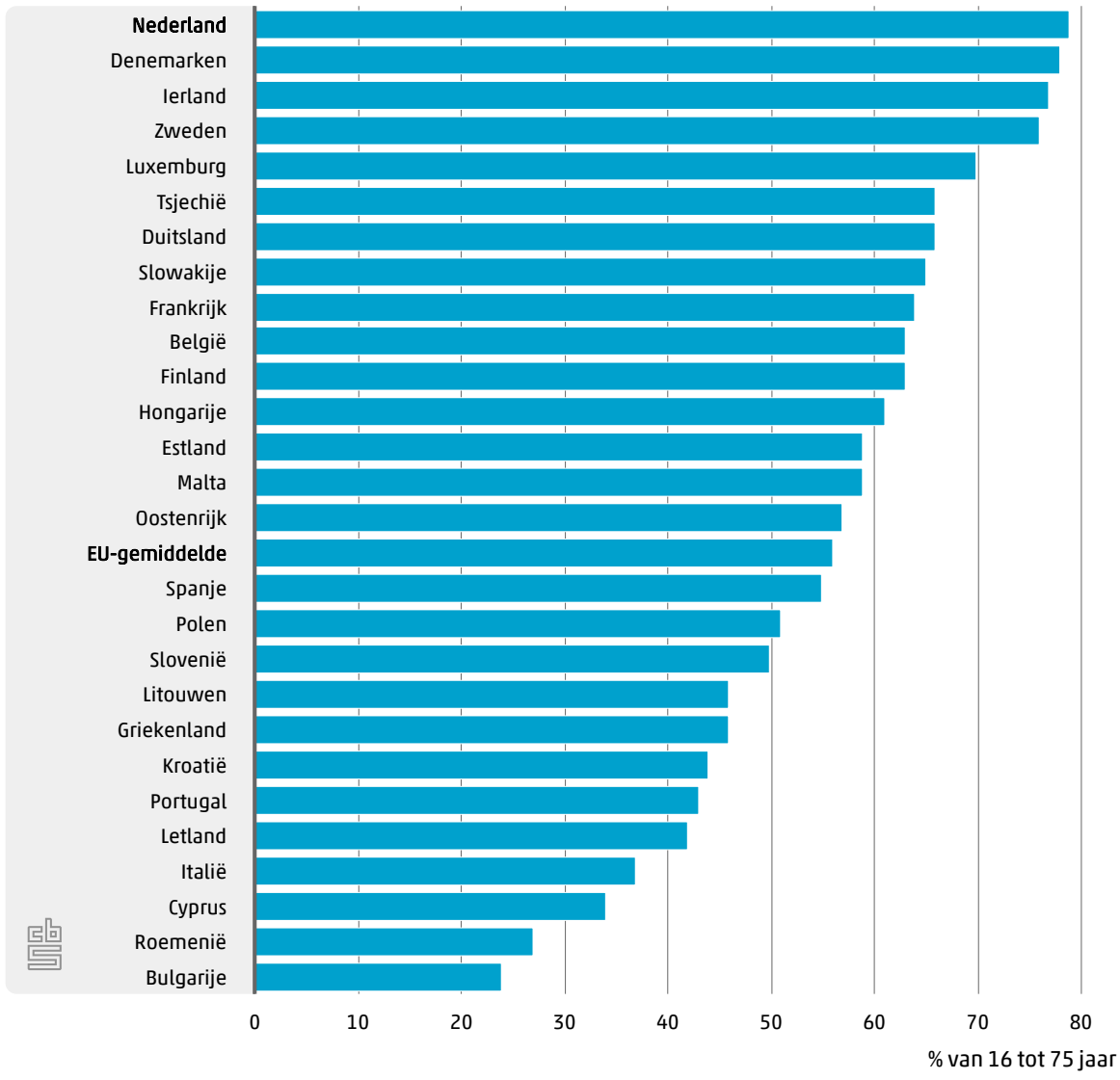
[1)] Meerdere antwoorden mogelijk.

De meeste producten of diensten werden bij grote, bekende webshops gekocht: 93 procent van de online kopers deed dat in 2022. Bij kleine, minder bekende webshops heeft ruim de helft iets gekocht. Iets meer dan een kwart winkelde online bij niet-Nederlandse webshops. Op online handelsplatforms zoals Marktplaats of eBay kocht ruim 40 procent producten of diensten. Via sociale media zoals Facebook of LinkedIn deed 1 op de 10 mensen online aankopen.

Online kopen in Nederland en de andere EU-landen

Het aandeel 16- tot 75-jarigen[5)] dat online aankopen deed (in de 3 maanden voorafgaand het onderzoek) was in 2022 met 79 procent in geen enkel ander EU-land zo hoog als in Nederland. Op de plaatsen 2, 3 en 4 volgden Denemarken, Ierland en Zweden met respectievelijk 78, 77 en 76 procent. Met 20 á 30 procent was het percentage online kopers het laagst in Roemenië en Bulgarije. Het gemiddelde van de 27 EU-landen bedroeg 56 procent in 2022. In 2021 was dat 57 procent.

Online kopers in de EU-landen, 2022



5) In statistieken over internetgebruik in de EU wordt een andere leeftijdsafbakening gebruikt (16- tot 75-jarigen) dan in de statistieken over internetgebruik in Nederland (12 jaar of ouder). Hierdoor wijken de cijfers in de EU-statistieken af van die in de Nederlandse statistieken.

3. Internetveiligheid en online veiligheidsbeleving

Nederlanders maken steeds meer gebruik van internet. Hiermee stijgt het risico om slachtoffer te worden van mensen die dit medium gebruiken voor criminele activiteiten. Het veilig gebruik maken van internet en de beleving van deze internetveiligheid zijn dan ook belangrijke thema's, zeker in relatie tot online criminaliteit. In dit hoofdstuk wordt ingegaan op een aantal aspecten van deze (beleving van) internetveiligheid, waaronder de bereidheid om persoonsgegevens online door te geven, de bescherming van privacy, de kennis en de bezorgdheid over internetveiligheid. Ook wordt beschreven welke concrete beveiligingsmaatregelen mensen treffen. Afgesloten wordt met een beeld van de algemene gevoelens van (on)veiligheid op internet en de risico-inschatting om slachtoffer te worden van online criminaliteit.

3.1 Privacy en bescherming persoonsgegevens

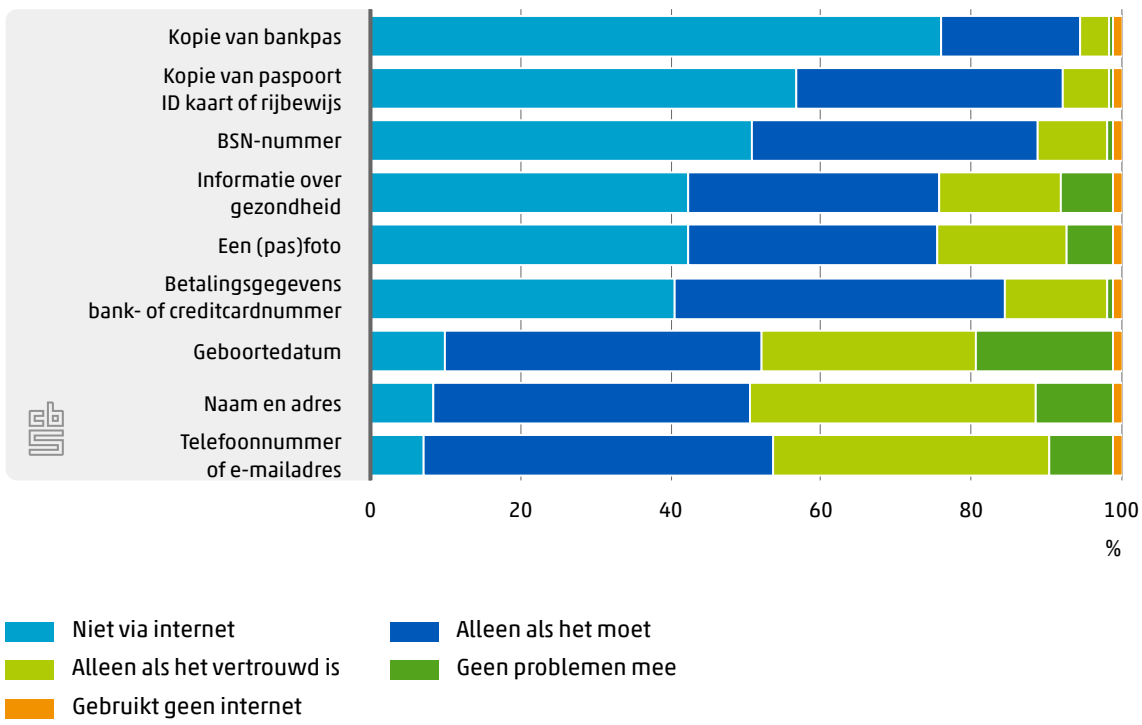
Bereidheid doorgeven persoonlijke informatie op internet

Nederlanders zijn relatief terughoudend om privacygevoelige persoonlijke informatie zoals een kopie van de bankpas, paspoort, ID-kaart of rijbewijs, of het Burgerservicenummer (BSN) online door te geven. Drie kwart gaf aan dat ze een kopie van de bankpas niet online doorgeven; 1 op de 5 doet het alleen als het moet. Ruim de helft deelt geen kopie van het paspoort, ID-kaart, rijbewijs of van het BSN via internet. Ruim een derde doet dit alleen als het moet.

Iets meer dan 40 procent gaf aan informatie over hun gezondheid of een (pas)foto niet via internet te delen; en iets meer dan 30 procent doet dat alleen als het moet. Ook betalingsgegevens zoals een bank- of creditcardnummer worden door ruim 40 procent niet online gedeeld. Een vergelijkbaar deel doet dit alleen als het moet.

Met het online doorgeven van persoonsgegevens zoals geboortedatum, naam, adres, telefoonnummer of e-mailadres zijn Nederlanders minder terughoudend: ongeveer 1 op de 10 zei dit niet te doen, ruim 4 op de 10 doen dit alleen als het moet.

3.1.1 Bereidheid om persoonlijke informatie online door te geven, 2022



Voor het online doorsturen van een kopie van een paspoort, identiteitskaart of rijbewijs is de zogeheten KopieIDApp van de Rijksoverheid beschikbaar. Twee derde van de mensen die een kopie van hun paspoort, identiteitskaart of rijbewijs online doorgaven, zei geen gebruik te maken van deze KopieIDApp. Bijna twee op de tien (18 procent) deden dat naar eigen zeggen altijd, en een vergelijkbaar deel (17 procent) deed dat soms.

Beschermingsmaatregelen persoonlijke informatie op internet

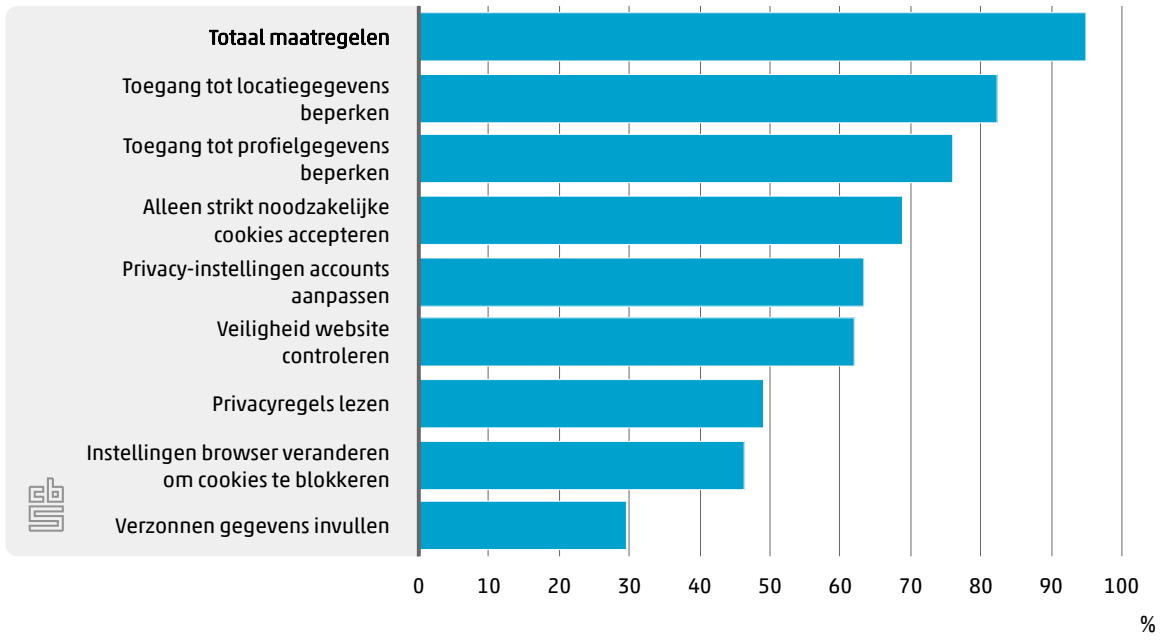
In OVeC 2022 is niet alleen onderzocht of mensen persoonlijke informatie online doorgeven, maar ook welke maatregelen ze treffen om privacygevoelige gegevens te beschermen.

Bijna alle Nederlanders nemen een of meer maatregelen om hun persoonlijke gegevens op internet te beschermen: 95 procent gaf aan dat te hebben gedaan in 2022. Van de acht in het onderzoek voorgelegde beschermingsmaatregelen heeft 60 procent van de Nederlanders 5 of meer maatregelen genomen, 25 procent 3 of 4 maatregelen, en 11 procent 1 of 2.

Als het gaat om de afzonderlijke beschermingsmaatregelen gaf ruim 80 procent aan de toegang tot (online) locatiegegevens te beperken of te weigeren. Ongeveer 75 procent zei de toegang tot hun profiel en geplaatste berichten op sociale media te beperken. Het alleen accepteren van strikt noodzakelijke cookies bij gebruik van websites, het aanpassen van privacy-instellingen van accounts, en het controleren van de veiligheid van het url-adres van de website worden elk door een meerderheid van 60 á 70 procent gedaan.

Minder vaak genomen maatregelen zijn het lezen van de privacyregels en het veranderen van browserinstellingen (beide minder dan 50 procent) en het invullen van verzonnen persoonsgegevens (minder dan 30 procent).

3.1.2 Beschermingsmaatregelen persoonlijke gegevens op internet[1)], 2022

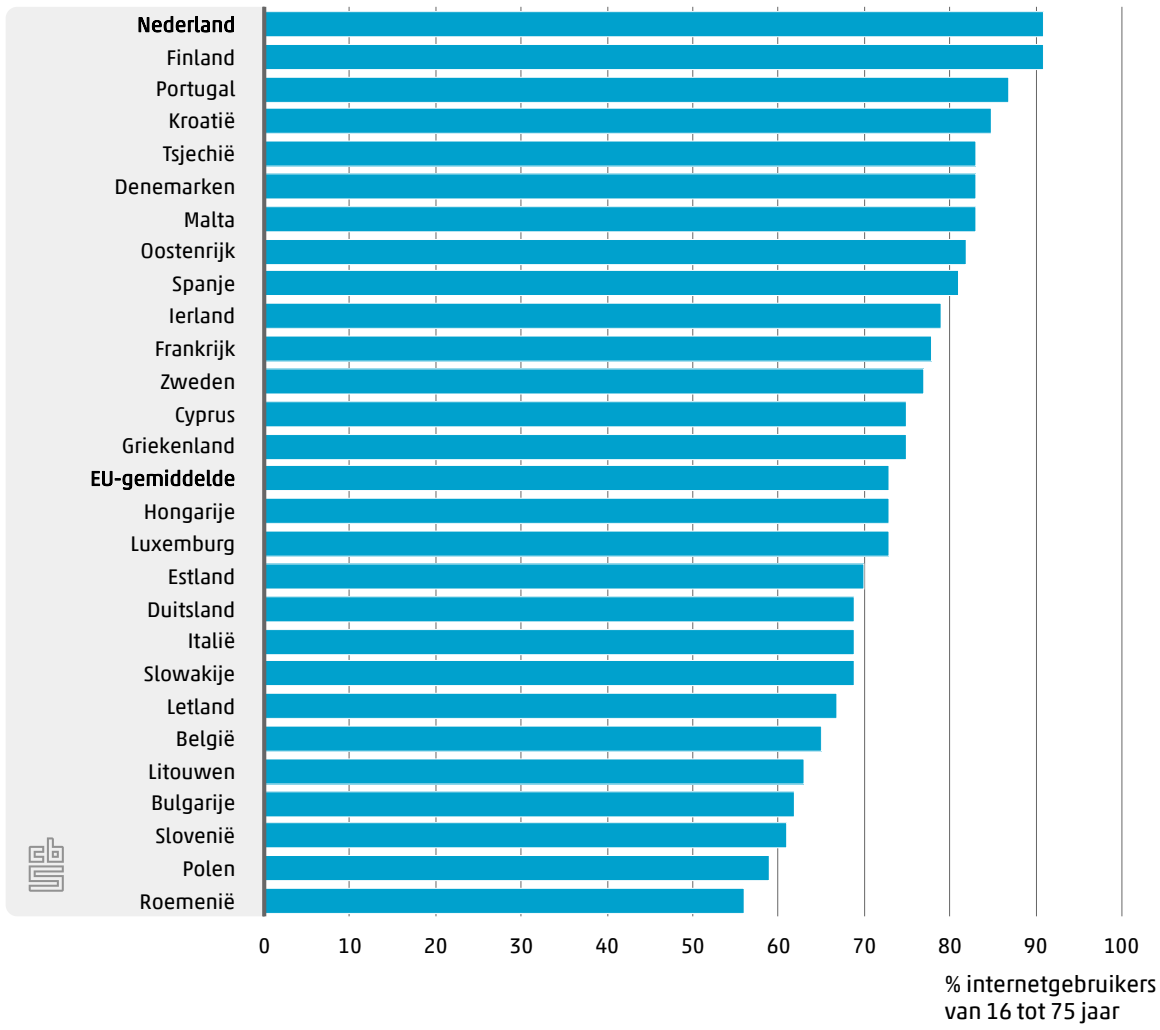


[1)] Meerdere antwoorden mogelijk.

Beschermingsmaatregelen persoonlijke gegevens in Nederland en de andere EU-landen

In 2021, het meest recente jaar waarvoor EU-cijfers beschikbaar zijn, had Nederland, samen met Finland, met 91 procent het hoogste percentage 16- tot 75-jarige internetgebruikers dat maatregelen nam om persoonlijke informatie op internet te beschermen. Het laagst was dit percentage met respectievelijk 59 en 56 procent in Polen en Roemenië. Het EU-gemiddelde bedroeg 73 procent.

Beschermingsmaatregelen persoonlijke gegevens op internet in Nederland en de EU, 2021



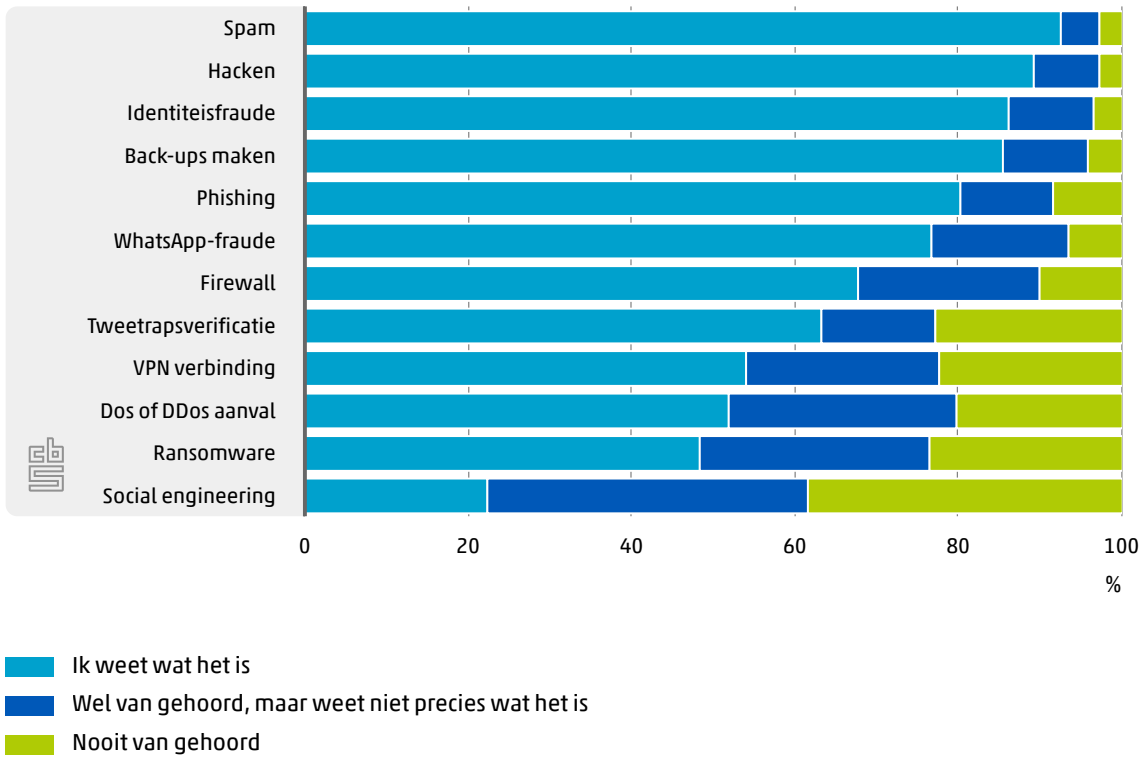
Bron: Eurostat

Als het gaat om afzonderlijke maatregelen zoals het beperken of het weigeren van de toegang tot locatiegegevens had Nederland in 2021 met 80 procent verreweg het hoogste percentage in de EU, waar het gemiddelde 50 procent was.

3.2 Bekendheid met begrippen internetveiligheid

Nederlanders zijn het meest bekend met de begrippen spam, hacken, identiteitsfraude en back-ups maken: van elk van deze begrippen zegt ongeveer 90 procent van de 15-plussers te weten wat het betekent. 80 procent weet wat phishing is en bijna 80 procent weet wat met WhatsApp-fraude wordt bedoeld. Het minst bekend zijn Nederlanders met het relatief nieuwe begrip social engineering[6)]: 23 procent weet wat dit is. Ook de begrippen VPN-verbinding, Dos- of DDos-aanval, en ransomware zijn minder bekend: ongeveer de helft weet wat hiermee bedoeld wordt.

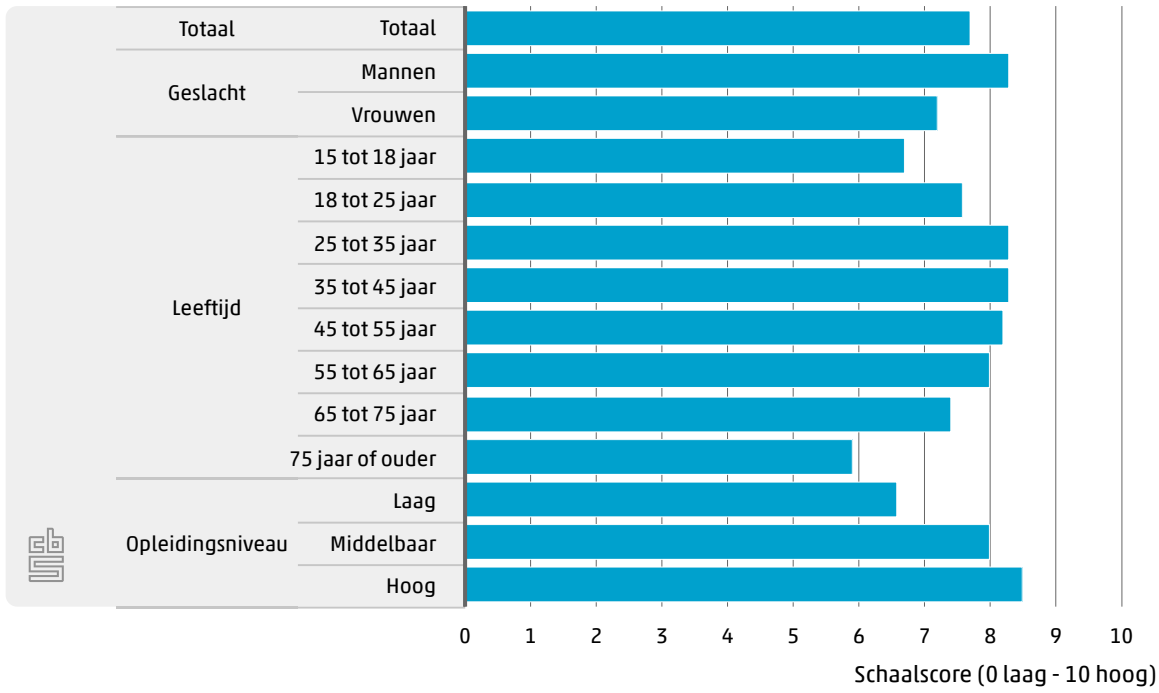
3.2.1 Bekendheid met begrippen internetveiligheid, 2022



Bekendheid met begrippen internetveiligheid naar persoonskenmerken

Op basis van de antwoorden op de 12 afzonderlijke items over bekendheid met veiligheidsbegrippen is een schaalscore voor bekendheid met begrippen internetveiligheid berekend. Deze loopt van 0 (laag) –10 (hoog)[7)]. De gemiddelde score is een 7,7. Deze schaalscore verschilt tussen bevolkingsgroepen. Mannen zijn vaker bekend met veiligheidsbegrippen dan vrouwen. 25- tot 45-jarigen zijn het meest op de hoogte en 75-plussers het minst. Ook 15- tot 18-jarigen scoren relatief laag. Hoogopgeleiden zijn vaker bekend met veiligheidsbegrippen dan middelbaar opgeleiden en vooral dan laagopgeleiden.

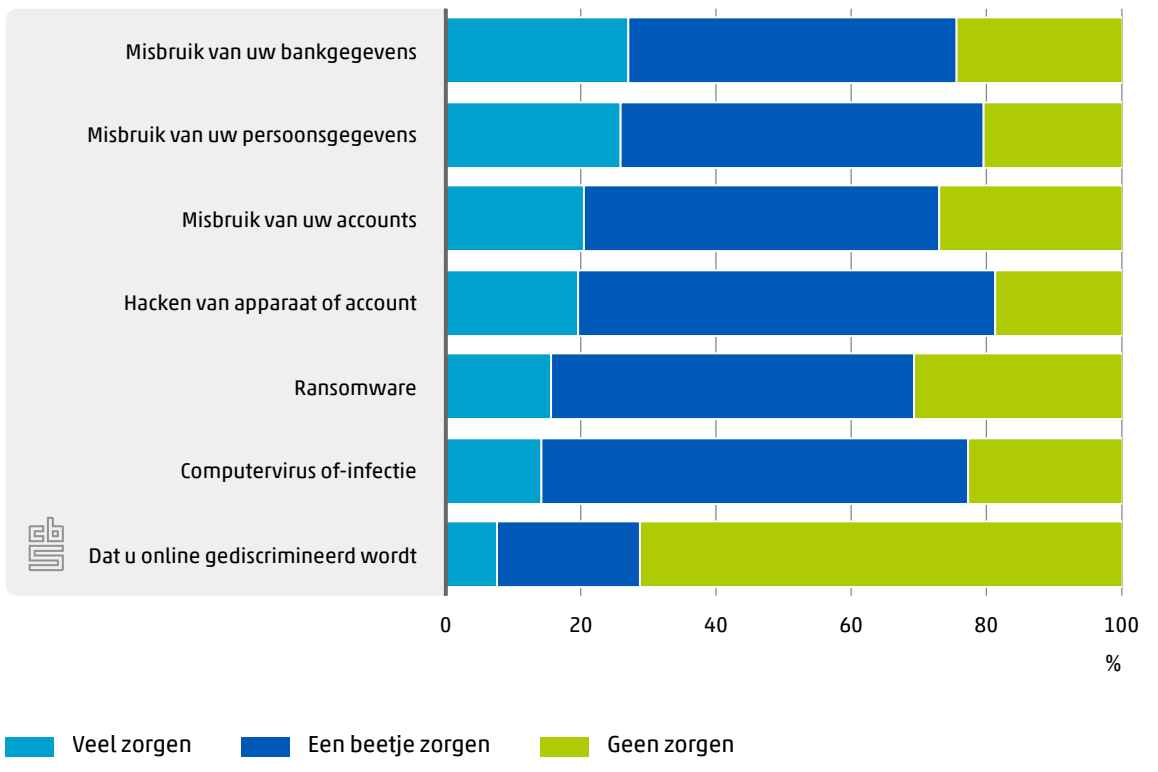
3.2.2 Bekendheid met begrippen internetveiligheid naar persoonskenmerken, 2022



3.3 Bezorgdheid over internetveiligheid

De meeste zorgen als het gaat om internetveiligheid hebben Nederlanders over misbruik van bankgegevens en misbruik van persoonsgegevens: ruim een kwart maakt zich veel zorgen over deze veiligheidsaspecten. Over het misbruik van accounts en hacken van een apparaat of account maakt ongeveer 20 procent zich veel zorgen. Het laagst is de bezorgdheid om online gediscrimineerd te worden: 8 procent maakt zich hierover veel zorgen en meer dan 70 procent niet.

3.3.1 Bezorgdheid over internetveiligheid, 2022



Internet op openbare plekken en veiligheid

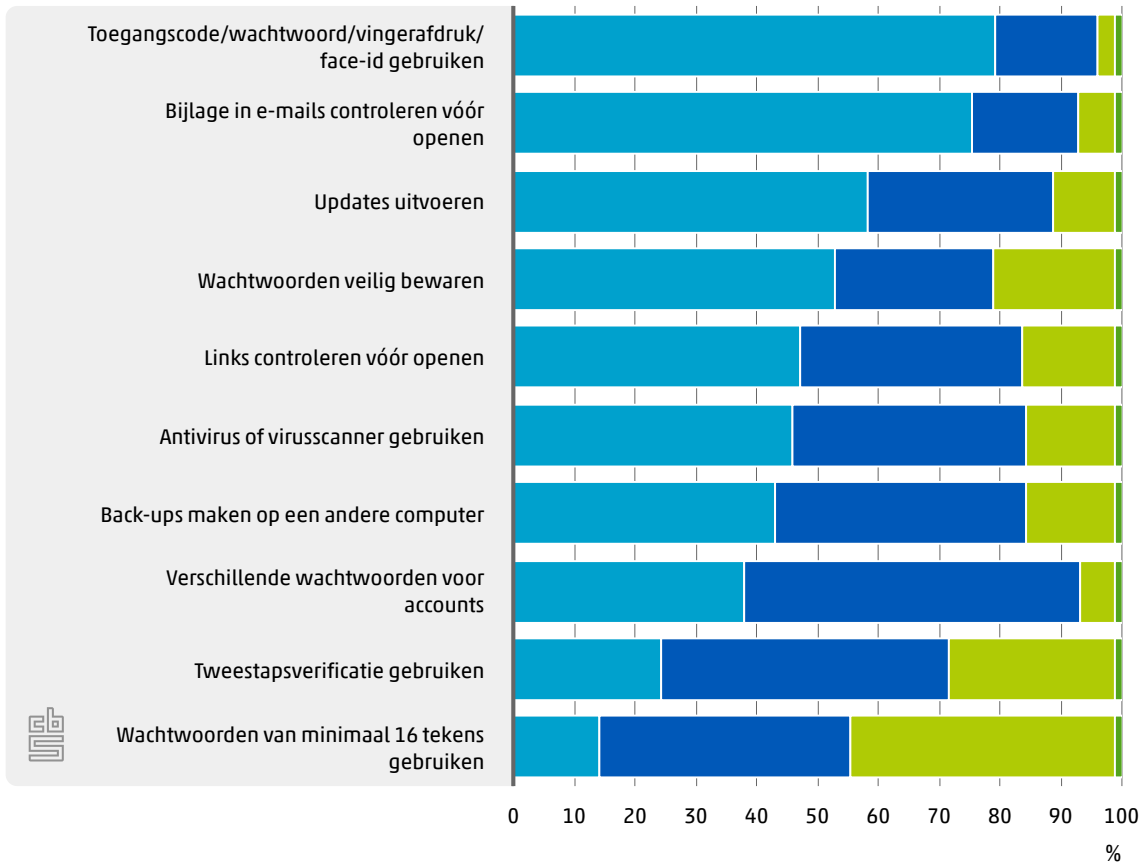
Mensen kunnen tegenwoordig overal online zijn, ook op openbare plekken. Openbare wifi-netwerken zijn niet altijd veilig. Omdat openbare wifi-hotspots voor iedereen toegankelijk zijn is het voor een hacker een mooi doelwit om in een keer veel gegevens buit te maken.

In 2022 maakten 6 op de 10 Nederlanders van 15 jaar of ouder naar eigen zeggen weleens gebruik van een openbaar wifi-netwerk (hotspot), bijvoorbeeld in een café, winkel, trein of hotel. Bijna de helft gebruikte weleens een openbaar WiFi-netwerk dat was beveiligd met een wachtwoord en 40 procent gebruikte weleens een openbare WiFi-verbinding zonder wachtwoord. Ruim een derde gaf aan geen openbaar wifi-netwerk te hebben gebruikt, maar altijd een eigen internetabonnement of -bundel te gebruiken.

3.4 Beveiligingsmaatregelen apparatuur en accounts

De meest gebruikte maatregelen om apparatuur en/of accounts met persoonlijke informatie te beveiligen tegen misbruik door anderen zijn het vergrendelen van apparaten door middel van een toegangscode, wachtwoord, vingerafdruk en/of face-id en het controleren van bijlages in e-mails vóór het openen ervan: de eerste maatregel werd door 8 op de 10 Nederlanders vaak genomen, de tweede door drie kwart. Bijna 6 op de 10 zeiden updates van apparatuur of apps direct of zo snel mogelijk uit te voeren. Het gebruik van tweetrapsverificatie en vooral het gebruik van wachtwoorden van minimaal 16 tekens zijn maatregelen die het minst vaak worden genomen. Wel gaven relatief veel Nederlanders aan voor sommige (maar niet voor alle) accounts een ander wachtwoord te gebruiken.

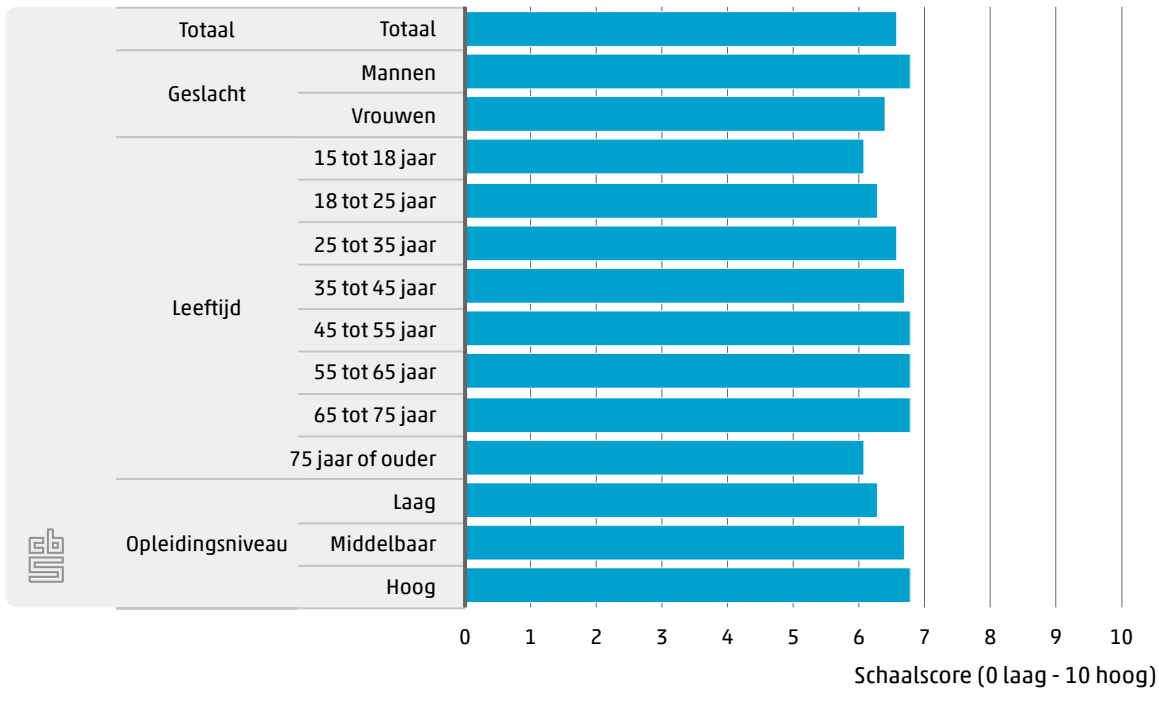
3.4.1 Beveiligingsmaatregelen apparaten en accounts, 2022



* De antwoorden 'Ja, vaak' en 'Ja, soms' hebben betrekking op de beveiligsmaatregelen 'back-ups maken op een andere computer', 'links controleren vóór openen' en 'bijlage in e-mails controleren vóór openen'.

Op basis van de antwoorden op de 10 beveiligingsitems is een schaalscore voor beveiligingsmaatregelen berekend die loopt van 0 (laag) –10 (hoog)[8)]. De gemiddelde score is een 6,6. Deze schaalscore voor beveiligingsmaatregelen verschilt tussen bevolkingsgroepen. Mannen geven vaker dan vrouwen aan beveiligingsmaatregelen te nemen. 45- tot 75-jarigen scoren relatief hoog, jongeren van 15 tot 18 jaar en 75-plussers relatief laag. Middelbaar- en hoogopgeleiden nemen vaker beveiligingsmaatregelen dan laagopgeleiden.

3.4.2 Beveiligingsmaatregelen apparatuur en accounts naar persoonskenmerken, 2022



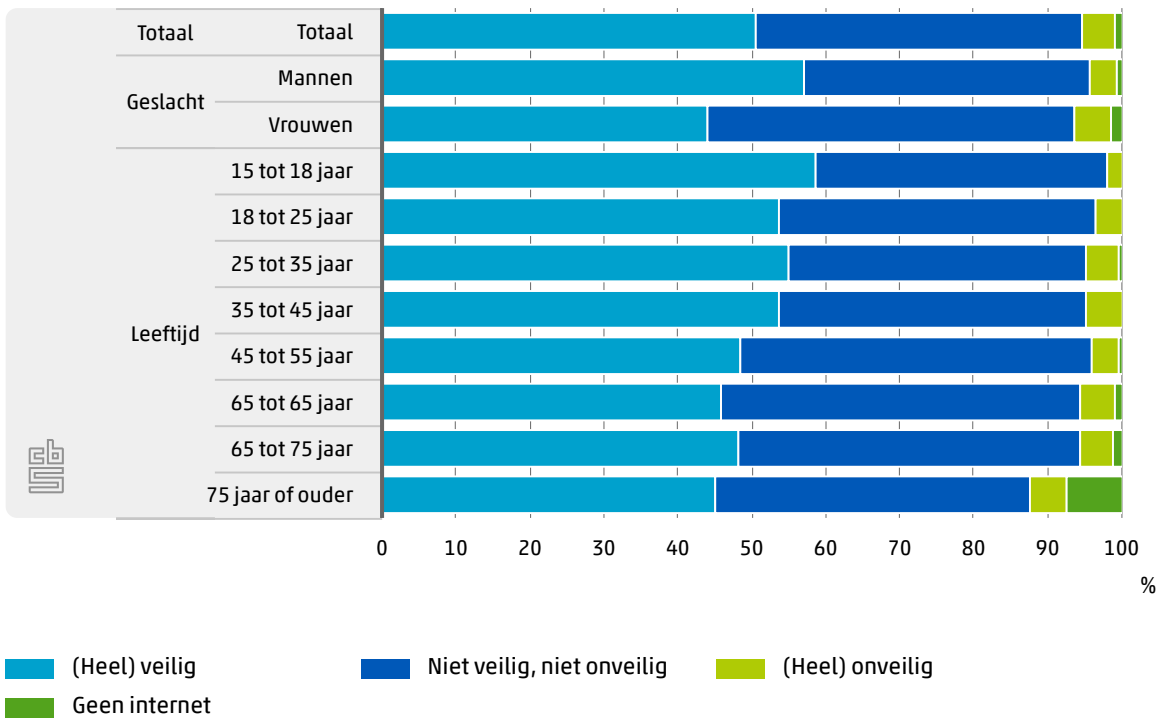
Redenen om beveiligingsmaatregelen niet te treffen

De redenen die mensen hebben om bepaalde beveiligingsmaatregelen niet te treffen lopen voor de verschillende maatregelen sterk uiteen. Zo geven degenen die geen back-ups op een andere computer maken hiervoor het vaakst als reden dat ze niet weten hoe het moet (37 procent) en dat ze het niet nodig vinden (31 procent) (zie tabellenset). Ook het veilig bewaren van wachtwoorden wordt vaak nagelaten omdat men het niet nodig vindt (36 procent). Het achterwege laten van updates gebeurt het vaakst omdat men niet weet hoe het moet (26 procent), omdat het te veel tijd kost (24 procent) of omdat men dit niet nodig vindt (24 procent). Voor de minst getroffen maatregel, het gebruiken van wachtwoorden van minimaal 16 tekens, speelt vooral de complexiteit een rol: 63 procent van degenen die dit niet doen geeft aan dat ze dit te moeilijk vinden.

3.5 Veiligheidsbeleving op internet

In 2022 gaf de helft van de Nederlanders aan zich (heel) veilig te voelen als ze internet gebruiken. 4 procent voelde zich (heel) onveilig. De rest (44 procent) voelde zich veilig noch onveilig.
Vooral 15- tot 18-jarigen en mannen voelden zich (heel) veilig op internet. Vrouwen en 75-plussers voelden zich er het vaakst (heel) onveilig. De veiligheidsbeleving op internet verschilt niet naar opleidingsniveau.

3.5.1 Veiligheidsgevoelens op internet naar persoonskenmerken, 2022



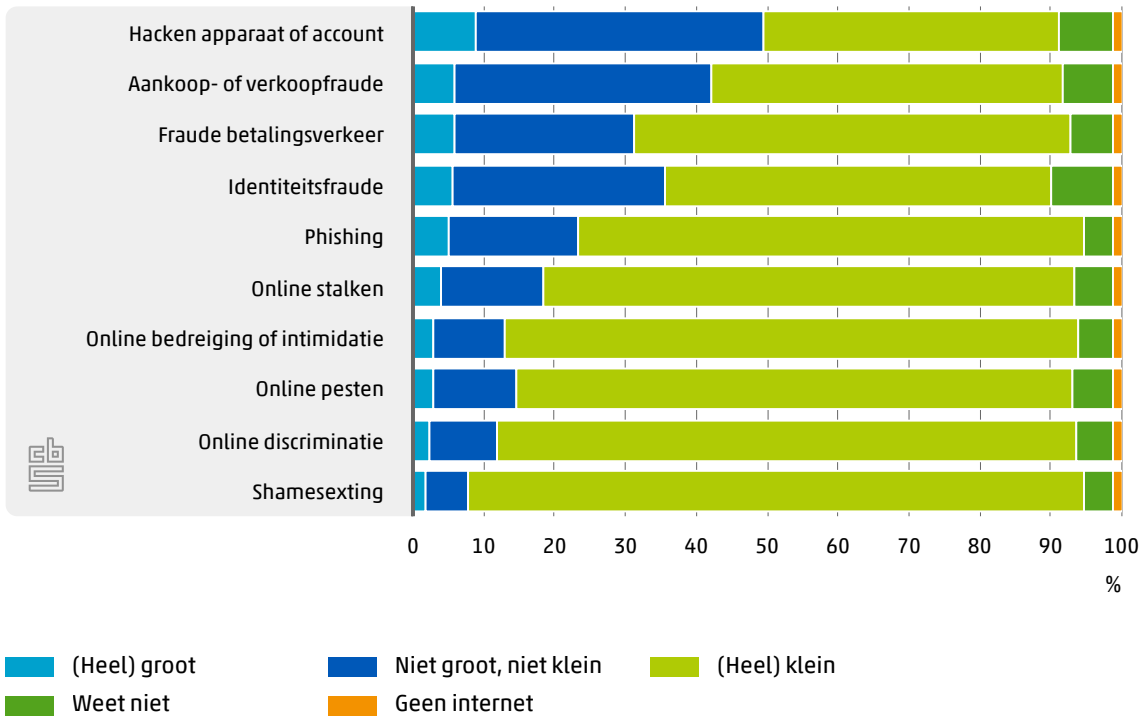
Inschatting betrouwbaarheid webshops

Ruim 70 procent van de Nederlanders gaf aan in de afgelopen 12 maanden getwijfeld te hebben aan de betrouwbaarheid van een webshop. Bij twijfel zoeken de meesten van hen reviews over de webshop op (71 procent) en/of verlaten ze de website of breken ze de online bestelling af (70 procent). De helft controleert of men met een echte webshop te maken heeft, bijvoorbeeld door te letten op een keurmerk. Ongeveer 20 procent trekt de website na, bijvoorbeeld op politie.nl of op checkjelinkje.nl, en een vergelijkbaar deel betaalt met creditcard, PayPal of achteraf betalen.

Inschatting kans op slachtofferschap online criminaliteit

Vooral als het gaat om online bedreiging en intimidatie schatten Nederlanders de kans om zelf hiervan slachtoffer te worden relatief laag in. Grofweg 10 procent acht de kans aanwezig (dat wil zeggen '(heel) groot' of 'niet groot, niet klein') om zelf slachtoffer te worden van online pesten, bedreiging of discriminatie. Bij online stalken is dit bijna 20 procent. Delicten in de sfeer van online bedreiging en intimidatie treffen vooral jongeren en daardoor ligt het voor de hand dat anderen de kans om hier zelf slachtoffer van te worden als niet zo groot inschatten. Voorvallen op het gebied van online oplichting en fraude en van hacken treffen ook andere leeftijdsgroepen dan jongeren verhoudingsgewijs vaker en hiervoor is de risico-inschatting dan ook groter. Zo schat bijna de helft van de bevolking de kans aanwezig om slachtoffer te worden van aankoop- of verkoopfraude, en acht men vooral de kans gehackt te worden vrij groot.

3.5.2 Inschatting kans op slachtofferschap online criminaliteit, 2022

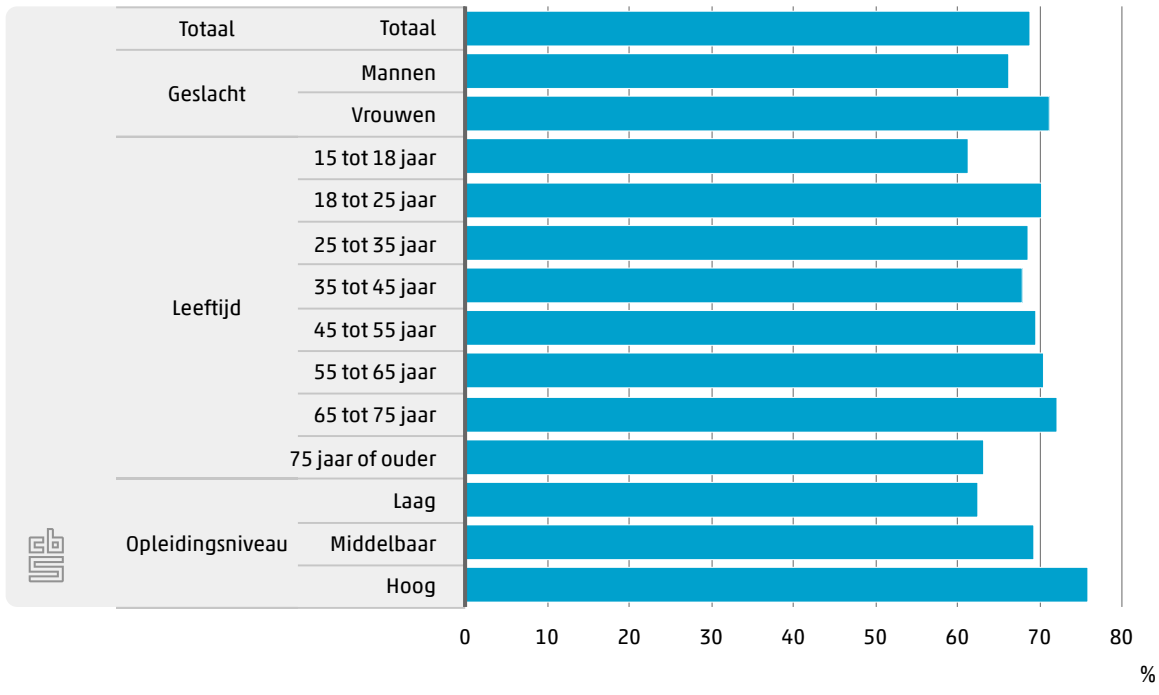


Behoefte aan voorlichting over online criminaliteit

Op de vraag waaraan men behoefte heeft om zich beter te kunnen beschermen tegen online criminaliteit, antwoordde bijna de helft van de Nederlanders behoefte te hebben aan meer informatie over beschermende maatregelen die zij zelf kunnen nemen. Bijna 4 op de 10 hebben behoefte aan meer informatie over hoe oplichters te werk gaan en waar men op moet letten. Ruim een kwart wilde meer informatie over de verschillende vormen van online criminaliteit. Hulp bij het nemen van beschermende maatregelen werd door 2 op de 10 genoemd. Eenzelfde deel gaf aan geen behoefte aan informatie over bescherming tegen online criminaliteit te hebben.

Vrouwen geven vaker dan mannen aan behoefte te hebben aan voorlichting over hoe ze zich kunnen beschermen tegen online criminaliteit; 71 tegen 66 procent. Jongeren (15-tot 18-jarigen) en ouderen (75-plussers) hebben minder behoefte aan voorlichting dan anderen. Hoogopgeleiden (76 procent) hebben meer behoefte aan informatie dan middelbaar opgeleiden (69 procent) en laagopgeleiden (63 procent).

3.5.3 Behoefte aan voorlichting naar persoonskenmerken, 2022



[6] Social engineering is het misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid. Criminelen (social engineers) proberen vertrouwelijke informatie van iemand los te krijgen. Ze willen bijvoorbeeld persoonlijke gegevens (phishing) en beveiligingscodes te weten komen of malware installeren (bron: Veiligbankieren.nl).
[7] De schaalscore is bepaald door de antwoorden op de 12 items op te tellen, waarbij 'nooit van gehoord' de score 0 heeft, 'wel van gehoord, maar weet niet precies wat het is' score 1, en 'ik weet wat het is' score 2. Het minimum van deze som is 0 en het maximum 24. Om tot een score op een schaal van 0 – 10 te komen is de som vermenigvuldigd met de factor 10/24.
[8] De schaalscore is bepaald door de antwoorden op de 10 items op te tellen, waarbij 'nee, geen maatregel' de score 0 heeft, 'Ja, soms/ voor sommige apparaten of accounts' score 1 en 'Ja, vaak/ voor alle apparaten of accounts' score 2. Het minimum van deze som is 0 en het maximum is 20. Om tot een score op een schaal van 0 - 10 te komen is de som vermenigvuldigd met de factor 10/20.

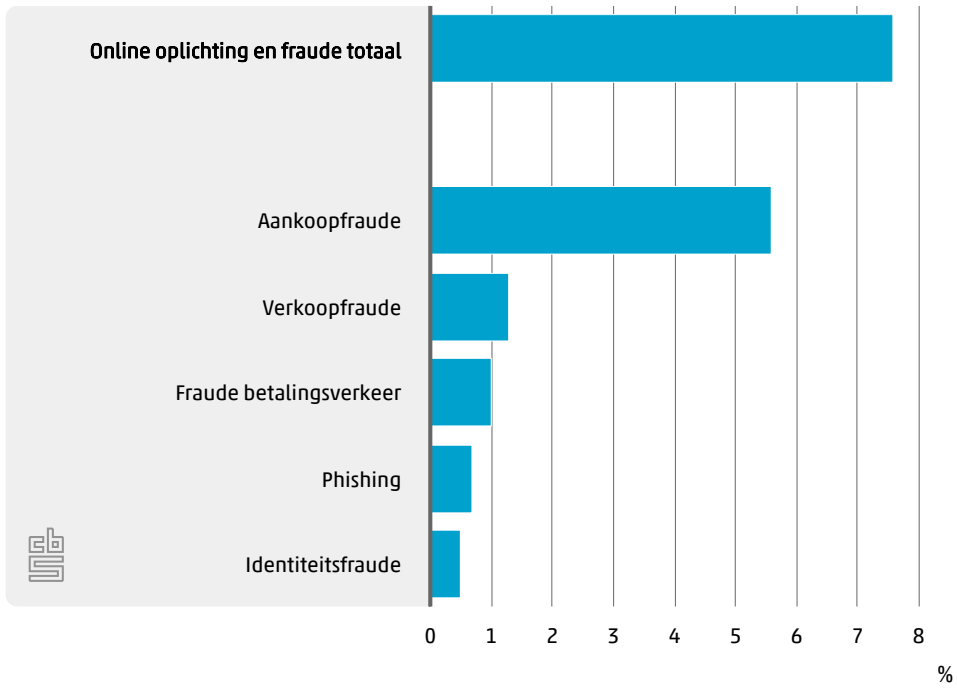
4. Online oplichting en fraude

Bijna alle Nederlanders maken gebruik van het internet. Het overgrote deel doet online aankopen, bankiert online en maakt gebruik van sociale media (zie hoofdstuk 2). Dit maakt Nederlanders aantrekkelijk én kwetsbaar voor oplichting door cybercriminelen. Hierover gaat dit hoofdstuk. Hoeveel mensen werden in 2022 slachtoffer van fraude bij online handel, zowel bij het kopen als verkopen van producten en diensten, van fraude in het betalingsverkeer, van identiteitsfraude en van phishing? Hoe gebeurde dit? Wat waren de gevolgen voor het slachtoffer? En hebben ze gemeld of bij de politie aangegeven wat hen overkomen is?

4.1 Slachtoffers online oplichting en fraude

In 2022 werd 8 procent van de Nederlanders van 15 jaar of ouder slachtoffer van een of meerdere vormen van online oplichting en fraude. Aankoopfraude kwam het vaakst voor: 6 procent bestelde en betaalde producten of diensten (zoals bijvoorbeeld tickets of reizen) die nooit werden geleverd. Van verkoopfraude, waarbij het slachtoffer iets verkoopt maar niet betaald werd, werd 1 procent slachtoffer. Fraude in het betalingsverkeer overkwam 1 procent en van phishing en identiteitsfraude werd minder dan 1 procent slachtoffer[9)]. Onder phishing worden in dit onderzoek alle vormen van spoofing verstaan, dat wil zeggen het slachtoffer raakt geld kwijt aan een crimineel die zich voordoet als iemand anders of als een vertrouwde instantie.

4.1.1 Slachtoffers online oplichting en fraude, 2022



Slachtoffers online oplichting en fraude naar persoonskenmerken

Jongeren zijn vaker op internet actief. Dit vergroot de kans dat ze online worden opgelicht. Van de 15- tot 45-jarigen werd 9 procent slachtoffer van oplichting, tegen 5 procent van de 65-plussers. Het patroon dat jongere Nederlanders vaker slachtoffer worden dan ouderen is met name te zien bij aankoopfraude, verkoopfraude en identiteitsfraude. Bij phishing zijn het juist 65-plussers die vaker slachtoffer worden.

Mensen met lage welvaart worden vaker slachtoffer dan meer welvarende Nederlanders. Dit geldt voor alle oplichtingsvormen met uitzondering van phishing. Bij slachtofferschap van phishing speelt welvaart een minder onderscheidende rol.

4.1.2 Slachtoffers online oplichting en fraude naar persoonskenmerken, 2022

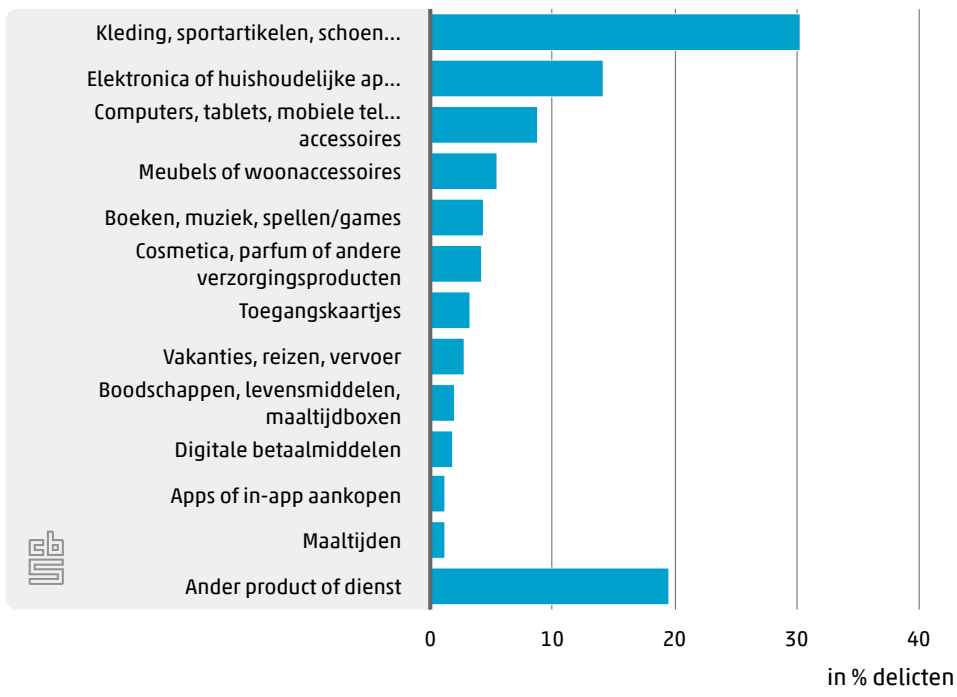
	Totaal	Aankoopfraude	Verkoopfraude	Fraude betalingsverkeer	Identiteitsfraude	Phishing
	%	%	%	%	%	%
Totaal	7,6	5,6	1,3	1,0	0,5	0,7
Mannen	7,5	5,4	1,3	1,1	0,5	0,7
Vrouwen	7,8	5,7	1,4	0,9	0,6	0,7
Leeftijd						
15 tot 25 jaar	8,6	6,5	1,8	1,1	0,7	0,4
25 tot 45 jaar	9,2	6,8	1,8	1,1	0,8	0,7
45 tot 65 jaar	7,6	5,8	1,3	0,8	0,4	0,7
65 jaar en ouder	5,1	3,2	0,6	1,0	0,3	1,0
Onderwijsniveau						
Laag	7,4	5,3	1,4	0,9	0,6	0,9
Middelbaar	7,7	5,8	1,2	1,0	0,4	0,6
Hoog	7,2	5,2	0,8	1,0	0,5	0,6
Welvaart huishouden						
1e 20%-groep (laagste welvaart)	10,1	7,2	2,2	1,6	1,1	0,8
2e 20%-groep	7,7	5,7	1,6	0,9	0,5	0,9
3e 20%-groep	7,5	5,5	1,3	1,0	0,3	0,6
4e 20%-groep	7,1	5,3	0,8	1,0	0,4	0,5
5e 20%-groep (hoogste welvaart)	6,9	5,0	1,2	0,8	0,6	0,8

Slachtofferschap aankoopfraude: details

In 2022 werd 6 procent slachtoffer van aankoopfraude: online bestellingen werden betaald maar nooit geleverd. De meeste slachtoffers (74 procent) werden in 2022 één keer slachtoffer van deze vorm van fraude, 26 procent werd minstens 2 keer slachtoffer.

Bij 30 procent van de delicten van aankoopfraude ging het om kleding, sportartikelen, schoenen of (kleding)accessoires. Bij 14 procent ging het om elektronica of huishoudelijke apparatuur. Ook computers, tablets, mobiele telefoons of bijbehorende accessoires werden vaak besteld maar niet ontvangen (9 procent van de delicten).

4.1.3 Aankoopfraude: producten en diensten, 2022

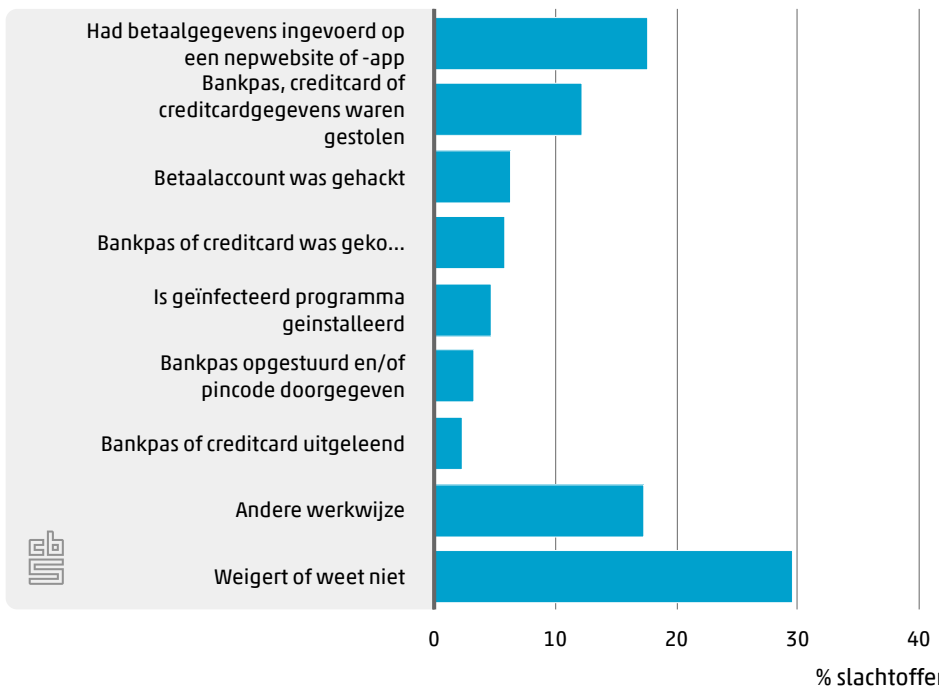


Slachtofferschap fraude in betalingsverkeer: details

Bij 1 procent van de 15-plussers kreeg een crimineel toegang tot de creditcard of bankrekening van het slachtoffer en boekte daar geld vanaf, ook wel fraude in het betalingsverkeer genoemd. Daarbij kunnen de toegangsgegevens via internet verkregen zijn maar ook op een andere manier, bijvoorbeeld door het stelen van een bankpas of creditcard.

De meest voorkomende manier waarop toegang tot de rekening werd verkregen, was doordat het slachtoffer zijn of haar betaalgegevens had ingevoerd op een nepwebsite of –app. Dit werd door 18 procent van de slachtoffers genoemd. 12 procent zei dat de bankpas, creditcard of creditcardgegevens waren gestolen. Hacken of het kopiëren van de bankpas werden elk door ongeveer 6 procent van de slachtoffers genoemd. Opsturen van passen of codes en uitlenen van passen waren vrijwel nooit de aanleiding, bij 3 procent respectievelijk 2 procent van de slachtoffers.

4.1.4 Fraude betalingsverkeer: manier waarop slachtoffer geworden, 2022

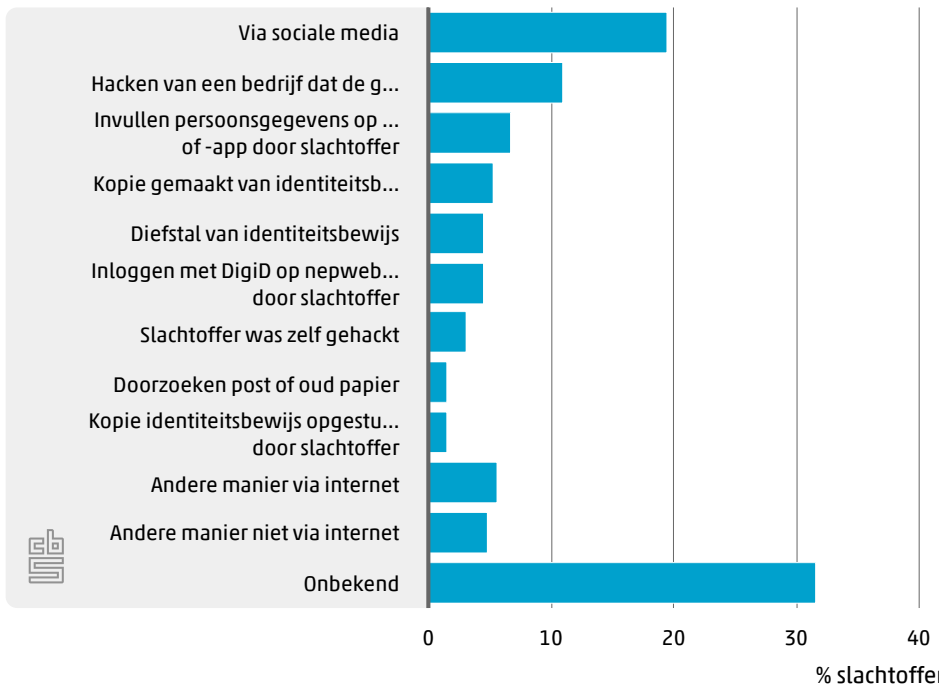


Slachtofferschap identiteitsfraude: details

Een half procent van de 15-plussers gaf aan in 2022 slachtoffer te zijn geweest van identiteitsfraude, dat wil zeggen dat iemand illegaal gebruik heeft gemaakt van zijn/haar persoonsgegevens.

Bij minstens de helft van deze slachtoffers van identiteitsfraude kwam de dader via internet aan deze gegevens. Dit gebeurde het vaakst via sociale media: 20 procent van de slachtoffers zei dat de dader op deze manier aan de gegevens kwam. Bij 11 procent werden de gegevens via een gehackt bedrijf verkregen. Bijna 1 op de 3 slachtoffers weet niet hoe de dader aan de gegevens is gekomen.

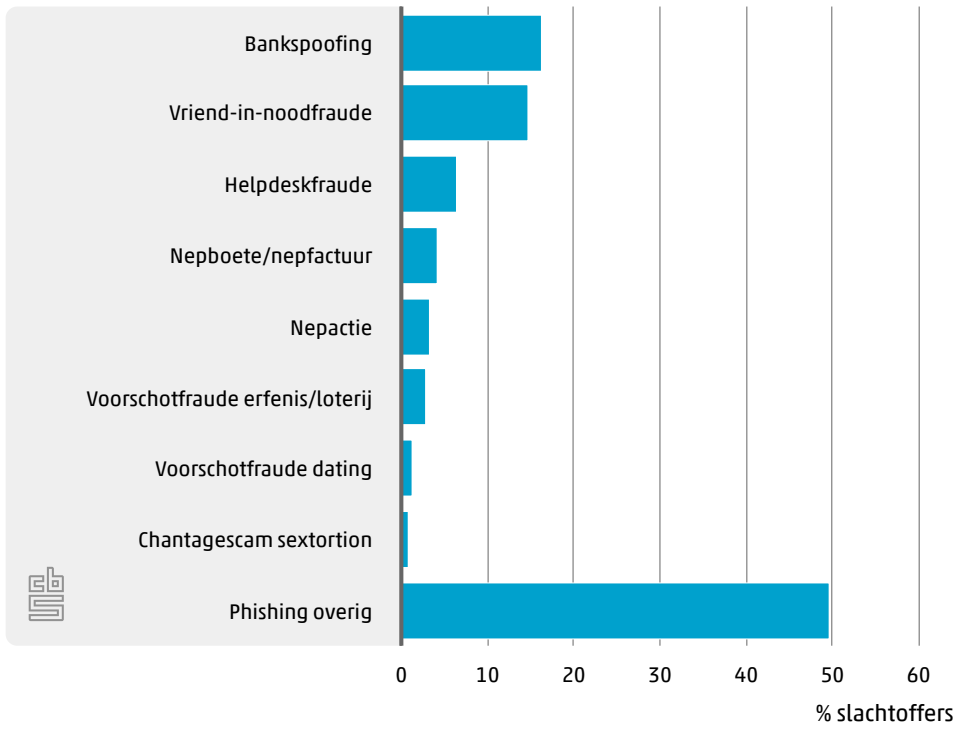
4.1.5 Identiteitsfraude: manier waarop slachtoffer geworden, 2022



Slachtofferschap phishing: details

In 2022 had 16 procent van de slachtoffers van phishing te maken met bankspoofing: de dader deed alsof hij een medewerker van de bank was. Een vergelijkbaar deel (15 procent) werd slachtoffer van vriend-in-nood-fraude, waarbij hij/zij geld betaalde aan een zogenaamde vriend(in), familielid of bekende. Bij 7 procent ging het om een zogenaamde medewerker van een helpdesk. Nepboetes of nepfacturen werden door 4 procent van de slachtoffers genoemd. Voorschotfraude, waarbij het slachtoffer geld voorschoot om een zogenaamde erfenis in ontvangst te kunnen nemen dan wel geld voorschoot aan een zogenaamde geliefde werd door respectievelijk 3 en 1 procent van de slachtoffers hiervan genoemd. Bij de helft van de phishing slachtoffers ging het om andere vormen van oplichting.

4.1.6 Phishing: waarvan slachtoffer, 2022

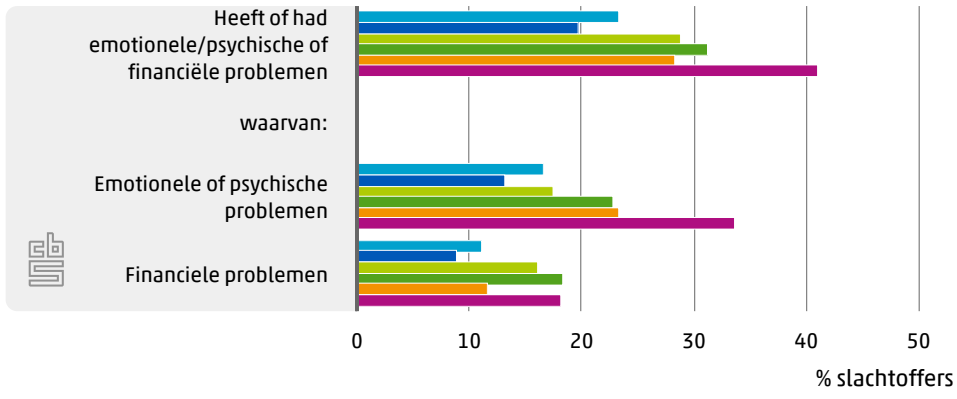


4.2 Gevolgen online oplichting en fraude

Problemen voor slachtoffers

Bijna een kwart van de slachtoffers (23 procent) gaf aan problemen te hebben (gehad) door de online oplichting en fraude. Bij 11 procent ging het om financiële problemen, 17 procent kreeg emotionele of psychische problemen. Bij alle vormen van oplichting en fraude werden vaker emotionele of psychische problemen dan financiële gemeld. Zo kreeg een derde van de slachtoffers van phishing emotionele of psychische problemen, 18 procent kreeg financiële problemen. En van de slachtoffers van aankoopfraude kreeg 13 procent emotionele of psychische problemen, 9 procent financiële.

4.2.1 Problemen door online oplichting en fraude[1)], 2022

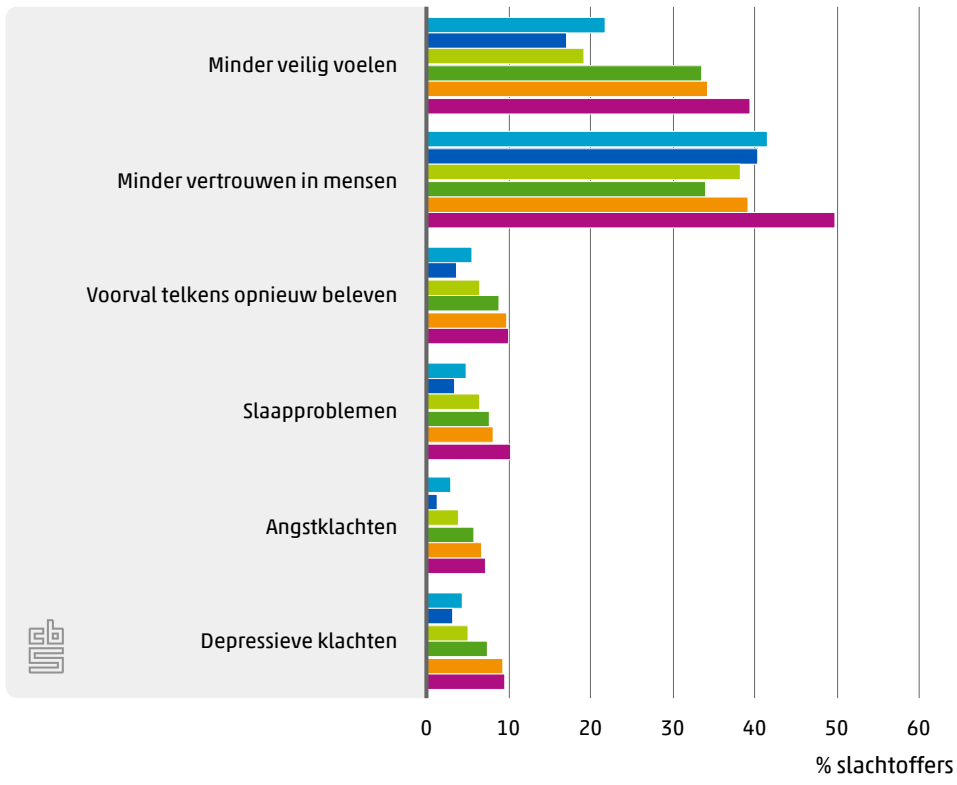


[1)] Meerdere antwoorden mogelijk.

Emotionele of psychische gevolgen

Ruim 4 op de 10 slachtoffers van online oplichting en fraude gaven aan minder vertrouwen in andere mensen te hebben door wat hen overkomen is en ruim 2 op de 10 voelen of voelden zich er minder veilig door. Ongeveer 5 procent zei het voorval telkens opnieuw te beleven, slaapproblemen, angstklachten, en/ of depressieve klachten te hebben of te hebben gehad. Bij fraude in het betalingsverkeer, identiteitsfraude en vooral phishing ervaren de slachtoffers vaker emotionele of psychische gevolgen dan bij aan- of verkoopfraude.

4.2.2 Emotionele of psychische gevolgen online oplichting en fraude[1)], 2022



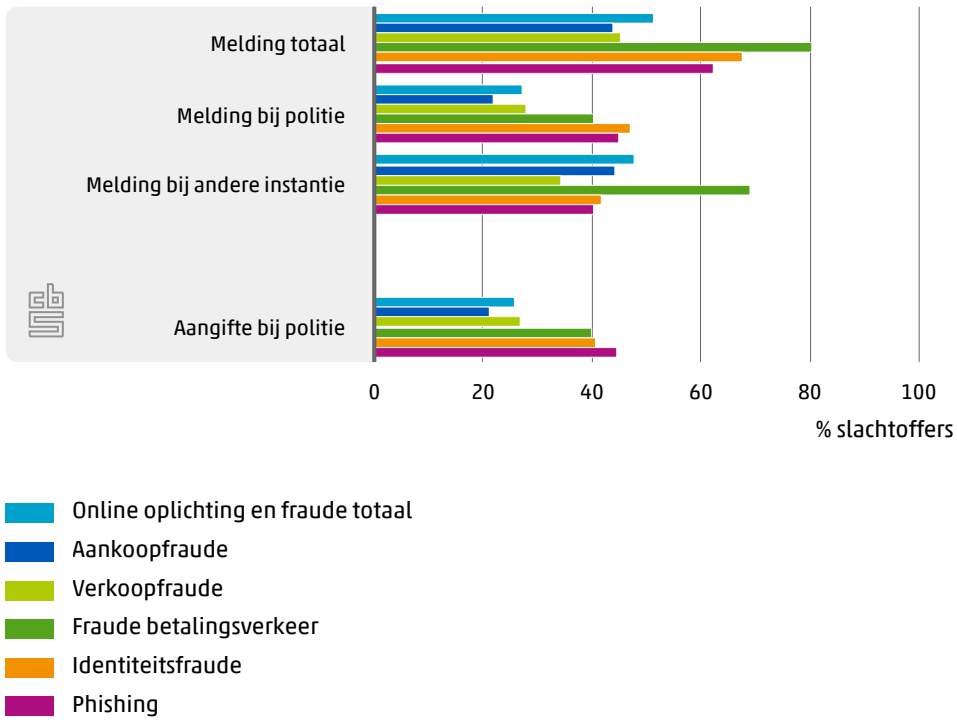
[1)] Meerdere antwoorden mogelijk.

4.3 Melding en aangifte online oplichting en fraude

Ruim de helft van de slachtoffers van online oplichting en fraude (52 procent) meldde ergens wat hen overkomen is. 27 procent van de slachtoffers heeft een melding gedaan bij de politie, 48 procent bij een andere instantie. Een kwart van de slachtoffers (26 procent) deed aangifte.

De meldings- en aangiftebereidheid wisselt sterk tussen de verschillende soorten delicten. Zo werd aankoopfraude door 44 procent van de slachtoffers ergens gemeld, 21 procent deed aangifte bij de politie. Fraude in het betalingsverkeer werd door 81 procent van de slachtoffers bij een instantie (bijvoorbeeld de politie of de bank) gemeld, 40 procent deed aangifte bij de politie.

4.3.1 Melding en aangifte online oplichting en fraude, 2022

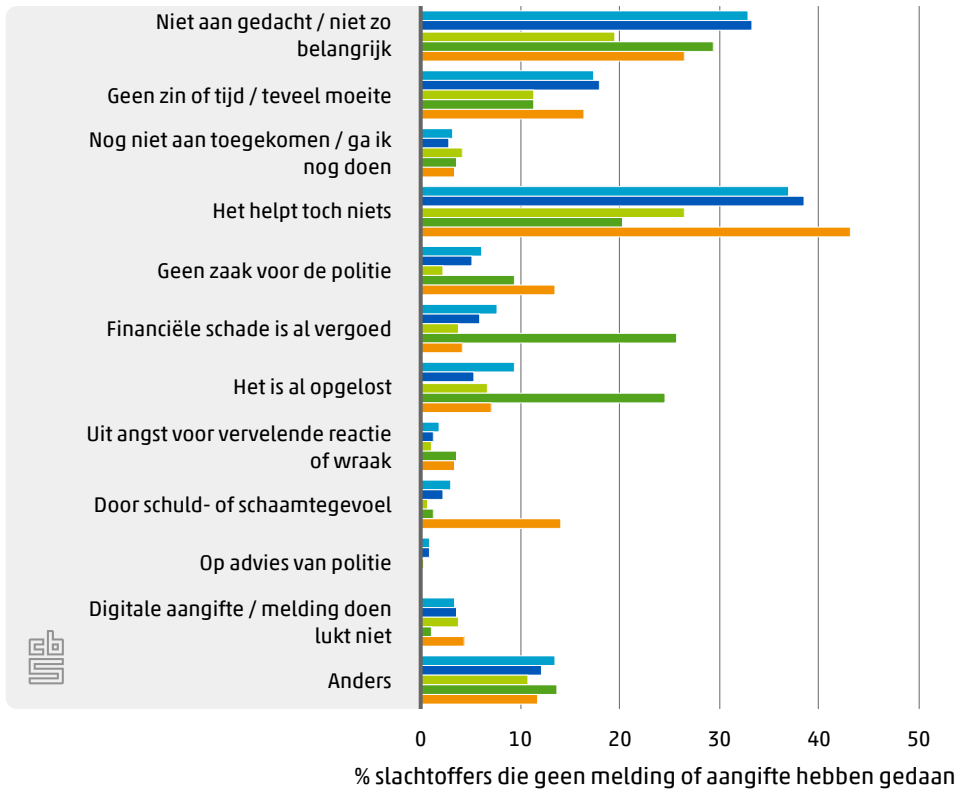


Ruim de helft (53 procent) van de slachtoffers die aangifte deden deed dit via internet. 28 procent van de slachtoffers deed aangifte op het bureau en 17 procent telefonisch. De manier waarop aangifte werd gedaan verschilt sterk tussen de soorten delicten (zie tabellenset). Zo deed 66 procent van de slachtoffers van aankoopfraude die aangifte deden dit online, tegen 26 procent van de slachtoffers van fraude in het betalingsverkeer. Bij deze laatste vorm van fraude en ook bij phishing werd de aangifte relatief vaak op het politiebureau gedaan.

Redenen geen melding of aangifte bij politie

De meest genoemde redenen om geen melding of aangifte bij de politie te doen waren, bij alle delictsoorten, dat het ‘toch niets helpt’ en dat ‘er niet aan gedacht was/het niet zo belangrijk was’. Alleen bij fraude in het betalingsverkeer werd vaak als reden gegeven dat de financiële schade al vergoed was of dat het al was opgelost.

4.3.2 Reden geen melding of aangifte bij politie van online oplichting en fraude[1)2)], 2022



1) Meerdere antwoorden mogelijk.
2) Identiteitsfraude ontbreekt i.v.m. te weinig waarnemingen.

9) Er zit enige overlap tussen de verschillende vormen van oplichting en fraude, want sommige delicten kunnen onder meerdere vormen worden geschaard. Zo vallen sommige vormen van phishing ook onder aankoopfraude of onder fraude in het betalingsverkeer, en is fraude in het betalingsverkeer soms het gevolg van hacken.

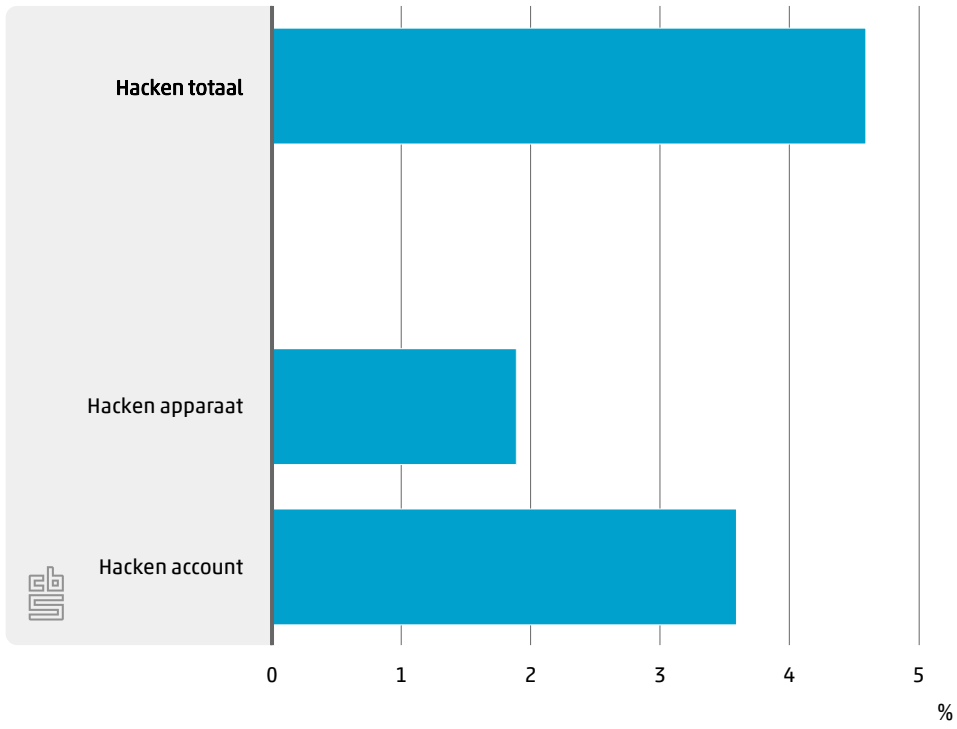
5. Hacken

Behalve van online oplichting en fraude worden Nederlanders ook slachtoffer van hacken. Hierbij breekt iemand met kwade bedoelingen zonder toestemming in op een apparaat (zoals een computer of tablet) of een account (zoals een e-mail- of bankaccount). Het gaat dan alleen om een apparaat of account dat voor privédoeleinden wordt gebruikt. Hoeveel mensen werden slachtoffer van hacken in 2022? Welke beveiligingsmaatregelen treffen slachtoffers van hacken? Wat waren de gevolgen van de hack voor de slachtoffers? En hebben ze het voorval gemeld of aangegeven bij de politie?

5.1 Slachtoffers hacken

In 2022 gaf 5 procent van de Nederlanders van 15 jaar of ouder aan in de afgelopen 12 maanden slachtoffer te zijn geweest van hacken van een apparaat of account. Het ging vaker om het hacken van een account dan om het hacken van een apparaat (4 tegen 2 procent).

5.1.1 Slachtoffers hacken, 2022



Slachtoffers hacken naar persoonskenmerken

Jongeren van 15 tot 25 jaar waren met 6 procent vaker slachtoffer van hacken dan oudere Nederlanders. 65-plussers waren het minst vaak slachtoffer. Het verschil tussen jongeren en ouderen is met name te zien bij het hacken van een account.

Geslacht en opleidingsniveau zijn over het algemeen weinig onderscheidend. Wel zijn laagopgeleiden vaker slachtoffer van het hacken van een apparaat. Personen met de laagste inkomens zijn vaker slachtoffer van hacken dan personen met hogere inkomens. Hierbij speelt mee dat personen met de laagste inkomens doorgaans lager opgeleid en jonger zijn.

5.1.2 Slachtofferschap hacken naar persoonskenmerken, 2022

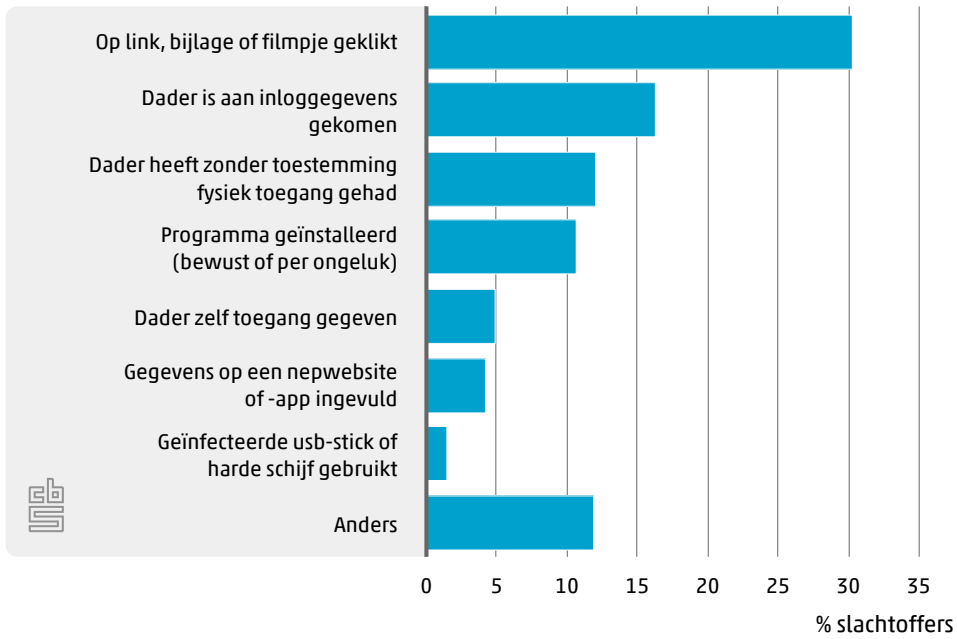
	Totaal	Hacken apparaat	Hacken account
	%	%	%
Totaal	4,6	1,9	3,6
Geslacht			
Mannen	4,6	1,9	3,6
Vrouwen	4,6	1,9	3,6
Leeftijd			
15 tot 25 jaar	6,1	1,8	5,2
25 tot 45 jaar	4,9	1,4	4,2
45 tot 65 jaar	4,4	1,9	3,5
65 jaar en ouder	3,6	2,5	2,1
Opleidingsniveau			
Laag	4,7	2,6	3,4
Middelbaar	4,6	1,7	3,5
Hoog	4,7	1,4	3,9
Huishoudinkomen			
Eerste (laagste) kwintielgroep	5,6	2,6	4,2
Tweede kwintielgroep	4,8	2,1	3,5
Derde kwintielgroep	4,2	1,9	3,2
Vierde kwintielgroep	4,4	1,8	3,3
Vijfde (hoogste) kwintielgroep	4,5	1,4	3,8

Slachtofferschap hacken apparaat: details

De smartphone (55 procent) en computer of laptop (42 procent) worden van alle apparaten het vaakst gehackt (zie tabellenset).

De manier waarop men het vaakst slachtoffer werd van een hack van een apparaat is door te klikken op een link, bijlage of filmpje: 30 procent van de slachtoffers gaf aan dit te hebben gedaan. 16 procent zei dat de dader aan de inloggegevens is gekomen. Het invullen van gegevens op een nepwebsite/-app of het gebruiken van een geïnfecteerde usb-stick of harde schijf worden het minst vaak als oorzaak genoemd.

5.1.3 Hacken apparaat: manier waarop slachtoffer geworden[1)], 2022



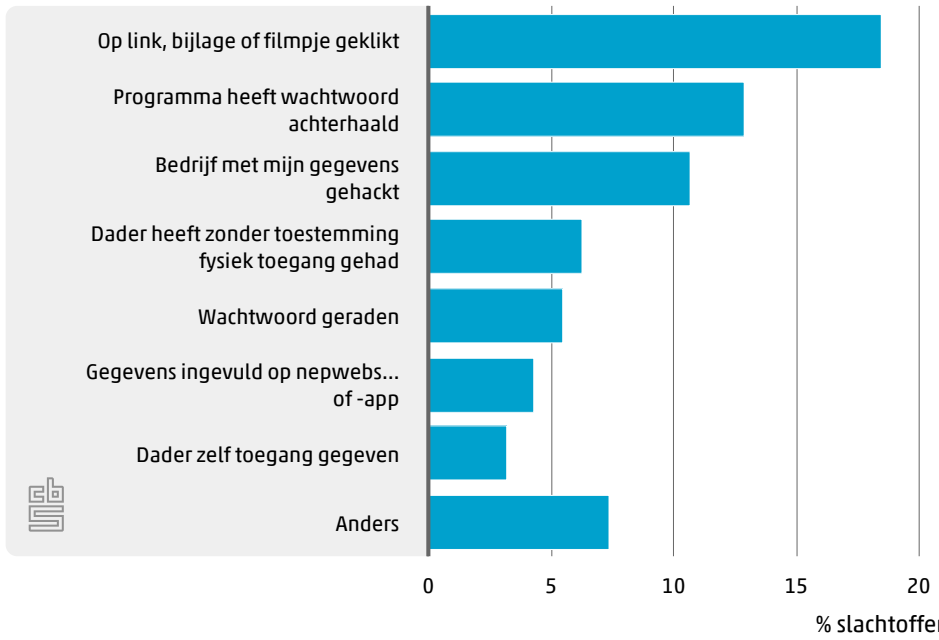
[1)] Meerdere antwoorden mogelijk.

Slachtofferschap hacken account: details

Bij het hacken van accounts gaat het in de meeste gevallen om een sociale-media-account (bijvoorbeeld Facebook, Instagram, WhatsApp, LinkedIn of Twitter): 51 procent van de slachtoffers gaf aan dat zo'n account was gehackt (zie tabellenset). Ook het hacken van de email werd relatief vaak door slachtoffers genoemd (27 procent).

Net zoals bij het hacken van apparaten is ook bij het hacken van accounts het klikken op een link, bijlage of filmpje de vaakst genoemde oorzaak van de hack: 19 procent van de slachtoffers gaf aan dat hun account op deze manier is gehackt. 13 procent zei dat het wachtwoord is achterhaald door een programma, en 11 procent gaf aan dat een bedrijf waar de gegevens van het slachtoffer bekend waren is gehackt. Het zelf invullen van gegevens op een nepwebsite/-app of de dader zelf toegang geven tot het apparaat werden het minst vaak als de oorzaak van de hack genoemd.

5.1.4 Hacken account: manier waarop slachtoffer geworden[1)], 2022



[1)] Meerdere antwoorden mogelijk.

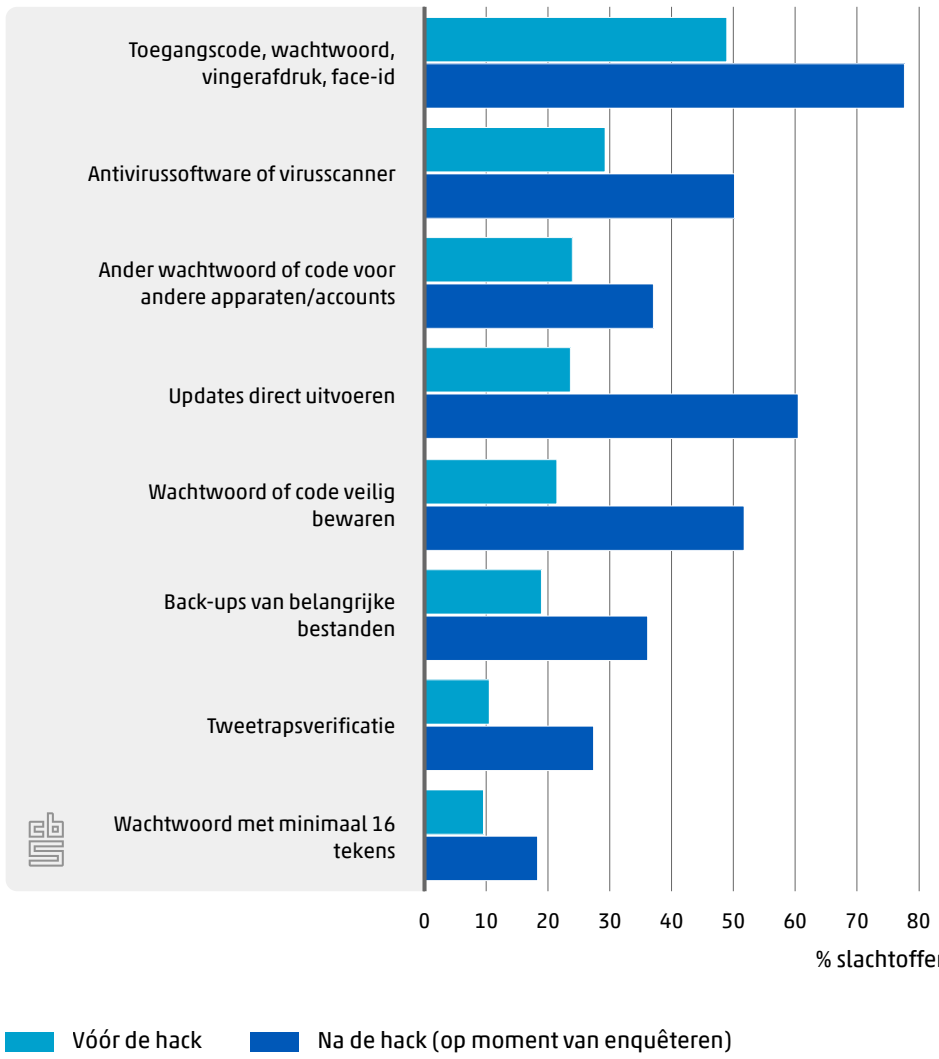
5.2 Beveiligingsmaatregelen voor en na slachtofferschap hacken

Beveiligingsmaatregelen voor en na hacken apparaat

Aan slachtoffers van een hack van een apparaat is gevraagd welke beveiligingsmaatregelen ze hebben genomen vóórdat dit apparaat gehackt werd. Bijna de helft (49 procent) had het apparaat vergrendeld door middel van een toegangscode, wachtwoord, vingerafdruk of face-id. 29 procent gebruikte antivirussoftware of een virusscanner. Ruim 1 op de 5 slachtoffers gebruikte verschillende wachtwoorden, een vergelijkbaar deel voerde updates direct uit, en een vergelijkbaar deel bewaarde hun wachtwoorden veilig. 14 procent zei geen van de genoemde maatregelen te hebben genomen om het apparaat te beveiligen.

Aan slachtoffers is ook op het moment van enquêteren gevraagd welke beveiligingsmaatregelen zij altijd of vaak nemen. Dit is per definitie na het moment dat de hack heeft plaatsgevonden. Na het hacken van hun apparaat zijn slachtoffers vaker beveiligingsmaatregelen gaan nemen[10)]. Waar vóór de hack 49 procent van de (latere) slachtoffers het apparaat met toegangscodes en dergelijke vergrendelde, lag het percentage dat zei dit te doen na de hack op 78. Vóór de hack voerde 24 procent direct updates uit, na slachtoffer te zijn geweest was dit 61 procent. Ook het veilig bewaren van wachtwoorden gebeurde aanzienlijk vaker: 22 procent deed dit vóór gehackt te zijn, 52 procent erna. En ook alle andere beveiligingsmaatregelen werden na de hack duidelijk vaker getroffen[11)].

5.2.1 Maatregelen voor en na hacken apparaat[1)], 2022



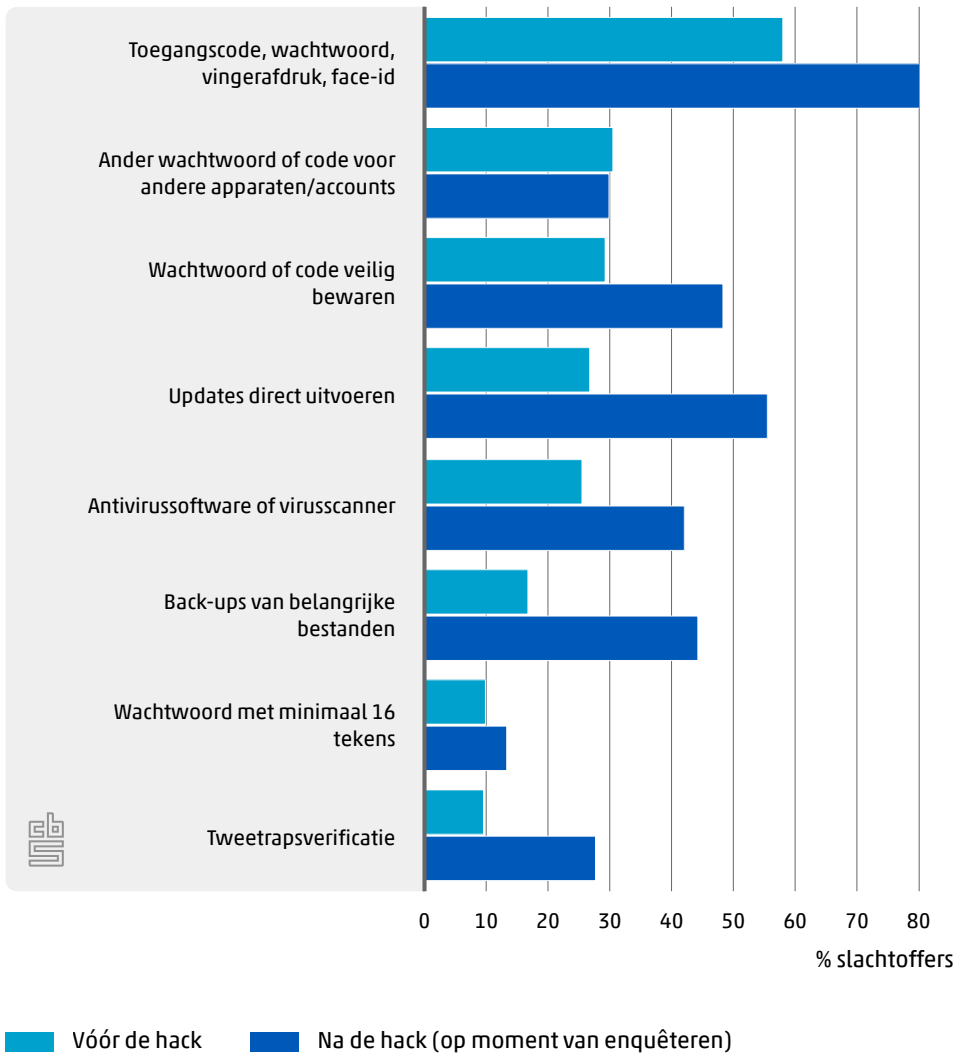
[1)] Meerdere antwoorden mogelijk.

Beveiligingsmaatregelen voor en na hacken account

Voordat het account werd gehackt gebruikte 58 procent van de slachtoffers iedere keer opnieuw een wachtwoord of toegangscode om dit account te vergrendelen. 31 procent gebruikte voordat het account werd gehackt een ander wachtwoord dan voor andere accounts of apparaten, en 29 procent bewaarde hun wachtwoord veilig. 10 procent gebruikte een wachtwoord met minimaal 16 tekens en eveneens 10 procent gebruikte tweetrapsverificatie.

Na de hack van het account zijn slachtoffers vaker beveiligingsmaatregelen gaan nemen[12)]. Het percentage dat het account vergrendelt steeg van 58 naar 83. Ook de meeste andere maatregelen werden duidelijk vaker getroffen, behalve het kiezen van verschillende wachtwoorden voor verschillende accounts en het kiezen van lange wachtwoorden[13)].

5.2.2 Maatregelen voor en na hacken account[1)], 2022



[1)] Meerdere antwoorden mogelijk.

5.3 Gevolgen hacken

Problemen voor slachtoffers

Bijna 2 op de 10 slachtoffers gaven aan emotionele en/of financiële problemen te hebben ondervonden als gevolg van de hack. Het gaat vaker om emotionele of psychische problemen dan om financiële problemen (14 tegen 6 procent).

Het hacken van een apparaat leidde vaker tot problemen dan het hacken van een account: 27 tegen 14 procent.

5.3.1 Problemen door hacken[1)], 2022

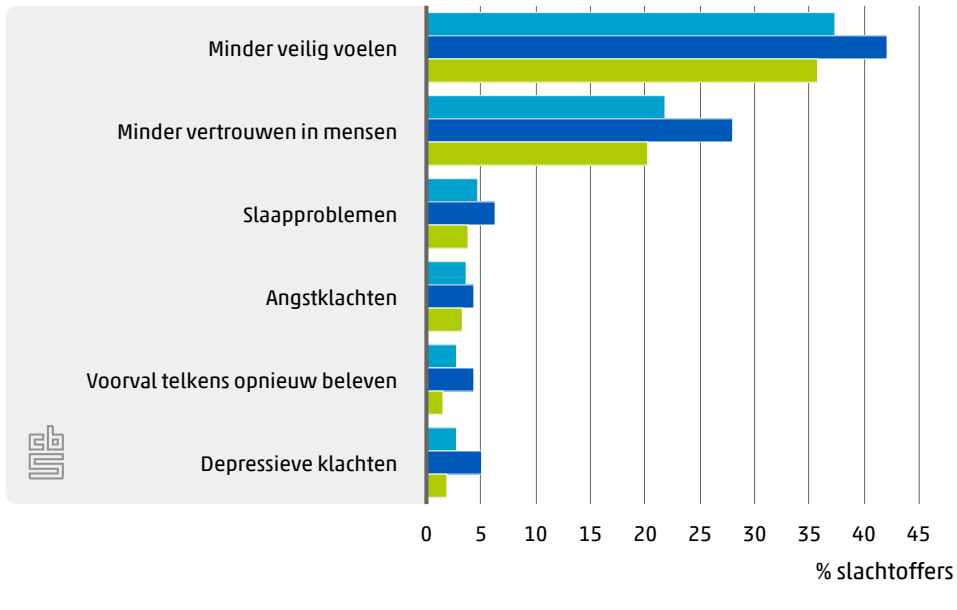
[1)] Meerdere antwoorden mogelijk.

Emotionele of psychische gevolgen

Voor de meeste slachtoffers van hacken had het voorval tot gevolg dat men zich minder veilig voelde (37 procent) en/of dat men minder vertrouwen had in mensen (22 procent). Slaapproblemen werden door 5 procent genoemd en angstklachten, depressieve klachten en het voorval steeds opnieuw beleven elk door ongeveer 3 procent.

Slachtoffers van het hacken van een apparaat geven vaker aan emotionele of psychische gevolgen te ondervinden dan slachtoffers van wie een account gehackt is.

5.3.2 Emotionele of psychische gevolgen door hacken[1)], 2022



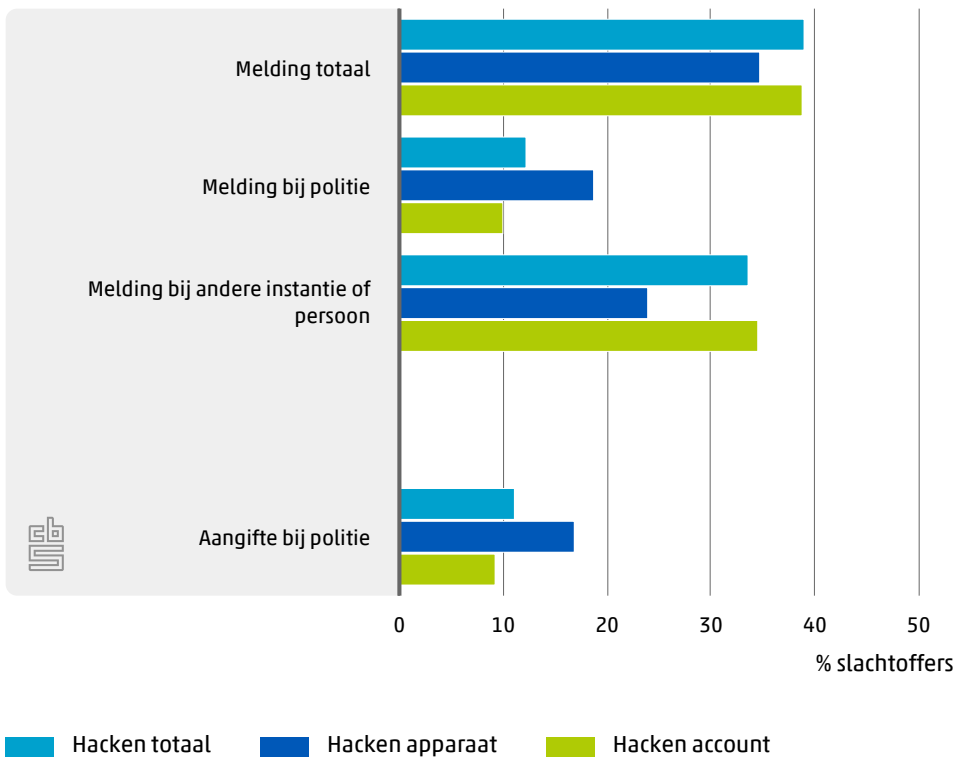
[1)] Meerdere antwoorden mogelijk.

5.4 Melding en aangifte hacken

39 procent van de slachtoffers van hacken heeft dit bij de politie en/of een andere instantie gemeld: 12 procent bij de politie en 34 procent bij een andere instantie. Bij die andere instanties gaat het bijvoorbeeld om meld- of adviespunten zoals Meld Misdaad Anoniem. Bij het hacken van accounts kan het ook gaan om de instantie die het account beheert (bijvoorbeeld de bank of Google) of om de internetprovider (bijvoorbeeld KPN of Vodafone).

Bijna alle meldingen van hacken bij de politie resulteerden in een aangifte (12 procent meldde het; 11 procent deed aangifte). Het hacken van apparaten werd vaker bij de politie gemeld en aangegeven dan het hacken van accounts. Slachtoffers van wie een account gehackt is meldden dit juist vaker bij een andere instantie dan de politie, en dan met name bij de instantie die het gehackte account beheerde (zie tabellenset).

5.4.1 Melding en aangifte hacken, 2022

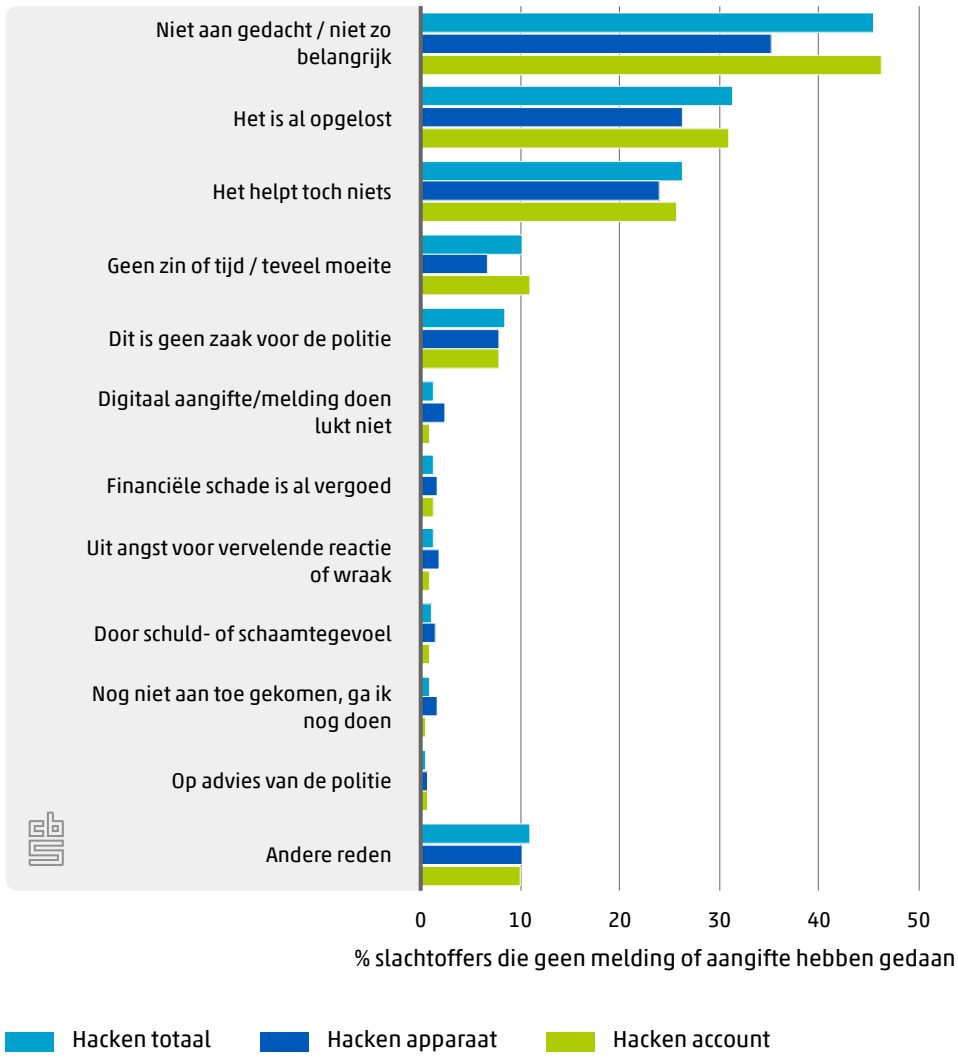


Slachtoffers van hacken deden het vaakst aangifte op het politiebureau (35 procent), gevolgd door telefonische aangifte (30 procent) en aangifte via internet (25 procent) (zie ook tabellenset).

Redenen geen melding of aangifte bij politie

De meest genoemde reden om de hack niet bij de politie te melden of aan te geven is dat er niet aan wordt gedacht of dat men het niet zo belangrijk vindt (46 procent). Daarna volgen 'het is al opgelost' (31 procent) en 'het helpt toch niets' (26 procent). Ongeveer 1 op de 10 heeft geen zin of tijd gehad, of vindt het te veel moeite.

5.4.2 Reden geen melding of aangifte bij politie van hacken[1)], 2022



[1)] Meerdere antwoorden mogelijk.

[10)] Bij de beveiligingsmaatregelen op het moment van enquêteren gaven enkele respondenten aan dat ze die alleen bij 'sommige' apparaten of accounts nemen. In deze gevallen is onbekend of dit ook voor het gehackte apparaat of account geldt. Aangenomen is dat dat niet zo is.

[11)] Het niet gebruiken van de genoemde maatregelen is in verreweg de meeste gevallen niet de oorzaak van de hack. Het klikken op een link, bijlage of filmpje is door slachtoffers de meest genoemde oorzaak (zie paragraaf 5.1).

[12)] Bij de maatregelen gaven enkele respondenten aan dat ze die alleen bij 'sommige' apparaten of accounts nemen. In deze gevallen is onbekend of dit ook voor het gehackte apparaat of account geldt. Aangenomen is dat dat niet zo is.

[13)] Het niet toepassen van de genoemde maatregelen is in verreweg de meeste gevallen niet de oorzaak van de hack. Het klikken op een link, bijlage of filmpje is door slachtoffers de meest genoemde oorzaak (zie paragraaf 5.1).

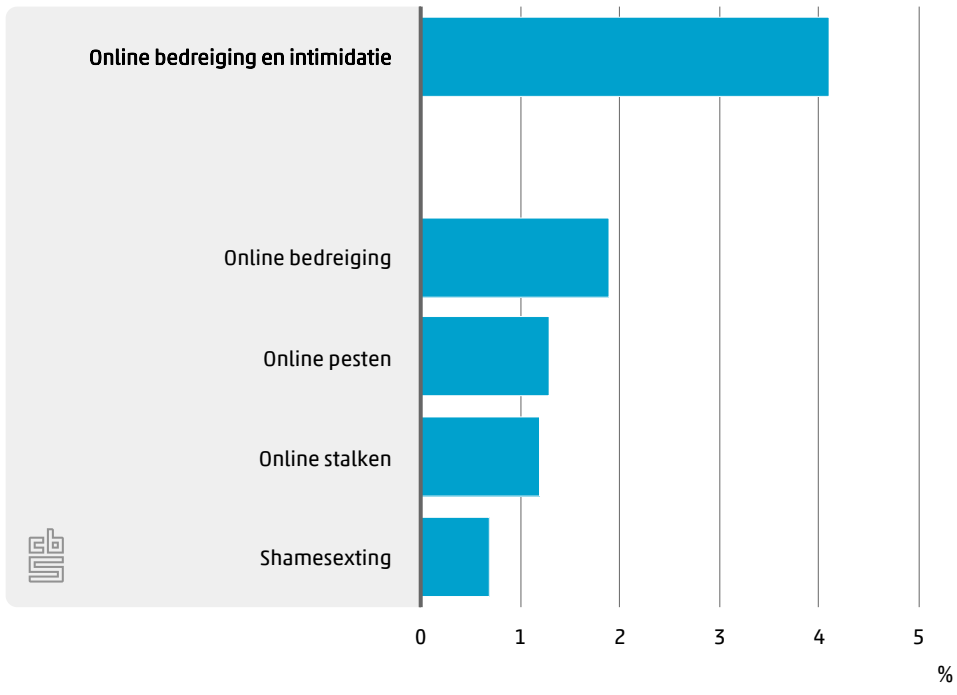
6. Online bedreiging en intimidatie

Het internet wordt niet alleen misbruikt om mensen op te lichten, te frauderen of om te hacken, maar ook om mensen te bedreigen en intimideren. Het gaat dan om dreigen met geweld, pesten, stalken en shamesexting, een vorm van seksueel grensoverschrijdend gedrag waarbij naaktfoto's of -filmpjes van het slachtoffer worden verspreid of hiermee wordt gedreigd. Bedreiging en intimidatie via internet verschilt van bedreiging en intimidatie in de fysieke wereld in de zin dat berichten en beeldmateriaal breder en sneller verspreid kunnen worden, voor anderen (lang) zichtbaar kunnen blijven en moeilijk te verwijderen zijn. Eerst komt het slachtofferschap van online bedreiging en intimidatie aan de orde. Daarna wordt beschreven wie de daders zijn, wat de gevolgen voor het slachtoffer zijn, en in welke mate slachtoffers melden wat hen overkomen is.

6.1 Slachtoffers online bedreiging en intimidatie

In 2022 gaf 4 procent van de Nederlanders van 15 jaar of ouder aan in de afgelopen 12 maanden slachtoffer te zijn geweest van online bedreiging en intimidatie. Dit zijn 600 duizend mensen. De meesten, 2 procent, waren slachtoffer van online bedreiging. Met online pesten en met online stalking had elk ruim 1 procent te maken. Van shamesexting werd 0,7 procent slachtoffer in 2022.

6.1.1 Slachtoffers online bedreiging en intimidatie, 2022



Slachtoffers online bedreiging en intimidatie naar persoonskenmerken

Jongeren, en dan vooral jonge vrouwen, werden relatief vaak slachtoffer van online bedreiging en intimidatie. Zo werd 12 procent van de vrouwen van 15 tot 25 jaar slachtoffer. Zij werden met name vaker slachtoffer van bedreiging en pesten. Personen met het laagste opleidingsniveau gaven vaker dan anderen aan slachtoffer te zijn geweest van online bedreiging en intimidatie. Biseksuele mannen en vrouwen, homoseksuele mannen en aseksuele personen hadden relatief vaak met online bedreiging en intimidatie te maken. Vooral biseksuele vrouwen waren met 14 procent vaak slachtoffer, met name van online bedreiging, pesten en stalken.

6.1.2 Slachtofferschap online bedreiging en intimidatie naar persoonskenmerken, 2022

	Totaal	Online bedreiging	Online pesten	Online stalken	Shamesexting
	%	%	%	%	%
Totaal	4,1	1,9	1,3	1,2	0,7
Geslacht					
Mannen	4,2	2,1	1,4	1,0	0,8
Vrouwen	4,0	1,8	1,3	1,5	0,5
Leeftijd					
15 tot 25 jaar	9,8	4,8	4,0	2,6	1,4
25 tot 45 jaar	4,4	2,0	1,7	1,3	0,7
45 tot 65 jaar	3,1	1,6	0,6	1,0	0,5
65 jaar en ouder	1,6	0,6	0,2	0,7	0,3
Geslacht x leeftijd					
Mannen, 15 tot 25 jaar	8,2	4,0	3,6	1,3	1,3
Mannen, 25 tot 45 jaar	4,7	2,2	1,9	1,2	0,9
Mannen, 45 tot 65 jaar	3,4	1,9	0,6	0,8	0,7
Mannen, 65 jaar en ouder	2,1	0,9	0,2	0,8	0,4
Vrouwen, 15 tot 25 jaar	11,5	5,7	4,4	3,9	1,5
Vrouwen, 25 tot 45 jaar	4,0	1,8	1,5	1,3	0,5
Vrouwen, 45 tot 65 jaar	2,8	1,2	0,6	1,2	0,3
Vrouwen, 65 jaar en ouder	1,1	0,4	0,1	0,6	0,2
Opleidingsniveau					
Laag	4,9	2,4	2,0	1,5	0,8
Middelbaar	4,4	2,0	1,3	1,3	0,8
Hoog	3,3	1,7	0,9	1,0	0,3
Seksuele oriëntatie					
Homoseksuele mannen	7,2	4,0	2,6	1,8	1,3
Homoseksuele vrouwen	4,3	1,4	2,5	1,1	0,5
Biseksuele mannen	8,2	2,7	4,1	1,4	2,1
Biseksuele vrouwen	14,0	6,9	6,0	4,6	1,2
Heteroseksuele mannen	3,9	2,0	1,2	0,9	0,6
Heteroseksuele vrouwen	3,7	1,7	1,0	1,4	0,5
Aseksuele personen[1)]	8,5	2,7	5,1	2,2	1,4

[1)] Voor aseksuele personen ontbreekt de uitsplitsing naar geslacht i.v.m. te weinig waarnemingen.

Slachtofferschap online seksueel grensoverschrijdend gedrag iets toegenomen

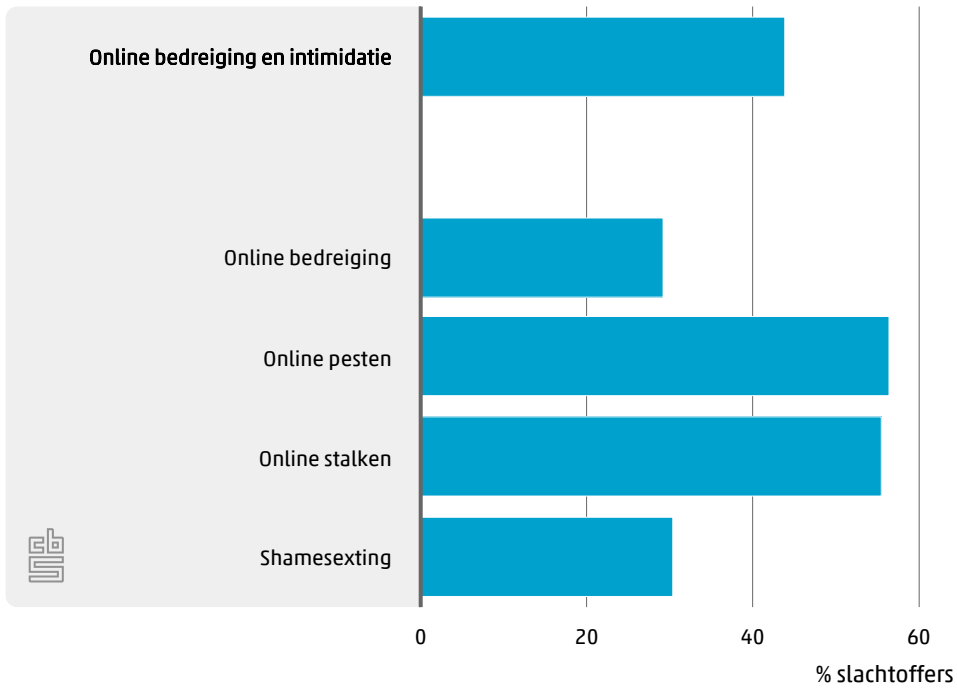
In de Prevalentiemonitor Huiselijk Geweld en Seksueel Grensoverschrijdend gedrag is aan Nederlanders van 16 jaar of ouder gevraagd of zij te maken hebben gehad met online seksueel grensoverschrijdend gedrag (Akkermans, Derksen, Kloosterman, Moons en Wingen, 2023). Het gaat daarbij om ongewenste seksuele ervaringen die online plaatsvinden, uiteenlopend van het ontvangen van seksueel getinte opmerkingen via sociale media, WhatsApp, (video)chat of e-mail tot het gedwongen worden tot seksuele handelingen. In 2022 gaf 6 procent van de Nederlanders van 16 jaar of ouder (bijna 930 duizend personen) aan dit in de afgelopen twaalf maanden te hebben meegemaakt. In 2020 was dit 5 procent.

Vrouwen gaven in 2022 bijna twee keer zo vaak als mannen aan in de afgelopen 12 maanden ongewenst seksueel gedrag te hebben meegemaakt op het internet (8 tegen 4 procent). Biseksuele en homoseksuele personen kregen er vaker mee te maken dan heteroseksuele personen. Jongeren zijn duidelijk het vaakst slachtoffer van online seksueel grensoverschrijdend gedrag, en dan met name jonge vrouwen: 35 procent van de 16- tot 18-jarige vrouwen en 28 procent van de 18- tot 24-jarige vrouwen gaven aan hier in de afgelopen 12 maanden mee te zijn geconfronteerd, tegen 9 procent van hun mannelijke leeftijdgenoten.

6.2 Daders online bedreiging en intimidatie

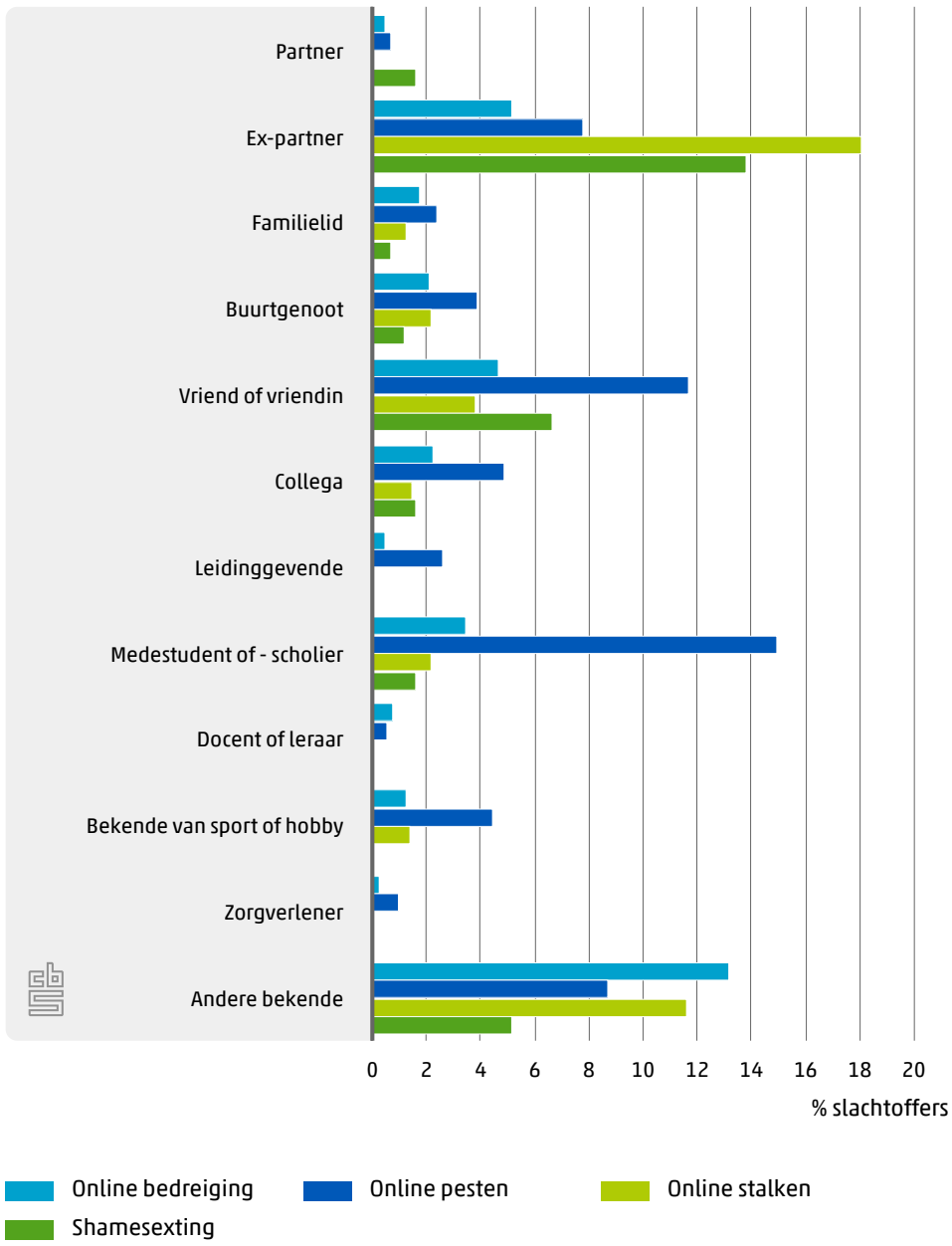
Bij ruim 4 op de 10 slachtoffers van online bedreiging en intimidatie was bekend wie de dader was. Bij pesten en stalken kende de slachtoffers de dader(s) het vaakst.

6.2.1 Kende dader(s) van online bedreiging en intimidatie, 2022



De meest genoemde daders zijn de ex-partner, een vriend/vriendin of een medestudent/-scholier. De ex-partner wordt bij online stalken en shamesexting het vaakst als dader genoemd, respectievelijk door 18 en 14 procent van de slachtoffers. Bij online pesten wordt een medestudent/-scholier (15 procent) of een vriend/vriendin (12 procent) het vaakst als dader genoemd.

6.2.2 Daders van online bedreiging en intimidatie[1)], 2022



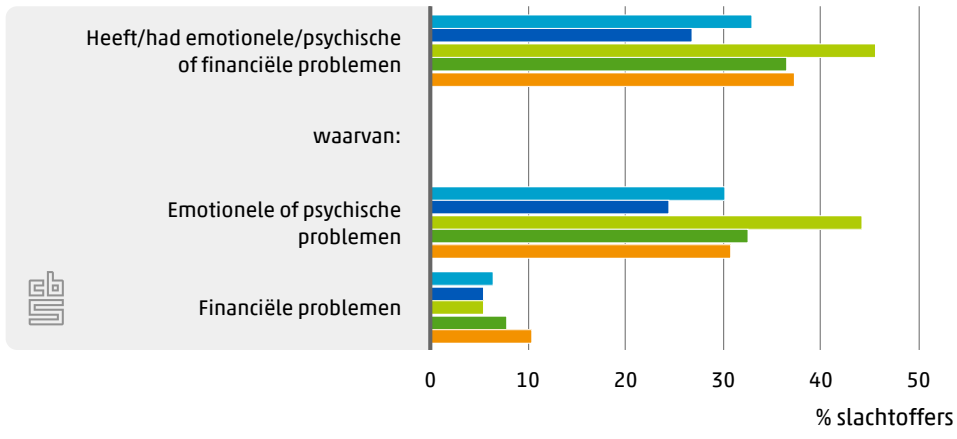
[1)] Meerdere antwoorden mogelijk.

6.3 Gevolgen online bedreiging en intimidatie

Problemen voor slachtoffers

Een derde van de slachtoffers van online bedreiging en intimidatie zei emotionele of psychische problemen dan wel financiële problemen te hebben of te hebben gehad als gevolg van het voorval. Slachtoffers van online pesten hebben het vaakst emotionele of psychische problemen ervaren: 44 procent. Van de slachtoffers van online stalken en shamesexting kreeg elk ruim 30 procent dit soort problemen. Slachtofferschap van online bedreiging en intimidatie leidde vaker tot emotionele of psychische problemen dan tot financiële problemen: 30 tegen 7 procent. Financiële problemen werden het vaakst genoemd bij shamesexting. Ongeveer de helft (49 procent) van de slachtoffers hiervan gaf aan dat de dader om geld had gevraagd om het verspreiden van de beelden te voorkomen.

6.3.1 Problemen door online bedreiging en intimidatie[1)], 2022



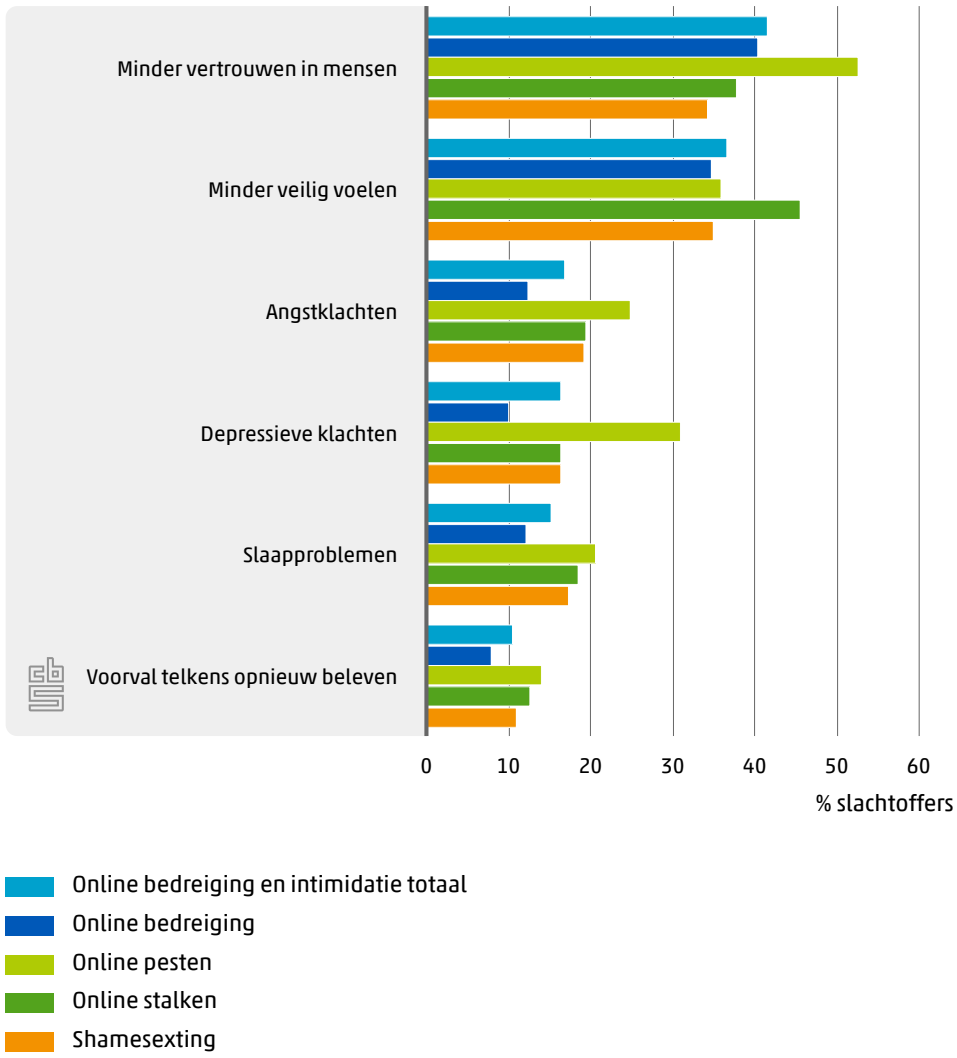
[1)] Meerdere antwoorden mogelijk.

Emotionele of psychische gevolgen

Voor de meeste slachtoffers van online bedreiging en intimidatie heeft of had het voorval tot gevolg dat men minder vertrouwen had in mensen (42 procent) en dat men zich minder veilig voelde (37 procent). Slaapproblemen, depressieve klachten, angstklachten en het voorval steeds opnieuw beleven werden met percentages tussen de 10 en 20 procent minder vaak genoemd.

Slachtoffers van online stalken geven het vaakst aan zich minder veilig te voelen door het voorval. Minder vertrouwen hebben in mensen en depressieve klachten worden vaker als gevolg genoemd door slachtoffers van online pesten.

6.3.2 Emotionele of psychische gevolgen door online bedreiging en intimidatie[1)], 2022



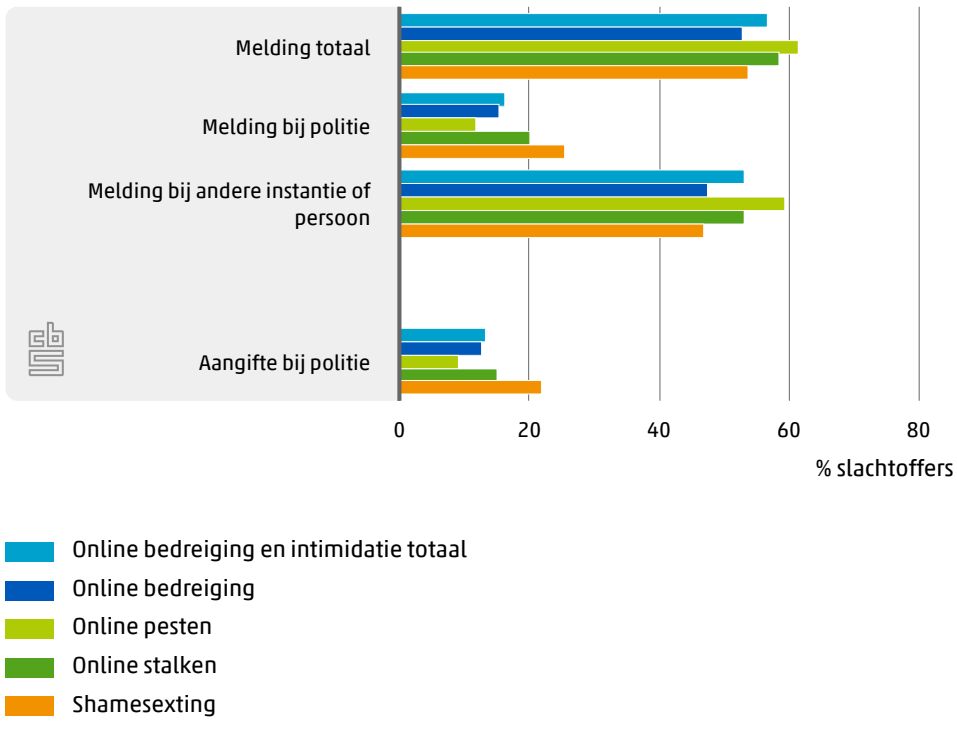
[1)] Meerdere antwoorden mogelijk.

6.4 Melding en aangifte online bedreiging en intimidatie

In totaal heeft 57 procent van de slachtoffers het voorval ergens gemeld: bijna 2 op de 10 bij de politie en ruim 5 op de 10 bij een andere instantie of persoon. Bij instanties gaat het bijvoorbeeld om meld- of adviespunten zoals Meld Misdaad Anoniem of Veilig Thuis. Bij personen kan het bijvoorbeeld gaan om professionele hulpverleners zoals huisartsen, psychologen of maatschappelijk werkers, om andere professionals zoals leerkrachten of leidinggevenden, en om mensen uit het eigen, informele circuit zoals andere gezinsleden, familie of vrienden.

Bijna alle meldingen van online bedreiging en intimidatie bij de politie resulteerden in een aangifte (17 procent maakte melding; 13 procent deed aangifte). Van shamesexting werd door slachtoffers het vaakst aangifte gedaan bij de politie (22 procent), van pesten het minst vaak (9 procent).

6.4.1 Melding en aangifte online bedreiging en intimidatie, 2022



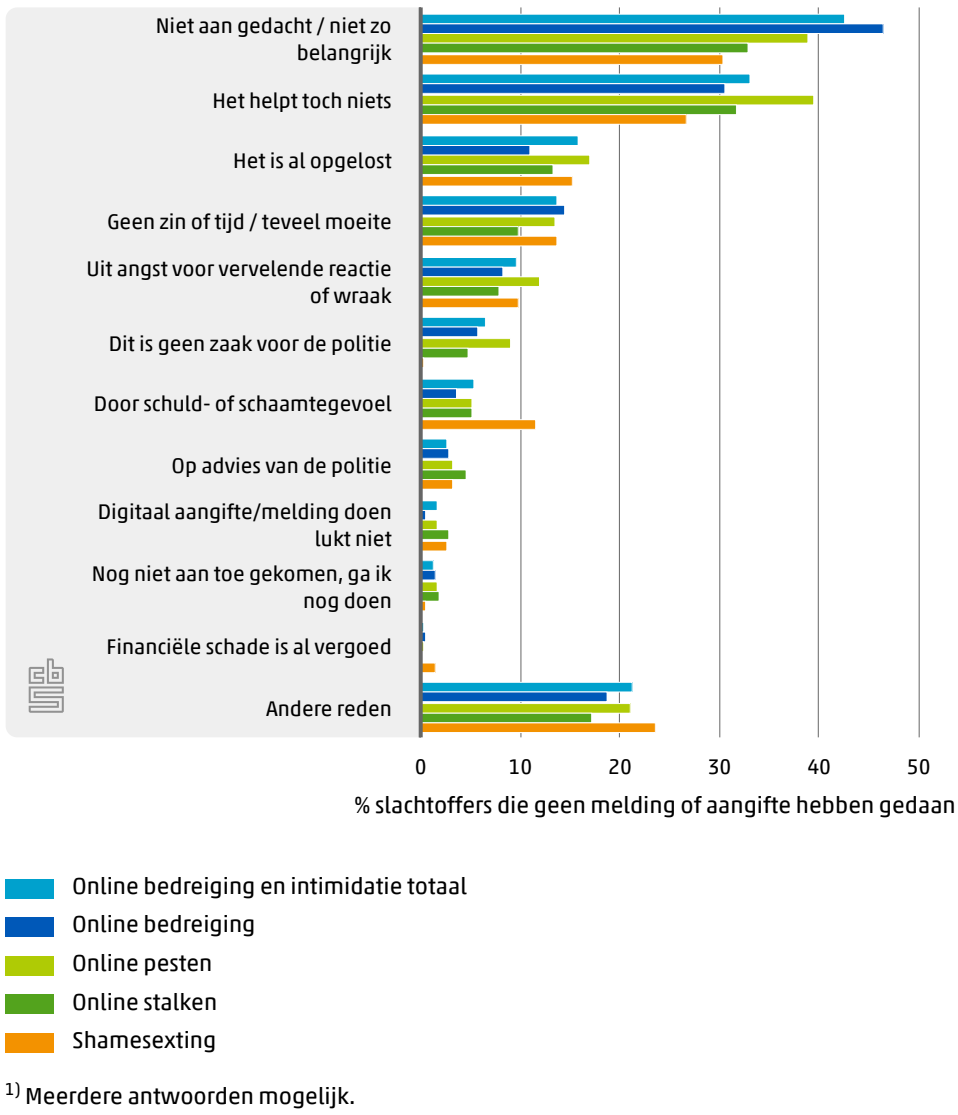
De meeste slachtoffers van online bedreiging en intimidatie die aangifte deden, deden dit op het politiebureau (zie ook tabellenset). Daarnaast deed 31 procent telefonisch aangifte en 14 procent via internet. Bijna 2 op de 10 heeft op een andere manier aangifte gedaan.

Redenen geen melding of aangifte bij politie

De meest genoemde reden om het voorval niet bij de politie te melden of aangifte te doen is dat er niet aan wordt gedacht of dat men het niet zo belangrijk vindt (43 procent), gevolgd door 'het helpt toch niets' (33 procent). Ongeveer 16 procent zei dat het al is opgelost en 14 procent heeft geen zin of tijd gehad, of vindt het te veel moeite. Alle andere redenen worden door slachtoffers minder vaak genoemd.

Slachtoffers van online pesten geven vaker dan slachtoffers van andere delicten 'het helpt toch niets' als reden om geen melding of aangifte te doen bij de politie. Slachtoffers van shamesexting noemen vaker het hebben van schuld- of schaamtegevoel als reden.

6.4.2 Reden geen melding of aangifte van online bedreiging en intimidatie[1)], 2022



[1)] Meerdere antwoorden mogelijk.

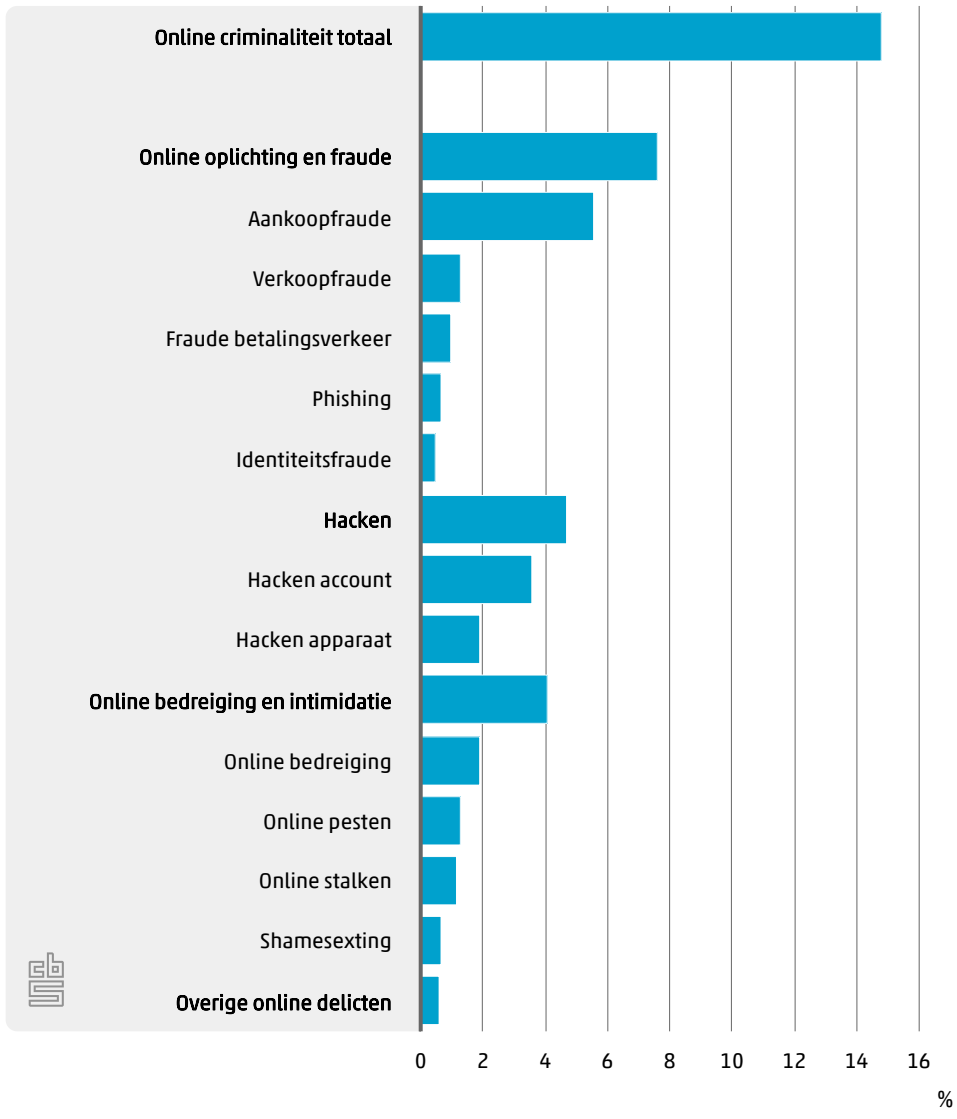
7. Online criminaliteit totaal

In de hoofdstukken 4, 5 en 6 stonden de verschillende soorten online criminaliteit centraal. In dit hoofdstuk worden deze in onderlinge samenhang beschreven en wordt een totaalbeeld van online criminaliteit geschetst. Zoals in de vorige hoofdstukken komen achtereenvolgens slachtofferschap, gevolgen, en melding en aangifte aan de orde.

7.1 Slachtoffers online criminaliteit

In 2022 gaf 15 procent van de Nederlanders van 15 jaar of ouder aan in de afgelopen 12 maanden slachtoffer te zijn geweest van online criminaliteit. Dit zijn 2,2 miljoen mensen. De meesten, 8 procent, waren slachtoffer van oplichting en fraude, vooral van aankoopfraude.5 procent had te maken met hacken en 4 procent met bedreiging en intimidatie. Een half procent werd slachtoffer van andere online delicten.

7.1.1 Slachtoffers online criminaliteit, 2022



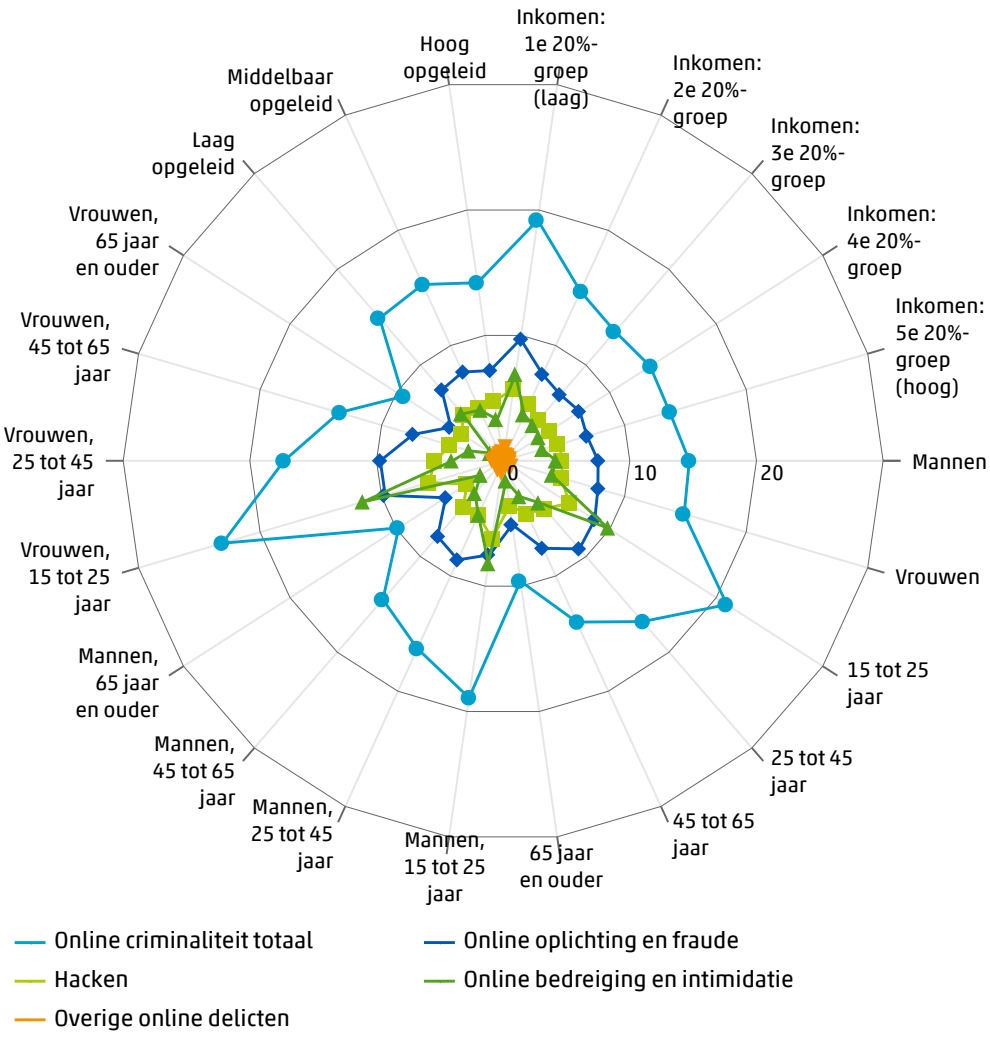
Overige online delicten

In dit onderzoek is aan de deelnemers via een open antwoordmogelijkheid gevraagd of ze weleens slachtoffer zijn geweest van een ander misdrijf via internet, dus van een misdrijf dat bij oplichting en fraude, hacken of online bedreiging en intimidatie niet aan de orde kwam. Uit een analyse van de ingevulde antwoorden bleek dat het overgrote deel van de misdrijven binnen een van deze drie delictgroepen past. Daarom is ervoor gekozen om deze ‘overige online delicten’ niet in detail te beschrijven zoals dat in de hoofdstukken 4 t/m 6 voor online oplichting en fraude, hacken, en online bedreiging en intimidatie is gebeurd. In dit hoofdstuk dat een totaalbeeld van online criminaliteit geeft zijn de overige online delicten volledigheidshalve wel meegenomen. Het achterliggende cijfermateriaal is beschikbaar in de bijlagetabellen en de tabellenset.

Slachtoffers online criminaliteit naar persoonskenmerken

Jongeren werden relatief vaak slachtoffer van online criminaliteit. Zo werd 21 procent van de 15- tot 25-jarigen slachtoffer, jonge vrouwen iets vaker dan jonge mannen. Vooral bij het slachtofferschap van online bedreiging en intimidatie is er een groot verschil tussen jongeren en oudere leeftijdsgroepen. Ook personen uit huishoudens met de laagste inkomens werden vaak met online criminaliteit geconfronteerd (19 procent). Biseksuele vrouwen en aseksuelen hadden er vaker mee te maken dan anderen (zie tabellenset), dit houdt verband met hun hoge slachtofferschap van online bedreiging en intimidatie.

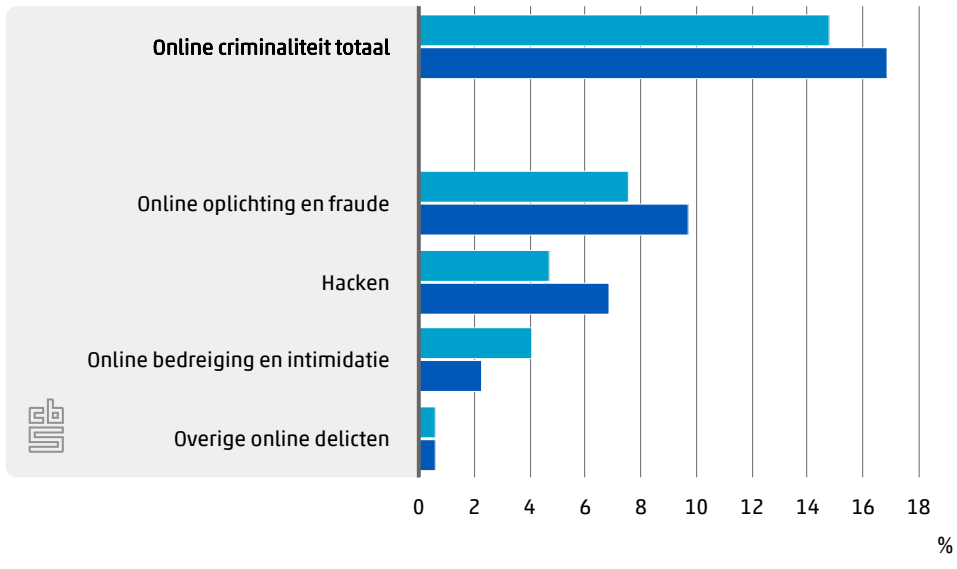
7.1.2 Slachtoffers online criminaliteit naar persoonskenmerken, 2022



Ontwikkeling slachtofferschap online criminaliteit

In 2021 is het slachtofferschap van online criminaliteit in de Veiligheidsmonitor onderzocht. 17 procent van de Nederlanders van 15 jaar of ouder gaf toen aan in de afgelopen 12 maanden slachtoffer te zijn geweest van een of meerdere vormen van online criminaliteit. Dat is iets hoger dan de 15 procent slachtoffers van online criminaliteit in 2022 zoals gemeten in dit onderzoek. Bij online oplichting en fraude was het percentage slachtoffers in 2022 lager dan in 2021 (8 tegen 10 procent), evenals bij hacken (5 tegen 7 procent). Online bedreiging en intimidatie daarentegen werd in 2022 meer gerapporteerd dan in 2021 (4 tegen 2 procent). Het percentage slachtoffers van overige online delicten bleef gelijk.

Slachtoffers online criminaliteit[1)], 2021-2022



[1)] Door methodologische verschillen zijn de cijfers van OVeC 2022 en de VM 2021 niet zonder meer vergelijkbaar (zie tekstkader paragraaf 7.1 en de Onderzoeksverantwoording).

De vraagstellingen om slachtofferschap van online criminaliteit te meten zijn in de Veiligheidsmonitor 2021 en Online Veiligheid en Criminaliteit 2022 op een enkele uitzondering[14)] na identiek, en ook de opzet en uitvoering van de beide onderzoeken is gelijk gehouden (het steekproefontwerp is vergelijkbaar, de dataverzameling vond plaats via internetenquêtering, en de veldwerkperiode liep van augustus t/m oktober). Desondanks zijn de uitkomsten van beide onderzoeken door verschillen in de context waarbinnen de vragen gesteld zijn (OVeC gaat hoofdzakelijk over online criminaliteit, in de Veiligheidsmonitor is dit één van de thema's) en door mogelijke selectie-effecten (het is denkbaar dat beide enquêtes, afhankelijk van de affiniteit met het onderwerp verschillende typen respondenten aantrekken) niet zonder meer vergelijkbaar (zie de toelichting in de Onderzoeksverantwoording). Hoe groot deze effecten zijn is nog niet vastgesteld. Om meer inzicht hierin te krijgen is verder onderzoek nodig zoals wordt aanbevolen in paragraaf 10.2.

Hoewel de uitkomsten van de Veiligheidsmonitor 2021 en OVeC 2022 dus niet 1-op-1 vergelijkbaar zijn, zijn er indicaties dat de in de bovenstaande figuur getoonde cijfers de feitelijke ontwikkeling van het slachtofferschap van online criminaliteit tussen 2021 en 2022 weergeven:

- Volgens de registratie van de politie nam het aantal aangiften van online oplichting en van computervredebreuk tussen 2021 en 2022 af. Het aantal geregistreerde misdrijven in de categorie 'cybercrime'[15)] (waaronder hacken) daalde van afgerond 14 200 in 2021 naar 14 000 in 2022 (Politie data.politie.nl, 2023). In de categorie 'horizontale fraude' (waaronder fraude online handel, fraude betalingsverkeer, identiteitsfraude) daalde het aantal geregistreerde misdrijven in dezelfde periode in totaal van afgerond 118 duizend naar 87 duizend, waarvan fraude online handel van 51 duizend naar 42 duizend, fraude betalingsverkeer van 10 duizend naar 8 duizend, en identiteitsfraude van 10 duizend naar 9 duizend[16)].
- Uit de enquête ICT-gebruik huishoudens en personen 2022 blijkt dat het percentage Nederlanders van 12 jaar of ouder dat aangeeft in de afgelopen drie maanden iets online te hebben gekocht is gedaald van 77 procent in 2021 naar 74 procent in 2022 (CBS, 2022). Mogelijk speelt hierbij mee dat in het coronajaar 2021 mensen door lockdowns en andere beperkende maatregelen meer aan huis gebonden waren, en daardoor meer online kochten dan in 2022, het jaar waarin de beperkingen geleidelijk werden versoepeld of losgelaten. Wanneer minder mensen online kopen ligt het voor de hand dat ook minder mensen slachtoffer worden, in dit geval met name van aankoopfraude.
- Uit de Prevalentiemonitor Huiselijk Geweld en Seksueel Grensoverschrijdend gedrag 2022 blijkt dat het percentage slachtoffers van online seksueel grensoverschrijdend gedrag (waaronder shamesexting) licht is gestegen van 5 procent in 2020 naar 6 procent in 2022 (Akkermans, Derksen, Kloosterman, Moons en Wingen, 2023). Dit kan mogelijk te maken hebben met de maatschappelijke discussie over (seksueel) grensoverschrijdend gedrag in 2022 en de daaraan gekoppelde grotere bewustwording van slachtoffers van wat hen overkomen is, maar ook de coronapandemie kan een rol hebben gespeeld.

Deze bevindingen zijn in lijn met het beeld dat uit de figuur naar voren komt, namelijk dat het slachtofferschap van online oplichting en fraude en van hacken tussen 2021 en 2022 licht lijkt te zijn afgenomen en dat de rapportage van het slachtofferschap van online bedreiging en intimidatie in dezelfde periode licht lijkt te zijn toegenomen.

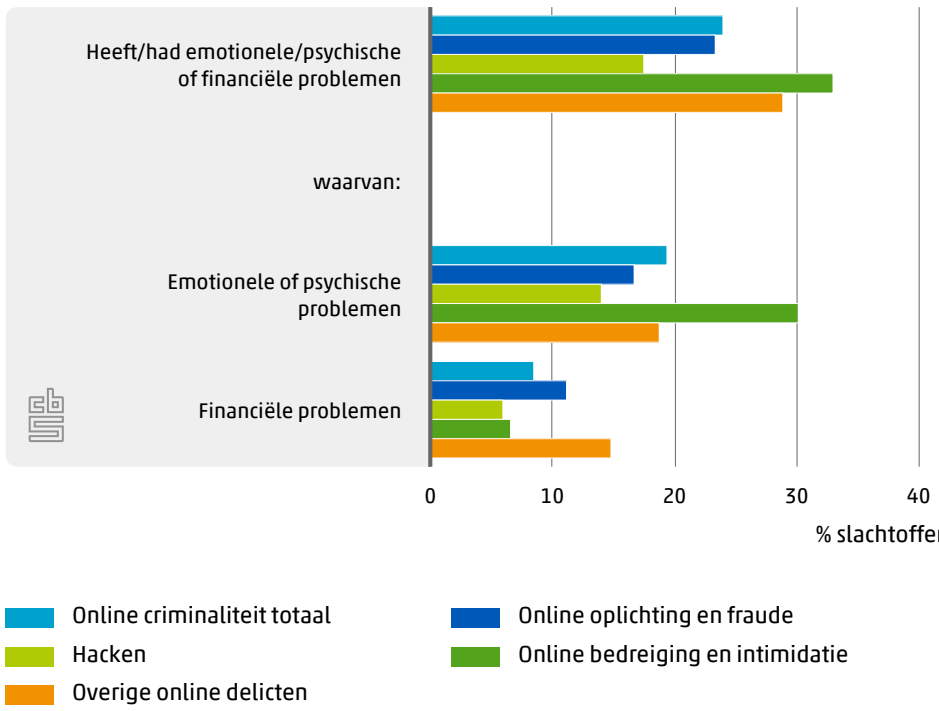
7.2. Gevolgen online criminaliteit

Problemen voor slachtoffers

Bijna een kwart (24 procent) van de slachtoffers van online criminaliteit zei emotionele of psychische problemen dan wel financiële problemen te hebben of te hebben gehad als gevolg van het voorval. Het vaakst ervoeren slachtoffers van online bedreiging en intimidatie problemen: 33 procent. Het minst vaak slachtoffers van hacken: 18 procent.

Slachtofferschap van online criminaliteit leidde vaker tot emotionele of psychische problemen dan tot financiële problemen: 20 tegen 9 procent. Vooral bij online bedreiging en intimidatie is dit verschil relatief groot (30 tegen 7 procent).

7.2.1 Problemen door online criminaliteit[1)], 2022



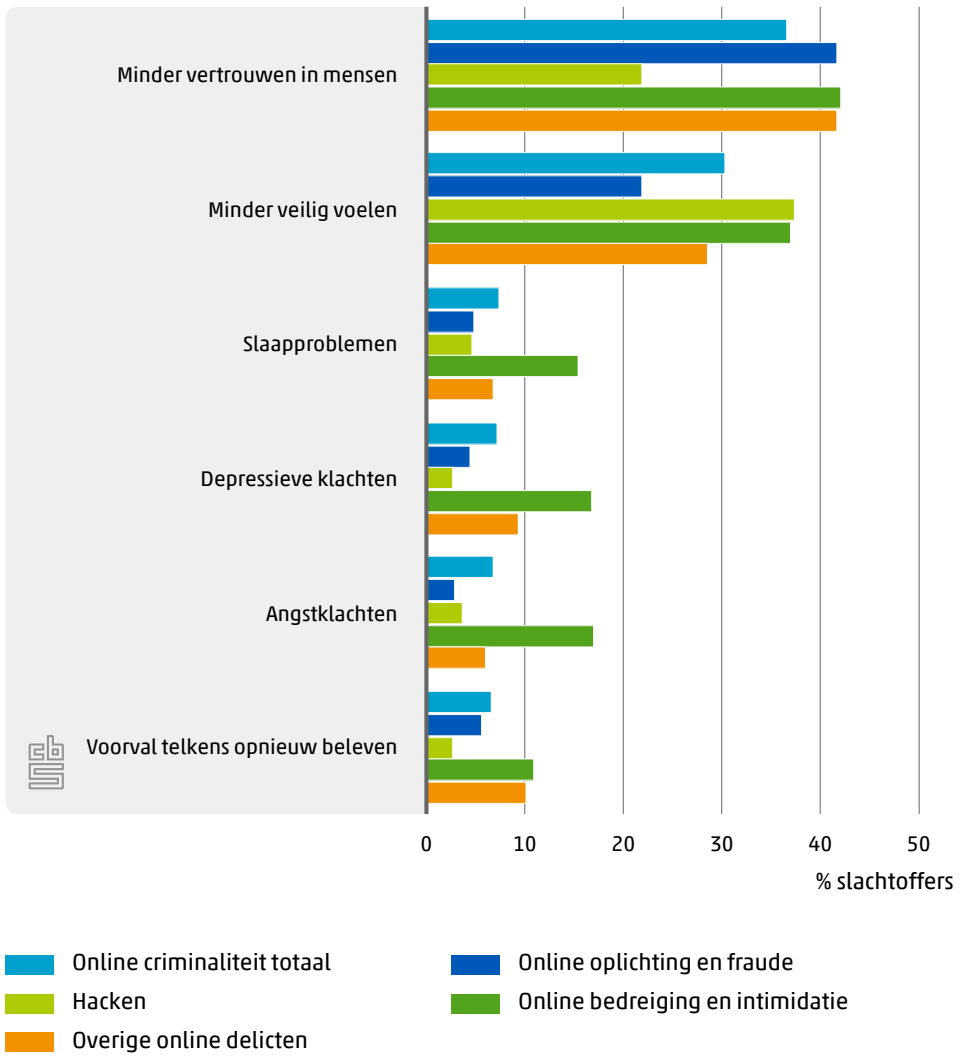
[1)] Meerdere antwoorden mogelijk.

Emotionele of psychische gevolgen

Voor de meeste slachtoffers van online criminaliteit heeft of had het voorval tot gevolg dat men minder vertrouwen had in mensen (37 procent) en dat men zich minder veilig voelde (30 procent). Slaapproblemen, depressieve klachten, angstklachten en het voorval steeds opnieuw beleven werden elk door 7 á 8 procent van de slachtoffers genoemd.

Hacken leidde met ruim 20 procent minder vaak tot afname van vertrouwen in mensen dan andere online delicten (ongeveer 40 procent). Online oplichting leidde met ruim 20 procent minder vaak tot onveiligheidsgevoelens. Bij hacken en bij online bedreiging en intimidatie gaf bijna 40 procent aan zich minder veilig te voelen. Het telkens opnieuw beleven van het voorval, slaapproblemen, depressieve klachten en angstklachten werden door slachtoffers van online bedreiging en intimidatie vaker gerapporteerd dan door slachtoffers van de andere online delicten.

7.2.2 Emotionele of psychische gevolgen online criminaliteit[1)], 2022

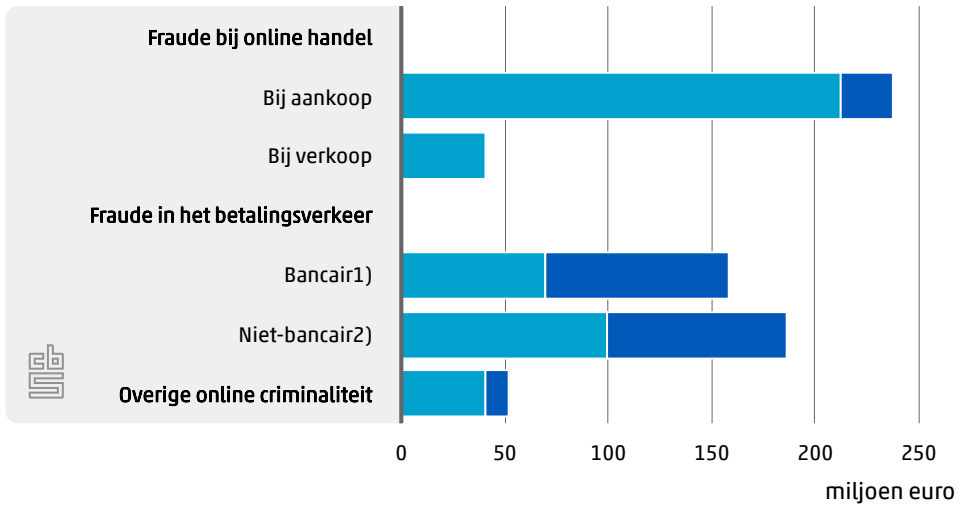


1) Meerdere antwoorden mogelijk.

Financiële schade online criminaliteit

In de Veiligheidsmonitor 2021 is aan slachtoffers van vermogensdelicten gevraagd hoeveel geld ze hierdoor zijn kwijtgeraakt en welk bedrag vergoed is door een financiële instelling zoals een bank of verzekeraar. Als het gaat om online criminaliteit bedroeg het totale schadebedrag in 2021 afgerond 680 miljoen euro (Reep, 2022). Het grootste deel hiervan (350 miljoen euro) had betrekking op fraude in het betalingsverkeer, gevolgd door aankoopfraude (240 miljoen). Financiële schade die slachtoffers leden door fraude in het betalingsverkeer werd voor grofweg de helft vergoed, schade als gevolg van aankoopfraude voor ongeveer een tiende deel.

Financiële schade online criminaliteit, 2021



1) Bij bancaire fraude had de dader toegang tot de bankrekening van het slachtoffer. Bij niet-bancaire fraude maakte het slachtoffer het geld zelf over.
2) Minstens 38 duizend euro van de niet- bancaire fraude zal zijn terugbetaald door de dader en betreft dus geen schade voor de financiële instellingen.

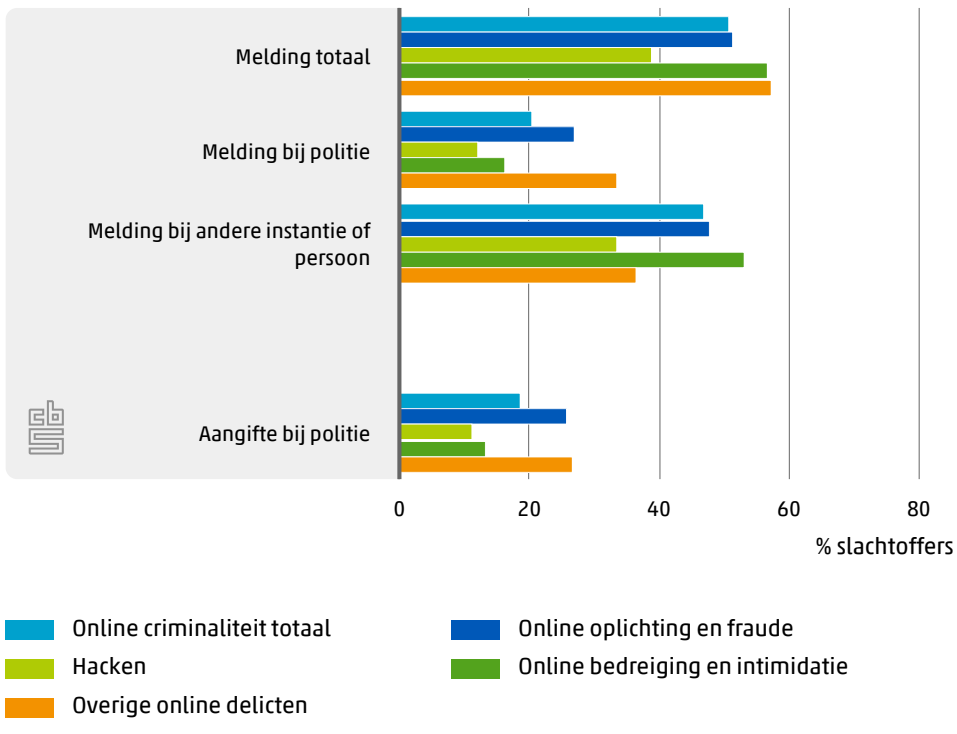
Ook in OVeC 2022 is aan slachtoffers van online vermogenscriminaliteit op dezelfde manier als in de Veiligheidsmonitor gevraagd naar de financiële schade die hierdoor ontstaan is. Aanbevolen wordt hierover in een separate publicatie te rapporteren (zie Conclusies en aanbevelingen).

7.3 Melding en aangifte online criminaliteit

Ruim 2 op de 10 slachtoffers van online criminaliteit hebben bij de politie gemeld wat hen overkomen is, en bijna 5 op de 10 slachtoffers hebben dit bij een andere instantie of persoon gedaan. Bij instanties gaat het bijvoorbeeld om meld- of adviespunten voor online criminaliteit. Bij personen kan het bijvoorbeeld gaan om professionele hulpverleners zoals huisartsen, psychologen of maatschappelijk werkers, om andere professionals zoals leerkrachten of leidinggevenden, of om mensen uit het eigen, informele circuit zoals andere gezinsleden, familie of vrienden. In totaal heeft 51 procent van de slachtoffers van online criminaliteit in 2022 bij de politie en/of een andere instantie of persoon melding gemaakt. Bijna alle meldingen van online criminaliteit bij de politie resulteerden in een aangifte (21 procent maakte melding; 19 procent deed aangifte).

Hacken werd met 39 procent minder vaak gemeld dan online oplichting en fraude (52 procent), online bedreiging en intimidatie (57 procent) en overige online delicten (58 procent). Meldingen bij de politie, en in het verlengde daarvan aangiften, gingen relatief vaak over online oplichting en fraude en overige online delicten, en relatief minder vaak over hacken en online bedreiging en intimidatie.

7.3.1 Melding en aangifte online criminaliteit, 2022



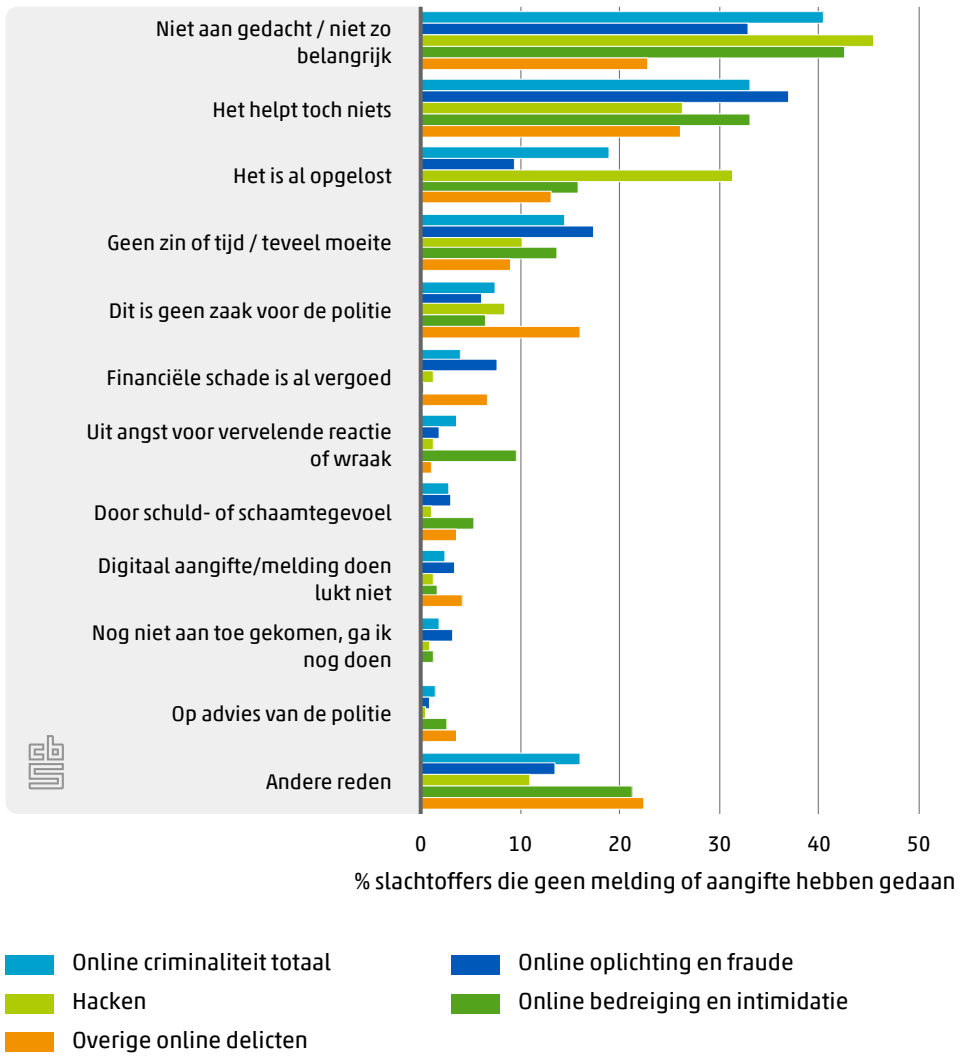
De meeste slachtoffers van online criminaliteit (44 procent) deden aangifte via internet (zie ook tabellenset). Ruim 3 op de 10 deden dit op het politiebureau, ruim 2 op de 10 telefonisch, en ruim 1 op de 10 op een andere manier.

Redenen geen melding of aangifte bij politie

De meest genoemde reden om het voorval niet bij de politie te melden of aangifte te doen is dat er niet aan wordt gedacht of dat men het niet zo belangrijk vindt (41 procent), gevolgd door 'het helpt toch niets' (33 procent). Ongeveer 20 procent zei dat het al is opgelost en 15 procent heeft geen zin of tijd gehad, of vindt het te veel moeite. Alle andere redenen worden door 8 procent of minder van de slachtoffers van online criminaliteit genoemd.

Slachtoffers van hacken noemden relatief vaak 'het is al opgelost' als reden om het voorval niet bij de politie te melden of aangifte te doen, slachtoffers van overige online delicten zeiden vaak dat het geen zaak voor de politie is, en slachtoffers van online bedreiging en intimidatie deden vaak uit angst voor een vervelende reactie of wraak geen melding of aangifte.

7.3.2 Reden geen melding of aangifte bij politie van online criminaliteit[1)], 2022



[1)] Meerdere antwoorden mogelijk.

[14)] De vraagstelling om het slachtofferschap van de delictsoort online bedreiging te meten verschilt tussen de VM 2021 en OVeC 2022 (zie de Onderzoeksverantwoording voor meer informatie).

[15)] Op data.politie.nl worden onder de categorie 'cybercrime' verstaan alle vormen van bezitsaantasting waarbij de computer zowel het middel als het doel is.

[16)] Deze cijfers zijn afkomstig uit een secundaire analyse van de data op data.politie.nl. De cijfers van de categorie 'horizontale fraude' zijn uitgesplitst naar de genoemde subcategorieën.

8. Online discriminatie

Niet alleen criminaliteit maar ook discriminatie kan online plaatsvinden. Net zoals voor online bedreiging en intimidatie geldt ook voor online discriminatie dat opmerkingen en beelden via internet breder en sneller verspreid kunnen worden, voor anderen (lang) zichtbaar kunnen blijven en moeilijk te verwijderen zijn. Hoeveel Nederlanders voelen zich online gediscrimineerd? Op welke gronden, manieren en via welke kanalen vindt online discriminatie plaats? Wat is de impact op degenen die de discriminatie ervaren? En melden ze de discriminatie, en zo ja, waar? Deze vragen staan in dit hoofdstuk centraal.

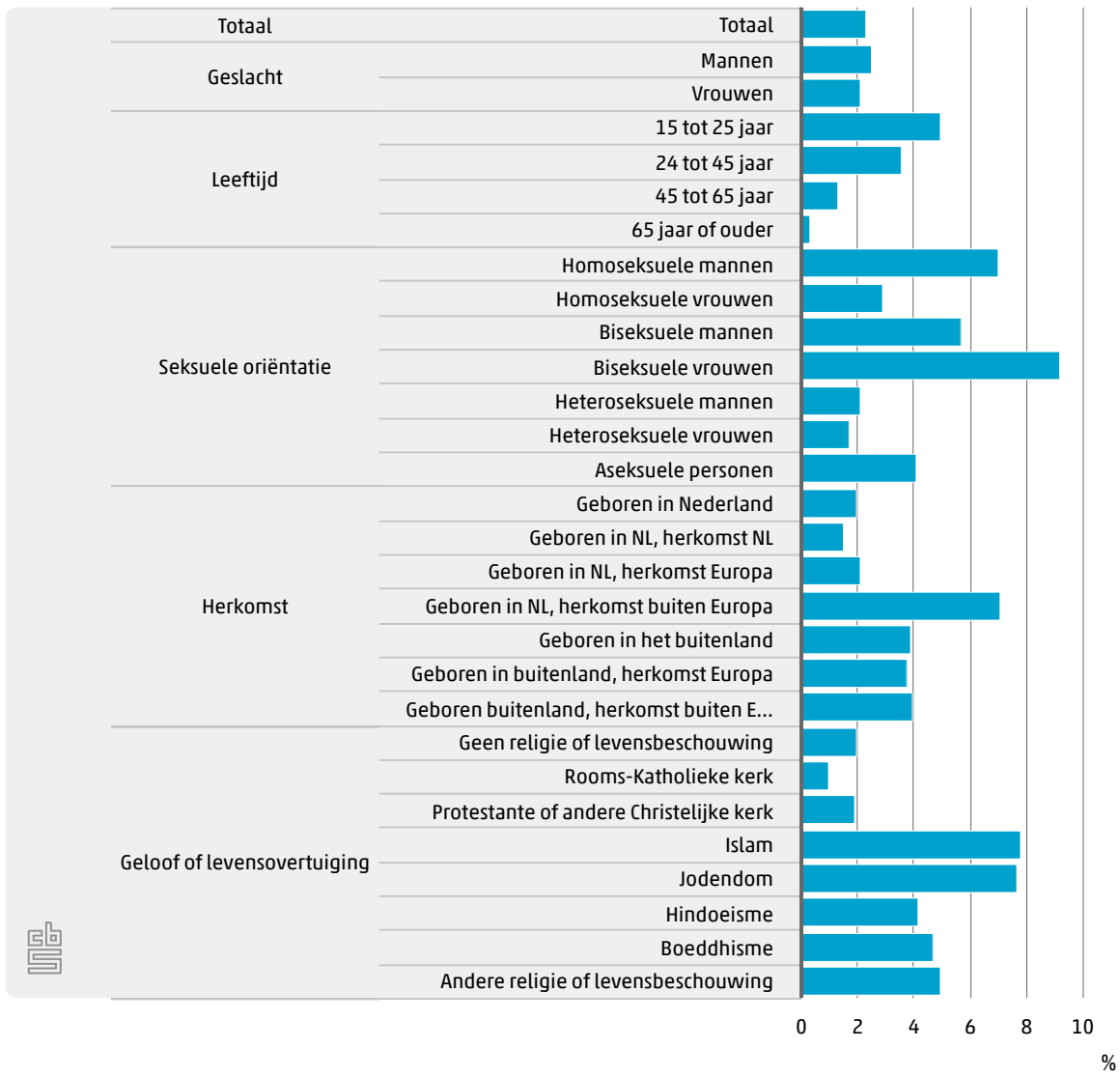
8.1 Ervaren van online discriminatie

In 2022 zei 2 procent van de Nederlanders van 15 jaar of ouder zich in de afgelopen 12 maanden weleens online gediscrimineerd te hebben gevoeld. Dat zijn bijna 340 duizend mensen.
Jongeren van 15 tot 25 jaar gaven dit met 5 procent relatief vaak aan. Biseksuele vrouwen (9 procent) en homoseksuele mannen (7 procent) hadden er vaker mee te maken dan personen met een andere seksuele oriëntatie.

Personen geboren in Nederland met herkomst buiten Europa (tweede generatie) ervoeren met 7 procent het vaakst online discriminatie[17)]. Personen geboren in het buitenland voelden zich met 4 procent vaker gediscrimineerd dan personen geboren in Nederland (2 procent). Deze verschillen blijven bestaan na correctie voor geslacht, leeftijd en opleidingsniveau. Wat godsdienst of levensbeschouwing betreft voelde 8 procent van de islamieten en 8 procent van de joden zich online gediscrimineerd. Rooms-katholieken voelden zich het minst online gediscrimineerd (1 procent).

Personen uit huishoudens met de laagste inkomens werden vaker met online discriminatie geconfronteerd dan personen uit huishoudens met hogere inkomens (zie tabellenset).

8.1.1 Online discriminatie naar persoonskenmerken, 2022



Tegen wie is online discriminatie gericht?

Discriminatie kan tegen de persoon zelf gericht zijn of tegen de groep waartoe men zich rekent. In 2022 gaf 28 procent van de Nederlanders die zich online gediscrimineerd voelden aan dat dit tegen hen persoonlijk gericht was. Meer dan twee derde (69 procent) zei dat de online discriminatie tegen de groep waartoe zij zichzelf rekenen gericht was.

Bekendheid dader(s)

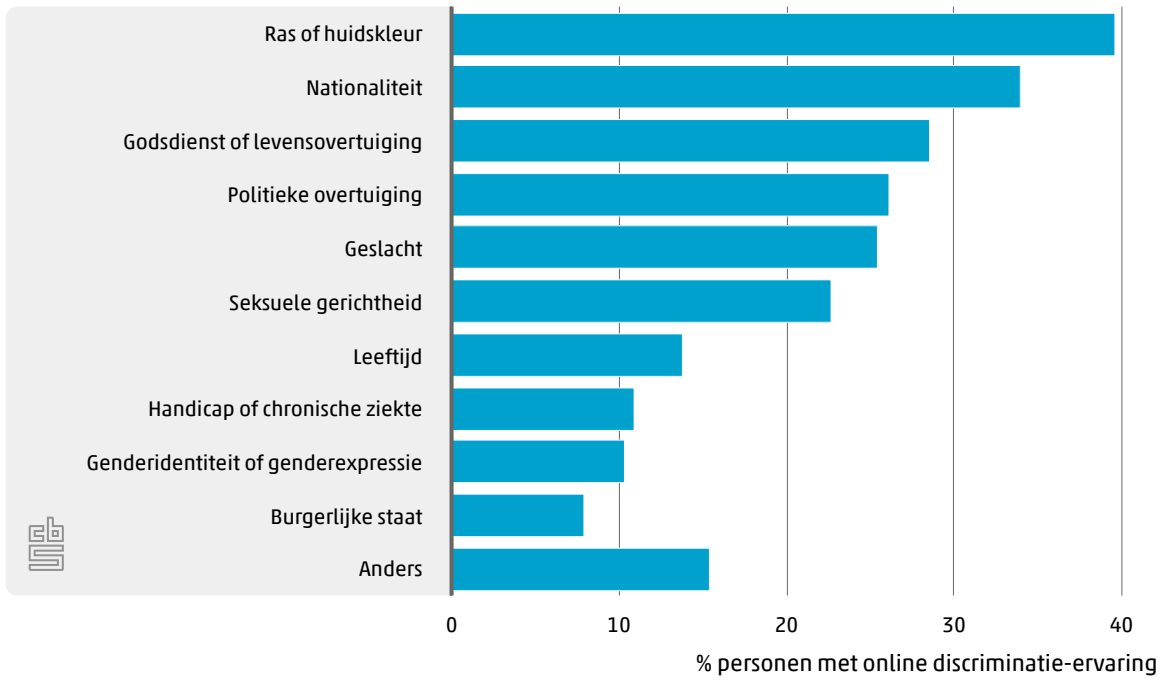
Op de vraag of men de dader of daders kende, zei 23 procent de dader(s) te kennen. 69 procent kende de dader(s) niet en 8 procent gaf geen antwoord.

8.2 Gronden, manieren en plaats van online discriminatie

Discriminatiegronden

Van degenen die in 2022 online discriminatie ervoeren ging het bij 40 procent om discriminatie op grond van ras of huidskleur, gevolgd door discriminatie op grond van nationaliteit (34 procent) en godsdienst of levensbeschouwing (29 procent). Ongeveer een kwart noemde politieke overtuiging, geslacht of seksuele gerichtheid als grond. De andere discriminatiegronden (leeftijd, handicap, genderidentiteit en burgerlijke staat) werden minder vaak genoemd.

8.2.1 Gronden voor online discriminatie[1)], 2022



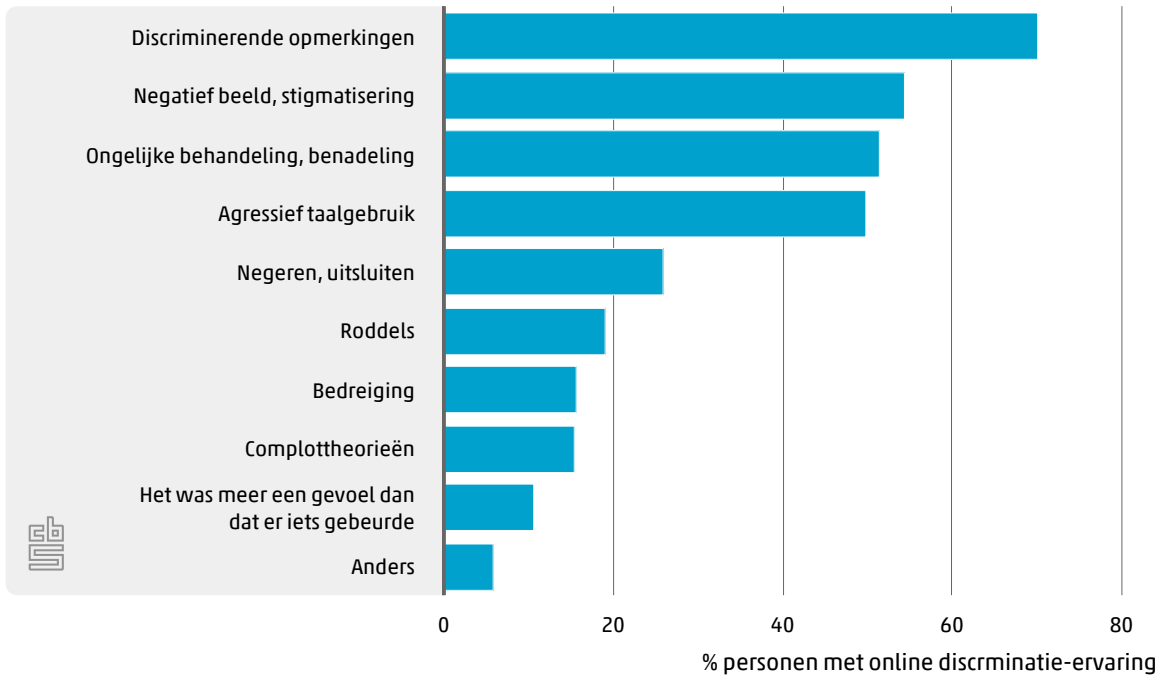
[1)] Meerdere antwoorden mogelijk.

Discriminatiegronden verschillen tussen bevolkingsgroepen. Discriminatie op grond van ras of huidskleur werd met 71 procent vaker gerapporteerd door personen met herkomst buiten Europa dan door personen met herkomst binnen Europa (20 procent) en met herkomst Nederland (19 procent). Ook godsdienst of levensovertuiging is onderscheidend: dit werd door 77 procent van de islamieten als grond gerapporteerd, terwijl bijvoorbeeld 42 procent van de protestanten en 9 procent van de katholieken deze discriminatiegrond noemden. Vrouwen voelden zich op grond van geslacht twee keer zo vaak gediscrimineerd als mannen: 35 tegen 17 procent.

Manieren van discriminatie

7 op de 10 personen die discriminatie ervoeren, gaven aan dat dit kwam door discriminerende opmerkingen. Grofweg 5 op de 10 zeiden dat dit kwam door een negatief beeld/stigmatisering, door ongelijke behandeling/benadeling/voortrekken van bepaalde groepen, of door agressief taalgebruik. Andere manieren van discriminatie zoals negeren/uitsluiten, roddels of bedreiging werden minder vaak genoemd.

8.2.2 Manier van online discriminatie[1)], 2022

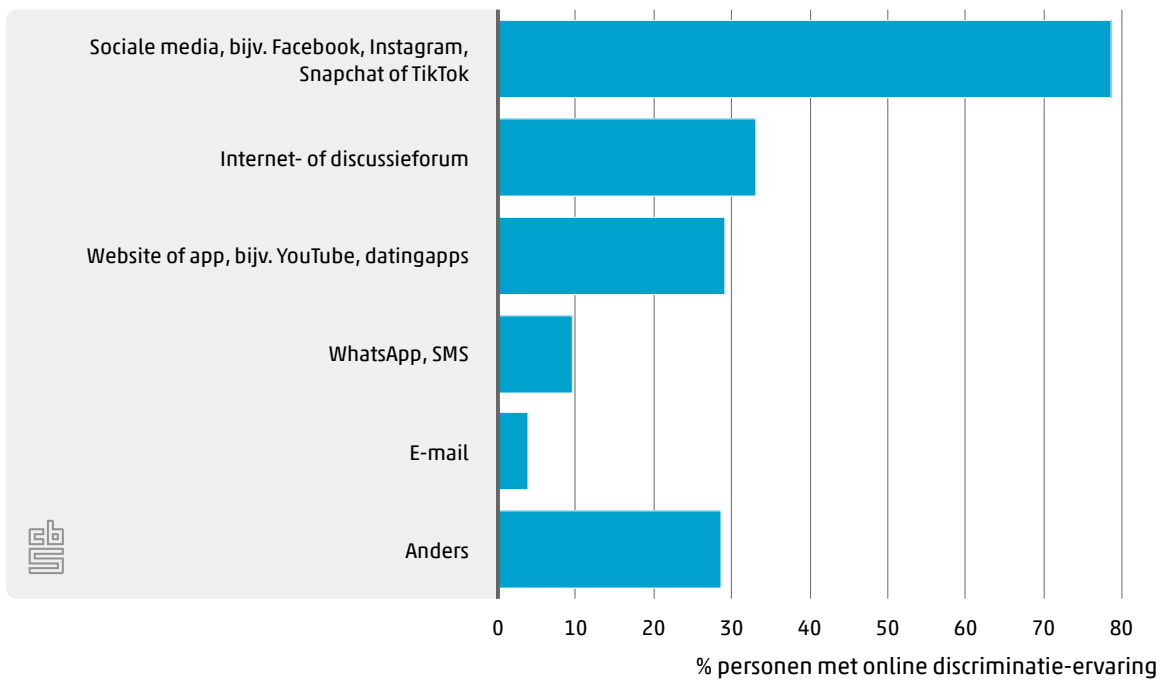


[1)] Meerdere antwoorden mogelijk.

Waar werd online discriminatie ervaren?

De meesten (bijna 80 procent) zeiden zich op sociale media zoals Facebook, Instagram, Snapchat of TikTok gediscrimineerd te hebben gevoeld. Op internet- of discussiefora en op websites of apps ervoer ongeveer 30 procent discriminatie, en 10 procent maakte dit via WhatsApp of SMS mee.

8.2.3 Waar online discriminatie ervaren[1)], 2022



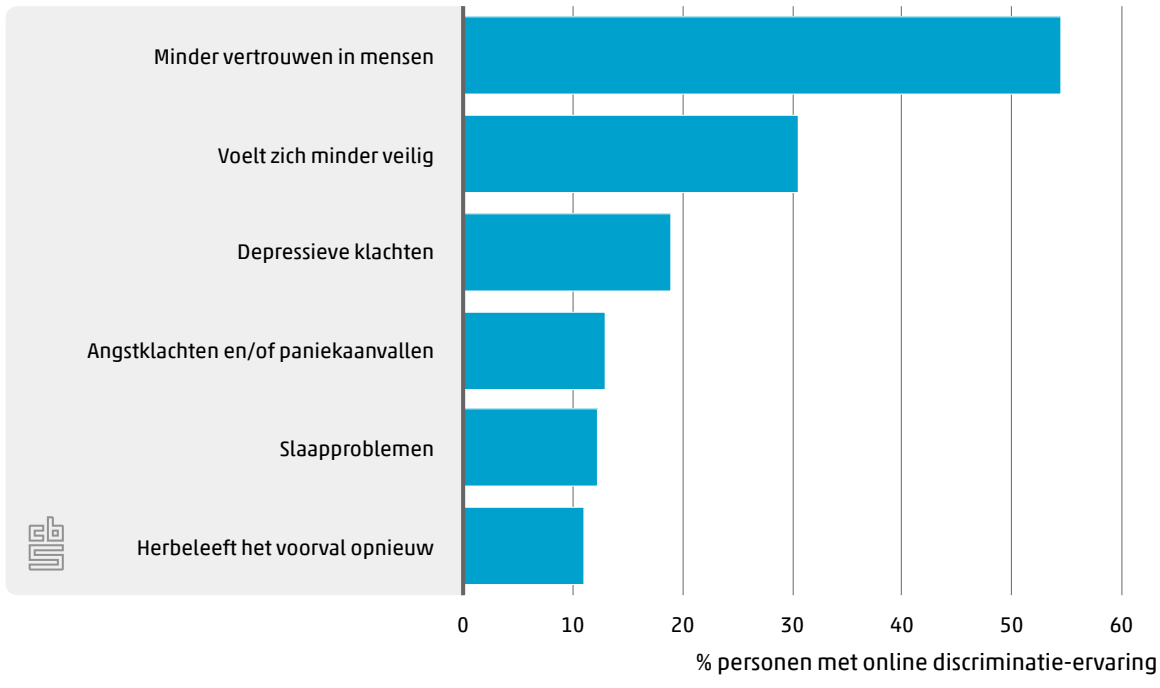
[1)] Meerdere antwoorden mogelijk.

8.3 Gevolgen online discriminatie

Ruim een derde van de personen die die online discriminatie ervoeren zei problemen te hebben of te hebben gehad als gevolg van het voorval (zie tabellenset). Verreweg de meesten hebben/hadden emotionele of psychische problemen (32 procent); 5 procent gaf aan er financiële problemen door te hebben (gehad).

Als het gaat om emotionele of psychische gevolgen gaf meer dan de helft (55 procent) van degenen die online discriminatie ervoeren aan dat ze daardoor minder vertrouwen in mensen hebben. Iets meer dan 30 procent voelt/voelde zich minder veilig en 20 procent heeft/had depressieve klachten. Angstklachten en/of paniekaanvallen, slaapproblemen en het voorval telkens opnieuw beleven werden door ruim 1 op de 10 genoemd.

8.3.1 Gevolgen online discriminatie[1)], 2022

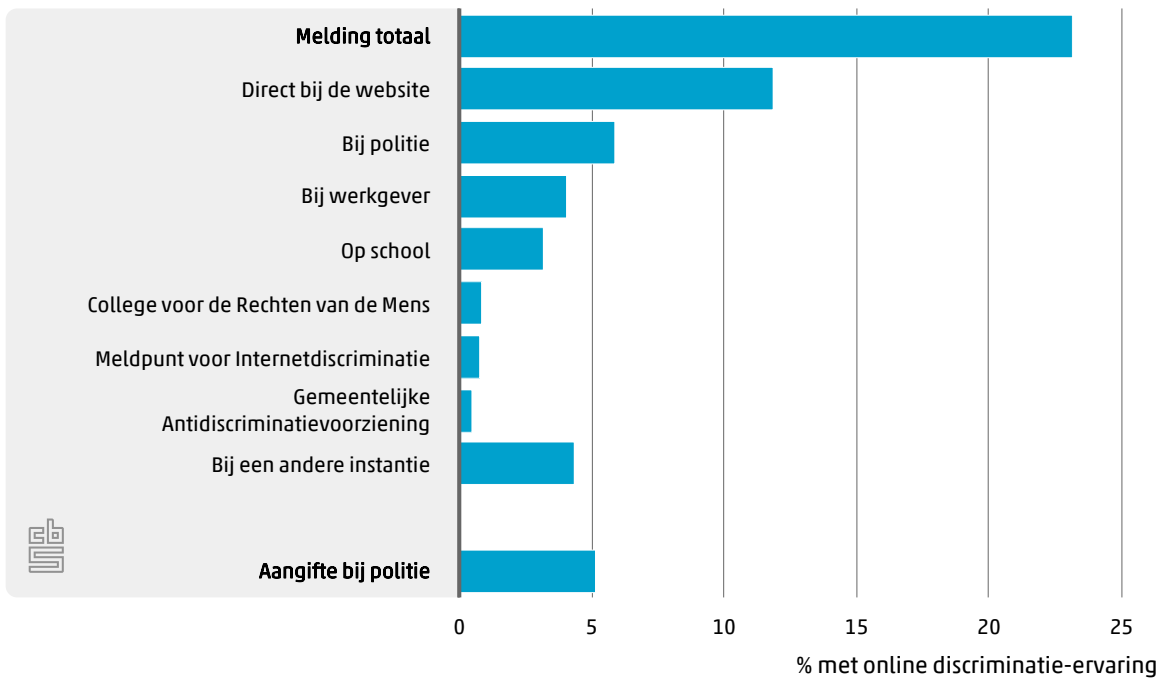


[1)] Meerdere antwoorden mogelijk.

8.4 Melding en aangifte online discriminatie

Bijna een kwart (23 procent) van de mensen die zich in de afgelopen 12 maanden online gediscrimineerd voelden, heeft dit ergens gemeld. De meesten meldden het direct bij de website (12 procent); 6 procent meldde het bij de politie, 4 procent op het werk (bijvoorbeeld bij de leidinggevende of vertrouwenspersoon) en 3 procent op school (bijvoorbeeld bij een leerkracht of vertrouwenspersoon). Bij het Meldpunt voor Internetdiscriminatie (MiND), bij het College voor de Rechten van de Mens of bij een gemeentelijke antidiscriminatievoorziening (ADV) maakte minder dan 1 procent van de mensen die online discriminatie ervoeren melding. 5 procent van degenen die online discriminatie ervoeren, deden hiervan aangifte bij de politie.

8.4.1 Melding en aangifte online discriminatie[1)], 2022

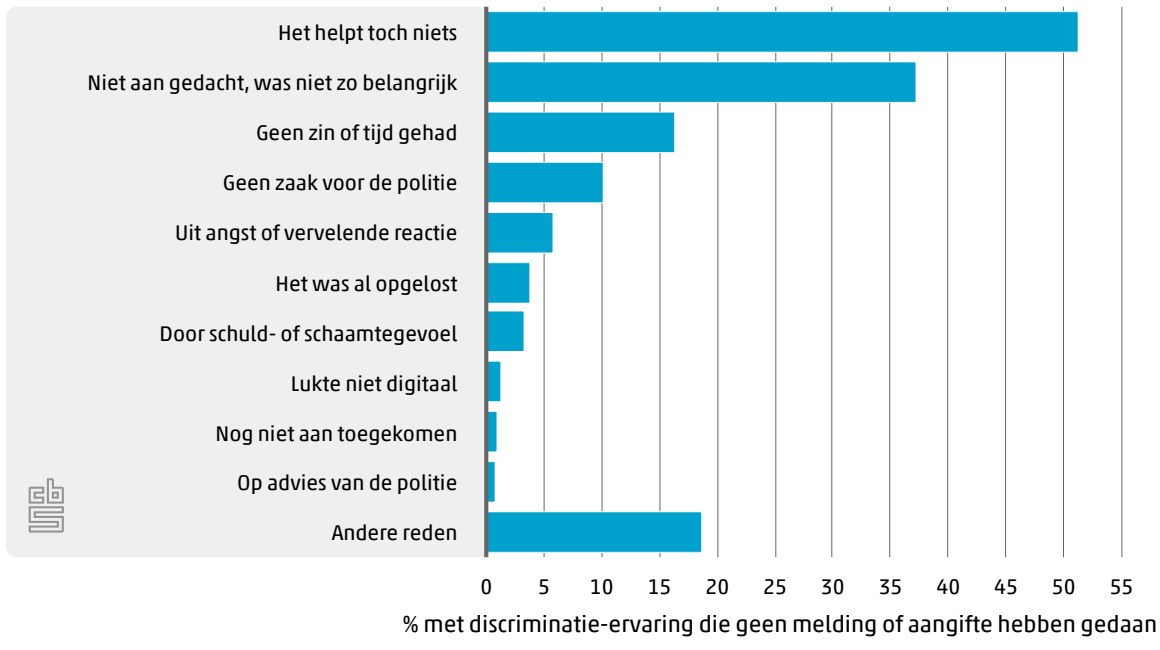


[1)] Meerdere antwoorden mogelijk.

Redenen geen melding of aangifte bij politie

De meest genoemde reden om geen melding of aangifte bij de politie te doen is dat het toch niets helpt (51 procent), gevolgd door dat er niet aan is gedacht/dat het niet zo belangrijk was (37 procent). Ongeveer 15 procent heeft geen zin of tijd gehad en 10 procent zei dat het geen zaak van de politie was. De andere in het onderzoek voorgelegde redenen worden door minder dan 6 procent genoemd.

8.4.2 Reden geen melding of aangifte bij politie van online discriminatie[1)], 2022



[1)] Meerdere antwoorden mogelijk.

[17)] Na correctie voor geslacht, leeftijd en opleiding is dit 6 procent.

9. Online oproepen tot openbare-ordeverstoring

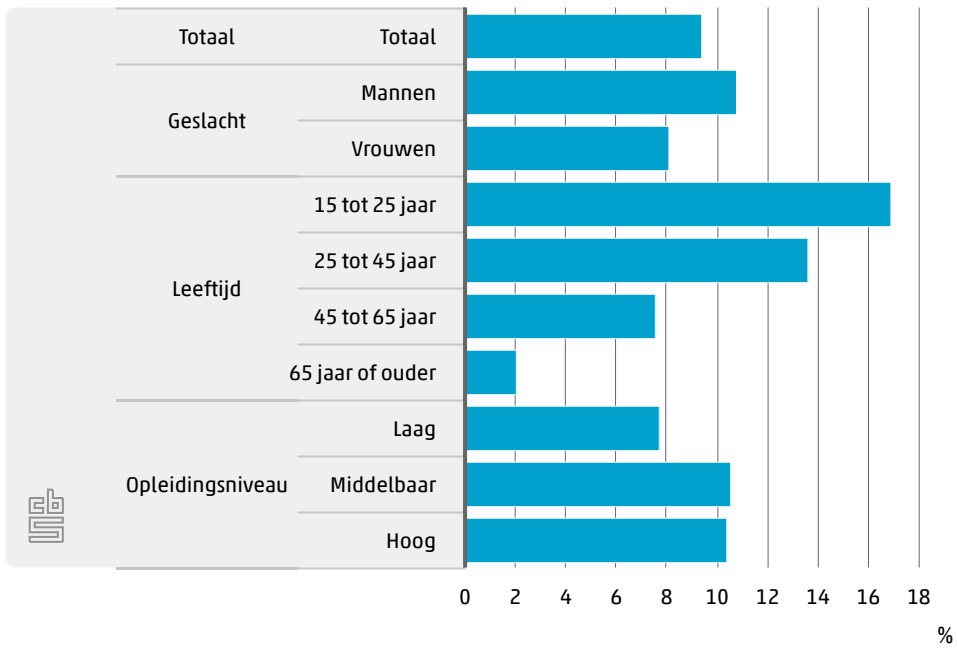
Internet wordt ook gebruikt om oproepen te doen om de openbare orde te verstoren. Denk aan de oproepen bij de avondklokrellen in de coronapandemie en bij de boerenprotesten. Hoe vaak komen Nederlanders dit soort oproepen op internet tegen? Om wat voor soort oproepen gaat het? En ervaren ze er zelf overlast van in de eigen woonomgeving. Deze vragen worden in dit hoofdstuk beantwoord.

9.1 Prevalentie online oproepen openbare-ordeverstoring in algemeen

In 2022 gaf 9 procent van de Nederlanders aan in de afgelopen 12 maanden weleens online berichten, bijvoorbeeld via sociale media of in app-groepen, gezien te hebben waarin opgeroepen werd tot openbare-ordeverstoring of activiteiten die vaak daartoe leiden, zoals demonstraties, rellen of illegale feesten. Dat zijn 1,4 miljoen mensen.

Jongeren in de leeftijd van 15 tot 25 jaar zagen met 17 procent het vaakst weleens online berichten tot openbare-ordeverstoring, met name jongvolwassenen (19 procent; zie ook tabellenset). 65-plussers kwamen dergelijke oproepen het minst vaak tegen. Mannen zeiden vaker online berichten gezien te hebben dan vrouwen. Middelbaar opgeleiden en hoogopgeleiden zagen dit soort berichten vaker dan laagopgeleiden.

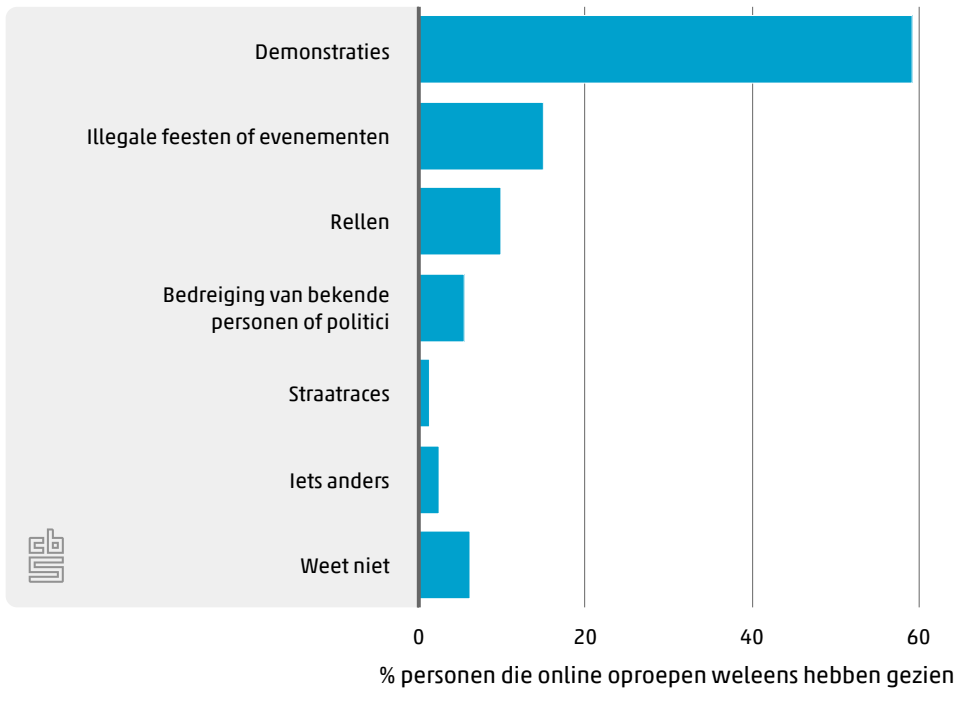
9.1.1 Berichten van online oproepen tot openbare ordeverstoring gezien naar persoonskenmerken, 2022



Soort openbare-ordeverstoring: waartoe werd opgeroepen?

Verreweg de meesten die berichten zagen waarin werd opgeroepen tot openbare-ordeverstoring, gaven aan dat het (laatste) bericht ging om een oproep tot demonstratie (59 procent). Berichten die oproepen tot illegale feesten of evenementen werden door 15 procent genoemd en oproepen tot rellen door 10 procent. 6 procent zei dat het bericht opriep tot het bedreigen van bekende personen of politici. 1 procent zei dat het om oproepen tot straatraces ging. 3 procent noemde berichten met een andere inhoud, waaronder oproepen tot burgerlijke ongehoorzaamheid, ageren tegen politiek beleid, boycotten van producten, pesterijen, niet laten vaccineren, onwaarheden of complottheorieën verspreiden, of onrust veroorzaken bij de werkgever.

9.1.2 Soort openbare ordeverstoring waartoe werd opgeroepen, 2022



Actie na zien oproep tot openbare-ordeverstoring

Het leeuwendeel (85 procent) gaf aan niets met het bericht dat oproept tot openbare-ordeverstoring te hebben gedaan. 5 procent meldde het bij de politie. 3 procent zei te hebben deelgenomen aan de activiteit waartoe werd opgeroepen, met name aan illegale feesten of evenementen, en aan straatraces. 2 procent deelde het bericht online.

9.2 Prevalentie openbare-ordeverstoring in de buurt

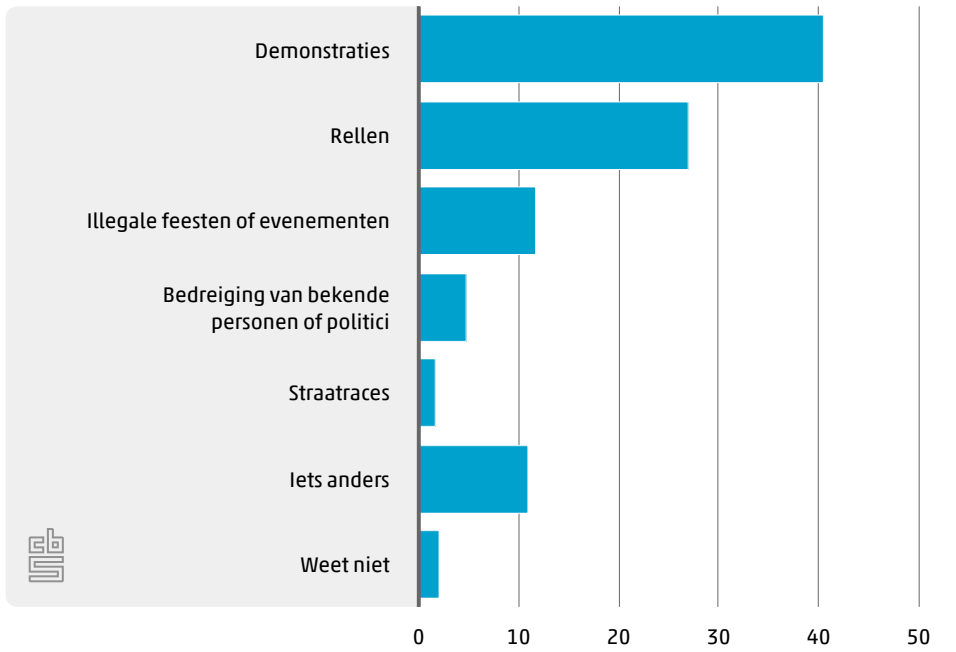
In 2022 gaf 5 procent van de Nederlanders aan dat er in de afgelopen 12 maanden in hun eigen buurt weleens een evenement heeft plaatsgevonden waarbij de openbare orde werd verstoord.

Openbare-ordeverstoring in de eigen buurt vindt in de stad vaker plaats dan op het platteland. Zo maakte 7 procent van de inwoners van zeer sterk stedelijke gemeenten dit mee, tegen 3 procent van de inwoners van niet-stedelijke gemeenten. In de G4, de vier grote steden samen, werd dit door 9 procent van de bewoners meegemaakt.

Soort openbare ordeverstoring in de buurt

De meesten (41 procent) zeiden dat het bij de openbare-ordeverstoring in eigen buurt ging om demonstraties. Daarna volgden rellen (27 procent), illegale feesten of evenementen (12 procent), straatraces (5 procent) en bedreiging van bekende personen of politie (2 procent). Ruim 10 procent noemde iets anders, bijvoorbeeld bedreiging en vernieling, hangjongeren, boerenprotesten/blokkades door boeren met trekkers, brandstichting, corona-ongeregeldheden en lockdownprotesten, samenscholingen tijdens corona, ordeverstoring vanwege vuurwerkverbod/illegaal vuurwerk afsteken, oudejaarsongeregeldheden, of feestjes waar mensen kwamen die niet welkom waren.

9.2.1 Soort openbare-ordeverstoring in buurt, 2022

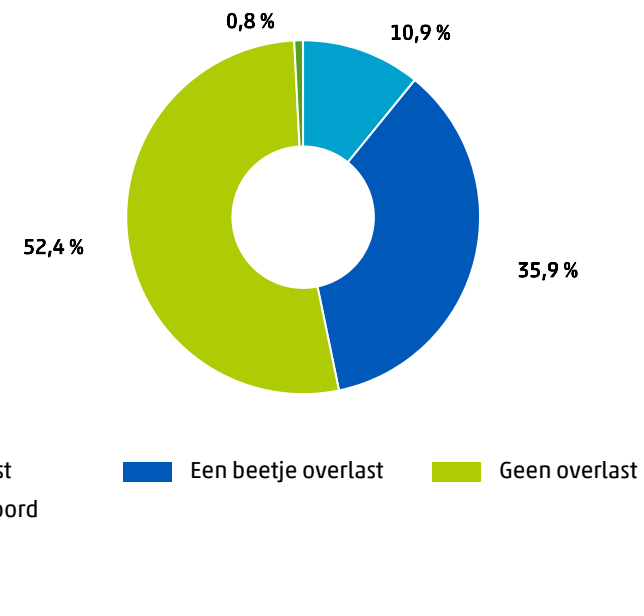


Overlast van openbare-ordeverstoring in de buurt

Van de mensen die aangaven dat openbare-ordeverstoring in de eigen buurt in de afgelopen 12 maanden weleens is voorgekomen, zei 11 procent hier zelf veel overlast van te hebben ervaren. 36 procent ervoer een beetje overlast. Ruim de helft (52 procent) had er zelf geen overlast van.

Wanneer het ervaren van overlast wordt berekend voor de totale populatie, dus alle Nederlanders van 15 jaar of ouder, geeft 0,6 procent aan zelf veel overlast te hebben ervaren van verstoring van de openbare orde in de eigen buurt.

9.2.2 Overlast ervaren van openbare-ordeverstoring in buurt[1)], 2022

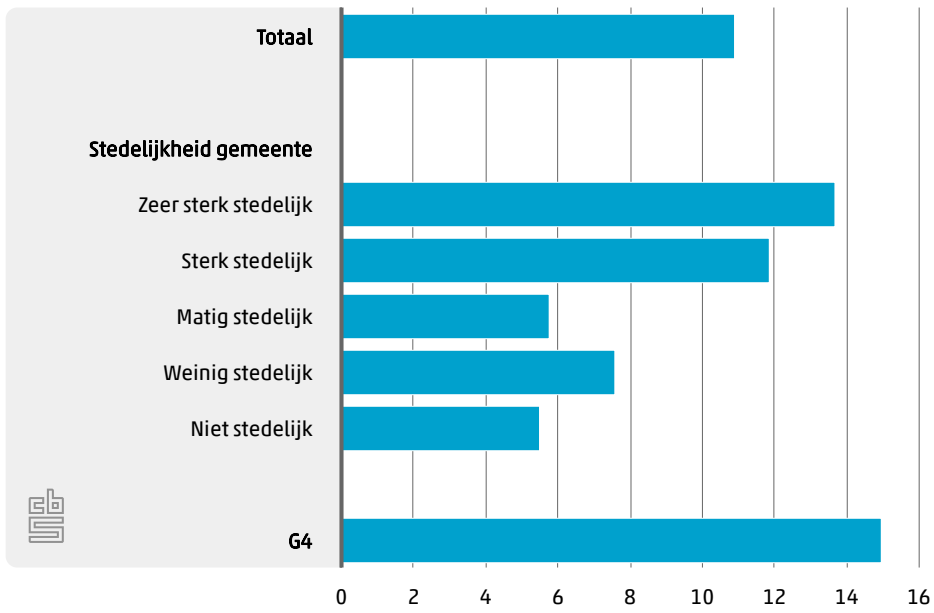


[1)] De percentages hebben betrekking op de personen die zeggen dat openbare-ordeverstoring in de eigen buurt in de afgelopen 12 maanden weleens is voorgekomen.

Overlast van openbare-ordeverstoring in de buurt naar stedelijkheid en G4

Inwoners van zeer sterk stedelijke gemeenten en sterk stedelijke gemeenten die openbare-ordeverstoring meemaakten ervoeren met respectievelijk 14 en 12 procent daar vaker veel overlast van dan inwoners van minder stedelijke gemeenten (grofweg 6 procent). In de G4 zei 15 procent van de inwoners die weleens openbare-ordeverstoring in de buurt hebben gezien, dat ze hier veel overlast van hebben ervaren.

9.2.3 Veel overlast ervaren van openbare-ordeverstoring in buurt naar stedelijkheid gemeente en G4, 2022



10. Conclusies en aanbevelingen

Dit afsluitende hoofdstuk bevat de belangrijkste conclusies van Online Veiligheid en Criminaliteit 2022 en een aantal aanbevelingen voor toekomstig onderzoek.

10.1 Conclusies

Meer dan 9 op de 10 Nederlanders nemen maatregelen om hun persoonlijke gegevens op internet te beschermen

In 2022 gaf 95 procent van de Nederlanders aan persoonlijke gegevens op internet te beschermen. Van de acht in het onderzoek voorgelegde beschermingsmaatregelen (waaronder bijvoorbeeld het beperken van de toegang tot profielgegevens, het controleren van de veiligheid van websites en het blokkeren van cookies) heeft (afgerond) 60 procent van de Nederlanders 5 of meer maatregelen genomen, 25 procent 3 of 4 maatregelen, en 11 procent 1 of 2.

Begrippen spam, hacken, ID-fraude en back-ups maken het meest bekend, ransomware en vooral social engineering het minst

Ongeveer 9 op de 10 Nederlanders hebben niet alleen van de begrippen spam, hacken, identiteitsfraude en back-ups maken gehoord, maar ze geven ook aan te weten wat het is. 80 procent weet wat phishing is en bijna 80 procent weet wat met WhatsApp-fraude wordt bedoeld. Minder dan de helft weet wat ransomware is, en minder dan een kwart wat social engineering is.

Ruim een kwart Nederlanders maakt zich zorgen over misbruik van bankgegevens en persoonsgegevens

De meeste zorgen als het gaat om internetveiligheid hebben Nederlanders over misbruik van bankgegevens en misbruik van persoonsgegevens: ruim een kwart maakt zich veel zorgen over elk van deze veiligheidsaspecten. Over zowel het misbruik van accounts als over het hacken van een apparaat of account maakt ongeveer 20 procent zich veel zorgen. Het laagst is de bezorgdheid om online gediscrimineerd te worden: 8 procent maakt zich hierover veel zorgen.

Vergrendeling apparaten en accounts door toegangscodes/wachtwoorden meest gebruikte beveiligingsmaatregel, gebruik lange wachtwoorden de minst gebruikte

Acht op tien Nederlanders vergrendelen hun apparaten of accounts door middel van een toegangscode, wachtwoord, vingerafdruk en/of face-id. Drie kwart controleert bijlages in e-mails vóór het openen ervan. Bijna 6 op de 10 zeggen updates van apparatuur of apps direct of zo snel mogelijk uit te voeren. Het gebruik van tweetrapsverificatie en vooral het gebruik van wachtwoorden van minimaal 16 tekens zijn maatregelen die met respectievelijk 25 en 14 procent het minst vaak worden genomen.

Helft Nederlanders voelt zich veilig op internet, 4 procent voelt zich onveilig

51 procent van de Nederlanders voelt zich veilig of heel veilig als ze internet gebruiken. Ondanks het feit dat ruim een kwart van de Nederlanders zich veel zorgen maakt over zaken als misbruik van gegevens op internet, voelt slechts 4 procent zich onveilig of heel onveilig als ze het internet gebruiken. Het grootste deel (44 procent) van de anderen voelt zich veilig noch onveilig.

Bijna helft heeft behoefte aan voorlichting over bescherming tegen online criminaliteit

Bijna de helft van de Nederlanders heeft behoefte aan meer informatie over beschermende maatregelen die zij zelf kunnen nemen. Bijna 4 op de 10 hebben behoefte aan meer informatie over hoe oplichters te werk gaan en waar men op moet letten. Ruim een kwart wil meer informatie over de verschillende vormen van online criminaliteit. Hulp bij het nemen van beschermende maatregelen wordt door 2 op de 10 genoemd.

2,2 miljoen Nederlanders in 2022 slachtoffer van online criminaliteit

In 2022 is 15 procent van de Nederlanders van 15 jaar en ouder naar eigen zeggen slachtoffer geweest van online criminaliteit. Dit zijn 2,2 miljoen mensen. De meesten, 8 procent, werden slachtoffer van oplichting en fraude, vooral van aankoopfraude. 5 procent heeft te maken gehad met hacken en 4 procent met bedreiging en intimidatie. Een half procent werd slachtoffer van andere online delicten.

Jongeren, en vooral jonge vrouwen vaak slachtoffer van online criminaliteit

Een op de vijf jongeren van 15 tot 25 jaar werd in 2022 slachtoffer van online criminaliteit, jonge vrouwen (23 procent) iets vaker dan jonge mannen (19 procent). Vooral bij het slachtofferschap van online bedreiging en intimidatie is er een groot verschil tussen jongeren en oudere leeftijdsgroepen. Biseksuele vrouwen en aseksuelen hadden vaker met online criminaliteit te maken dan anderen. Dit komt door hun hoge slachtofferschap van online bedreiging en intimidatie.

Ruim 4 op de 10 slachtoffers van online bedreiging en intimidatie kent de dader

44 procent van de slachtoffers van online bedreiging en intimidatie kende de dader. Bij pesten en stalken was dit het vaakst het geval. De meest genoemde daders van online bedreiging en intimidatie zijn de ex-partner, een vriend/vriendin of een medestudent/-scholier. De ex-partner wordt bij online stalken en shamesexting het vaakst als dader genoemd, respectievelijk door 18 en 14 procent van de slachtoffers. Bij online pesten, waarvan jongeren het vaakst slachtoffer zijn, wordt een medestudent/-scholier (15 procent) of een vriend/vriendin (12 procent) het vaakst als dader genoemd.

3 op de 10 slachtoffers van online criminaliteit voelen zich minder veilig

Voor 37 procent van de slachtoffers van online criminaliteit heeft of had het voorval tot gevolg dat men minder vertrouwen in mensen heeft en voor 30 procent dat men zich minder veilig voelt of voelde. Slaapproblemen, depressieve klachten, angstklachten en het voorval steeds opnieuw beleven werden elk door 7 á 8 procent van de slachtoffers genoemd. Deze laatste klachten worden door slachtoffers van online bedreiging en intimidatie meer dan dubbel zo vaak gerapporteerd als door slachtoffers van de andere online delicten.

2 op de 10 slachtoffers van online criminaliteit doen melding en aangifte bij de politie

21 procent van de slachtoffers van online criminaliteit hebben bij de politie gemeld wat hen overkomen is, en bijna 5 op de 10 hebben dit bij een andere instantie of persoon gedaan. Bijna alle meldingen van online criminaliteit bij de politie resulteerden in een aangifte (19 procent deed aangifte). De meest genoemde reden om het voorval niet bij de politie te melden of aangifte te doen is dat er niet aan wordt gedacht of dat men het niet zo belangrijk vindt, gevolgd door ‘het helpt toch niets’.

340 duizend Nederlanders voelden zich in 2022 online gediscrimineerd

2 procent van de Nederlanders voelden zich in 2022 weleens online gediscrimineerd. Dat zijn bijna 340 duizend mensen. Van degenen die online discriminatie ervoeren ging het bij 40 procent om discriminatie op grond van ras of huidskleur, gevolgd door discriminatie op grond van nationaliteit (34 procent) en godsdienst of levensbeschouwing (29 procent). Het gaat vooral om discriminerende opmerking (genoemd door 70 procent), gevolgd door stigmatisering, ongelijke behandeling, en agressief taalgebruik (elk door ongeveer de helft genoemd). De meesten (bijna 80 procent) zeiden zich op sociale media zoals Facebook, Instagram, Snapchat of TikTok gediscrimineerd te hebben gevoeld. Meer dan de helft van degenen die online discriminatie ervoeren zeggen dat zij daardoor minder vertrouwen in mensen hebben. Iets meer dan 30 procent voelt/voelde zich minder veilig en 20 procent heeft/had depressieve klachten. Bijna een kwart van de mensen die zich in de afgelopen 12 maanden online gediscrimineerd voelden, heeft dit ergens gemeld.

1,4 miljoen Nederlanders zagen in 2022 online oproepen tot openbare-ordeverstoring

In 2022 zei 9 procent van de Nederlanders in de afgelopen 12 maanden weleens online berichten, bijvoorbeeld via sociale media of in app-groepen gezien te hebben waarin opgeroepen werd tot openbare-ordeverstoring of bijeenkomsten die dit tot gevolg kunnen hebben, bijvoorbeeld rellen, demonstraties, illegale feesten of straatraces. Dat zijn 1,4 miljoen mensen. Verreweg de meesten die deze berichten zagen, zeiden dat het ging om een oproep tot demonstratie (59 procent). Berichten die oproepen tot illegale feesten of evenementen werden door 15 procent genoemd en oproepen tot rellen door 10 procent.

760 duizend Nederlanders maakten ordeverstorende evenementen in eigen buurt mee

In 2022 gaf 5 procent van de Nederlanders aan dat er in de afgelopen 12 maanden in hun eigen buurt weleens een bijeenkomst heeft plaatsgevonden waarbij de openbare orde werd verstoord. Dat zijn 760 duizend mensen. De meesten (41 procent) zeiden dat het ging om demonstraties. Daarna volgden rellen (27 procent), illegale feesten of evenementen (12 procent), straatraces (5 procent) en bedreiging van bekende personen of politie (2 procent). Openbare-ordeverstoring in de buurt vindt in de stad vaker plaats dan op het platteland. Van de mensen die openbare-ordeverstoring in de eigen buurt ervoeren, zei 1 op de 10 hier zelf veel overlast van te hebben ervaren.

10.2 Aanbevelingen voor toekomstig onderzoek

Onderzoek naar mogelijkheid jaarcijfers online criminaliteit

Criminelen zijn steeds op zoek naar nieuwe manieren om mensen online op te lichten, computers te hacken en mensen te bedreigen of te intimideren. Burgers, bedrijven en overheid proberen zich steeds beter hiertegen te beschermen. Dit betekent dat het terrein van online veiligheid en criminaliteit permanent in beweging is en zich steeds nieuwe vormen van online criminaliteit en nieuwe middelen om zich daartegen te beschermen ontwikkelen. Het is daarom wenselijk de ontwikkeling van Online Veiligheid en Criminaliteit jaarlijks te monitoren: van OVeC naar MOVeC (= *Monitor* Online Veiligheid en Criminaliteit) dus. Dit kan door dit onderzoek Online Veiligheid en Criminaliteit in de even jaren, afwisselend met de Veiligheidsmonitor in de oneven jaren, te herhalen. In 2024 zou dan dus een tweede onderzoek plaatsvinden.

De cijfers van de Veiligheidsmonitor en dit onderzoek Online Veiligheid en Criminaliteit zijn door (context-)verschillen van de vraagstellingen en mogelijke selectieverschillen niet zonder meer vergelijkbaar (zie paragraaf 7.1 en de Onderzoeksverantwoording). Om inzicht te krijgen of, en in welke mate, deze verschillen effect hebben op de onderzoeksresultaten – en dus in hoeverre de jaarlijkse metingen door twee onderzoeken een betrouwbare trend weergeven - zouden beide onderzoeken eenmalig tegelijk gehouden moeten worden (met de Veiligheidsmonitor in beperkte omvang). Door dit 'dubbeldraaien' is het mogelijk om vast te stellen in hoeverre de cijfers van beide onderzoeken bij het meten van de prevalentie van dezelfde delicten verschillen. Op basis daarvan kunnen omrekenfactoren worden berekend waardoor de cijfers vergelijkbaar zijn en daarmee jaarcijfers beschikbaar komen. Dit is een beproefde methodiek die bij de Veiligheidsmonitor al meerdere keren is toegepast (Van den Brakel, 2021).

Separate publicatie over financiële schade online criminaliteit

In de Veiligheidsmonitor 2021 is voor het eerst aan slachtoffers van traditionele en online vermogenscriminaliteit gevraagd welke financiële schade ze zelf hierdoor hebben geleden en welk deel door financiële instellingen zoals banken en verzekeraars vergoed is. Als het gaat om online criminaliteit bedroeg het totale schadebedrag in 2021 afgerond 680 miljoen euro. Hierover is in september 2022 separaat gepubliceerd (Reep, 2022) (zie ook paragraaf 7.2). Aanbevolen wordt, indien mogelijk, ook op basis van de data van Online Veiligheid en Criminaliteit een vervolg-publicatie uit te brengen waar de financiële schade van online criminaliteit tegen burgers ook voor het jaar 2022 in beeld wordt gebracht.

Aanpassing van de OVeC-vragenlijst

Bij de analyse van de data van OVeC 2022 en de totstandkoming van deze publicatie zijn een aantal vragen naar boven gekomen waarvan het de moeite waard zou zijn om deze – bij herhaling van OVeC in 2024 en volgende jaren – te onderzoeken. Een voorbeeld is om niet alleen, zoals nu gebeurd is, aan slachtoffers van hacken te vragen of ze voorafgaand aan het voorval al beveiligingsmaatregelen hadden getroffen, maar om dit ook voor een aantal vormen van online oplichting en fraude te vragen. Een ander voorbeeld is om bij openbare-ordeverstoring niet alleen te vragen in hoeverre men zelf in de eigen buurt overlast van heeft ervaren van ordeverstorende bijeenkomsten of evenementen, maar ook daarbuiten. Herhaling van OVeC in 2024 zou ook de gelegenheid bieden om met de vragenlijst in te spelen op nieuwe, nu nog niet te voorziene fenomenen op het gebied van online veiligheid en criminaliteit. Denk bij internetveiligheid bijvoorbeeld aan nieuwe maatregelen om apparaten of accounts te beveiligen, en bij online criminaliteit aan nieuwe manieren die criminelen weten te vinden om hun misdrijven te plegen.

Bijlage A. Tabellen

Deze bijlage bevat de tabellen met de kerncijfers van de in deze publicatie beschreven onderwerpen, geordend volgens de nummering van de betreffende hoofdstukken.

2. Internetgebruik, activiteiten op internet en online aankopen, 2022

	Nederlanders van 15 jaar of ouder
	%
Internetgebruik	
In afgelopen 12 maanden	99,0
Activiteiten op internet[1)]	
E-mailen	93,5
Informatie zoeken, surfen	92,3
Internetbankieren of mobiel bankieren	90,4
Tekstberichten sturen	86,8
Bellen of beeldbellen	78,9
Social media	70,8
Muziek luisteren of downloaden	66,0
Films of series streamen	57,4
Gamen of spelletjes spelen	41,0
Datingsites bezoeken	5,3
Goksites bezoeken	2,8
Andere activiteiten	11,7
Online aankopen	
In afgelopen 12 maanden	86,4

[1)] Het gaat hier om activiteiten op het internet in de afgelopen 12 maanden.

3. Internetveiligheid, 2022

	Nederlanders van 15 jaar of ouder
	%
Online veiligheidsgevoelens	
Voelt zich online (heel) veilig	50,6
Voelt zich online (heel) onveilig	4,3
	schaalscore (0-10)
Bekendheid internetveiligheid[1)]	
Kennis over internetveiligheid	7,7
Beveiligingsmaatregelen[2)]	
Beveiligingsmaatregelen genomen	6,6

[1)] De schaalscoerscore is bepaald op basis van 12 kennisitems over internetveiligheid.

[2)] De schaalscore is bepaald op basis van 10 maatregelen om apparatuur of persoonlijke informatie op internet te beschermen.

4a. Slachtofferschap online oplichting en fraude, 2022

	Nederlanders van 15 jaar of ouder
	%
Slachtoffer in afgelopen 12 maanden	
Online oplichting en fraude	7,6
Aankoopfraude	5,6
Verkoopfraude	1,3
Fraude betalingsverkeer	1,0
Identiteitsfraude	0,5
Phishing	0,7

4b. Informatie over online oplichting en fraude, 2022

	Online oplichting en fraude in afgelopen 12 maanden	Aankoopfraude in afgelopen 12 maanden	Verkoopfraude in afgelopen 12 maanden	Fraude betalingsverkeer in afgelopen 12 maanden	Identiteitsfraude in afgelopen 12 maanden	Phishing in afgelopen 12 maanden
	% slachtoffers	*% slachtoffers*	*% slachtoffers*	*% slachtoffers*	*% slachtoffers*	*% slachtoffers*
Problemen						
Emotionele en/of financiële problemen	23,4	19,8	28,8	31,3	28,3	41,1
Emotionele of psychische problemen	16,7	13,3	17,5	22,9	23,4	33,6
Financiële problemen	11,2	9,0	16,1	18,4	11,7	18,2
Emotionele of psychische gevolgen						
Minder veilig voelen	22,0	17,2	19,3	33,6	34,3	39,5
Minder vertrouwen in mensen	41,7	40,5	38,4	34,2	39,3	50,0
Voorval telkens opnieuw beleven	5,7	3,7	6,5	9,0	9,9	10,1
Slaapproblemen	4,9	3,5	6,5	7,7	8,3	10,3
Angstklachten	3,0	1,5	3,9	6,0	6,8	7,2
Depressieve klachten	4,5	3,2	5,2	7,5	9,4	9,6
Melding						
Melding gedaan totaal	51,5	44,0	45,4	80,5	67,6	62,4
Melding gedaan bij politie	27,2	22,0	28,1	40,3	47,2	45,2
Melding gedaan bij andere instantie	48,0	44,5	34,3	69,2	41,8	40,4
Aangifte						
Aangifte gedaan bij politie	25,9	21,1	26,9	40,2	40,9	44,6

5a. Slachtofferschap hacken, 2022

	Nederlanders van 15 jaar of ouder
	%
Slachtoffer in afgelopen 12 maanden	
Hacken totaal	4,6
Hacken van apparaat	1,9
Hacken van account	3,6

5b. Informatie over hacken, 2022

	Hacken totaal in afgelopen 12 maanden	Hacken apparaat in afgelopen 12 maanden	Hacken account in afgelopen 12 maanden
	% slachtoffers	*% slachtoffers*	*% slachtoffers*
Problemen			
Emotionele en/of financiële problemen	17,5	27,0	14,1
Emotionele of psychische problemen	14,1	20,0	12,0
Financiële problemen	6,0	11,6	3,6
Emotionele of psychische gevolgen			
Minder veilig voelen	37,4	42,2	35,8
Minder vertrouwen in mensen	21,9	28,1	20,3
Voorval telkens opnieuw beleven	2,8	4,5	1,6
Slaapproblemen	4,8	6,4	3,9
Angstklachten	3,7	4,5	3,3
Depressieve klachten	2,8	5,1	2,0
Melding			
Melding gedaan totaal	39,0	34,7	38,9
Melding gedaan bij politie	12,2	18,7	10,0
Melding gedaan bij andere instantie	33,6	23,9	34,6
Aangifte			
Aangifte gedaan bij politie	11,2	16,9	9,3

6a. Slachtofferschap online bedreiging en intimidatie, 2022

	Nederlanders van 15 jaar of ouder
	%
Slachtoffer in afgelopen 12 maanden	
Online bedreiging en intimidatie	4,1
Online bedreiging	1,9
Online pesten	1,3
Online stalken	1,2
Shamesexting	0,7

6b. Informatie over online bedreiging en intimidatie, 2022

	Online bedreiging en intimidatie in afgelopen 12 maanden	Online bedreiging in afgelopen 12 maanden	Online pesten in afgelopen 12 maanden	Online stalken in afgelopen 12 maanden	Shamesexting in afgelopen 12 maanden
	% slachtoffers	*% slachtoffers*	*% slachtoffers*	*% slachtoffers*	*% slachtoffers*
Daders					
Dader was een bekende	44,0	29,2	56,6	55,5	30,4
Problemen					
Emotionele en/of financiële problemen	33,1	26,9	45,7	36,5	37,4
Emotionele of psychische problemen	30,2	24,5	44,3	32,6	30,9
Financiële problemen	6,6	5,5	5,5	8,0	10,4
Emotionele of psychische gevolgen					
Minder veilig voelen	36,7	34,8	36,0	45,6	35,0
Minder vertrouwen in mensen	41,7	40,5	52,6	37,9	34,4
Voorval telkens opnieuw beleven	10,7	7,9	14,1	12,6	11,1
Slaapproblemen	15,4	12,3	20,7	18,7	17,3
Angstklachten	16,9	12,4	25,0	19,6	19,3
Depressieve klachten	16,4	10,1	31,0	16,5	16,5
Melding					
Melding gedaan totaal	56,9	52,8	61,7	58,5	53,9
Melding gedaan bij politie	16,5	15,6	11,9	20,2	25,5
Melding gedaan bij andere instantie	53,3	47,7	59,5	53,1	47,0
Aangifte					
Aangifte gedaan bij politie	13,3	12,7	9,3	15,1	22,1

7a. Slachtofferschap online criminaliteit, 2022

	Nederlanders van 15 jaar of ouder
	%
Slachtoffer in afgelopen 12 maanden	
Online criminaliteit totaal	14,8
Online oplichting en fraude	7,6
Hacken	4,6
Online bedreiging en intimidatie	4,1
Overige online delicten	0,6

7b. Informatie over online criminaliteit totaal, 2022

	Online criminaliteit totaal in afgelopen 12 maanden	Online oplichting en fraude in afgelopen 12 maanden	Hacken in afgelopen 12 maanden	Online bedreiging en intimidatie in afgelopen 12 maanden	Overige online delicten in afgelopen 12 maanden
	% slachtoffers	*% slachtoffers*	*% slachtoffers*	*% slachtoffers*	*% slachtoffers*
Problemen					
Emotionele en/of financiële problemen	24,0	23,4	17,5	33,1	28,9
Emotionele of psychische problemen	19,5	16,7	14,1	30,2	18,8
Financiële problemen	8,5	11,2	6,0	6,6	14,9
Emotionele of psychische gevolgen					
Minder veilig voelen	30,3	22,0	37,4	36,7	28,7
Minder vertrouwen in mensen	36,6	41,7	21,9	41,7	41,7
Voorval telkens opnieuw beleven	6,6	5,7	2,8	10,7	10,2
Slaapproblemen	7,5	4,9	4,8	15,4	6,9
Angstklachten	6,8	3,0	3,7	16,9	6,1
Depressieve klachten	7,2	4,5	2,8	16,4	9,4
Melding					
Melding gedaan totaal	50,8	51,5	39,0	56,9	57,5
Melding gedaan bij politie	20,5	27,2	12,2	16,5	33,7
Melding gedaan bij andere instantie	47,0	48,0	33,6	53,3	36,6
Aangifte					
Aangifte gedaan bij politie	18,6	25,9	11,2	13,3	26,8

8a. Slachtofferschap online discriminatie, 2022

	Nederlanders van 15 jaar of ouder
	%
Slachtoffer in afgelopen 12 maanden	
Online discriminatie	2,3

8b. Informatie over online discriminatie, 2022

	Online discriminatie in afgelopen 12 maanden
	% slachtoffers
Dader	
Dader was een bekende	22,7
Gronden voor discriminatie	
Ras, huidskleur	39,6
Nationaliteit	34,0
Godsdienst of levensovertuiging	28,6
Politieke overtuiging	26,2
Geslacht	25,5
Seksuele gerichtheid	22,7
Leeftijd	13,8
Handicap of chronische ziekte	10,9
Genderidentiteit of genderexpressie	10,4
Burgelijke staat	7,9
Anders	15,4
Manieren van discriminatie	
Discriminerende opmerkingen	70,2
Ongelijke behandeling / benadeling / voortrekken van bepaalde groepen	51,5
Bedreiging	15,7
Agresief taalgebruik	50,0
Negeren / uitsluiting	25,9
Roddels	19,1
Meer een gevoel dan dat er iets gebeurde	10,7
Negatief beeld/ stigmatisering	54,4
Complottheorieën	15,4
Anders	5,9
Problemen	
Emotionele en/of financiële problemen	33,5
Emotionele of psychische problemen	31,6
Financiële problemen	5,1
Emotionele of psychisch gevolgen	
Minder veilig voelen	30,6
Minder vertrouwen in mensen	54,5
Voorval telkens opnieuw beleven	11,0
Slaapproblemen	12,3
Angstklachten	13,0
Depressieve klachten	19,0
Melding	
Melding gedaan totaal	23,2
Melding gedaan bij politie	5,9
Melding gedaan bij andere instantie	21,6
Aangifte	
Aangifte gedaan bij politie	5,2

9. Online openbare-ordeverstoring, 2022

	Nederlanders van 15 jaar of ouder
	%
Online oproep tot openbare ordeverstoring	
Gezien in afgelopen 12 maanden	9,4
Openbare ordeverstoring in de buurt	
Voorgekomen in afgelopen 12 maanden	5,1
Overlast van openbare ordeverstoring in de buurt	
Veel overlast ervaren	10,9

[1)] Percentage gebaseerd op Nederlanders van 15 jaar en ouder die zeggen dat een openbare-ordeverstoring in de eigen buurt in de afgelopen 12 maanden is voorgekomen.

Bijlage B. Onderzoeksverantwoording

In deze onderzoeksverantwoording wordt de opzet en uitvoering van het onderzoek *Online Veiligheid en Criminaliteit 2022* op beknopte wijze beschreven. Achtereenvolgens komen aan de orde:

- Steekproef en respons
- Veldwerk
- Vragenlijst
- Weging
- Betrouwbaarheidsmarges
- Gebruikte analysemethoden
- Schaalscores
- Verschillen met Veiligheidsmonitor en ICT-enquête.

Voor geïnteresseerden zijn separate notities over het steekproefontwerp, veldwerk, en de weging van het onderzoek OVeC 2022 op aanvraag beschikbaar.

Steekproef en respons

Omwille van de vergelijkbaarheid met de Veiligheidsmonitor die ook het slachtofferschap van online criminaliteit meet, is bij het steekproefontwerp van OVeC 2022 zoveel mogelijk aangesloten bij dat van de VM 2021.

De doelpopulatie voor OVeC 2022 bestaat uit alle in Nederland woonachtige personen die 15 jaar of ouder zijn en die deel uitmaken van particuliere huishoudens. De institutionele bevolking, dat zijn personen in inrichtingen, instellingen of tehuizen, behoort niet tot de doelpopulatie en is dus niet benaderd.

Het steekproefontwerp heeft als uitgangspunt dat in totaal 32.500 personen aan het onderzoek meedoen. Dit aantal is bepaald om niet alleen voor de 15-plus bevolking als geheel maar ook voor groepen uit de bevolking betrouwbare uitspraken te kunnen doen. Uitgaande van de verwachte respons van 32,5 procent (was eerder ongeveer de respons op de Veiligheidsmonitor) zijn in totaal 100 duizend personen voor deelname aan het onderzoek benaderd. In totaal hebben 32 861 personen meegedaan, het responspercentage bedroeg daarmee bijna 32,9 procent.

Veldwerk

Het veldwerk vond plaats van 12 augustus t/m 31 oktober 2022. Bij de uitvoering ervan is uitsluitend gebruik gemaakt van internetenquêtering. De steekproefpersonen ontvingen bij aanvang van de veldwerkperiode een aanschrijfbrief met daarin het verzoek om via internet deel te nemen aan het onderzoek, en de bijbehorende inloggegevens. Drie weken na de aanschrijfbrief is aan steekproefpersonen een eerste rappelbrief verstuurd met daarin opnieuw het verzoek om via internet deel te nemen aan het onderzoek. Deze brief is alleen verstuurd aan steekproefpersonen waarvan geen respons is ontvangen. Drie weken daarna is een tweede rappelbrief verstuurd aan de steekproefpersonen die op dat moment de internetvragenlijst nog niet hadden ingevuld. Om de respons te verhogen is er conform CBS-beleid gebruik gemaakt van een incentive (kans om bij deelname een IPad of cadeaubonnen te winnen). De steekproef is uitgezet in drie porties. Dit in verband met risicospreiding, bijvoorbeeld door problemen met de postbezorging en/of servers die niet goed werken.

Vragenlijst

De vragenlijst van OVeC 2022 is door het CBS opgesteld in overleg met het ministerie van J&V. Voor online veiligheid is daarvoor zoveel mogelijk aangesloten bij de vraagstellingen van de ICT-enquête en het pilotonderzoek Digitale Veiligheid en Criminaliteit (Akkermans et al., 2018) en voor online criminaliteit is zoveel mogelijk aangesloten bij de vraagstellingen in de Veiligheidsmonitor 2021[17)].

De vragenlijst is modulair opgebouwd en bevat de volgende vraagblokken:

1. Internetgebruik en -activiteiten
2. Privacy en beveiliging persoonsgegevens
3. Internetveiligheid en veiligheidsbeleving
4. Huidige maatregelen beveiliging

5. Slachtofferschap van online criminaliteit
   5a. Aan- en verkoopfraude
   5b. Hacken
   5c. Online oplichting
   5d. Fraude betalingsverkeer
   5e. Identiteitsfraude
   5f. Interpersoonlijke delicten
6. Online discriminatie
7. Online bedreiging en intimidatie
8. Online oproepen tot openbare ordeverstoring
9. Overige online delicten
10. Maatregelen vóór slachtofferschap hacken
11. Achtergrondkenmerken

Weging

De weging van OVeC 2022 is vergelijkbaar met die van de Veiligheidsmonitor 2021 en houdt rekening met geografische, demografische en sociaaleconomische kenmerken. Het weegmodel is gebaseerd op het weegmodel van de VM 2021.

Betrouwbaarheidsmarges

Bij elk gegeven uit OVeC 2022 is de betrouwbaarheidsmarge (aangegeven met een boven- en ondergrens) bepaald. Deze betrouwbaarheidsmarge is behalve van het gekozen betrouwbaarheidsniveau en het onderzoeksdesign, vooral afhankelijk is van de spreiding in de antwoorden en van het aantal ondervraagde personen. Meestal wordt een betrouwbaarheidsniveau van 95 procent gekozen. Dit betekent dat de werkelijke waarde in 95 van de 100 steekproeven tussen de grenzen zal liggen van de marges behorende bij de gevonden waarde en de steekproefomvang. De betrouwbaarheidsintervallen zijn beschikbaar in de tabellenset behorend bij deze publicatie.

Gebruikte analysemethoden

In bivariate analyses is de relatie tussen twee variabelen bekeken, in dit geval de relatie tussen de doelvariabelen over online veiligheid en online criminaliteit enerzijds en de achtergrondkenmerken anderzijds. Met behulp van significantietoetsing is onderzocht of het verband tussen twee variabelen in de populatie statistisch significant is op basis van het steekproefresultaat. De in deze publicatie beschreven verschillen zijn statistisch significant, tenzij anders aangegeven.

In sommige gevallen bestaat er een samenhang tussen de achtergrondkenmerken. Zo kunnen bijvoorbeeld verschillen die op een doelvariabele gemeten worden voor het kenmerk opleiding indirect (mede)bepaald worden door het kenmerk leeftijd (jongeren zijn gemiddeld genomen hoger opgeleid). Met behulp van multivariate logistische regressieanalyses is gekeken of de verschillen naar achtergrondkenmerken in stand blijven wanneer gecorrigeerd wordt voor deze samenhangen tussen deze kenmerken. De in deze publicatie beschreven verschillen blijven na correctie voor deze samenhangen bestaan, tenzij anders aangegeven.

Schaalscores

In hoofdstuk 3 is bij het beschrijven van de bekendheid met internetveiligheid en het nemen van beveiligingsmaatregelen gebruik gemaakt van schaalscores. Op een schaal van 0 (= laag) – 10 (= hoog) is weergegeven hoe respondenten op deze onderwerpen scoren. De schaalscore geeft een totaalbeeld van de antwoorden op onderliggende items die bekendheid met internetveiligheid respectievelijk het nemen van beveiligingsmaatregelen meten. Hoe de berekening van beide schaalscores heeft plaatsgevonden is te lezen in hoofdstuk 3.

Verschillen met Veiligheidsmonitor en ICT-enquête

De vraagstellingen om slachtofferschap van online criminaliteit en aanverwante thema's (bekendheid met daders, gevolgen, melding en aangifte) te meten zijn in de Veiligheidsmonitor 2021 en OVeC 2022 op een enkele uitzondering na identiek. Ook de opzet en uitvoering van de beide onderzoeken is gelijk gehouden: de dataverzameling vond plaats via internetenquêtering en de veldwerkperiode liep van augustus t/m oktober. Desondanks zijn de uitkomsten van beide onderzoeken niet zonder meer vergelijkbaar. De Veiligheidsmonitor is een algemene veiligheids- en slachtofferenquête waarin online criminaliteit één van de onderzochte thema's is, terwijl OVeC een enquête is waarin online criminaliteit centraal staat. Als gevolg daarvan worden ook de vragen over online criminaliteit in de vragenlijst van beide onderzoeken in een andere context gesteld: in de Veiligheidsmonitor volgt het vragenblok over online criminaliteit na vragenblokken over veiligheidsbeleving in de fysieke wereld en slachtofferschap van traditionele, offline criminaliteit, terwijl in OVeC het vragenblok over online criminaliteit volgt na vragenblokken over internetgebruik en internetveiligheid. Bekend is dat verschillen in de context waarin onderzoeken worden gehouden en verschillen in de context waarin vragen worden gesteld, kunnen leiden tot andere onderzoeksuitkomsten (Tourangeau, Rips en Rasinsky, 2000). Het gegeven dat het thema online veiligheid en criminaliteit in OVeC veel meer op de voorgrond staat dan in de Veiligheidsmonitor kan bovendien tot selectie-effecten hebben geleid: het is denkbaar dat beide enquêtes, afhankelijk van de affiniteit met het onderwerp verschillende typen respondenten aantrekken. Hoe groot deze context- en selectie-effecten zijn kan nog niet worden vastgesteld, maar er zijn methoden om hier meer inzicht in te krijgen (zie ook Conclusies en aanbevelingen).

Ook voor de ICT-enquête geldt dat de uitkomsten hiervan niet zonder meer vergelijkbaar zijn met die van OVeC. Ook hier spelen context-effecten een rol. En daarnaast ook verschillen in vraagstellingen en in opzet en uitvoering van het onderzoek, zoals een andere onderzoekspopulatie (12 jaar en ouder), een andere veldwerkperiode (april – juli) en manier van dataverzameling (niet alleen via internet maar ook telefonisch).

[17] Voor de VM 2021 hebben ook de vraagstellingen uit het pilotonderzoek Digitale Veiligheid en Criminaliteit als basis gediend.

Bijlage C. Referenties

Akkermans, M., Derksen, E, Kloosterman, R., Moons, E. en M. Wingen (2023). *Prevalentiemonitor Huiselijk Geweld en Seksueel Grensoverschrijdend gedrag 2022*. Den Haag: Wetenschappelijk Onderzoek- en Documentatie Centrum/Centraal Bureau voor de Statistiek.

Akkermans, M., Gielen, W., Kloosterman, R., Knoops, K., Linden, G., Moons, E. en C. Reep (2019). *Digitale Veiligheid & Criminaliteit 2018*. Centraal Bureau voor de Statistiek, Den Haag/Heerlen/Bonaire.

Akkermans, M., Kloosterman, Moons, E., Reep, C. en M. Tummers-van der Aa (2022). *Veiligheidsmonitor 2021*. Centraal Bureau voor de Statistiek, Den Haag/Heerlen/Bonaire.

Boonstra, H-J., en J. van den Brakel (2022). *Methodebreuken Veiligheidsmonitor 2021*. Centraal Bureau voor de Statistiek, Den Haag/Heerlen/Bonaire.

CBS (2022). *Nederlander koopt meer digitale producten maar minder goederen online*, 21 oktober 2022 (cbs.nl).

Politie data.politie.nl (2023). Geregistreerde misdrijven en aangiften; soort misdrijf, gemeente 2023.

Reep, C. (2021). *Financiële schade van criminaliteit tegen burgers*. Statistische Trends. Centraal Bureau voor de Statistiek, Den Haag/Heerlen/ Bonaire.

Tourangeau, R., Rips, L.J. and Rasinski, K. (2000), *The Psychology of Survey Response.* Cambridge University Press, New York.

Bijlage D. Meer cijfers

Het achterliggende cijfermateriaal dat behoort bij de in deze publicatie gepresenteerde uitkomsten is inclusief 95% betrouwbaarheidsmarges (boven- en ondergrens) opgenomen in een Tabellenset die aan deze publicatie is toegevoegd.

Bijlage E. Medewerkers

Math Akkermans
Judit Arends
Elianne Derksen
Carin Reep

Verklaring van tekens

Niets (blanco)	Een cijfer kan op logische gronden niet voorkomen
.	Het cijfer is onbekend, onvoldoende betrouwbaar of geheim
*	Voorlopige cijfers
**	Nader voorlopige cijfers
–	(indien voorkomend tussen twee getallen) tot en met
0 (0,0)	Het cijfer is kleiner dan de helft van de gekozen eenheid
2022–2023	2022 tot en met 2023
2022/2023	Het gemiddelde over de jaren 2022 tot en met 2023
2022/'23	Oogstjaar, boekjaar, schooljaar enz., beginnend in 2022 en eindigend in 2023
2020/'21–2022/'23	Oogstjaar, enz., 2020/'21 tot en met 2022/'23

In geval van afronding kan het voorkomen dat het weergegeven totaal niet overeenstemt met de som van de getallen.
Verbeterde cijfers in de staten en tabellen zijn niet als zodanig gekenmerkt.

Colofon

Uitgever
Centraal Bureau voor de Statistiek
Henri Faasdreef 312, 2492 JP Den Haag
www.cbs.nl

Prepress
Centraal Bureau voor de Statistiek

Ontwerp
Edenspiekermann

Inlichtingen
Tel. 088 570 70 70
Via contactformulier: www.cbs.nl/infoservice