



Cybersecurity onderzoek Alert Online 2023

Rapport I&O Research

Colofon

Uitgave

I&O Research
Piet Heinkade 55
1019 GM Amsterdam

Rapportnummer

2023/169

Datum

september 2023

Opdrachtgever

Ministerie van Economische Zaken en Klimaat

Auteurs

Melle Conradie
Bram Doms

Copyright

Het overnemen uit deze publicatie is toegestaan, mits de bron duidelijk wordt vermeld.

Inhoudsopgave

Colofon	2
Inhoudsopgave	3
1. Managementsamenvatting	4
2. Inleiding en achtergrond	13
3. Kennis en ervaring online risico's	17
4. Zorgen om digitale veiligheid	25
5. Online gedrag	31
6. Slachtofferschap en aangiftebereidheid	41
Contactgegevens	47

1. Managementsamenvatting



Samenvatting | kennis en ervaring online risico's

In dit rapport richten we ons op Nederlanders van 16 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 managementsamenvatting van dit rapport leggen we kruisverbanden met deze rapportages.

Driekwart Nederlanders tevreden over eigen kennis, phishing blijft meest ervaren vorm van cybercrime¹

De kennis over digitale risico's schat men vergelijkbaar in als in eerdere jaren. Driekwart van de Nederlanders vindt de eigen kennis redelijk tot goed. Een ruime meerderheid zegt de meeste vormen van cybercrime dan ook te kennen. Het aandeel dat de eigen kennis matig vindt, is iets toegenomen tot 22 procent. Zes procent beoordeelt de eigen kennis als slecht of zeer slecht. 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. Nederlanders onder de 40 jaar schatten hun eigen kennis hoger in dan ouderen.

Twee op de vijf (38%) Nederlanders hebben zelf eens met phishing te maken gehad. Malware (20%) en hacking (10%) completeren de top drie. In de afgelopen 12 maanden had men ook veel te maken met (pogingen tot) WhatsAppfraude (27%). De meerderheid van de Nederlanders acht het ook waarschijnlijk om met phishing (75%), malware (65%) en hacking (65%) te maken te krijgen. Vergeleken met vorig jaar is de groep die denkt met deze vormen van cybercrime te maken te krijgen groter geworden. Ook het aandeel dat te maken denkt te krijgen met helpdeskfraude en QR-codefraude is groter dan in 2022. Om te bepalen of men een e-mail vertrouwt, kijkt 72 procent naar het (al dan niet) vragen om financiële gegevens in de e-mail. Ook het verzoek om inloggegevens en wachtwoord in te voeren (69%), de afzender (66%) en het taalgebruik (65%) zijn veelgenoemde aspecten om de betrouwbaarheid van e-mails te bepalen. Nederlanders jonger dan 40 jaar letten vaker dan ouderen op verschillende aspecten van de e-mail.

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 42.

Samenvatting | zorgen om digitale veiligheid

Zorgen over eigen digitale veiligheid nemen verder af

De helft (53%) van de Nederlanders maakt zich geen of weinig zorgen over digitale veiligheid in de privésituatie. Bij digitale veiligheid op het werk is dat zelfs driekwart (75%). In zowel de privésituatie als op het werk maken Nederlanders zich minder zorgen over hun digitale veiligheid dan in 2022. De voornaamste aspecten waarover men zich wel zorgen maakt zijn het kwijtraken van financiële of persoonlijke gegevens, en dat internetcriminelen steeds slimmer te werk gaan. Naarmate Nederlanders ouder zijn, maken ze zich meer zorgen over hun digitale veiligheid in de privésituatie (65+: 33% weinig/geen zorgen). Ook lageropgeleiden maken zich meer zorgen dan gemiddeld (34% weinig/geen zorgen). Zes op de tien (60%) Nederlanders maken zich minimaal enige zorgen over de digitale veiligheid van hun naasten. Deze zorgen spelen naar verhouding meer bij Nederlanders van 40 jaar of ouder.

De helft van de Nederlanders die zich relatief weinig zorgen maken over hun digitale veiligheid in hun privésituatie geeft aan dat ze altijd de apparaten updaten. Ook het gebruikmaken van twee-staps-inloggen en het controleren op valse websites/links geeft voor de helft van de Nederlanders een veilig gevoel. Het twee-staps-inloggen wordt vaker als reden genoemd dan in 2022.

In 2023 waren een aantal grote datalekken in het nieuws. Een op de vijf Nederlanders maakt zich nu in grote mate zorgen om een datalek. Twee op de vijf geven aan dat ze zich beperkt of helemaal geen zorgen maken. Twee derde paste het gedrag aan naar aanleiding van de datalekken begin 2023: 21 procent is veel voorzichtiger en 45 procent is iets voorzichter. Een derde veranderde niets aan het eigen gedrag.

Samenvatting | online gedrag

Nederlanders geven zichzelf net als in 2022 een ruime voldoende voor omgang met online risico's

Nederlanders geven zichzelf een 6,8 voor het omgaan met online risico's. Dit is vergelijkbaar met 2022 (6,9). Zes op de tien Nederlanders geven zichzelf een 6 of een 7, dat is een stijging ten opzichte van 2022. Een kwart geeft zichzelf een 8 of hoger en 12 procent geeft zichzelf een onvoldoende. Nederlanders onder de 40 jaar geven zichzelf vaker een 8 of hoger dan ouderen.

Twee-staps-inloggen is de meest genomen beveiligingsmaatregel (door 86%). Dit is toegenomen ten opzichte van een jaar eerder. Bijna net zoveel Nederlanders hebben automatische updates ingeschakeld (84%). Ook het gebruik van een virusscanner is een populaire maatregel (80%).

Veel voorgelegde beveiligingsmaatregelen neemt men al of is men bereid te gaan nemen. Bijna negen op de tien Nederlanders controleren al op welke links ze klikken. Vier op de vijf installeren updates en driekwart gebruikt antivirussoftware. Het gebruik van lange wachtwoorden en VPN-verbinding is toegenomen. Wel zeggen meer Nederlanders dan vorig jaar dat ze geen antivirussoftware gebruiken en dit ook niet willen doen (13%; 2022: 9%). 65-plussers maken vaker gebruik van antivirussoftware en zijn vaker bereid om een specialist in te huren. Nederlanders onder de 40 jaar maken vaker gebruik van unieke wachtwoorden, een wachtwoordmanager en browserextensies om cookies, advertenties en automatisch toegang tot Javascript te blokkeren.

De voornaamste belemmeringen voor het vertonen van veilig online gedrag zijn hetzelfde als in 2022. Net als een jaar geleden wil ruim de helft niet betalen voor een wachtwoordmanager (58%). Daarnaast vindt de helft (48%) het te veel gedoe om voor alle apparaten en accounts een ander wachtwoord te hebben. Voor 37 procent is beveiligingssoftware te duur, dit noemt men vaker dan een jaar eerder (2022: 33%). Voor Nederlanders tot 40 jaar hebben de belemmeringen vaker te maken met gedoe en kosten. Lageropgeleiden en 65-plussers ervaren meer belemmeringen in de complexiteit en het vertrouwen in de maatregelen. De helft van de Nederlanders verwacht zich te zullen schamen als ze in phishing zouden trappen. De meeste werkenden zouden het melden als ze per ongeluk een virus downloaden op het werk.

Samenvatting | slachtofferschap en aangiftebereidheid

Een op drie Nederlanders doet melding of aangifte na slachtofferschap cybercrime

Driekwart van de Nederlanders heeft in de 12 maanden voor het onderzoek te maken gehad met een voorval van cybercrime. Dat is vergelijkbaar met het onderzoek van 2022. Het meest maakte men (poging tot) phishing mee (58%). De ervaring met (pogingen tot) WhatsAppfraude is toegenomen naar 27 procent en staat op plek twee. Hogeropgeleiden zeggen vaker dan anderen incidenten mee te maken.

Een op de drie Nederlanders die privé met cybercrime te maken heeft, doet daar melding of aangifte van. Het meest doet men melding bij de Fraudehelpdesk (14%). Drie procent doet aangifte bij de politie en ook 3 procent maakt melding bij de politie. Nederlanders ouder dan 40 jaar doen vaker een melding of aangifte.

De voornaamste reden om geen actie te ondernemen is dat men weinige schade ondervond (54%). Daaraan gerelateerd vindt 18 procent het te veel moeite en vindt 16 procent het niet zo belangrijk. Drie op de tien Nederlanders denken dat het doen van een melding geen zin heeft omdat er niks mee gedaan wordt. 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 (67%).

Twee op de vijf (38%) geven aan dat ze naar aanleiding van de cybercrime die ze meemaakten op een andere manier omgaan met digitale veiligheid.

Samenvatting | vergelijking uitkomsten onderzoek bedrijfsleven

Hieronder worden resultaten uit het deelrapport bedrijfsleven beschreven en vergeleken met het algemeen Nederlands publiek.

ICT-verantwoordelijken schatten kennisniveau hoger in dan andere groepen medewerkers

Een op de vijf (21%) werkenden schat de eigen kennis over online veiligheid in als (zeer) goed (Nederland gemiddeld: 31%). ICT-verantwoordelijken schatten hun kennis beter in dan werkenden en Nederlanders in het algemeen: 48 procent van de ICT-verantwoordelijken beoordeelt de eigen kennis als (zeer) goed.

ICT-verantwoordelijken beter bekend met cybercrime

De bekendheid met verschillende vormen van cybercrime is onder werkenden ongeveer even groot als onder de gemiddelde Nederlander. ICT-verantwoordelijken hebben een hoger kennisniveau dan anderen. Ook achten zij het waarschijnlijker dan andere werkenden te maken te krijgen met vormen van cybercrime op het werk.

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

Bijna de helft van de ICT-verantwoordelijken (46%) maakt zich zorgen over de eigen online veiligheid op het werk. Voor andere medewerkers is dit percentage significant lager (23%). Wel geven ICT-verantwoordelijken zichzelf een hoger cijfer als het gaat om het omgaan met online risico's (7,1; medewerkers totaal 6,6). De gemiddelde Nederlander zit hier met 6,8 tussenin.

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

Twee-staps-inloggen is de meest genomen actie ten behoeve van veilig online gedrag bij bedrijven. De helft van de ICT-verantwoordelijken (49%) en medewerkers van grote bedrijven noemt deze maatregel. Kleine bedrijven ondernemen minder acties. Bovendien onderneemt een vijfde van deze bedrijven (19%) geen enkele actie ten behoeve van veilig online gedrag. Wanneer we kijken naar alle medewerkers, dan geeft 8 procent aan dat er binnen hun bedrijf geen maatregelen worden genomen. Grote bedrijven ondernemen naar verhouding juist meer acties.

Phishing komt het vaakst voor in de werksituatie

Een op de vijf (21%) medewerkers ontving in de afgelopen 12 maanden op het werk een phishingmail. Onder ICT-verantwoordelijken was dit zelfs 50 procent. Bij beide groepen is dit de vorm van cybercrime die men het meest meemaakt. Net zoals in 2022 hebben ICT-verantwoordelijken vaker te maken met verschillende voorgelegde vormen van cybercrime dan andere medewerkers.

Meerderheid onderneemt geen actie op cybercrime

Zes op de tien (59%) medewerkers die te maken kregen met cybercrime deden hier geen melding of aangifte van. Doet men dit wel, dan is de ICT-afdeling van het bedrijf de plek waar men zich het vaakste meldt (34%). Belangrijke redenen om aangifte of melding te doen zijn om te voorkomen dat de dader opnieuw slachtoffers maakt (56%) en om een veiliger online omgeving te creëren (47%). Redenen om geen aangifte of melding te doen zijn de geringe schade (door 41% genoemd), de moeite die het kost (17%) en het idee dat het weinig zin heeft (13%).

Samenvatting | uitkomsten onderzoek overheid

Hieronder worden resultaten uit het deelrapport bedrijfsleven beschreven en vergeleken met het algemeen Nederlands publiek.

Driekwart ambtenaren vindt kennis online veiligheid redelijk tot goed

Vier op de vijf ambtenaren beoordelen de eigen kennis over online veiligheid als redelijk (36%) tot (zeer) goed (43%). Dat is meer dan Nederlanders gemiddeld (71%). Een kwart van de ambtenaren vindt het eigen kennisniveau matig of nog minder (17% matig, 4% slecht, 1% zeer slecht). Ambtenaren schatten de eigen kennis vergelijkbaar in als de gemiddelde Nederlander.

Kwart ambtenaren maakt zich wel eens zorgen om digitale veiligheid op het werk

Net als onder alle werkenden, maakt driekwart van de ambtenaren (74%) zich weinig zorgen over de digitale veiligheid in de werksituatie. Zowel ambtenaren als Nederlanders beoordelen zichzelf gemiddeld met een 6,8 als het gaat om het veilig omgaan met online risico's.

Twee derde ambtenaren moet twee-staps-inloggen

Twee-staps-inloggen is de meest genomen maatregel ten behoeve van online veilig gedrag bij de overheid. Twee derde van de ambtenaren is verplicht dit te doen (2022: 54%). Daarnaast zijn er voor ambtenaren adviezen, richtlijnen en/of regels over veilig digitaal werken. Zo zijn er bij de helft richtlijnen over veilig online thuiswerken. Ambtenaren hebben meer met veiligheidsmaatregelen te maken dan medewerkers van het grootbedrijf. Vijftien procent van de ambtenaren geeft aan niet te weten welke acties binnen de organisatie worden ondernomen om veilig online gedrag te borgen, dit is meer dan in 2022 (9%).

De meeste ambtenaren vinden dat de regels over online gedrag duidelijk zijn (76%), goed na te leven zijn (83%) en dat men de juiste instrumenten krijgt om eraan te voldoen (83%). De instrumenten worden beter gewaardeerd dan onder medewerkers van het grootbedrijf. Daarentegen vinden medewerkers van het grootbedrijf de afspraken binnen hun organisatie vaker duidelijk.

Communicatie en vergroten kennis zijn verbeterpunten bij borgen gedragsregels

De voornaamste belemmering die ambtenaren ervaren voor het borgen van afspraken voor online gedrag, is weinig aansprekende communicatie (16%). Dit speelt minder bij medewerkers van het grootbedrijf. De helft van de ambtenaren ervaart geen belemmeringen bij het borgen van afspraken over veilig online gedrag. Wel ziet driekwart nog verbetermogelijkheden. Het meest noemt men het vergroten van kennis binnen de organisatie (41%), cyberoefenen (28%) en meer communicatie (23%). In 2022 noemde nog 55 procent dat het vergroten van kennis een verbeterpunt was.

Phishing meest meegemaakte vorm van cybercrime op werk

Een kwart (24%) van de ambtenaren heeft de afgelopen 12 maanden een phishingmail op het werk ontvangen. Vier procent werd benaderd voor WhatsAppfraude en ook 4 procent werd zogenaamd gebeld door een bekende of officiële instantie met als doel geld te ontvangen. Ambtenaren krijgen vaker neptelefoontjes dan in 2022. De situatie is vergelijkbaar met die van medewerkers van het grootbedrijf en werkenden in het algemeen.

Vier op de tien ambtenaren deden geen aangifte of melding van de cybercrime waar ze slachtoffer van werden. De helft deed melding bij de eigen ICT-afdeling. Medewerkers van het grootbedrijf melden vaker dan ambtenaren een meegemaakt voorval bij de ICT-afdeling of bij de politie. De voornaamste reden om geen actie te ondernemen is dat er geen of weinig schade ondervonden werd (40%). De belangrijkste redenen om wel aangifte te doen zijn het creëren van een veiligere online omgeving (56%) en voorkomen dat de dader nieuwe slachtoffers maakt (53%).

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 cyber veilig 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 in oktober wordt afgetrapt.

In opdracht van het ministerie van Economische Zaken en Klimaat (EZK) voerde I&O Research 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 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 16 jaar en ouder;
- 2 medewerkers MKB en grootbedrijf;
- 3 ICT-verantwoordelijken;
- 4 ambtenaren.

In dit rapport richten we ons op Nederlanders van 16 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 managementsamenvatting van dit rapport leggen we kruisverbanden met deze rapportages.

Leeswijzer

Hoofdstuk 3 t/m 6 van dit rapport behandelt 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 2022. 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

I&O Research voerde een landelijk representatief onderzoek uit onder Nederlanders van 16 jaar en ouder. In totaal werd een representatieve groep van 2.250 Nederlanders uitgenodigd waarvan er 1.074 (48%) meededen met het onderzoek. De dataverzameling vond plaats in het I&O Research Panel² van 10 tot 24 juli 2023. Niet alle vragen die in dit rapport worden gepresenteerd zijn aan alle 1.074 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



Drie op vier Nederlanders vinden eigen kennis redelijk tot goed



Drie op de tien Nederlanders beoordelen de eigen kennis over digitale en online veiligheid goed tot zeer goed (24% goed, 7% zeer goed). Nog eens 39 procent noemt de eigen kennis redelijk. Een vijfde (22%) beoordeelt dit als matig en 6 procent als (zeer) slecht.

Vergelijking met 2022

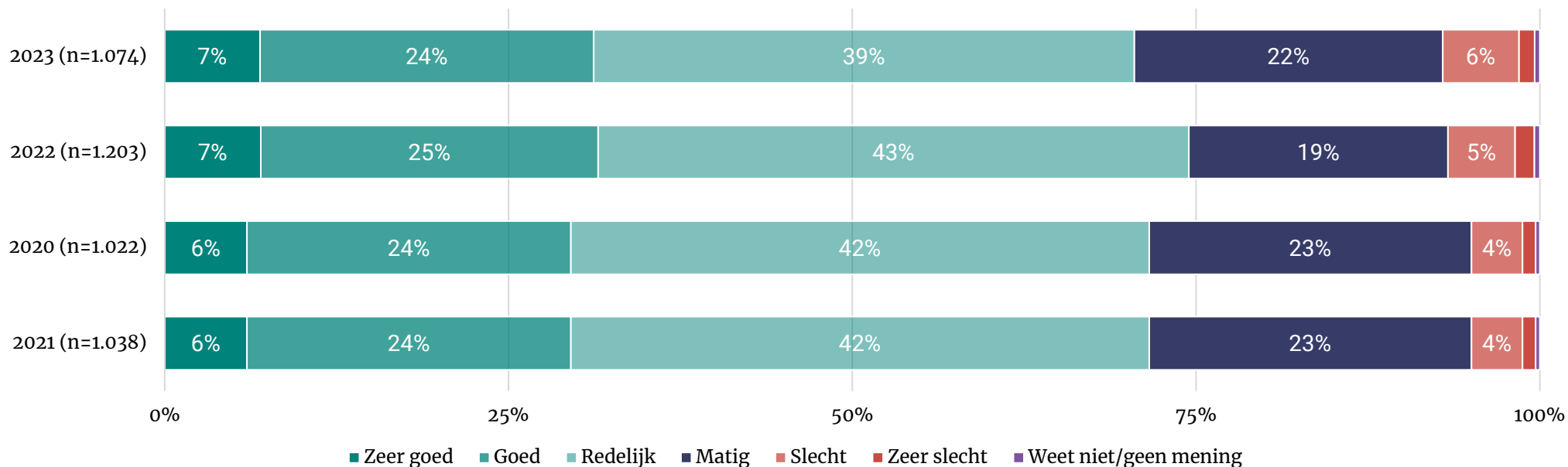
Het beeld is vergelijkbaar met eerdere jaren, maar het aandeel dat de eigen kennis als matig beoordeelt, is toegenomen.



Resultaten subgroepen

Nederlanders tot 40 jaar, mannen en hogeropgeleiden schatten hun eigen kennis over digitale veiligheid hoger in dan anderen.

Hoe schat u uw eigen kennis over digitale en online veiligheid in?



Familie en vrienden belangrijke kennisbron



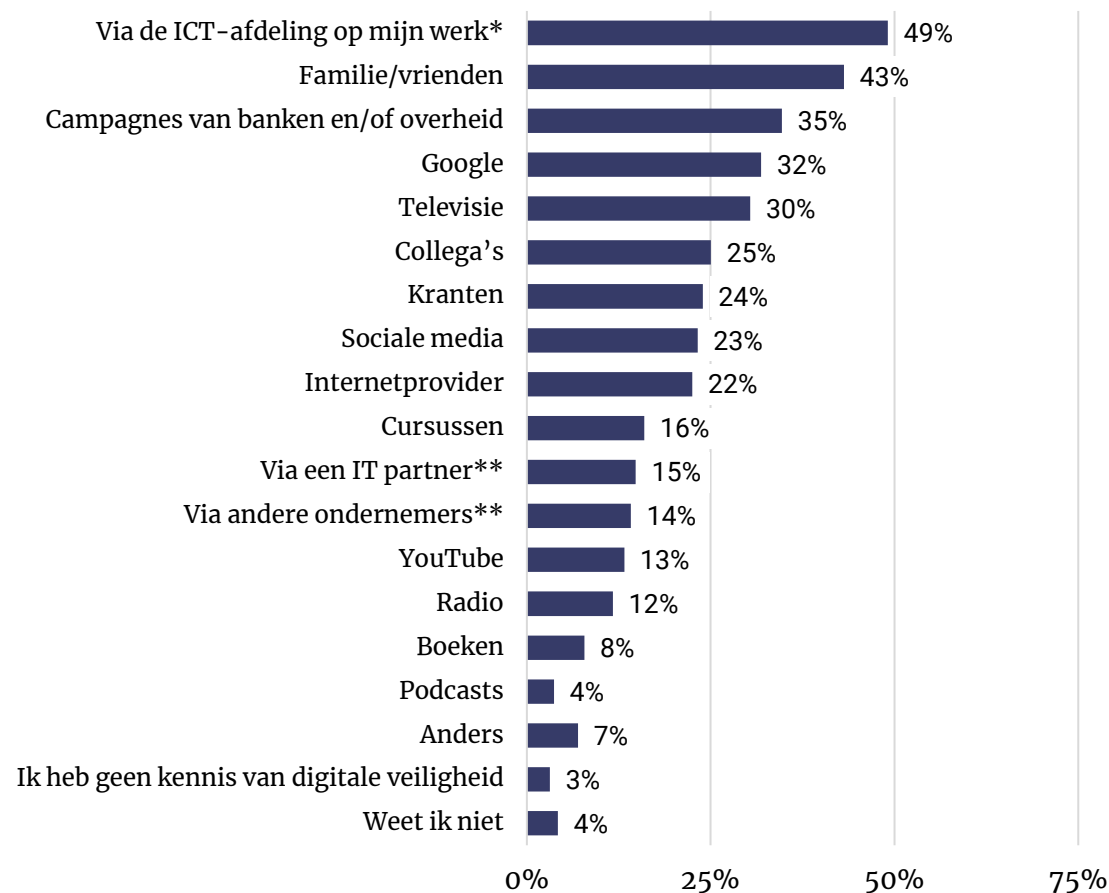
- Van de werkenden geeft de helft aan dat ze kennis over digitale veiligheid opdeden via de ICT-afdeling op het werk.
- Vrienden en familie zijn voor vier op de tien Nederlanders een belangrijke kennisbron.
- Drie procent zegt geen kennis van digitale veiligheid te hebben.

Resultaten subgroepen



- Nederlanders onder de 40 jaar, doen hun kennis naar verhouding vaker op via YouTube, podcasts, Google en social media.
- 65-plussers halen vaker informatie uit kranten en via campagnes.
- Hogeropgeleiden leren relatief vaak over digitale veiligheid via podcasts.

Op welke manier heeft u kennis over digitale veiligheid opgedaan? (n=1.074)



*Alleen voorgelegd aan werkenden (n=591).

**Alleen voorgelegd aan ondernemers (n=65).

Phishing en hacking bij vrijwel iedereen bekend



- Met uitzondering van social engineering zijn alle voorgelegde vormen van cybercriminaliteit bij de meerderheid van de Nederlanders bekend.
- Vrijwel iedereen kent phishing en hacking.

Vergelijking met 2022

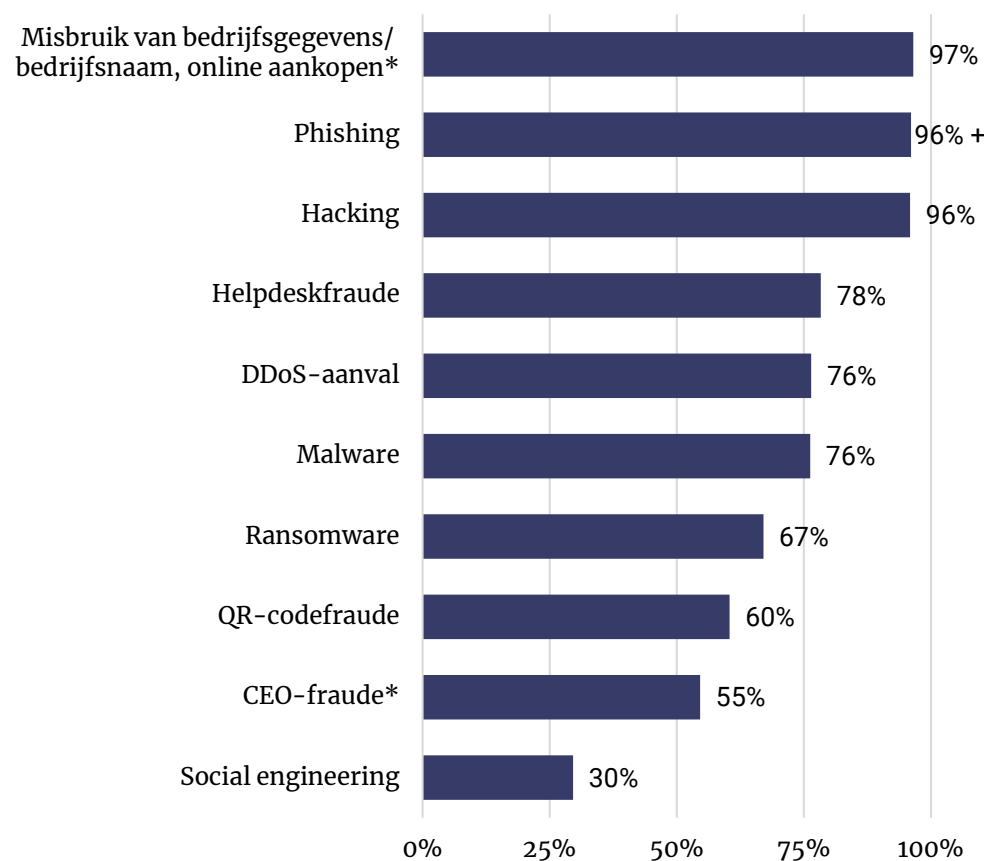
- De bekendheid met phishing is toegenomen ten opzichte van 2022.

Resultaten subgroepen

- Vrouwen geven vaker dan mannen aan nooit van malware (12% tegenover 2%), ransomware, DDoS-Aanvallen (15% tegenover 4%) en social engineering te hebben gehoord (47% tegenover 35%).
- QR-codefraude is minder bekend in de leeftijdsgroep 40 tot 65 jaar, dan bij jongeren en ouderen.
- Het begrip social engineering is het best bekend bij Nederlanders onder de 40 jaar.



In welke mate bent u bekend met de onderstaande zaken?
(n=1.074; % bekend)



*Alleen voorgelegd aan ondernemers (n=65) en nieuwe categorie in 2023.

Ervaringen met phishing toegenomen in 2023



- Met phishing (51%), malware (29%) en hacking (15%) hebben meer Nederlanders te maken (zelf of in de kennissenkring) dan met andere vormen van cybercrime.

Vergelijking met 2022

- Net als in 2022 zijn phishing, malware en hacking de vormen van cybercrime waar men het meest mee te maken heeft.
- Meer Nederlanders dan in 2022 hebben ervaring met phishing, zowel doordat ze dit zelf meemaakten als doordat een bekende hiermee te maken had.
- Ook kennen meer Nederlanders dan een jaar eerder bekenden die met DDoS-aanvallen te maken hadden.

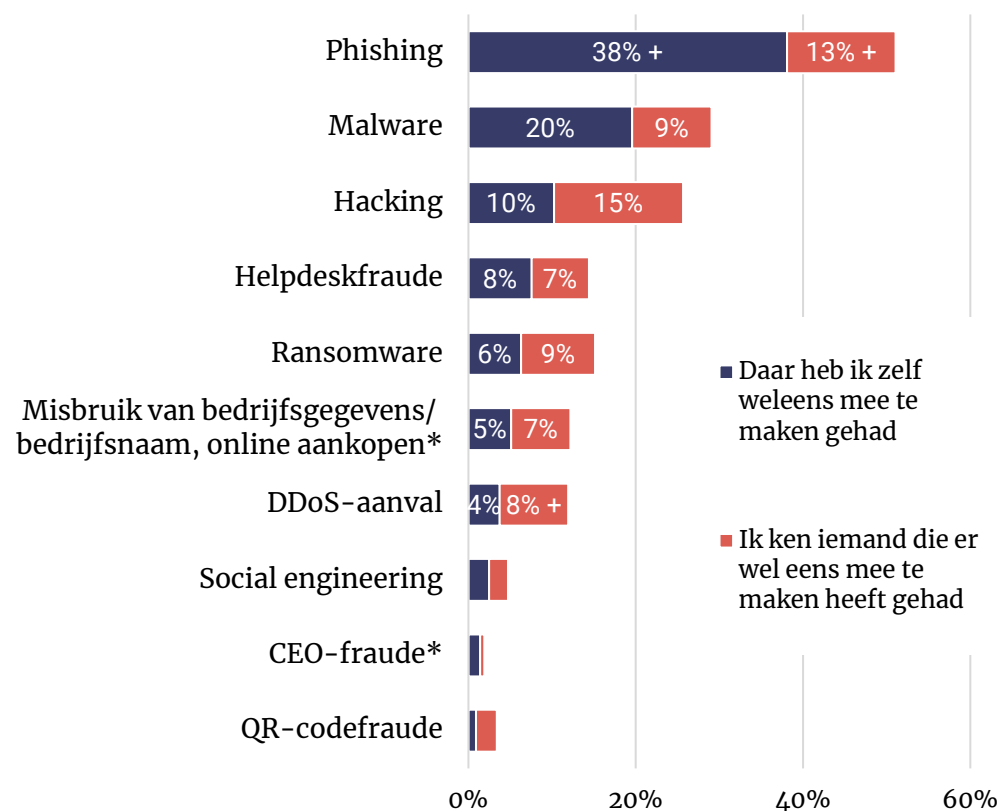
Resultaten subgroepen

- Hogeropgeleiden en mannen geven vaker aan dat ze zelf helpdeskfraude en social engineering meemaakten.
- Hogeropgeleiden hebben naar verhouding vaker te maken met phishing.



In welke mate bent u bekend met de onderstaande zaken?

(n=1.074) - ervaring



*Alleen voorgelegd aan ondernemers (n=65) en nieuwe categorie in 2023.

Driekwart acht ervaring met phishing in privésituatie waarschijnlijk



- De vormen van cybercrime die het meest bekend zijn, zijn ook de vormen die men vervolgens het meest waarschijnlijk acht mee te maken.
- Drie op de vier Nederlanders denken privé met phishing te maken te kunnen krijgen.
- Twee derde acht het waarschijnlijk malware en hacking mee te maken.
- Het minst verwacht men slachtoffer te worden van DDoS-aanvallen.

Vergelijking met 2022

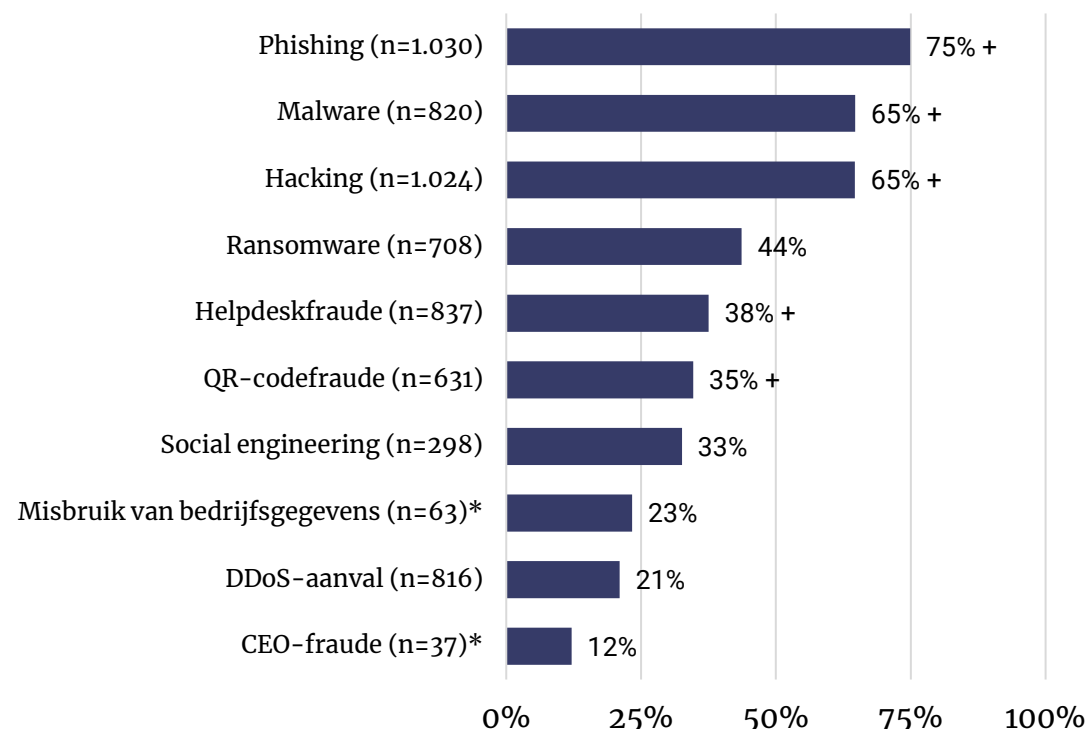
- Vaker dan vorig jaar denkt men te maken te kunnen krijgen met phishing, malware, hacking, helpdesk- en QR-codefraude.

Resultaten subgroepen

- Hogeropgeleiden achten slachtofferschap van malware, phishing, ransomware en social engineering vaker waarschijnlijk dan anderen.
- 65-plussers denken minder vaak met malware, ransomware en social engineering te maken te kunnen krijgen.



Denkt u dat u in uw privésituatie te maken kunt krijgen met deze vormen van cybercriminaliteit? (% Genoemd; men kreeg begrippen voorgelegd die men zegt te kennen)



*Alleen voorgelegd aan ondernemers en nieuwe categorie in 2023.

Vraag naar financiële gegevens in e-mail belangrijkste aspect voor bepalen betrouwbaarheid



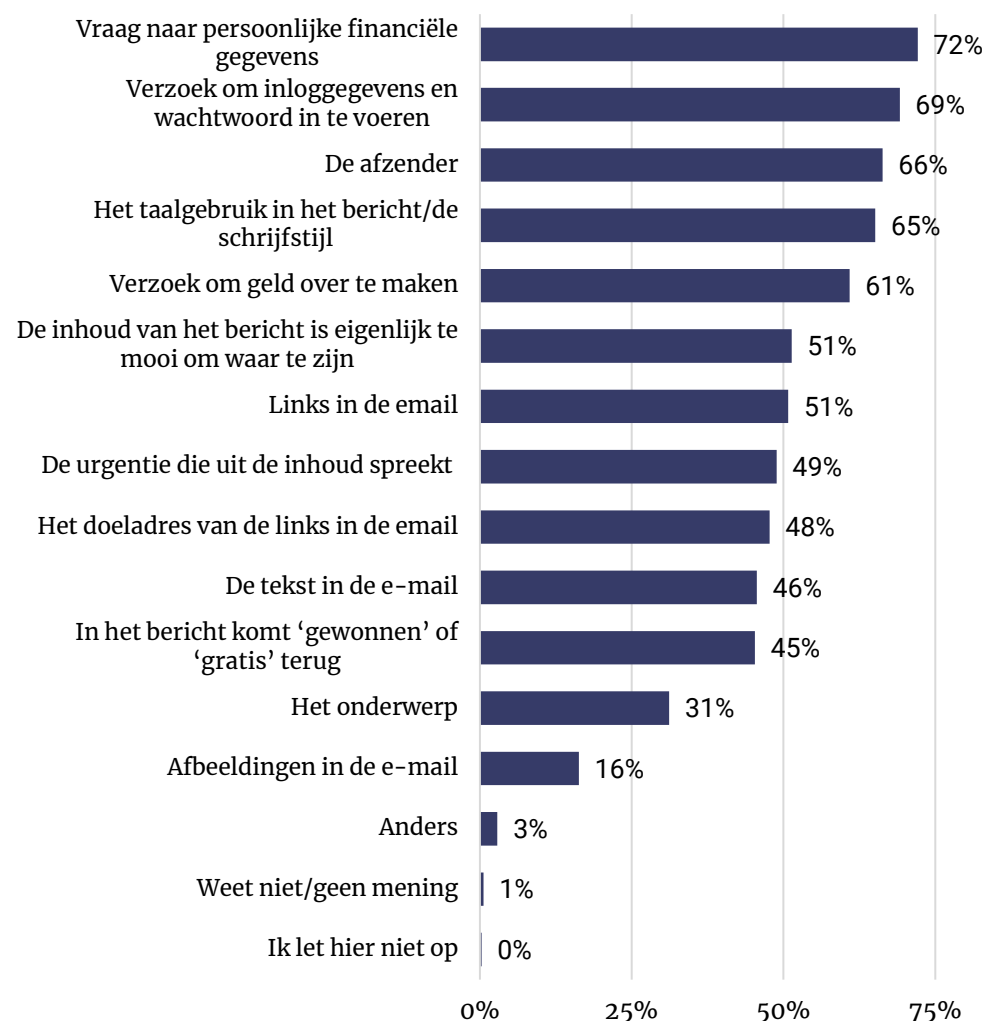
- De meerderheid van de Nederlanders bekijkt verschillende aspecten van e-mails om te bepalen of ze te vertrouwen zijn.
- Driekwart zegt bij het bepalen van de betrouwbaarheid van een e-mail te kijken naar de vraag om financiële gegevens.
- Het verzoek om inloggegevens en wachtwoord in te voeren doet bij twee derde alarmbellen rinkelen.
- Vervolgens kijkt men het meest naar de afzender, taalgebruik/schrijfstijl, en of men verzocht wordt om geld over te maken.

Resultaten subgroepen

- Nederlanders jonger dan 40 jaar letten vaker dan ouderen op verschillende aspecten in de e-mail om te bepalen of ze de e-mail vertrouwen.
- Ook hogeropgeleiden controleren ontvangen e-mails op meer aspecten dan gemiddeld.



Stel dat u een e-mail krijgt. Op welke aspecten let u om te bepalen of de e-mail te vertrouwen is of niet? (n=1.074)



Phishing op telefoon: alarmbellen gaan af bij vraag om geld en financiële gegevens



- Bij sms en WhatsApp kijkt men minder dan bij e-mail naar verschillende onderdelen om phishing te herkennen.
- De helft van de Nederlanders zegt phishing via sms of WhatsApp te herkennen door de vraag om persoonlijke financiële gegevens. Net zo vaak noemt men bedenkingen te hebben als er gevraagd wordt om geld over te maken.
- Andere veelgenoemde alarmsignalen zijn de vraag om inloggegevens in te voeren, een link of betaalverzoek en de schrijfstijl in het bericht.

Vergelijking met 2022

- In vergelijking met 2022 kijkt men vaker naar het nummer van de afzender, de profielfoto en zegt men vaker alle ongevraagde berichten weg te gooien.

Resultaten subgroepen

- Nederlanders onder de 40 jaar en hogeropgeleiden kijken vaker naar het nummer en de profielfoto om phishing per telefoon te herkennen.
- Jongeren kijken verder ook vaker naar het taalgebruik in het bericht.



Naar welke onderdelen van een bericht kijkt u vooral om phishing via SMS of WhatsApp te herkennen?

(n=1.074)



4. Zorgen om digitale veiligheid



Zorgen over digitale veiligheid nemen af



- De meeste Nederlanders maken zich niet veel zorgen over hun digitale veiligheid.
- Zes procent maakt zich veel zorgen over digitale veiligheid in de privésituatie. Twee op de vijf maken zich enige zorgen en de helft maakt zich weinig of geen zorgen.

Vergelijking met eerdere jaren

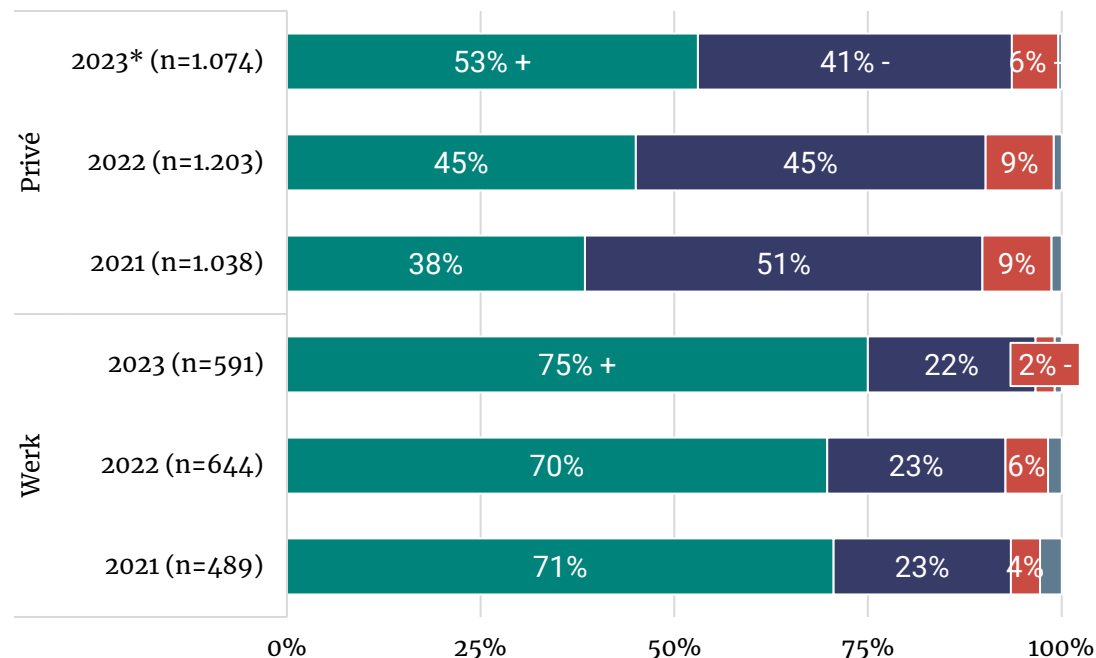
- Gemiddeld genomen zijn de zorgen afgenomen ten opzichte van 2022.
- In 2021 maakte de helft zich nog enige zorgen.
- In de werksituatie maakt men zich minder zorgen dan in de privésituatie. Driekwart maakt zich geen of weinig zorgen. Dit is een toename ten opzichte van 2022.

Resultaten subgroepen



- In de privésituatie geldt: hoe ouder men is, hoe meer zorgen over digitale veiligheid.
- Lageropgeleiden maken zich meer zorgen over hun digitale veiligheid dan gemiddeld.

In hoeverre maakt u zich zorgen over uw digitale veiligheid in uw...?



■ (zeer) weinig / geen zorgen ■ enige zorgen ■ (zeer) veel zorgen ■ weet niet

*In 2023 is voor het eerst de categorie 'geen zorgen' opgenomen. Voor de vergelijkbaarheid met eerdere jaren is dit samengevoegd met 'zeer weinig zorgen' en 'weinig zorgen'. In 2023 gaf 6 procent aan zich privé geen zorgen te maken. Op het werk maakt 16 procent zich geen zorgen.

Meer dan helft Nederlanders maakt zich zorgen over naasten



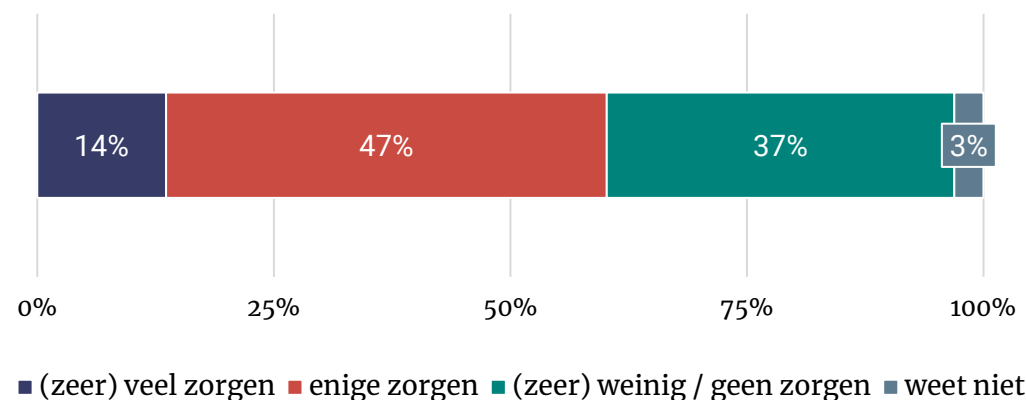
- Zes op de tien Nederlanders (60%) maken zich zorgen over de digitale veiligheid van hun naasten.
- Bijna de helft (47%) maakt zich enige zorgen en 14 procent maakt zich veel zorgen.
- Daarmee maken Nederlanders zich meer zorgen over hun naasten dan over zichzelf.

Resultaten subgroepen



- Nederlanders onder de 40 jaar maken zich minder zorgen over de digitale veiligheid van hun naasten dan oudere Nederlanders.

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



Meeste zorgen in privésituatie om gegevens die in verkeerde handen vallen



- Financiële schade en het verliezen van persoonsgegevens zijn veelgenoemde zaken waar men zich zorgen over maakt.
- Het eigen gedrag en (beperkte) kennis zijn minder een reden tot zorgen.

Vergelijking met 2022

- Een aantal zaken spelen een grotere rol bij de zorgen die men zich maakt dan in 2022. Het gaat vooral om het verliezen en misbruik van gegevens.

Resultaten subgroepen

- Nederlanders ouder dan 40 jaar maken zich vaker zorgen om de slimmere werkwijze van internetcriminelen.



Waarover maakt u zich zorgen als het gaat om uw digitale veiligheid in uw privésituatie? (gesteld aan de 47% die zich enige zorgen maakt; n=546)



Weinig zorgen digitale veiligheid omdat men update, twee-staps-inloggen gebruikt en controleert op valse links



- Bij de helft van de Nederlanders die zich veilig voelen online, speelt het mee dat ze hun apparaten altijd updaten.
- Het gebruikmaken van twee-staps-inloggen en het controleren op valse websites en links wordt door de helft genoemd.

Vergelijking met 2022

- Net als een jaar eerder is het gebruik van twee-staps-inloggen toegenomen.

Resultaten subgroepen

- 65-plussers en lageropgeleiden geven vaker dan gemiddeld aan dat ze veel zaken offline regelen en zich daarom geen zorgen maken.
- Nederlanders onder de 40 jaar noemen minder dat ze regelmatig een virusscan doen.



Waarom maakt u zich (zeer) weinig zorgen als het gaat om uw digitale veiligheid in uw privésituatie? (gesteld aan de 48% die zich weinig of geen zorgen maakt; n=467)



Een op vijf heeft zorgen om datalek, meerderheid is nu voorzichtiger



Een minderheid van een op de vijf Nederlanders maakt zich vanwege het datalek in maart 2023² (grote) zorgen om slachtoffer te worden van een datalek. Twee op de vijf maken zich weinig zorgen.

Wel is twee derde voorzichtiger geworden vanwege het datalek: 21 procent is veel voorzichtiger en nog eens 45 procent is iets voorzichtiger. Een op drie Nederlanders veranderde naar aanleiding van het datalek niets aan het gedrag.

² <https://nos.nl/artikel/2469510-datalek-nederlandse-bedrijven-steeds-groter-zeker-2-miljoen-klanten-getroffen>.

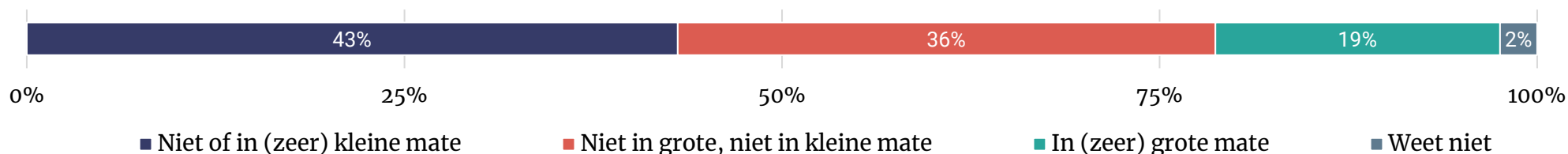


Resultaten subgroepen

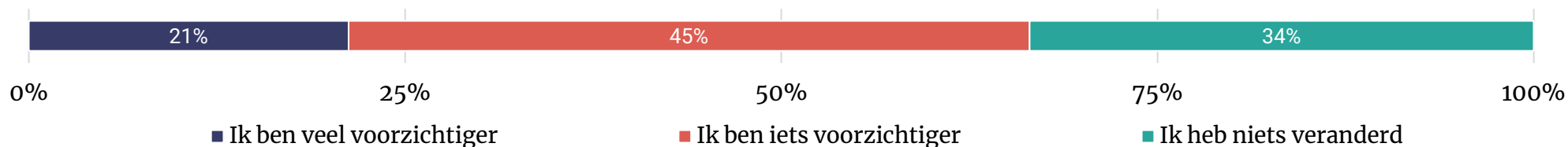
Nederlanders ouder dan 40 jaar en lageropgeleiden zijn vaker dan anderen veel voorzichtiger geworden naar aanleiding van het datalek.

In maart 2023 was er een datalek waarbij diverse Nederlandse bedrijven en daarmee miljoenen Nederlanders werden getroffen. De gegevens worden vermoedelijk gebruikt voor online oplichting. Doordat bijvoorbeeld een e-mailadres in combinatie met een naam bekend is, kan een geloofwaardige oplichtingsmail worden opgesteld.

In welke mate maakt u zich zorgen dat u slachtoffer wordt van een datalek? (n=1.074)



In hoeverre heeft u uw gedrag hierop aangepast? (n=1.074)



5. Online gedrag



Nederlanders geven vaker een 6 of een 7 voor omgang met online risico's



Nederlanders geven zichzelf een ruime voldoende voor het veilig omgaan met online risico's. Een kwart van de Nederlanders geeft zichzelf een 8 of hoger. Zes op de tien (61%) geven zichzelf een 6 of een 7. Twaalf procent beoordeelt het eigen gedrag als onvoldoende.

Vergelijking met 2022

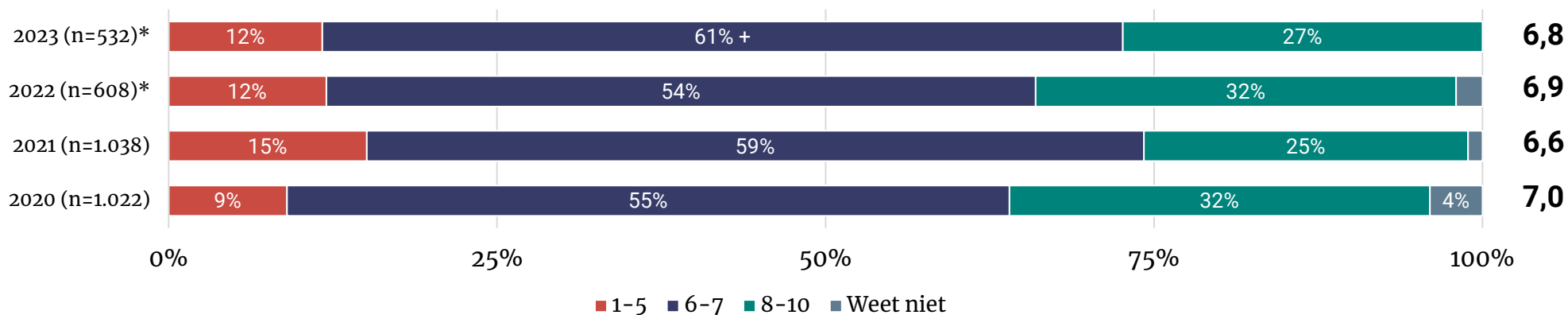
Men geeft zichzelf vaker een 6 of een 7 dan in 2022. Het gemiddelde cijfer is vergelijkbaar voor 2022 (6,9) en 2023 (6,8).



Resultaten subgroepen

- Nederlanders tot 40 jaar geven zichzelf vaker een 8 of hoger dan ouderen.
- Mannen schatten zichzelf hoger in dan vrouwen.

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 vorige jaren 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 alleen de uitkomsten weergegeven voor de vraag op de "oude" plek.

Toelichtingen bij cijfer omgang online risico's

Cijfer 1-5 (12%)

- *“Ik heb er weinig verstand van en eerlijk gezegd interesseert het mij te weinig.”*
- *“Ik heb bij alles hulp nodig van mijn partner hieromtrent.”*
- *“Het is zoveel moeite en je moet op zoveel dingen letten. Altijd die veiligheid in de gaten houden. Het is zo abstract ook.”*

Cijfer 9-10 (27%)

- *“Ik ben voorzichtig en bij twijfel doe ik altijd een controle of delete of meld het.”*
- *“Bij elke mail of download risico factoren eerst voor mijzelf inscannen vooraleer er verder actie wordt ondernomen.”*
- *“Volg veel cursussen, is een onderdeel van mijn vak, maar kan altijd nog iets leren.”*
- *“Ik bouw mijn eigen computers, gebruik uitsluitend opensource Linux en draai apps in containers en sandboxes.”*
- *“Ik ben nogal redelijk op de hoogte en behoorlijk argwanend als het om verzoeken en links gaat.”*

Cijfer 6-7 (54%)

- *“Ik probeer zo goed mogelijk op te letten en op de hoogte te blijven maar weet gewoon dat ik ook wel eens slordig ben met bijv. wachtwoorden en ik alles m.b.t. tot dit onderwerp niet voldoende volg.”*
- *“Ben niet heel erg goed in computergebruik.”*
- *“Ik weet hoeveel ik nog kan doen en weet dat ik nog heel veel niet weet.”*
- *“Ik ben me zeer bewust van de risico's, maar ik doe er zelf niet genoeg aan om deze in te perken.”*
- *“Ik heb redelijke beveiligingen, maar realiseer me dat de "hackers" slimmer zijn dan ik.”*
- *“Denk dat ik al heel voorzichtig en oplettend ben, maar vergaar niet de laatste info om me gelijk te wapenen.”*

Toename gebruik twee-staps-inloggen en wachtwoordenkluisje



- Een ruime meerderheid gebruikt twee-staps-inloggen, automatische updates en virusscanners.

Vergelijking met 2022

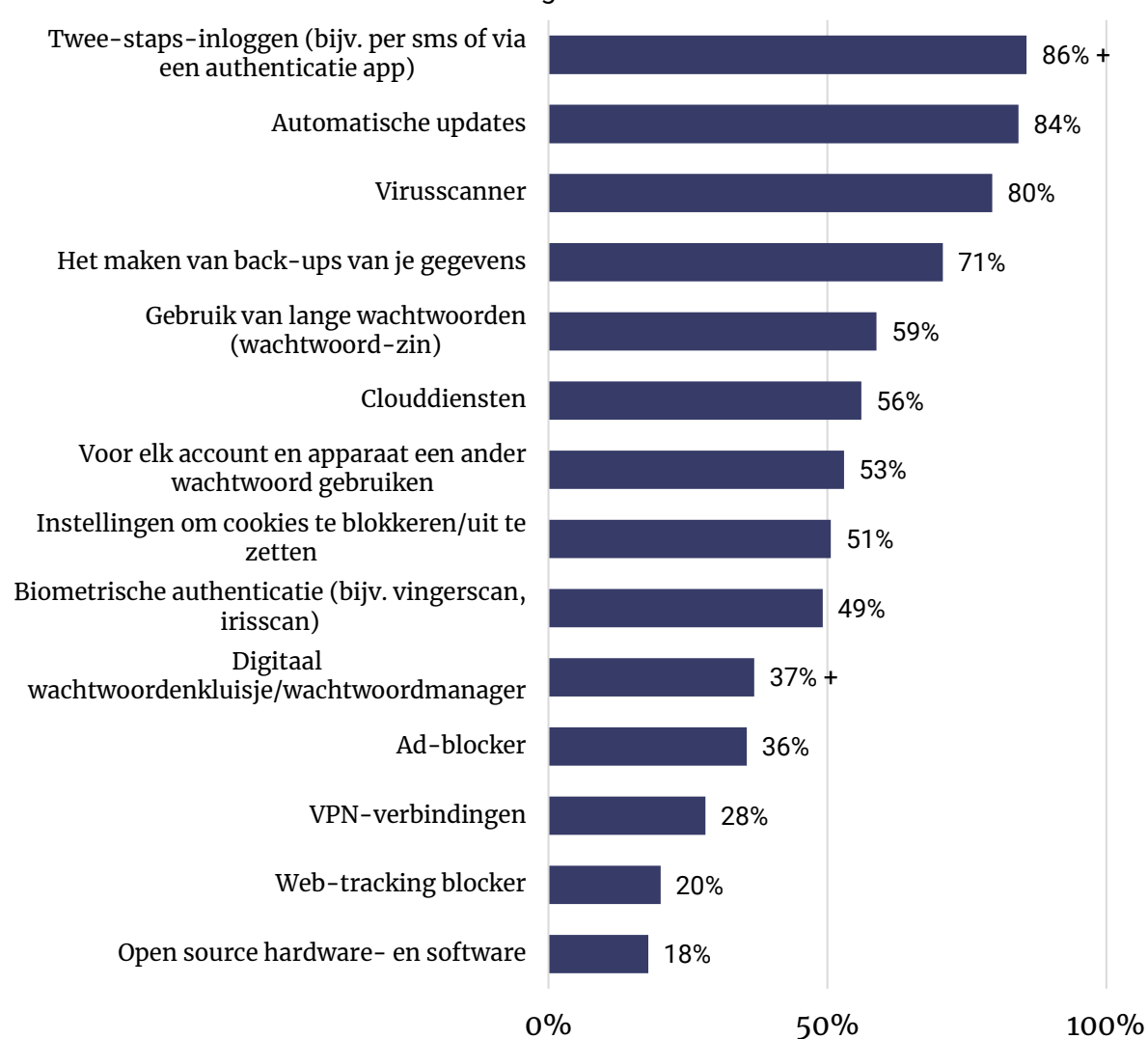
- De drie meest toegepaste maatregelen zijn dezelfde als in 2022.
- Nederlanders maken meer gebruik van twee-staps-inloggen dan in 2022 en dit is nu de maatregel die men het meest toepast.
- Ook het gebruik van een wachtwoordenmanager is toegenomen in vergelijking met een jaar eerder.

Resultaten subgroepen

- Er zijn veel verschillen in gebruik van maatregelen tussen doelgroepen. Over het algemeen nemen Nederlanders onder de 40 jaar en hogeropgeleiden meer maatregelen.
- Uitzonderingen zijn virusscanners en het gebruik van verschillende wachtwoorden: dit wordt beide meer door Nederlanders van 40 jaar en ouder gedaan.



In welke mate bent u bekend met onderstaande zaken? (n=1.074) - gebruik



Driekwart Nederlanders update software altijd



- Driekwart van de Nederlanders doet naar eigen zeggen altijd tijdig software-updates. Bijna net zoveel mensen downloaden apps/software alleen via officiële kanalen, controleren goed op links voor erop te klikken en maken altijd gebruikmaken van sterke en unieke wachtwoorden.
- Een minderheid van drie procent past geen enkele maatregel altijd toe

Vergelijking met 2022

- Een aantal maatregelen worden door meer mensen toegepast dan in 2022. Net als een jaar eerder neemt 3 procent geen beveiligingsmaatregelen.

Resultaten subgroepen

- 65-plussers zijn vaker up to date met hun software dan Nederlanders onder de 40 jaar. Ook laten Nederlanders onder de 40 jaar naar verhouding vaker anderen gebruikmaken van hun apparaten.
- 65-plussers passen minder dan jongeren de privacyinstellingen van apps aan.

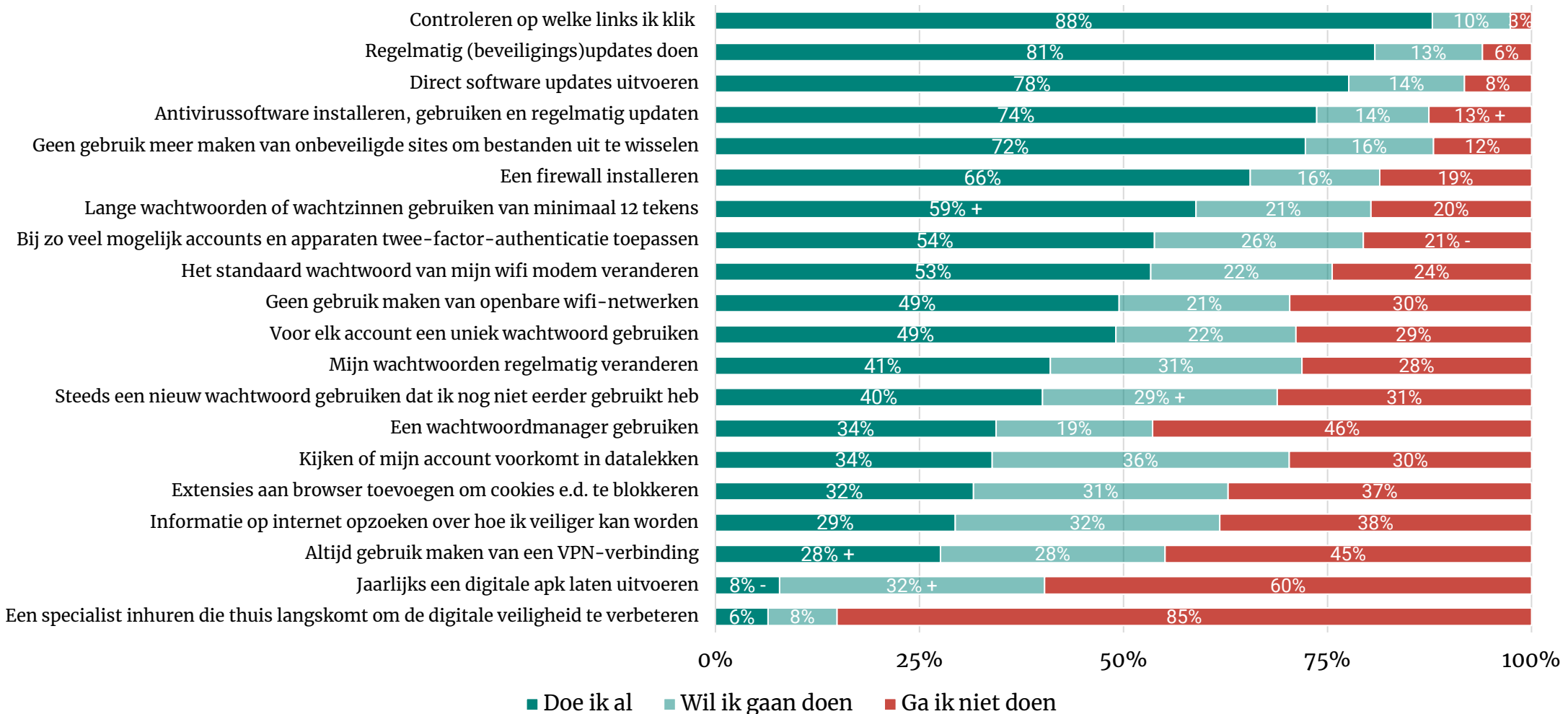


Welke van de volgende maatregelen neemt u zelf?
(elke respondent kreeg een deel van de opties voorgelegd; nmin=563; % altijd)



Veel acties voor verbetering digitale veiligheid zijn al ondernomen of is men bereid om te doen (1)

Welke van onderstaande acties heeft u ondernomen om uw digitale veiligheid te verbeteren?
 (elke respondent kreeg een deel van de opties voorgelegd; nmin=563) (toelichting op volgende pagina)



Veel acties voor verbetering digitale veiligheid zijn al ondernomen of is men bereid om te doen (2)



- Er is veel bereidwilligheid onder Nederlanders om de digitale veiligheid te verbeteren. Vrijwel alle voorgelegde acties (zie vorige pagina) doet de meerderheid al (al is hier niet uitgevraagd hoe frequent), of is men bereid te doen. Alleen een jaarlijkse digitale apk en een specialist inhuren wil een meerderheid niet doen.
- Bijna negen op de tien Nederlanders controleren al op welke links ze klikken. Vier op de vijf installeert updates en driekwart gebruikt antivirussoftware.

Vergelijking met 2022

- Positief voor de digitale veiligheid is dat het gebruik van lange wachtwoorden en VPN-verbinding is toegenomen. Minder positief is dat een grotere groep dan in 2022 zegt geen antivirussoftware te willen installeren.

Resultaten subgroepen

- Nederlanders onder de 40 jaar zeggen vaker dat ze niet gaan opzoeken hoe ze veiliger kunnen worden online. Ook willen ze minder vaak gebruikmaken van antivirussoftware. Wel passen ze al meer het gebruik van unieke wachtwoorden, een wachtwoordmanager en browserextensies toe.
- 65-plussers maken vaker gebruik van antivirussoftware en zijn vaker bereid om een specialist in te huren. Aan de andere kant controleert een kleiner deel van de 65-plussers (80%) de links waar ze op klikken.
- Van de lager en middelbaar opgeleiden laat een groter deel jaarlijks een digitale apk uitvoeren dan van de hogeropgeleiden.



Twee derde Nederlanders controleert of ze op veilige website zitten

In hoeverre zijn de volgende uitspraken van toepassing op uw gedrag?

(n=1.074; vragen over werk gesteld aan werkenden: n=591)



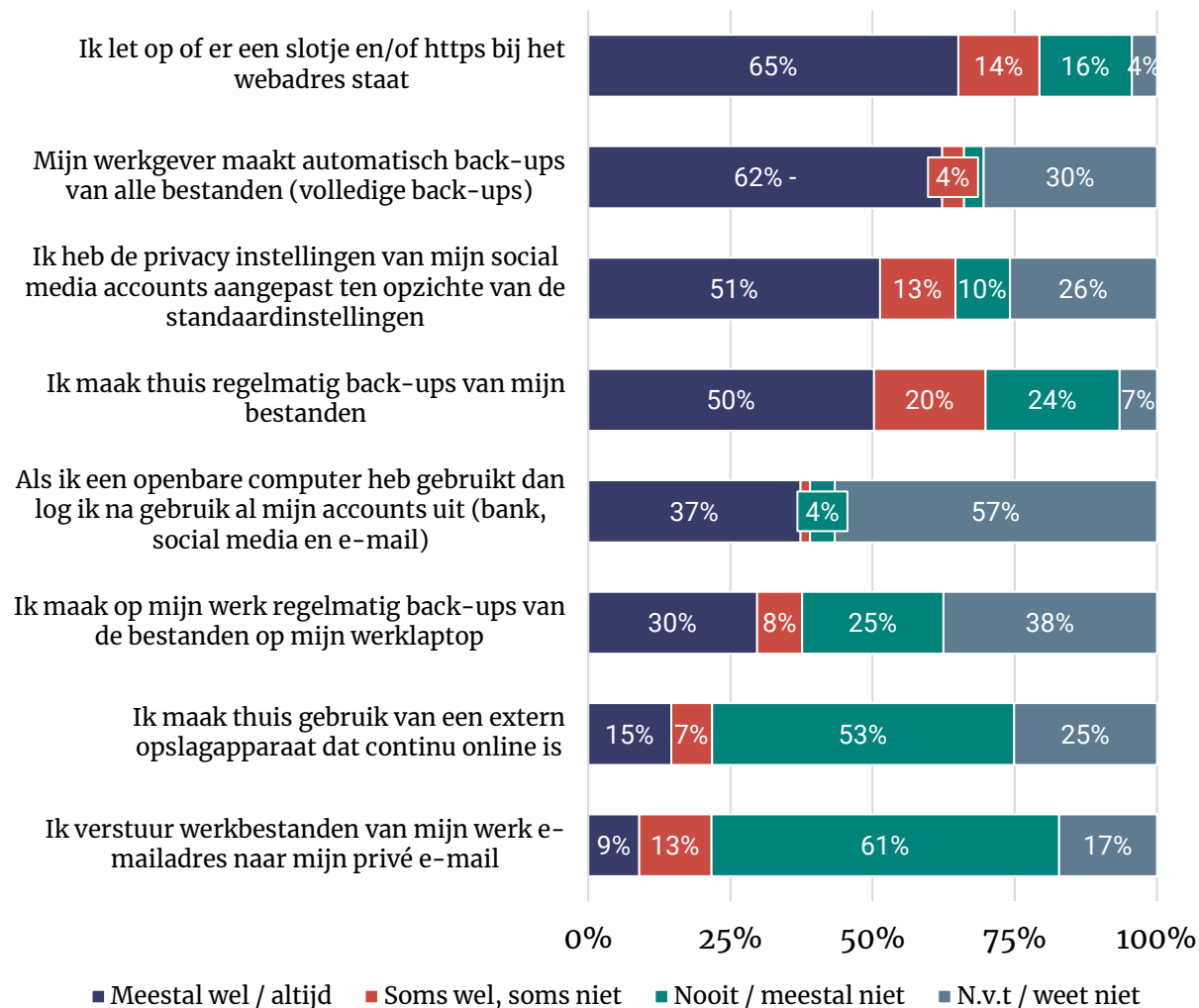
- Twee op de drie Nederlanders maken alleen gebruik van websites met een slotje.
- De helft van de Nederlanders maakt thuis back-ups van bestanden.
- Een meerderheid (62%) denkt dat hun werkgever automatisch back-ups maakt van alle bestanden, 30 procent weet het niet.
- Een op de tien Nederlanders stuurt wel eens werkbestanden via de werkmail naar de privé e-mail.

Vergelijking met 2022

- Men zegt in 2023 minder vaak dat de werkgever automatische back-ups maakt.

Resultaten subgroepen

- Nederlanders ouder dan 40 jaar en lager en middelbaar opgeleiden antwoorden vaker met 'weet niet' of 'niet van toepassing'.
- Nederlanders onder de 40 jaar geven vaker aan dat ze meestal niet controleren of ze op een veilige website zitten.



Meerderheid vertelt ICT-afdeling als ze (per ongeluk) een virus op het werk downloaden



- Ondanks schaamte, zou vrijwel iedereen het melden als ze op het werk een virus downloaden
- Twee derde van de werkenden geeft aan dat ze dit bij de ICT-afdeling zouden melden. Zeven procent geeft aan dit vanwege schaamte niet te doen.
- De helft van de Nederlanders zou zich ook schamen als ze in een phishing e-mail trappen.
- Drie procent van de Nederlanders acht het waarschijnlijk dat ze zouden betalen als ze getroffen worden door ransomware.

Vergelijking met 2022

- Minder mensen dan een jaar eerder denken zich te schamen wanneer ze in phishing trappen.

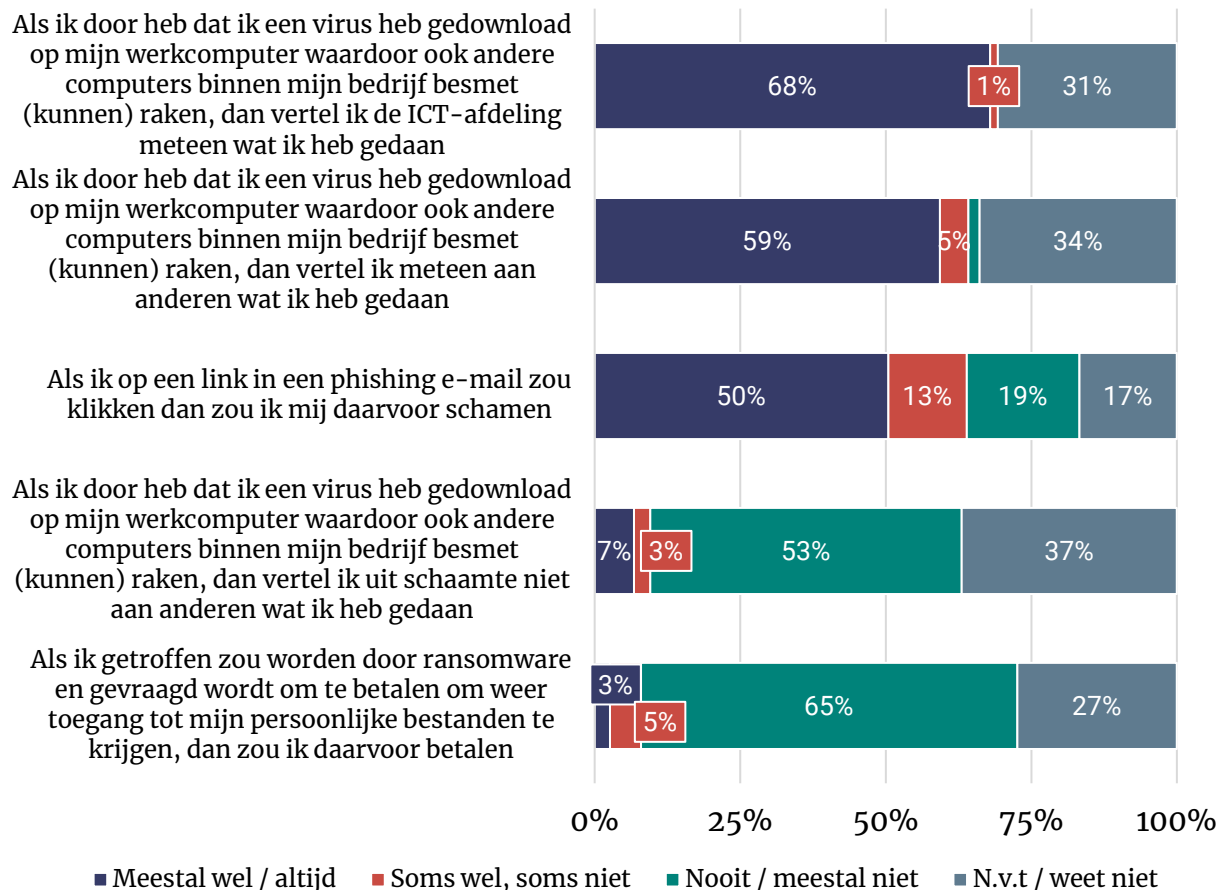


Resultaten subgroepen

- Er zijn geen relevante verschillen tussen subgroepen.

In hoeverre zijn de volgende uitspraken van toepassing op uw gedrag?

(n=1.074; vragen over werk n=591)



Kosten, gedoe en kennis grootste belemmering bij nemen maatregelen digitale veiligheid



- Ruim de helft van de Nederlanders wil niet betalen voor een wachtwoordmanager.
- In mindere mate vormen gedoe en gebrek aan kennis en vaardigheden ook belemmeringen voor online veilig gedrag.

Vergelijking met 2022

- Men vindt vaker dan in 2022 dat beveiligingssoftware te duur is.
- Ook noemt men vaker dat het te veel gedoe is om elke keer software-updates te installeren (2023: 20%; 2022: 16%).

Resultaten subgroepen

- Nederlanders tot 40 jaar ervaren meer belemmeringen door het “gedoe” en kosten van beveiliging.
- Bij 65-plussers en lageropgeleiden zitten de belemmeringen meer in de complexiteit en vertrouwen.
- Nederlanders tot 40 jaar en hogeropgeleiden hebben minder vaak vertrouwen in gratis diensten.



Kunt u aangeven in hoeverre u het eens bent met de volgende stellingen? (n=1.074; % (helemaal) mee eens)



6. Slachtofferschap en aangiftebereidheid



Poging tot phishing komt meest voor, poging tot WhatsAppfraude neemt toe



- Driekwart van de Nederlanders (74%) maakt minimaal één poging tot of voorval van cybercrime mee.
- Pogingen tot phishing kwamen het meest voor, zes op de tien Nederlanders maakten dit mee.
- Een kwart ervaren (een poging tot) WhatsAppfraude.

Vergelijking met 2022

- Ook in 2022 had driekwart van de Nederlanders zelf te maken met cybercrime en ging het vaak om pogingen tot phishing.
- Pogingen tot WhatsAppfraude komen meer voor in 2023.
- Het aantal neptelefoontjes is afgenomen.

Resultaten subgroepen

- Hogeropgeleiden hebben vaker dan anderen te maken met cybercrime. Vooral pogingen tot phishing maakten zij vaker mee.
- Nederlanders tot 40 jaar hebben minder vaak ervaring met (pogingen tot) WhatsAppfraude.



Heeft u in de afgelopen 12 maanden zelf weleens te maken gehad met één van de onderstaande voorvallen? (n=1.074)



Twee derde doet geen melding of aangifte van cybercrime in privésituatie



- Twee derde van de Nederlanders die slachtoffer van cybercrime waren, deed hier geen melding of aangifte van.
- Het meest maakt men melding bij de Fraudehelpdesk of de instantie waar het voorval zich voordeed.
- Drie procent deed aangifte bij de politie.

Vergelijking met 2022

- In 2022 deden slachtoffers vaker aangifte bij de politie (5%).
- Het aandeel dat niks doet is in 2023 vergelijkbaar met een jaar eerder.

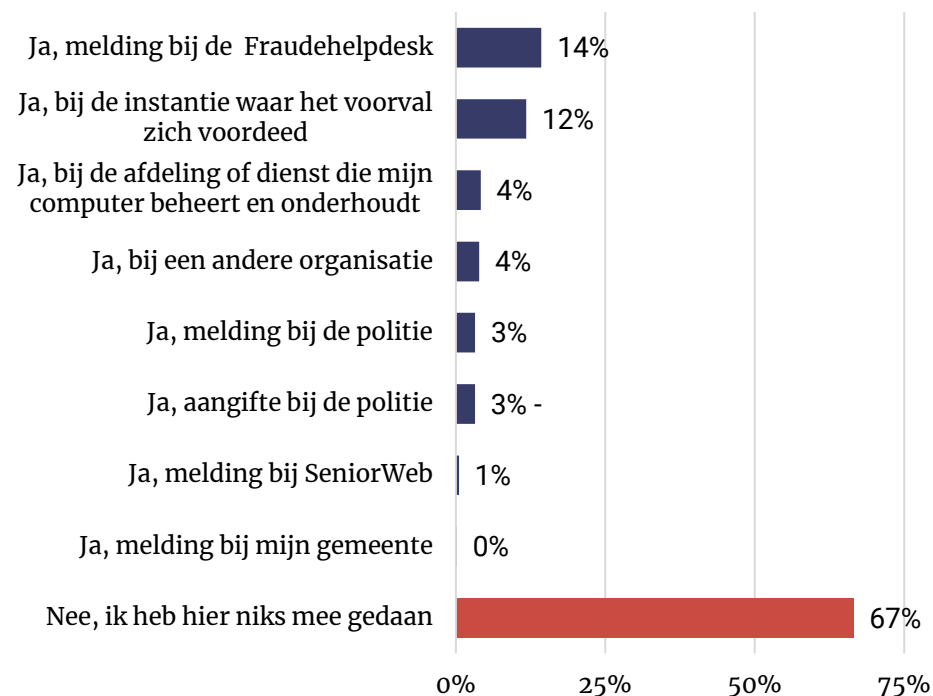
Resultaten subgroepen

- Lageropgeleiden en Nederlanders ouder dan 40 jaar doen vaker melding of aangifte dan anderen.
- 65-plussers doen naar verhouding vaker een melding bij de politie.



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=765)



Vaak geen aangifte of melding vanwege beperkte gevolgen



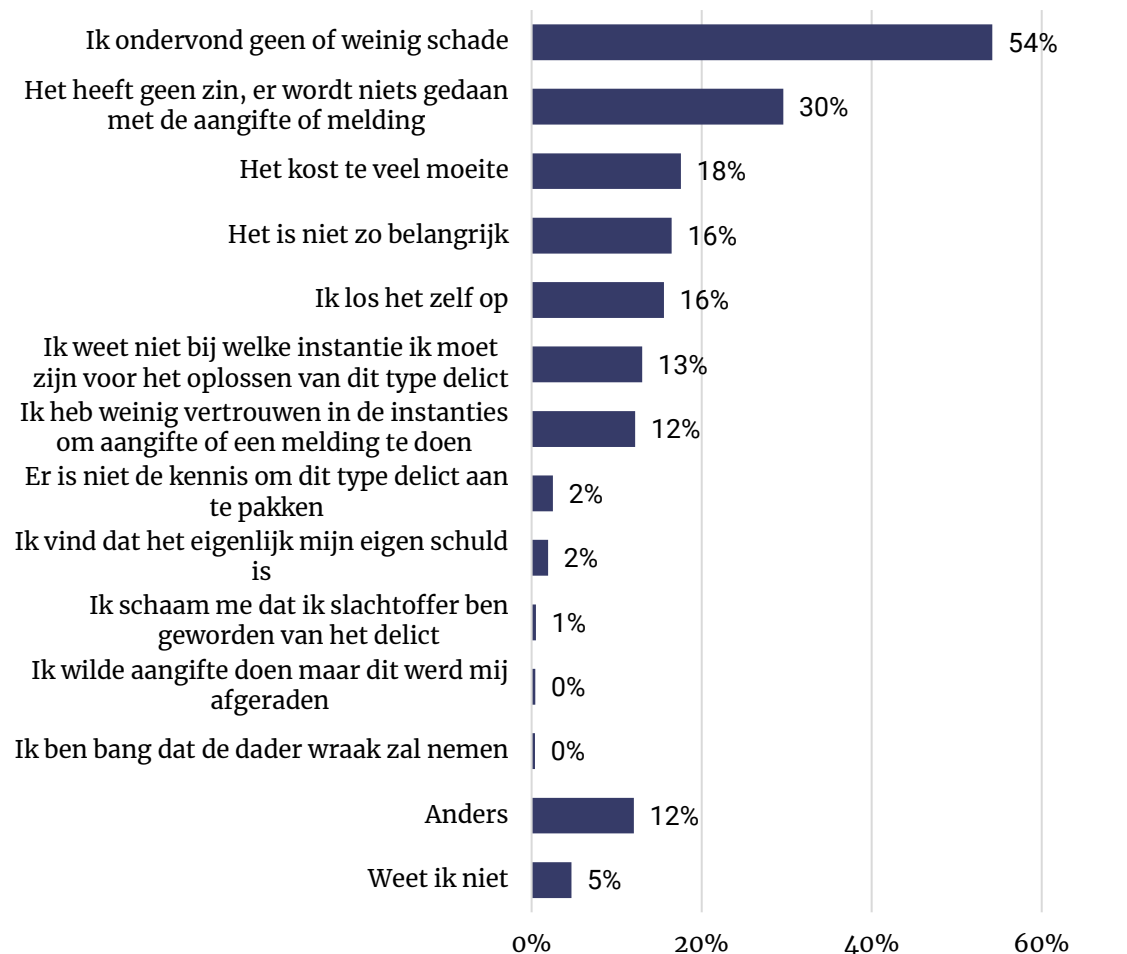
- Ruim de helft van de Nederlanders die met cybercrime te maken hebben en geen melding of aangifte doen, doen dit niet omdat ze weinig of geen schade ondervonden.
- Een vijfde zegt dat het te veel moeite kost en 16 procent zegt dat het niet zo belangrijk is.
- Drie op de tien noemen dat het geen zin heeft om melding of aangifte te doen.
- Schaamte, angst voor wraak en gevoel van 'eigen schuld' zijn voor weinig mensen reden om melding of aangifte te doen.

Resultaten subgroepen



- Nederlanders tot 40 jaar geven vaker aan dat aangifte of melding geen zin heeft.
- Nederlanders van 40 jaar en ouder willen het vaker zelf oplossen.

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=489) (maximaal 3)



Voorkomen herhaling bij anderen belangrijkste motivatie voor rapporteren cybercrime



- De voornaamste reden om aangifte of melding te doen, is te voorkomen dat de dader dit opnieuw doet.
- Vergoeding van schade is de minst belangrijke reden.

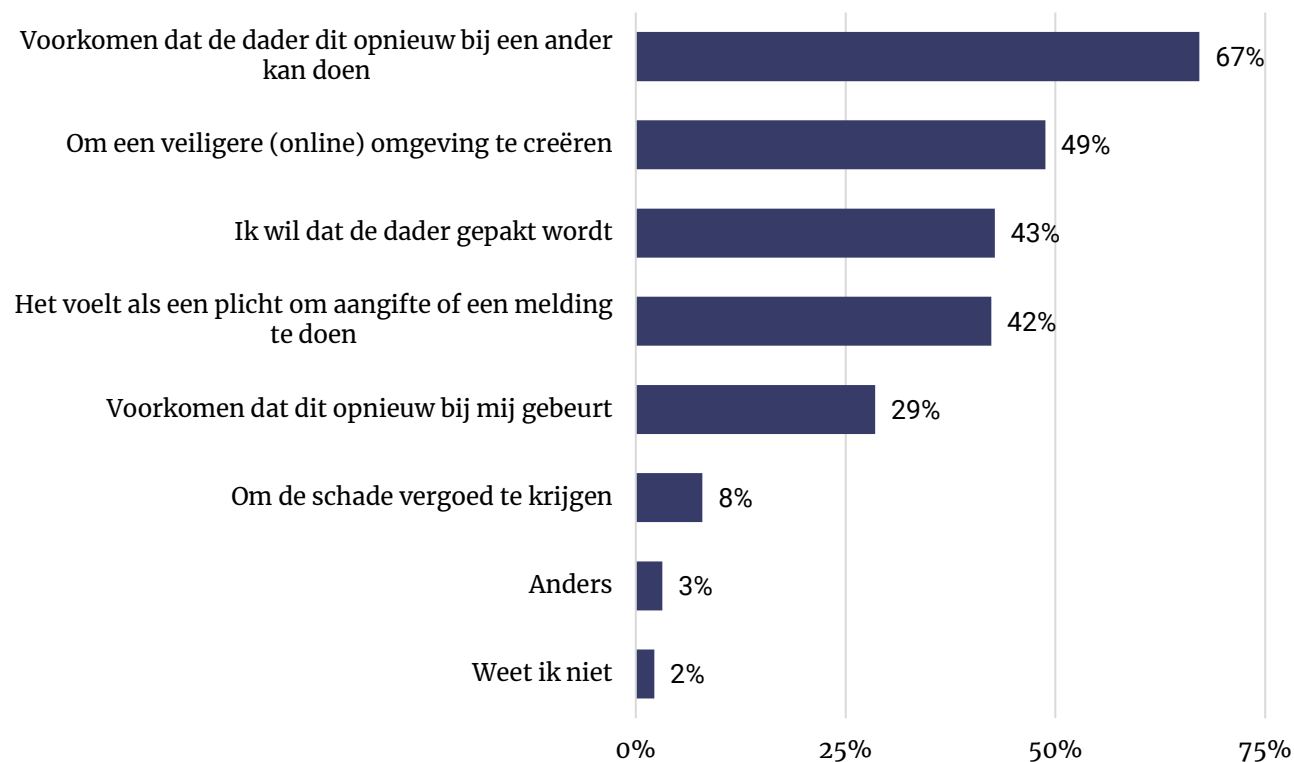
Resultaten subgroepen

- Er zijn geen relevante verschillen tussen subgroepen in redenen om geen melding of aangifte te doen.



Wat is de belangrijkste reden om wel aangifte of melding te doen?

(gesteld aan iedereen die privé een geval van cybercrime meemaakte en aangifte/melding deed; n=276)
(maximaal 3)



Twee op vijf Nederlanders passen gedrag aan na meemaken cybercrime



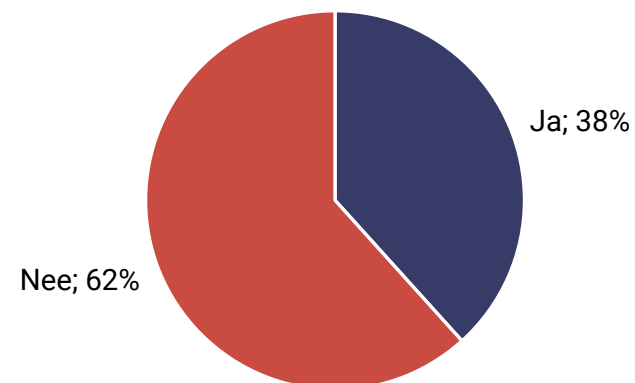
- Twee op de vijf Nederlanders die een of meerdere voorvallen van cybercrime meemaakten, gaan sindsdien op een andere manier om met de eigen digitale veiligheid.



Resultaten subgroepen

- Nederlanders onder de 40 jaar passen hun gedrag het minst vaak aan naar aanleiding van het voorval dat ze meemaakten.

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 mensen die een voorval meemaakten; n=783)



Contactgegevens

I&O Research Enschede

Zuiderval 70

Postbus 563

7500 AN Enschede

053 - 200 52 00

KVK-nummer 08198802

info@ioresearch.nl

www.ioresearch.nl

I&O Research Amsterdam

Piet Heinkade 55

1019 GM Amsterdam

020 - 308 48 00

info@ioresearch.nl

www.ioresearch.nl