Paper

Online Veiligheid en Criminaliteit 2024

Judit Arends
Elianne Derksen
Mattijn Morren

April 2025

Online Veiligheid en Criminaliteit 2024

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 criminaliteit. Bij online criminaliteit gaat het om slachtofferschap van online delicten, gevolgen die slachtoffers ervaren van wat hen overkomen is, en of ze melding of aangifte gedaan hebben. Naast deze twee centrale 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 2024, kortweg OVeC 2024. Dit onderzoek heeft plaatsgevonden in augustus, september en oktober 2024. In totaal hebben ruim 33 duizend personen van 15 jaar of ouder meegedaan aan de internetenquête. Aanvullend is ook gebruikgemaakt van gegevens 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 inwoners van Nederland van 15 jaar of ouder zich als ze online zijn? Zijn ze bang om slachtoffer te worden van online criminaliteit? Weten ze hoe ze zich kunnen beschermen op internet en welke maatregelen nemen ze? En hoeveel mensen worden slachtoffer van online criminaliteit? In hoeverre hebben ze te maken met andere voorvallen, zoals online discriminatie en online oproepen tot openbare-ordeverstoring? Al deze vragen, en nog meer, worden in deze publicatie beantwoord.

Online Veiligheid en Criminaliteit (OVeC) is niet het enige onderzoek met deze thematiek dat het Centraal Bureau voor de Statistiek (CBS) uitvoert. In de jaarlijkse ICT-enquête Personen en Huishoudens wordt onderzoek gedaan naar online veiligheid en in de tweejaarlijkse Veiligheidsmonitor naar online criminaliteit. Daarnaast wordt in de tweejaarlijkse Prevalentiemonitor Huiselijk Geweld en Seksueel Grensoverschrijdend gedrag het thema online seksuele intimidatie onderzocht (zie kader hieronder).

Op verzoek van het ministerie van Justitie en Veiligheid heeft het CBS met OVeC in 2022 voor het eerst de stand van zaken op het terrein van online veiligheid en criminaliteit in samenhang onderzocht. In 2024 is het de tweede keer dat het CBS deze beide thema's in één onderzoek heeft gecombineerd. De intentie bestaat om het onderzoek in de even jaren (de jaren waarin er geen Veiligheidsmonitor wordt gehouden) te herhalen, zodat het een monitorfunctie krijgt. De volgende meting zal dan plaatsvinden in 2026.

Het onderzoek richt zich op inwoners van Nederland van 15 jaar of ouder. Het verslagjaar is 2024. In de enquête is gevraagd naar (slachtofferschap van) online criminaliteit in de twaalf maanden voorafgaand aan het onderzoek. De enquêtering heeft plaatsgevonden van augustus tot en met oktober. Dit betekent dat de cijfers over online criminaliteit gaan over de periode augustus t/m oktober 2023 – augustus t/m oktober 2024. Het gaat om zelfrapportage, dus om opvattingen, percepties en ervaringen van respondenten. OVeC is een steekproefonderzoek. Dit betekent dat de weergegeven cijfers schattingen zijn waarvoor betrouwbaarheidsintervallen gelden. In de bijbehorende Tabellenset 2024 zijn deze betrouwbaarheidsintervallen opgenomen in de vorm van boven- en ondergrenzen behorende bij de schattingen.

Onderzoeksvragen

In deze publicatie staan de volgende onderzoeksvragen centraal:

Online veiligheid

- Hoe wordt omgegaan met privacy en het beschermen van persoonlijke gegevens op internet?
- In welke mate zijn begrippen rondom internetveiligheid bekend?
- In welke mate bestaan er zorgen over internetveiligheid?
- Welke maatregelen worden genomen om slachtofferschap van online criminaliteit te voorkomen?
- Hoe wordt de veiligheid op internet ervaren en hoe wordt de kans op slachtofferschap van online criminaliteit ingeschat?

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 vindt online discriminatie plaats?
- Op welke gronden en op welke manieren voelen slachtoffers zich online gediscrimineerd?
- Wat zijn de gevolgen van online discriminatie voor de slachtoffers?
- In welke mate wordt er melding gemaakt en aangifte gedaan van online discriminatie?

Online oproep tot openbare-ordeverstoring

- Hoe vaak en waar worden online oproepen tot openbare-ordeverstoring gezien?
- Om welke soorten verstoringen van de openbare orde gaat het dan?
- Wat wordt met de oproep gedaan?

Opzet van het onderzoek

De cijfers uit dit onderzoek zijn gebaseerd op een internetenquête onder de Nederlandse bevolking van 15 jaar of ouder (15,0 miljoen personen in 2024). Het onderzoek heeft plaatsgevonden van augustus tot en met oktober 2024. Voor het onderzoek zijn 100 duizend personen benaderd. Ruim 33 duizend van hen hebben de vragenlijst ingevuld, een respons van 33,2 procent. Dit grote aantal respondenten maakt het mogelijk om zowel voor de totale 15-plus bevolking als 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 Justitie en Veiligheid, waarbij zoveel mogelijk is aangesloten bij de vraagstellingen in OVeC 2022. Voor het onderzoek van 2024 zijn vragen toegevoegd over nieuwe vormen van online veiligheid en criminaliteit.

Extra informatiebronnen: ICT-enquête, Veiligheidsmonitor en Prevalentiemonitor

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

ICT-enquête Personen en Huishoudens

In de ICT-enquête wordt informatie verzameld over de toegang en het gebruik van ICT-apparatuur en internet van personen en huishoudens. Het CBS voert deze enquête jaarlijks uit in de periode april t/m juli onder personen van 12 jaar of ouder. In 2024 hebben ruim 6 duizend mensen deelgenomen aan het onderzoek. Dit onderzoek wordt in opdracht van de Europese Unie (EU) door alle lidstaten uitgevoerd onder 16- tot 75-jarigen.

Veiligheidsmonitor

De Veiligheidsmonitor (Akkermans et al, 2024) 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 2023 hebben ruim 180 duizend mensen van 15 jaar of ouder aan het onderzoek deelgenomen.

Prevalentiemonitor Huiselijk Geweld en Seksueel Grensoverschrijdend gedrag

De Prevalentiemonitor Huiselijk Geweld en Seksueel Grensoverschrijdend gedrag (Derksen et al, 2024) is een tweejaarlijkse enquête die het CBS uitvoert als aanvullende statistische dienstverlening voor het Wetenschappelijk Onderzoek en Datacentrum (WODC). Eén van de thema's van dit onderzoek is online seksuele intimidatie. In 2024 hebben ruim 25 duizend mensen van 16 jaar of ouder deelgenomen aan het onderzoek.

Antwoorden op de onderzoeksvragen

Online veiligheid

Hoe wordt omgegaan met privacy en het beschermen van persoonlijke gegevens op internet?

De meerderheid van de 15-plussers is terughoudend met het online delen van privacygevoelige persoonlijke informatie, zoals een kopie van bankpas, paspoort, ID-kaart of rijbewijs, of Burgerservicenummer (BSN). Driekwart gaf in 2024 aan dat ze een kopie van de bankpas niet online doorgeven; 19 procent deed het alleen als het moest. Ruim de helft deelde geen kopie van het paspoort, de ID-kaart of het rijbewijs via internet. Ruim een derde deed dit alleen als het moest.

Bijna iedereen nam maatregelen om persoonlijke gegevens op internet te beschermen. Van de negen in het onderzoek voorgelegde beschermingsmaatregelen, variërend van het gebruik van een webcamcover of schuifje voor de camera tot het beperken of weigeren van toegang tot (online) locatiegegevens, had 95 procent er in 2024 minstens één genomen.

In welke mate zijn begrippen rondom internetveiligheid bekend?

Het meest bekend waren de begrippen spam, hacken, identiteitsfraude en back-ups maken: ongeveer 90 procent had hiervan gehoord en weet ook wat het is. Verder wist 80 procent wat phishing is en 77 procent wat met WhatsApp-fraude wordt bedoeld. Het minst bekend waren 15-plussers met de relatief nieuwe begrippen doxing, social engineering, en passkey: 20 à 30 procent wist wat dit zijn. In 2024 wisten meer mensen wat de begrippen tweetrapsverificatie, VPN-verbinding en social engineering betekenen dan in 2022.

In welke mate bestaan er zorgen over internetveiligheid?

Aspecten van internetveiligheid die het vaakst werden genoemd als bron van zorgen, waren diefstal van persoonsgegevens bij een organisatie na een hack of door een datalek, misbruik van bankgegevens, en misbruik van persoonsgegevens. Ruim een kwart van de mensen maakte zich veel zorgen over deze veiligheidsaspecten. Over het misbruik van accounts, het hacken van een apparaat of account, en het verspreiden van foto's of video's zonder toestemming maakte ongeveer 20 procent zich veel zorgen. Het minst bezorgd waren mensen om online gediscrimineerd te worden: 7 procent maakte zich hierover veel zorgen en meer dan 70 procent niet.

Welke maatregelen worden genomen om slachtofferschap van online criminaliteit te voorkomen?

De meest gebruikte maatregelen om apparatuur en accounts met persoonlijke informatie te beveiligen tegen misbruik door anderen waren het vergrendelen van apparaten met een toegangscode, wachtwoord, vingerafdruk of Face ID, en het controleren van bijlages in e-mails vóór het openen ervan. Ruim 4 op de 5 mensen gebruikten toegangsbeveiliging voor alle apparaten, en bijna 4 op de 5 controleerden e-mailbijlages. Bijna 3 op de 5 zeiden updates van apparatuur of apps direct of zo snel mogelijk uit te voeren. Maatregelen die het minst vaak werden genomen waren het gebruik van tweetrapsverificatie en vooral het gebruik van een VPN-verbinding, en wachtwoorden van minimaal zestien tekens. Wel gaven relatief veel mensen aan voor sommige (maar niet voor alle) accounts een ander wachtwoord te gebruiken (55 procent).

Hoe wordt de veiligheid op het internet ervaren en hoe wordt de kans op slachtofferschap van online criminaliteit ingeschat?

In 2024 gaf de helft van de bevolking van 15 jaar of ouder aan zich (heel) veilig te voelen als ze internet gebruiken. 4 procent voelde zich (heel) onveilig. De rest (45 procent) voelde zich niet veilig en niet onveilig. Vooral 15- tot 18-jarigen en mannen voelden zich (heel) veilig op internet. Vrouwen en 65-plussers voelden zich online het vaakst (heel) onveilig.

Vooral als het gaat om online bedreiging en intimidatie schatten mensen de kans om hiervan zelf slachtoffer te worden relatief laag in. Bijna 10 procent achtte de kans aanwezig (dat wil zeggen '(heel) groot' of 'niet groot, niet klein') om zelf slachtoffer te worden van shamesexting en ongeveer 15 procent van online pesten, bedreiging of discriminatie. Ruim 40 procent van de bevolking achtte de kans aanwezig om zelf slachtoffer te worden van aan- of verkoopfraude en ongeveer de helft van hacken.

Online criminaliteit

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

In 2024 gaf 16 procent van de bevolking van 15 jaar of ouder aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van online criminaliteit. Dit zijn bijna 2,4 miljoen mensen. De meesten werden slachtoffer van oplichting en fraude (9 procent), en dan met name van aankoopfraude. Met hacken had 4 procent te maken, en eveneens 4 procent met online bedreiging en intimidatie. Krap 1 procent werd slachtoffer van andere online delicten.

In 2024 gaven meer mensen aan slachtoffer te zijn geweest van online criminaliteit dan in 2022 (15 procent). Deze toename is met name zichtbaar bij slachtoffers van online oplichting en fraude. Het aandeel slachtoffers van hacken was in 2024 juist lager dan in 2022. Van online bedreiging en intimidatie en van andere online delicten werden in beide jaren ongeveer evenveel mensen slachtoffer.

Jongeren werden vaker slachtoffer van online criminaliteit dan ouderen. Zo werd 20 procent van de 15- tot 25-jarigen slachtoffer, tegenover 10 procent van de 65-plussers. Vooral bij het slachtofferschap van online bedreiging en intimidatie is dit verschil tussen jongere en oudere leeftijdsgroepen groot. Ook homoseksuele en bi-plus personen werden vaker slachtoffer van deze vorm van online criminaliteit dan heteroseksuele personen.

Wie zijn de daders van online criminaliteit?

Bij delicten in de persoonlijke sfeer zijn ook vragen gesteld over de relatie van het slachtoffer met de dader(s). Deze delicten zijn vaak gericht op het veroorzaken van negatieve emoties bij het slachtoffer. Dit speelt bij uitstek bij online bedreiging en intimidatie. Bij 4 op de 10 slachtoffers van online bedreiging en intimidatie kende het slachtoffer de dader. Bij pesten en stalken was dit het vaakst het geval.

De meest genoemde daders waren de ex-partner, een vriend(in) of een medestudent/-scholier. De ex-partner werd bij online stalken het vaakst als dader genoemd (17 procent). Bij online pesten was dat een medestudent/-scholier (15 procent) en bij online bedreiging het vaakst een andere bekende (13 procent).

Wat zijn de gevolgen van online criminaliteit voor de slachtoffers?

Voor de meeste slachtoffers van online criminaliteit leidde het voorval ertoe 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 5 à 7 procent van de slachtoffers genoemd.

Van de verschillende vormen van online criminaliteit gaven slachtoffers van online oplichting en fraude het vaakst aan minder vertrouwen in mensen te hebben. Zich minder veilig voelen, slaapproblemen, depressieve klachten, het voorval telkens opnieuw beleven en angstklachten werden het vaakst gerapporteerd door slachtoffers van online bedreiging en intimidatie.

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

Van de slachtoffers van online criminaliteit heeft 18 procent in 2024 bij de politie gemeld wat hen overkomen was en 45 procent deed dit bij een andere instantie of persoon. Bijna alle meldingen van online criminaliteit bij de politie resulteerden in een aangifte (18 procent maakte melding, 16 procent deed aangifte). De meest genoemde redenen om het voorval niet bij de politie te melden of aangifte te doen was dat men er niet aan heeft gedacht of het niet zo belangrijk vond, gevolgd door 'het helpt toch niets'.

Online discriminatie

In welke mate vindt online discriminatie plaats?

In 2024 voelde 4 procent van de bevolking van 15 jaar of ouder zich weleens online gediscrimineerd. Dat is een verdubbeling ten opzichte van 2022, toen 2 procent dit aangaf. Personen van 15 tot 45 jaar gaven dit met 6 procent relatief vaak aan. Ook homoseksuele mannen (12 procent), homoseksuele vrouwen (10 procent) en bi-plus vrouwen (9 procent) hadden hier relatief vaak mee te maken. Personen geboren in Nederland met herkomst buiten Europa ervoeren met 13 procent het vaakst online discriminatie. Personen met een Nederlandse herkomst het minst vaak (2 procent).

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

Van degenen die online discriminatie ervoeren, ging het bij 41 procent om discriminatie op grond van ras of huidskleur, gevolgd door discriminatie op grond van nationaliteit (38 procent) en godsdienst of levensbeschouwing (33 procent).

Bijna 7 op de 10 mensen personen die zich gediscrimineerd voelden, gaven aan dat dit kwam door discriminerende opmerkingen. Bijna 6 op de 10 zeiden dat dit kwam door een negatief beeld/stigmatisering of door ongelijke behandeling/benadeling/het voortrekken van bepaalde groepen. Bij ruim 4 op de 10 was sprake van 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 58 procent van degenen die online discriminatie ervoeren aan dat ze daardoor minder vertrouwen in mensen hadden. Een derde voelde zich minder veilig en 14 procent had depressieve klachten. Angstklachten en/of paniekaanvallen, slaapproblemen en het voorval telkens opnieuw beleven werden door ongeveer 10 procent genoemd. Verder gaf meer dan 30 procent aan dat zij door het voorval minder social media zijn gaan gebruiken.

In welke mate wordt er melding gemaakt en aangifte gedaan van online discriminatie?

Ruim 20 procent van de mensen die zich in de afgelopen twaalf maanden online gediscrimineerd voelden, heeft dit ergens gemeld. De meesten meldden dit direct bij de website (12 procent). Verder meldde 5 procent het bij de politie, 3 procent op het werk en eveneens 3 procent op school. Bij Meld.Online Discriminatie maakte 1 procent melding, en bij het College voor de Rechten van de Mens en bij een gemeentelijke antidiscriminatievoorziening (ADV) minder dan 1 procent. Van degenen die online discriminatie ervoeren, deed 4 procent aangifte bij de politie.

Online oproepen tot openbare-ordeverstoring

Hoe vaak en waar worden online oproepen tot openbare-ordeverstoring gezien?

In 2024 gaf 7 procent van de bevolking van 15 jaar of ouder aan in de afgelopen twaalf maanden weleens online berichten te hebben gezien, waarin werd opgeroepen tot openbare-ordeverstoring of activiteiten die vaak daartoe leiden, zoals straatraces, demonstraties of illegale feesten. In 2022 was dit aandeel hoger, namelijk 9 procent. Online oproepen tot openbare-ordeverstoring werden het vaakst gezien op Facebook en Instagram. Een kleiner deel noemde ook X, WhatsApp of TikTok.

Om welke soorten verstoringen van de openbare orde gaat het dan?

Verreweg de meeste mensen die berichten zagen waarin werd opgeroepen tot openbare-ordeverstoring, gaven aan het ging om een oproep tot demonstratie (55 procent). Berichten die oproepen tot illegale feesten of evenementen werden door 12 procent genoemd en oproepen tot rellen door 9 procent. Verder gaf 8 procent aan dat het bericht opriep tot het bedreigen van bekende personen of politici.

Wat wordt met de oproep gedaan?

Het merendeel van de mensen die een online oproep tot ordeverstoring hebben gezien, gaf aan niets met het bericht te hebben gedaan (84 procent). 4 procent meldde het bij de politie en eveneens 4 procent zei te hebben deelgenomen aan de activiteit waartoe werd opgeroepen, met name aan illegale feesten of evenementen, aan straatraces, en aan demonstraties. Het bericht werd door 3 procent online gedeeld, en dan met name via WhatsApp.

1.2 Leeswijzer

Dit rapport is als volgt opgebouwd. Eerst wordt in hoofdstuk 2 een beeld geschetst van het internetgebruik van 15-plussers en hun online activiteiten. Dit als introductie op hoofdstuk 3 waarin het thema internetveiligheid en online veiligheidsbeleving 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. Er wordt afgesloten met conclusies en aanbevelingen (hoofdstuk 10).

De bijlagen bevatten een onderzoeksbeschrijving, referenties, een verwijzing naar meer cijfers, en een overzicht van medewerkers die aan deze publicatie hebben bijgedragen.

2. Internetgebruik

In de periode dat het OVeC-onderzoek is uitgevoerd (augustus t/m oktober 2024) gaf 99 procent van de 15-plussers aan in de afgelopen twaalf maanden internet te hebben gebruikt. Dit hoofdstuk is een introductie op de volgende hoofdstukken over online veiligheid en criminaliteit en beschrijft kort waarvoor internet wordt gebruikt.

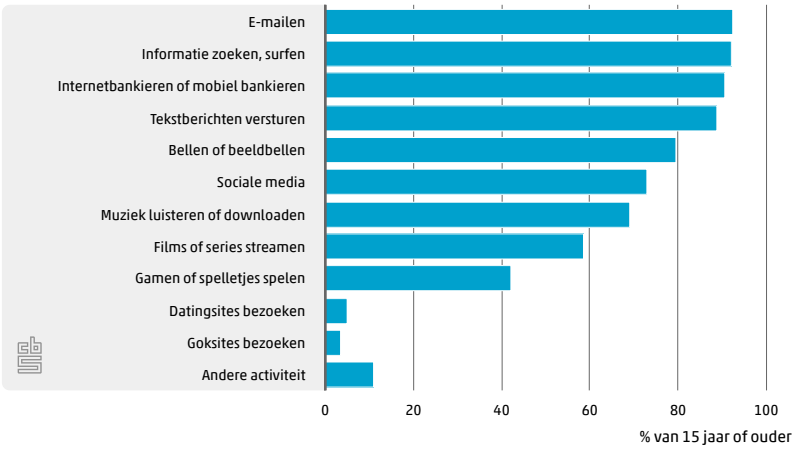
In de Tabellenset 2024 die bij deze publicatie hoort, zijn alle resultaten van dit hoofdstuk opgenomen bij '2 Internetgebruik' en '2 Details'.

2.1 Online activiteiten

Internet wordt het vaakst gebruikt om te e-mailen en voor het opzoeken van informatie/surfen op internet: in 2024 gaf ruim 90 procent aan deze online activiteiten te hebben gedaan in de afgelopen twaalf maanden. Ook voor internet- of mobiel bankieren werd het internet door ongeveer 90 procent gebruikt. Andere veelvoorkomende online activiteiten waren (WhatsApp-) berichten versturen (89 procent), bellen of beeldbellen (80 procent) en social mediagebruik (73 procent). Bijna 70 procent gebruikte internet voor ontspanning, zoals muziek luisteren of downloaden en bijna 60 procent voor het streamen van films of series. Van de onderzochte online activiteiten was het aandeel gebruikers van datingsites (5 procent) en goksites (3 procent) het laagst.

In 2024 gaven minder mensen aan het internet te gebruiken voor e-mailen dan in 2022. Het internet werd in 2024 juist vaker gebruikt voor het versturen van (WhatsApp-) berichten, social media, het luisteren of downloaden van muziek, het streamen van films of series, en het bezoeken van goksites.

2.1.1 Activiteiten op internet[1) 2)], 2024



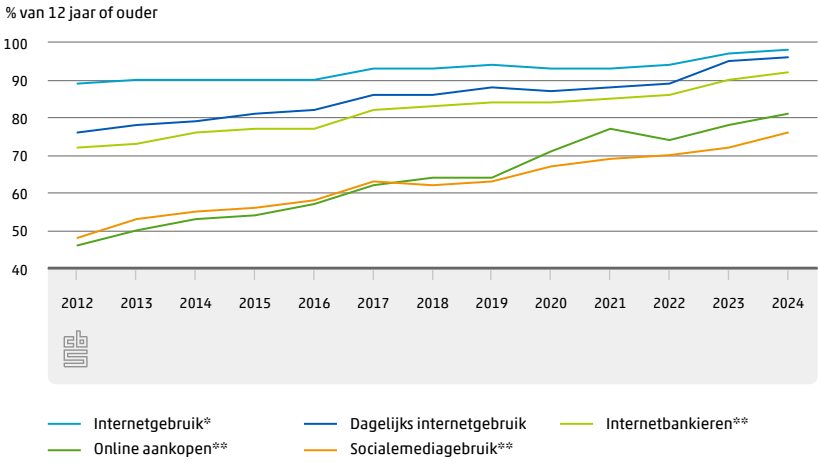
[1)] Het gaat om activiteiten in de periode van 12 maanden voorafgaand aan het onderzoek.
[2)] Meerdere antwoorden mogelijk.

Trend internetgebruik en online activiteiten

Uit de ICT-enquête personen en huishoudens, waarmee sinds 2012 informatie wordt verzameld over het gebruik van ICT-apparatuur en internet door de bevolking van 12 jaar of ouder, blijkt dat internet niet meer weg te denken is uit het dagelijks leven van de meeste mensen. In 2024 gebruikten vrijwel alle 12-plussers (98 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 96 procent in 2024.

Online activiteiten zoals internetbankieren en social mediagebruik zijn in de afgelopen tien jaar vrijwel elk jaar gestegen. Het online kopen van producten steeg sterk in 2020 en 2021, toen mensen tijdens de coronapandemie meer aan huis gebonden waren. Na een lichte daling in 2022, nam het in 2023 en 2024 weer toe.

Internetgebruik en online activiteiten



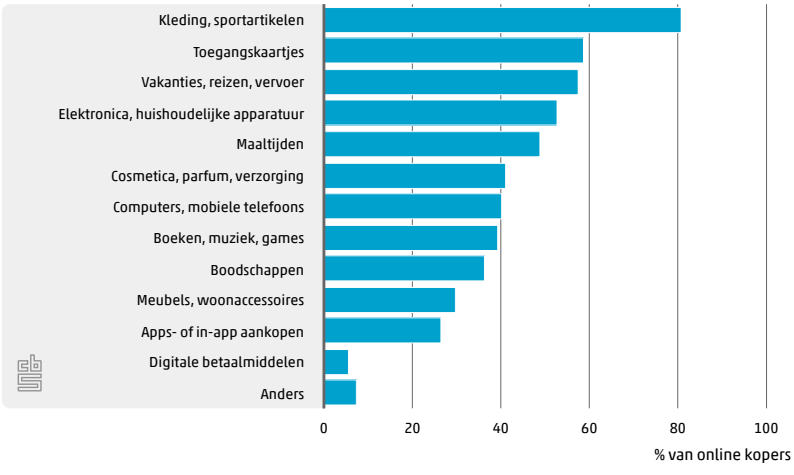
Bron: ICT-enquête personen en huishoudens
* Het gaat om internetgebruik in de periode van 12 maanden voorafgaand aan het onderzoek.
** Het gaat om activiteiten in de periode van 3 maanden voorafgaand aan het onderzoek.

2.2 Online (ver)kopen

Ruim 40 procent van de mensen van 15 jaar of ouder gaf in 2024 aan weleens online een product of dienst te hebben verkocht in de afgelopen twaalf maanden. Veel vaker gaven zij aan een online aankoop te hebben gedaan (87 procent).

Kleding, sportartikelen en schoenen werden in 2024, evenals in 2022, het meest online gekocht: 81 procent van de online kopers deed dit. Daarna volgden toegangskaartjes en vakanties/reizen, met elk ongeveer 60 procent. Elektronica of huishoudelijke apparatuur en maaltijden bij een restaurant of snackbar werden beide door ongeveer 50 procent online gekocht. Ongeveer 40 procent kocht cosmetica of verzorgingsproducten, een computer, tablet, mobiele telefoon of accessoires, boeken of e-books, muziek, spellen of games, en boodschappen of levensmiddelen online. Meubels of woonaccessoires, en apps- of in-app aankopen werden door ongeveer 30 procent gedaan. Digitale betaalmiddelen (bijv. cryptovaluta of NFT's) werden door 6 procent gekocht.

2.2.1 Online gekochte producten of diensten[1)], 2024



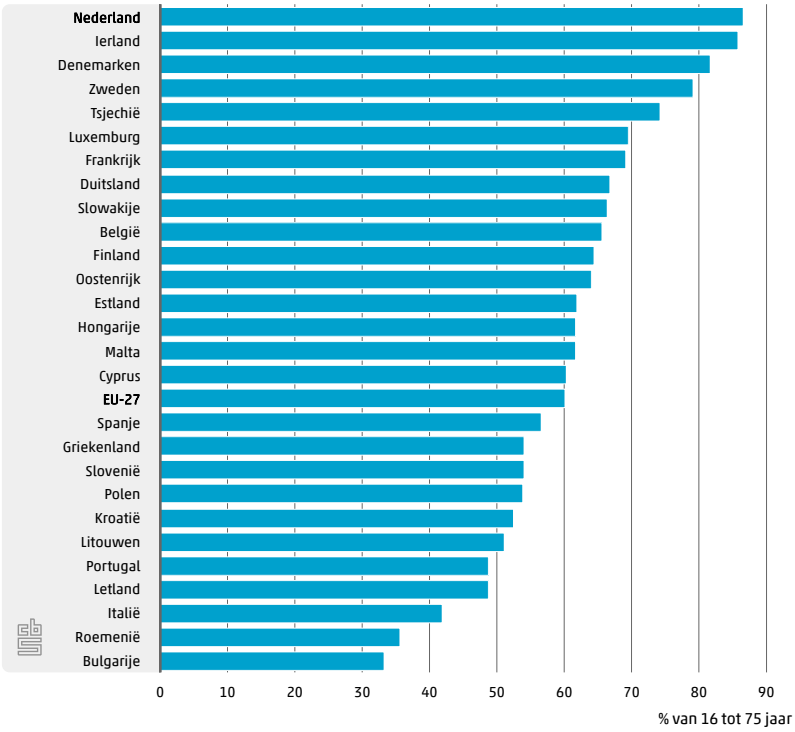
[1)]Meerdere antwoorden mogelijk.

De meeste producten of diensten werden bij grote, bekende webshops gekocht: 93 procent van de online kopers deed dat in 2024. Bij kleine, minder bekende webshops heeft ruim de helft iets gekocht, en 30 procent winkelde online bij niet-Nederlandse webshops. Op online handelsplatforms, zoals Marktplaats of eBay, kocht 42 procent producten of diensten en via social media zoals Facebook of LinkedIn deed 10 procent online aankopen.

Online kopen in Nederland en in de andere EU-landen

Het aandeel 16- tot 75-jarigen (EU-leeftijdsafbakening) dat online aankopen deed (in de drie maanden voorafgaand het onderzoek) was in 2024 met 87 procent in geen enkel ander EU-land zo hoog als in Nederland. Daarna volgden Ierland, Denemarken en Zweden met respectievelijk 86, 82 en 79 procent. Met 30 à 35 procent was het aandeel online kopers het laagst in Roemenië en Bulgarije. Het gemiddelde van de 27 EU-landen bedroeg 60 procent in 2024.

Online kopers in de EU-landen, 2024



Bron: Eurostat

3. Internetveiligheid en online veiligheidsbeleving

Er wordt steeds meer gebruik gemaakt van internet. Hiermee stijgt het risico om slachtoffer te worden van criminele activiteiten. Het veilig gebruik van internet en de beleving van 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[1)] en de kennis van en de bezorgdheid over internetveiligheid. Ook wordt beschreven welke beveiligingsmaatregelen mensen treffen. Vervolgens komt de veiligheidsbeleving en de inschatting van mensen om slachtoffer te worden van online criminaliteit aan bod. Dit hoofdstuk sluit af met de online vaardigheden die men heeft om online criminaliteit te voorkomen, de hulpbronnen die men hierbij kan aanspreken en welke informatiebehoefte men daarbij heeft.

In de Tabellenset 2024 die bij deze publicatie hoort, zijn alle resultaten van dit hoofdstuk opgenomen bij '3 Internetveiligheid' en '3a Details'. Voor de resultaten van 2022, zie Tabellenset 2022.

3.1 Privacy en bescherming persoonsgegevens

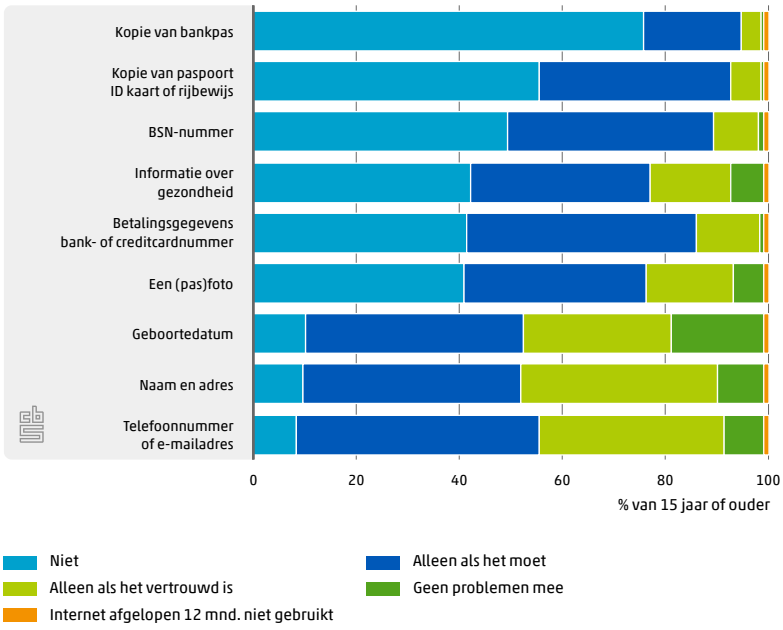
Bereidheid doorgeven persoonlijke informatie op internet

Mensen zijn relatief terughoudend met het online delen van privacygevoelige persoonlijke informatie, zoals een kopie van hun bankpas, paspoort, ID-kaart of rijbewijs, of Burgerservicenummer (BSN). Driekwart gaf aan dat ze een kopie van de bankpas niet online doorgeven. 19 procent deed het alleen als het moest. Ruim de helft deelde geen kopie van het paspoort, de ID-kaart of het rijbewijs via internet. Ruim een derde deed dit alleen als het moest.

Iets meer dan 40 procent gaf aan informatie over hun gezondheid of een (pas)foto niet via internet te delen en 35 procent deed dit alleen als het moest. Ook betalingsgegevens, zoals een bank- of creditcardnummer, werden door ruim 40 procent niet online gedeeld. Een vergelijkbaar deel deed dit alleen als het moest.

Met het online doorgeven van persoonsgegevens, zoals geboortedatum, naam, adres en contactgegevens als telefoonnummer en e-mailadres, zijn mensen minder terughoudend: ongeveer 1 op de 10 zei dit niet te doen, ruim 4 op de 10 deden dit alleen als het moest. In 2024 waren meer mensen terughoudend om hun naam en adresgegevens online door te geven dan in 2022. Dat geldt ook voor het online doorgeven van contactgegevens, zoals telefoonnummer of e-mailadres.

3.1.1 Bereidheid om persoonlijke informatie online door te geven, 2024



Voor het online doorsturen van een kopie van paspoort, identiteitskaart of rijbewijs is de zogeheten KopieID app van de Rijksoverheid beschikbaar. Van de mensen die een kopie van hun paspoort, identiteitskaart of rijbewijs online doorgaven, zei 60 procent geen gebruik te maken van deze KopieID app. Dit is lager dan in 2022; toen was dat 66 procent. Verder maakte in 2024 naar eigen zeggen 20 procent altijd gebruik van deze app; eveneens 20 procent deed dat soms. Dat is hoger dan in 2022, toen respectievelijk 18 en 16 procent dit deed.

Beschermingsmaatregelen persoonlijke informatie op internet

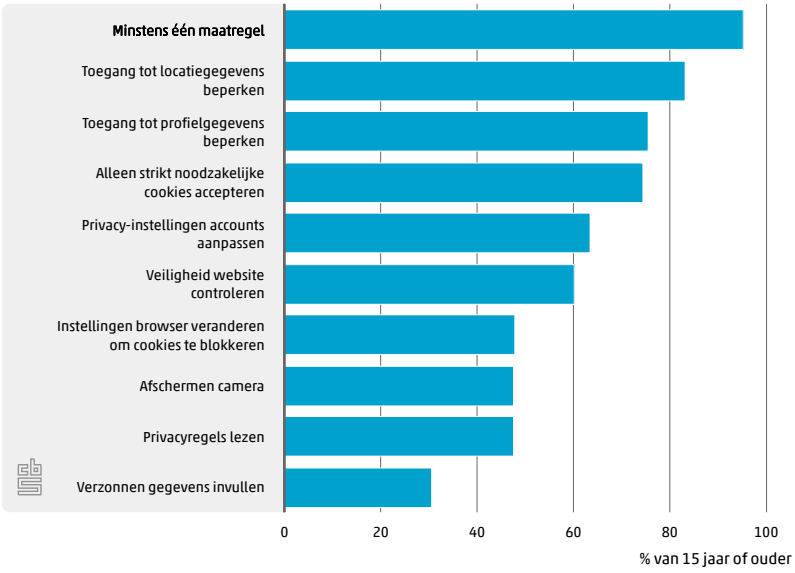
In OVeC 2024 is niet alleen onderzocht of mensen persoonlijke informatie online doorgeven, maar ook welke maatregelen ze treffen om privacygevoelige gegevens te beschermen. In de enquête werden negen beschermingsmaatregelen voorgelegd. Bijna iedereen nam één of meer van deze maatregelen om persoonlijke gegevens op internet te beschermen: 95 procent gaf aan dit te hebben gedaan in 2024, evenveel als in 2022. Van de negen beschermingsmaatregelen had 66 procent vijf of meer maatregelen genomen, 20 procent drie of vier maatregelen, en 9 procent één of twee.

Bij de afzonderlijke beschermingsmaatregelen gaf 83 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 social media te beperken, en alleen strikt noodzakelijke cookies bij gebruik van websites te accepteren. Het aanpassen van privacy-instellingen van accounts en het controleren van de veiligheid van de URL (dat is het adres) van de website werden elk door ongeveer 60 procent gedaan.

Minder vaak genomen maatregelen waren het lezen van de privacyregels, het afschermen van de camera van de computer, tablet of mobiele telefoon door bijv. het gebruik van een webcamcover of schuifje voor de camera, het veranderen van browserinstellingen (alle drie 48 procent) en het invullen van verzonnen persoonsgegevens (31 procent).

In 2024 was er in vergelijking met 2022 een toename in verschillende maatregelen die mensen treffen. Meer mensen zeiden dat zij alleen strikt noodzakelijke cookies accepteren, de instellingen van de browser veranderen om cookies te blokkeren, en verzonnen gegevens invullen. Het lezen van de privacyregels en het controleren van de veiligheid van websites werd iets minder vaak gedaan.

3.1.2 Beschermingsmaatregelen persoonlijke gegevens op internet[1)], 2024

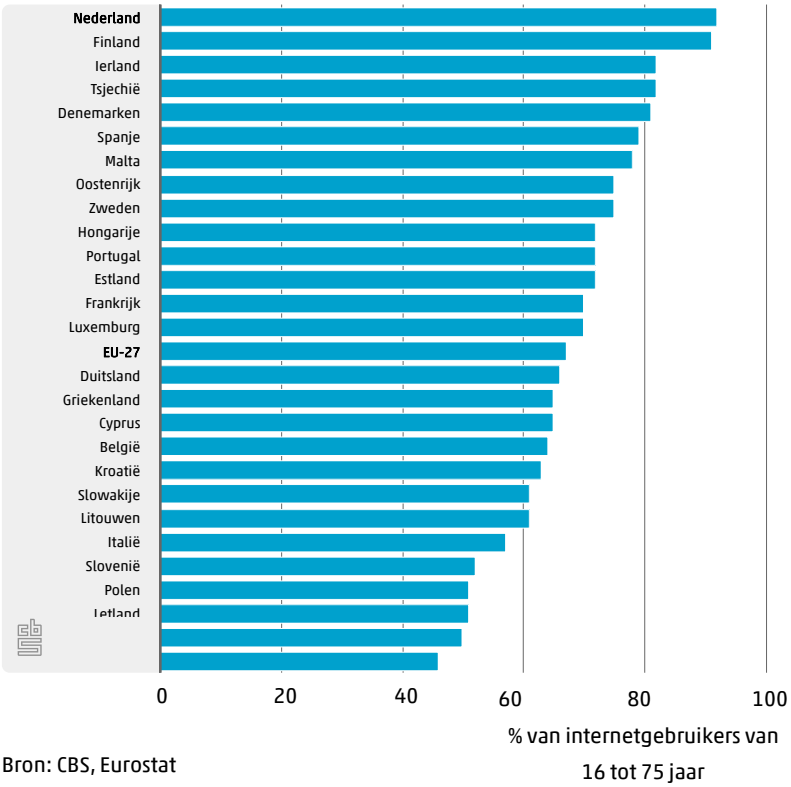


[1)]Meerdere antwoorden mogelijk.

Beschermingsmaatregelen persoonlijke gegevens in Nederland en de andere EU-landen

In 2023, het meest recente jaar waarvoor EU-cijfers beschikbaar zijn over dit onderwerp, had Nederland van alle EU-landen het hoogste aandeel internetgebruikers in de leeftijd van 16 tot 75 jaar dat maatregelen nam om persoonlijke informatie op internet te beschermen (92 procent). Nederland werd op de voet gevolgd door Finland. Inwoners van Roemenië troffen relatief het minst vaak beschermingsmaatregelen online. Het EU-gemiddelde was 67 procent.

Beschermen persoonsgegevens op internet, EU-27, 2023



Bron: CBS, Eurostat

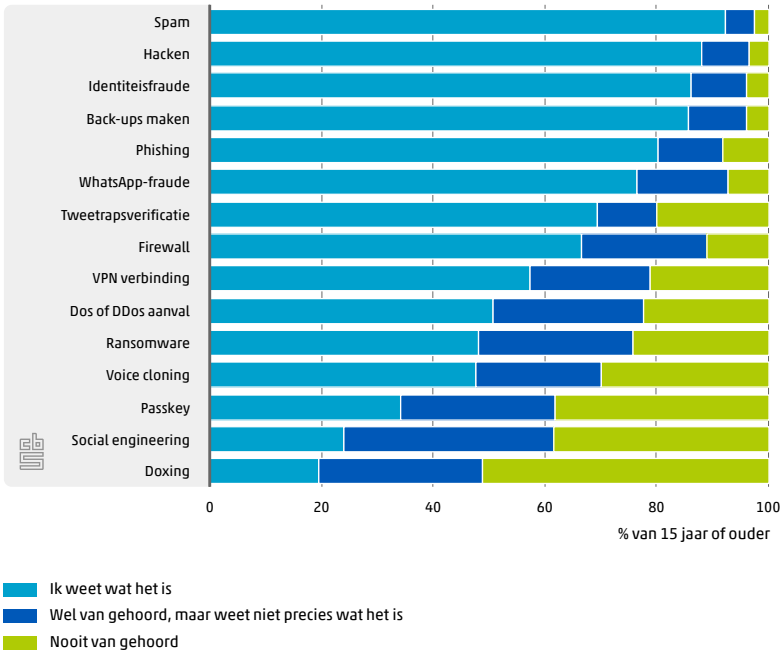
Ook bij veel afzonderlijke maatregelen, zoals het beperken of het weigeren van de toegang tot locatiegegevens, had Nederland in 2023 met 81 procent verreweg het hoogste aandeel in de EU. Ook controleerden Nederlanders vaker dan andere inwoners van EU-lidstaten de veiligheid van een website, voordat ze persoonlijke gegevens achterlaten.

3.2 Bekendheid met begrippen internetveiligheid

Wanneer mensen een lijstje met begrippen over internetveiligheid werd voorgelegd, bleek dat zij het meest bekend waren met de begrippen spam, hacken, identiteitsfraude en back-ups maken. Van elk van deze begrippen zei in 2024 ongeveer 90 procent van de 15-plussers te weten wat het betekent. Verder wist 80 procent wat phishing is en 77 procent wat met WhatsApp-fraude wordt bedoeld. De begrippen tweetrapsverificatie en firewall waren bekend bij ongeveer 70 procent en VPN-verbinding bij bijna 60 procent. Ongeveer de helft wist wat bedoeld wordt met de begrippen Dos- of DDos-aanval, ransomware, en voice cloning. Het minst bekend waren de relatief nieuwe begrippen doxing, social engineering, en passkey: 20 à 30 procent wist wat deze inhouden.

In 2024 wisten meer mensen wat de begrippen tweetrapsverificatie, VPN-verbinding en social engineering betekenen dan in 2022.

3.2.1 Bekendheid met internetveiligheid, 2024



Nieuwe vormen van online criminaliteit

Voice cloning

Een technologie waarmee je de stem van iemand kunt kopiëren. Er wordt een precieze kopie van de stem gemaakt, die vervolgens wordt gebruikt om iemand dingen te laten zeggen die hij zelf nooit heeft gezegd (Veiginternetten.nl, 2024).

Doxing

Het verzamelen of (verder) verspreiden van persoonlijke of gevoelige informatie (bijv. woonadres, telefoonnummer of foto). Dit met het doel om iemand angst aan te jagen, ernstige overlast te bezorgen, of ernstig te hinderen bij het werk dat diegene doet (Politie, 2024).

Social engineering

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 en beveiligingscodes te weten komen of malware installeren (Veiligbankieren.nl, 2024).

Passkey

Een manier om zonder wachtwoord in te loggen bij accounts en apps. Passkey maakt gebruik van biometrische authenticatie (Veiginternetten.nl, 2024).

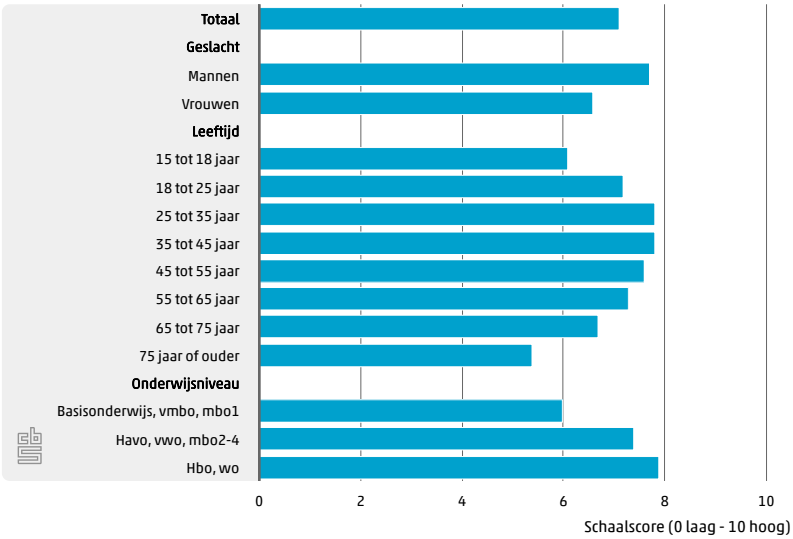
Bekendheid met begrippen internetveiligheid naar persoonskenmerken

Op basis van de antwoorden op de vijftien afzonderlijke items over bekendheid met internetveiligheid is een schaalscore berekend. Deze loopt van 0 (laag) tot 10 (hoog). De schaalscore is berekend door de antwoorden op de vijftien items op te tellen, waarbij 'nooit van gehoord' de score 0 heeft, 'wel van gehoord, maar weet niet precies wat het is' de score 1, en 'ik weet wat het is' de score 2. Het minimum van deze som is 0 en het maximum 30. Om tot een score op een schaal van 0 tot 10 te komen is de som vermenigvuldigd met de factor 10/30. De gemiddelde score was 7,1 in 2024.

In 2022 is bekendheid met internetveiligheid met twaalf items gemeten. De gemiddelde schaalscore was toen 7,7. De begrippen doxing, passkey en voice cloning zijn in 2024 toegevoegd. Als de schaalscore van 2024 op basis van de antwoorden van de twaalf items over bekendheid met internetveiligheid van 2022 berekend wordt, dan is de gemiddelde schaalscore 7,8. Dit gemiddelde is vergelijkbaar met 2022. De nieuwe begrippen doxing en passkey waren in 2024 nog niet zo bekend (zie figuur 3.2.1). Door het toevoegen van deze items is de gemiddelde schaalscore in 2024 lager dan in 2022.

De bekendheid met internetveiligheid (schaalscore) verschilt tussen bevolkingsgroepen. Mannen gaven vaker dan vrouwen aan bekend te zijn met veiligheidsbegrippen. Verder waren 25- tot 45-jarigen het meest op de hoogte en 75-plussers het minst. Ook 15- tot 18-jarigen scoorden relatief laag. Personen met een afgeronde hbo- of wo-opleiding waren meer bekend met veiligheidsbegrippen dan personen met een havo, vwo of mbo2-4 diploma en vooral meer dan personen met basisonderwijs, vmbo of mbo1.

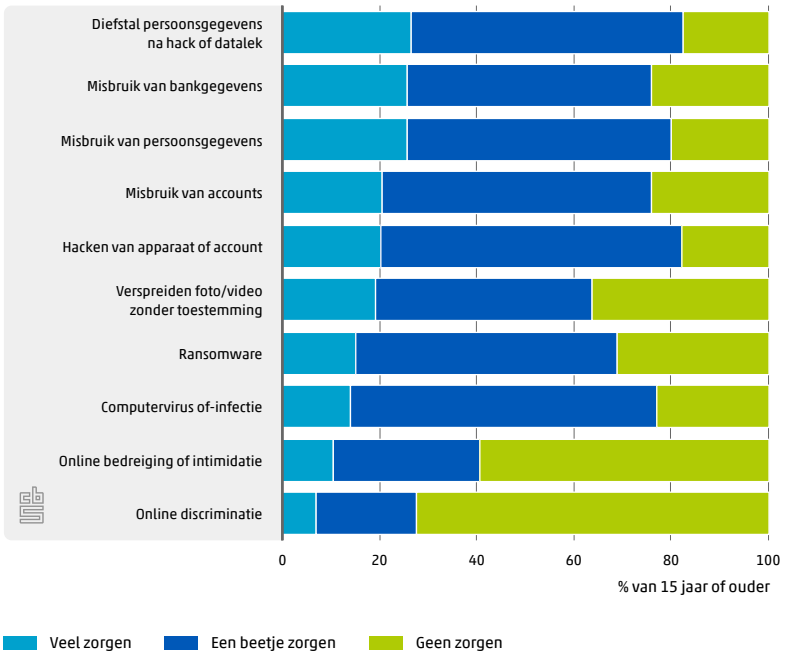
3.2.2 Bekendheid met internetveiligheid naar persoonskenmerken, 2024



3.3 Bezorgdheid over internetveiligheid

De veiligheidsaspecten waarover mensen zich het meest zorgen maakten, waren diefstal van persoonsgegevens bij een organisatie na een hack of door een datalek, misbruik van bankgegevens, en misbruik van persoonsgegevens. Ruim een kwart maakte zich hier veel zorgen over. Over het misbruik van accounts, het hacken van een apparaat of account, en het verspreiden van foto's of video's zonder toestemming maakte ongeveer 20 procent zich veel zorgen. Het minst bezorgd waren mensen om online gediscrimineerd te worden: 7 procent maakte zich hierover veel zorgen en meer dan 70 procent niet.

3.3.1 Bezorgdheid over internetveiligheid, 2024



Internet op openbare plekken en veiligheid

Mensen kunnen tegenwoordig overal online zijn, ook op openbare plekken. Openbare wifinetwerken zijn niet altijd veilig. Openbare wifinetwerken zijn voor iedereen toegankelijk en dit maakt deze voor kwaadwillende hackers een makkelijk doelwit om gegevens buit te maken.

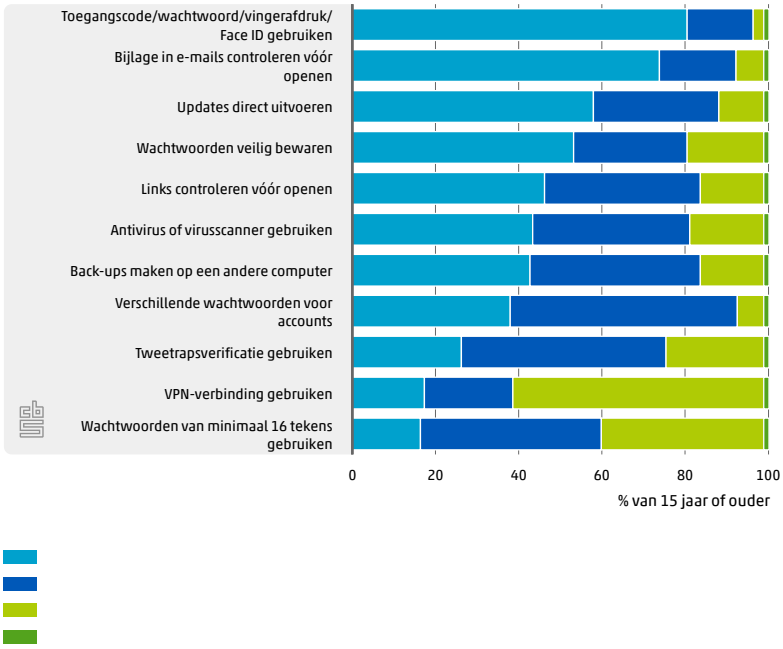
In 2024 maakte 62 procent van de 15-plussers naar eigen zeggen weleens gebruik van een openbaar wifinetwerk, bijvoorbeeld in een café, winkel, trein of hotel. De helft gebruikte weleens een openbaar wifinetwerk dat was beveiligd met een wachtwoord en 40 procent gebruikte (ook) weleens een openbaar wifinetwerk zonder wachtwoord. Ruim een derde gaf aan geen openbaar wifinetwerk te hebben gebruikt, maar altijd het eigen internetabonnement of -bundel te gebruiken.

3.4 Beveiligingsmaatregelen apparaten en accounts

De meest gebruikte maatregelen om apparatuur en accounts met persoonlijke informatie te beveiligen tegen misbruik door anderen waren het vergrendelen van apparaten met een toegangscode, wachtwoord, vingerafdruk of Face ID, en het controleren van bijlages in e-mails vóór het openen ervan. Ruim 4 op de 5 mensen gebruikten toegangsbeveiliging voor alle apparaten, en bijna 4 op de 5 controleerden e-mailbijlages. Bijna 3 op de 5 zeiden updates van apparatuur of apps direct of zo snel mogelijk uit te voeren. Maatregelen die het minst vaak werden genomen, waren het gebruik van tweetrapsverificatie en vooral het gebruik van een VPN-verbinding en wachtwoorden van minimaal zestien tekens. Wel gaven relatief veel mensen aan voor sommige (maar niet voor alle) accounts een ander wachtwoord te gebruiken (55 procent).

In vergelijking met 2022 gebruikten in 2024 meer mensen een toegangscode, wachtwoord, vingerafdruk of Face ID voor alle apparaten of accounts. Ook gaven relatief meer mensen aan wachtwoorden van minimaal zestien tekens voor al hun accounts te gebruiken en werd tweetrapsverificatie vaker toegepast waar dat mogelijk was. Wel gebruikten minder mensen antivirussoftware of een virusscanner voor alle apparaten en controleerde men minder vaak de afzender van de e-mail en/of het bestandstype vóór het openen van een bijlage in een e-mail.

3.4.1 Beveiligingsmaatregelen apparaten en accounts, 2024



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

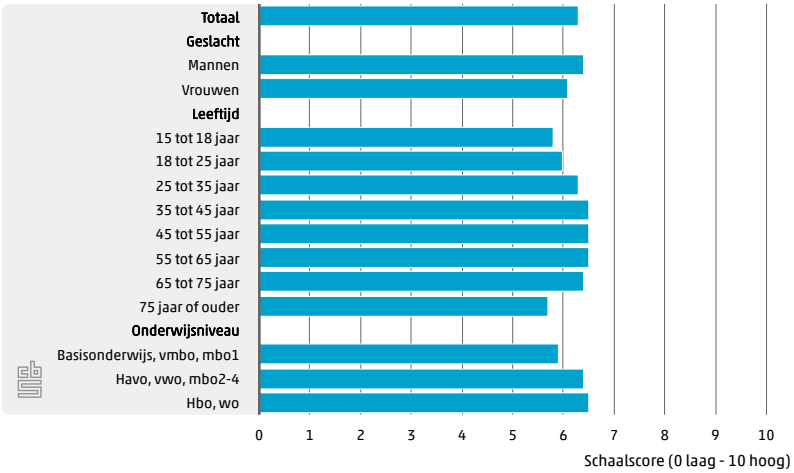
Beveiligingsmaatregelen apparaten en accounts naar persoonskenmerken

Op basis van de antwoorden op de elf beveiligingsitems is een schaalscore voor beveiligingsmaatregelen berekend die loopt van 0 (laag) tot 10 (hoog). De schaalscore is bepaald door de antwoorden op de elf 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 22. Om tot een score op een schaal van 0 tot 10 te komen is de som vermenigvuldigd met de factor 10/22. Voor mensen van 15 jaar of ouder was de gemiddelde score een 6,3.

Het gebruik van beveiligingsmaatregelen voor apparaten en accounts is in 2022 met tien items gemeten. De gemiddelde schaalscore was toen 6,6. De beveiligingsmaatregel VPN-verbinding gebruiken is in 2024 toegevoegd. Als de schaalscore van 2024 eveneens op basis van de antwoorden van tien items berekend wordt (zonder VPN-verbinding gebruiken), dan is de gemiddelde schaalscore van beveiligingsmatregelen 6,6. Dit is hetzelfde als in 2022.

De schaalscore voor beveiligingsmaatregelen (elf items) verschilt tussen bevolkingsgroepen. Mannen gaven vaker dan vrouwen aan beveiligingsmaatregelen te nemen. Verder scoorden 25- tot 75-jarigen relatief hoog en 15- tot 25-jarigen en 75-plussers relatief laag. Mensen met basisonderwijs, vmbo of mbo1 scoorden ook relatief laag ten opzichte van de andere groepen.

3.4.2 Beveiligingsmaatregelen apparaten en accounts naar persoonskenmerken, 2024



Redenen om beveiligingsmaatregelen niet te treffen

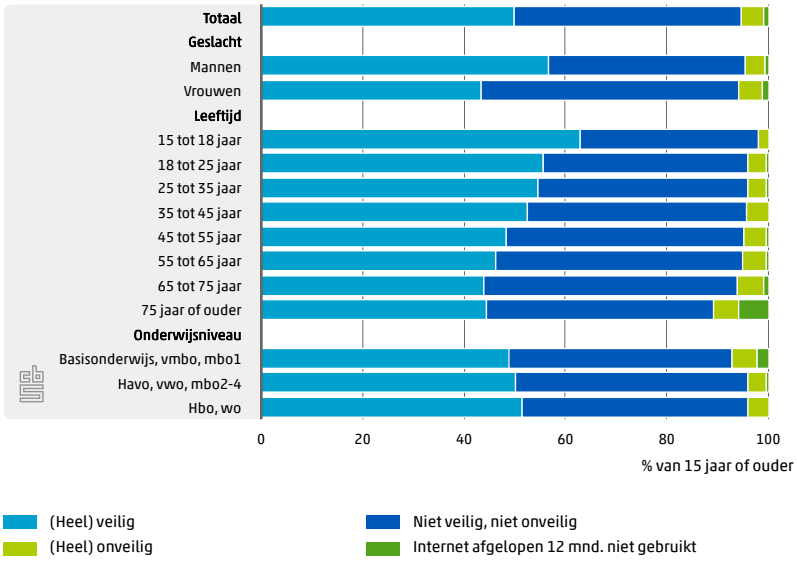
De redenen die mensen hebben om bepaalde beveiligingsmaatregelen niet te treffen lopen voor de verschillende maatregelen sterk uiteen. Zo gaven degenen die geen back-ups op een andere computer maken hiervoor het vaakst als reden dat ze niet wisten hoe het moest (35 procent) en dat ze het niet nodig vonden (31 procent). Het veilig bewaren van wachtwoorden werd vaak nagelaten, omdat men de wachtwoorden onthoudt (58 procent). Het achterwege laten van updates gebeurde het vaakst omdat men niet wist hoe het moest (26 procent), het te veel tijd kostte (26 procent) of men het niet nodig vond (23 procent). Voor de minst getroffen maatregel, het gebruiken van wachtwoorden van minimaal zestien tekens, speelde vooral de complexiteit een rol: 63 procent van degenen die niet zo'n wachtwoord gebruikten, gaf aan dat ze dit te moeilijk vinden of niet weten hoe het moet.

3.5 Online veiligheidsbeleving

In 2024 gaf de helft van de bevolking van 15 jaar of ouder aan zich (heel) veilig te voelen als ze internet gebruiken. 4 procent voelde zich (heel) onveilig. De rest (45 procent) voelde zich niet veilig en niet onveilig. De online veiligheidsbeleving verschilt niet met die van 2022.

Vooral 15- tot 18-jarigen en mannen voelden zich (heel) veilig op internet. Vrouwen en 65-plussers voelden zich online het vaakst (heel) onveilig. De veiligheidsbeleving op internet verschilt tussen mensen met een afgeronde hbo- of wo-studie en mensen met basisonderwijs, vmbo of mbo1.

3.5.1 Veiligheidsgevoelens op internet naar persoonskenmerken, 2024



Inschatting betrouwbaarheid webshops en overheidswebsites

Bijna 80 procent van de 15-plussers gaf aan in de afgelopen twaalf maanden getwijfeld te hebben aan de betrouwbaarheid van een webshop. Bij twijfel zochten de meesten van hen reviews over de webshop (76 procent) en/of verlieten de website of braken de online bestelling af (68 procent). Ruim de helft zei te controleren of ze met een echte webshop te maken hebben, bijvoorbeeld door te letten op een keurmerk. Ongeveer 20 procent trok de website na, bijvoorbeeld op politie.nl of op checkjelinkje.nl, en een vergelijkbaar deel betaalde met creditcard, PayPal of achteraf betalen.

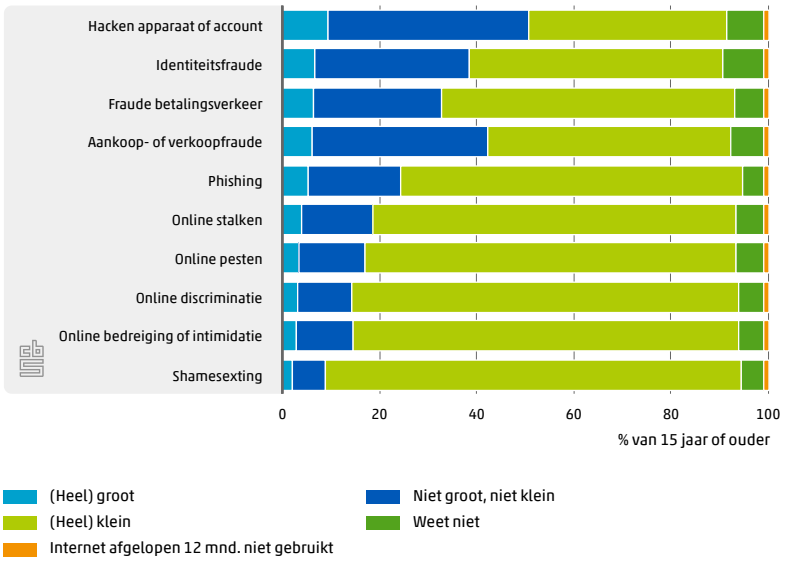
Aan de betrouwbaarheid van een overheidswebsite had 17 procent in de voorafgaande twaalf maanden weleens getwijfeld.

Inschatting kans op slachtofferschap online criminaliteit

Vooral als het gaat om online bedreiging en intimidatie schatten mensen de kans om hiervan zelf slachtoffer te worden relatief laag in. Bijna 10 procent achtte de kans aanwezig (dat wil zeggen '(heel) groot' of 'niet groot, niet klein') om zelf slachtoffer te worden van shamesexting en ongeveer 15 procent van online pesten, bedreiging of discriminatie. Bij online stalken was dit bijna 20 procent. Ruim 40 procent van de bevolking achtte de kans aanwezig om zelf slachtoffer te worden van aan- of verkoopfraude en ongeveer de helft van hacken.

In 2024 werd de kans om slachtoffer te worden van identiteitsfraude en fraude betalingsverkeer vaker (heel) groot ingeschat dan in 2022. Dat gold ook voor online pesten en online discriminatie.

3.5.2 Inschatting kans op slachtofferschap online criminaliteit, 2024

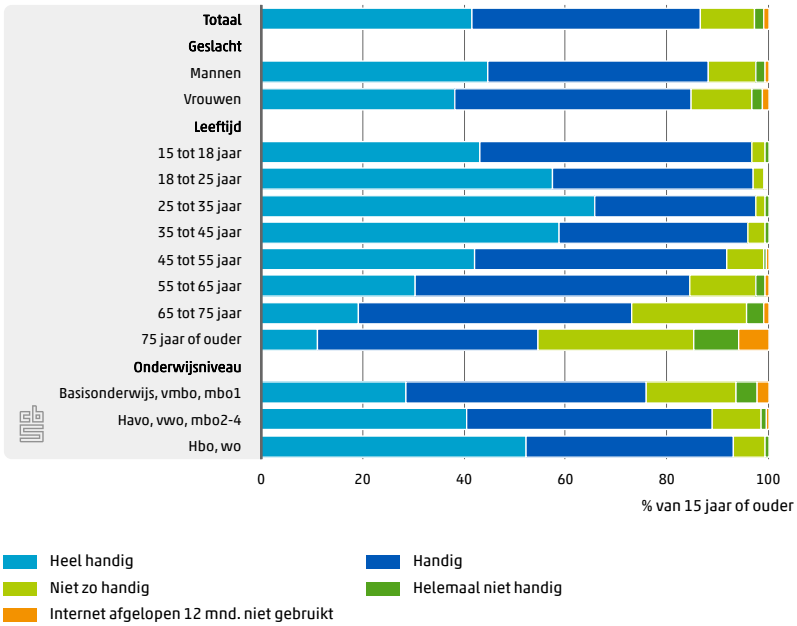


3.6 Online vaardigheden, hulp en informatiebehoefte

Inschatting eigen online vaardigheden

De meeste 15-plussers vonden zichzelf (heel) handig in het online opzoeken en regelen van dingen: 45 procent vond zichzelf handig en 42 procent heel handig. Slechts 2 procent gaf aan helemaal niet handig te zijn en 11 procent vond zichzelf niet zo handig. Vooral 25- tot 35-jarigen (66 procent), mannen (45 procent) en mensen met een afgeronde hbo- of universitaire opleiding (52 procent) vonden zichzelf heel handig in het online opzoeken en regelen van dingen. Vrouwen, 75-plussers, en mensen met een afgerond basisonderwijs, vmbo of mbo1 vonden zichzelf het vaakst helemaal niet handig.

3.6.1 Inschatting eigen online vaardigheden naar persoonskenmerken, 2024



Op de vraag wat mensen doen als ze een probleem hebben met het online regelen van dingen of met een computerprogramma of app, antwoordde 57 procent dat ze dit meestal alleen oplossen. 40 procent vroeg meestal of altijd iemand om hulp. Slechts 3 procent gaf aan ooit problemen te ervaren bij het online regelen van dingen.

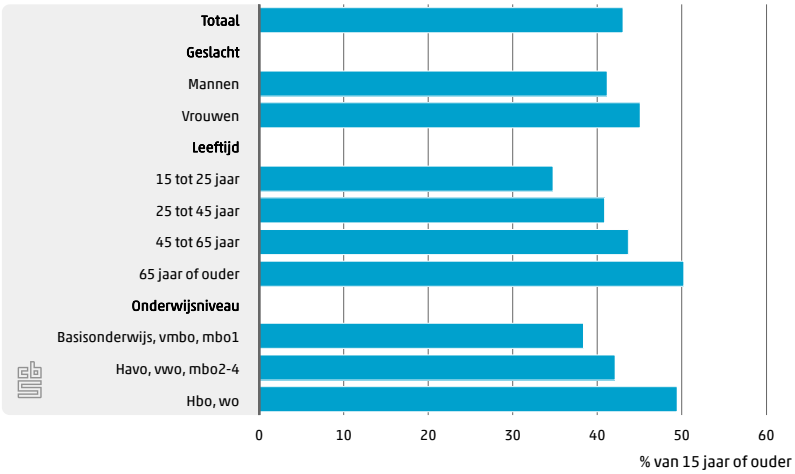
Diensten waar men terecht kan als men hulp nodig heeft

Het Informatiepunt Digitale Overheid (in de bibliotheek) was de meest bekende dienst waar iemand terecht kan voor hulp bij het online regelen van dingen of bij het gebruik van een computerprogramma of app. Deze dienst kende 34 procent van naam en 2 procent heeft weleens om hulp gevraagd bij het Informatiepunt Digitale Overheid. DigiHulplijn en Veiliginternetten.nl waren minder bekende diensten: 15 procent kende de naam van DigiHulplijn en 18 procent de naam van Veiliginternetten.nl. Bij beide diensten heeft 1 procent weleens om hulp gevraagd.

Behoefte aan voorlichting over online criminaliteit

Ruim 40 procent van de 15-plussers gaf aan behoefte te hebben aan informatie of voorlichting om zichzelf beter te beschermen tegen online criminaliteit. Vrouwen gaven dit vaker aan dan mannen (45 tegen 41 procent). De minste behoefte hebben 15- tot 25-jarigen, 65-plussers hebben de meeste behoefte aan voorlichting. Hbo- of universitair geschoolden hebben meer behoefte aan informatie dan personen met een ander onderwijsniveau.

3.6.2 Behoefte aan voorlichting naar persoonskenmerken, 2024



Op de vraag waaraan mensen behoefte hebben om zich beter te kunnen beschermen tegen online criminaliteit, antwoordde 31 procent meer informatie te willen over beschermende maatregelen die zij zelf kunnen nemen. Iets meer dan 20 procent had behoefte aan meer informatie over hoe oplichters te werk gaan en waar men op moet letten. Eenzelfde deel (21 procent) gaf aan duidelijkheid te willen over waar men meer informatie over online criminaliteit kan vinden. Meer informatie over de verschillende vormen van online criminaliteit en hulp bij het nemen van beschermende maatregelen werden minder vaak genoemd.

[1)] *Privacy gaat om de controle over persoonlijke informatie.*

4. Online oplichting en fraude

Bijna alle mensen van 15 jaar of ouder maken gebruik van het internet. Het merendeel doet online aankopen, bankiert online en maakt gebruik van social media (zie hoofdstuk 2). Dit maakt ze aantrekkelijk én kwetsbaar voor oplichting door cybercriminelen. Hierover gaat dit hoofdstuk. Hoeveel mensen werden in 2024 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 ergens gemeld of bij de politie aangegeven wat hen overkomen is?

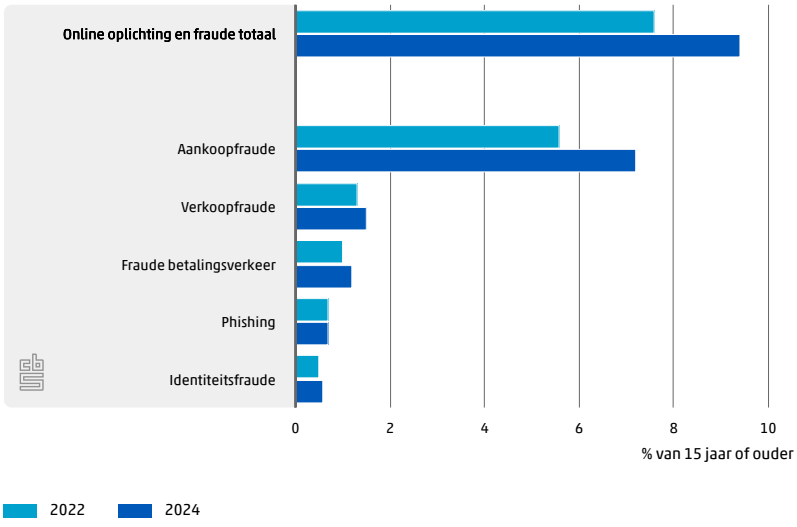
In de Tabellenset 2024 die bij deze publicatie hoort, zijn alle resultaten van dit hoofdstuk opgenomen bij '4 Oplichting en fraude', '4 Gevolgen, melding, aangifte' en '4 Overige details'.

4.1 Slachtoffers online oplichting en fraude

In 2024 werd ruim 9 procent van de bevolking van 15 jaar of ouder (1,4 miljoen personen) slachtoffer van één of meerdere vormen van online oplichting en fraude. Dat is meer dan in 2022, toen bijna 8 procent slachtoffer werd. Het verschil is vrijwel helemaal toe te schrijven aan het verhoogde slachtofferschap van aankoopfraude.

Aankoopfraude kwam met 7 procent het vaakst voor. Van verkoopfraude werd 1 procent slachtoffer, fraude in het betalingsverkeer overkwam 1 procent en van phishing en identiteitsfraude werd krap 1 procent slachtoffer.

4.1.1 Slachtoffers online oplichting en fraude



Slachtoffer online oplichting en fraude naar persoonskenmerken

Van de 65-plussers werd 6 procent slachtoffer van oplichting, tegenover 9 tot 11 procent van de leeftijdsgroepen tussen 15 en 65 jaar. Dit patroon, dat mensen ouder dan 65 jaar minder vaak slachtoffer worden dan jongere leeftijdsgroepen, is met name te zien bij aankoopfraude, verkoopfraude en identiteitsfraude. Ook mensen in huishoudens met de laagste welvaart werden vaker slachtoffer dan mensen in meer welvarende huishoudens.

4.1.2 Slachtoffers online oplichting en fraude naar persoonskenmerken, 2024 (%)

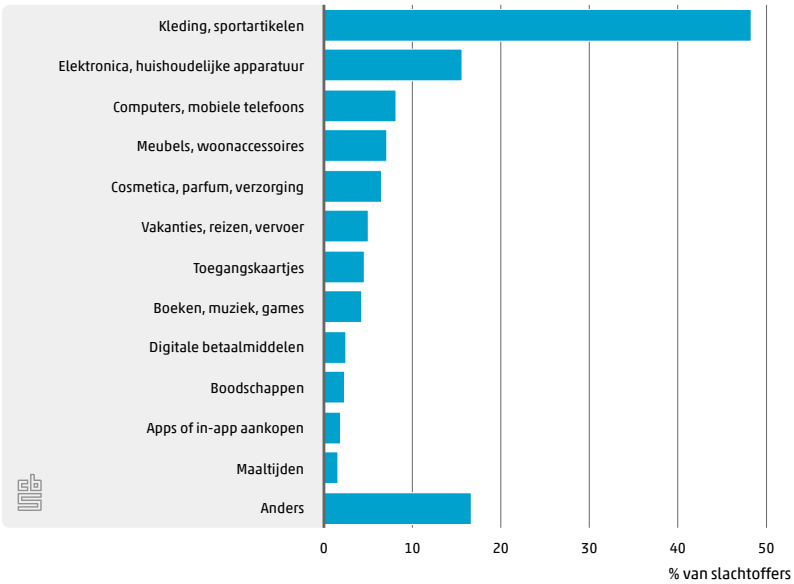
	Totaal	Aankoopfraude	Verkoopfraude	Fraude betalingsverkeer	Identiteitsfraude	Phishi
Totaal	9,4	7,2	1,5	1,2	0,6	(
Geslacht: Mannen	9,2	6,9	1,5	1,3	0,7	(
Geslacht: Vrouwen	9,5	7,5	1,4	1,1	0,5	(
Leeftijd: 15 tot 25 jaar	9,2	7,2	2,1	0,8	0,8	(
Leeftijd: 25 tot 45 jaar	10,8	8,2	1,9	1,3	0,9	(
Leeftijd: 45 tot 65 jaar	10,2	8,1	1,3	1,3	0,6	(
Leeftijd: 65 jaar of ouder	6,5	4,9	0,7	1,1	0,3	(
Onderwijsniveau: Basisonderwijs, vmbo, mbo1	9,0	6,9	1,8	1,0	0,7	(
Onderwijsniveau: Havo, vwo, mbo2-4	9,4	7,5	1,3	1,1	0,5	(
Onderwijsniveau: Hbo, wo	9,3	6,9	0,9	1,4	0,6	(
Welvaart huishouden: 1e 20%-groep (laagst)	10,6	8,0	2,9	0,9	0,7	(
Welvaart huishouden: 2e 20%-groep	9,9	7,8	1,6	1,2	0,8	(
Welvaart huishouden: 3e 20%-groep	9,5	7,3	1,4	1,2	0,7	(
Welvaart huishouden: 4e 20%-groep	8,7	6,8	1,1	1,3	0,4	(
Welvaart huishouden: 5e 20%-groep (hoogst)	8,8	6,8	1,0	1,2	0,5	(

Slachtofferschap aan- en verkoopfraude

In 2024 werd 7 procent slachtoffer van aankoopfraude: online bestellingen werden betaald, maar nooit geleverd. De meeste slachtoffers (74 procent) werden één keer slachtoffer van deze vorm van fraude, 26 procent vaker.

Bij 48 procent van de slachtoffers van aankoopfraude ging het om kleding, sportartikelen, schoenen of (kleding)accessoires. Daarnaast ging het bij 16 procent van de slachtoffers om elektronica of huishoudelijke apparatuur. Ook computers, tablets, mobiele telefoons of bijbehorende accessoires werden relatief vaak besteld maar niet ontvangen (8 procent).

4.1.3 Aankoopfraude: producten en diensten[1)], 2024



[1)]Meerdere antwoorden mogelijk.

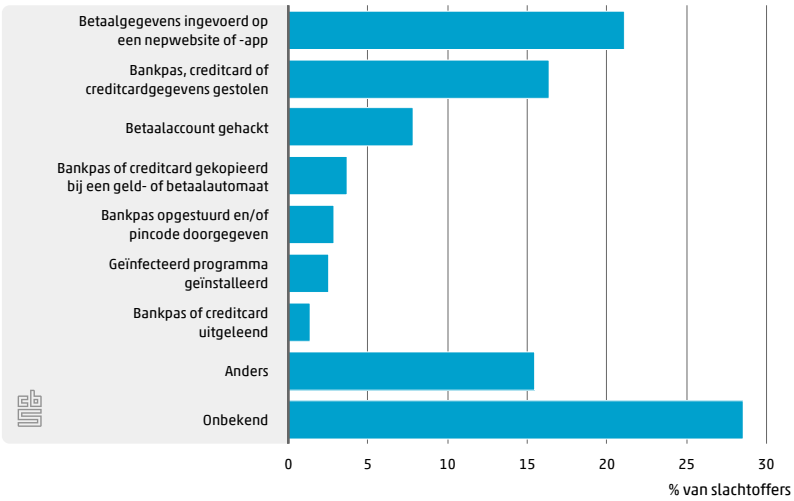
In 2024 werd 1 procent slachtoffer van verkoopfraude: producten werden online verkocht maar nooit betaald. De meeste slachtoffers (69 procent) werden één keer slachtoffer van deze vorm van fraude, 31 procent vaker.

Diensten waar men terecht kan als men hulp nodig heeft

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 (21 procent). Verder zei 16 procent dat de bankpas, creditcard of creditcardgegevens waren gestolen en noemde 8 procent het hacken van het betaalaccount. De andere manieren van fraude in het betalingsverkeer werden minder vaak genoemd. Voor de grootste groep slachtoffers, namelijk 29 procent, was het niet duidelijk hoe de fraude tot stand was gekomen.

4.1.4 Fraude betalingsverkeer: methode delict, 2024

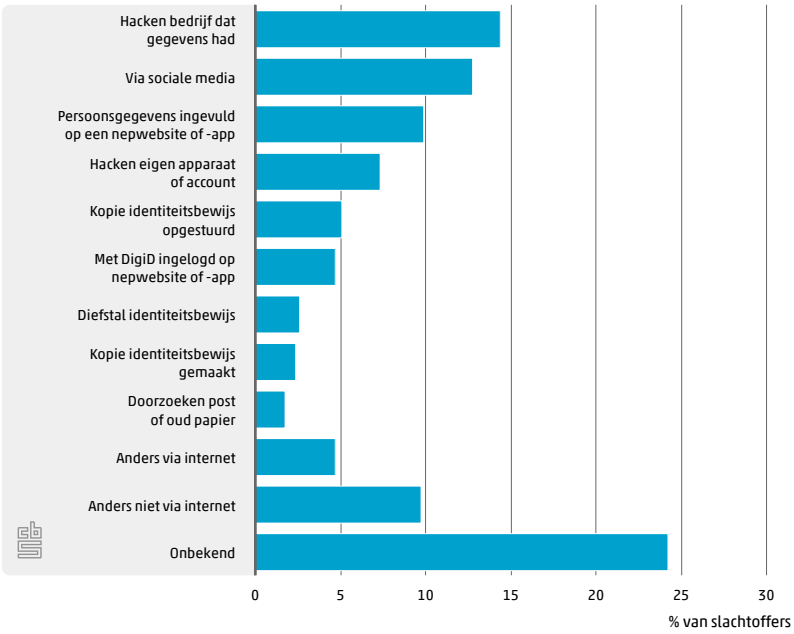


Slachtofferschap identiteitsfraude

Krap 1 procent van de 15-plussers gaf aan in 2024 slachtoffer te zijn geweest van identiteitsfraude. Dat wil zeggen dat iemand anders illegaal gebruik heeft gemaakt van de persoonsgegevens van het slachtoffer.

Bij ruim de helft van de slachtoffers van identiteitsfraude kwam de dader via internet aan de gegevens. Een hack van een bedrijf dat gegevens had opgeslagen of via social media waren de meest genoemde manieren waarop de gegevens van het slachtoffer werden gestolen. Respectievelijk 14 en 13 procent van de slachtoffers zei dat dit was hoe de dader aan de gegevens kwam. Bijna een kwart van de slachtoffers wist niet hoe de dader aan de gegevens is gekomen.

4.1.5 Identiteitsfraude: methode delict, 2024

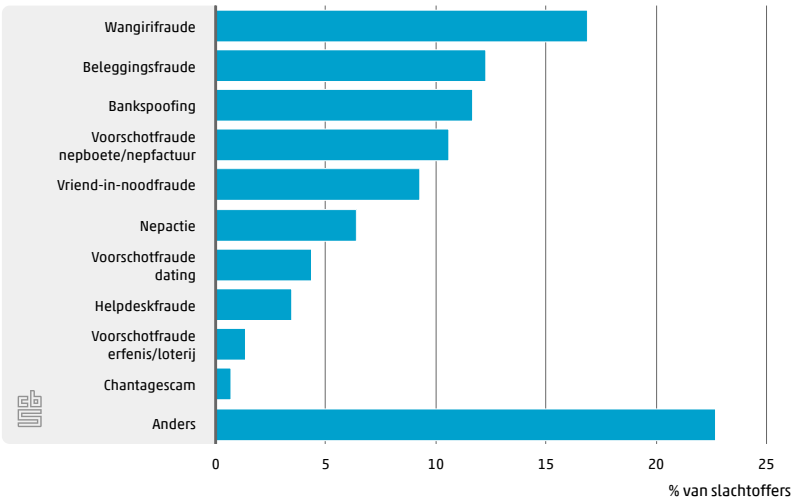


Slachtofferschap phishing

Krap 1 procent van de mensen werd in 2024 slachtoffer van phishing. Bij phishing gaat het om het kwijtraken van geld aan een oplichter die zich voordoet als iemand anders of een vertrouwde instantie.

Bij 17 procent van de slachtoffers ging het om wangirifraude: de dader probeert het slachtoffer te laten terugbellen naar dure betaalnummers. Verder kreeg 12 procent te maken met beleggingsfraude en eenzelfde deel werd slachtoffer van bankspoofing, waarbij de oplichter zich voordoet als een bankmedewerker. Nepboetes of nepfacturen werden door 11 procent van de slachtoffers genoemd. Vriend-in-nood-fraude, waarbij iemand geld betaalde aan een zogenaamde bekende (via een nepbericht of voice cloning), en nepacties troffen respectievelijk 9 en 6 procent van de slachtoffers. De andere vormen van phishing werden door 4 procent of minder genoemd.

4.1.6 Phishing: methode delict, 2024



Voice cloning

Voice cloning is een relatief nieuwe vorm van online criminaliteit, die gebruikmaakt van een kopie van iemands stem (Politie, 2024). Hierbij wordt een korte opname van iemands stem gebruikt om een computerprogramma via kunstmatige intelligentie (AI, *artificial intelligence*) te leren spreken met een stem die precies klinkt als die persoon.

Wanneer deelnemers aan OVeC 2024 aangaven dat zij slachtoffer waren van vriend-in-nood-fraude, werd hen gevraagd op welke manier zij waren opgelicht. In de meeste gevallen (98 procent) was dit met een nepbericht via bijv. WhatsApp of een sms. Slechts 2 procent van deze vorm van oplichting gebeurde via voice cloning.

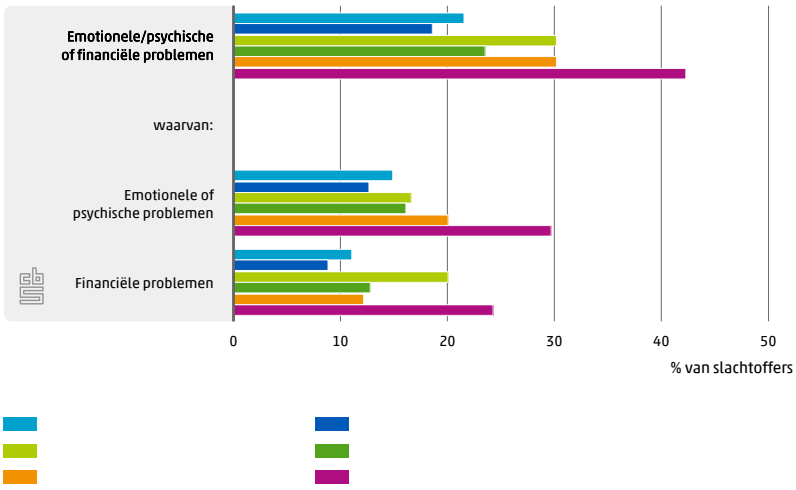
4.2 Gevolgen online oplichting en fraude

Problemen voor slachtoffers

Ruim een vijfde van de slachtoffers gaf aan problemen te hebben (gehad) door de online oplichting en fraude. Bij 15 procent ging het om emotionele of psychische problemen en bij 11 procent om financiële problemen.

Slachtoffers van phishing gaven het vaakst aan dat zij problemen hadden ondervonden: bij 30 procent ging het om emotionele of psychische problemen en bij 24 procent om financiële problemen. Emotionele en psychische problemen werden ook relatief vaak door slachtoffers van identiteitsfraude genoemd, financiële problemen juist relatief vaak door slachtoffers van verkoopfraude.

4.2.1 Problemen door online oplichting en fraude[1)], 2024

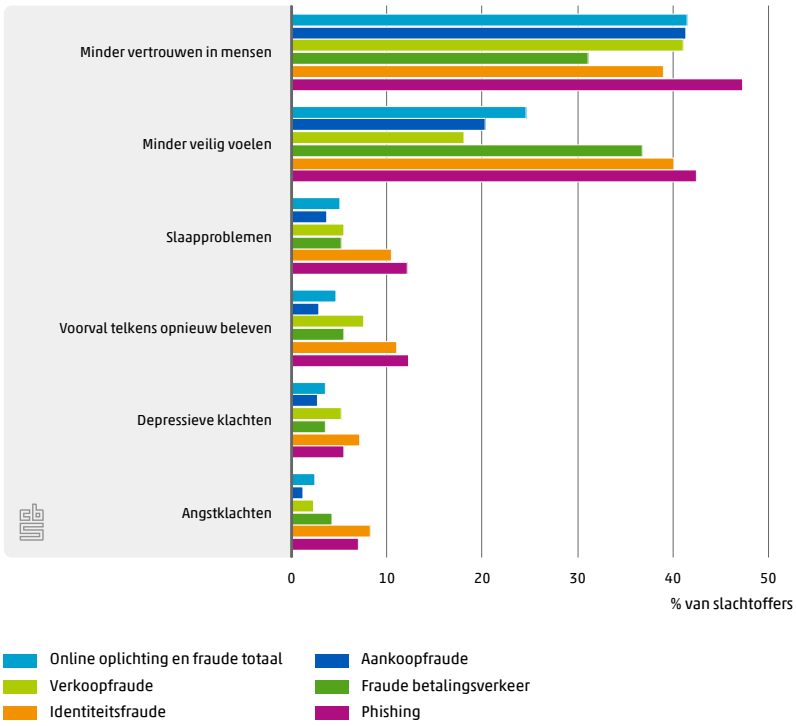


Emotionele of psychische gevolgen

Ruim 40 procent van de slachtoffers van online oplichting en fraude gaf aan minder vertrouwen in mensen te hebben door wat hen was overkomen en bijna 25 procent voelde zich er minder veilig door. Ongeveer 5 procent zei het voorval telkens opnieuw te beleven of had slaapproblemen. Angstklachten en depressieve klachten werden elk door minder dan 4 procent van de slachtoffers genoemd.

Vooral slachtoffers van identiteitsfraude en phishing ervoeren na het voorval psychische en emotionele klachten, zoals het voorval telkens opnieuw beleven, slaapproblemen, angst en depressieve klachten. Bij aan- en verkoopfraude en fraude in het betalingsverkeer was dit minder vaak het geval.

4.2.2 Emotionele of psychische gevolgen online oplichting en fraude[1)], 2024



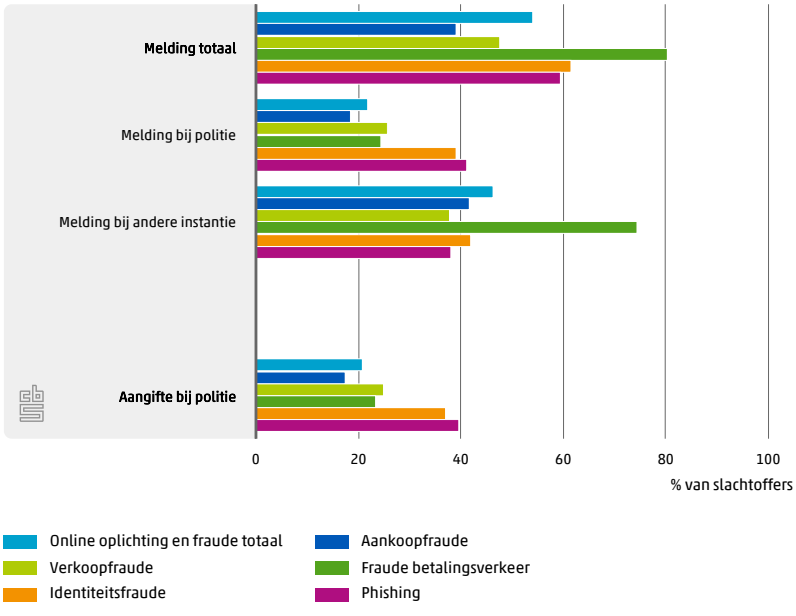
[1)] Meerdere antwoorden mogelijk.

4.3 Melding en aangifte online oplichting en fraude

Ruim de helft van de slachtoffers van online oplichting en fraude maakte melding van hetgeen hen overkomen was. Bij de politie meldde 22 procent het voorval en bij een andere instantie 47 procent. Een vijfde van de slachtoffers (21 procent) deed aangifte.

De meldings- en aangiftebereidheid wisselt sterk tussen de verschillende soorten delicten. Zo werd aankoopfraude door bijna 40 procent van de slachtoffers ergens gemeld en deed 18 procent aangifte bij de politie. Fraude in het betalingsverkeer werd door 80 procent van de slachtoffers gemeld bij een instantie (bijvoorbeeld de politie of de bank) en 23 procent deed aangifte bij de politie.

4.3.1 Melding en aangifte online oplichting en fraude[1)], 2024



[1)] Meerdere antwoorden mogelijk.

Ruim de helft (55 procent) van de slachtoffers die aangifte deden, deed dit via internet. Een kwart van de slachtoffers deed aangifte op het politiebureau en 16 procent telefonisch.

Redenen geen melding of aangifte bij politie

De meest genoemde redenen om geen melding of aangifte bij de politie te doen waren dat 'het toch niets helpt' (37 procent) en dat 'er niet aan gedacht was/het niet zo belangrijk was' (34 procent). Bij fraude in het betalingsverkeer werd verder vaak als reden gegeven dat de financiële schade al vergoed was of dat het al was opgelost. Ook bij identiteitsfraude werd relatief vaak aangegeven dat het al was opgelost.

5. Hacken

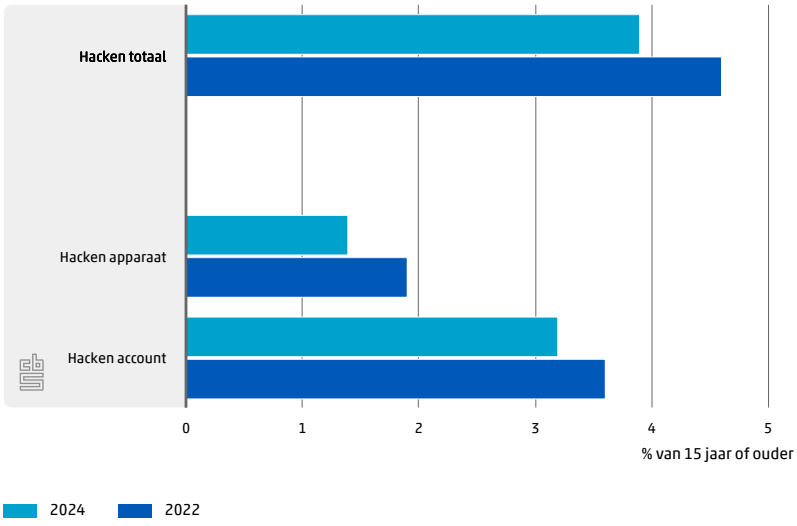
In het vorige hoofdstuk werd stilgestaan bij online oplichting en fraude. Een andere vorm van online criminaliteit waar mensen relatief vaak slachtoffer van worden is hacken. Hierbij verschaft iemand zich toegang tot een apparaat (zoals een computer of tablet) of account (zoals een e-mail- of bankaccount), zonder dat de eigenaar hiervoor toestemming heeft gegeven. In dit hoofdstuk gaat het alleen om apparaten en accounts die voor privédoeleinden worden gebruikt. Hoeveel mensen werden slachtoffer van hacken in 2024? Welke beveiligingsmaatregelen treffen slachtoffers? Wat waren de gevolgen van de hack voor de slachtoffers? En hebben ze het voorval gemeld of aangegeven bij de politie?

In de Tabellenset 2024 die bij deze publicatie hoort, zijn alle resultaten van dit hoofdstuk opgenomen bij '5 Hacken', '5 Gevolgen', '5 Melding, aangifte' en '5 Overige details'.

5.1 Slachtoffers van hacken

In 2024 gaf 4 procent van de bevolking van 15 jaar of ouder (580 duizend personen) aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van hacken van een apparaat of account. Dat was lager dan in 2022 toen een kleine 5 procent dit aangaf. Net als in 2022 werd een account in 2024 vaker gehackt dan een apparaat (3 tegen 1 procent).

5.1.1 Slachtoffers hacken



Slachtoffers hacken naar persoonskenmerken

Jongeren van 15 tot 25 jaar waren met 5 procent het vaakst slachtoffer van hacken, 65-plussers het minst vaak (3 procent). Het verschil tussen jongeren en ouderen was met name te zien bij het hacken van een account. Geslacht, onderwijsniveau en het welvaartsniveau van het huishouden waren nauwelijks onderscheidend.

5.1.2 Slachtofferschap hacken naar persoonskenmerken, 2024 (%)

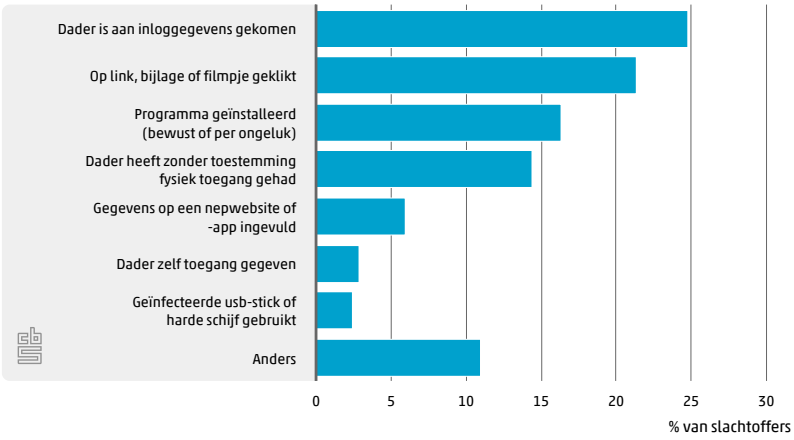
	Totaal	Hacken apparaat	Hacken account
Totaal	3,9	1,4	3,2
Geslacht: Mannen	3,9	1,4	3,3
Geslacht: Vrouwen	3,8	1,4	3,2
Leeftijd: 15 tot 25 jaar	5,3	1,8	4,5
Leeftijd: 25 tot 45 jaar	4,5	1,1	4,0
Leeftijd: 45 tot 65 jaar	3,5	1,4	2,9
Leeftijd: 65 jaar of ouder	2,7	1,5	1,8
Onderwijsniveau: Basisonderwijs, vmbo, mbo1	3,9	1,9	3,1
Onderwijsniveau: Havo, vwo, mbo2-4	4,0	1,4	3,4
Onderwijsniveau: Hbo, wo	3,8	1,0	3,3
Welvaart huishouden: 1e 20%-groep (laagst)	4,7	2,0	4,0
Welvaart huishouden: 2e 20%-groep	4,1	1,7	3,4
Welvaart huishouden: 3e 20%-groep	3,6	1,4	2,8
Welvaart huishouden: 4e 20%-groep	3,4	1,0	2,9
Welvaart huishouden: 5e 20%-groep (hoogst)	3,9	1,2	3,3

Slachtofferschap hacken apparaat

Apparaten die het vaakst werden gehackt, zijn de smartphone (49 procent) en de computer/laptop (42 procent). Een tablet, smartwatch, wifi-router of huishoudelijk apparaat werden minder vaak gehackt.

Het vaakst werd men slachtoffer van een hack doordat de dader aan de inloggegevens is gekomen: 25 procent van de slachtoffers gaf dit aan. Ook op een link, bijlage of filmpje klikken werd relatief vaak als oorzaak genoemd (21 procent). De dader zelf toegang geven tot het apparaat of het gebruik van een geïnfecteerde usb-stick of harde schijf werden het minst vaak genoemd.

5.1.3 Hacken apparaat: manier waarop slachtoffer geworden[1)], 2024



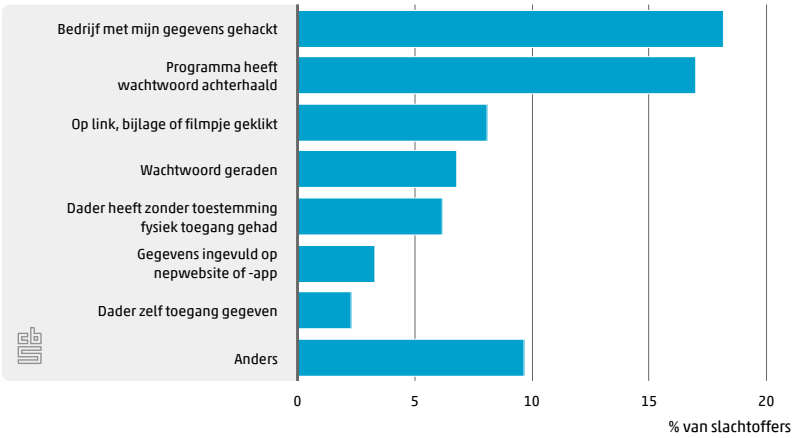
[1)] Meerdere antwoorden mogelijk.

Slachtofferschap hacken account

Bij het hacken van accounts ging het in de meeste gevallen om een social media account (bijvoorbeeld Facebook, Instagram, WhatsApp, LinkedIn of X): 44 procent van de slachtoffers gaf aan dat dit type account was gehackt. Ook het e-mailaccount werd relatief vaak door slachtoffers genoemd (34 procent).

Accounts werden het vaakst gehackt met inloggegevens verkregen via het hacken van een bedrijf dat deze gegevens bewaarde: 18 procent van de slachtoffers gaf aan dat hun account op deze manier was gehackt. Ook een programma dat het wachtwoord heeft achterhaald werd vaak als oorzaak genoemd (17 procent). Het zelf invullen van gegevens op een nepwebsite/-app of de dader zelf toegang geven tot het account werden het minst vaak als de oorzaak van de hack genoemd.

5.1.4 Hacken account: manier waarop slachtoffer geworden[1)], 2024



[1)] Meerdere antwoorden mogelijk.

5.2 Beveiligingsmaatregelen voor en na slachtofferschap hacken

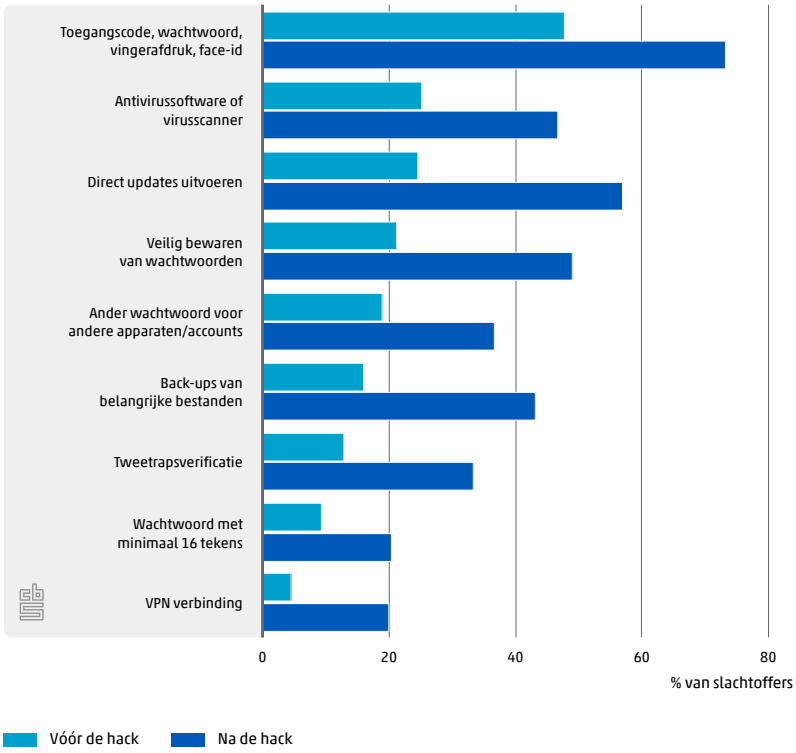
Het niet nemen van beveiligingsmaatregelen om een apparaat of account te beschermen was in de meeste gevallen niet de oorzaak van een gehackt apparaat of account. Toch is de kans om slachtoffer te worden van een hack kleiner als er wel beveiligingsmaatregelen worden genomen.

Beveiligingsmaatregelen voor en na hacken apparaat

Aan slachtoffers van een gehackt apparaat is gevraagd welke beveiligingsmaatregelen ze hadden genomen vóórdat dit apparaat gehackt werd. Het apparaat werd door 48 procent vergrendeld met een toegangscode, wachtwoord, vingerafdruk of Face ID. Verder gebruikte 25 procent antivirussoftware of een virusscanner en voerde eveneens 25 procent updates direct uit. Van de slachtoffers bewaarde 21 procent hun wachtwoorden veilig, en 19 procent gebruikte verschillende wachtwoorden. 16 procent gaf aan geen van de genoemde maatregelen te hebben genomen om het apparaat te beveiligen.

Er is ook aan slachtoffers gevraagd welke beveiligingsmaatregelen zij altijd of vaak namen op het moment dat de enquête werd afgenomen. Dit is per definitie nadat de hack heeft plaatsgevonden. Na het hacken van hun apparaat zijn slachtoffers vaker beveiligingsmaatregelen gaan nemen[2)3)]. Waar vóór de hack 48 procent van de (latere) slachtoffers het apparaat met een toegangscode vergrendelde, lag het aandeel dat zei dit te doen na de hack op 73. Vóór de hack voerde 25 procent direct updates uit, na slachtoffer te zijn geweest was dit 58 procent. Ook het veilig bewaren van wachtwoorden gebeurde aanzienlijk vaker: 21 procent deed dit vóór gehackt te zijn, 49 procent erna. En ook de andere beveiligingsmaatregelen werden na de hack vaker getroffen

5.2.1 Maatregelen voor en na hacken apparaat[1)], 2024



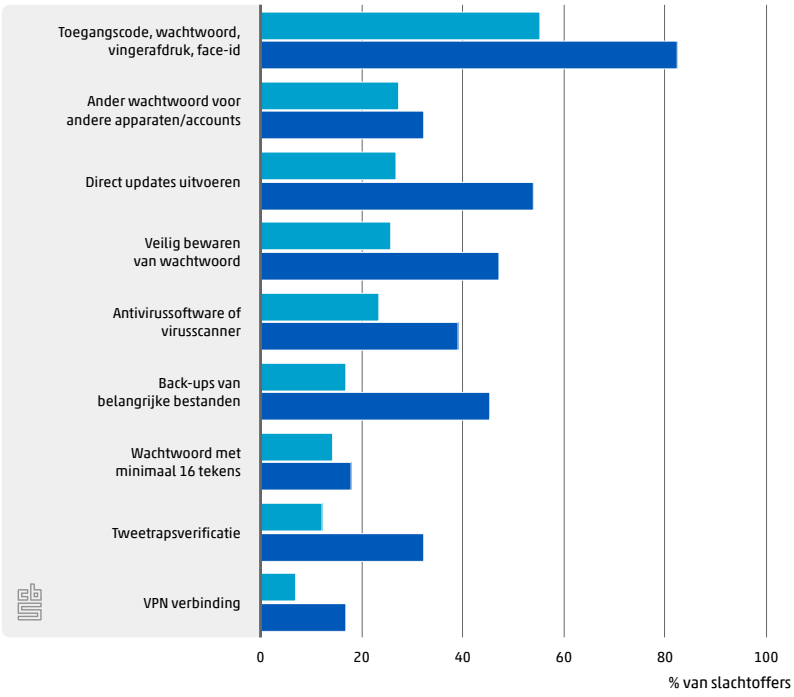
[1)] Meerdere antwoorden mogelijk.

Beveiligingsmaatregelen voor en na hacken account

Voordat het account werd gehackt, gebruikte 55 procent van de slachtoffers een wachtwoord of toegangscode om het account te vergrendelen. Van verschillende wachtwoorden voor apparaten en accounts maakte 28 procent van de slachtoffers gebruik, 27 procent voerde direct updates uit en 26 procent bewaarde hun wachtwoord veilig. Ruim 10 procent nam geen van de beveiligingsmaatregelen vóór de hack.

Waar vóór het hacken van het account 55 procent aangaf gebruik te maken van accountvergrendeling, was dit na de hack (op het moment van enquêteren) met 82 procent hoger. Ook de meeste andere maatregelen werden duidelijk vaker getroffen, behalve het kiezen van verschillende wachtwoorden voor verschillende accounts en het kiezen van lange wachtwoorden.

5.2.2 Maatregelen voor en na hacken account[1)], 2024



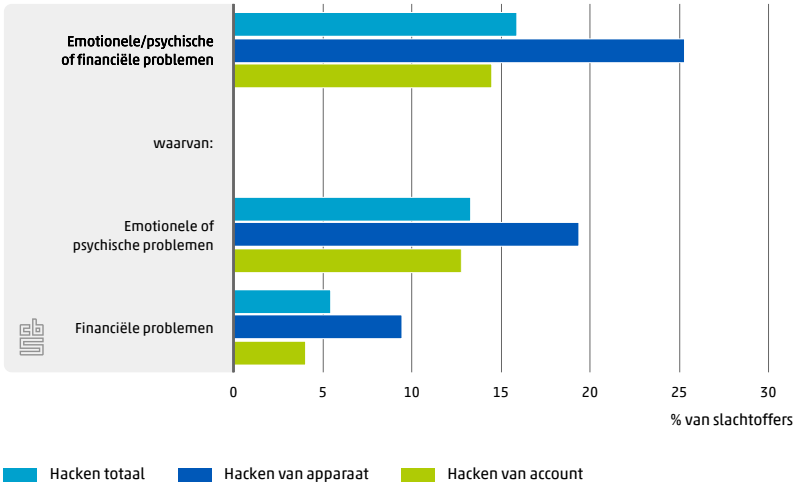
[1)] Meerdere antwoorden mogelijk.

5.3 Gevolgen hacken

Problemen voor slachtoffers

Van de slachtoffers van hacken gaf 16 procent aan emotionele en/of financiële problemen te hebben ondervonden als gevolg van de hack. Emotionele en/of psychische problemen werden vaker genoemd dan financiële problemen (14 tegen 5 procent). Het hacken van een apparaat leidde vaker tot problemen dan het hacken van een account: 25 tegenover 14 procent.

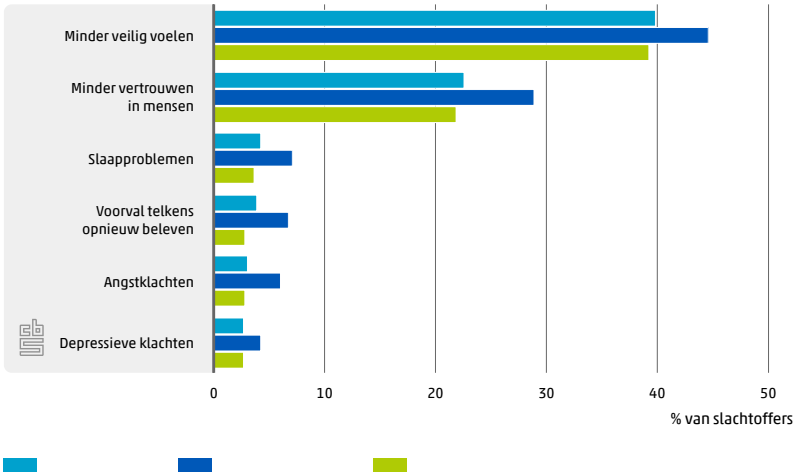
5.3.1 Problemen door hacken[1)], 2024



[1)] Meerdere antwoorden mogelijk.

Emotionele of psychische gevolgen

Minder veilig voelen (40 procent) en minder vertrouwen in andere mensen (23 procent) waren de gevolgen die slachtoffers van een gehackt apparaat of account het vaakst noemden. Slaapproblemen, angstklachten, depressieve klachten en het voorval steeds opnieuw beleven werden elk door ongeveer 3 à 4 procent genoemd. Het voorkomen van emotionele of psychische gevolgen na de hack verschilde niet veel tussen slachtoffers van een gehackt apparaat en slachtoffers van een gehackt account.

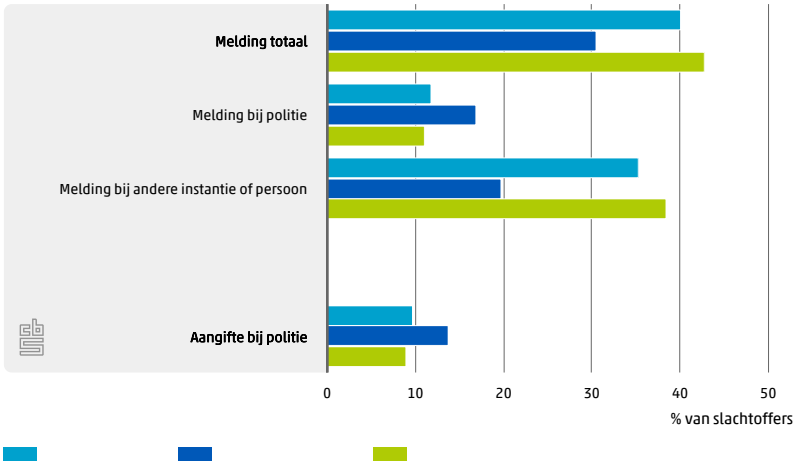


[1] Meerdere antwoorden mogelijk.

5.4 Melding en aangifte hacken

Van de slachtoffers van hacken heeft 40 procent dit bij de politie en/of een andere instantie gemeld: 12 procent bij de politie en 35 procent bij een andere instantie. Het gaat dan om bijvoorbeeld meld- of adviespunten, zoals Meld Misdaad Anoniem. Bij het hacken van accounts kan het ook de instantie zijn die het account beheert (bijvoorbeeld de bank of Google) of de internetprovider (bijvoorbeeld KPN of Vodafone).

Een groot deel van de meldingen van hacken bij de politie resulteerde in een aangifte (12 procent meldde het; 10 procent deed aangifte). Slachtoffers van een gehackt apparaat deden ongeveer even vaak melding en aangifte bij de politie als slachtoffers van een gehackt account. Slachtoffers van wie een account gehackt werd, meldden dit vaker bij een andere instantie dan de politie en dan met name bij de instantie die het gehackte account beheerde.



[1] Meerdere antwoorden mogelijk.

Slachtoffers van hacken deden het vaakst aangifte op het politiebureau (33 procent), gevolgd door aangifte via internet (26 procent) en telefonische aangifte (19 procent).

Redenen geen melding of aangifte bij politie

De meest genoemde reden om de hack niet bij de politie te melden of aan te geven was dat er niet aan wordt gedacht of dat men het niet zo belangrijk vond (47 procent). Daarna volgden 'het is al opgelost' (27 procent) en 'het helpt toch niets' (25 procent). Ruim 10 procent had geen zin of tijd, of vond het te veel moeite.

[2] 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 geldt. Aangenomen is dat dat niet zo is.

[3] Het is niet uit te sluiten dat personen die geen slachtoffer waren van een hack in de twaalf maanden voorafgaand aan het invullen van de enquête eveneens hun beveiligingsniveau hebben opgeschroefd, maar gegevens hierover ontbreken.

6. Online bedreiging en intimidatie

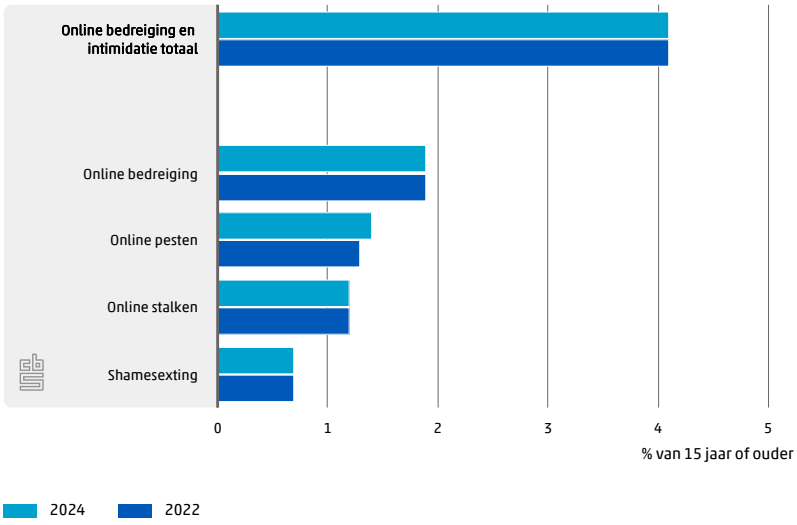
Het internet wordt niet alleen misbruikt om mensen op te lichten, te frauderen of om te hacken, maar ook om mensen te bedreigen en te intimideren. Het gaat dan om bedreiging, pesten, stalken en shamesexting. Bedreiging en intimidatie via internet verschilt van bedreiging en intimidatie in de fysieke 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. In dit hoofdstuk komt eerst 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.

In de Tabellenset 2024 die bij deze publicatie hoort', zijn alle resultaten van dit hoofdstuk opgenomen bij '6 Online bedreiging en intimidatie' en '6 Gevolgen, melding, aangifte'.

6.1 Slachtoffers online bedreiging en intimidatie

In 2024 gaf 4 procent van de bevolking van 15 jaar of ouder (620 duizend personen) aan in de afgelopen twaalf maanden slachtoffer zijn geweest van online bedreiging of intimidatie. Dit was vergelijkbaar met 2022. De meeste slachtoffers hadden te maken met online bedreiging (2 procent). Met online pesten en met online stalking had elk ruim 1 procent te maken. Van shamesexting, waarbij naaktfoto's of -filmpjes van het slachtoffer online worden verspreid of hiermee wordt gedreigd, werd krap 1 procent slachtoffer.

6.1.1 Slachtoffers online bedreiging en intimidatie



Slachtoffers online bedreiging en intimidatie naar persoonskenmerken

Mannen en vrouwen gaven ongeveer even vaak aan slachtoffer te zijn geweest van online bedreiging en intimidatie. Jongeren van 15 tot 25 jaar werden met 9 procent het vaakst slachtoffer, 65-plussers met 2 procent het minst vaak. Jongeren werden met name vaker slachtoffer van online bedreiging en online pesten. Homoseksuele mannen en bi-plus personen hadden gemiddeld twee keer zo vaak met online bedreiging en intimidatie te maken dan mensen met een andere seksuele oriëntatie.

6.1.2 Slachtofferschap online bedreiging en intimidatie naar persoonskenmerken, 2024 (%)

	Totaal	Online bedreiging	Online pesten	Online stalken	Shame-sexting
Totaal	4,1	1,9	1,4	1,2	0,7
Geslacht: Mannen	4,4	2,1	1,5	0,9	0,9
Geslacht: Vrouwen	3,9	1,7	1,4	1,4	0,5
Leeftijd: 15 tot 25 jaar	8,8	4,1	3,9	2,1	1,6
Leeftijd: 25 tot 45 jaar	4,7	1,7	1,9	1,4	0,9
Leeftijd: 45 tot 65 jaar	3,1	1,7	0,8	0,8	0,4
Leeftijd: 65 jaar of ouder	2,0	1,0	0,2	0,7	0,3
Geslacht, leeftijd: Mannen, 15 tot 25 jaar	8,3	3,6	4,0	0,9	1,9
Geslacht, leeftijd: Mannen, 25 tot 45 jaar	5,1	2,0	2,1	1,2	1,1
Geslacht, leeftijd: Mannen, 45 tot 65 jaar	3,3	2,0	0,7	0,7	0,5
Geslacht, leeftijd: Mannen, 65 jaar of ouder	2,6	1,3	0,3	0,9	0,6
Geslacht, leeftijd: Vrouwen, 15 tot 25 jaar	9,4	4,7	3,8	3,3	1,4
Geslacht, leeftijd: Vrouwen, 25 tot 45 jaar	4,3	1,4	1,7	1,6	0,6
Geslacht, leeftijd: Vrouwen, 45 tot 65 jaar	2,9	1,4	0,8	0,9	0,3
Geslacht, leeftijd: Vrouwen, 65 jaar of ouder	1,4	0,7	0,2	0,6	0,1
Onderwijsniveau: Basisonderwijs, vmbo, mbo1	4,3	1,9	1,8	1,4	0,9
Onderwijsniveau: Havo, vwo, mbo2-4	4,4	2,1	1,5	1,1	0,8
Onderwijsniveau: Hbo, wo	3,8	1,8	1,2	1,0	0,5
Seksuele oriëntatie: Heteroseksuele mannen	4,0	2,0	1,2	0,8	0,7
Seksuele oriëntatie: Heteroseksuele vrouwen	3,6	1,6	1,1	1,3	0,5
Seksuele oriëntatie: Homoseksuele mannen	9,4	4,1	5,0	2,4	2,1
Seksuele oriëntatie: Homoseksuele vrouwen	4,9	1,6	3,0	2,3	2,0
Seksuele oriëntatie: Bi-plus mannen	8,5	3,6	3,8	1,4	2,3
Seksuele oriëntatie: Bi-plus vrouwen	8,3	3,6	3,8	2,6	0,6
Seksuele oriëntatie: Aseksuele mannen	6,0	3,0	2,1	0,1	1,8
Seksuele oriëntatie: Aseksuele vrouwen	4,0	1,5	2,3	0,8	0,3

Slachtofferschap online seksuele intimidatie

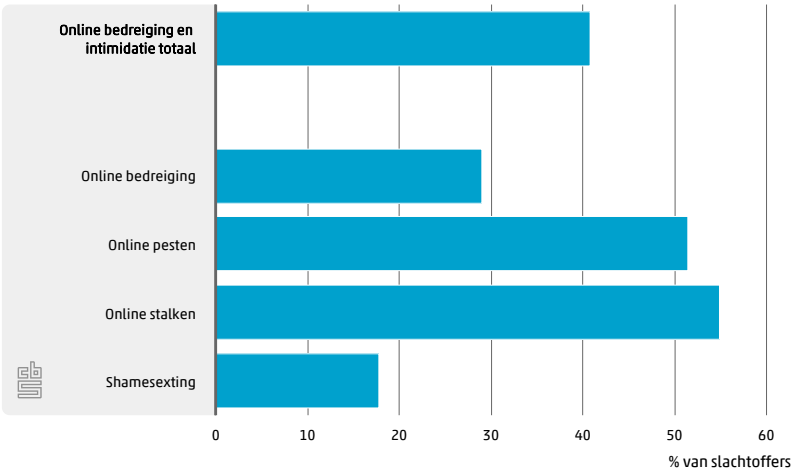
In de Prevalentiemonitor Huiselijk Geweld en Seksueel Grensoverschrijdend gedrag is aan mensen van 16 jaar of ouder gevraagd of zij te maken hebben gehad met online seksuele intimidatie (Derksen et al, 2024). Het gaat daarbij om ongewenste seksuele ervaringen die online plaatsvinden, uiteenlopend van het ontvangen van seksueel getinte opmerkingen via social media, WhatsApp, (video)chat of e-mail tot het gedwongen worden tot seksuele handelingen. In 2024 gaf 5 procent van de bevolking van 16 jaar of ouder (ruim 760 duizend personen) aan dit in de afgelopen twaalf maanden te hebben meegemaakt.

Vrouwen zeiden vaker dan mannen online seksuele intimidatie te hebben meegemaakt (6 tegen 4 procent). Jongeren waren hier duidelijk het vaakst slachtoffer van en dan met name jonge vrouwen: ruim 20 procent van de 16- tot 24-jarige vrouwen gaf aan hier in de afgelopen twaalf maanden mee te zijn geconfronteerd, tegenover ruim 7 procent van hun mannelijke leeftijdgenoten. Ook homoseksuele mannen en bi-plus vrouwen waren relatief vaak slachtoffer van online seksuele intimidatie.

6.2 Daders online bedreiging en intimidatie

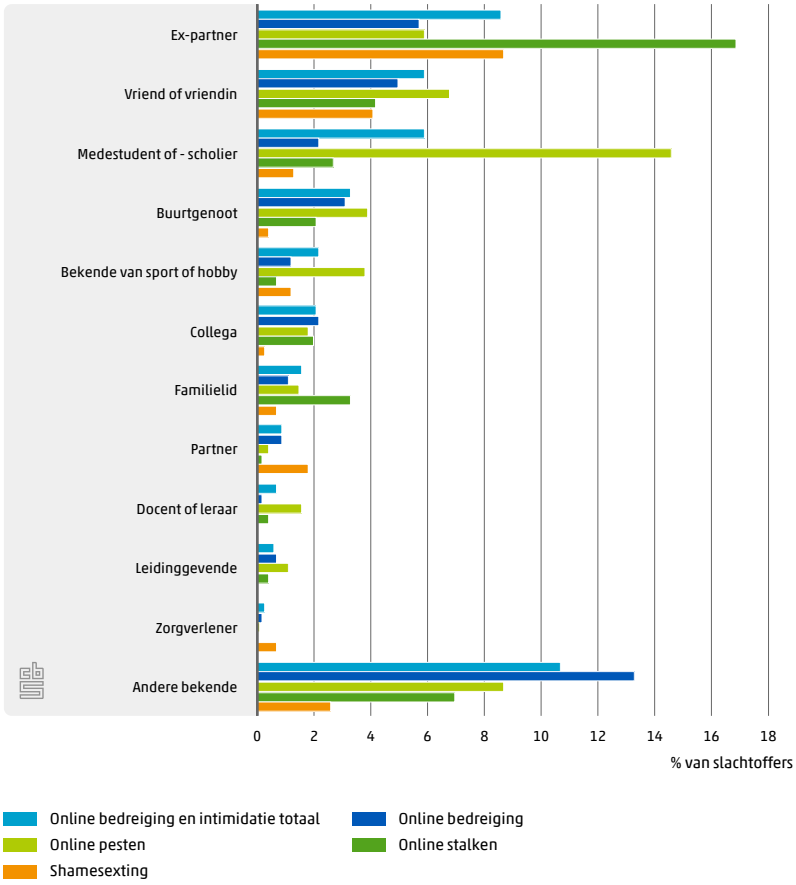
Bij 4 op de 10 slachtoffers van online bedreiging en intimidatie was de dader bekend. Bij pesten en stalken kende het slachtoffer de dader(s) het vaakst.

6.2.1 Kende dader(s) van online bedreiging en intimidatie, 2024



De meest genoemde daders waren de ex-partner, een vriend/vriendin of een medestudent/-scholier. De ex-partner werd bij online stalken het vaakst als dader genoemd door de slachtoffers (17 procent). Bij online pesten was dat een medestudent/-scholier (15 procent) en bij online bedreiging een andere bekende (13 procent).

6.2.2 Daders van online bedreiging en intimidatie[1)], 2024



[1)] Meerdere antwoorden mogelijk.

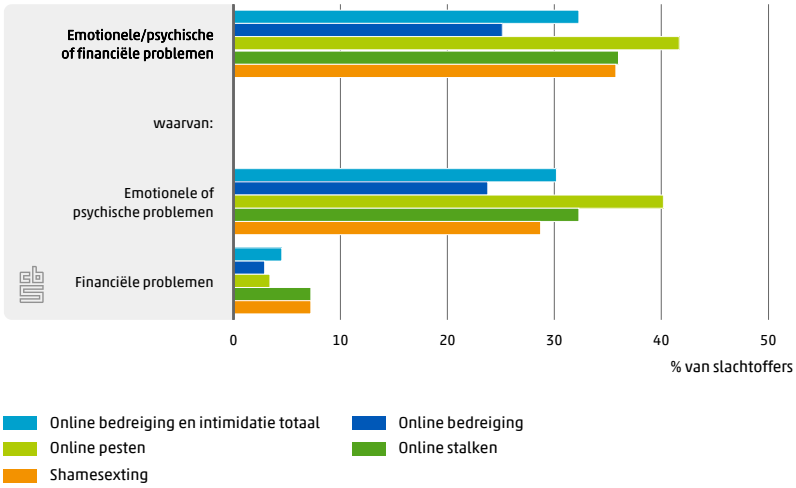
6.3 Gevolgen online bedreiging en intimidatie

Problemen voor slachtoffers

Bijna een derde (32 procent) van de slachtoffers van online bedreiging en intimidatie zei emotionele of psychische problemen dan wel financiële problemen te (hebben) gehad als gevolg van het voorval. Emotionele of psychische problemen werden door slachtoffers vaker genoemd dan financiële problemen (30 tegen 5 procent).

Slachtoffers van online pesten ervoeren het vaakst emotionele of psychische problemen (40 procent) en slachtoffers van online bedreiging het minst vaak (25 procent). Financiële problemen werden het vaakst genoemd bij online stalking en shamesexting, bij beide vormen door 7 procent van deze slachtoffers.

6.3.1 Problemen door online bedreiging en intimidatie[1)], 2024



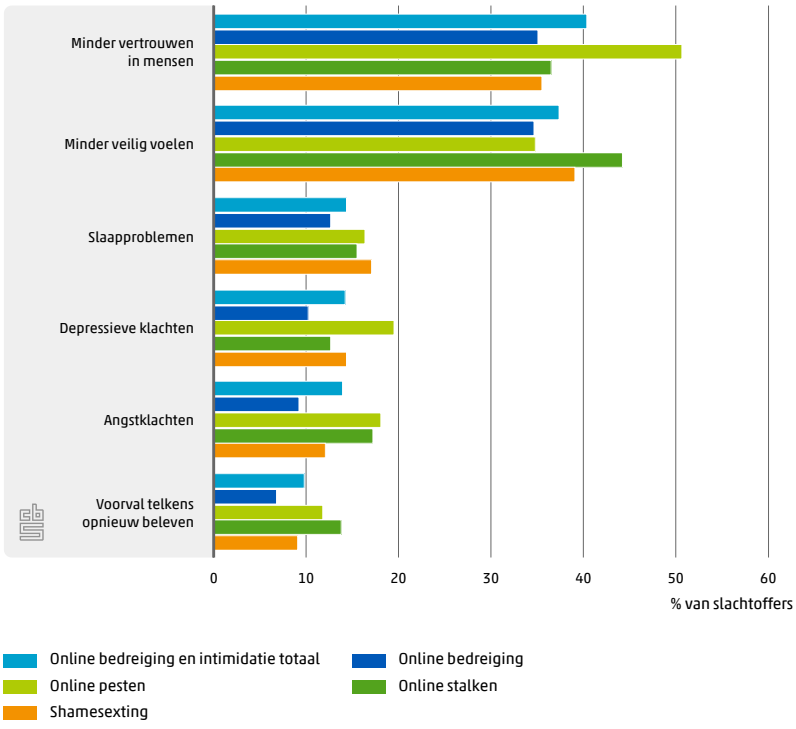
[1)] Meerdere antwoorden mogelijk.

Emotionele of psychische gevolgen

Voor de meeste slachtoffers van online bedreiging en intimidatie leidde het voorval ertoe dat men minder vertrouwen had in mensen (40 procent) en dat men zich minder veilig voelde (37 procent). Slaapproblemen, depressieve klachten, angstklachten en het voorval telkens opnieuw beleven werden minder vaak genoemd.

Slachtoffers van online stalken gaven het vaakst aan zich minder veilig te voelen door het voorval. Minder vertrouwen hebben in mensen en depressieve klachten kwamen het vaakst voor bij slachtoffers van online pesten.

6.3.2 Emotionele of psychische gevolgen door online bedreiging en intimidatie[1)], 2024



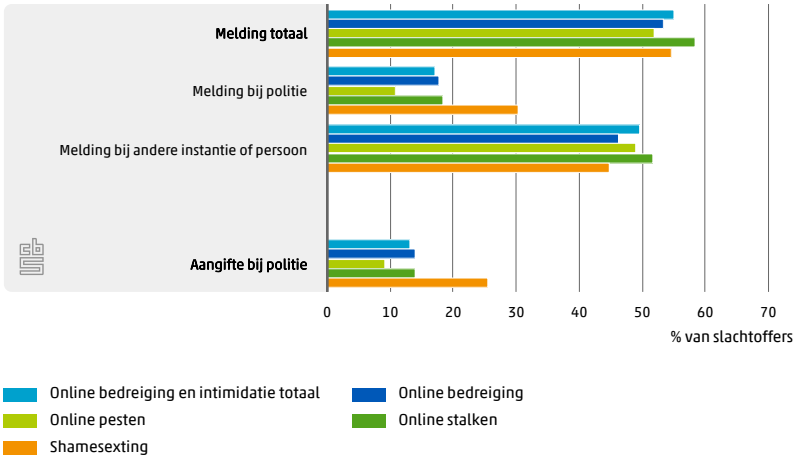
[1)] Meerdere antwoorden mogelijk.

6.4 Melding en aangifte online bedreiging en intimidatie

In totaal heeft 55 procent van de slachtoffers van online bedreiging en intimidatie het voorval ergens gemeld: 17 procent bij de politie en 50 procent bij een andere instantie of persoon. Bij andere instanties gaat het bijvoorbeeld om meld- of adviespunten zoals Meld Misdaad Anoniem of Veilig Thuis. Personen aan wie het voorval werd gemeld, waren bijvoorbeeld professionele hulpverleners zoals huisartsen, psychologen of maatschappelijk werkers, andere professionals zoals leerkrachten of leidinggevenden, en mensen uit het eigen, informele circuit zoals andere gezinsleden, familie of vrienden.

Het grootste deel van de meldingen van online bedreiging en intimidatie bij de politie resulteerde in een aangifte (17 procent maakte melding; 13 procent deed aangifte). Van shamesexting werd door slachtoffers het vaakst aangifte gedaan bij de politie (26 procent), van online pesten het minst vaak (9 procent).

6.4.1 Melding en aangifte online bedreiging en intimidatie[1)], 2024



[1)] Meerdere antwoorden mogelijk.

De meeste slachtoffers van online bedreiging en intimidatie die aangifte deden, deden dit op het politiebureau (40 procent). Daarnaast deed 24 procent aangifte via internet, 22 procent telefonisch en 25 procent 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, was dat er niet aan is gedacht of dat men het niet zo belangrijk vond (41 procent), gevolgd door 'het helpt toch niets' (33 procent). Ongeveer 14 procent zei dat het al was opgelost en 13 procent heeft geen zin of tijd gehad, of vond het te veel moeite. Andere redenen, zoals 'door schuld of schaamtegevoel' en 'op advies van de politie', werden door slachtoffers minder vaak genoemd.

Slachtoffers van online stalking gaven vaker dan slachtoffers van andere delicten 'het is al opgelost' als reden om geen melding of aangifte te doen bij de politie. Slachtoffers van shamesexting noemden vaker het hebben van schuld- of schaamtegevoel als reden.

Slachtofferschap doxing

In 2024 is in het onderzoek Online Veiligheid en Criminaliteit voor het eerst gevraagd naar slachtofferschap van doxing. Doxing is het verzamelen of (verder) verspreiden van persoonlijke of gevoelige informatie (bijv. woonadres, telefoonnummer of foto). Dit met het doel om iemand angst aan te jagen, ernstige overlast te bezorgen, of ernstig te hinderen bij het werk dat diegene doet (Politie, 2024).

Van de 15-plussers gaf minder dan 1 procent (90 duizend personen) aan met doxing te maken te hebben gehad in de twaalf maanden voorafgaand aan het onderzoek. Bijna een derde van de slachtoffers dacht of wist zeker dat hun beroep te maken had met het voorval.

---

7. Online criminaliteit totaal

In de hoofdstukken 4, 5 en 6 stonden de verschillende soorten online criminaliteit centraal: oplichting en fraude, hacken, en bedreiging en intimidatie. In dit hoofdstuk worden deze in onderlinge samenhang besproken en wordt een totaalbeeld van online criminaliteit geschetst. Net als in de vorige hoofdstukken komen achtereenvolgens slachtofferschap, gevolgen, melding en aangifte aan de orde.

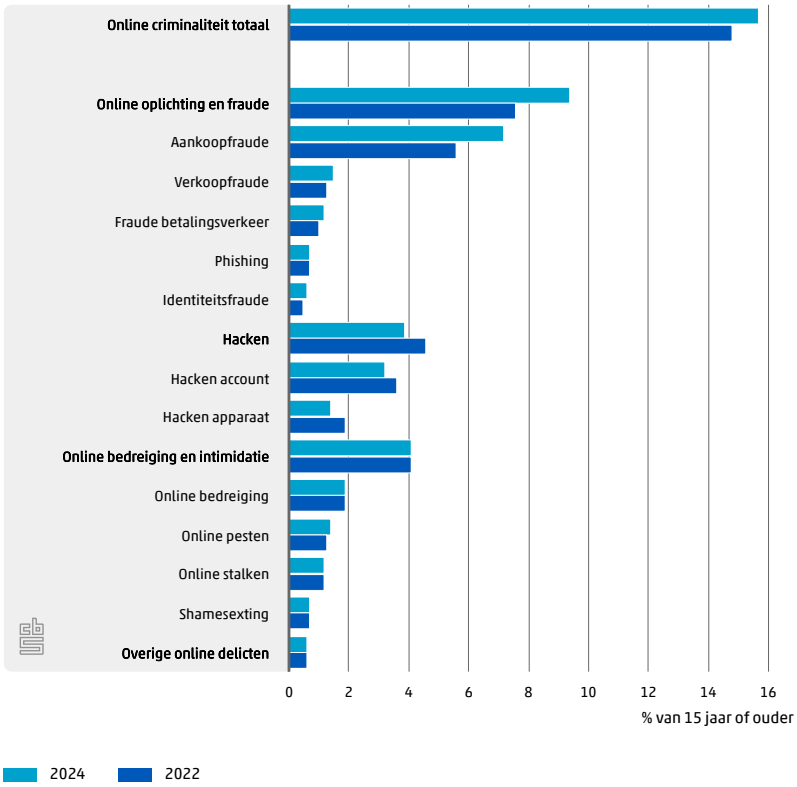
In de Tabellenset 2024 die bij deze publicatie hoort, zijn alle resultaten van dit hoofdstuk opgenomen bij '7 Online criminaliteit' en '7 Gevolgen, melding, aangifte'.

7.1 Slachtoffers online criminaliteit

In 2024 gaf 16 procent van de bevolking van 15 jaar of ouder aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van online criminaliteit. Dit zijn bijna 2,4 miljoen mensen. De meesten werden slachtoffer van oplichting en fraude (9 procent) en dan met name van aankoopfraude. Met hacken kreeg 4 procent te maken en eveneens 4 procent met online bedreiging en intimidatie. Krap 1 procent werd slachtoffer van andere online delicten (zie kader hieronder).

In 2024 gaven meer mensen aan slachtoffer te zijn geweest van online criminaliteit dan in 2022. Deze toename was met name zichtbaar bij slachtoffers van online oplichting en fraude. Het aandeel slachtoffers van hacken was in 2024 juist lager dan in 2022. Van online bedreiging en intimidatie en van andere online delicten werden in beide jaren ongeveer evenveel mensen slachtoffer.

7.1.1 Slachtoffers online criminaliteit



Overige online delicten

In dit onderzoek is aan de deelnemers gevraagd of ze weleens slachtoffer zijn geweest van een 'ander' misdrijf via internet, dus van een misdrijf dat bij de enquêtevragen over oplichting en fraude, hacken of online bedreiging en intimidatie niet aan de orde kwam. Dit kon men via een open vraag aangeven. Hieruit bleek dat het overgrote deel van de antwoorden binnen één van de drie genoemde delictgroepen past. Daarom is ervoor gekozen om deze 'overige online delicten' niet in detail te beschrijven. Deze delicten zijn echter wel meegenomen in het totale slachtofferschap van online criminaliteit.

Slachtoffers online criminaliteit naar persoonskenmerken

Slachtofferschap van online criminaliteit verschilde nauwelijks naar geslacht en onderwijsniveau. Wel werden jongeren vaker getroffen dan ouderen: 20 procent van de 15- tot 25-jarigen, tegenover 10 procent van de 65-plussers. Vooral bij het slachtofferschap van online bedreiging en intimidatie was het verschil tussen jongere en oudere leeftijdsgroepen groot. Ook mensen uit huishoudens met de laagste welvaart werden relatief vaak met online criminaliteit geconfronteerd (18 procent). Dit heeft er mee te maken dat zij vaker slachtoffer waren van online oplichting en fraude dan mensen in meer welvarende huishoudens.

7.1.2 Slachtofferschap online criminaliteit naar persoonskenmerken, 2024 (%)

	Online criminaliteit totaal	Online oplichting en fraude	Hacken	Online bedreiging en intimidatie	Overige online delicten
Totaal	15,7	9,4	3,9	4,1	0,6
Geslacht: Mannen	15,7	9,2	3,9	4,4	0,6
Geslacht: Vrouwen	15,8	9,5	3,8	3,9	0,7
Leeftijd: 15 tot 25 jaar	20,3	9,2	5,3	8,8	0,7
Leeftijd: 25 tot 45 jaar	17,9	10,8	4,5	4,7	0,7
Leeftijd: 45 tot 65 jaar	15,6	10,2	3,5	3,1	0,6
Leeftijd: 65 jaar of ouder	10,4	6,5	2,7	2,0	0,5
Onderwijsniveau: Basisonderwijs, vmbo, mbo1	15,2	9,0	3,9	4,3	0,6
Onderwijsniveau: Havo, vwo, mbo2-4	16,1	9,4	4,0	4,4	0,6
Onderwijsniveau: Hbo, wo	15,9	9,3	3,8	3,8	0,7
Welvaart huishouden: 1e 20%-groep (laagst)	18,0	10,6	4,7	4,9	0,6
Welvaart huishouden: 2e 20%-groep	16,7	9,9	4,1	4,8	0,7
Welvaart huishouden: 3e 20%-groep	15,6	9,5	3,6	4,0	0,5
Welvaart huishouden: 4e 20%-groep	14,6	8,7	3,4	3,8	0,5
Welvaart huishouden: 5e 20%-groep (hoogst)	15,1	8,8	3,9	3,8	0,8

Slachtofferschap online criminaliteit Veiligheidsmonitor 2023

In 2023 is het slachtofferschap van online criminaliteit ook in de Veiligheidsmonitor onderzocht. Van de bevolking van 15 jaar of ouder gaf 16 procent in dat jaar aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van één of meerdere vormen van online criminaliteit (online oplichting en fraude, hacken, online bedreiging en intimidatie, en overige online delicten). Dat is vergelijkbaar met de bevindingen van dit onderzoek.

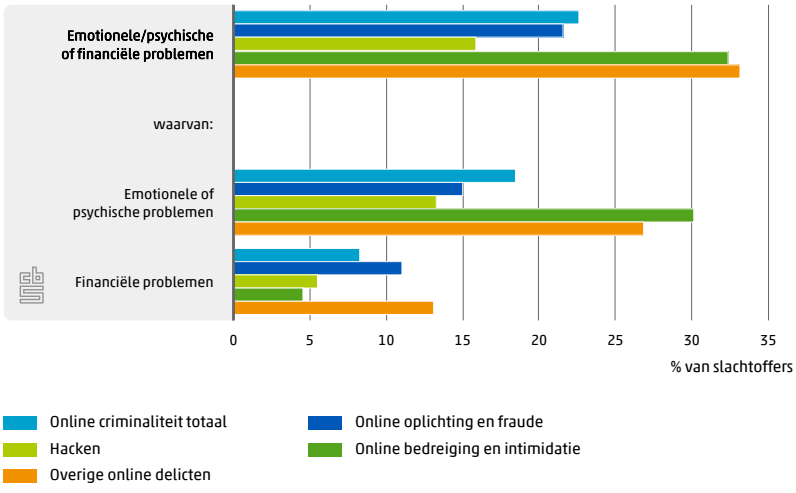
7.2. Gevolgen online criminaliteit

Problemen voor slachtoffers

Bijna een kwart 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 (32 procent). Slachtoffers van hacken met 16 procent het minst vaak.

Slachtofferschap van online criminaliteit leidde vaker tot emotionele of psychische problemen dan tot financiële problemen: 19 tegenover 8 procent. Vooral bij online bedreiging en intimidatie is dit verschil relatief groot (30 tegen 5 procent).

7.2.1 Problemen door online criminaliteit[1)], 2024



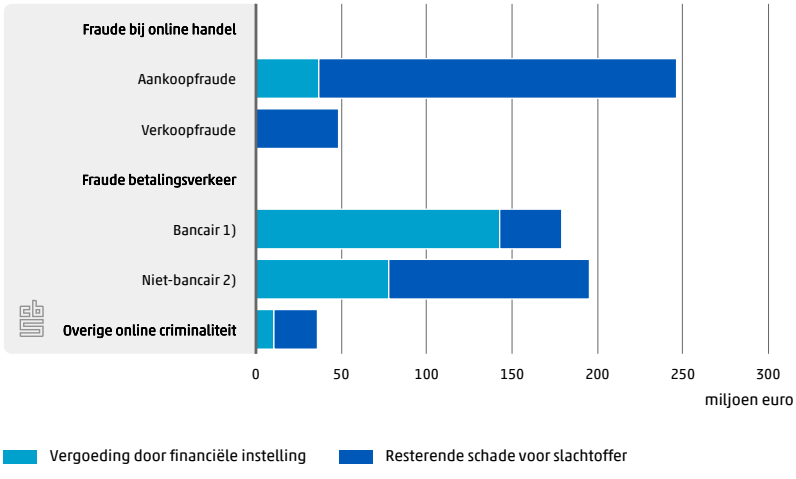
[1)] Meerdere antwoorden mogelijk.

Financiële schade online criminaliteit

In de Veiligheidsmonitor 2023 is aan slachtoffers van online vermogensdelicten (delicten waarbij spullen of geld wordt gestolen) gevraagd hoeveel geld ze zijn kwijtgeraakt door het voorval. Ook is gevraagd welk bedrag vergoed is door een financiële instelling, zoals een bank of verzekeraar. Op basis hiervan kan de financiële schade van online criminaliteit worden geschat.

Bij online criminaliteit bedroeg het totale schadebedrag in 2023 naar schatting 707 miljoen euro (Kennis en Reep, 2024). Het grootste deel hiervan (375 miljoen euro) had betrekking op fraude in het betalingsverkeer, gevolgd door aankoopfraude (247 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, 2023



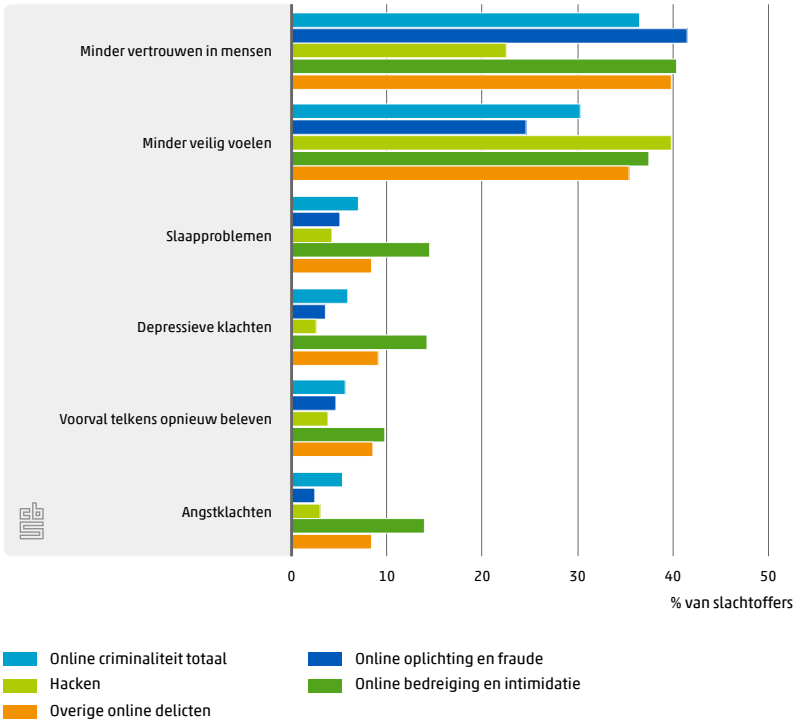
[1)] Dader had toegang tot de bankrekening van het slachtoffer.
[2)] Het slachtoffer maakte het geld zelf over.

Emotionele of psychische gevolgen

Voor de meeste slachtoffers van online criminaliteit leidde het voorval ertoe dat zij minder vertrouwen hadden in mensen (37 procent) en zich minder veilig voelden (30 procent). Slaapproblemen, depressieve klachten, angstklachten en het voorval steeds opnieuw beleven werden elk door 5 à 7 procent van de slachtoffers genoemd.

Minder vertrouwen in mensen werd het vaakst als gevolg genoemd door slachtoffers van online oplichting en fraude. Zich minder veilig voelen, slaapproblemen, depressieve klachten, het voorval telkens opnieuw beleven en angstklachten werden het vaakst gerapporteerd door slachtoffers van online bedreiging en intimidatie.

7.2.2 Emotionele of psychische gevolgen online criminaliteit[1)], 2024



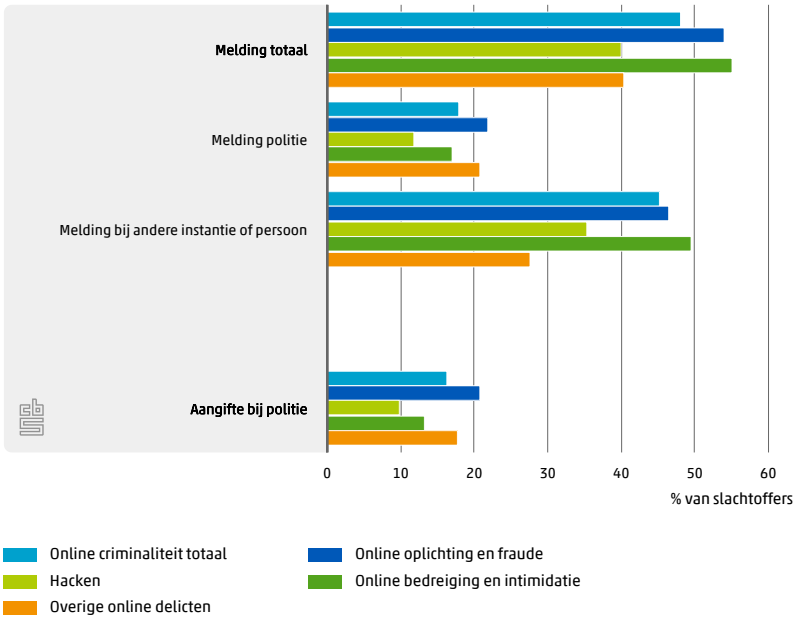
[1)] Meerdere antwoorden mogelijk.

7.3 Melding en aangifte online criminaliteit

Van de slachtoffers van online criminaliteit heeft 18 procent bij de politie gemeld wat hen overkomen was en heeft 45 procent dit bij een andere instantie of persoon gedaan. Het gaat dan om instanties als meld- of adviespunten voor online criminaliteit. Bij personen kan het 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 48 procent van de slachtoffers van online criminaliteit in 2024 bij de politie en/of een andere instantie of persoon melding gemaakt. Het grootste deel van de meldingen bij de politie resulteerde in een aangifte (18 procent maakte melding; 16 procent deed aangifte). Hacken werd het minst vaak bij de politie gemeld en aangegeven (respectievelijk door 12 en 10 procent van de slachtoffers).

7.3.1 Melding en aangifte online criminaliteit[1)], 2024



[1)] Meerdere antwoorden mogelijk.

De meeste slachtoffers van online criminaliteit die aangifte deden van het voorval, deden dit via internet (47 procent). Verder deed 27 procent aangifte op het politiebureau, 17 procent telefonisch en 15 procent 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 om geen aangifte te doen, was dat er niet aan wordt gedacht of dat men het niet zo belangrijk vond (40 procent), gevolgd door 'het helpt toch niets' (32 procent). Verder gaf 17 procent aan dat het geen zaak voor de politie was, zei 15 procent dat het al was opgelost en eveneens 15 procent heeft geen zin of tijd gehad, of vond het te veel moeite. Andere redenen, zoals 'door schuld- of schaamtegevoel' en 'op advies van de politie', werden door 5 procent of minder van de slachtoffers van online criminaliteit genoemd.

Slachtoffers van hacken die geen aangifte hebben gedaan, 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 deden relatief vaak uit angst voor een vervelende reactie of wraak geen melding of aangifte.

8. Online discriminatie

Niet alleen criminaliteit, maar ook discriminatie kan online plaatsvinden. Het College voor de Rechten van de Mens (2024) beschrijft discriminatie als mensen anders behandelen, achterstellen of uitsluiten op basis van (persoonlijke) kenmerken. Deze kenmerken worden discriminatiegronden genoemd. Discriminatie op de volgende gronden is wettelijk niet toegestaan: godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, seksuele gerichtheid, burgerlijke staat, handicap of chronische ziekte, leeftijd, arbeidsduur, vast of tijdelijk contract, en zwangerschap, bevalling en moederschap. Net als voor online bedreiging en intimidatie geldt ook voor online discriminatie dat opmerkingen en beelden via internet breder en sneller verspreid kunnen worden, voor anderen langer zichtbaar kunnen blijven en moeilijk te verwijderen zijn. De impact kan daardoor groter zijn dan bij offline discriminatie.

Hoeveel 15-plussers voelden zich online gediscrimineerd in 2024 en is dit veranderd ten opzichte van 2022? Op welke gronden, manieren en via welke kanalen vindt online discriminatie plaats? Wat is de impact op degenen die de discriminatie ervaren? En melden zij discriminatie, en zo ja, waar? Deze vragen staan in dit hoofdstuk centraal.

In de Tabellenset 2024 die bij deze publicatie hoort, zijn alle resultaten van dit hoofdstuk opgenomen bij '8 Online discriminatie' en '8 Details'.

Discriminerende content gezien op internet

In 2024 gaf ruim de helft (53 procent) van de bevolking van 15 jaar of ouder aan dat zij in de afgelopen twaalf maanden op internet iets hadden gezien of gelezen dat zij discriminerend, beledigend of kwetsend vonden voor een persoon of groep mensen. De meest genoemde gronden voor discriminatie in deze uitingen waren ras of huidskleur (70 procent), politieke overtuiging (57 procent), godsdienst of levensovertuiging (53 procent) en seksuele oriëntatie (51 procent).

8.1 Ervaren van online discriminatie

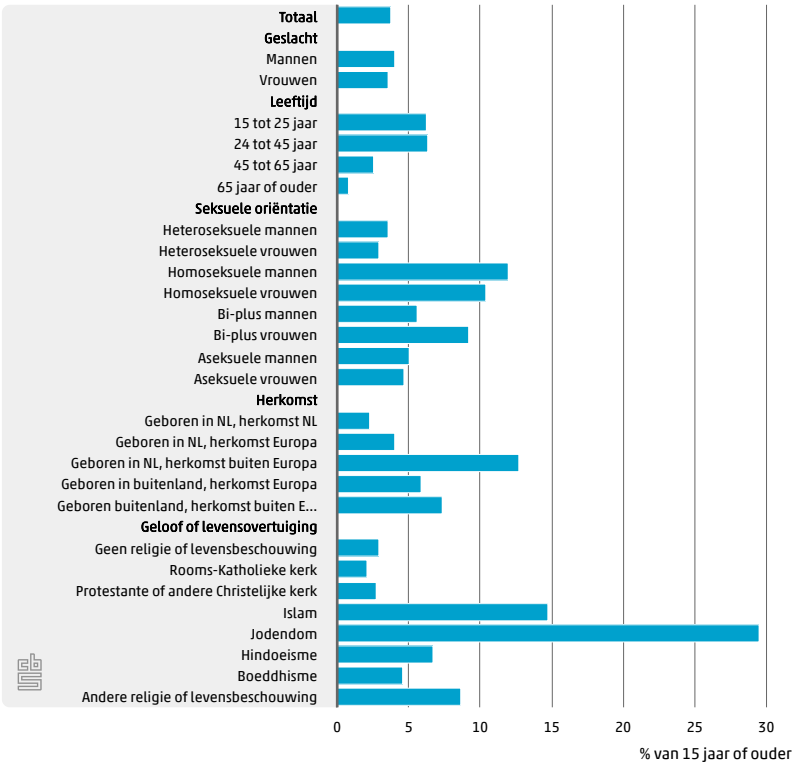
In 2024 zei 4 procent van de bevolking van 15 jaar of ouder (bijna 580 duizend personen) dat zij zich in de afgelopen twaalf maanden weleens online gediscrimineerd hadden gevoeld. Dat is een verdubbeling ten opzichte van 2022, toen 2 procent dit aangaf.

Mannen en vrouwen gaven ongeveer even vaak aan online discriminatie te hebben meegemaakt. Personen van 15 tot 45 jaar gaven dit met 6 procent relatief vaak aan. Ook homoseksuele mannen (12 procent), homoseksuele vrouwen (10 procent) en bi-plus vrouwen (9 procent) hadden hier relatief vaak mee te maken.

Personen geboren in Nederland met een herkomst buiten Europa (tweede generatie) ervoeren met 13 procent het vaakst online discriminatie. Ook personen geboren in het buitenland (migranten) met een herkomst buiten of binnen Europa voelden zich met respectievelijk 7 en 6 procent relatief vaak online gediscrimineerd. Bij personen met een Nederlandse herkomst was dit met 2 procent het laagst. Deze verschillen zijn ook statistisch significant als rekening wordt gehouden met verschillen tussen herkomstgroepen in geslacht, leeftijd en onderwijsniveau.

Wat godsdienst of levensbeschouwing betreft voelde 30 procent van de joden en 15 procent van de moslims zich online gediscrimineerd. Rooms-katholieken voelden zich het minst vaak online gediscrimineerd (2 procent). Verder werden mensen uit huishoudens met de laagste welvaart vaker met online discriminatie geconfronteerd dan mensen uit huishoudens met een hogere welvaart.

8.1.1 Online discriminatie naar persoonskenmerken, 2024



Tegen wie is online discriminatie gericht?

Discriminatie kan tegen de persoon zelf gericht zijn en/of tegen de groep waartoe men zich rekent. In 2024 gaf 11 procent van de 15-plussers die zich online gediscrimineerd voelden aan dat dit tegen hen persoonlijk gericht was. Bijna 60 procent zei dat de online discriminatie gericht was tegen de groep waartoe zij zichzelf rekenen. Bij 27 procent was online discriminatie gericht tegen de persoon zelf én tegen de groep waartoe zij zichzelf rekenen.

Bekendheid dader(s)

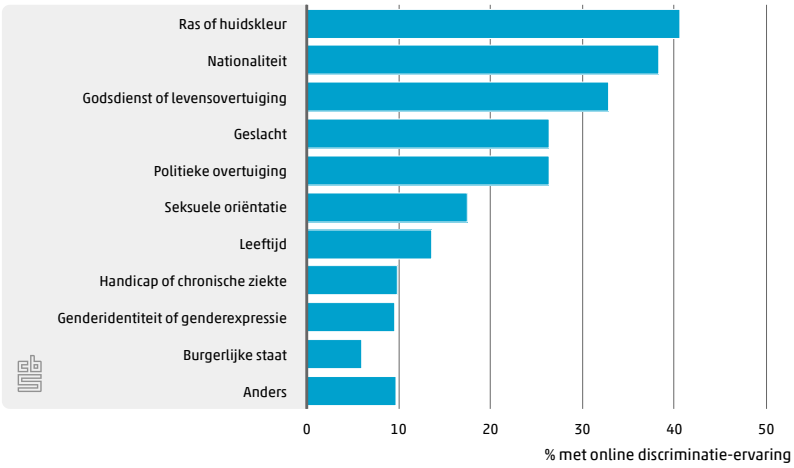
Op de vraag of men de dader of daders kende, zei 22 procent dat dit het geval was. Daarentegen kende 69 procent de dader(s) niet; 9 procent gaf geen antwoord. Bekende daders waren het vaakst collega's.

8.2 Gronden, manieren en plaats van online discriminatie

Discriminatiegronden

Van degenen die in 2024 online discriminatie ervoeren, ging het bij 41 procent om discriminatie op grond van ras of huidskleur, gevolgd door discriminatie op grond van nationaliteit (38 procent) en godsdienst of levensbeschouwing (33 procent). Iets meer dan een kwart (26 procent) noemde politieke overtuiging of geslacht en 18 procent seksuele oriëntatie. Andere gronden voor discriminatie, zoals leeftijd, handicap, genderidentiteit en burgerlijke staat, werden minder vaak genoemd.

8.2.1 Gronden voor online discriminatie[1)], 2024



[1)] Meerdere antwoorden mogelijk.

Discriminatiegronden verschillen tussen bevolkingsgroepen. Online discriminatie op grond van ras of huidskleur werd met 72 procent het vaakst gerapporteerd door de tweede generatie met een herkomst buiten Europa. Migranten geboren buiten Europa ervoeren vaker online discriminatie op grond van ras of huidskleur dan migranten geboren in Europa: 62 tegenover 23 procent.

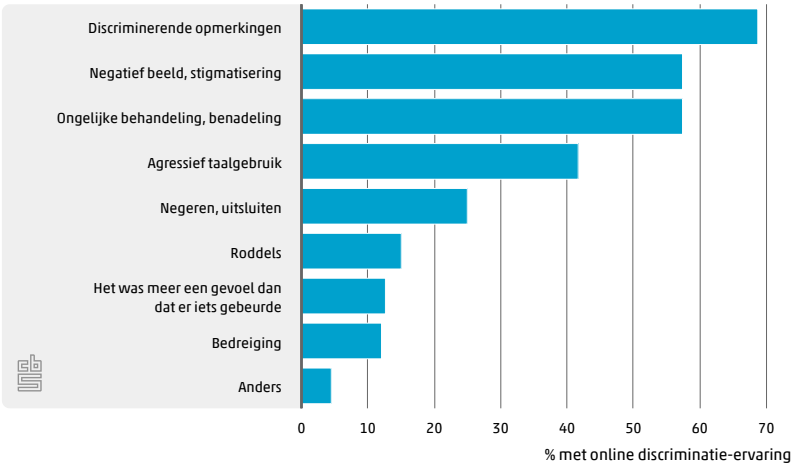
Ook godsdienst of levensovertuiging is onderscheidend. Dit werd door 80 procent van de moslims als grond voor discriminatie gerapporteerd, terwijl bijvoorbeeld 25 procent met een andere religie of levensbeschouwing deze discriminatiegrond noemde.

Discriminatie op grond van geslacht wordt door beide sekse eveneens verschillend ervaren. Vrouwen voelden zich op grond van geslacht twee keer zo vaak gediscrimineerd als mannen: 38 tegenover 17 procent.

Manieren van discriminatie

Bijna 7 op de 10 mensen die zich in 2024 gediscrimineerd voelden, gaven aan dat dit kwam door discriminerende opmerkingen. Bijna 6 op de 10 zeiden dat dit kwam door een negatief beeld/stigmatisering of door ongelijke behandeling/benadeling/het voortrekken van bepaalde groepen. Ruim 4 op de 10 gaven aan dat ze zich gediscrimineerd voelden door agressief taalgebruik. Andere manieren van discriminatie, zoals negeren of uitsluiten, roddels of bedreiging, werden minder vaak genoemd.

8.2.2 Manieren van online discriminatie[1)], 2024

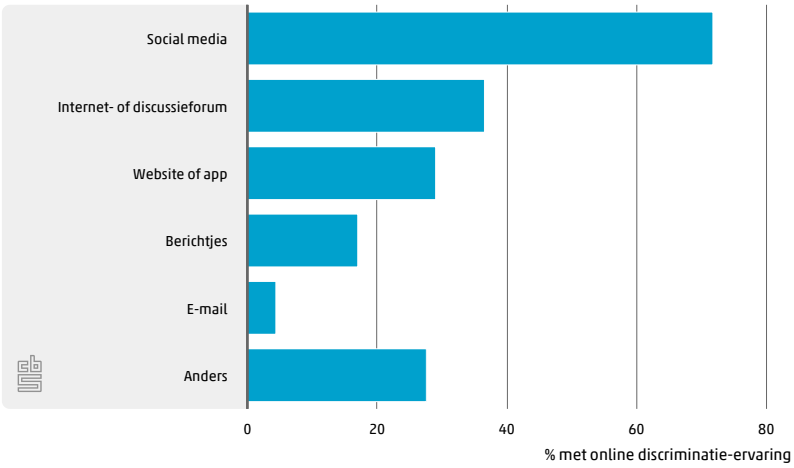


[1)] Meerdere antwoorden mogelijk.

Waar werd online discriminatie ervaren?

De meeste mensen die online discriminatie hadden ervaren (72 procent), zeiden dat dit op social media had plaatsgevonden, zoals Facebook, Instagram, Snapchat, TikTok of X. Discriminatie op internet- of discussiefora ervoer 37 procent, op een website of app (bijv. YouTube of een datingapp) was dat 29 procent en 17 procent maakte dit mee via berichtjes (bijv. WhatsApp, Messenger, Signal, Snapchat of TikTok).

8.2.3 Waar online discriminatie ervaren[1)], 2024



[1)] Meerdere antwoorden mogelijk.

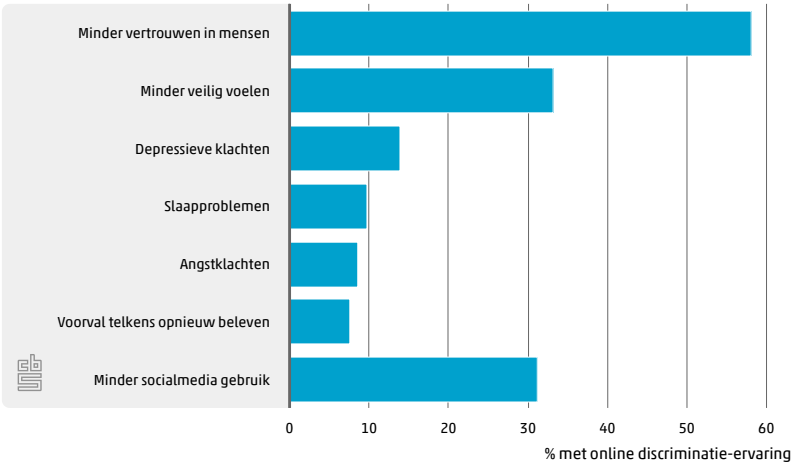
8.3 Gevolgen online discriminatie

Ruim een kwart van de personen die online discriminatie hadden ervaren, zei problemen te hebben (gehad) als gevolg van het voorval. Verreweg de meesten noemden emotionele of psychische problemen (25 procent); 4 procent gaf aan er financiële problemen door te hebben (gehad).

Als het gaat om emotionele of psychische gevolgen, gaf 58 procent van degenen die online discriminatie hadden ervaren aan dat ze daardoor minder vertrouwen in mensen hadden. 33 procent voelde zich minder veilig en 14 procent had depressieve klachten. Angstklachten en/of paniekaanvallen, slaapproblemen en het voorval telkens opnieuw beleven werden door ongeveer 10 procent genoemd.

Verder gaf ruim 30 procent aan dat zij door de online discriminatie minder social media zijn gaan gebruiken.

8.3.1 Gevolgen online discriminatie[1)], 2024



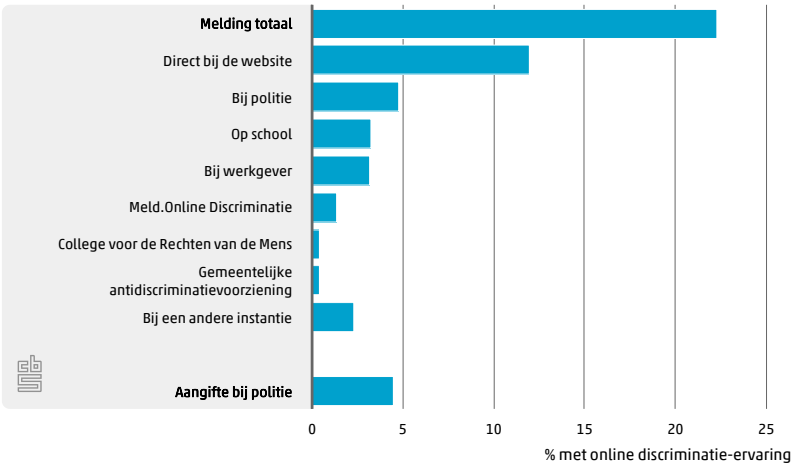
[1)] Meerdere antwoorden mogelijk.

8.4 Melding en aangifte online discriminatie

Ruim een vijfde (22 procent) van de 15-plussers die zich in de afgelopen twaalf maanden online gediscrimineerd voelden, heeft dit ergens gemeld. De meesten meldden dit direct bij de website waar de discriminatie plaatsvond (12 procent). Verder meldde 5 procent het bij de politie, 3 procent op het werk (bijvoorbeeld bij de leidinggevende of vertrouwenspersoon) en eveneens 3 procent op school (bijvoorbeeld bij een leerkracht of vertrouwenspersoon). Bij Meld.Online Discriminatie maakte 1 procent melding, en bij het College voor de Rechten van de Mens en bij een gemeentelijke antidiscriminatievoorziening (ADV) minder dan 1 procent.

Het grootste deel van de meldingen bij de politie resulteerde in een aangifte. Van degenen die online discriminatie ervoeren, deed 4 procent aangifte bij de politie.

8.4.1 Melding en aangifte online discriminatie[1)], 2024



[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' (52 procent), gevolgd door 'niet aan gedacht/niet zo belangrijk' (36 procent). 17 procent had geen zin of tijd om aangifte te doen en 11 procent vond het geen zaak voor de politie. De andere in het onderzoek voorgelegde redenen, zoals uit angst voor vervelende reacties en door schuld- of schaamtegevoel, werden elk door minder dan 6 procent genoemd.

9. Online oproepen tot openbare-ordeverstoring

Internet wordt ook gebruikt om oproepen te doen om de openbare orde te verstoren. Denk aan berichten via social media of in app-groepen, waarin opgeroepen wordt tot straatraces, demonstraties of illegale feesten. Hoe vaak komen 15-plussers dit soort oproepen op internet tegen? Om wat voor soort oproepen gaat het? En wat doen mensen met zulke berichten? Deze vragen worden in dit hoofdstuk beantwoord.

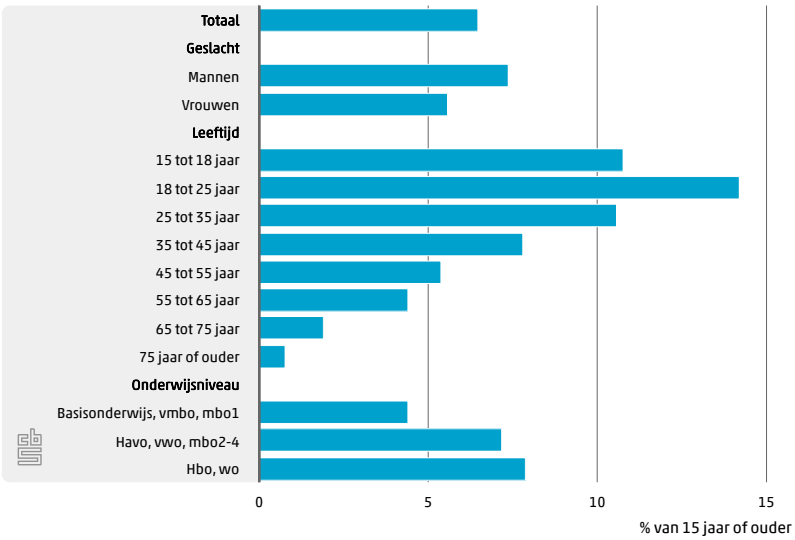
In de Tabellenset 2024 die bij deze publicatie hoort, zijn alle resultaten van dit hoofdstuk opgenomen bij '9 Openbare-ordeverstoring' en 'Details'.

9.1 Online oproepen tot openbare-ordeverstoring

In 2024 gaf 7 procent van de bevolking van 15 jaar of ouder (bijna 980 duizend personen) aan in de afgelopen twaalf maanden weleens online berichten gezien te hebben, waarin werd opgeroepen tot openbare-ordeverstoring of activiteiten die vaak daartoe leiden, zoals straatraces, demonstraties of illegale feesten. In 2022 was dit aandeel hoger, namelijk 9 procent.

Mannen gaven vaker aan online berichten over openbare-ordeverstoring gezien te hebben dan vrouwen. Jongeren in de leeftijd van 18 tot 25 jaar zagen met 14 procent het vaakst een online bericht tot openbare-ordeverstoring, 65-plussers kwamen deze online berichten het minst tegen. Mensen met basisonderwijs, vmbo of mbo1 zagen dit soort berichten minder vaak dan mensen met een ander onderwijsniveau.

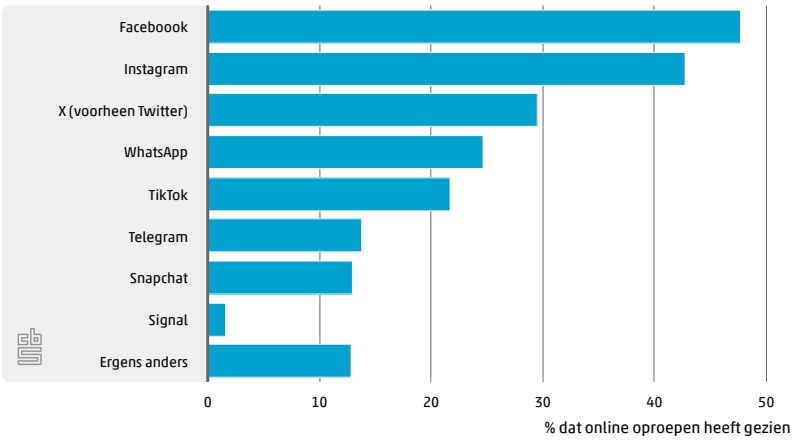
9.1.1 Berichten van online oproepen tot openbare-ordeverstoring, 2024



Waar worden berichten gezien?

Bijna de helft van de 15-plussers die online berichten zagen waarin werd opgeroepen tot openbare-ordeverstoring, gaf aan zulke berichten op Facebook te hebben gezien. Voor ruim 40 procent was dit op Instagram en voor bijna 30 procent op X. WhatsApp en TikTok werden elk door ruim 20 procent genoemd als bron van berichten voor openbare-ordeverstoring. Dit gold in mindere mate voor Telegram, Snapchat of Signal.

9.1.2 Waar oproep(en) tot openbare-ordeverstoring gezien[1)], 2024



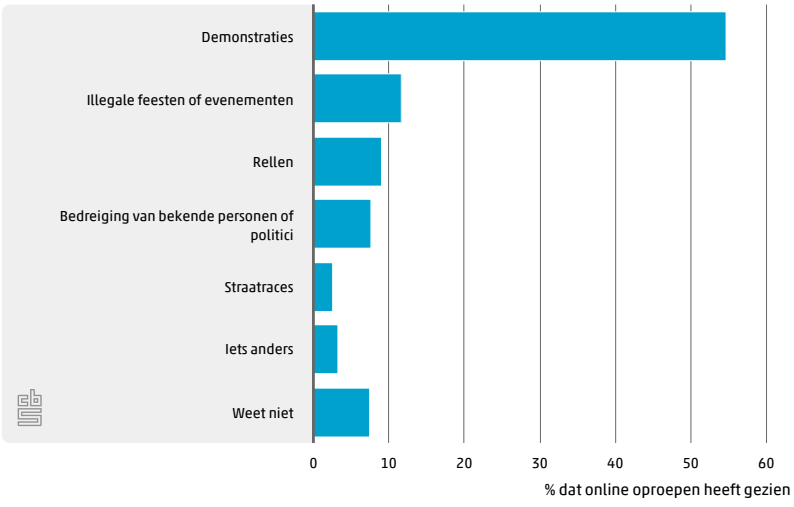
[1)] Meerdere antwoorden mogelijk.

Waartoe wordt opgeroepen?

Verreweg de meeste mensen die berichten zagen waarin werd opgeroepen tot openbare-ordeverstoring, gaven aan dat het (laatste) bericht ging om een oproep tot demonstraties (55 procent). Bij 14 procent van de oproepen tot demonstraties, zei men dat het om illegale demonstraties ging (zonder een vergunning); 29 procent gaf aan dat het om legale demonstraties (met een vergunning) ging en 22 procent zei dat het om zowel legale als illegale demonstraties ging. De meeste mensen (34 procent) wisten niet of de oproepen tot demonstraties legaal of illegaal waren.[4)]

Berichten die oproepen tot illegale feesten of evenementen werden door 12 procent genoemd en berichten die oproepen tot rellen door 9 procent. Verder gaf 8 procent aan dat het bericht opriep tot het bedreigen van bekende personen of politici. 3 procent zei dat het om oproepen tot straatraces ging. Eveneens 3 procent noemde berichten met een andere inhoud. In een open antwoord kon men aangeven waartoe dan opgeroepen werd. De antwoorden waren zeer divers, zoals tekenen van een petitie, boycotten van producten of bedrijven, gegevens van mensen verder verspreiden, DDoS-aanvallen, onwaarheden verspreiden of onrust veroorzaken.

9.1.3 Waartoe werd opgeroepen, 2024



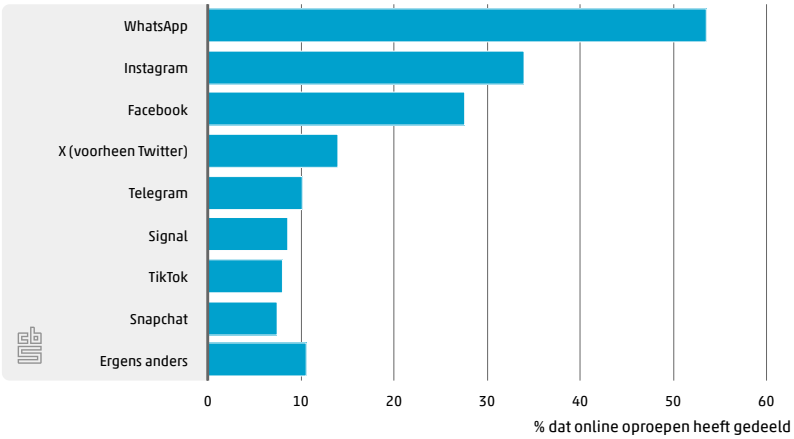
In 2024 zagen meer mensen online oproepen tot bedreiging van bekende personen of politici dan in 2022. Online oproepen tot demonstraties, tot illegale feesten of evenementen, en tot straatraces werden daarentegen in 2024 door minder mensen gezien.

9.2 Actie na zien oproep tot openbare-ordeverstoring

Het merendeel van de mensen die een online oproep tot openbare-ordeverstoring hadden gezien, gaf aan niets met het bericht te hebben gedaan (84 procent). 4 procent meldde het bij de politie en eveneens 4 procent zei te hebben deelgenomen aan de activiteit waartoe werd opgeroepen. Het ging dan met name om het meedoen aan illegale feesten of evenementen, straatraces en demonstraties.

Een klein deel van de mensen die een online oproep tot openbare-ordeverstoring hadden gezien, deelde het bericht online (3 procent). Verreweg de meeste mensen die een oproep deelden, deden dat via WhatsApp (54 procent), Instagram (34 procent) en Facebook (28 procent). Op andere social media werd dit soort berichten steeds door minder dan 15 procent gedeeld (bijv. X, TikTok, Signal en Snapchat).

9.2.1 Waar oproep tot openbare-ordeverstoring gedeeld[1)], 2024



[1)] Meerdere antwoorden mogelijk.

[4)] In dit onderzoek worden oproepen voor legale demonstraties ook als openbare-ordeverstoring beschouwd.

10. Conclusies en aanbevelingen

Dit afsluitende hoofdstuk bevat de belangrijkste conclusies van Online Veiligheid en Criminaliteit 2024 en een aantal aanbevelingen voor toekomstig onderzoek.

10.1 Conclusies

2,4 miljoen mensen in 2022 slachtoffer van online criminaliteit

In 2024 gaf 16 procent van de bevolking van 15 jaar of ouder aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van online criminaliteit. Dit zijn bijna 2,4 miljoen mensen. De meesten werden slachtoffer van oplichting en fraude (9 procent) en dan met name van aankoopfraude. Met hacken had 4 procent te maken en eveneens 4 procent met online bedreiging en intimidatie. Krap 1 procent werd slachtoffer van een ander online delict.

In 2024 gaven meer mensen aan slachtoffer te zijn geweest van online criminaliteit dan in 2022 (15 procent). Deze toename was met name zichtbaar bij slachtoffers van online oplichting en fraude. Het aandeel slachtoffers van hacken was in 2024 juist lager dan in 2022. Van online bedreiging en intimidatie en van andere online delicten was het aandeel slachtoffers vergelijkbaar.

Jongeren vaker slachtoffer van online criminaliteit dan ouderen

Jongeren werden vaker slachtoffer van online criminaliteit dan ouderen. Zo werd 20 procent van de 15- tot 25-jarigen slachtoffer, tegenover 10 procent van de 65-plussers. Vooral bij online bedreiging en intimidatie was er een groot verschil tussen jongeren en ouderen. Ook homoseksuele en bi-plus personen kregen vaker met deze vorm van online criminaliteit te maken dan heteroseksuele personen.

4 op de 10 slachtoffers van online bedreiging en intimidatie kennen de dader

Bij 4 op de 10 slachtoffers van online bedreiging en intimidatie was bekend wie de dader was. Bij pesten en stalken kende het slachtoffer de dader(s) het vaakst. De meest genoemde daders waren de ex-partner, een vriend(in) of een medestudent/-scholier. De ex-partner werd bij online stalken door slachtoffers het vaakst als dader genoemd. Bij online pesten was dat een medestudent/-scholier (15 procent) en bij online bedreiging een andere bekende (13 procent).

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

Bij 37 procent van de slachtoffers van online criminaliteit leidde het voorval ertoe dat ze minder vertrouwen in mensen hadden en bij 30 procent dat ze zich minder veilig voelden. Slaapproblemen, depressieve klachten, angstklachten en het voorval steeds opnieuw beleven werden elk door 5 à 7 procent van de slachtoffers genoemd; slachtoffers van online bedreiging en intimidatie rapporteerden deze klachten het vaakst.

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

Van de slachtoffers van online criminaliteit heeft 18 procent bij de politie gemeld wat hen overkomen was en 45 procent heeft dit bij een andere instantie of persoon gedaan. Een groot deel van de meldingen van online criminaliteit bij de politie resulteerde in een aangifte (16 procent deed aangifte). De meest genoemde reden om het voorval niet bij de politie te melden of geen aangifte te doen is dat men er niet aan heeft gedacht of het niet zo belangrijk vond, gevolgd door 'het helpt toch niets'.

Ruim 40 procent heeft behoefte aan voorlichting over bescherming tegen online criminaliteit

Ruim 40 procent van de 15-plussers gaf aan behoefte te hebben aan informatie of voorlichting om zichzelf beter te kunnen beschermen tegen online criminaliteit. Het meest behoefte hadden mensen aan meer informatie over beschermende maatregelen die ze zelf kunnen nemen (31 procent). Iets meer dan 20 procent gaf aan behoefte te hebben aan meer informatie over hoe oplichters te werk gaan en waar men op moet letten. Eenzelfde deel gaf aan meer duidelijkheid te willen over waar meer informatie te vinden is.

Meer dan een half miljoen mensen voelde zich in 2024 online gediscrimineerd

In 2024 zei 4 procent van de inwoners van Nederland van 15 jaar of ouder dat zij zich in de afgelopen twaalf maanden weleens online gediscrimineerd hebben gevoeld. Dit zijn bijna 580 duizend mensen, een verdubbeling ten opzichte van 2022. Van degenen die online discriminatie ervoeren, ging het bij 41 procent om discriminatie op grond van ras of huidskleur, gevolgd door discriminatie op grond van nationaliteit (38 procent) en godsdienst of levensbeschouwing (33 procent). Online discriminatie gebeurde vooral door discriminerende opmerkingen, gevolgd door stigmatisering en ongelijke behandeling.

Bijna 60 procent van degenen die online discriminatie ervoeren, zei dat zij daardoor minder vertrouwen in mensen hadden. 33 procent voelde zich minder veilig en 14 procent had depressieve klachten. Verder gaf meer dan 30 procent aan dat zij door het voorval minder social media zijn gaan gebruiken.

Ruim 20 procent van degenen die zich in de afgelopen twaalf maanden online gediscrimineerd voelden, heeft dit ergens gemeld. Door 4 procent werd aangifte bij de politie gedaan.

Bijna 1 miljoen mensen zagen in 2024 online oproepen tot openbare-ordeverstoring

In 2024 gaf 7 procent van de 15-plussers aan in de afgelopen twaalf maanden weleens online berichten gezien te hebben waarin opgeroepen werd tot openbare-ordeverstoring of activiteiten die daar vaak toe leiden (zoals straatraces, demonstraties of illegale feesten). Dat zijn bijna 980 duizend mensen. In 2022 was het aandeel hoger, namelijk 9 procent.

Verreweg de meeste mensen die deze berichten zagen, zeiden dat het ging om een oproep tot demonstratie (55 procent). Berichten die oproepen tot illegale feesten of evenementen werden door 12 procent genoemd en berichten die oproepen tot rellen door 9 procent.

Het merendeel dat een online oproep tot ordeverstoring had gezien, gaf aan niets met het bericht te hebben gedaan (84 procent). Een melding bij de politie maakte 4 procent en eveneens 4 procent zei te hebben deelgenomen aan de activiteit waartoe werd opgeroepen.

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

De helft van de bevolking van 15 jaar of ouder gaf aan zich (heel) veilig te voelen als ze internet gebruiken. Ondanks het feit dat ruim een kwart zich veel zorgen maakt over zaken als misbruik van bank- en persoonsgegevens op internet, voelde slechts 4 procent zich onveilig of heel onveilig als ze het internet gebruikten. Het grootste deel (45 procent) voelde zich niet veilig en ook niet onveilig.

Vrijwel iedereen neemt maatregelen om persoonlijke gegevens op internet te beschermen

In 2024 gaf, net als in 2022, 95 procent van de 15-plussers aan persoonlijke gegevens op internet te beschermen. Van de negen in het onderzoek voorgelegde beschermingsmaatregelen (zoals het beperken van de toegang tot locatie- of profielgegevens, het controleren van de veiligheid van websites en het blokkeren van cookies) had 66 procent vijf of meer maatregelen genomen, 20 procent drie of vier maatregelen en 9 procent één of twee.

Spam, hacken, ID-fraude en back-ups maken het meest bekend, passkey, social engineering en doxing het minst

Mensen waren het meest bekend met de begrippen spam, hacken, identiteitsfraude en back-ups maken. Ongeveer 90 procent heeft niet alleen van één of meer van deze begrippen gehoord, maar weet ook wat ze betekenen. 80 procent gaf aan te weten wat phishing is en bijna 80 procent weet wat met WhatsApp-fraude wordt bedoeld. Het minst bekend waren de relatief nieuwe begrippen doxing, social engineering en passkey.

De meeste zorgen over diefstal of misbruik van bank- en persoonsgegevens

Op het gebied van internetveiligheid maakten mensen zich het meest zorgen over diefstal van persoonsgegevens bij een organisatie na een hack of door een datalek, misbruik van bankgegevens en misbruik van persoonsgegevens. Ruim een kwart maakte zich veel zorgen over deze veiligheidsaspecten. Over het misbruik maken van accounts, het hacken van een apparaat of account en het verspreiden van foto's of video's zonder toestemming maakte ongeveer 20 procent zich veel zorgen. De minste bezorgdheid was er om online gediscrimineerd te worden: 7 procent maakte zich hierover veel zorgen en meer dan 70 procent niet.

Toegangscode of wachtwoord meest gebruikte en lang wachtwoord minst gebruikte beveiligingsmaatregel

De meest gebruikte maatregelen om apparaten en accounts met persoonlijke informatie te beveiligen tegen misbruik door anderen waren het vergrendelen van apparaten met een toegangscode, wachtwoord, vingerafdruk of Face ID, en het controleren van bijlages in e-mails vóór het openen ervan. Ruim 4 op de 5 mensen gebruikten toegangsbeveiliging voor alle apparaten en bijna 4 op de 5 controleerden e-mailbijlages. Bijna 3 op de 5 zeiden updates van apparaten of apps direct of zo snel mogelijk uit te voeren. Het gebruik van tweetrapsverificatie en vooral het gebruik van een VPN-verbinding en wachtwoorden van minimaal 16 tekens waren maatregelen die het minst vaak werden genomen.

Informatiepunt Digitale Overheid meest bekende dienst als men hulp nodig heeft

Het Informatiepunt Digitale Overheid (te vinden in openbare bibliotheken) was de meest bekende dienst waar men terecht kan voor hulp bij het online regelen van dingen of bij het gebruik van een computerprogramma of app. Deze dienst kende 34 procent van naam en 2 procent had weleens om hulp gevraagd bij het Informatiepunt Digitale Overheid. DigiHulplijn en Veiliginternetten.nl waren minder bekende diensten.

10.2 Aanbevelingen voor toekomstig onderzoek

10.2 Aanbevelingen voor toekomstig onderzoek

Criminelen zijn voortdurend op zoek naar nieuwe manieren om mensen online op te lichten, computers te hacken, of 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 er steeds nieuwe vormen van online criminaliteit en nieuwe beschermingsmaatregelen worden ontwikkeld en toegepast. Om deze veranderingen goed in het vizier te houden, is het wenselijk de ontwikkeling van online veiligheid en criminaliteit jaarlijks te monitoren.

Bij het analyseren van de data van OVeC 2024 en bij de totstandkoming van deze publicatie is een aantal vragen naar boven gekomen die de moeite waard zijn om verder te onderzoeken.

- Een eerste belangrijke vraag is welke persoonskenmerken de beste voorspellers zijn van slachtofferschap. Wanneer er een samenhang is tussen bepaalde persoonskenmerken en online criminaliteit, is dit een aanwijzing dat er bij deze groep(en) een kwetsbaarheid bestaat om slachtoffer te worden van cybercrime. In OVeC 2024 zijn aanwijzingen gevonden dat een dergelijke kwetsbaarheid bestaat bij personen met een andere seksuele oriëntatie dan een heteroseksuele. Uit eerder onderzoek komt een vergelijkbaar beeld naar voren (Kennis, 2024). Ook personen met een genderidentiteit anders dan man of vrouw (ook wel non-binair/genderqueer personen) bleken zich vaker onveilig te voelen en vaker slachtoffer te zijn van criminaliteit, en dan met name van geweldsdelicten. Er wordt aanbevolen om in een volgende editie van OVeC meer aandacht te besteden aan seksuele oriëntatie en genderidentiteit, om zo inzicht te krijgen in de omvang van het probleem als het gaat om slachtofferschap van online criminaliteit, met name van online bedreiging en intimidatie.
- Naast vragen over online criminaliteit werd in OVeC 2024 ook ingegaan op internetgebruik en online veiligheid. Hierdoor is het mogelijk om onderwerpen zoals digitale vaardigheden, het nemen van beveiligingsmaatregelen en de veiligheidsbeleving te relateren aan slachtofferschap van online criminaliteit (van verschillende delicten).
- In OVeC 2024 gaf het merendeel van de bevolking aan geen behoefte te hebben aan informatie of voorlichting over online criminaliteit. Dit roept de vraag op wat de voornaamste redenen hiervoor zijn. Is dat omdat mensen al voldoende weten, bijvoorbeeld omdat online criminaliteit vaker in de media komt? Of omdat informatiecampagnes, zoals Laat je niet interneppen hun vruchten hebben afgeworpen? Of heeft men het vanwege de complexiteit van de materie juist opgegeven het te begrijpen? Verder onderzoek zou meer licht kunnen werpen op deze en andere vragen omtrent informatiebehoefte en voorlichting.
- Een andere interessante kwestie is in hoeverre de meldings- en aangiftebereidheid van online criminaliteit samenhangt met de aard en ernst van het voorval. Worden bepaalde typen delicten vaker gemeld of aangegeven? Speelt de mate waarin mensen de delicten als strafbaar beschouwen een rol in de meldings- en aangiftebereidheid? Of draagt juist de mate waarin mensen een delict als inbreuk op hun leven beschouwen bij tot hun aangiftebereidheid?
- In OVeC 2024 werd aan alle deelnemers gevraagd welke beveiligingsmaatregelen zij hadden getroffen op het moment dat zij de vragenlijst invulden. Alleen aan slachtoffers van hacken werd ook gevraagd welke maatregelen zij al vóór het delict hadden getroffen. Het kan zinvol zijn om in meer detail uit te zoeken of ook de slachtoffers van andere online delicten meer of nog andere beveiligingsmaatregelen zijn gaan treffen naar aanleiding van het voorval. Met andere woorden, worden mensen die minder beveiligingsmaatregelen treffen eerder slachtoffer van online criminaliteit en hangt dit af van het soort beveiligingsmaatregel? Zijn er verschillen tussen de verschillende vormen van online criminaliteit?
- Naast het treffen van beveiligingsmaatregelen kan ook worden ingezoomd op veranderingen in het gebruik van internet als gevolg van de ervaren online criminaliteit. Zijn slachtoffers van online criminaliteit bijvoorbeeld minder of op een andere manier internet gaan gebruiken? En hoe zit dat het met gebruik van social media? Hebben zij zich (beter) laten informeren over mogelijke veiligheidsrisico's op het internet?

Los van deze aanvullingen en aanpassingen, zou een herhaling van OVeC in 2026 de gelegenheid bieden om beter in te spelen op de ontwikkeling van de mate waarin mensen worden blootgesteld aan de verschillende vormen van online criminaliteit en hier slachtoffer van worden. Tevens geeft het de mogelijkheid om nieuwe fenomenen op het gebied van online veiligheid en criminaliteit en de behoefte aan informatie, voorlichting en bescherming van de bevolking in kaart te brengen. Dit kan bestuurders en beleidsmakers helpen bij het maken van keuzes aangaande online criminaliteit.

Bijlage A. Onderzoeksbeschrijving

In deze onderzoeksbeschrijving wordt de opzet en uitvoering van het onderzoek *Online Veiligheid en Criminaliteit 2024* kort beschreven. Achtereenvolgens komen aan de orde:

- Steekproef en respons
- Dataverzameling
- Vragenlijst
- Weging
- Schattingen en betrouwbaarheidsmarges
- Gebruikte analysemethoden

Voor geïnteresseerden zijn separate notities over het steekproefontwerp, dataverzameling en de weging van het onderzoek OVeC 2024 op aanvraag beschikbaar.

Steekproef en respons

Voor de vergelijkbaarheid met de Veiligheidsmonitor (VM), die onder andere ook het slachtofferschap van online criminaliteit meet, is bij het steekproefontwerp van OVeC 2024 zoveel mogelijk aangesloten bij dat van de VM 2023 en OVeC 2022.

De doelpopulatie voor OVeC 2024 bestaat uit alle in Nederland woonachtige personen die 15 jaar of ouder zijn en die deel uitmaken van een particulier huishouden. De institutionele bevolking, dat zijn personen in inrichtingen, instellingen of tehuizen, behoort niet tot de doelpopulatie en wordt dus niet benaderd.

Het steekproefontwerp heeft als uitgangspunt dat minimaal 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 responsschattingen zijn in totaal 100 duizend personen voor deelname aan het onderzoek benaderd. In totaal hebben 33 236 personen meegedaan, het responspercentage bedroeg daarmee 33,2 procent.

Dataverzameling

De dataverzameling vond plaats van 14 augustus tot 28 oktober 2024. Bij de uitvoering ervan is uitsluitend gebruikgemaakt van internetenquêtering. De 100 duizend steekproefpersonen ontvingen bij aanvang van het onderzoek een aanschrijfbrief met daarin het verzoek om via internet deel te nemen. Drie weken na de aanschrijfbrief is aan mensen die nog niet gerespondeerd hadden, een eerste rappelbrief verstuurd met daarin opnieuw het verzoek om via internet deel te nemen aan het onderzoek. 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 smartwatch of cadeaubon te winnen). De steekproef is in drie groepen verdeeld en elke groep ontving op een ander moment de aanschrijfbrief. Zo werden risico's, bijvoorbeeld door problemen met de postbezorging of servers die niet goed werken, gespreid.

Vragenlijst

De vragenlijst van OVeC 2024 is door het CBS opgesteld in overleg met het ministerie van Justitie en Veiligheid, waarbij zoveel mogelijk aangesloten is bij de vraagstellingen in OveC 2022. Voor de vragenlijst van OveC 2022 is voor online veiligheid zoveel mogelijk aangesloten bij de vraagstellingen van de ICT-enquête en het pilotonderzoek Digitale Veiligheid en Criminaliteit (Akkermans et al, 2019), en voor online criminaliteit is zoveel mogelijk aangesloten bij de vraagstellingen in de Veiligheidsmonitor 2021. Voor de VM 2021 hebben ook de vraagstellingen uit het pilotonderzoek Digitale Veiligheid en Criminaliteit als basis gediend.

Vragen over nieuwe vormen van online veiligheid en criminaliteit (zoals doxing) zijn in 2024 toegevoegd. Verder zijn enkele vragen over online oproepen tot openbare ordeverstoring in overleg aangepast.

De vragenlijst 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
    a. Aan- en verkoopfraude
    b. Hacken
    c. Online oplichting
    d. Fraude betalingsverkeer
    e. Identiteitsfraude
    f. Interpersoonlijke delicten
6. Online discriminatie
7. Online bedreiging en intimidatie
8. Doxing
9. Online oproepen tot openbare ordeverstoring
10. verige online delicten
11. Maatregelen vóór slachtofferschap hacken
12. Achtergrondkenmerken

Weging

Door non-respons is de groep respondenten van OVeC 2024 selectief. Om de uitkomsten te corrigeren voor deze selectiviteit, krijgt iedere respondent een weegfactor. De factoren zijn tot stand gekomen met hetzelfde weegmodel als dat van OVeC 2022. De weegvariabelen zijn ook hetzelfde als die van de Veiligheidsmonitor 2021/2023, en bestaan uit geografische, demografische en sociaaleconomische kenmerken.

Schattingen en betrouwbaarheidsmarges

Omdat OVeC 2024 een steekproefonderzoek is, zijn alle gepresenteerde cijfers schattingen met een bijbehorende betrouwbaarheidsmarge (aangegeven met een boven- en ondergrens). Deze betrouwbaarheidsmarge is behalve van het gekozen betrouwbaarheidsniveau en het onderzoeksdesign, vooral afhankelijk 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 bij herhaald uitvoeren van het onderzoek met dezelfde steekproefomvang in 95 van de 100 gevallen zou liggen tussen de marges behorende bij de gevonden waarde. De 95%-betrouwbaarheidsintervallen zijn beschikbaar in de bijbehorende Tabellenset 2024.

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 welvaart indirect (mede)bepaald worden door het kenmerk leeftijd (jongeren hebben relatief lagere welvaart dan ouderen). Met behulp van multivariate logistische regressieanalyses is gekeken of de verschillen naar achtergrondkenmerken statistisch significant blijven wanneer gecorrigeerd wordt voor de samenhang tussen deze kenmerken.

Bijlage B. Referenties

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. https://www.cbs.nl/nl-nl/nieuws/2019/29/1-2-miljoen-slachtoffers-van-digitale-criminaliteit

Akkermans, M., Derksen, E., Kennis, M., Kloosterman, R., en E. Moons (2024). *Veiligheidsmonitor 2023.* Centraal Bureau voor de Statistiek, Den Haag/Heerlen/Bonaire. https://www.cbs.nl/nl-nl/longread/rapportages/2024/veiligheidsmonitor-2023

College voor de Rechten van de Mens (2024). *Wat is discriminatie?* https://www.mensenrechten.nl/mensenrechten-voor-jou/discriminatie-en-gelijke-behandeling/wat-is-discriminatie

Derksen, E, Kennis, M., Kloosterman, R., Moons, E., en V. Peters (2024). *Prevalentiemonitor Huiselijk Geweld en Seksueel Grensoverschrijdend gedrag 2024.* Den Haag: Wetenschappelijk Onderzoek- en Documentatie Centrum samen met het Centraal Bureau voor de Statistiek. https://www.cbs.nl/nl-nl/longread/rapportages/2024/prevalentiemonitor-huiselijk-geweld-en-seksueel-grensoverschrijdend-gedrag-2024

Kennis, M. (2024). *Slachtofferschap en veiligheidsbeleving LHBTQIA personen.* Centraal Bureau voor de Statistiek, Den Haag/Heerlen/ Bonaire. https://www.cbs.nl/nl-nl/longread/statistische-trends/2024/slachtofferschap-en-veiligheidsbeleving-lhbtqia-personen

Kennis, M., en C. Reep (2024). *Schade van criminaliteit tegen burgers.* Centraal Bureau voor de Statistiek, Den Haag/Heerlen/ Bonaire. https://www.cbs.nl/nl-nl/longread/rapportages/2024/schade-van-criminaliteit-tegen-burgers

Politie (2024). *Wat is doxing?*
https://www.politie.nl/informatie/wat-is-doxing.html

Veiligbankieren.nl (2024). *Social engineering*
https://www.veiligbankieren.nl/fraude/social-engineering/

Veiliginternetten.nl (2024). *Wat is een passkey?*
https://veiliginternetten.nl/thema/basisbeveiliging/wat-is-een-passkey/

Veiliginternetten.nl (2024). *Wat is voice cloning?*
https://veiliginternetten.nl/thema/dagelijks-gebruik/ai/wat-is-voice-cloning/

Bijlage C. 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 2024 die aan deze publicatie is toegevoegd.

Bijlage D. Medewerkers

Judit Arends
Elianne Derksen
Mattijn Morren