Cybersecurity onderzoek Alert Online 2024

Rapport Ipsos I&O

Ipsos i&O

Ministerie van Economische Zaken

Colofon

Uitgave
Ipsos I&O
Piet Heinkade 55
1019 GM Amsterdam

Rapportnummer
2024/194

Datum
september 2024

Opdrachtgever
Ministerie van Economische Zaken

Auteurs
Melle Conradie
Sara Kellij

Inhoudsopgave

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.

Drie op de tien Nederlanders vinden eigen kennis matig tot zeer slecht

De kennis over digitale risico's schat men vergelijkbaar in als in eerdere jaren. Drie op de tien Nederlanders vinden hun kennis matig of zeer slecht. Ook drie op de tien beoordelen hun kennis als goed tot zeer goed. De grootste groep (41%) 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. Nederlanders onder de 40 jaar en hogeropgeleiden schatten hun kennis relatief hoger in.

Phishing meest ervaren vorm cybercrime[1]

Eén op de drie (33%) Nederlanders heeft zelf weleens met phishing te maken gehad. Wanneer we naar de afgelopen twaalf maanden kijken heeft men vooral te maken gehad met (geslaagde en niet geslaagde pogingen tot) phishing (55%) en WhatsAppfraude (30%). Benaderingen voor WhatsAppfraude komen meer voor dan een jaar eerder (2023: 27%). De meerderheid van de Nederlanders die de begrippen kennen, acht het ook waarschijnlijk om met phishing (77%), hacking (72%) en malware (62%) te maken te krijgen. Dit beeld is vergelijkbaar met vorig jaar. Van alle vormen van cybercrime die men waarschijnlijk acht om mee te maken, lijkt 59 tot 86 procent het (heel) erg om mee te maken. Om te bepalen of men een e-mail vertrouwt, kijkt 76 procent naar het mailadres. Ook de schrijfstijl (72%), vraag om persoonlijke financiële gegevens (70%) en vraag om wachtwoorden in te voeren (68%) zijn elementen waar veel Nederlanders phishing aan herkennen.

---

[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 toe
De helft (48%) van de Nederlanders maakt zich geen of weinig zorgen over digitale veiligheid in de privésituatie. Bijna de helft van de Nederlanders (45%) maakt zich hier enige zorgen over. Dat is een toename ten opzichte van 2023 (41%). Over de digitale veiligheid op het werk, maakt driekwart (74%) zich geen zorgen. Meer dan over de eigen digitale veiligheid maakt men zich zorgen over de digitale veiligheid van naasten. Zes op de tien maken zich minimaal enige zorgen hierover (13% (zeer) veel; 47% enige zorgen). Nederlanders onder de 40 jaar maken zich minder zorgen over hun eigen digitale veiligheid in de privésituatie dan oudere Nederlanders. Hogeropgeleiden maken zich relatief veel zorgen over hun naasten.

De voornaamste aspecten waarover men zich zorgen maakt bij de eigen digitale veiligheid zijn, het in de verkeerde handen vallen van gegevens (69%), het kwijtraken van geld (56%) en dat de computer niet meer werkt (48%).

Nederlanders die zich geen of weinig zorgen maken over hun digitale veiligheid in hun privésituatie geven onder meer aan dat ze veel gebruikmaken van twee-staps-inloggen (48%). Ook het updaten van apparaten (45%), het controleren op valse websites/links (44%) en het gebruiken van veel verschillende wachtwoorden (42%) geeft voor een grote groep Nederlanders een veilig gevoel. Minder dan in 2023 noemt men het maken van back-ups als reden om zich veilig te voelen.

Samenvatting | online gedrag

Nederlanders geven zichzelf minder onvoldoendes omgang met online risico's

Nederlanders geven zichzelf een 7,0 voor het omgaan met online risico's. Dit is vergelijkbaar met 2023 (6,9). Zes op de tien Nederlanders geven zichzelf een 6 of een 7, dat is een stijging ten opzichte van 2022. Een derde geeft zichzelf een 8 of hoger. Negen procent geeft zichzelf een onvoldoende. Het aantal onvoldoendes is lager dan een jaar eerder. Mannen geven zichzelf relatief hogere cijfers dan vrouwen (mannen: 7,2; vrouwen: 6,8).

Vrijwel alle Nederlanders maken gebruik van automatische updates (94% doet dit soms of altijd). Ook controleren veel Nederlanders de links waar ze op klikken (91%) en gebruiken ze twee-staps-inloggen (91%), lange wachtwoorden (91%) en virusscanners (88%). Hogeropgeleiden en Nederlanders onder de 40 jaar passen naar verhouding meer verschillende maatregelen toe dan 65-plussers en lageropgeleiden.

Twee derde van de Nederlanders (63%) zegt altijd te controleren of ze op een veilige website zitten. Dit is iets afgenomen ten opzichte van 2023. Positief is dat twee derde van de werkenden zegt geen werkbestanden naar de privémail te sturen. Dit is meer dan in 2023. Zes op de tien Nederlanders schamen zich als ze in phishing trappen. Dit schaamtegevoel speelt minder bij 40-64-jarigen en hogeropgeleiden. Vrijwel alle werkenden waarvoor het van toepassing zou kunnen zijn, verwachten dat ze het aan de ICT-afdeling zouden vertellen als ze een virus downloaden.

Samenvatting | slachtofferschap en aangiftebereidheid

Een op drie Nederlanders doet melding of aangifte na slachtofferschap cybercrime
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 2023. Het meest maakte men (poging tot) phishing mee (55%). De ervaring met (pogingen tot) WhatsAppfraude is toegenomen naar 30 procent en staat op plek twee. Hogeropgeleiden zeggen vaker dan anderen incidenten mee te maken, 65-plussers juist minder.

Wanneer men een voorval meemaakt, zijn de gevolgen in de meeste gevallen niet ernstig of zijn er helemaal geen gevolgen. Ook bij het daadwerkelijk aanklikken van een link met een poging tot cybercrime, zijn de gevolgen voor driekwart (75%) niet ernstig en ervaarde een vijfde (20%) helemaal geen gevolgen. Twee procent ervaarde ernstige gevolgen doordat ze op de phishinglink klikten.

Eén op de vier Nederlanders die privé met cybercrime te maken heeft, doet daar melding of aangifte van. Het meest doet men melding bij de bank (14%). Vijf procent doet aangifte bij de politie en ook 3 procent maakt melding bij de politie. Wanneer men (lichte of ernstige) gevolgen ervaarde van het voorval, doet men vaker melding of aangifte (in 55% van de gevallen) dan wanneer men geen gevolgen ervaart (actie in 25% van de gevallen). Ook Nederlanders ouder dan 65 jaar doen vaker aangifte of melding.

De voornaamste reden om geen actie te ondernemen is dat men weinige schade ondervond (55%). Daaraan gerelateerd vindt 15 procent het te veel moeite en vindt 11 procent het niet zo belangrijk. Een kwart denkt dat het doen van een melding geen zin heeft, omdat men denkt dat 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 (64%).

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. Naarmate de gevolgen van het meegemaakte incident ernstiger zijn, passen meer mensen hun gedrag aan.

Samenvatting | vergelijking uitkomsten onderzoek bedrijfsleven

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

Medewerkers schatten eigen kennis over online veiligheid hoger in dan in 2023

Ruim een kwart (27%) van de medewerkers schat hun eigen kennis over online veiligheid in als (zeer) goed (Nederlanders totaal: 30%). ICT-verantwoordelijken schatten hun kennis hoger in dan andere medewerkers: 53 procent beoordeelt de eigen kennis als (zeer) goed.

ICT-verantwoordelijken schatten risico cybercrime hoger in

ICT-verantwoordelijken zijn beter bekend met de betekenis van de verschillende vormen van cybercrime dan andere medewerkers. Net als bij de gemiddelde Nederlander zijn bij medewerkers hacking en phishing de meest bekende vormen van cybercrime. Het meest denken medewerkers met phishing te maken te kunnen krijgen (36%). Onder ICT-verantwoordelijken is dit aandeel 61 procent. Ook alle andere voorgelegde vormen van cybercrime worden door ICT-verantwoordelijken aannemelijker geacht om op het werk mee te maken te krijgen dan door andere medewerkers.

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

Vier op de tien ICT-verantwoordelijken (40%) maakt zich (zeer) veel of enige zorgen over de eigen online veiligheid in de werksituatie. Voor andere medewerkers is dit percentage significant lager (23%). Wel geven ICT-verantwoordelijken zichzelf een hoger cijfer (7,4) als het gaat om het veilig omgaan met online risico's dan medewerkers (7,0) en de gemiddelde Nederlander (7,0).

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

Twee-staps-inloggen is de meest genomen actie ten behoeve van online veilig gedrag bij bedrijven (medewerkers: 38%). Ook door ICT-verantwoordelijken (54%) en medewerkers van grote bedrijven (50%) wordt deze maatregel het vaakst genoemd. Kleine bedrijven ondernemen minder acties. Bovendien onderneemt een derde van deze bedrijven (32%) geen enkele actie ten behoeve van veilig online gedrag. Wanneer we kijken naar medewerkers, dan geeft 9 procent aan dat er binnen hun bedrijf geen maatregelen worden genomen. Grote bedrijven ondernemen naar verhouding juist meer acties. Bij bedrijven waar afspraken zijn gemaakt over veilig online gedrag, vinden vier op de vijf medewerkers het gemakkelijk om zich aan die afspraken te houden.

Phishing komt het vaakst voor

Zes op de tien (58%) medewerkers ontving in de afgelopen twaalf maanden een phishingmail. Onder ICT-verantwoordelijken was dit zelfs 72 procent. Bij beide groepen is dit de vorm van cybercrime die men het meest meemaakt. Net zoals in 2023 hebben ICT-verantwoordelijken vaker te maken met verschillende voorgelegde vormen van cybercrime dan andere medewerkers.

Meerderheid onderneemt geen actie op cybercrime

De helft (47%) van de 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 dit het vaakst meldt (39%). De belangrijkste redenen om aangifte of melding te doen, zijn het creëren van een veiligere online omgeving (70%) en voorkomen dat de dader opnieuw slachtoffers maakt (46%). Een derde van de medewerkers die geen aangifte doen, geven aan dat ze geen of weinig schade ondervonden. Een vijfde (21%) vindt het (daarnaast) niet zo belangrijk. Achttien procent zegt dat het geen zin heeft om aangifte of melding te doen.

Samenvatting | uitkomsten onderzoek overheid

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

Acht op de tien ambtenaren vinden eigen kennis online veiligheid redelijk tot goed

Acht op de tien ambtenaren is van mening dat de eigen kennis over online veiligheid redelijk tot zeer goed is. Een vijfde vindt het eigen kennisniveau matig of nog minder (16% matig, 2% slecht, 1% zeer slecht). Dat is vergelijkbaar met de vorige meting in 2023. De gemiddelde Nederlander schat de eigen kennis over online veiligheid lager in (22% matig; 5% slecht; 2% zeer slecht).

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

Driekwart van de ambtenaren (76%) maakt zich weinig zorgen over de digitale veiligheid in de werksituatie. Twee procent maakt zich veel zorgen. Dat is vergelijkbaar met een jaar eerder. In het grootbedrijf zijn vergelijkbare cijfers te zien. Gemiddeld geven ambtenaren zichzelf een 7,1 voor het omgaan met online risico's. In het grootbedrijf geeft men een 7,0. Zeven procent van de ambtenaren geeft zichzelf een onvoldoende hiervoor. Het aandeel ambtenaren dat zichzelf een 8 of hoger geeft, is toegenomen ten opzichte van 2023 van 26 naar 37 procent. In het algemeen geeft 33 procent van de Nederlanders zichzelf een 8 of hoger. Negen procent geeft zichzelf een onvoldoende.

Overheid heeft meer maatregelen voor online veilig gedrag dan het grootbedrijf

Twee-staps-inloggen is de meest genomen maatregel voor online veilig gedrag bij de overheid, bij twee derde van de ambtenaren is dat verplicht om toegang te krijgen. Daarnaast hebben ambtenaren vaker adviezen/richtlijnen en/of regels over verschillende zaken dan het grootbedrijf. Zo is er bij de helft van de ambtenaren afspraken gemaakt over het versturen of uitwisselen van bestanden en persoonsgegevens. Elf procent is niet op de hoogte van welke acties er binnen de organisatie zijn voor online veilig gedrag.

De meeste ambtenaren vinden dat ze goede tools en instrumenten krijgen om veilig online gedrag te bevorderen (85%), ook vinden ze het makkelijk om zich aan de afspraken te houden (84%) en zijn de regels voldoende duidelijk (80%). Dit beeld is hetzelfde voor het grootbedrijf. Ambtenaren vinden het goed als collega's hen aanspreken als ze zich niet aan de werkafspraken houden, bij de helft wordt dit ook gedaan.

Vergroten kennis en cyberoefenen dragen bij aan borging gedragsregels

De helft van de ambtenaren ervaart geen belemmeringen bij het borgen van afspraken over veilig online gedrag. Toch ziet driekwart nog wel verbetermogelijkheden. Het meest noemt men het vergroten van kennis binnen de organisatie (43%), cyberoefenen (31%). De voornaamste belemmering die ambtenaren ervaren voor het borgen van afspraken voor online gedrag, is dat er weinig communicatie is hierover (12%). In 2023 werd het niet aansprekend communiceren over online gedrag nog het meest genoemd (toen 16%, nu 7%).

De helft van de ambtenaren meldt een incident bij de ICT-afdeling

Eén op de vijf (22%) ambtenaren heeft de afgelopen twaalf maanden een phishingmail op het werk ontvangen. Zeven procent werd benaderd voor WhatsAppfraude en ook 3 procent werd benaderd op sociale media met een onbekende link. Ambtenaren krijgen minder vaak phishingmails (22%) dan medewerkers van het grootbedrijf (29%).

De helft van de ambtenaren deed geen aangifte of melding van de cybercrime waar ze slachtoffer van werden. Als ze wel een melding deden, deed men dit vaak bij de eigen ICT-afdeling. De voornaamste reden om geen actie te ondernemen is dat er geen of weinig schade ondervonden werd (33%). De belangrijkste redenen om wel aangifte te doen zijn het creëren van een veiligere online omgeving (77%) en voorkomen dat de dader nieuwe slachtoffers maakt (55%).

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 30 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 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 2023. 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 16 jaar en ouder. In totaal werd een representatieve groep van 3.300 Nederlanders uitgenodigd waarvan er 1.336 (40%) meededen met het onderzoek. De dataverzameling vond plaats in het Ipsos I&O Panel[2] van 25 juni tot 9 juli 2024. Niet alle vragen die in dit rapport worden gepresenteerd zijn aan alle 1.336 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

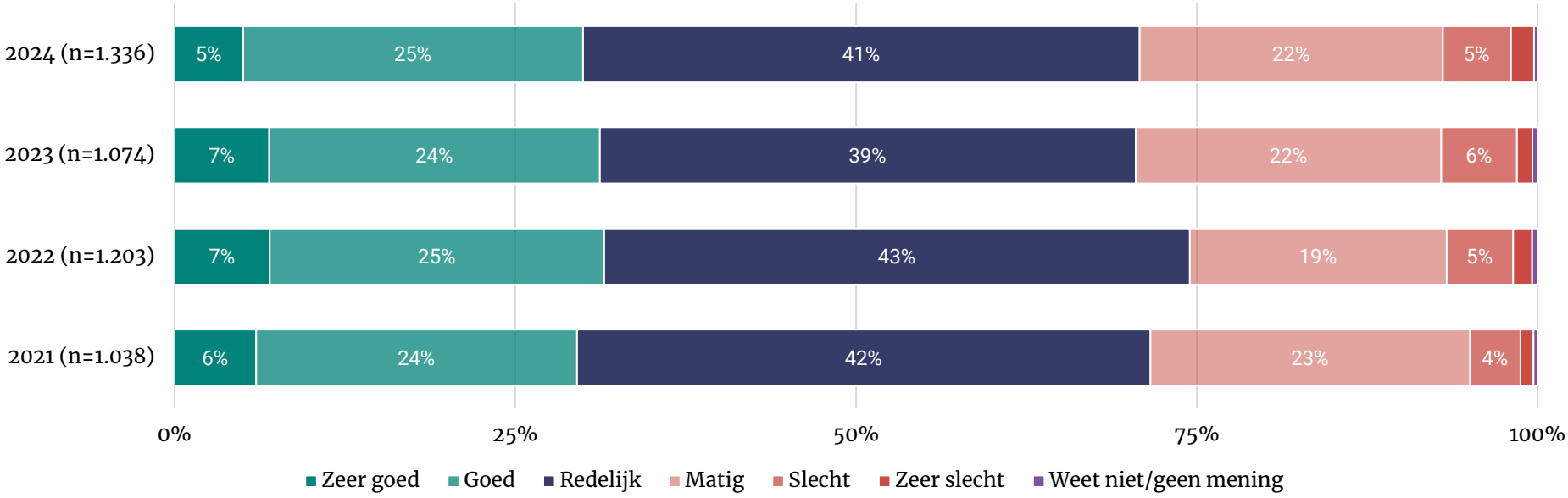
Drie op de tien Nederlanders vinden eigen kennis matig tot zeer slecht

Drie op de tien Nederlanders (30%) beoordelen hun eigen kennis goed tot zeer goed. Ook drie op de tien (29%) vinden dat ze over matige of (zeer) slechte kennis beschikken. De grootste groep (41%) noemt de eigen kennis redelijk.

Vergelijking met eerdere jaren
Het beeld is in vergelijking met 2023 stabiel. In 2022 schatte nog een iets groter deel van de Nederlanders de eigen kennis over digitale veiligheid als redelijk tot zeer goed in.

Resultaten subgroepen
Nederlanders onder de 40 vinden vaker dan anderen dat de eigen kennis over digitale veiligheid goed is. Ook mannen en hogeropgeleiden schatten de eigen kennis over digitale veiligheid vaak hoger in.

Hoe schat u uw eigen kennis over digitale veiligheid in?



Eén op drie Nederlanders deed kennis op via campagnes

- De helft van de werkenden (46%) deed kennis over digitale veiligheid op via de ICT-afdeling op het werk.
- Voor twee op de vijf Nederlanders vormen familie en vrienden een belangrijk kennisbron.
- Een derde noemt campagnes van banken en/of overheid.

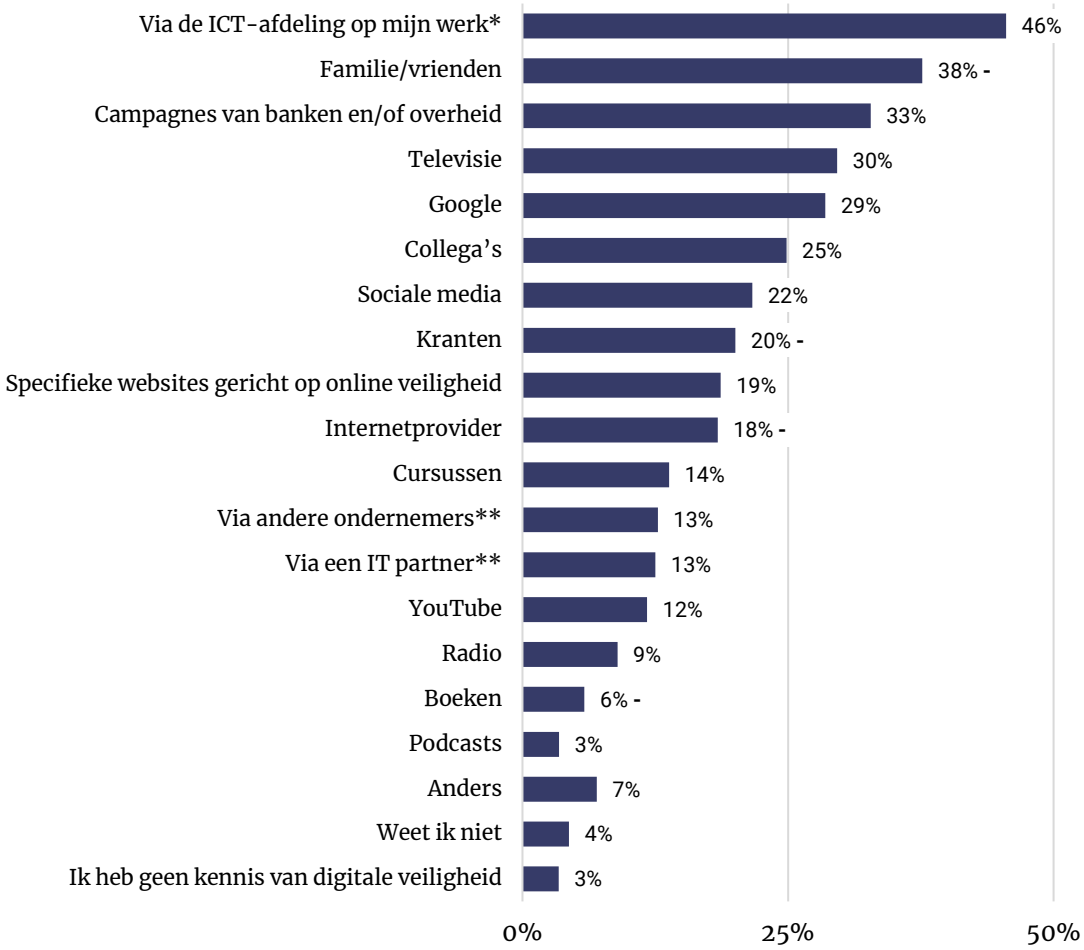
Vergelijking met 2023

- Minder vaak dan in 2023 noemt men familie en vrienden, kranten, internetproviders en boeken als informatiebron.

Resultaten subgroepen

- Er zijn veel verschillen tussen subgroepen.
- Nederlanders onder de 40 jaar hebben vaker kennis via YouTube, podcasts, Google en sociale media.
- Hogeropgeleiden deden de kennis vaker op via cursussen, collega's of de ICT-afdeling op het werk.

Op welke manier heeft u kennis over digitale veiligheid opgedaan? (n=1.336)



* Alleen voorgelegd aan werkenden (n=730)

** Alleen voorgelegd aan ondernemers (n=76).

Phishing en hacking bekendste vormen van cybercrime

- De bekendste vormen van cybercrime zijn hacking (96%) en phishing (94%)
- Vrijwel alle ondernemers zijn bekend met cybercrime waarbij misbruik wordt gemaakt van de bedrijfsnaam.
- CEO-fraude en social engineering (beide 29%) zijn het minst bekend bij Nederlanders. Ook van de werkenden is de minderheid bekend met CEO-fraude (31%).

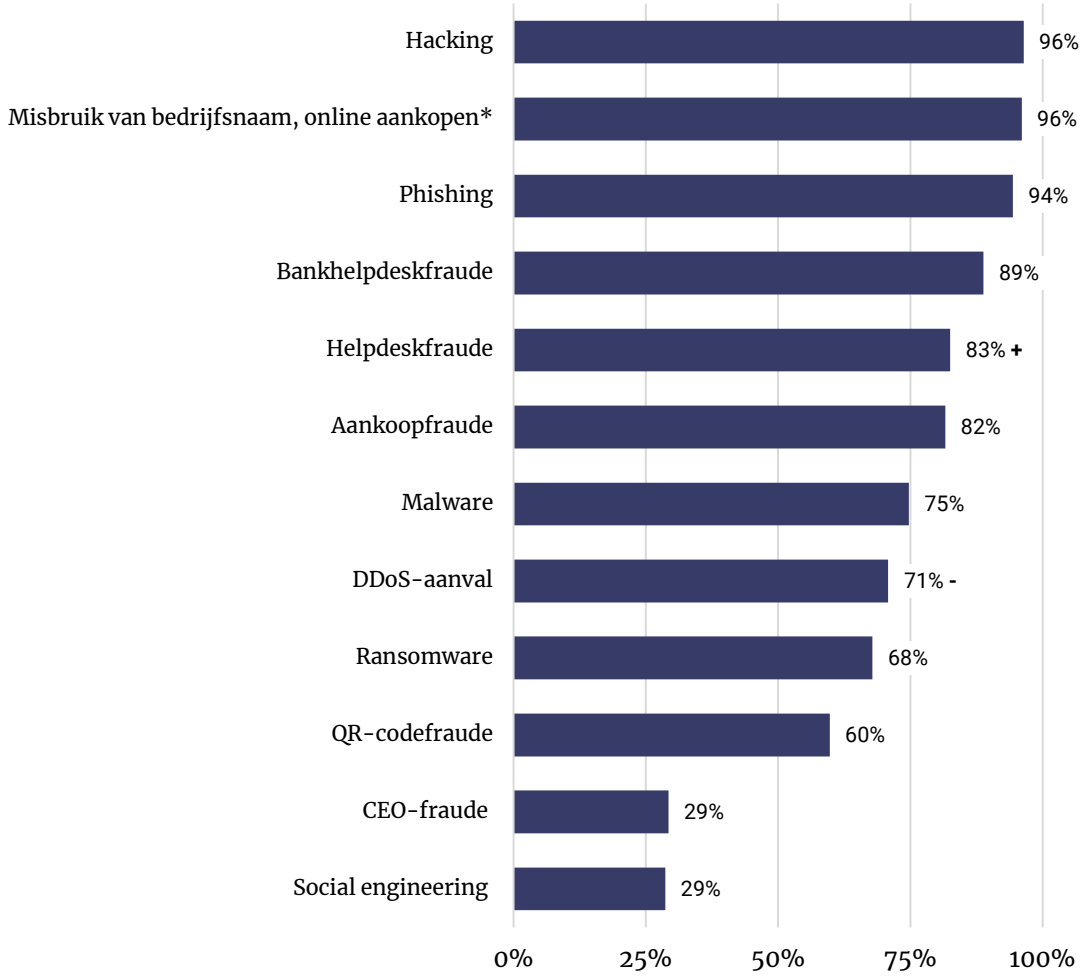
Vergelijking met 2023

- Ten opzichte van 2023 hebben meer Nederlanders gehoord van helpdeskfraude en minder Nederlanders van DDoS-aanvallen.

Resultaten subgroepen

- Bij verschillende vormen van cybercrime geven vrouwen vaker aan er nooit van gehoord te hebben.
- Hogeropgeleiden zijn vaker dan anderen bekend met malware, helpdeskfraude en CEO-fraude.
- 65-plussers hoorden minder vaak dan anderen van social engineering. Nederlanders onder de 40 jaar zijn relatief vaker onbekend met bankhelpdeskfraude.

In welke mate bent u bekend met de onderstaande zaken? (% bekend met; n=1.336)



* Alleen voorgelegd aan ondernemers (n=76).

Een derde van de Nederlanders heeft zelf ervaring met phishing

- Eén op de drie Nederlanders (33%) heeft weleens te maken gehad met phishing. Dat is een groter deel dan bij andere vormen van cybercrime.
- Een vijfde (19%) had te maken met malware en 12 procent met hacking.
- Dit zijn de drie meest voorkomende vormen van cybercrime. Zowel wanneer we kijken naar eigen ervaring als wat men hoort van bekenden.

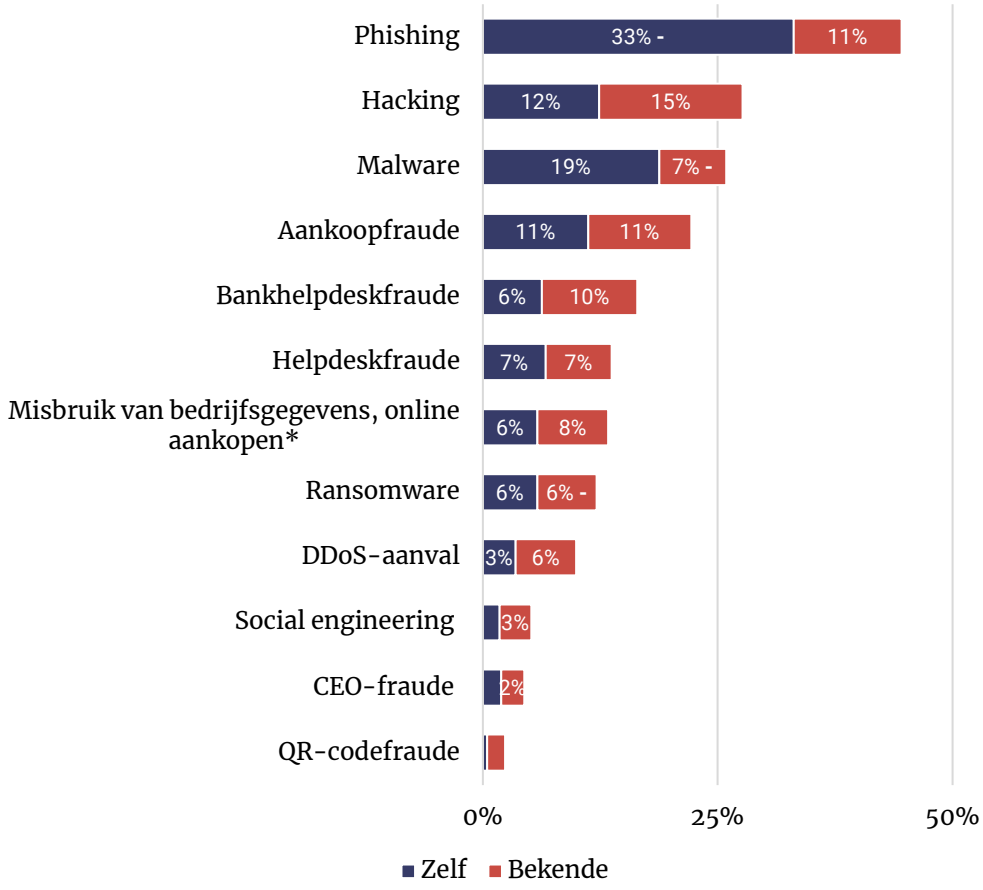
Vergelijking met 2023

- In 2023 gaven meer mensen aan zelf ervaring te hebben met phishing. Ook kenden meer Nederlanders anderen die ervaring hadden met malware en ransomware.

Resultaten subgroepen

- Mannen hebben vaker dan vrouwen persoonlijke ervaringen met Malware, DDoS-aanvallen en ransomware.
- Hogeropgeleiden hebben naar verhouding vaak zelf met phishing en CEO-fraude te maken gehad.
- Nederlanders tot 40 jaar hebben minder vaak zelf ervaring met bankhelpdeskfraude.

In welke mate bent u bekend met de onderstaande zaken? (% meegemaakt; n=1.336)



* Alleen voorgelegd aan ondernemers (n=76).

Driekwart acht ervaring met phishing in privésituatie waarschijnlijk

- De vormen van cybercrime die het meest bekend zijn, zijn ook die vormen die men het meest waarschijnlijk acht om mee te maken.
- Driekwart van de Nederlanders die bekend zijn met phishing, denken dit privé mee te kunnen maken. Hetzelfde geldt voor hacking.
- Minder Nederlanders (26% van degenen die het kennen) verwachten privé slachtoffer te worden van een DDoS-aanval.

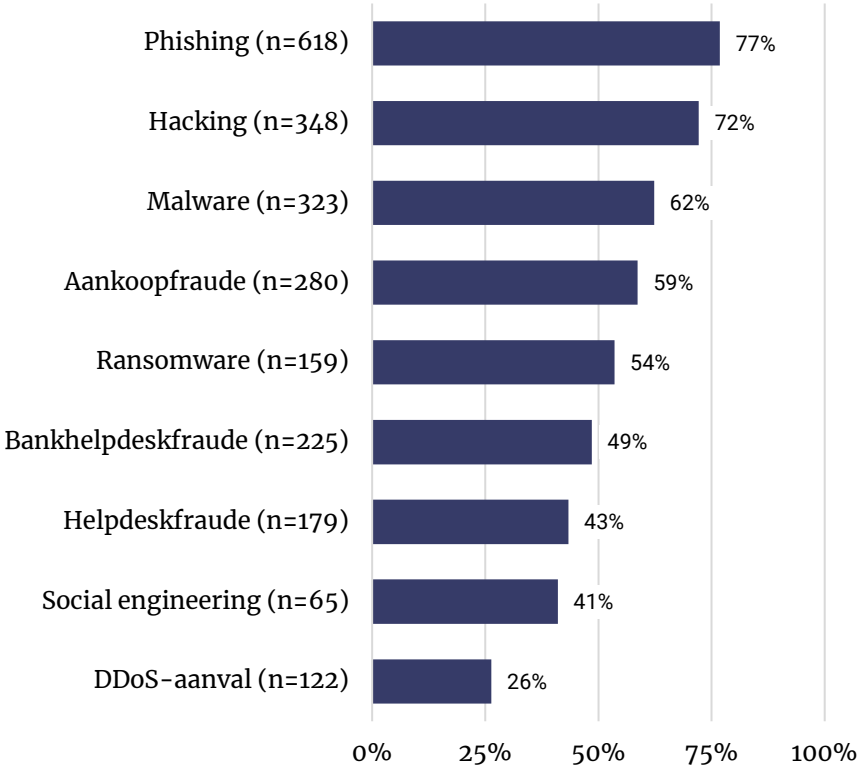
Vergelijking met 2023

- In 2023 is de vraag ook voorgelegd aan mensen die zeiden weleens van de vorm van cybercrime gehoord te hebben, maar niet exact te weten wat het in hield. De resultaten zijn daardoor niet volledig vergelijkbaar.
- Wel stond destijds phishing bovenaan, gevolgd door malware en hacking.

Resultaten subgroepen

- Lageropgeleiden en 65-plussers achten het van verschillende vormen van cybercrime minder waarschijnlijk om hier in de privésituatie mee te maken te krijgen.
- Hogeropgeleiden vinden het vaker realistisch om privé met malware en social engineering in aanraking te komen.

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*)



* Door een fout in het vragenlijstscript zijn sommige minder vaak voorgelegd. Dit heeft geen invloed op de onderzoeksresultaten.

Hacking, bankhelpdeskfraude en aankoopfraude meest gevreesd

- Van alle voorvallen die men in de privésituatie waarschijnlijk acht om mee te maken, lijkt een meerderheid het (heel) erg als dit het geval is.
- Dat geldt het meest voor hacking, bankhelpdeskfraude en aankoopfraude.
- Relatief gezien zouden minder mensen het erg vinden om slachtoffer te worden van malware: zes op de tien mensen die dit kennen, lijkt het erg hier mee te maken te krijgen.

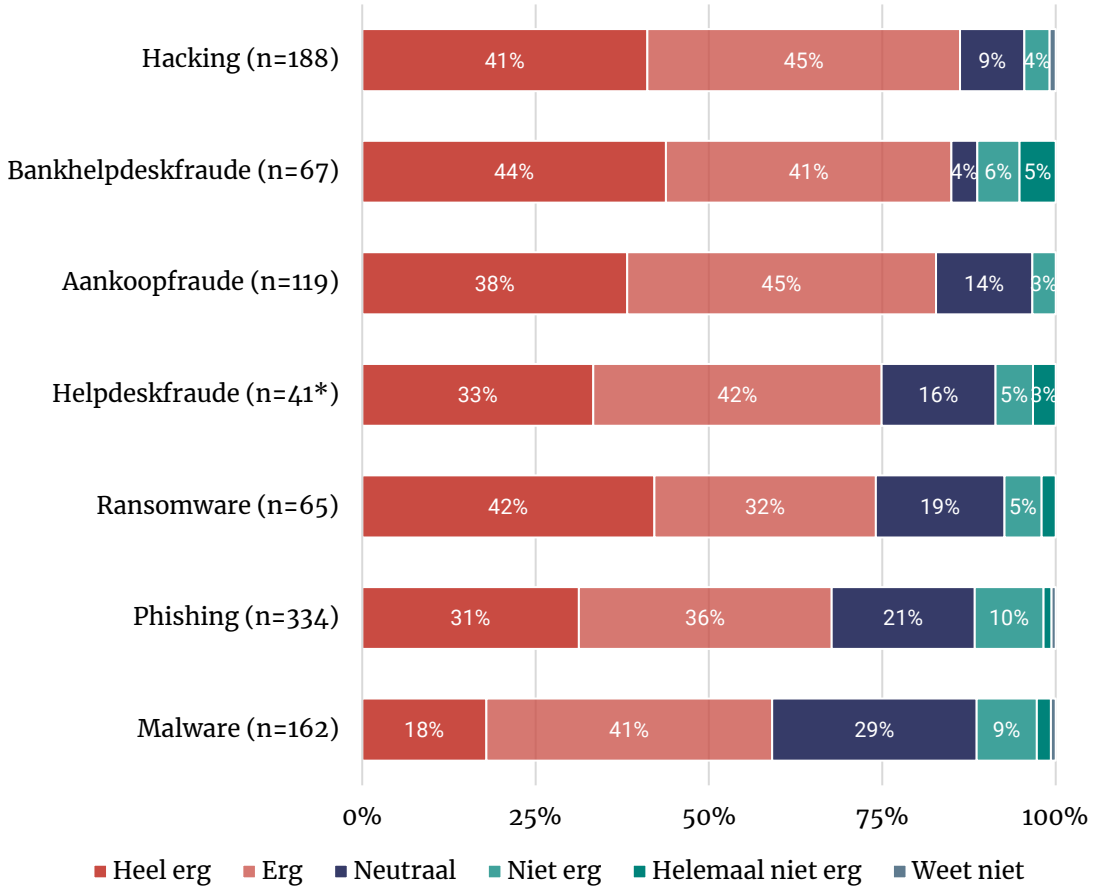
Vergelijking met 2023

- Deze vraag is in 2024 voor het eerst voorgelegd. Vergelijking met 2023 is daarom niet mogelijk.

Resultaten subgroepen

- Het lijkt vrouwen erger dan mannen om met malware en phishing te maken te krijgen.

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*)



*Laag aantal: indicatieve uitkomsten.

**Door een fout in het vragenlijstscript zijn sommige minder vaak voorgelegd. Dit heeft geen invloed op de onderzoeksresultaten.

Mailadres, schrijfstijl en geldverzoek wekken argwaan bij phishing

- Om phishing te herkennen kijkt men vooral naar het e-mailadres (76%) en de schrijfstijl (72%).
- Zeven op de tien Nederlanders krijgen argwaan als gevraagd wordt om geld of persoonlijke financiële gegevens (70%) of om het wachtwoord in te voeren (68%).

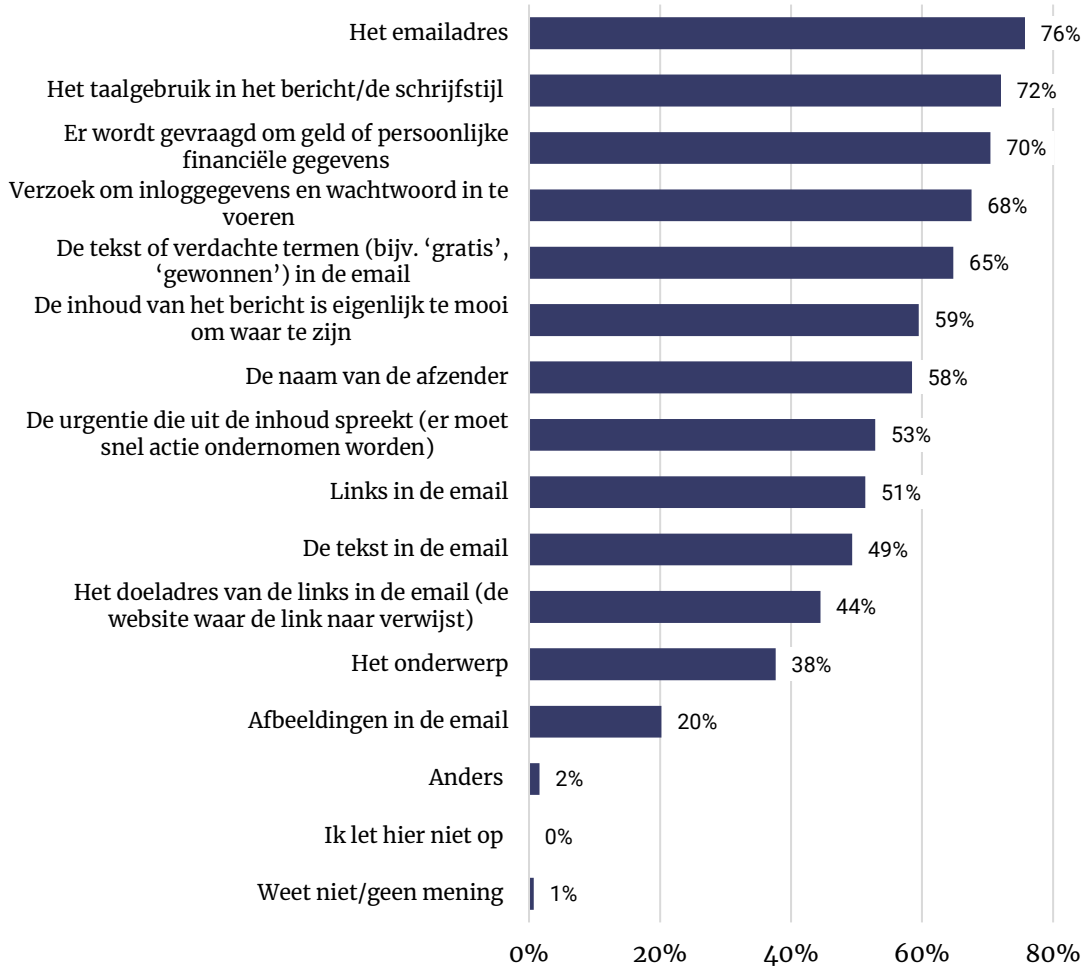
Vergelijking met 2023

- De antwoordcategorieën zijn toegankelijker geformuleerd dan in 2023 en daardoor niet exact heftzelfde. Maar ook destijds keek men vooral naar of er om gegevens werd gevraagd, de afzender, de schrijfstijl en het verzoek om geld over te maken.

Resultaten subgroepen

- Nederlanders onder de 40 jaar noemen relatief vaker het mailadres, de naam, afbeeldingen en links in de mail.
- Lageropgeleiden noemen verschillende aspecten minder dan anderen.

Stel dat u een email krijgt. Op welke aspecten let u om te bepalen of de mail te vertrouwen is of niet?
(% genoemd; n=675*)



*De helft van de steekproef kon maximaal 5 antwoorden geven. De percentages zijn anders, maar de uitkomsten vergelijkbaar.

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

- De helft van de Nederlanders kijkt bij het herkennen van phishing via telefoon of er om financiële gegevens (53%) of om het overmaken van geld (48%) gevraagd wordt.
- Bijna net zo vaak herkent men phishing doordat om inloggegevens en wachtwoord gevraagd worden (44%).

Vergelijking met 2023

- In 2024 geven meer mensen dan in 2023 aan telefonische phishing te herkennen door het verzoek om inloggegevens en wachtwoord in te voeren.
- Destijds gaf men wel vaker aan alle ongevraagde berichten weg te gooien.

Resultaten subgroepen

- Nederlanders onder de 40 kijken meer naar de naam, het nummer, de profielfoto en het taalgebruik. Ze kijken minder naar het verzoek om wachtwoorden en de opmaak van het bericht.
- Hogeropgeleiden kijken vaker naar het taalgebruik, maar minder of ‘gratis’ terugkomt.

Naar welke onderdelen van een bericht kijkt u vooral om phishing via sms of WhatsApp te herkennen?
(% genoemd; n=1.336) (maximaal 5 antwoorden)

4. Zorgen om digitale veiligheid

Iets meer zorgen om digitale veiligheid in privésituatie dan in 2023

- De meeste Nederlanders hebben niet veel zorgen over hun digitale veiligheid. Zeven procent zegt zich (zeer) veel zorgen hierover te maken in de privésituatie.
- Voor de werksituatie is dat 1 procent.
- De helft heeft weinig tot geen zorgen over de digitale veiligheid privé en op het werk is driekwart (nagenoeg) zorgenvrij.

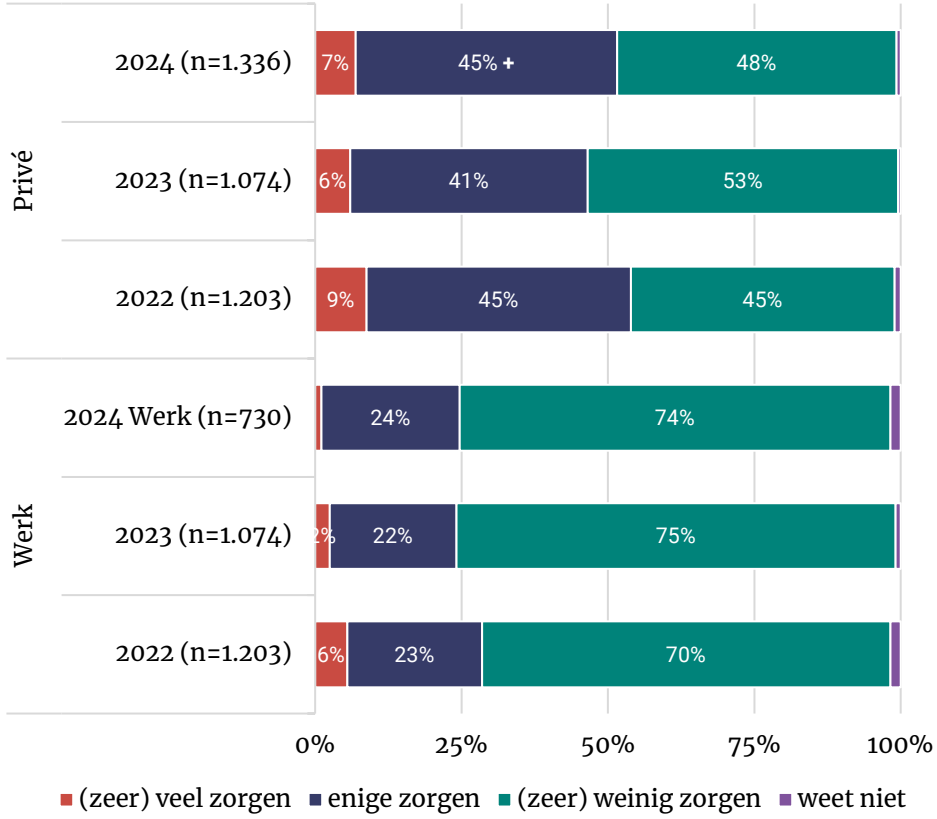
Vergelijking met 2023

- De zorgen zijn iets toegenomen ten opzichte van 2023. Nu geven Nederlanders iets vaker aan zich enige zorgen te maken over de eigen digitale veiligheid in de privésituatie.

Resultaten subgroepen

- Privé maken Nederlanders onder de 40 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 weinig verschillen.

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



Nederlanders maken zich vooral zorgen om hun naasten

- Nederlanders maken zich meer zorgen om de digitale veiligheid van hun naasten dan die van henzelf.
- De helft heeft enige zorgen en 13 procent (zeer) veel zorgen.
- Een derde maakt zich geen zorgen over de digitale veiligheid van naasten.

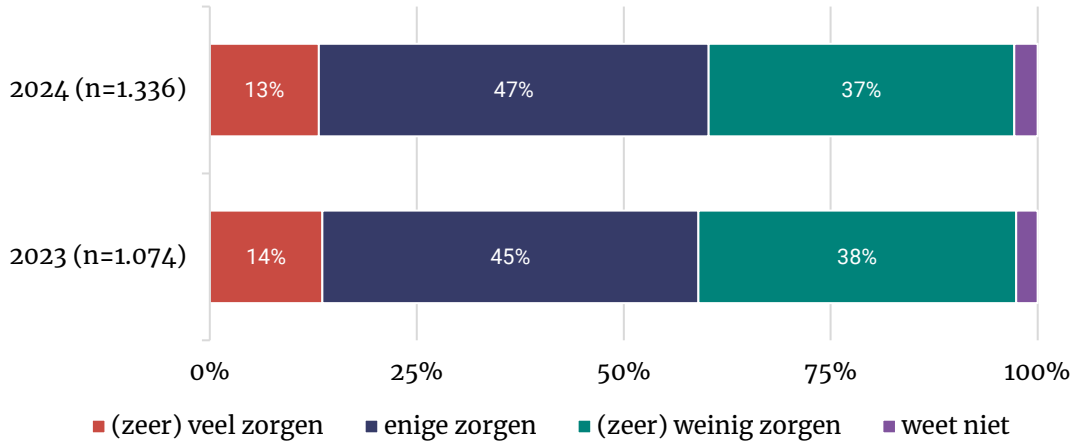
Vergelijking met 2023

- Men maakt zich evenveel zorgen over de digitale veiligheid van naasten als een jaar eerder.

Resultaten subgroepen

- Hogeropgeleiden maken zich meer zorgen om de digitale veiligheid van hun naasten dan andere Nederlanders.

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



Meeste zorgen in privésituatie over kwijtraken gegevens en geld

- Zeven op de tien Nederlanders die zich zorgen maken over de eigen digitale veiligheid, zijn bang dat hun gegevens in de verkeerde handen vallen.
- De helft (56%) is bang om geld kwijt te raken of dat de computer niet meer werkt (48%).
- Vier procent maakte eerder cybercrime mee en maakt zich daarom nu zorgen.

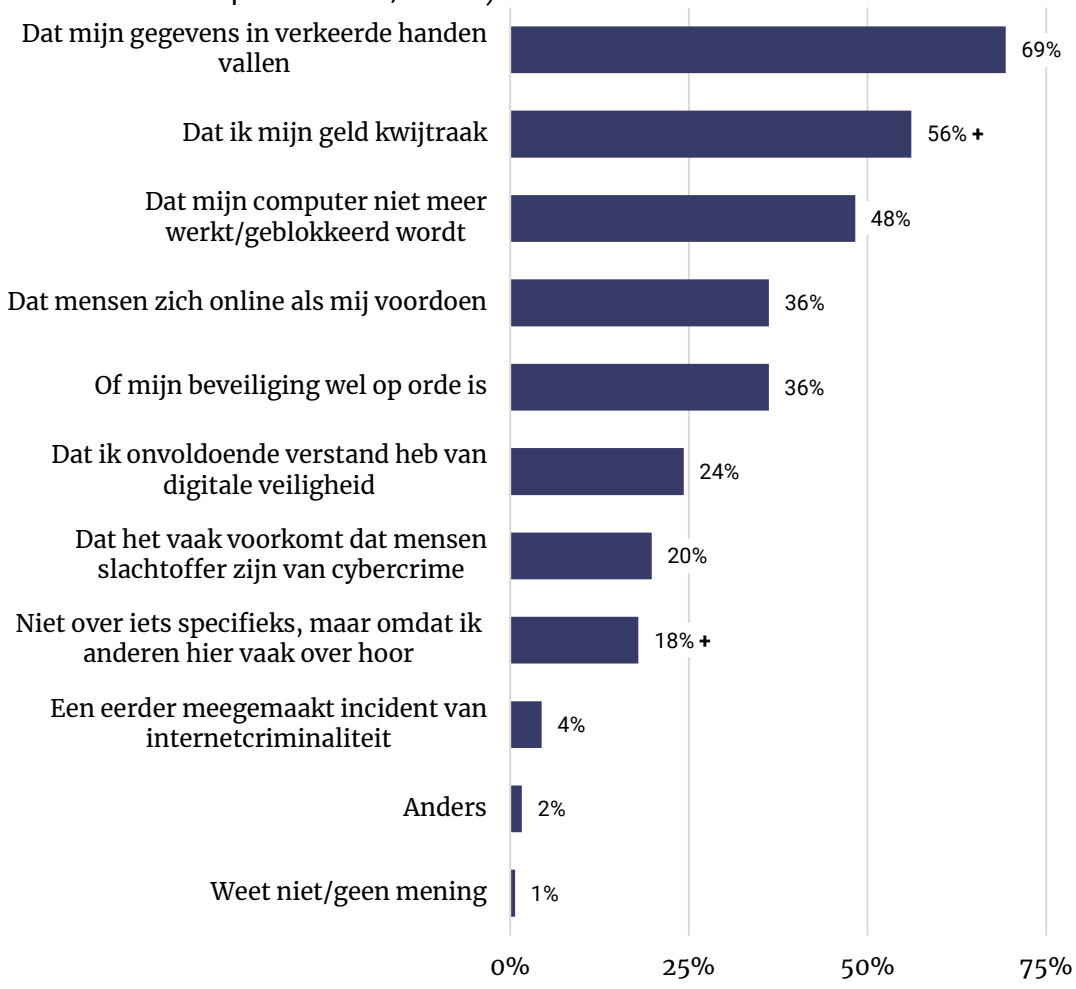
Vergelijking met 2023

- Meer dan 2023 is het kwijtraken van geld een reden tot bezorgdheid.
- Ook is men vaker bezorgd omdat men anderen over digitale (on)veiligheid hoort.

Resultaten subgroepen

- Nederlanders onder de 40 jaar maken zich minder zorgen dat hun computer geblokkeerd wordt en niet meer werkt.
- Mannen maken zich hier meer zorgen over dan vrouwen.
- Vrouwen zijn vaker bang dat gegevens in verkeerde handen vallen of dat 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=727)



Twee-staps-inloggen zorgt 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 gebruik van twee-staps-inloggen als reden om zich veilig te voelen.
- Andere veelgenoemde redenen zijn het updaten van apparaten (45%), controleren op valse links en websites (44%) en het gebruik van verschillende wachtwoorden (42%).

Vergelijking met 2023

- Men noemt minder vaak zich veilig te voelen vanwege regelmatig maken van back-ups.

Resultaten subgroepen

- Mannen noemen verschillende veiligheidsmaatregelen zoals back-ups en twee-staps-inloggen vaker.
- Lageropgeleiden voelen zich minder vaak veilig omdat ze twee-staps-inloggen gebruiken.
- Nederlanders onder 40 jaar noemen minder vaak het gebruik van virusscanners als reden.

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=528)

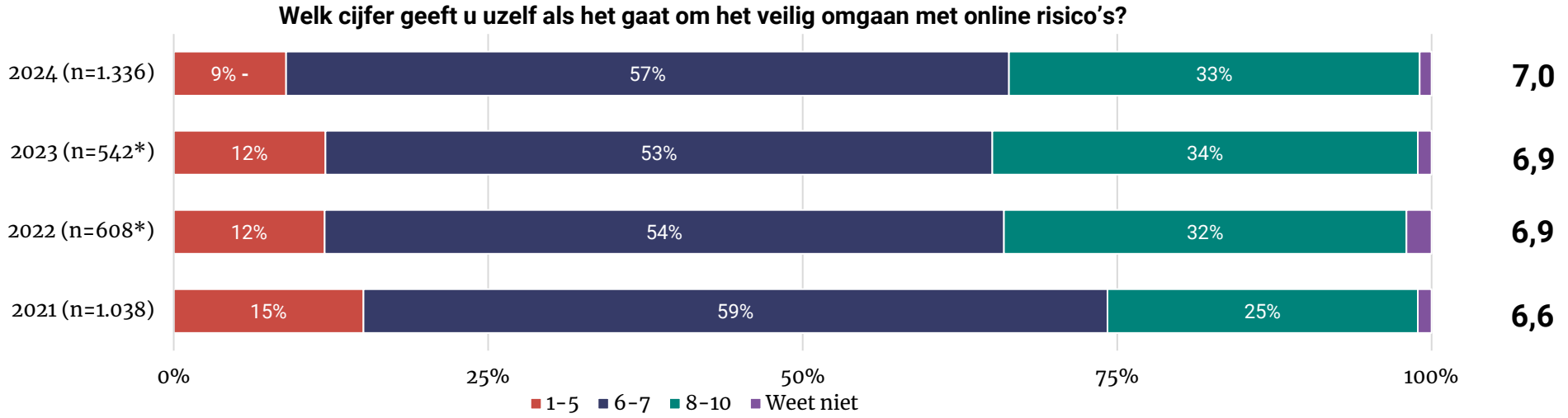
5. Online gedrag

Nederlanders positiever over hun omgang met online risico's

Zes op de tien Nederlanders geven zichzelf een 6 of een 7 voor de omgang met online risico's. Een derde beoordeelt de eigen omgang als goed (8 of hoger). Negen procent geeft zichzelf een onvoldoende. Het gemiddelde oordeel is een 7,0.

Vergelijking met eerdere jaren
Minder Nederlanders geven zichzelf een onvoldoende dan in 2023. Ook in eerdere jaren gaf men zich vaker onvoldoendes. Na 2021 valt op dat meer mensen vinden dat ze goed omgaan met online risico's.

Resultaten subgroepen
Mannen geven zichzelf gemiddeld een 7,2 voor de eigen omgang met online risico's en vrouwen een 6,8. Verder zijn er geen verschillen tussen subgroepen.



*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 voor de jaren 2023 en 2022 alleen de uitkomsten weergegeven voor de vraag op de "oude" plek.

Toelichtingen bij cijfer omgang online risico's

Cijfer 1-5 (9%)

- *"Voor bijna alles hetzelfde wachtwoord. Hekel hebben aan 2 staps verificatie. Niet weten hoe je links kunt herkennen die virussen of malware met zich meedragen enzovoort enzovoort."*
- *"Volgens mijn kinderen trap ik er recht in, en de keren dat ik zonder te weten getest werd, was dat ook echt zo."*

Cijfer 9-10 (33%)

- *"Genoeg kennis om verantwoordelijkheid met data om te gaan."*
- *"Ik overleg voordat ik actie onderneem."*
- *"Ik heb alles redelijk onder controle, maar toch kan het je eens gebeuren."*
- *"Ik heb technische informatica en bedrijfskunde gestudeerd met specialisatie in cybersecurity."*
- *"Ik ben volledig beschermd via hardware firewall software antivirus, ook eenieder in mijn gezin hou ik in de gaten."*
- *"Leest eerst heel goed, klikt nergens zomaar op."*

Cijfer 6-7 (57%)

- *"Ik doe wel m'n best maar ik wil ook niet m'n leven er door laten leiden."*
- *"Ik denk voldoende op de hoogte te zijn, maar zal waarschijnlijk net als zovelen toch de fout ingaan ben ik bang."*
- *"Ik heb niet zoveel verstand van de manier waarop je bijv. je laptop / mail kunt beveiligen."*
- *"Ik gebruik veel ongeveer dezelfde wachtwoorden en ben niet altijd even voorzichtig met welke websites ik gebruik."*
- *"Ik probeer goed op te letten en heb veiligheidssoftware."*
- *"Ik waan mij veilig, maar sluit niet uit dat ik ooit een fout maak(leeftijd/vergeetachtig)."*
- *"Ben er niet bewust mee bezig. Heb geen computer. Onze telefoon is onze computer. Houd wel de noodzakelijke updates bij."*

Automatische updates en twee-staps-inloggen veel toegepast (1)

- Bijna alle Nederlanders (94%) doen automatische updates.
- Negen op de tien Nederlanders controleren links voordat ze er op klikken (91%), gebruiken twee-staps-inloggen (91%), lange wachtwoorden (90%) en virusscanners (88%).
- Web tracking blockers (42% kent dit niet), passkeys (42%) en open source hardware en software (45%) zijn bij veel Nederlanders niet bekend (zie ook volgende pagina).

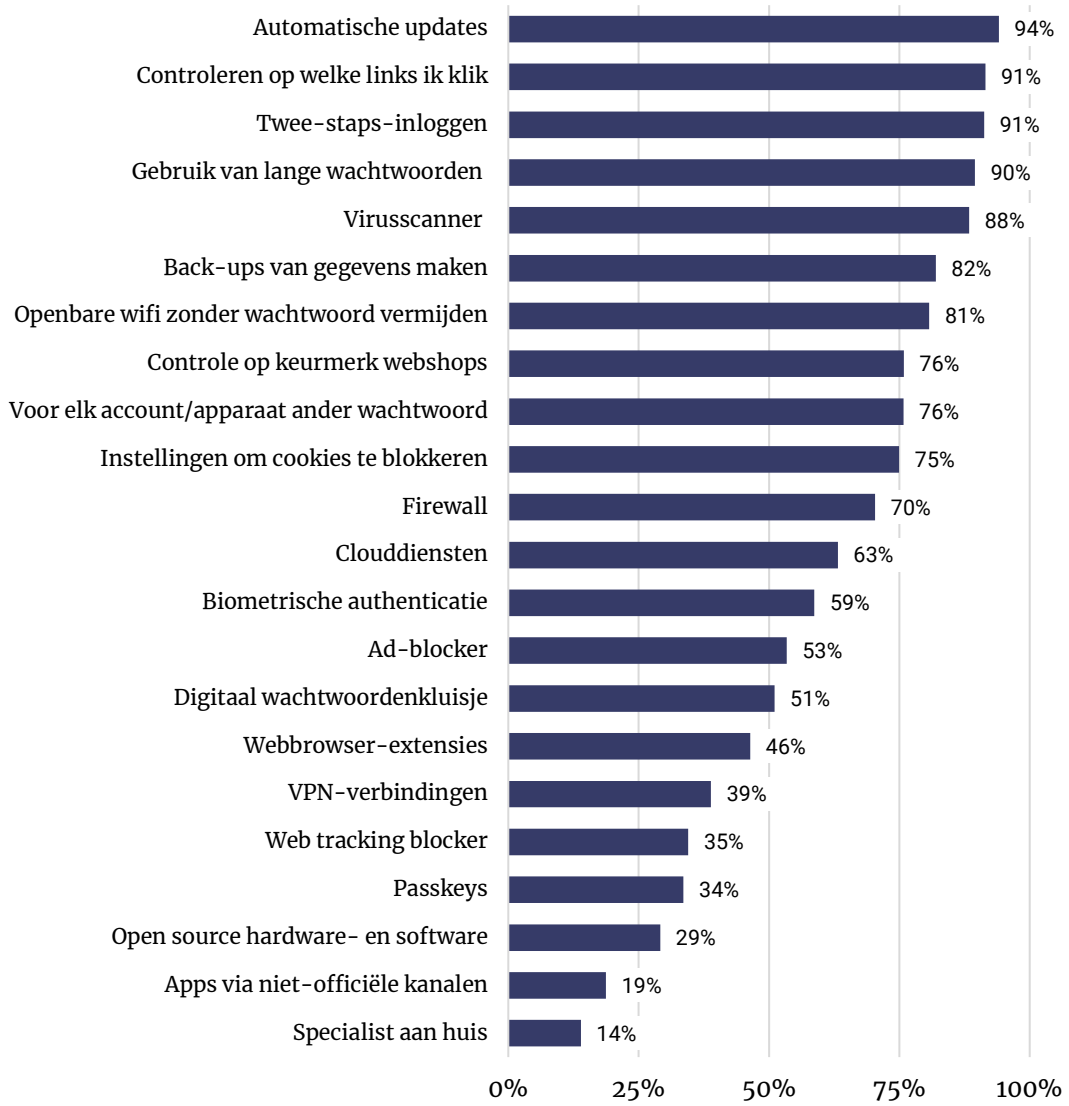
Vergelijking met 2023

- In 2023 was de vraagstelling iets anders, maar ook destijds zei een ruime meerderheid twee-staps-inloggen en virusscanners te gebruiken en automatische updates toe te passen.

Resultaten subgroepen

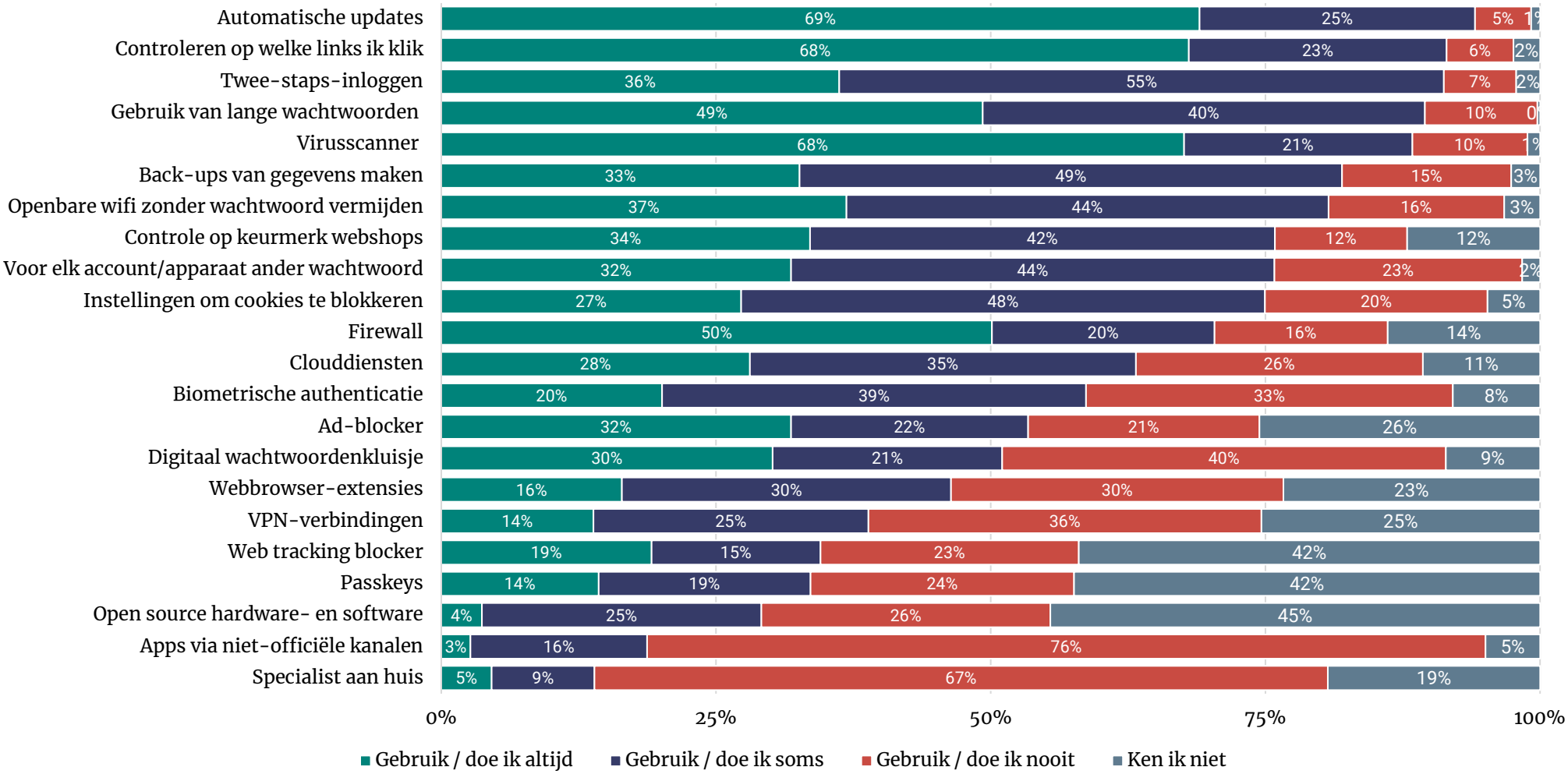
- Verschillende maatregelen worden meer door hogeropgeleiden en Nederlanders onder de 40 jaar gebruikt.
- 65-plussers en lageropgeleiden nemen naar verhouding minder maatregelen.

Welke van onderstaande zaken gebruikt u of past u toe?
(% doe ik altijd/soms; men kreeg willekeurig de helft van de opties; nmin=678)



Automatische updates en twee-staps-inloggen veel toegepast (2)

Welke van onderstaande zaken gebruikt u of past u toe?
(men kreeg willekeurig de helft van de opties; nmin=678)



Meerderheid Nederlanders controleert of ze op veilige website zitten

- De meeste Nederlanders (60%) controleren meestal of altijd of er een slotje bij de website staat.
- Men maakt vaker niet (53%) dan wel (13%) gebruik van een extern opslagapparaat dat continu online is.

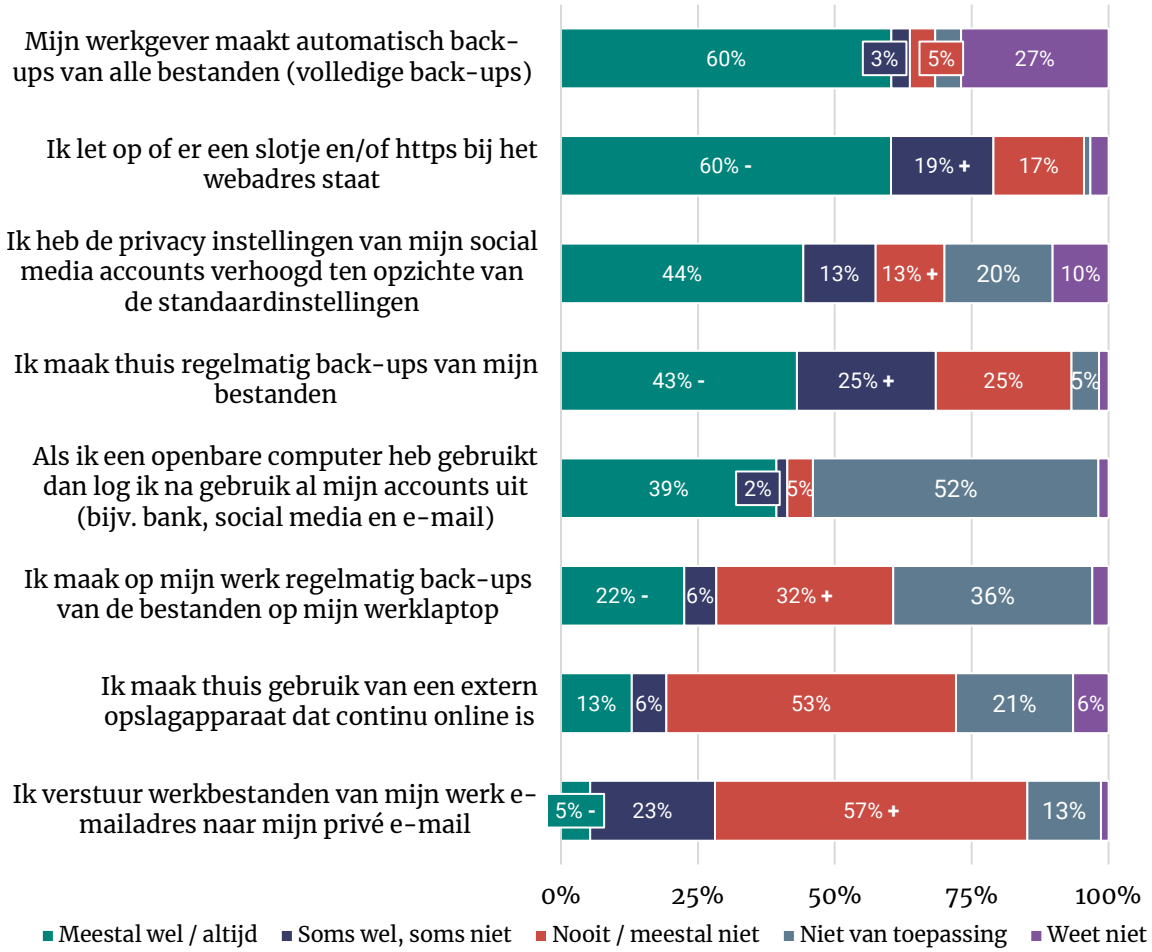
Vergelijking met 2023

- In vergelijking met de vorige meting, controleert men minder vaak op de veiligheid van websites. Ook past men minder de privacy-instellingen van sociale media aan en maakt men minder back-ups.
- Positief is dat men ook minder werkbestanden naar de privémail verstuurt.

Resultaten subgroepen

- 65-plussers loggen minder vaak uit op een openbare computer.
- Nederlanders onder de 40 maken minder regelmatig back-ups, maar hebben wel vaker de privacy-instellingen van sociale media-accounts aangepast.

In hoeverre zijn de volgende uitspraken op u van toepassing?*
(n=1.336; vragen over werk zijn alleen gesteld aan werkenden; n=730)



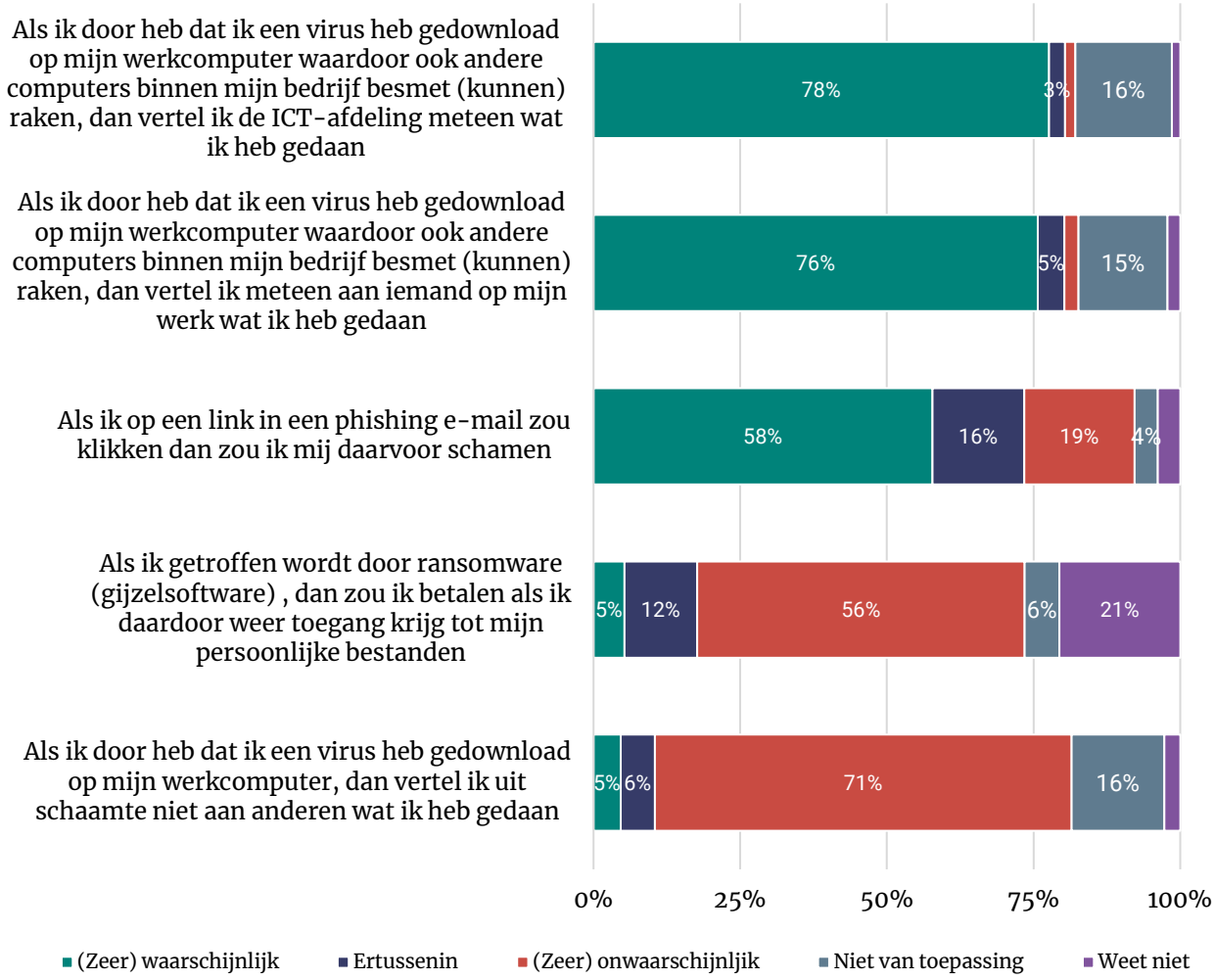
Zes op de tien zouden zich schamen als ze in phishing trappen

- Zes op de tien Nederlanders (58%) zouden zich waarschijnlijk schamen als ze in phishing trappen.
- Toch denkt driekwart van de werkenden (78%) het aan de ICT-afdeling en anderen (71%) te vertellen wanneer ze een virus downloaden.
- Vrijwel niemand (1 tot 2%) verwacht het niet te vertellen.

Vergelijking met 2023
- De vraagstelling is iets aangepast ten opzichte van 2023, maar het algemene beeld is vergelijkbaar.

Resultaten subgroepen
- Nederlanders tussen de 40 en 65 jaar verwachten vaker dan ouderen en jongeren zich niet te schamen als ze in phishing trappen
- Ook hogeropgeleiden denken zich minder te schamen hiervoor.

In hoeverre zijn de volgende uitspraken op u van toepassing?
(n=1.336; vragen over werk zijn alleen gesteld aan werkenden; n=730)



6. Slachtofferschap en aangiftebereidheid

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

- Driekwart (72%) van de Nederlanders maakte in de twaalf maanden voorafgaand aan het onderzoek één of meerdere voorvallen van cybercrime mee.
- Het meest meegemaakt voorval is net als in eerdere jaren phishing (55%) gevolgd door WhatsAppfraude (30%).

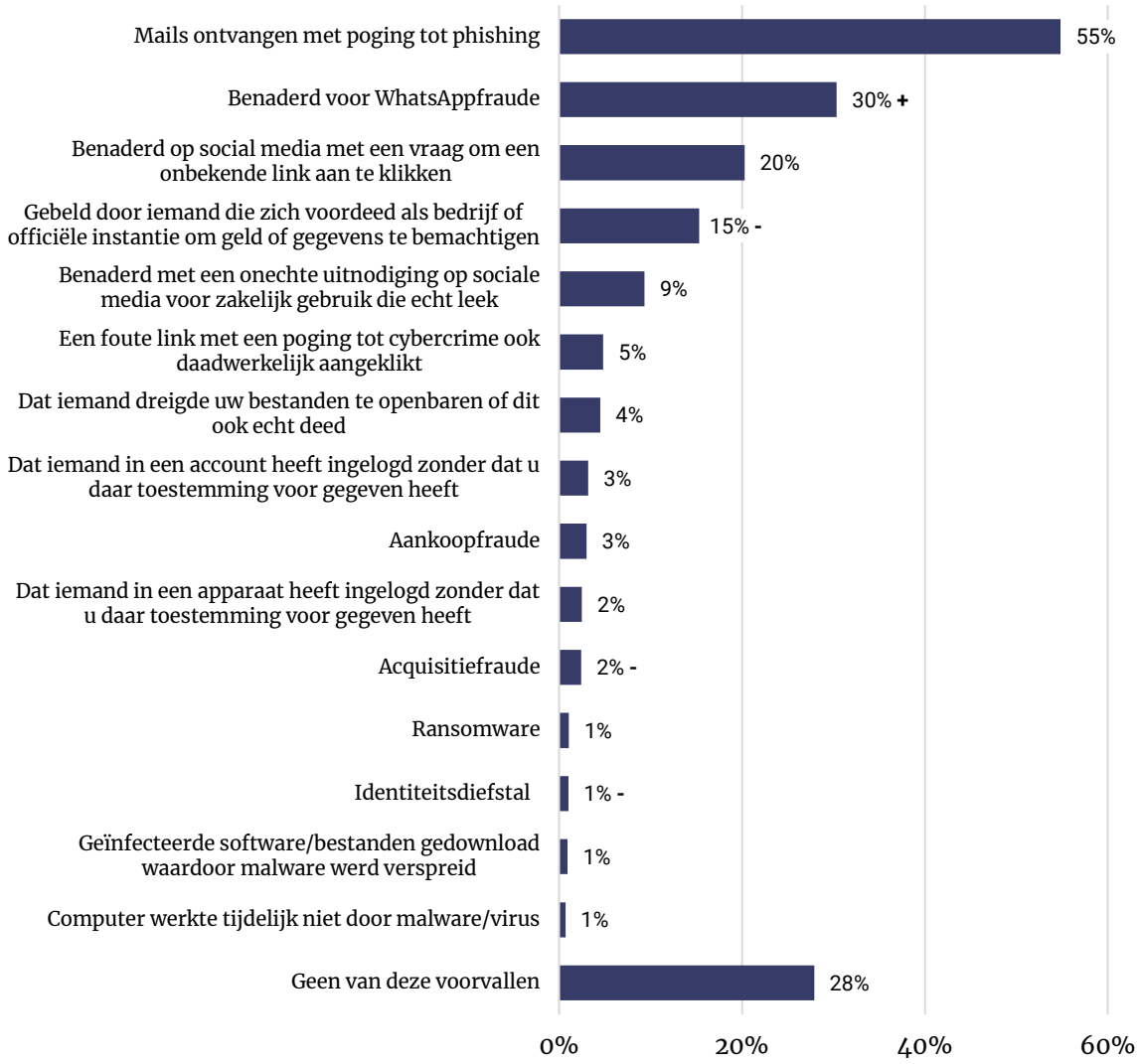
Vergelijking met 2023

- WhatsAppfraude komt nu meer voor dan een jaar eerder.
- Minder mensen maakten spoofing (zogenaamd gebeld door een bedrijf of officiële instantie), acquisitiefraude en identiteitsdiefstal mee dan een jaar eerder.

Resultaten subgroepen

- 65-plussers maken minder voorvallen dan gemiddeld mee. Ze zeggen vooral minder te maken te hebben met phishing.
- Hogeropgeleiden maken meer voorvallen mee, vooral phishing.
- Nederlanders tussen de 40 en 65 jaar hebben relatief vaak WhatsAppfraude meegemaakt.

Heeft u in de afgelopen twaalf maanden zelf weleens te maken gehad met één van de onderstaande voorvallen? (% genoemd; n=1.336)



Gevolgen aankoopfraude in één op tien gevallen ernstig

- In de meerderheid van de gevallen ervaart men geen ernstige gevolgen wanneer men te maken krijgt met cybercrime.
- Vooral bij aankoopfraude (11%) en wanneer anderen zonder toestemming inloggen in accounts (9%) zijn de gevolgen relatief vaak ernstig.
- Ook bij het aanklikken van een foute link, loopt het in veel gevallen met een sisser af: 2% ervaart grote schade.

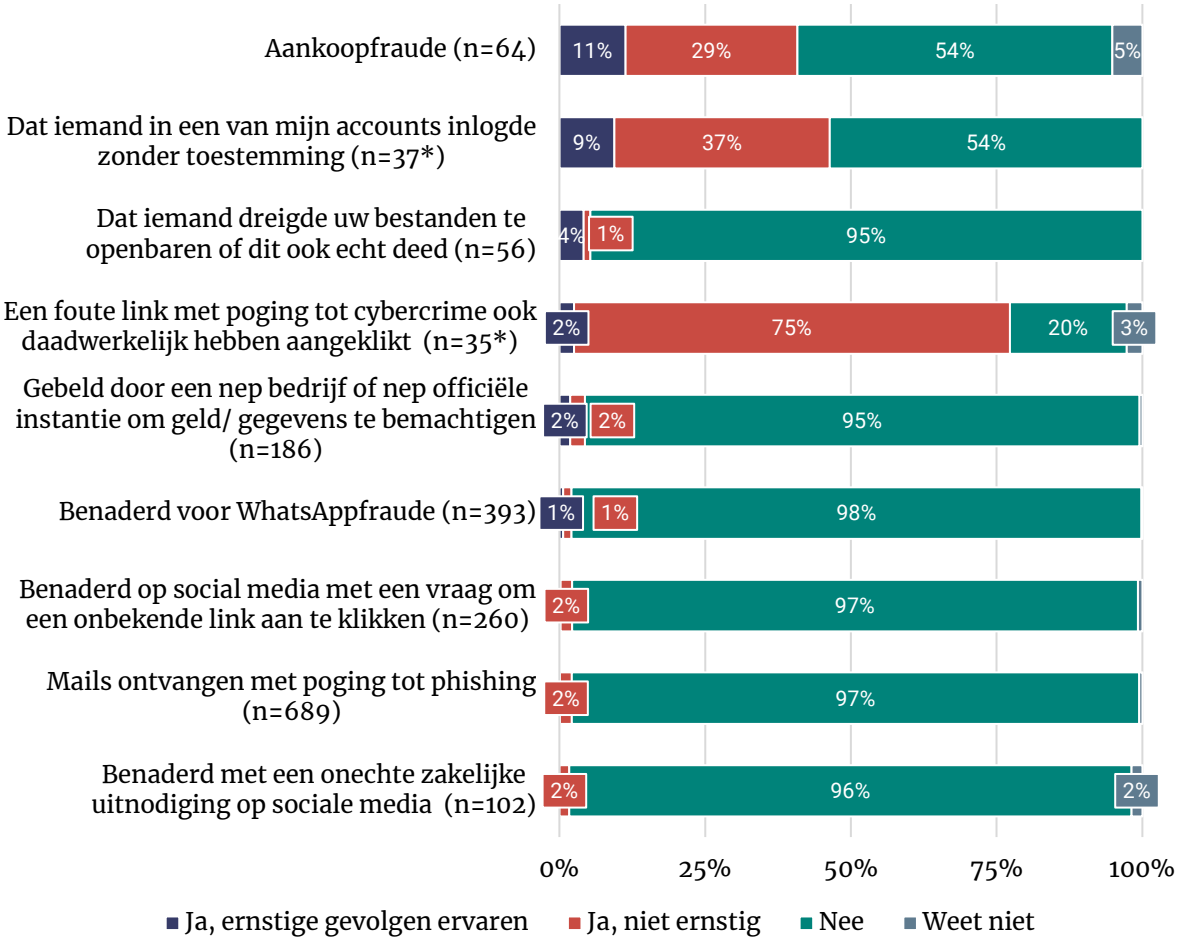
Vergelijking met 2023

- Deze vraag is in 2023 niet gesteld en daarom is vergelijking niet mogelijk.

Resultaten subgroepen

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

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



*Laag aantal: indicatieve uitkomsten.

Driekwart doet geen melding of aangifte van cybercrime in privésituatie

- Driekwart van de Nederlanders die een voorval van cybercrime meemaakten in de privésituatie deden hier geen aangifte of melding van.
- Wanneer men dat wel doet, is dat vooral bij de bank (10%), Fraudehelpdesk (8%) of bij de instantie waar het voorval gebeurde.
- Vijf procent doet aangifte bij de politie en 3 procent maakt een melding aldaar.

Vergelijking met 2023

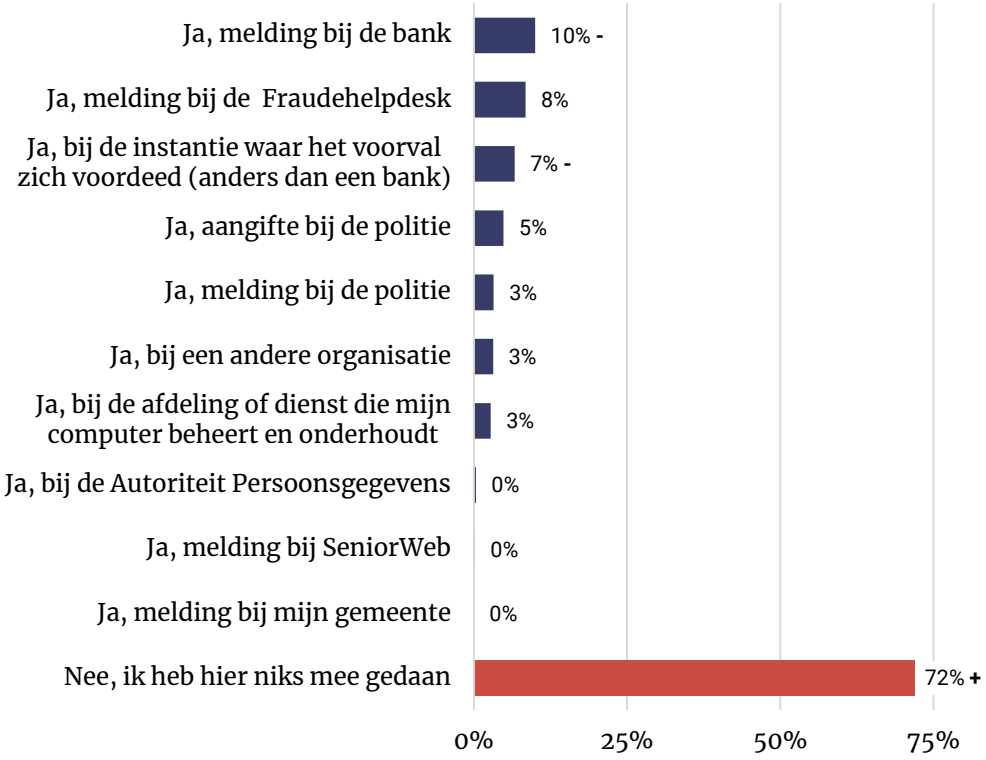
- Men doet minder vaak iets met het meegemaakte voorval dan in 2023.
- Er worden vooral minder meldingen bij de bank en de instantie gedaan waar het voorval zich voordeed.

Resultaten subgroepen

- Wanneer men lichte of ernstige gevolgen van het voorval heeft ervaren, doet men vaker aangifte of melding. Men gaat dan vaker naar de politie en de bank.
- 65-plussers doen vaker iets met het meegemaakte incident. Zo doen ze vaker melding bij de bank dan andere leeftijdsgroepen.
- Ook lageropgeleiden maken relatief vaak melding bij de bank.

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=951)



Vaak geen aangifte of melding vanwege beperkte gevolgen

- De voornaamste reden om geen aangifte of melding te doen is dat men weinig schade ondervond (55%).
- Een kwart denkt dat er niet veel met de melding of aangifte gedaan wordt (25%).

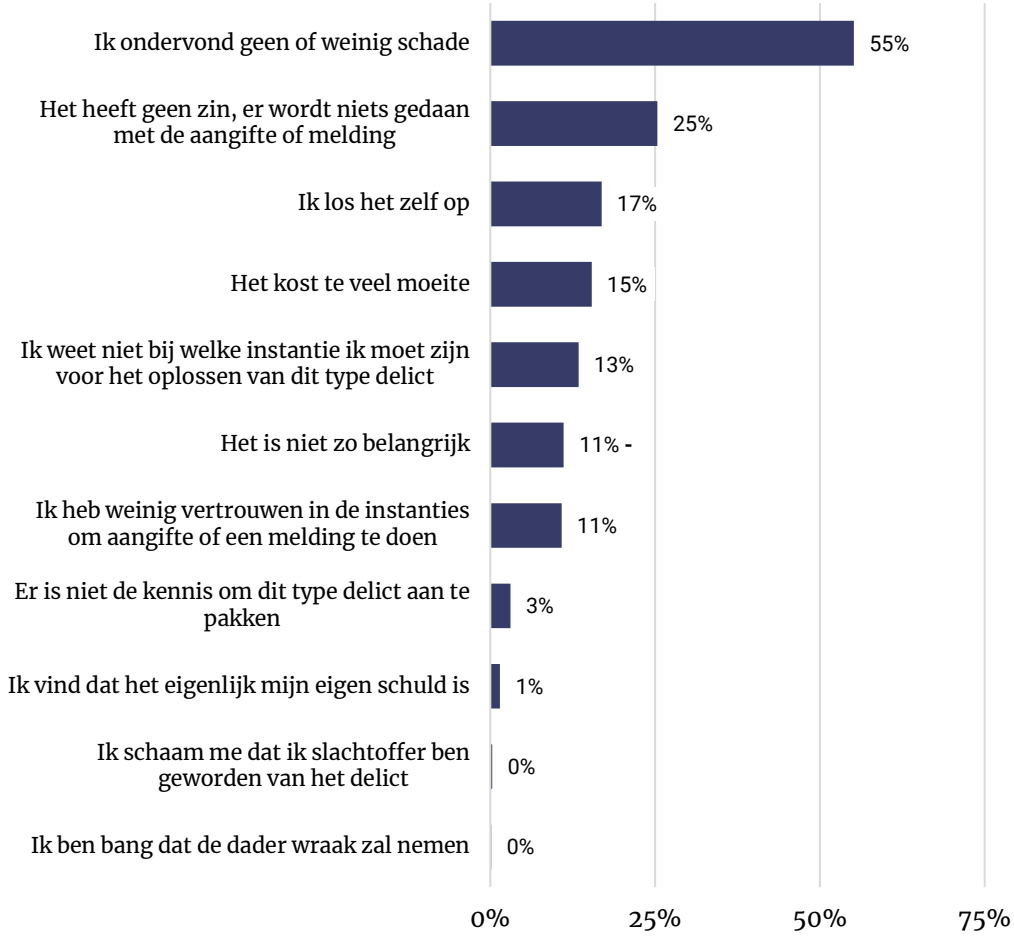
Vergelijking met 2023

- Minder dan in 2023 is het gebrek aan belang een reden om niks te doen met het meegemaakte voorval.

Resultaten subgroepen

- Nederlanders onder de 40 jaar vinden het vaker te veel moeite om aangifte of melding te doen.
- 65-plussers noemen minder dat ze niet weten waar ze voor aangifte moeten zijn. Wel zeggen ze vaker geen aangifte te doen omdat ze het meegemaakte incident hun eigen schuld vinden.

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=665) (maximaal 3 antwoorden)



Eén op vijf doet aangifte of melding om schade vergoed te krijgen

- 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 (64%).
- In het verlengde hiervan wil de helft (49%) een veiligere omgeving creëren.
- Eén op de vijf doet aangifte of melding om schade vergoed te krijgen.

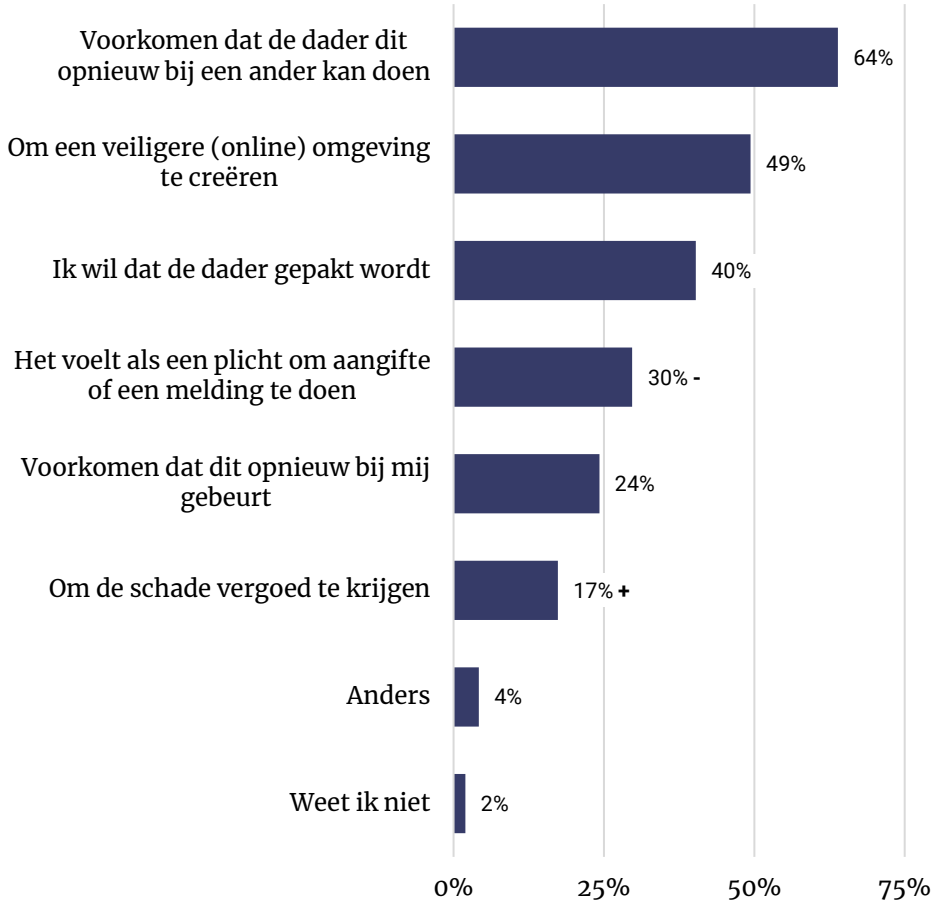
Vergelijking met 2023

- Minder vaak dan bij de vorige meting doet men aangifte/melding om dat het 'de plicht' is.
- In 2024 doet men het vaker om schade vergoed te kunnen krijgen.

Resultaten subgroepen

- Vrouwen vinden het vaker dan mannen hun plicht om aangifte te doen.

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=286)
(maximaal 3 antwoorden)



Twee op vijf passen gedrag aan na meemaken cybercrime

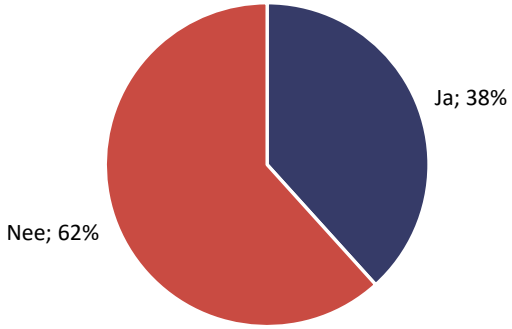
- Twee op de vijf (38%) Nederlanders die één of meerdere voorvallen van cybercrime meemaakten, gaan sindsdien op een andere manier om met de eigen digitale veiligheid.
- Als men gevolgen heeft ervaren van de meegemaakte voorvallen, is men vaker voorzichtig. Dat geldt helemaal wanneer de gevolgen ernstig waren.

Resultaten subgroepen

- Van de Nederlanders onder de 40 jaar past driekwart (72%) het gedrag niet aan na het meemaken van een incident.

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=975)



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