# Cybersecurity onderzoek Alert Online 2025

Rapport Ipsos I&O

Ipsos i&O

Ministerie van Economische Zaken

# Colofon

**Uitgave**
Ipsos I&O
Piet Heinkade 55
1019 GM Amsterdam

**Rapportnummer**
2025/153

**Datum**
augustus 2025

**Opdrachtgever**
Ministerie van Economische Zaken

**Auteurs**
Melle Conradie
Bram Doms

# Inhoudsopgave

# 1. Samenvatting

# Samenvatting | Achtergrond

Alert Online is een gezamenlijk initiatief van overheid, bedrijfsleven en wetenschap, dat zich richt op het creëren van bewustwording rondom digitale veiligheid. Onderdeel van de campagne is sinds 2012 het jaarlijks terugkerende Cybersecurityonderzoek Alert Online. Dit onderzoek naar de beleving van de digitale veiligheid onder Nederlanders wordt sinds 2021 door Ipsos I&O in opdracht van het ministerie van Economische Zaken (EZ) uitgevoerd.

In dit rapport richten we ons op Nederlanders van 18 jaar en ouder. De resultaten van medewerkers mkb en grootbedrijf en ICT-verantwoordelijken staan in het separate rapport *Bedrijfsleven*. De resultaten voor ambtenaren komen terug in het separate rapport *Overheid*. In de samenvatting van dit rapport leggen we kruisverbanden met deze rapportages.

# Samenvatting | kennis en ervaring online risico's

**Driekwart Nederlanders vindt eigen kennis redelijk tot zeer goed**

De kennis over digitale risico's schat men vergelijkbaar in als in eerdere jaren. Een kwart van de Nederlanders vindt hun kennis matig of zeer slecht. Drie op de tien beoordelen hun kennis als goed tot zeer goed. De grootste groep (43%) plaatst zich in het midden en vindt de eigen kennis redelijk. De kennis die men heeft, komt vooral van familie of vrienden en campagnes van banken of de overheid. Werkenden krijgen veel van hun kennis via de ICT-afdeling op hun werk en via collega's. Nederlanders onder de 40 jaar en theoretisch geschoolden schatten hun kennis relatief hoger in.
We vroegen Nederlanders dit jaar voor het eerst naar hun kennis over generatieve AI. Drie op de tien (30%) geven aan hier goed tot zeer goed bekend mee te zijn. Een kwart vindt de eigen kennis daarentegen slecht (16%) of zeer slecht (12%).

## Pogingen tot phishing en helpdeskfraude meest ervaren vorm cybercrime[1]

In de afgelopen twaalf maanden had driekwart van de Nederlanders (72%) te maken met (geslaagde en niet geslaagde pogingen tot) cybercrime. Het ging vooral om phishing (meegemaakt door 55%) en telefonische helpdeskfraude (29%). De ervaringen met telefonische helpdeskfraude zijn verdubbeld ten opzichte van 2024, toen 15 procent dit meemaakte.
Tien van de elf voorgelegde vormen van cybercrime zijn bij een ruime meerderheid (54 tot 97%) bekend. Van de vormen die men kent, acht men het vooral waarschijnlijk om met phishing te maken te krijgen: 67% van de mensen die weten wat phishing is, denken dit privé mee te kunnen maken. Daarna volgen hacking (55%), malware (55%) en helpdeskfraude (54%). Iets minder mensen dan in 2024 achten het nu waarschijnlijk om hacking mee te maken (2025: 55%; 2024: 61%). De geschatte kans op het meemaken van DDoS-aanvallen is iets hoger dit jaar (2025: 21%; 2024: 18%).Van de vormen van cybercrime die men waarschijnlijk acht om privé mee te maken, vroegen we hoe erg men dit zou vinden.
Van alle vormen van cybercrime die men waarschijnlijk acht om mee te maken, lijkt 63 tot 88 procent het (heel) erg om mee te maken. Nederlanders lijkt het vooral erg om identiteitsfraude mee te maken.

## Veel vertrouwen in overheid als het gaat om informatie digitale veiligheid

Een vijfde van de Nederlanders (21%) zet de overheid op plek 1 als partij die ze het meest vertrouwen als het gaat om informatie over digitale veiligheid. Daarna heeft men het meeste vertrouwen in de politie (14% plek 1) en banken (13% plek 1). Telefoonaanbieders (43%) en vrienden en kennissen (16%) worden het vaakst genoemd als partijen die men het minder dan andere partijen vertrouwt. We vroegen hierbij niet naar de mate van vertrouwen, wat betekent dat ook het vertrouwen in deze partijen nog steeds hoog kan zijn.

[1] *Er bestaan verschillende definities van cybercrime. In dit onderzoek is een brede definitie gehanteerd waar bijvoorbeeld ook poging tot WhatsAppfraude en CEO-fraude onder vallen. De volledige lijst staat in de figuur op pagina 20.*

# Samenvatting | zorgen om digitale veiligheid

### Zorgen over eigen digitale veiligheid nemen licht af

De helft (51%) van de Nederlanders maakt zich geen of weinig zorgen over digitale veiligheid in de privésituatie. Twee op de vijf (40%) maken zich hier enige zorgen over. Dat is een afname ten opzichte van 2024 (45%) en vergelijkbaar met 2023 (41%). Acht procent maakt zich veel zorgen over de eigen digitale veiligheid; dit is vergelijkbaar met 2024. Meer dan over de eigen digitale veiligheid maakt men zich zorgen over de digitale veiligheid van naasten en de digitale veiligheid van Nederland. De meerderheid maakt zich (zeer) veel (15%) of enige zorgen (40%) over hun naasten. Wel is het aandeel dat zich hier (zeer) weinig zorgen over maakt gegroeid van 37 procent in 2024 naar 42 procent in 2025. Dit jaar vroegen we voor het eerst naar de digitale veiligheid van Nederland: 31 procent maakt zich hier (zeer) veel over en 20 procent heeft weinig of geen zorgen. Nederlanders onder de 40 jaar maken zich minder zorgen over hun eigen digitale veiligheid in de privésituatie en de digitale veiligheid van Nederland dan oudere Nederlanders. Mensen in de leeftijd 40-64 jaar maken zich relatief vaak zorgen over hun naasten.

### Vooral zorgen over (controle)verlies van gegevens en kwijtraken geld

De voornaamste aspecten waarover men zich zorgen maakt bij de eigen digitale veiligheid zijn het in de verkeerde handen vallen van gegevens (70%), het geen controle hebben over wat er met gegevens gebeurt (64%) en het kwijtraken van geld (59%). Meer dan in 2024 zijn Nederlanders bezorgd dat anderen zich online als hen voordoen (2025: 42%; 2024: 36%).

### Updaten, controleren op valse websites/links en twee-staps-inloggen redenen om weinig zorgen te hebben

De Nederlanders die zich weinig of geen zorgen maken over hun digitale veiligheid in hun privésituatie, geven hier verschillende redenen voor. De helft (48%) noemt dat ze hun apparaten altijd updaten als reden om zich geen zorgen te maken. Het controleren op valse websites/links (47%) en het gebruik van twee-staps-inloggen (46%) zijn voor ongeveer evenveel mensen redenen om zich weinig zorgen te maken. Men noemt vaker dan in 2024 zich veilig te voelen door het doen van virusscans (2025: 37%; 2024: 31%) en het maken van back-ups (2025: 32%; 2024: 21%). Minder vaak dan een jaar eerder noemt men het hebben van veel verschillende wachtwoorden als reden waarom men zich veilig voelt (2025: 32%; 2024: 42%).

# Samenvatting | online gedrag

### Waardering omgang met online risico's stabiel

Nederlanders geven zichzelf een 6,9 voor het omgaan met online risico's. Sinds 2022 zit het gemiddelde elk jaar rond dit cijfer. Zes op de tien Nederlanders (59%) geven zichzelf een 6 of een 7. Drie op de tien (30%) geven zichzelf een 8 of hoger. Tien procent geeft zichzelf een onvoldoende. Mannen geven zichzelf relatief hogere cijfers dan vrouwen (mannen: 7,1; vrouwen: 6,7).

### Veel Nederlanders passen maatregelen toe ten behoeve van digitale veiligheid

Vrijwel alle Nederlanders controleren links waar ze op klikken (95%), downloaden apps via officiële kanalen (94%), voeren automatische updates uit (93%), gebruiken twee-staps-inloggen (92%) en lange wachtwoorden (92%). Nederlanders onder de 40 jaar gebruiken minder vaak virusscanners en firewalls. Ze gebruiken vaker adblockers en browserextensies. Vijfenzestigplussers en vrouwen schakelen vaker hulp in van familie/vrienden bij digitale vragen.

Twee derde van de Nederlanders (69%) zegt meestal of altijd te controleren of mobiele apps veilig en betrouwbaar zijn voordat ze deze installeren. De helft (46%) maakt meestal of altijd back-ups van bestanden thuis. Dit is toegenomen ten opzichte van 2024. Toen maakte een kwart (25%) thuis geen back-ups, nu is dat 20 procent. Twee derde (66%) zorgt er meestal of altijd voor dat slimme apparaten de laatste updates gebruiken. Dit doen ze vooral omdat ze willen dat de slimme apparaten goed werken (73%) en dat ze deze veilig kunnen gebruiken (70%).

### Meeste werkenden denken het te vertellen als ze per ongeluk een virus downloaden

Vier op de vijf werkenden verwachten het aan de ICT-afdeling (81%) of aan iemand anders op het werk (78%) te vertellen als ze per ongeluk een virus downloaden. Vrijwel niemand zegt dit zeker niet te doen. Een klein deel van de werkenden (4%) verwacht het door schaamte niet te vertellen als ze een virus op het werk downloaden. Van alle Nederlanders verwacht 55 procent zich te schamen wanneer ze in een phishingmail zouden trappen.

# Samenvatting | slachtofferschap en aangiftebereidheid

### Ervaringen met helpdeskfraude verdubbeld in afgelopen jaar

Driekwart van de Nederlanders (72%) heeft in de twaalf maanden voor het onderzoek te maken gehad met een voorval van cybercrime. Dat is vergelijkbaar met het onderzoek van 2024. Het meest maakte men (poging tot) phishing mee (55%). Daarna volgt telefonische helpdeskfraude (29%). Dit is toegenomen ten opzichte van 2024. Toen maakte 15 procent dit mee in de twaalf maanden voor het onderzoek. Theoretisch geschoolden zeggen vaker dan anderen voorvallen mee te maken, vooral pogingen tot phishing maken ze vaker mee.

### Minderheid schaamt zich na meemaken cybercrime

Wanneer men een voorval meemaakt, zijn de gevolgen in de meeste gevallen niet ernstig of zijn er helemaal geen gevolgen. Bijvoorbeeld als men wel is benaderd voor helpdeskfraude, maar hier niet intrapte.
Twee derde (69%) schaamde zich niet na het meemaken van cybercrime. Ook kostte het driekwart (73%) weinig moeite om aan anderen te vertellen wat er gebeurd was. Maar wanneer de ervaren gevolgen van de cybercrime ernstiger zijn, schaamt men zich vaker en heeft men meer moeite om het te vertellen.

### Twee derde doet geen melding of aangifte van cybercrime in privésituatie

Van de 72 procent Nederlanders die een voorval van cybercrime meemaakten, doet één op de drie (33%; 2024: 28%) aangifte of melding. Het meest doet men melding bij de Fraudehelpdesk (11%) of bij de bank (10%). Vier procent doet aangifte bij de politie en ook 3 procent maakt melding bij de politie. Wanneer men (lichte of ernstige) gevolgen ervaart van het voorval, doet men vaker melding of aangifte (in 64% van de gevallen) dan wanneer men geen gevolgen ervaart (actie in 29% van de gevallen).

De voornaamste reden om geen actie te ondernemen is dat men weinig schade ondervond (65%; 2024: 55%). Daaraan gerelateerd vindt 34 procent het niet zo belangrijk (2024: 11%). Zeventien procent doet niks omdat men denkt dat er niks gedaan wordt met een melding of aangifte. In 2024 noemde men dit vaker als reden (25%). Als men wel een melding maakt of aangifte doet, is dat vooral omdat men wil voorkomen dat de dader dit opnieuw bij een ander doet (62%).

Een kwart (25%) geeft aan dat ze naar aanleiding van de cybercrime die ze meemaakten op een andere manier omgaan met digitale veiligheid. Naarmate de gevolgen van het meegemaakte voorval ernstiger zijn, gaan mensen vaker op een andere manier om met hun digitale veiligheid.

# Samenvatting | uitkomsten onderzoek bedrijfsleven

Hieronder worden resultaten uit het deelrapport bedrijfsleven beschreven.

### Medewerkers schatten eigen kennis over online veiligheid hoger in dan in 2024

Een derde (34%) van de medewerkers schat hun eigen kennis over online veiligheid in als (zeer) goed. In 2024 lag dit percentage op 27 procent. ICT-verantwoordelijken schatten hun kennis hoger in dan andere medewerkers. Het aandeel ICT-verantwoordelijken dat zijn kennis als (zeer) goed beoordeeld is 61 procent.

### ICT-verantwoordelijken schatten risico cybercrime hoger in

ICT-verantwoordelijken zijn naar eigen zeggen beter bekend met de betekenis van de elf voorgelegde verschillende vormen van cybercrime dan andere medewerkers. Van de vormen van cybercrime die men kent, achten medewerkers het meemaken van phishing in de werksituatie het meest waarschijnlijk (61%). Van de ICT-verantwoordelijken vindt 70 procent het waarschijnlijk dat ze phishing op het werk meemaken. Ook van alle andere voorgelegde vormen van cybercrime wordt het door ICT-verantwoordelijken aannemelijker geacht om er op het werk mee te maken te krijgen dan door andere medewerkers.

### ICT-verantwoordelijken maken zich meer zorgen over online veiligheid dan medewerkers

Ruim vier op de tien ICT-verantwoordelijken (43%) maken zich (zeer) veel of enige zorgen over hun eigen online veiligheid op het werk. Onder medewerkers is dit percentage lager (27%). ICT-verantwoordelijken geven zichzelf een hoger cijfer (7,4) als het gaat om het veilig omgaan met online risico's dan andere medewerkers (6,9).

### Een vijfde van kleine bedrijven onderneemt geen actie om veilig online te zijn

Twee-staps-inloggen is de meest genomen actie ten behoeve van online veilig zijn bij bedrijven (55% noemt dat dit binnen hun organisatie verplicht is). Ook door ICT-verantwoordelijken (64%) en medewerkers van grote bedrijven (64%) wordt deze maatregel (net zoals in 2024) het vaakst genoemd. Kleine bedrijven (minder dan 10 medewerkers) ondernemen minder acties. Een vijfde van deze bedrijven (20%) onderneemt zelfs geen enkele actie ten behoeve van veilig online zijn. De meeste werknemers (80%) voelen zich comfortabel om cyberincidenten te melden binnen hun organisatie.

## In werksituatie komt phishing het vaakst voor

Drie op de tien medewerkers (31%) ontvingen in de afgelopen twaalf maanden een phishingmail op hun werk. Onder ICT-verantwoordelijken was dit 44 procent. Het aandeel medewerkers dat phishing meemaakte nam toe van 25% in 2024 naar 31% in 2025. Ook het gebeld worden door een zogenaamde officiële instantie nam toe (2024: 3%; 2025: 7%). Net zoals in 2024 zeggen ICT-verantwoordelijken vaker te maken te hebben met de verschillende voorgelegde vormen van cybercrime dan andere medewerkers.

## Meerderheid onderneemt geen actie op cybercrime

In de helft (47%) van de gevallen dat een medewerker te maken kreeg met cybercrime is er geen melding gemaakt of aangifte gedaan. Medewerkers die wel actie ondernamen deden dat overwegend door melding te maken bij de ICT-afdeling van hun bedrijf (45%).
De belangrijkste reden van medewerkers om aangifte of melding te doen is het creëren van een veiligere online omgeving (60%). Twee op de vijf medewerkers die geen aangifte doen, geven aan dat ze geen of weinig schade ondervonden (41%). Een derde (35%) vond het (daarnaast) niet zo belangrijk. Vijf procent zegt dat het geen zin heeft om aangifte of melding te doen, onder ICT-verantwoordelijken is dit aandeel een vijfde (22%).

## Meer dan helft medewerkers gebruik generatieve AI

Een op de drie medewerkers (36%) zegt uitstekend of zeer goed bekend te zijn met generatieve AI, zoals ChatGPT of beeld- en tekstgenererende AI-modellen. Een kwart weet er weinig (14%) of zeer weinig van (9%).
De helft van de medewerkers zegt dat zijn of haar organisatie soms (35%) of structureel (14%) generatieve AI gebruikt. Een kwart van de medewerkers weet niet of dit gebeurt. Een kwart van de medewerkers (26%) vindt dat hun organisatie duidelijke richtlijnen heeft voor het gebruik van generatieve AI om potentiële risico's (bijvoorbeeld op het gebied van dataveiligheid) te beheersen. Een kwart (23%) is het hier juist niet mee eens. Twee op de vijf (38%) kunnen het niet goed beoordelen.
ICT-verantwoordelijken schatten hun kennis over AI hoger in dan andere medewerkers. Ook weten ze beter wat binnen de organisatie gebeurt op het gebied van AI en zijn ze positiever over de richtlijnen voor AI in de organisatie. Bijna de helft van de ICT-verantwoordelijken (45%) vindt dat er goede richtlijnen zijn en een vijfde (22%) is het daar niet mee eens.

# Samenvatting | uitkomsten onderzoek overheid

Hieronder worden resultaten uit het deelrapport overheid beschreven.

### Acht op de tien ambtenaren schatten eigen kennis online veiligheid in als redelijk tot goed

Acht op de tien ambtenaren vinden dat de eigen kennis over online veiligheid redelijk tot zeer goed is. Een vijfde vindt het eigen kennisniveau matig of nog minder (17% matig, 3% slecht, 0% zeer slecht). Dat is vergelijkbaar met de inschatting van medewerkers in het grootbedrijf.

### Drie op de tien ambtenaren maken zich wel eens zorgen om digitale veiligheid op het werk

Zeven op de tien ambtenaren (71%) zijn relatief zorgeloos over de digitale veiligheid in de werksituatie. Drie op de tien maken zich enige (26%) of veel (3%) zorgen. Het beeld is vergelijkbaar met een jaar eerder. Onder medewerkers van het grootbedrijf is een vergelijkbaar beeld te zien. Ambtenaren beoordelen zichzelf met een 6,9 voor het omgaan met online risico's. Negen procent van de ambtenaren geeft zichzelf een onvoldoende hiervoor. Een kwart van de ambtenaren (25%) geeft zichzelf een 8 of hoger. Dat is minder dan vorig jaar (37% gaf zichzelf toen een 8 of hoger).

### Meer acties ondernomen voor online veilig gedrag

Twee-staps-inloggen is de meest genomen maatregel voor online veilig gedrag bij de overheid: bij driekwart van de ambtenaren is dat verplicht. Ten opzichte van 2024 worden er meer acties ondernomen om veilig gedrag te bevorderen. Zo worden er meer trainingen over online veiligheid gegeven (van 48% naar 59%) en is er vaker een digitale hulpverlener (van 42% naar 57%). Ook kunnen vaker alleen systeembeheerders software installeren.

## Melden mogelijke bedreigingen wordt in de meeste organisaties gewaardeerd

De meeste ambtenaren vinden dat het gemakkelijk is om zich aan de afspraken over veilig online gedrag te houden (91%). Ook de tools en instrumenten die men daarvoor krijgt, vinden ambtenaren goed (90%). Bij 87 procent van de ambtenaren wordt het gewaardeerd als mogelijke bedreigingen worden gemeld. Driekwart (77%) vindt dat digitale veiligheid hoog op de agenda staat van de directie. Wel vinden ambtenaren minder vaak dan medewerkers van het grootbedrijf dat afspraken voldoende worden toegepast.

## Schaamte weerhoudt ambtenaren niet om cyberincidenten te melden

Het overgrote deel van de ambtenaren zou een gedownload virus meteen melden bij de ICT-afdeling (94%), vier procent zou dit uit schaamte niet doen. Twee derde van de ambtenaren (64%) zou zich schamen als ze op een phishinglink zouden klikken. Toch voelen negen op de tien (88%) zich wel comfortabel genoeg om een incident te melden als ze dit zouden meemaken. Bij driekwart van de ambtenaren (74%) wordt open communicatie over cyberincidenten dan ook aangemoedigd.

Bij de helft van de ambtenaren wordt generatieve AI binnen de organisatie gebruikt. Een derde (35%) krijgt vanuit de organisatie ook duidelijke richtlijnen over het gebruik ervan.

## Meer meegemaakte voorvallen cybercrime op werk

Vier op de tien ambtenaren (43%) maakten in de afgelopen 12 maanden een of meerdere pogingen tot cybercrime mee op het werk. Dat is meer dan in 2024 (toen: 29%). Vooral phishing (van 22% naar 32%) en telefoontjes van iemand die zich anders voordeed (van 1% naar 10%) kwamen vaker voor.

De helft van de ambtenaren deed geen melding of aangifte van de cybercrime waar ze slachtoffer van werden op het werk. De helft die wel een melding maakte, deed dit vaak bij de eigen ICT-afdeling. De voornaamste reden om geen actie te ondernemen, is dat het incident niet als belangrijk werd gezien (34%) of dat er weinig schade ondervonden werd (33%). De belangrijkste redenen om wel aangifte te doen, zijn het creëren van een veiligere online omgeving (49%) en voorkomen dat de dader nieuwe slachtoffers maakt (42%).

# 2. Inleiding en achtergrond

# Inleiding

## Aanleiding en achtergrond

Alert Online is een gezamenlijk initiatief van overheid, bedrijfsleven en wetenschap, dat zich richt op het creëren van bewustwording rondom digitale veiligheid. Daarnaast beoogt Alert Online onder diverse doelgroepen de kennis over digitale veiligheid te vergroten en cyberveilig gedrag te stimuleren. Dit wordt gedaan door kennisoverdracht via veiliginternetten.nl, het Digital Trust Center en met een specifiek partnernetwerk van organisaties in Nederland. Onderdeel van de campagne is het jaarlijks terugkerende Cybersecurityonderzoek Alert Online, waarmee de cybersecuritymaand op 29 september wordt afgetrapt.

In opdracht van het ministerie van Economische Zaken (EZ) voerde Ipsos I&O dit onderzoek uit naar de beleving van de digitale veiligheid onder Nederlanders.

## Onderzoeksdoel

Het onderzoek beoogt aanknopingspunten te bieden voor communicatie en beleidsvorming. Dit doen we door middel van (1) het monitoren van het bewustzijn en de vaardigheden omtrent online veiligheid van Nederlanders door de jaren heen en (2) inzichten te vergaren in kennis, houding en gedrag van Nederlanders over digitale veiligheid.

## Onderzoeksvragen

De hoofdvraag van het onderzoek luidt:
**Wat is de kennis, houding en het gedrag van verschillende doelgroepen op het gebied van (verbeteren van) digitale veiligheid?**

Deze hoofdvraag bestaat uit drie deelvragen:
1 Wat weten de doelgroepen over digitale veiligheid en het verbeteren van de digitale veiligheid?
2 Wat vinden de doelgroepen van hun eigen online gedrag als het gaat om veiligheid en vaardigheden?
3 Wat doen de doelgroepen op het gebied van hun digitale veiligheid en het verbeteren daarvan?

Als doelgroepen onderscheiden we:
1 Nederlanders van 18 jaar en ouder;
2 medewerkers mkb en grootbedrijf;
3 ICT-verantwoordelijken;
4 ambtenaren.

In dit rapport richten we ons op Nederlanders van 18 jaar en ouder. De resultaten van medewerkers mkb en grootbedrijf en ICT-verantwoordelijken staan in het separate rapport *Bedrijfsleven*. De resultaten voor ambtenaren komen terug in het separate rapport *Overheid*. In de samenvatting van dit rapport leggen we kruisverbanden met deze rapportages.

## Leeswijzer

Hoofdstuk 3 tot en met 6 van dit rapport behandelen de resultaten van het algemeen publiek. Allereerst gaan we in op kennis van en ervaring met online risico's in hoofdstuk 3. De zorgen om digitale veiligheid worden in hoofdstuk 4 behandeld. In hoofdstuk 5 en 6 komen achtereenvolgens het online gedrag en aangiftebereidheid aan bod.

De percentages in deze rapportage worden afgerond op hele cijfers. Hierdoor tellen de percentages in sommige figuren en tabellen op tot 99 of 101 procent. In de rapportage zijn de uitkomsten waar mogelijk vergeleken met de resultaten van 2024. Significante toenames zijn weergegeven met het symbool "+" en significante afnames met het symbool "-". Daarnaast benoemen we verschillen tussen subgroepen van Nederlanders in de tekst, bij alle benoemde verschillen gaat het om significante verschillen ($p < .05$).

## Methode en respons algemeen publiek

Ipsos I&O voerde een landelijk representatief onderzoek uit onder Nederlanders van 18 jaar en ouder. In totaal werd een representatieve groep van 2.500 Nederlanders uitgenodigd waarvan er 1.230 (49%) meededen aan het onderzoek. De dataverzameling vond plaats in het I&O Research Panel[2] van 23 juni tot 7 juli 2025. Niet alle vragen die in dit rapport worden gepresenteerd, zijn aan alle 1.230 Nederlanders gesteld. Bij iedere tabel of figuur wordt de steekproefbasis vermeld.

De resultaten zijn gewogen naar leeftijd, geslacht, regio en opleidingsniveau. Daarmee zijn de resultaten representatief voor deze kenmerken.

[2] *https://www.ioresearch.nl/onderzoeksmethoden/io-research-panel/*

# 3. Kennis en ervaring online risico’s

# Driekwart Nederlanders vindt eigen kennis redelijk tot zeer goed

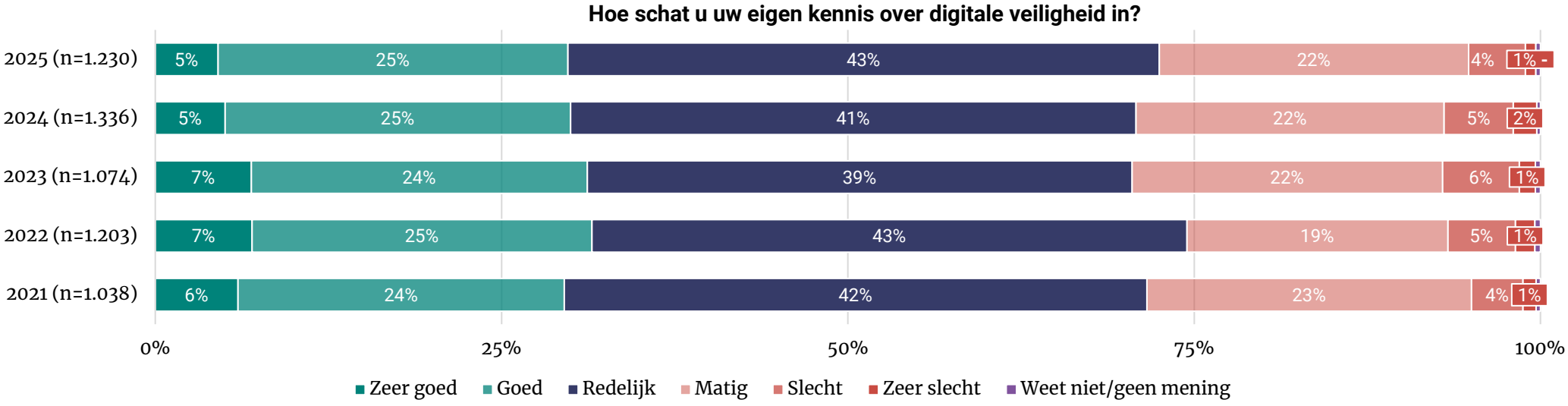
- Drie op de tien Nederlanders (30%) beoordelen hun eigen kennis als goed tot zeer goed. Een kwart (27%) vindt dat ze over matige of (zeer) slechte kennis beschikken. De grootste groep (43%) noemt de eigen kennis redelijk.

**Vergelijking met eerdere jaren**

- In 2024 zei nog 2 procent dat de eigen kennis zeer slecht is, in 2025 is dit gedaald naar 1 procent. Op de langere termijn valt op dat Nederlanders hun kennis vooral in 2022 iets minder vaak als matig of slecht inschatten.

**Resultaten subgroepen**

- Hoe jonger men is, des te vaker schat men de eigen kennis als (zeer) goed in. Ook mannen denken vaker dat ze goede kennis hebben van digitale veiligheid.
- Praktisch geschoolden geven naar verhouding minder vaak aan dat ze (zeer) goede kennis hebben.



# Twee op de vijf Nederlanders doen kennis via familie of vrienden op

- Voor twee op de vijf Nederlanders vormen familie en vrienden een belangrijke kennisbron.
- Drie op de tien noemen campagnes van banken en overheden.
- Onder werkenden is de ICT-afdeling op het werk een belangrijke bron van kennis over digitale veiligheid (45% van de werkenden noemt dit).

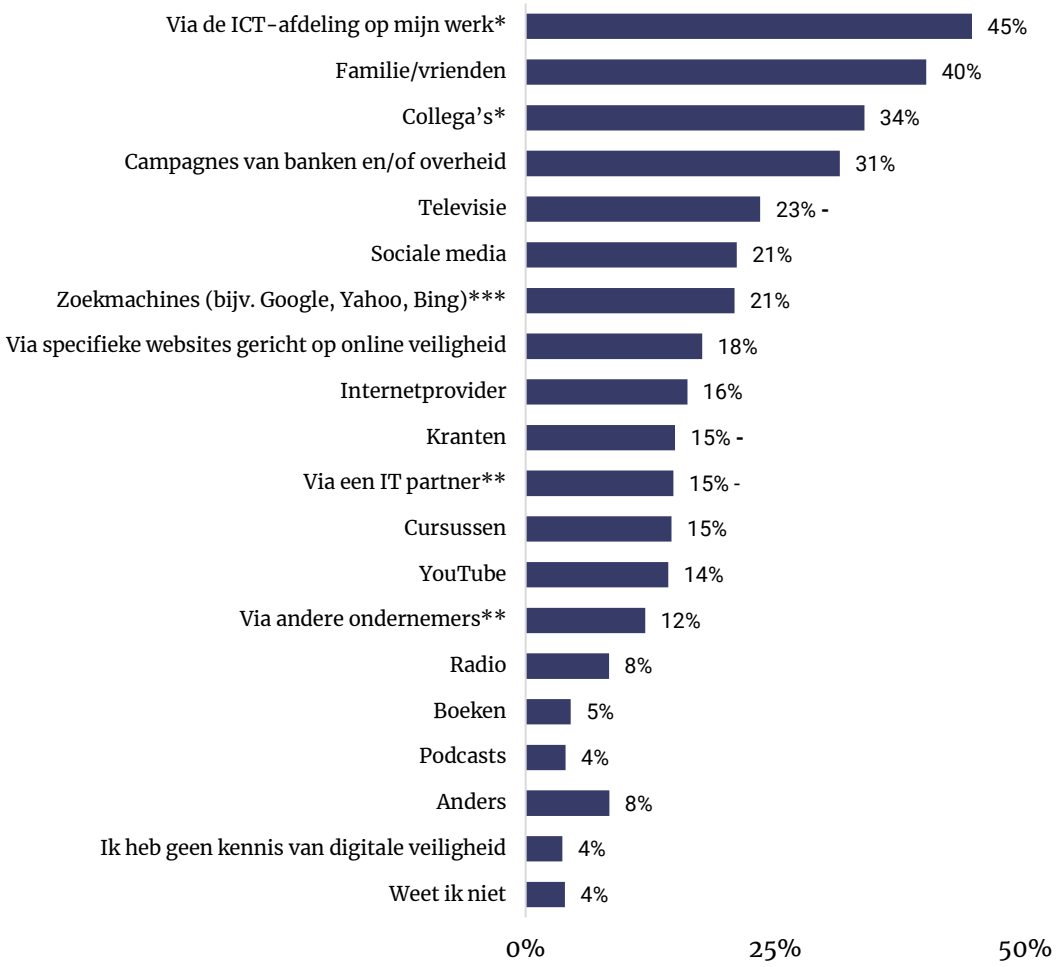
**Vergelijking met 2024**

- Minder vaak dan in 2024 noemt men televisie (van 30% naar 23%) en kranten (van 20% naar 15%).

**Resultaten subgroepen**

- Er zijn veel verschillen tussen subgroepen.
- Nederlanders onder de 40 jaar hebben vaker kennis via YouTube, podcasts, zoekmachines en sociale media opgedaan.
- Vijfenzestigplussers halen kennis vaker uit kranten en via familie/vrienden.
- Theoretisch geschoolden deden de kennis vaker op via podcasts, collega's of de ICT-afdeling op het werk.
- Praktisch geschoolden geven vaker dan anderen aan geen kennis te hebben over digitale veiligheid.

**Op welke manier heeft u kennis over digitale veiligheid opgedaan?** (n=1.230)




* Alleen voorgelegd aan werkenden (n=680).

** Alleen voorgelegd aan ondernemers (n=56).

*** Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

# Ruime meerderheid bekend diverse vormen van cybercrime

- De bekendste vormen van cybercrime zijn helpdeskfraude (97%), hacking (95%), identiteitsfraude (94%) en phishing (93%).
- Van de elf voorgelegde vormen is alleen CEO-fraude bij een minderheid bekend.

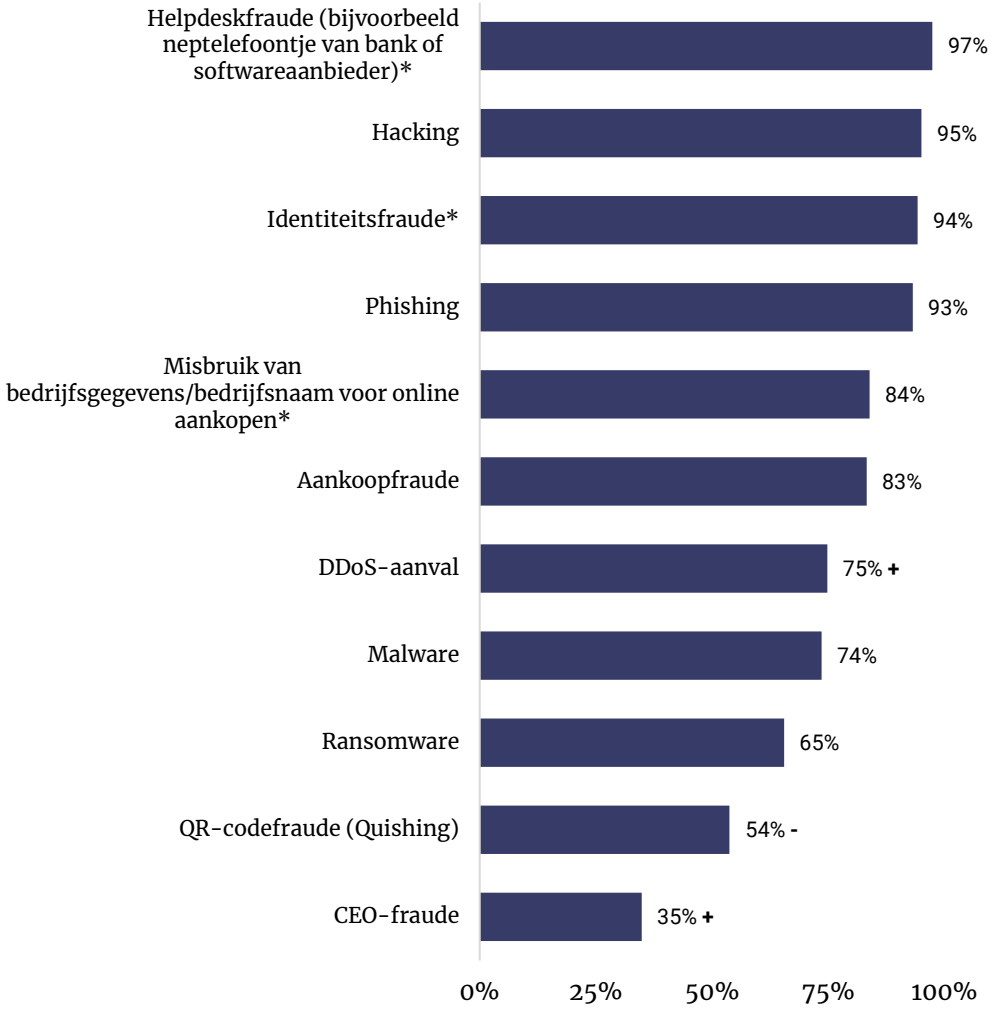
**Vergelijking met 2024**

- Men zegt vaker dan vorig jaar te weten wat een DDoS-aanval is (2025: 75%; 2024: 71%).
- Hoewel CEO-fraude het minst bekend is, is de bekendheid wel gestegen van 29 procent naar 35 procent.
- De bekendheid van QR-codefraude nam af van 60 procent naar 54 procent.

**Resultaten subgroepen**

- Bij vrijwel alle voorgelegde vormen van cybercrime geven theoretisch geschoolden vaker aan te weten wat het is.
- Ook is het kennisniveau van mannen naar eigen zeggen hoger dan dat van vrouwen.
- QR-codefraude, CEO-fraude en misbruik van bedrijfsgegevens zijn minder goed bekend bij 65-plussers.

**In welke mate bent u bekend met de onderstaande zaken?** (% bekend met; n=1.230)




* Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

# Phishing en helpdeskfraude maken relatief veel mensen mee

- Eén op de drie Nederlanders (32%) heeft weleens te maken gehad met phishing.
- Een kwart (27%) kreeg te maken met helpdeskfraude .
- Dit zijn duidelijk de twee meest voorkomende vormen van cybercrime. Zowel wanneer we kijken naar eigen ervaring als wat men hoort van bekenden.

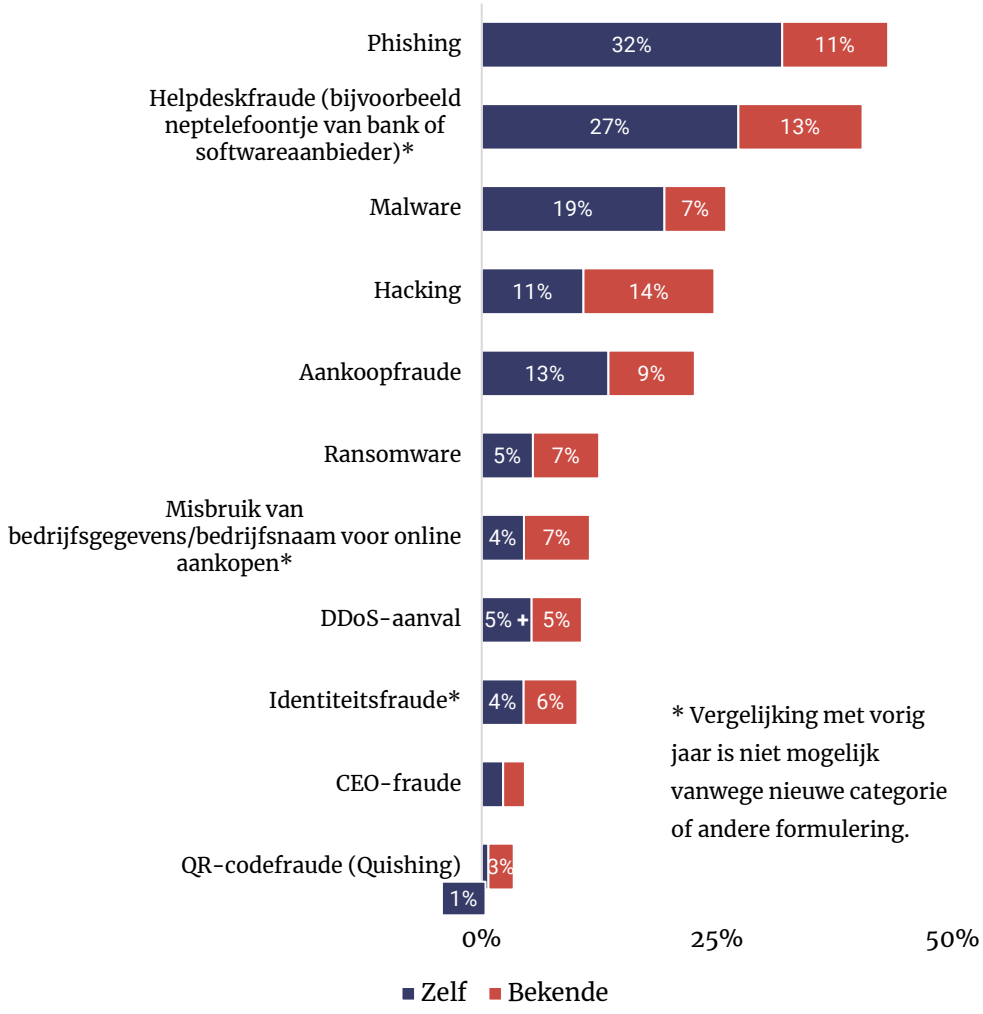
**Vergelijking met 2024**

- In 2025 geven meer mensen aan zelf ervaring te hebben met een DDoS-aanval (2025: 5%; 2024: 3%).

**Resultaten subgroepen**

- 18-39-jarigen kennen vaker dan andere leeftijdsgroepen mensen die malware, phishing of misbruik van bedrijfsgegevens meemaakten. Zelf maken ze naar verhouding vaker helpdeskfraude mee.
- Mannen hebben vaker dan vrouwen zelf ervaring met malware, ransomware, helpdeskfraude en DDoS-aanvallen.
- Theoretisch geschoolden hebben meer dan anderen zelf malware en phishing meegemaakt.

**In welke mate bent u bekend met de onderstaande zaken?** (% meegemaakt; n=1.230)



# Twee derde verwacht phishing in privésituatie mee te maken

- Van de mensen die bekend zijn met phishing, acht twee derde (67%) het waarschijnlijk hier in de privésituatie mee te maken te krijgen.
- Bij hacking (55%), malware (55%), helpdeskfraude (54%), identiteitsfraude (50%) en aankoopfraude (48%) is dat ongeveer de helft.

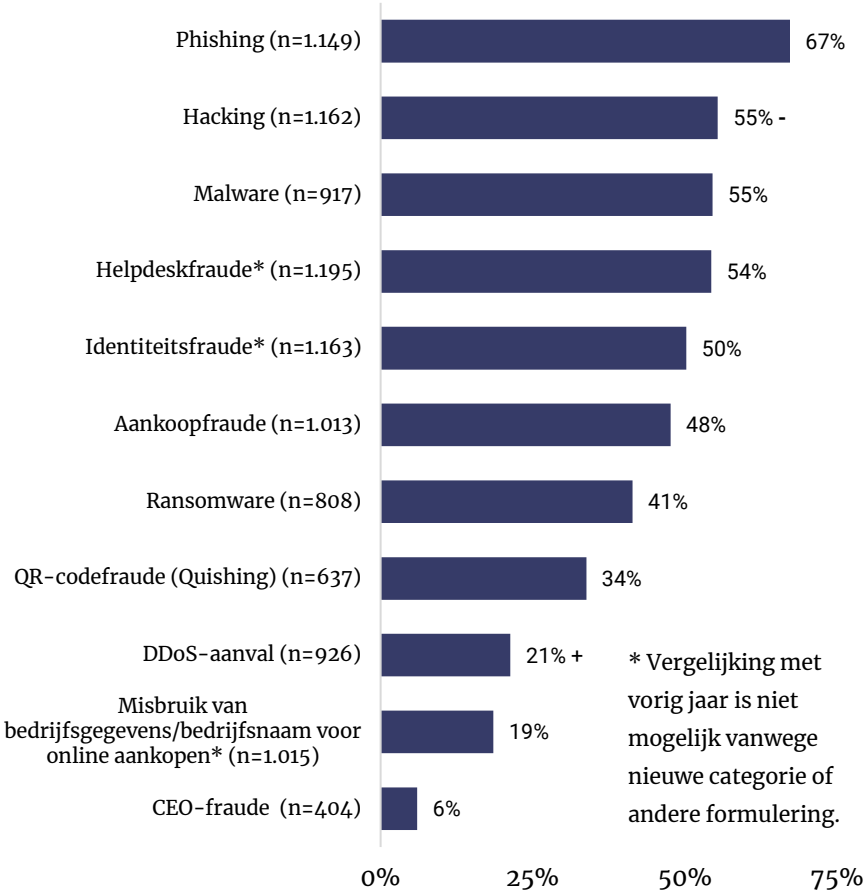
**Vergelijking met 2024**

- In 2025 denken minder mensen die er bekend mee zijn, slachtoffer te kunnen worden van hacking (2025: 55%; 2024: 61%).
- Dit jaar achten meer mensen het waarschijnlijk een DDoS-aanval mee te maken (2025: 21%; 2024: 18%).

**Resultaten subgroepen**

- Theoretisch geschoolden achten het meemaken van zeven van de elf voorgelegde vormen van cybercrime waarschijnlijker dan anderen.
- Vrouwen achten het van zes van de elf vormen waarschijnlijker dat ze ermee te maken krijgen dan mannen. Mannen denken naar verhouding vaker geen cybercrime mee te zullen maken.
- Vijfenzestigplussers achten de kans op het meemaken van malware, QR-codefraude en misbruik van bedrijfsgegevens kleiner dan anderen.

**Denkt u dat u in uw privésituatie te maken kunt krijgen met onderstaande vormen van cybercriminaliteit?**
(% genoemd; men kreeg begrippen voorgelegd waarvan men zei te weten wat het inhoudt*)



# Ruime meerderheid lijkt meemaken identiteitsfraude heel erg

- Van alle voorvallen die men in de privésituatie waarschijnlijk acht om mee te maken, lijkt een meerderheid het erg om ermee te maken te krijgen (63% tot 88% per vorm van cybercrime).
- Dat geldt het meest voor identiteitsfraude: zeven op de tien Nederlanders (70%) lijkt het heel erg om dit mee te maken en een vijfde (18%) lijkt het erg.
- Relatief gezien vinden minder mensen het erg om met een DDoS-aanval te maken te krijgen: 30 procent lijkt dit heel erg en 35 procent erg.

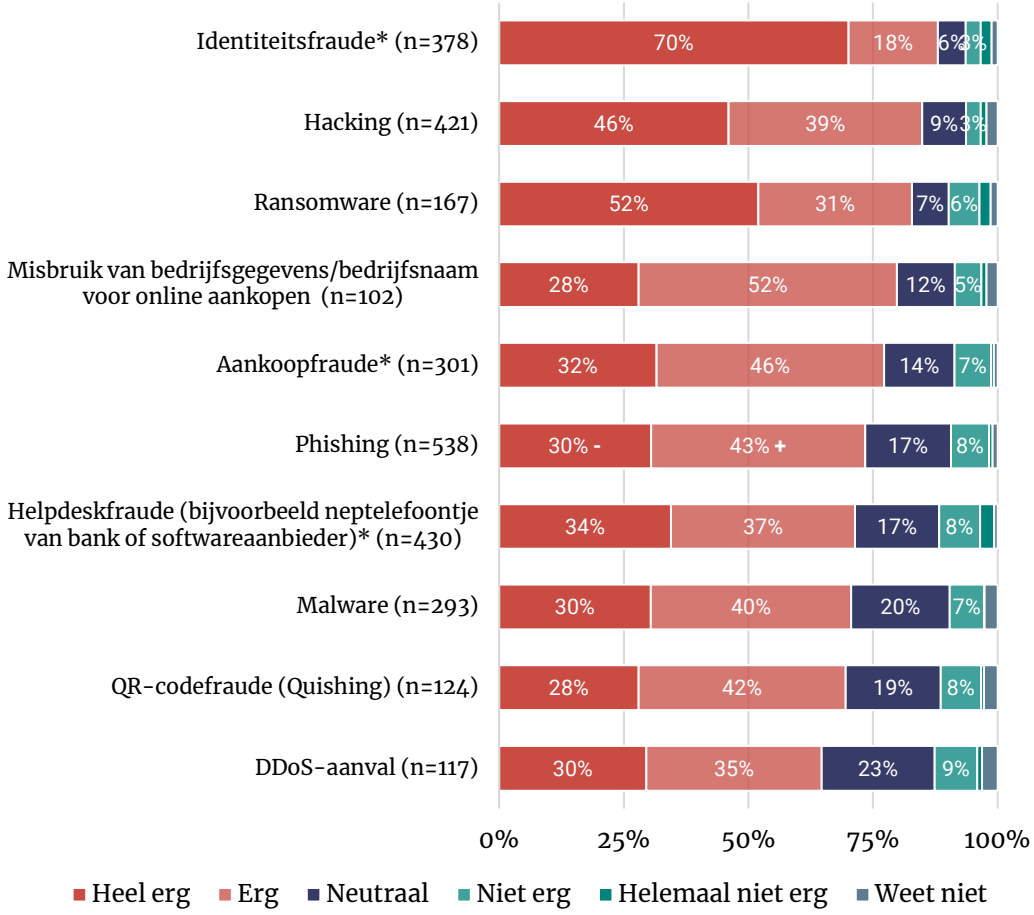
**Vergelijking met 2024**

- De gevolgen van phishing worden nu relatief minder ernstig ingeschat dan in 2024. Nu lijkt 30 procent het heel erg en 43 procent erg om dit mee te maken. In 2024 was dit respectievelijk 38 procent en 37 procent.

**Resultaten subgroepen**

- Vrouwen geven vaker dan mannen aan dat het ze erg lijkt om te maken te krijgen met malware, phishing, helpdeskfraude en een DDoS-aanval.
- Theoretisch geschoolden lijken het minder erg om met helpdeskfraude te maken te krijgen dan anderen.

**Hoe erg lijkt het u om hiermee te maken te krijgen?**
(% genoemd; men kreeg begrippen voorgelegd waarvan men zei dat ze het waarschijnlijk achten het mee te maken)




* Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

# Twee op de vijf zien overheid als betrouwbare bron voor informatie digitale veiligheid

- We vroegen Nederlanders welke twee partijen ze het meeste vertrouwen als het gaat om informatie over digitale veiligheid.
- De overheid wordt door twee op vijf Nederlanders (40%) genoemd en staat bij 21 procent op de eerste plaats.
- Ook in de politie heeft men veel vertrouwen: 14 procent zet de politie op plek 1 en nog eens 20 procent op plek 2.
- Telefoonaanbieders, scholen en bibliotheken kiest men niet vaak op plek 1 of plek 2.

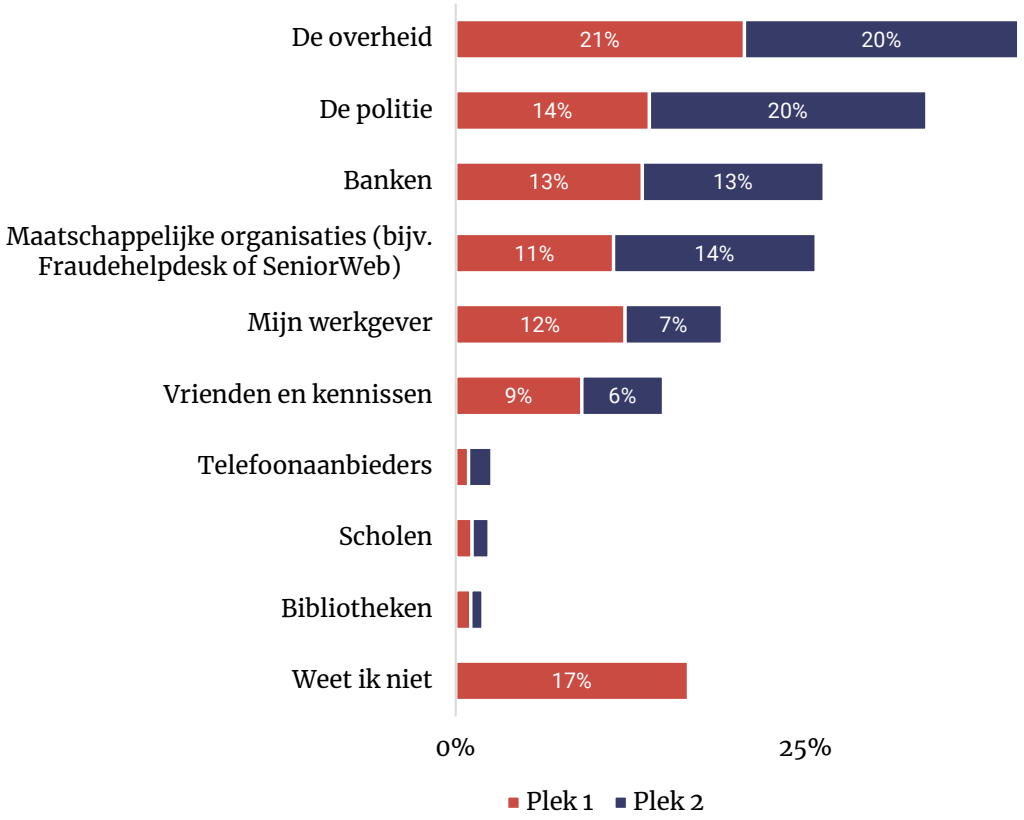
**Vergelijking met 2024**

- Deze vraag is in 2025 voor het eerst voorgelegd. Vergelijking met 2024 is daarom niet mogelijk.

**Resultaten subgroepen**

- Vijfenzestigplussers zetten vrienden en kennissen relatief vaker op de eerste plaats.
- Theoretisch geschoolden zetten vrienden en kennissen juist minder vaak bovenaan. Ten opzichte van anderen hebben theoretisch geschoolden vaker veel vertrouwen in de overheid.

**Welke van de volgende organisaties of partijen vertrouwt u het meest als het gaat om informatie over digitale veiligheid?**
(maximaal 2 antwoorden; n=1.230)



# Minder vertrouwen in telefoonaanbieders en eigen netwerk

- We vroegen Nederlanders ook welke partijen ze het minst vertrouwen als het gaat om informatie over digitale veiligheid.
- Telefoonaanbieders worden door meer dan de helft genoemd. Twee op de vijf Nederlanders (43%) zetten deze op de eerste plaats.
- Ook in vrienden en kennissen heeft men niet altijd vertrouwen. Zestien procent noemt hen als de partij die ze het minst vertrouwen en 18 procent zet hen op plek 2.

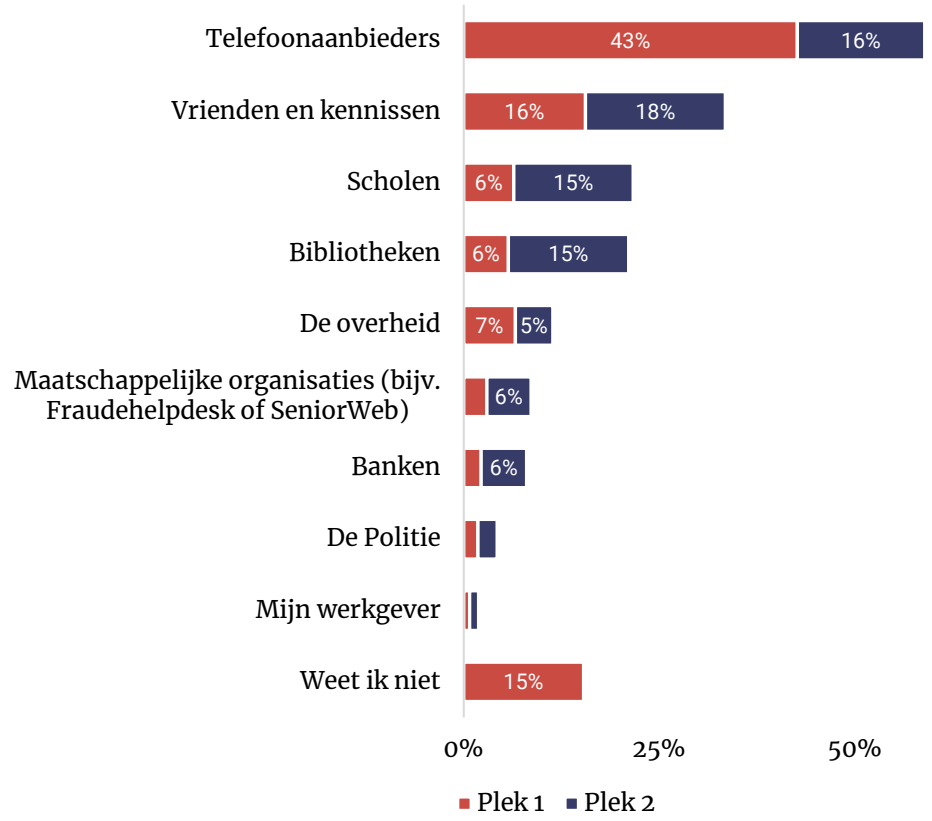
**Vergelijking met 2024**

- Deze vraag is in 2025 voor het eerst voorgelegd. Vergelijking met 2024 is daarom niet mogelijk.

**Resultaten subgroepen**

- Vijfenzestigplussers noemen telefoonaanbieders vaker dan jongeren als partij waar ze het minste vertrouwen in hebben.
- Nederlanders onder de 65 jaar noemen vaker dan 65-plussers dat ze weinig vertrouwen hebben in vrienden en kennissen.

**En welke van de volgende organisaties of partijen vertrouwt u het minst als het gaat om informatie over digitale veiligheid?** (men kreeg deze vraag niet voorgelegd als men bij de vorige vraag antwoordde met 'weet ik niet'; maximaal 2 antwoorden; n=1.034)



# Kennis generatieve AI wisselend ingeschat

- Drie op de tien Nederlanders (30%) zeggen goed tot zeer goed bekend te zijn met generatieve AI. Een kwart vindt de eigen kennis slecht (16%) of zeer slecht (12%). Ook een kwart (28%) plaatst zichzelf in het midden.

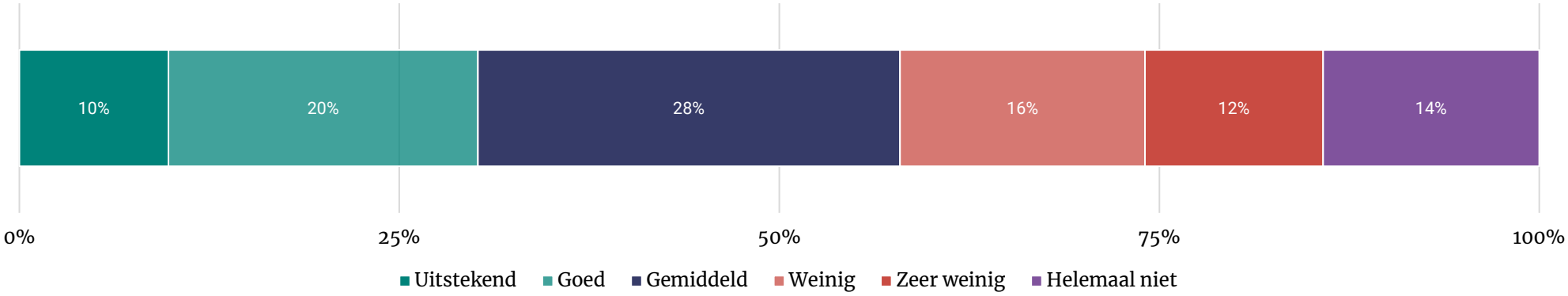
**Vergelijking met eerdere jaren**

- Deze vraag is in 2025 voor het eerst voorgelegd. Vergelijking met 2024 is daarom niet mogelijk.

**Resultaten subgroepen**

- Nederlanders onder de 40 geven vaker dan anderen aan uitstekend of goed op de hoogte te zijn van AI-toepassingen. Hetzelfde geldt voor theoretisch geschoolden.
- Praktisch geschoolden en 65-plussers geven vaker dan gemiddeld aan zeer weinig of helemaal geen kennis van AI te hebben.

**In hoeverre bent u bekend met toepassingen van generatieve AI, zoals ChatGPT of beeld- en tekstgenererende AI-modellen?** (n=1.230)



# 4. Zorgen om digitale veiligheid

# Zorgen om digitale veiligheid privé afgenomen na stijging in 2024

- De meeste Nederlanders hebben niet veel zorgen over hun digitale veiligheid (privé en werk). Acht procent zegt zich (zeer) veel zorgen hierover te maken in de privésituatie.
- Voor de werksituatie is dat 3 procent.
- De helft (51%) heeft weinig tot geen zorgen over de digitale veiligheid privé en op het werk is dat driekwart (75%).

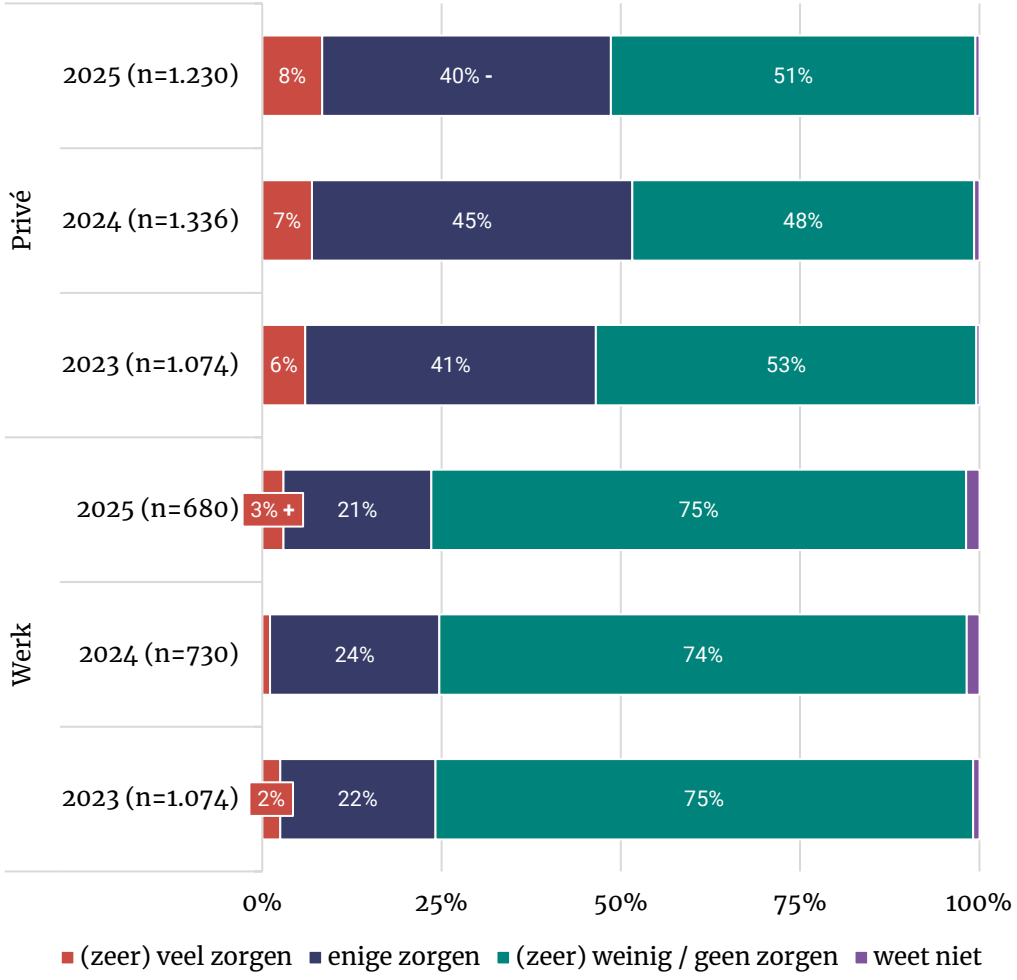
**Vergelijking met 2024**

- De zorgen zijn iets afgenomen ten opzichte van 2024. Nu geven Nederlanders minder vaak aan zich enige zorgen te maken over de eigen digitale veiligheid in de privésituatie. Na een stijging in 2024 is het beeld nu vergelijkbaar met 2023.

**Resultaten subgroepen**

- Privé maken Nederlanders onder de 40 jaar zich minder zorgen dan andere leeftijdsgroepen.
- Vrouwen maken zich vaker dan mannen ‘enige zorgen’ over de digitale veiligheid in de privésituatie. Mannen hebben vaker geen of weinig zorgen.
- Op het werk zijn er geen verschillen tussen subgroepen.

**In hoeverre maakt u zich zorgen over uw digitale veiligheid in uw privésituatie/werksituatie?**



# Zorgen over digitale veiligheid naasten nemen af

- Twee op de vijf (40%) hebben enige zorgen en 15 procent maakt zich (zeer) veel zorgen.
- Twee op de vijf (42%) maken zich (vrijwel) geen zorgen over de digitale veiligheid van naasten.

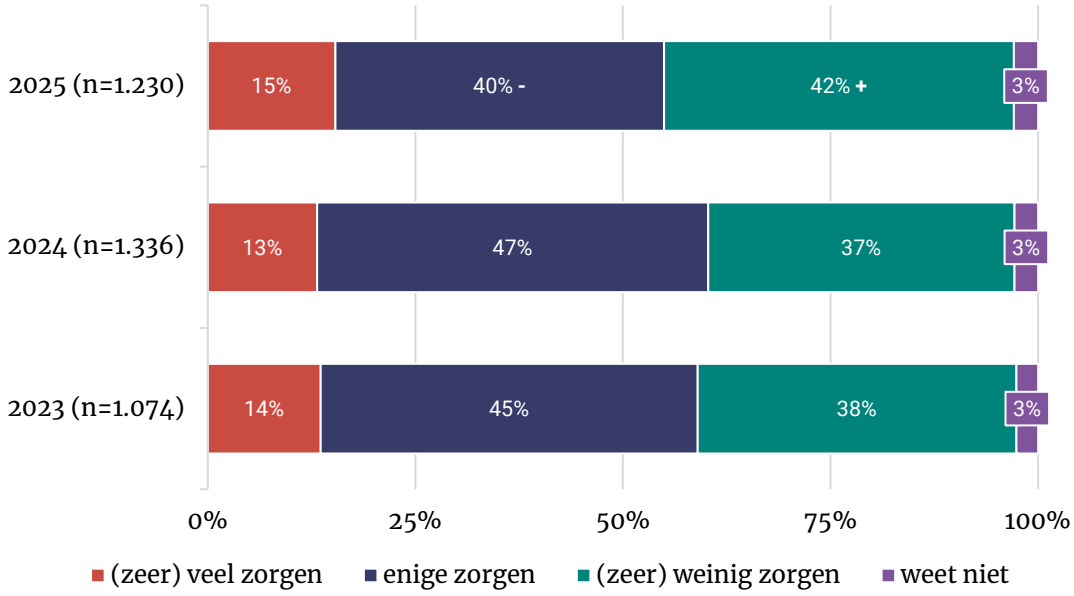
**Vergelijking met 2024**

- Men maakt zich minder zorgen dan in 2024. Destijds maakte 37 procent zich vrijwel geen zorgen (nu 42%). Het aandeel dat zich enige zorgen maakte was in 2024 (47%) groter dan in 2025 (40%).

**Resultaten subgroepen**

- Nederlanders tussen de 40 en 64 jaar maken zich vaker dan anderen zorgen over de digitale veiligheid van naasten.

**In hoeverre maakt u zich zorgen over de digitale veiligheid van uw naasten?**



# Drie op tien hebben veel zorgen over digitale veiligheid van Nederland

- Acht procent van de Nederlanders maakt zich zeer veel zorgen over de digitale veiligheid van Nederland. Daarnaast maakt een kwart (23%) zich veel zorgen hierover. In totaal maken drie op de tien Nederlanders (31%) zich dus (zeer) veel zorgen.
- Dit is een grotere groep dan de Nederlanders die zich (zeer) weinig zorgen maken. Dit is in totaal een vijfde (20%): 14 procent maakt zich weinig zorgen, 3 procent zeer weinig zorgen en 3 procent geen zorgen.
- Ongeveer de helft van de Nederlanders plaatst zich in het midden en maakt zich enige zorgen (46%).

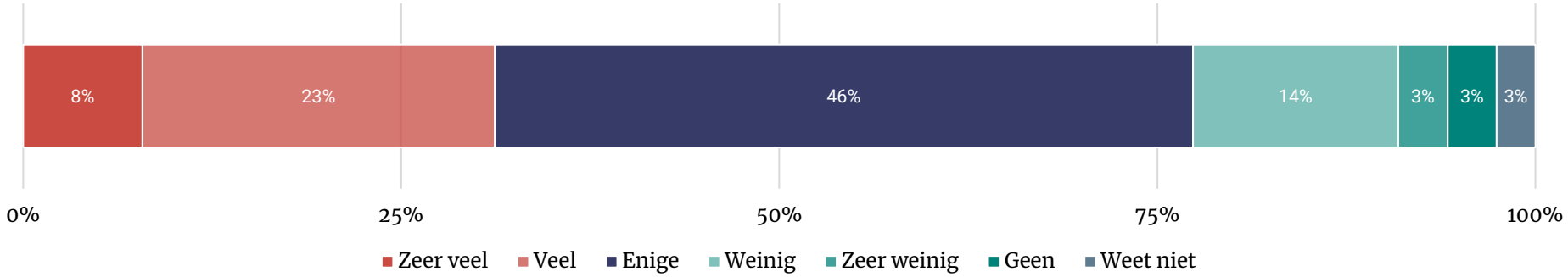
**Vergelijking met eerdere jaren**

- Deze vraag is in 2025 voor het eerst voorgelegd. Vergelijking met 2024 is daarom niet mogelijk.

**Resultaten subgroepen**

- Nederlanders onder de 40 jaar maken zich vaker (zeer) weinig zorgen (30%; totaal: 20%). Nederlanders van 65 jaar of ouder maken zich vaker (zeer) veel zorgen (42%; totaal: 31%).

**In hoeverre maakt u zich zorgen over de digitale veiligheid van Nederland?** (n=1.230)



# Meeste zorgen in privésituatie: verlies van controle over gegevens en geld

- Zeven op de tien Nederlanders die zich zorgen maken over de eigen digitale veiligheid, zijn bang dat hun gegevens in verkeerde handen vallen (70%).
- Twee derde (64%) maakt zich (ook) zorgen over het verlies van controle over eigen gegevens.
- Zes op de tien (59%) zijn bang om geld kwijt te raken.

**Vergelijking met 2024**

- Vaker dan in 2024 zijn Nederlanders bezorgd dat anderen zich online als hen voordoen (2025: 42%; 2024: 36%).

**Resultaten subgroepen**

- Vijfenzestigplussers en vrouwen noemen vaker dan anderen zich zorgen te maken omdat ze onvoldoende verstand hebben van digitale veiligheid.

**Waarover maakt u zich zorgen als het gaat om uw digitale veiligheid in uw privésituatie?** (% genoemd; gesteld aan Nederlanders die zich zorgen maken over digitale veiligheid in de privésituatie; n=633)

# Updates en twee-staps-inloggen zorgen voor veilig gevoel

- De helft (48%) van de Nederlanders die zich weinig tot geen zorgen maken over de eigen digitale veiligheid in de privésituatie, noemt het updaten van apparaten als reden om zich weinig zorgen te maken.
- Andere veelgenoemde redenen zijn het controleren op valse links en websites (47%) en het gebruik van twee-staps-inloggen (46%).

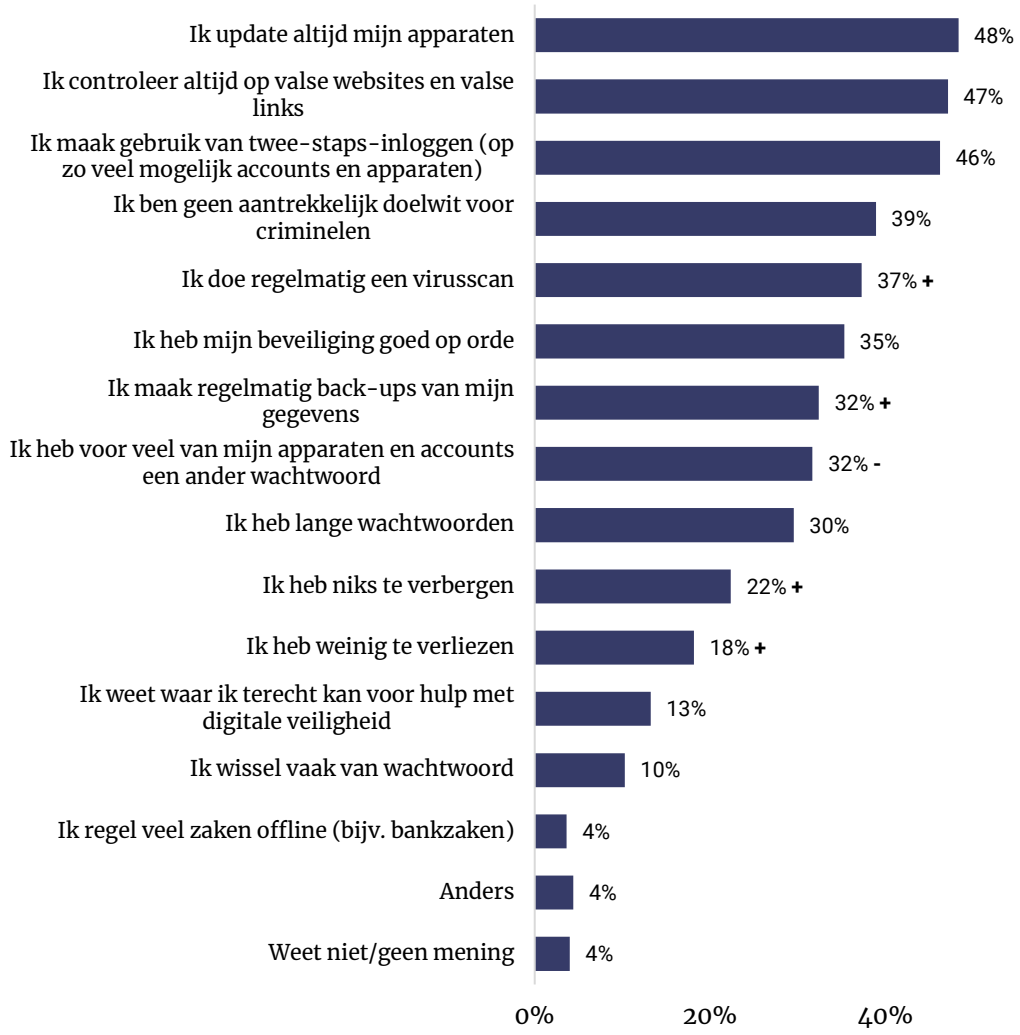
**Vergelijking met 2024**

- Men noemt vaker dan in 2024 zich weinig zorgen te maken door het doen van virusscans, het maken van back-ups en dat men weinig te verbergen of te verliezen heeft.
- Minder vaak noemt men dat men voor veel apparaten en accounts een ander wachtwoord heeft als reden om zich weinig zorgen te maken.

**Resultaten subgroepen**

- Mannen en theoretisch geschoolden noemen verschillende veiligheidsmaatregelen zoals back-ups en twee-staps-inloggen vaker.
- Nederlanders onder 40 jaar noemen vaker dat ze weinig te verliezen hebben en gebruikmaken van twee-staps-inloggen.

**Waarom maakt u zich (zeer) weinig zorgen als het gaat om uw digitale veiligheid in uw privésituatie?** (% genoemd; gesteld aan Nederlanders die zich weinig tot geen zorgen maken over digitale veiligheid in de privésituatie; n=591)



# Toelichtingen bij zorgen over digitale veiligheid

**Veel zorgen**

- *Criminelen worden steeds slimmer en niet hard genoeg aangepakt.*
- *De DDoS-aanvallen lijken meer en ernstiger voor te komen. Angst voor het kunnen stilleggen van belangrijke zaken, bedrijven, nationale veiligheid, etc.*
- *Moeilijk om te bepalen wat betrouwbaar is en wat niet. Lastig om inzicht te krijgen hoe er met persoonlijke gegevens wordt omgegaan door verschillende websites.*
- *Ik ben negentig jaar en afhankelijk van de kennis van mijn kinderen.*
- *Bij een gerichte (geavanceerde) aanval is veiligheid haast niet te waarborgen.*
- *Veel zorgen, zeker nu AI over gaat nemen waardoor echte berichten niet meer van cyberfraude berichten te onderscheiden zal zijn.*
- *Ik denk dat ik mijn eigen digitale veiligheid wel op orde heb. Maar maak me wel zorgen over de Nederlandse digitale veiligheid, omdat we voor veel landen een mikpunt kunnen zijn.*

**Weinig zorgen**

- *Ik heb niet het idee dat ik aan de digitale veiligheid van Nederland iets kan veranderen. Daarnaast kan het me voor mijn persoonlijke digitale veiligheid niet zo heel veel schelen en voor naasten zou ik het wel vervelend vinden als er iets gebeurt vooral bij ouderen.*
- *Ik denk dat we het in Nederland goed beveiligd hebben. Voor mijzelf geldt dat ook.*
- *Maak me er niet heel erg zorgen over omdat met gezond verstand er bijna niets mis kan gaan. Belangrijkste is dat mensen weten dat het bestaat en hoe het gebeurt.*
- *Ik ga ervan uit dat knappe koppen dat goed in de gaten houden. Ik pas op mijn eigen computer.*
- *Ik kan er toch niets aan veranderen.*
- *Als het moet gebeuren, dan is dat maar zo. Ik maak me er niet echt druk om.*

# 5. Online gedrag

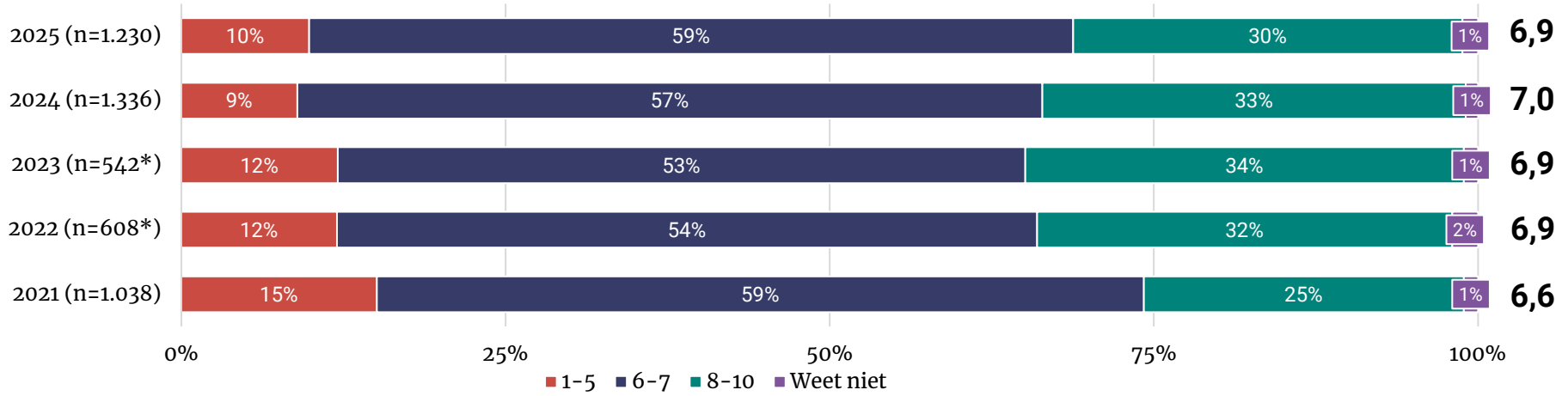
# Nederlanders geven zich een ruime voldoende voor omgang online risico's

Zes op de tien Nederlanders (59%) geven zichzelf een 6 of een 7 voor de omgang met online risico's. Drie op de tien (30%) geven zichzelf een 8 of hoger. Tien procent geeft zichzelf een onvoldoende. Het gemiddelde oordeel is een 6,9.

**Vergelijking met eerdere jaren**
In vergelijking met 2024 is het beeld stabiel. Op de langere termijn valt op dat men zichzelf in eerdere jaren vaker onvoldoendes gaf. In 2021 waren er ook minder beoordelingen van 8 of hoger en viel het gemiddelde met een 6,6 duidelijk lager uit dan in de jaren daarna.

**Resultaten subgroepen**
Mannen en Nederlanders onder de 40 jaar geven zichzelf gemiddeld een 7,1 voor de eigen omgang met online risico's. Vrouwen geven zichzelf een 6,7.

**Welk cijfer geeft u uzelf als het gaat om het veilig omgaan met online risico's?**




*De helft van de steekproef kreeg de vraag in 2023 en 2022 net als in 2021, 2024 en 2025 te zien nadat men vragen had gekregen over de verschillende maatregelen die men kan nemen om veilig om te gaan met online risico's. De andere helft kreeg deze vraag, voordat ze deze informatie hadden. Wanneer men meer informatie heeft over de maatregelen die men kan nemen, lijkt men gemiddeld een iets lager cijfer te geven, het verschil is echter net niet significant. In de figuur zijn voor de jaren 2023 en 2022 alleen de uitkomsten weergegeven voor de vraag op de dezelfde plek als de overige jaren.

# Toelichtingen bij cijfer omgang online risico's

**Cijfer 1-5 (10%)**

- *Ik ben niet zo zeer op de hoogte van dit soort zaken. Ik vraag het vaak aan mijn kinderen van 30 jaar. Veel meer op de hoogte van dit alles. Zijn er mee opgegroeid. Ik van 1964 niet zo.*
- *Ik voel me op digitaal gebied kwetsbaar.*
- *ik ben niet handig met de computer en weet dat ik te vaak dezelfde wachtwoorden gebruik.*

**Cijfer 9-10 (30%)**

- *Ik ben in grote mate bekend met de vormen van digitale criminaliteit, ben goed geïnformeerd en maak gebruik van een wachtwoordmanager, veilige wachtwoorden en 2FA.*
- *Let goed op, ben geen impulsief mens, die gewoon maar klikt als het gevraagd wordt.*
- *Ik ben aardig op de hoogte van de meest actuele oplichtingstrucs en kan ook vrij goed onderscheiden wat betrouwbaar is. Ik gebruik unieke wachtwoorden en, zeker voor kritieke diensten, twee-staps-verificatie.*
- *Ben heel erg op mijn hoede en controleer veel.*

**Cijfer 6-7 (59%)**

- *Ik neem wat meer risico's bij bezoeken sites maar heb feitelijk nooit problemen anders dan wat irritante reclames.*
- *Ik kan het een stuk beter doen, maar het gaat niet slecht.*
- *Ik gebruik wachtwoorden en virusscanner en malwarebytes. Dit beschermt deels, maar lang niet tegen alle mogelijke vormen van fraude.*
- *Het is niet allemaal optimaal, maar met de hulp van mijn zoon lukt het wel.*
- *Ik vertrouw erop dat mijn laptop en telefoon voldoende beveiligd zijn door de medewerker van Senior Service. (een gepensioneerd ICT'er)*
- *Ik heb veel verschillende wachtwoorden, heb weinig vertrouwen in het algemeen op internet, accepteer weinig cookies, en deel mijn gegevens niet.*
- *Als ik iets niet vertrouw, zoek ik het eerst op.*

# Veel veiligheidsmaatregelen door meerderheid toegepast (1)

- Van een lijst met voorgelegde veiligheidsmaatregelen en gedragingen, worden de meeste door de meerderheid toegepast.
- Veel Nederlanders controleren de links waarop ze klikken (95%), downloaden apps via officiële kanalen (94%), voeren automatische updates uit (93%), gebruiken twee-staps-inloggen (92%) en lange wachtwoorden (92%).

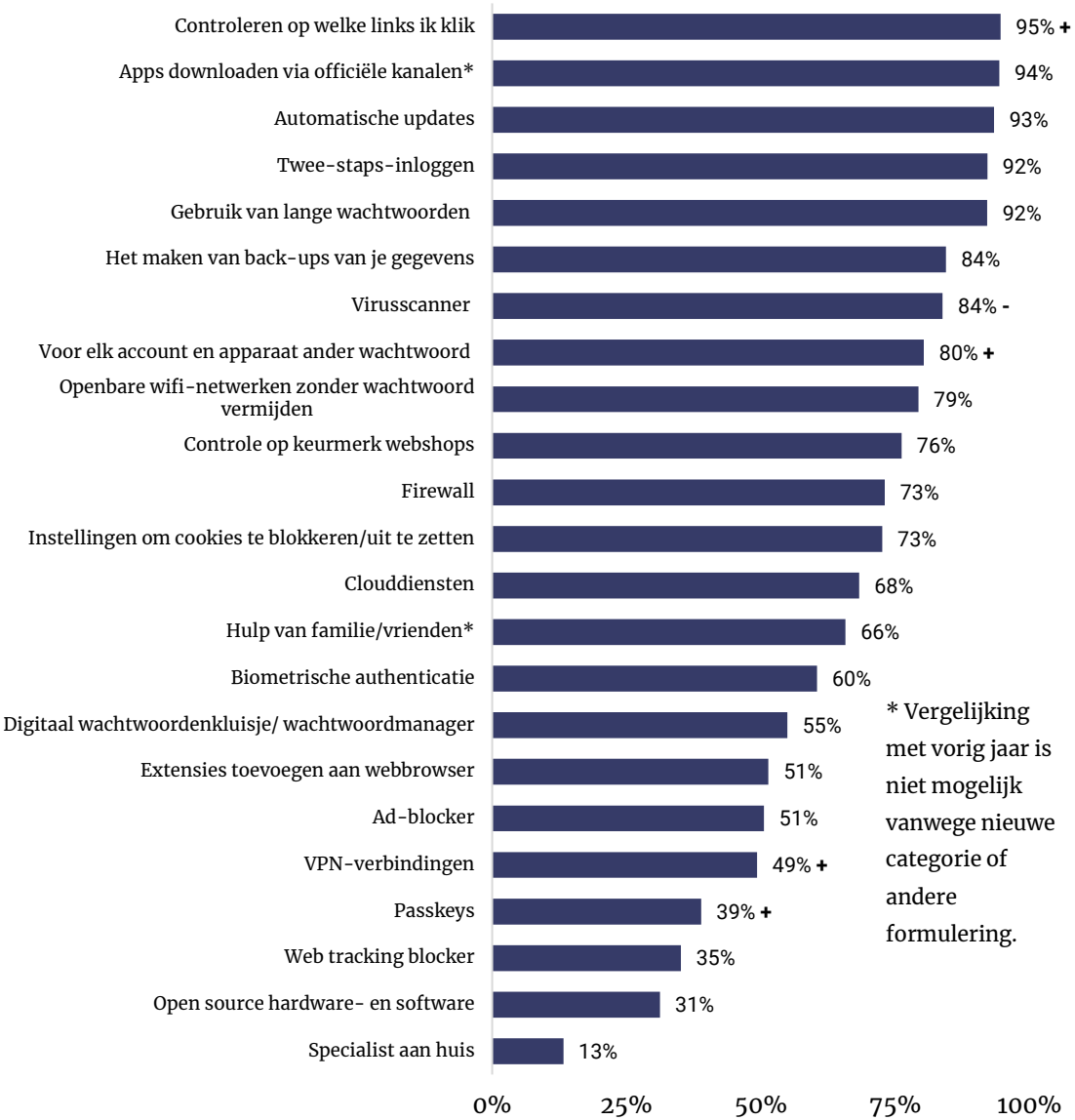
**Vergelijking met 2024**

- Het controleren van links, het hebben van verschillende wachtwoorden, VPN-verbindingen en passkeys zijn maatregelen die nu meer worden toegepast dan in 2024.
- Het gebruik van virusscanners daalde van 88 procent naar 84 procent.

**Resultaten subgroepen**

- Mannen gebruiken veel maatregelen meer dan vrouwen.
- Nederlanders onder de 40 jaar gebruiken minder vaak virusscanners en firewalls. Ze gebruiken vaker adblockers en browserextensies.
- Vijfenzestigplussers en vrouwen schakelen vaker hulp in van familie/vrienden.
- Praktisch geschoolden geven van verschillende maatregelen vaker aan er niet mee bekend te zijn.

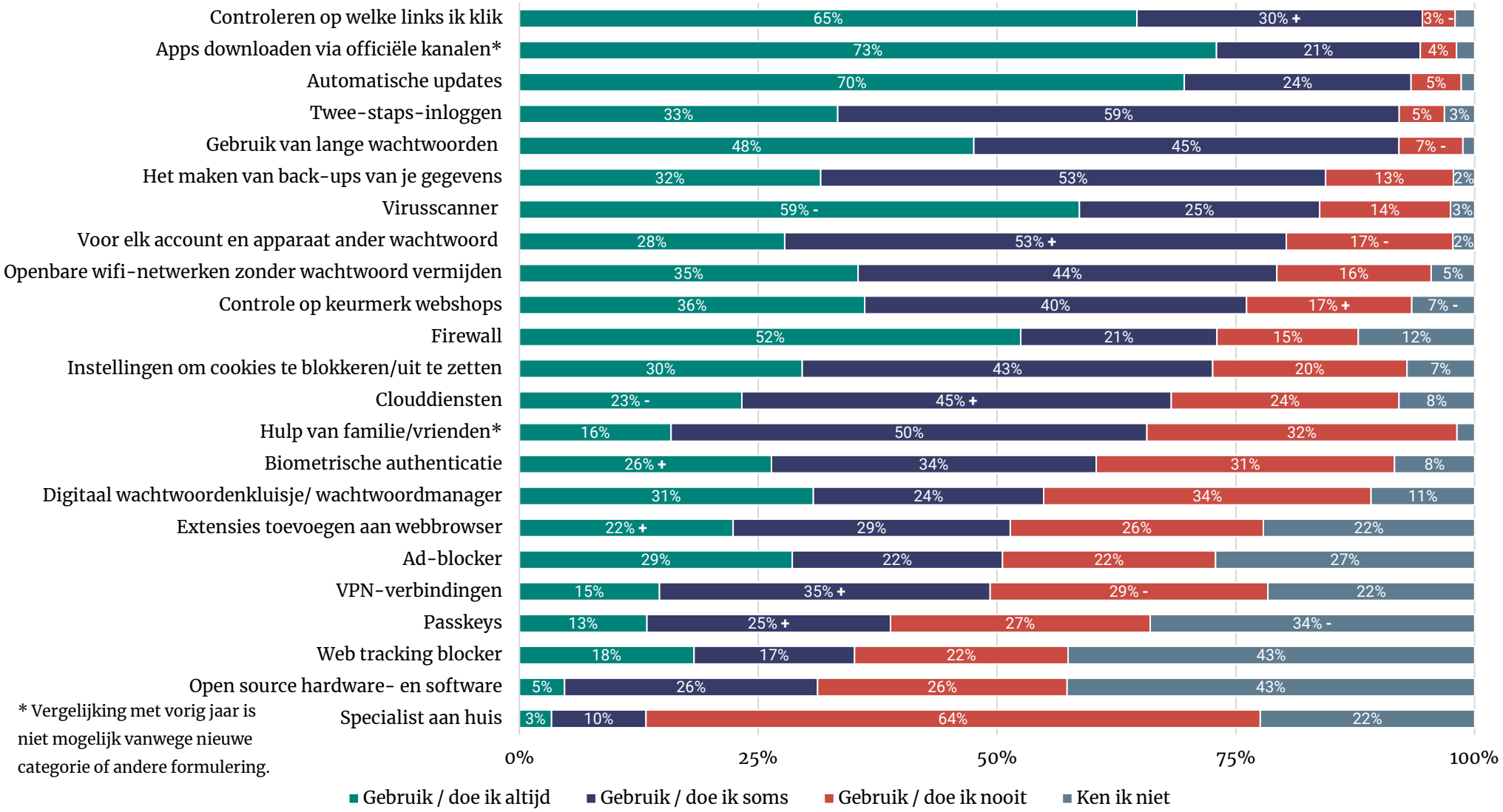
**Welke van onderstaande zaken gebruikt u of past u toe?**
(% doe ik altijd/soms; men kreeg willekeurig de helft van de opties; n=624)




* Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

# Veel veiligheidsmaatregelen door meerderheid toegepast (2)

**Welke van onderstaande zaken gebruikt u of past u toe?**
(men kreeg willekeurig de helft van de opties; n=624)




* Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

# Twee derde Nederlanders checkt mobiele apps op veiligheid en betrouwbaarheid

- Twee derde van de Nederlanders (69%) controleert meestal of altijd mobiele apps op veiligheid en betrouwbaarheid voordat ze deze installeren.
- Eenzelfde aandeel (66%) zorgt dat hun slimme apparaten de laatste updates gebruiken.
- Bij meeste werkenden (66%) maakt de werkgever meestal of altijd back-ups. Thuis doet 46 procent dit.

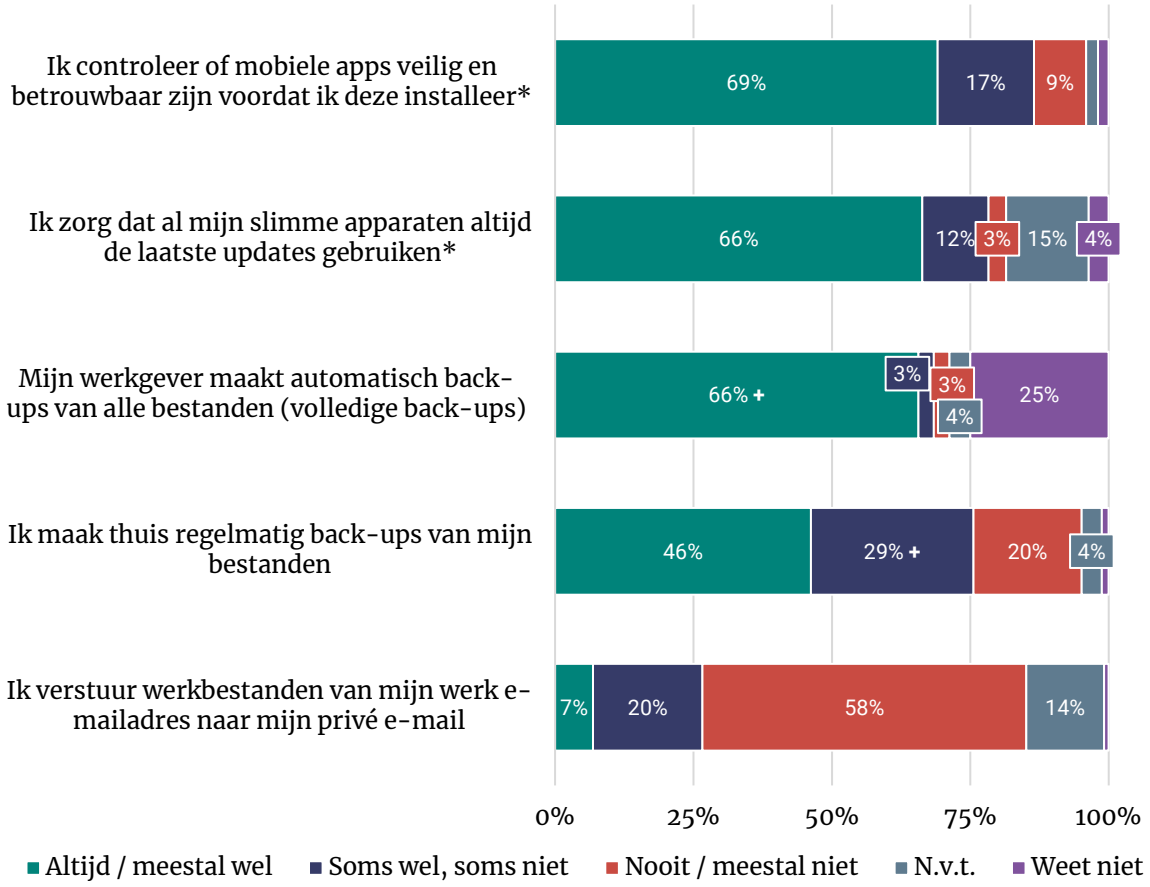
**Vergelijking met 2024**

- In vergelijking met de vorige meting, maken meer werkgevers altijd of meestal back-ups (2025: 66%; 2024: 60%).
- In 2024 maakte een kwart (25%) thuis geen back-ups, nu is dat 20%.

**Resultaten subgroepen**

- Mannen geven vaker dan vrouwen aan thuis back-ups te maken en apps op veiligheid en betrouwbaarheid te controleren voor installatie.
- Praktisch geschoolden maken relatief minder back-ups thuis.

**In hoeverre zijn de volgende uitspraken op u van toepassing?***
(n=1.230; vragen over werk zijn alleen gesteld aan werkenden; n=680)




* Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

# Updates voor veiligheid en goed werkende apparaten

- Driekwart van de Nederlanders die hun slimme apparaten updaten, geven aan dat ze dit doen omdat ze willen dat de apparaten goed werken (73%).
- Bijna net zoveel mensen doen dit zodat apparaten veilig gebruikt kunnen worden (70%).
- Minder vaak is de reden om geen bijzondere updates te willen missen (31%) en omdat men daartoe verplicht wordt (24%).

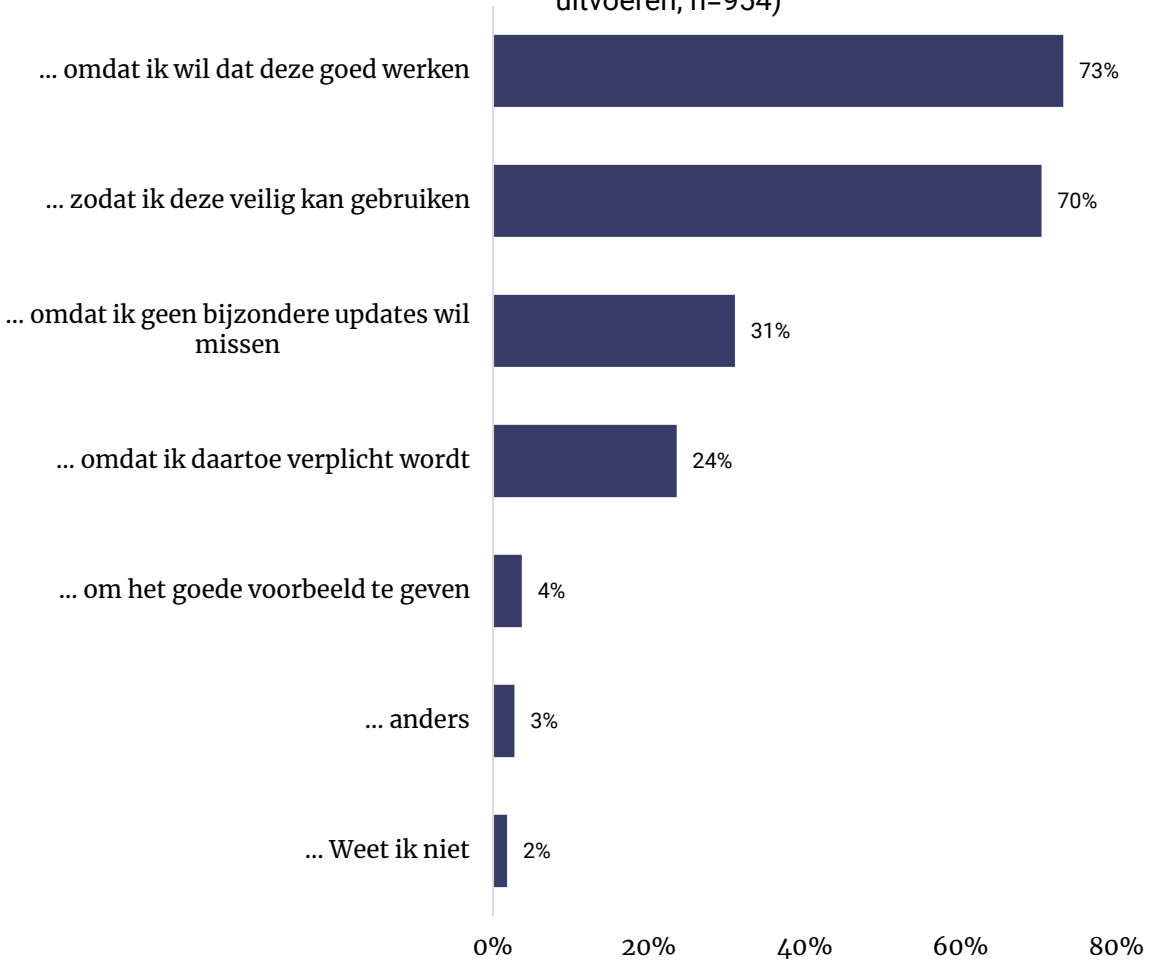
Vergelijking met 2024

- Deze vraag is in 2025 voor het eerst voorgelegd. Vergelijking met 2024 is daarom niet mogelijk.

Resultaten subgroepen

- Jongeren installeren updates vaker dan anderen omdat ze daartoe verplicht worden. Minder installeren ze de updates zodat de apparaten veilig te gebruiken zijn.
- Theoretisch geschoolden installeren vaker updates om het goede voorbeeld te geven.

**In hoeverre zijn de volgende uitspraken op u van toepassing?**
**Ik update apparaten…**
(gesteld aan mensen die updates voor hun slimme apparaten uitvoeren; n=954)



# Helft zou zich schamen als ze op een link in phishingmail zouden klikken

- Een meerderheid (55%) denkt zich te schamen als ze op een link in een phishingmail klikken.
- Wel verwachten vier op de vijf werkenden het te vertellen aan de ICT-afdeling (81%) of iemand anders (78%) op het werk als ze op het werk een virus downloaden. Vrijwel niemand zegt dit zeker niet te doen.
- Een klein deel van de werkenden (4%) verwacht het door schaamte niet te vertellen als ze een virus op het werk downloaden.

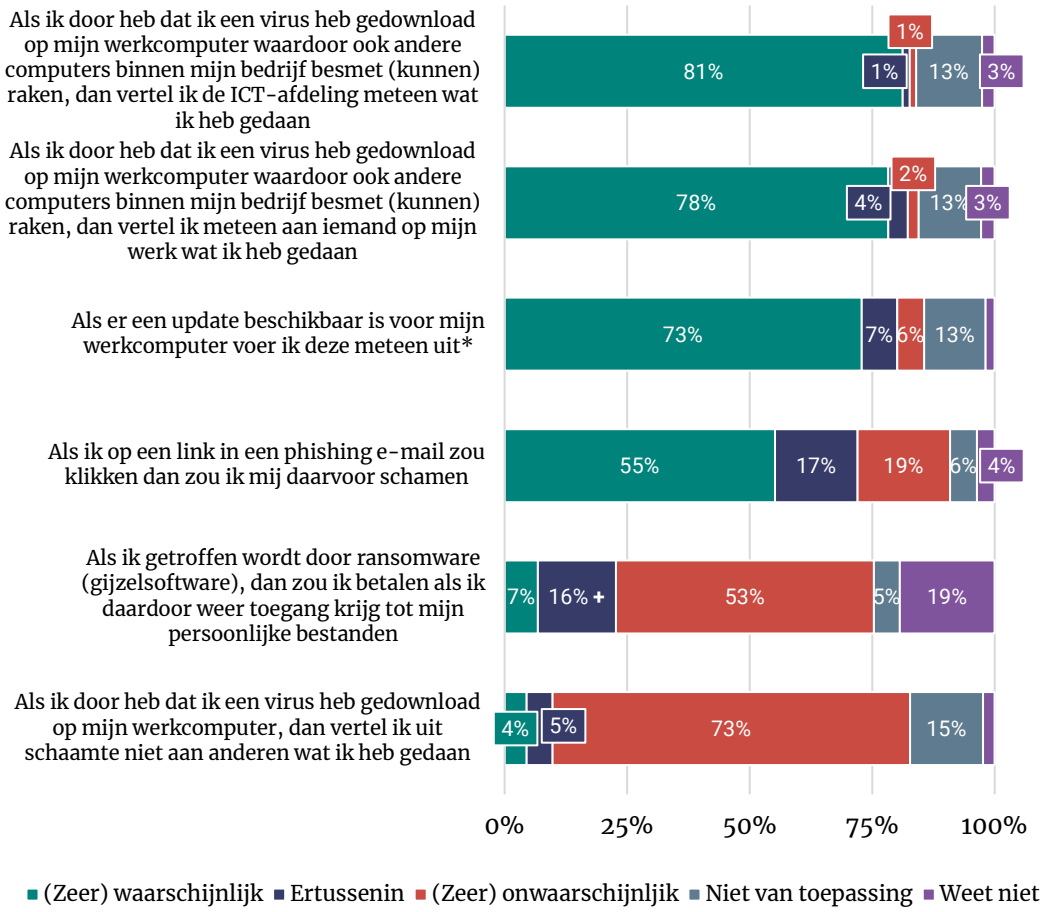
**Vergelijking met 2024**

- In 2024 zei 12 procent misschien wel, misschien niet te betalen als ze slachtoffer zouden worden van ransomware. Nu is dat toegenomen naar 16 procent.

Resultaten subgroepen

- Praktisch geschoolden verwachten minder dan anderen te zullen betalen als ze worden getroffen door ransomware.

**In hoeverre zijn de volgende uitspraken op u van toepassing?**
(n=1.230; vragen over werk zijn alleen gesteld aan werkenden; n=680)




* Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

# 6. Slachtofferschap en aangiftebereidheid

# Ervaringen met neptelefoontjes verdubbeld

- Driekwart (72%) van de Nederlanders maakte in de twaalf maanden voorafgaand aan het onderzoek één of meerdere voorvallen van cybercrime mee.
- Het meest meegemaakte voorval is net als in eerdere jaren phishing (55%), gevolgd door neptelefoontjes met als doel geld of gegevens te bemachtigen (ook wel telefonische spoofing genoemd; 29%).

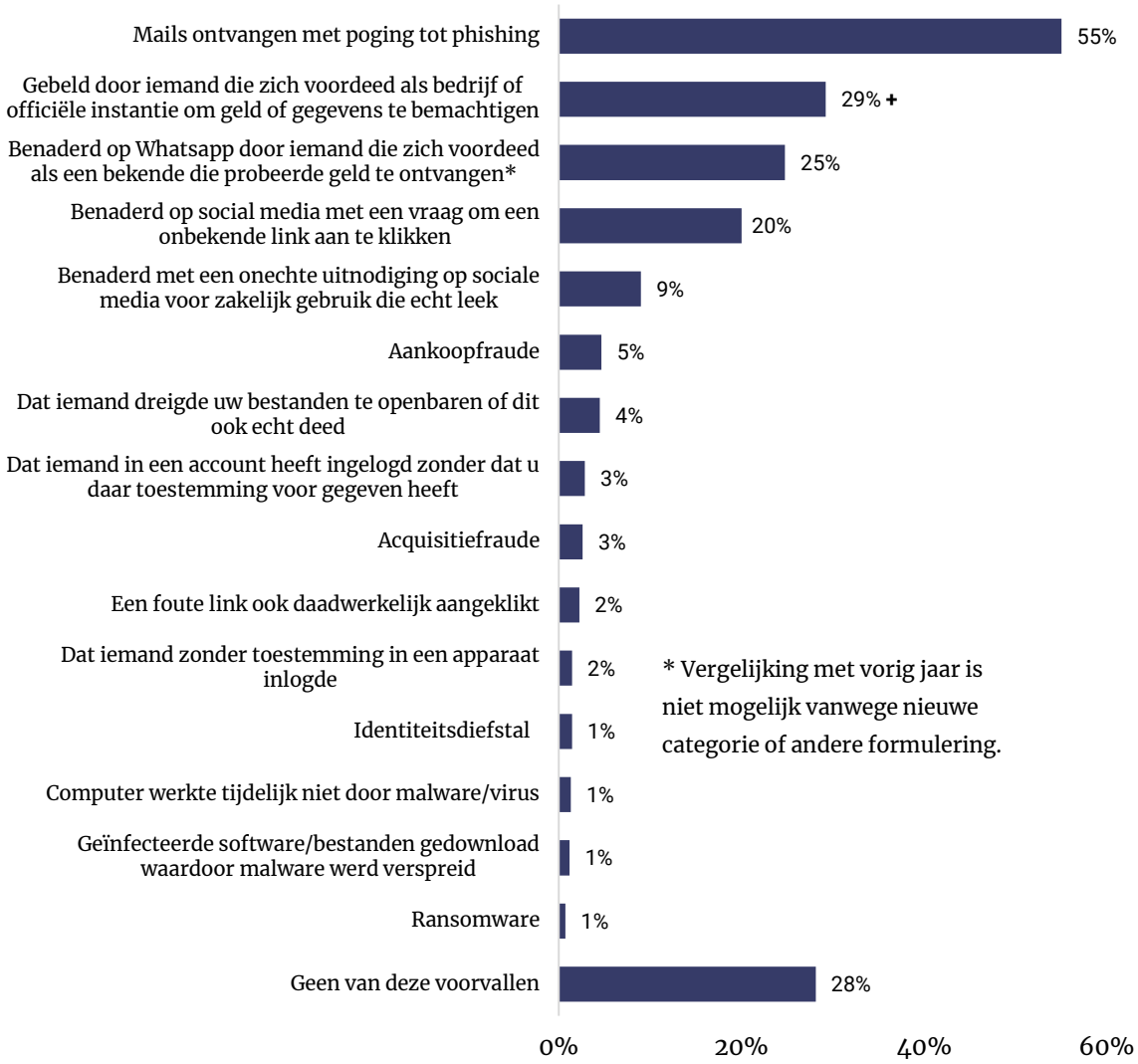
**Vergelijking met 2024**

- De ervaring met deze neptelefoontjes is duidelijk toegenomen ten opzichte van 2024. Toen maakte 15 procent dit mee in de twaalf maanden voor het onderzoek, dit jaar was dat 29 procent.

**Resultaten subgroepen**

- Mannen maakten verschillende vormen van cybercrime vaker mee dan vrouwen, o.a. het downloaden van geïnfecteerde bestanden.
- Onder theoretisch geschoolden heeft een groter deel te maken gehad met cybercrime. Vooral pogingen tot phishing maken ze vaker mee.

**Heeft u in de afgelopen twaalf maanden zelf weleens te maken gehad met één van de onderstaande voorvallen?** (% genoemd; n=1.230)



# Vaak gevolgen bij aankoopfraude, maar men ervaart dit niet altijd als ernstig

- In de meeste gevallen ervaart men geen ernstige gevolgen wanneer men te maken krijgt met cybercrime.
- Meer dan bij andere vormen van cybercrime ervaart men ernstige gevolgen bij aankoopfraude (7%), het aanklikken van een foute link (7%) en wanneer anderen zonder toestemming inloggen in accounts (6%).

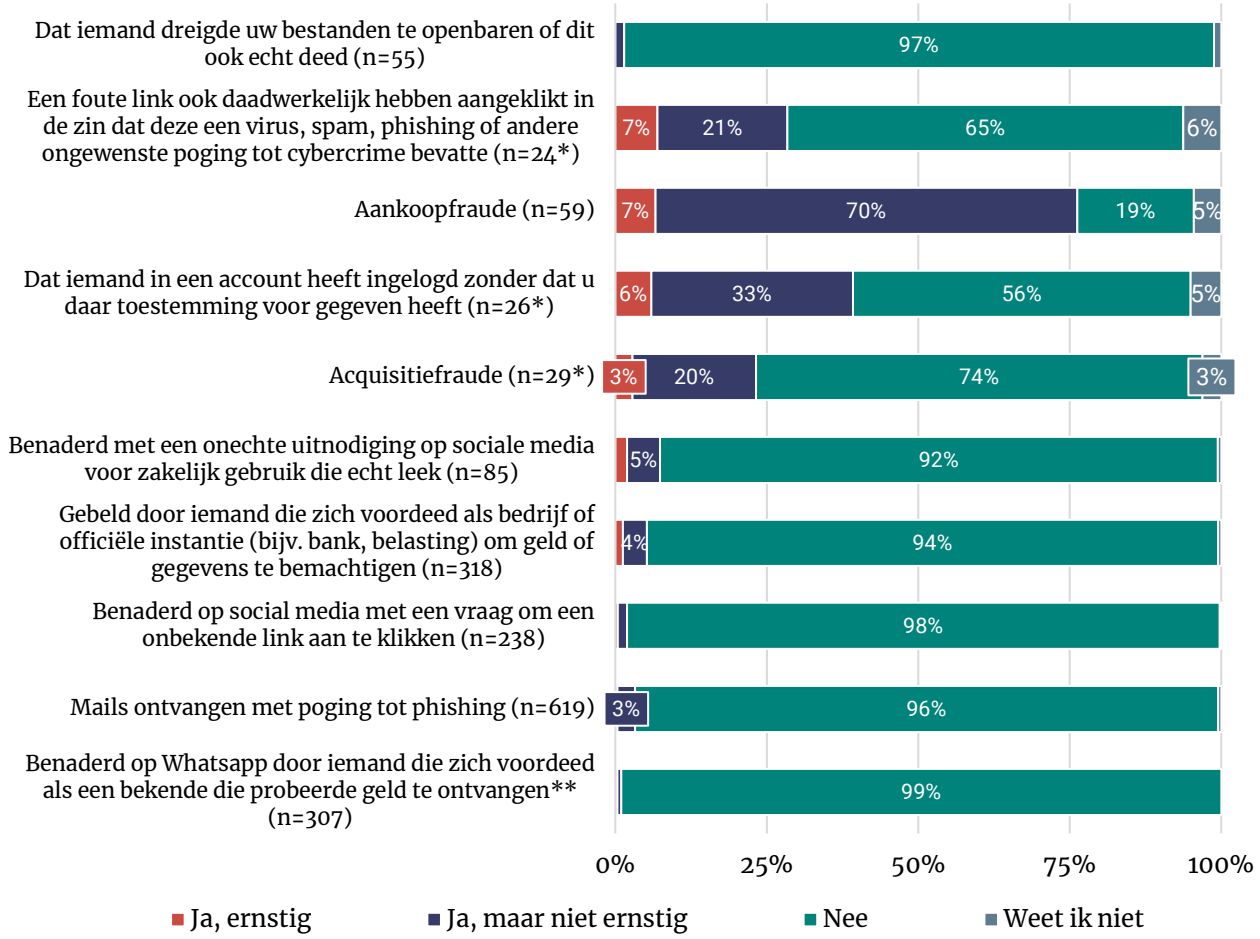
**Vergelijking met 2024**

- Er zijn geen significante verschillen met 2024.

**Resultaten subgroepen**

- Er zijn geen relevante verschillen tussen subgroepen in de gevolgen die men ervaart vanwege meegemaakte voorvallen.

**Heeft u gevolgen ondervonden van deze voorvallen in uw privésituatie?** (meegemaakte voorvallen in privésituatie)




*Laag aantal: indicatieve uitkomsten.

** Vergelijking met vorig jaar is niet mogelijk vanwege nieuwe categorie of andere formulering.

# Meeste mensen schamen zich niet na meemaken cybercrime

- Van degenen die een geval van cybercrime meemaakten, kostte het driekwart (73%) weinig moeite om te vertellen wat er was gebeurd.
- Twee derde (69%) schaamde zich hier ook niet voor.
- Veertien procent schaamde zich wel.

**Vergelijking met 2024**

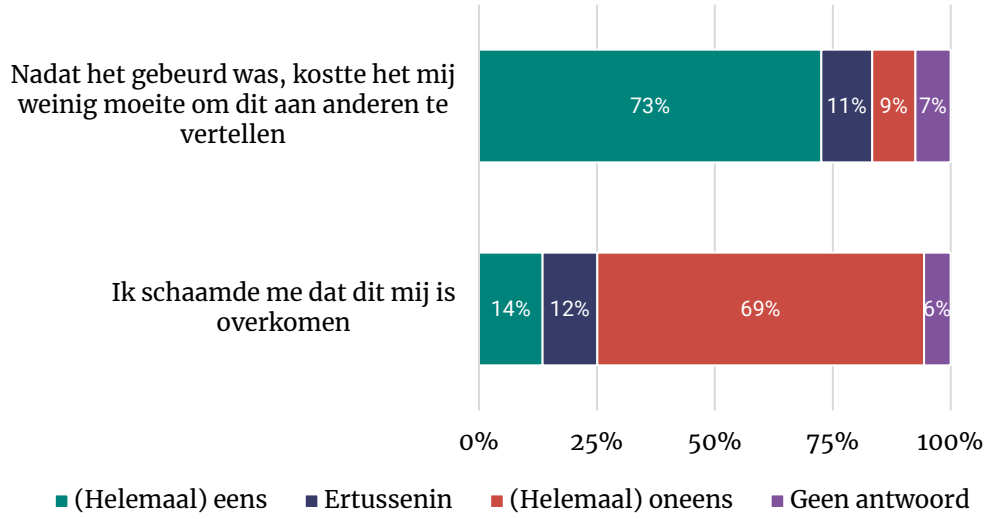
- Deze vraag is in 2025 voor het eerst voorgelegd. Vergelijking met 2024 is daarom niet mogelijk.

**Resultaten subgroepen**

- Wanneer de gevolgen van het voorval dat men meemaakte gering waren, schaamt men zich er minder voor en kost het hun ook minder moeite om het aan anderen te vertellen.

U heeft één of meer voorvallen meegemaakt van cybercrime.

**In hoeverre bent u het eens of oneens met de volgende stellingen?**
(gesteld aan iedereen die privé of op het werk een geval van cybercrime meemaakte; n=889)



# Slachtoffers doen vaker aangifte of melding van cybercrime in privésituatie

- Twee op de drie Nederlanders (67%) die een voorval van cybercrime meemaakten in de privésituatie deden hier geen aangifte of melding van.
- Wanneer men dat wel doet, is dat vooral een melding bij de Fraudehelpdesk (11%), bank (10%) of bij de instantie waar het voorval gebeurde (7%).
- Vier procent doet aangifte bij de politie en 3 procent maakt een melding bij de politie.

**Vergelijking met 2024**

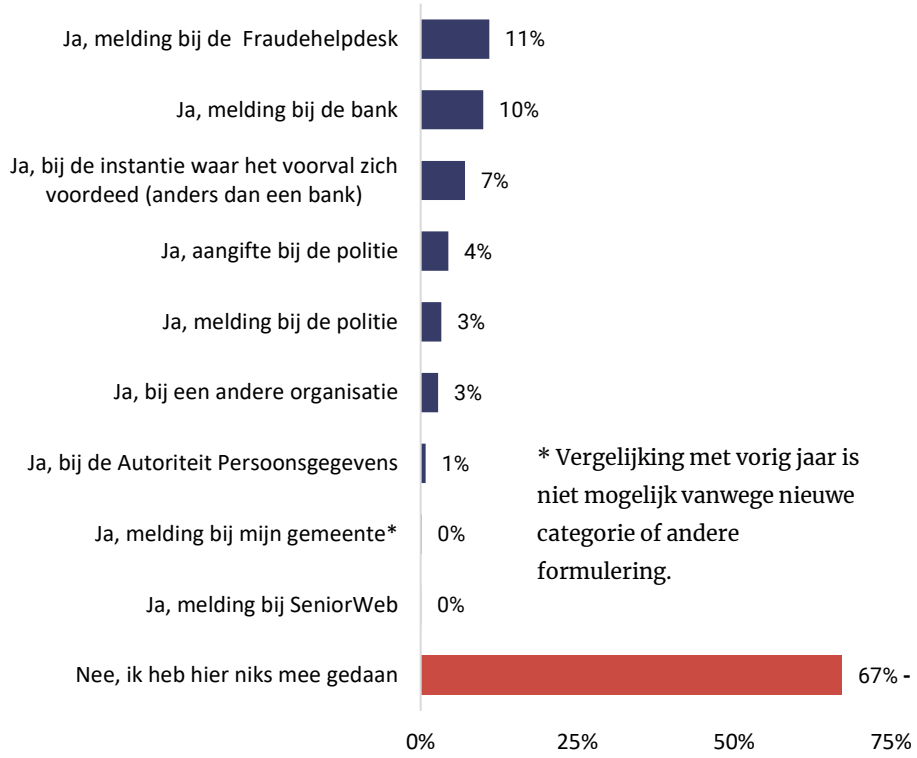
- Men doet vaker iets met het meegemaakte voorval dan in 2024, toen deed 28 procent aangifte of melding (nu 33%).

**Resultaten subgroepen**

- Wanneer men geen gevolgen ervaart van de cybercrime, is men ook minder geneigd om aangifte of melding te doen: 71 procent doet dit dan niet.
- Vijfenzestigplussers doen vaker iets met het meegemaakte voorval. Zo doen ze vaker melding bij de bank dan andere leeftijdsgroepen.
- Ook vrouwen en praktisch geschoolden doen relatief vaker melding bij de bank.
- Mannen doen vaker dan gemiddeld een melding bij de Fraudehelpdesk.

U geeft aan dat u zelf thuis of in uw privésituatie te maken heeft gehad met een of meerdere voorvallen van cybercrime.

**Heeft u toen een aangifte of melding gedaan?** (gesteld aan iedereen die privé een geval van cybercrime meemaakte; n=867)



# Weinig schade belangrijkste reden om geen aangifte of melding te doen

- De voornaamste reden om geen aangifte of melding te doen is dat men weinig schade ondervond (65%).
- Een derde geeft aan dat het niet zo belangrijk was (34%).

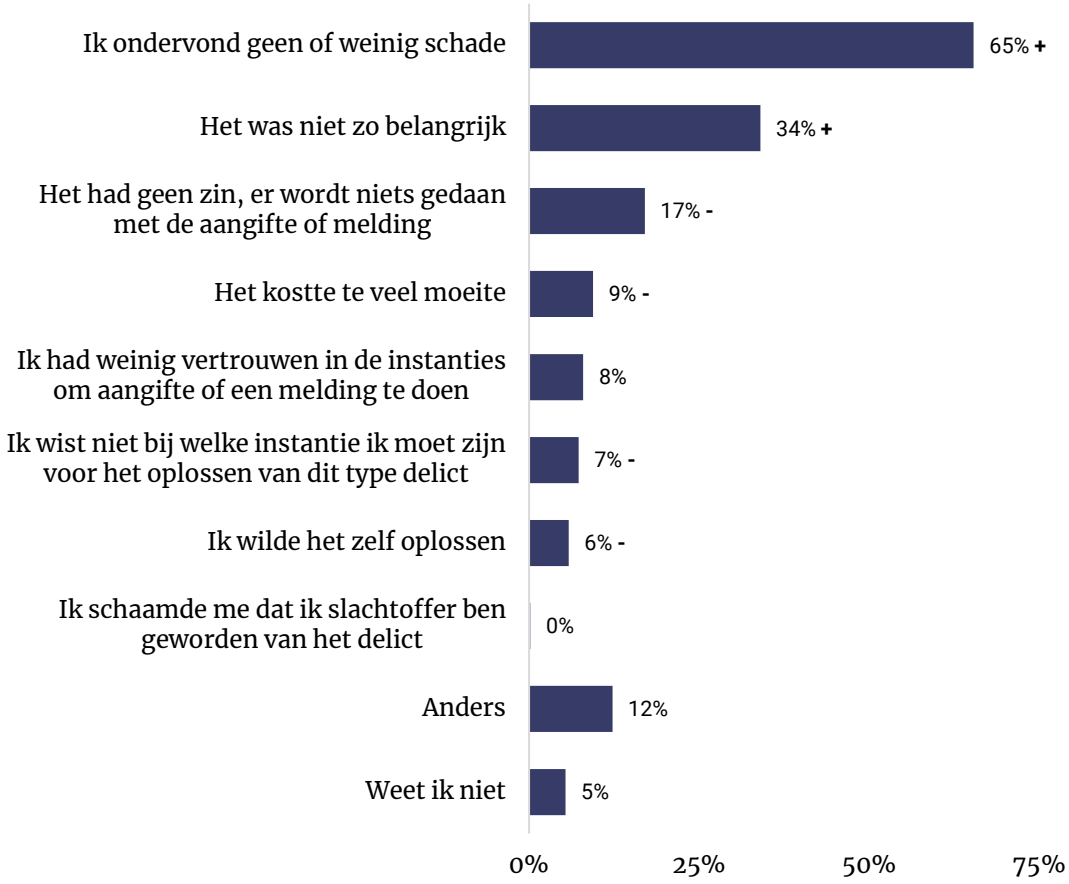
**Vergelijking met 2024**

- Men noemt vaker dan in 2024 dat er weinig schade was en dat aangifte of melding daarom niet nodig was (2025: 65%; 2024: 55%).
- Ook noemen meer mensen dat het niet zo belangrijk is (2025: 34%; 2024: 11%).
- Een aantal andere opties, zoals 'het heeft geen zin, er wordt niets gedaan met de aangifte/melding' worden nu minder genoemd (2025: 17%; 2024: 25%).

**Resultaten subgroepen**

- Nederlanders onder de 40 jaar vinden het vaker te veel moeite om aangifte of melding te doen. Ook geven ze vaker aan geen schade te hebben.
- Vrouwen noemen vaker dan mannen dat ze geen aangifte deden, omdat ze niet wisten waar ze dit moesten doen.

**Wat zijn de belangrijkste redenen om geen aangifte of melding te doen?** (gesteld aan iedereen die privé een geval van cybercrime meemaakte en hier niks mee deed; n=574) (maximaal 3 antwoorden)



# Voorkomen meer slachtoffers belangrijke reden voor aangifte of melding

- Twee op de drie Nederlanders die aangifte of melding doen nadat ze een voorval meemaken, doen dit om te voorkomen dat de dader opnieuw slachtoffers kan maken (62%).
- In het verlengde hiervan willen twee op de vijf (41%) een veiligere omgeving creëren.
- Vijftien procent doet aangifte om de schade vergoed te krijgen.

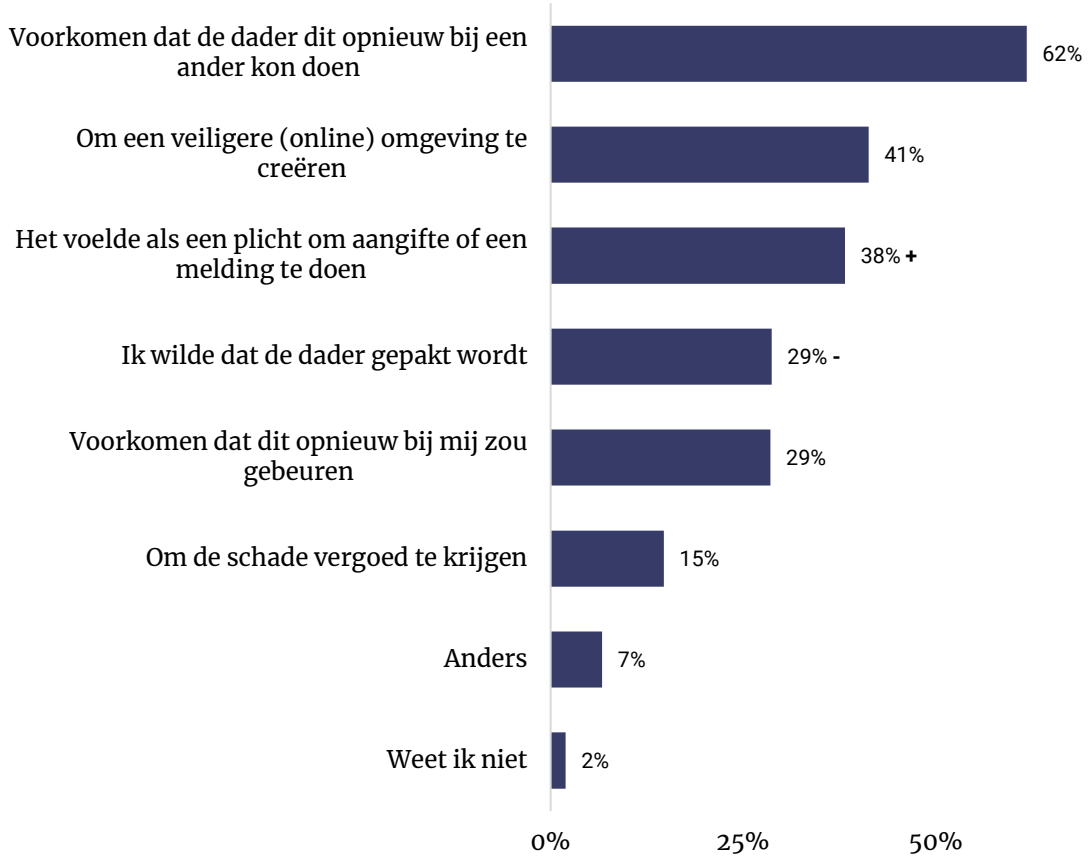
**Vergelijking met 2024**

- Vaker dan in 2024 doet men aangifte of melding omdat het als een plicht voelde (2025: 38%; 2024: 30%).
- Het willen dat de dader gepakt wordt, noemt men nu minder vaak dan een jaar eerder als reden om aangifte of melding te doen (2025: 29%; 2024: 40%).

**Resultaten subgroepen**

- Mannen geven vaker dan vrouwen aan dat ze willen dat de dader gepakt wordt en willen voorkomen dat de dader opnieuw toe kan slaan.
- Dit zijn ook relatief vaak redenen om een melding of aangifte te doen als men zelf geen of weinig gevolgen heeft ervaren.

**Wat zijn de belangrijkste redenen om aangifte of melding te doen?**
(gesteld aan iedereen die privé een geval van cybercrime meemaakte en hier aangifte of melding van deed; n=293)
(maximaal 3 antwoorden)



# Kwart gaat anders om met digitale veiligheid na meemaken cybercrime

- Een kwart (25%) van de Nederlanders die één of meerdere voorvallen van cybercrime meemaakten, gaat sindsdien op een andere manier om met de eigen digitale veiligheid.
- Als men gevolgen heeft ervaren van de meegemaakte voorvallen, verandert men vaker de omgang met digitale veiligheid. Dat geldt helemaal wanneer de gevolgen ernstig waren.

**Vergelijking met 2024**

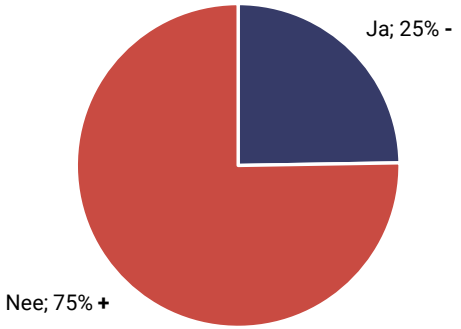
- In 2025 gaven minder Nederlanders aan dat ze op een andere manier omgaan met hun digitale veiligheid hebben naar aanleiding van het meemaken van cybercrime (2025: 25%; 2024: 38%).

**Resultaten subgroepen**

- Van de Nederlanders onder de 40 jaar gaat 13 procent anders om met hun digitale veiligheid na het meemaken van een voorval, 87 procent doet dit niet.
- Wanneer men geen of weinig gevolgen ervaarde van de cybercrime, verandert men de omgang met hun digitale veiligheid minder vaak.

U geeft aan dat u zelf thuis, in uw privésituatie of op het werk te maken heeft gehad met een of meerdere voorvallen van cybercrime.

**Gaat u sindsdien op een andere manier om met uw digitale veiligheid?**
(gesteld aan iedereen die een geval van cybercrime meemaakte; n=889)



# Contactgegevens

**Ipsos I&O Enschede**
Zuiderval 70
Postbus 563
7500 AN Enschede
053 - 200 52 00
KVK-nummer 08198802
nl-info-publiek@ipsos.com
www.ipsos-publiek.nl

**Ipsos I&O Amsterdam**
Piet Heinkade 55
1019 GM Amsterdam
020 – 308 48 00
nl-info-publiek@ipsos.com
www.ipsos-publiek.nl