# Cybersecurity onderzoek Alert Online 2024

## Deelrapport overheid

Ipsos i&O

Ministerie van Economische Zaken

www.ipsos-publiek.nl

# Colofon

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

**Rapportnummer**
2024/199

**Datum**
september 2024

**Opdrachtgever**
Ministerie van Economische Zaken

**Auteurs**
Sara Kellij
Bram Doms

# Inhoudsopgave

# 1. Managementsamenvatting

# Samenvatting | 1/2

### Acht op de tien ambtenaren vindt 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.

Met de meeste voorgelegde vormen van cybercriminaliteit is de meerderheid van de ambtenaren bekend. Phishing en hacking zijn de bekendste vormen van cybercrime. Social engineering en CEO-fraude zijn minder bekend, een derde kent hiervan de betekenis. De bekendheid met alle voorgelegde vormen van cybercrime is vergelijkbaar met 2023. Van de verschillende vormen van cybercriminaliteit wordt de kans op een DDoS-aanval en hacking het hoogst ingeschat. Van beide acht 58 procent van degenen die het kennen, het waarschijnlijk dit mee te maken. Ook phishing (56%) wordt als risico gezien.

### 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. Een derde van de ambtenaren (37%) geeft zichzelf een 8 of hoger. Dat is een duidelijke toename ten opzichte van 2023, toen dit een kwart (26%) was.

### 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.

# Samenvatting | 2/2

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%) en 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**
Een op de vijf (22%) ambtenaren heeft de afgelopen 12 maanden een phishingmail op het werk ontvangen. Zeven procent werd benaderd voor WhatsAppfraude en ook 3 procent werd benaderd op social 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 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) online veiligheid?**

Dit deelrapport richt zich specifiek op de doelgroep ambtenaren.

De hoofdvraag behandelen we in dit rapport in de volgende drie deelvragen:

1 Wat weten ambtenaren over online veiligheid en het verbeteren van de online veiligheid?
2 Wat vinden ambtenaren van hun eigen online gedrag als het gaat om veiligheid en vaardigheden?
3 Wat doen ambtenaren op het gebied van hun online veiligheid en het verbeteren daarvan?

## Leeswijzer

Dit deelrapport behandelt de resultaten van ambtenaren. De resultaten van ambtenaren worden vergeleken met de resultaten van medewerkers van grote bedrijven met meer dan 200 werknemers.

Hoofdstuk 3 t/m 5 van dit rapport behandelen de onderzoeksresultaten voor de drie onderzoeksvragen. Hoofdstuk 3 gaat in op kennis van en ervaring met online risico's. Hoofdstuk 4 behandelt de zorgen die men heeft over online risico's en het online gedrag en regels op het werk. Het rapport sluit af met hoofdstuk 5 over slachtofferschap en aangiftebereidheid.

Naast dit deelrapport is er nog een hoofdrapport dat ingaat op de resultaten voor de Nederlandse bevolking en een deelrapport gericht op het bedrijfsleven.

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 gaat het bij alle benoemde verschillen om significante verschillen ($p < .05$).

## Methode en respons

In totaal vulden 473 ambtenaren een online vragenlijst in. Het gaat om 192 ambtenaren werkzaam bij de overheid (Rijk, provincie, gemeente) en 281 die werkzaam zijn bij de semioverheid.[1] Respondenten zijn afkomstig uit het Ipsos I&O Panel[2]. Het online veldwerk vond plaats van 25 juni tot 9 juli 2024.

[1] *Dit is op basis van zelfopgave. Men kon in de vragenlijst de optie "Ik ben werkzaam bij de semioverheid (Waterschappen, Politie, etc.)" selecteren.*
[2] *https://www.ioresearch.nl/onderzoeksmethoden/io-research-panel/*

# 3. Kennis en ervaring online risico’s

# Acht op tien ambtenaren vindt eigen kennis digitale veiligheid redelijk tot goed

- Acht op de tien (80%) ambtenaren beoordeelt de eigen kennis over digitale veiligheid als redelijk tot zeer goed. Een vijfde vindt het eigen kennisniveau matig of nog minder (16% matig, 2% slecht, 1% zeer slecht).

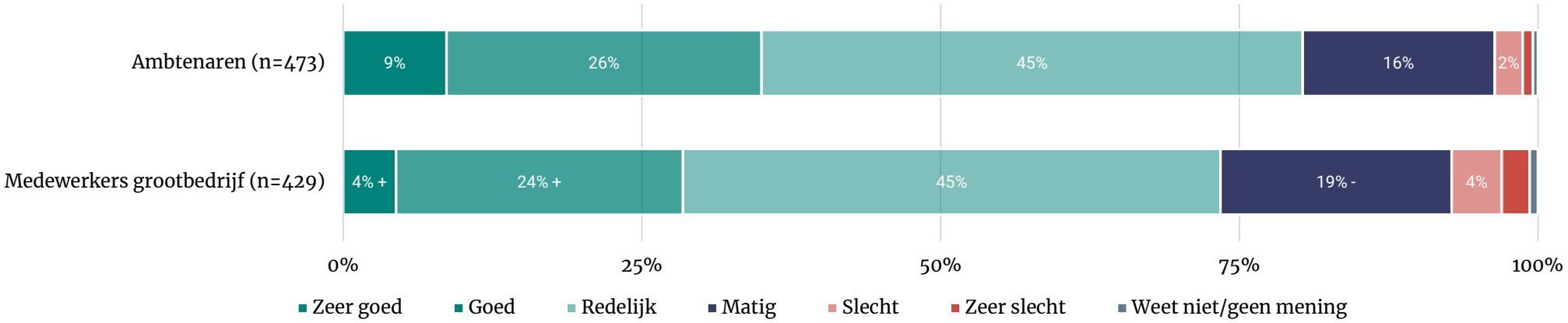
**Vergelijking met 2023**

- Het oordeel van de ambtenaren is vergelijkbaar met 2023. Medewerkers van een grootbedrijf zijn positiever over hun kennis dan een jaar eerder.

**Vergelijking grootbedrijf**

- Medewerkers van het grootbedrijf en ambtenaren schatten hun kennis gelijkwaardig in.

**Hoe schat u uw eigen kennis over digitale veiligheid in?**




Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

# Meerderheid ambtenaren denkt DDoS-aanval, phishing en hacking op werk mee te kunnen maken

- Negen van de elf voorgelegde vormen van cybercrime zijn bij een meerderheid van de ambtenaren bekend.
- Ruim de helft denkt op het werk met phishing en hacking te maken te kunnen krijgen.

**Vergelijking met 2023**

- Ambtenaren achten de kans om de verschillende phishing, DDoS-aanvallen, ransomware, helpdeskfraude en QR-fraude minder waarschijnlijk dan in 2023.

**Vergelijking grootbedrijf**

- De resultaten van het grootbedrijf lijken op die van de overheid. Ambtenaren verwachten vaker incidenten met malware mee te maken en minder CEO-fraude.

| In deze tabel staan 11 voorgelegde vormen van cybercriminaliteit, op volgorde van bekendheid | Kent de betekenis (naar eigen zeggen) | | Denkt er in werksituatie mee te maken te kunnen krijgen* | |
|---|---|---|---|---|
| | Ambtenaren (n=473) | Medewerkers grootbedrijf (n=429) | Ambtenaren | Medewerkers grootbedrijf |
| Phishing | 99% | 97% | 56% - n=467 | 55% - n=417 |
| Hacking | 98% | 97% | 58% n=463 | 53% - n=415 |
| Bankhelpdeskfraude** | 92% | 88% | 9% n=435 | 8% n=377 |
| Helpdeskfraude | 85% | 84% | 18% - n=404 | 19% - n=360 |
| Aankoopfraude** | 81% | 78% | | |
| Malware | 80% | 80% | 49% n=377 | 41% - n=344 |
| DDos-aanval | 79% | 75% | 58% - n=374 | 52% - n=322 |
| Ransomware | 75% | 76% + | 47% - n=358 | 44% - n=328 |
| QR-fraude | 64% | 63% | 14% - n=304 | 17% - n=270 |
| Social engineering | 32% | 30% | 38% n=156 | 36% n=129 |
| CEO-fraude | 32% | 37% | 31% n=152 | 46% n=158 |

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager).
Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).
*Alle begrippen voorgelegd waarvan men de betekenis zegt te kennen | percentage zeker + waarschijnlijk wel.
**Vergelijking met voorgaande jaar niet mogelijk door lage responsaantallen of omdat deze niet voorkwam in de vorige meting.

# 4. Zorgen en online gedrag op het werk

# Driekwart ambtenaren maakt zich weinig zorgen over digitale veiligheid op het werk

- Een kwart van de ambtenaren maakt zich wel eens zorgen over de digitale veiligheid op het werk. Twee procent maakt zich (zeer) veel zorgen.

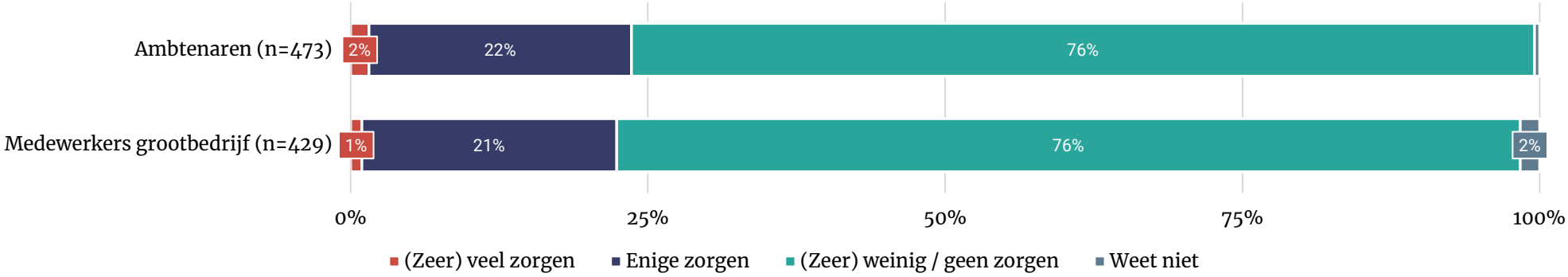
**Vergelijking met 2023**

- Ten opzichte van 2023 zijn de zorgen om digitale veiligheid op het werk niet veranderd.

**Vergelijking grootbedrijf**

- Ambtenaren en medewerkers van het grootbedrijf maken zich in vergelijkbare mate zorgen om de digitale veiligheid op het werk.

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



# Ambtenaren geven zichzelf een 7,1 voor omgaan met online risico's

- Een derde van de ambtenaren geeft zichzelf een 8 of hoger als het gaat om het veilig omgaan met online risico's. Zeven procent geeft zichzelf een onvoldoende. De meerderheid beoordeelt de omgang met online risico's als redelijk en geeft zichzelf een 6 of een 7. Ambtenaren geven zichzelf gemiddeld een 7,1.
- Ambtenaren die een hoog cijfer geven, zijn zich bewust van de risico's en zijn voorzichtig. Een aantal is zich door cursussen meer bewust geworden van de gevaren. Maar er wordt ook genoemd dat er altijd ruimte is voor verbetering. Ambtenaren die een lager cijfer geven, hebben soms weinig kennis of staan te weinig stil bij de risico's. Ook geven sommigen aan moeite te hebben om qua kennis bij te blijven.

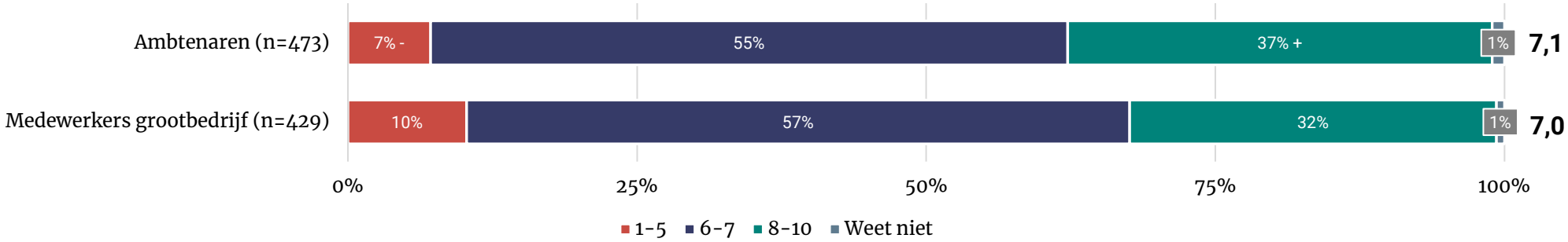
**Vergelijking met 2023**

- Het aantal ambtenaren dat zichzelf een onvoldoende geeft voor het omgaan met online risico's is afgenomen ten opzichte van 2023 (12%). Het aandeel ambtenaren dat zichzelf een 8 of hoger geeft, is sterk toegenomen van 26 naar 37 procent.

**Vergelijking grootbedrijf**

- Medewerkers van het grootbedrijf beoordelen hun omgang met online risico's vergelijkbaar met ambtenaren.

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



# Bij ambtenaren meer maatregelen online veilig gedrag dan grootbedrijf

- Bij de overheid moet twee derde twee-staps-inloggen.
- Zes op de tien ambtenaren hebben zelf geen rechten om software te installeren op hun werkcomputer.

**Vergelijking met 2023**

- Ten opzichte van 2023 daalde het aantal ambtenaren dat aangeeft met andere dan de genoemde maatregelen te maken te hebben gehad.

**Vergelijking grootbedrijf**

- Medewerkers van het grootbedrijf hebben minder te maken met maatregelen voor online veilig gedrag binnen het bedrijf. Ook zijn ze vaker niet op de hoogte van de maatregelen die zijn getroffen.

| Welke acties zijn er binnen uw bedrijf/organisatie ondernomen ten behoeve van online veilig gedrag? | Ambtenaren (n=473) | Medewerkers grootbedrijf (n=429) |
|---|---|---|
| Er is twee-staps-inloggen verplicht voor toegang | 68% | 50% |
| Alleen de systeembeheerders kunnen software installeren | 59% | 51% |
| Er worden trainingen gegeven binnen mijn organisatie over online veiligheid* | 48% | 41% |
| Er zijn afspraken gemaakt over het versturen/uitwisselen van bestanden en/of persoonsgegevens | 47% | 35% |
| Er zijn adviezen/richtlijnen over hoe je veilig online thuiswerkt | 47% | 36% |
| Er zijn afspraken gemaakt over het gebruik van zakelijke smartphones, laptops en/of tablets voor privé en/of zakelijk gebruik | 46% | 38% |
| Er zijn regels over hoe je veilig online thuiswerkt | 43% | 34% |
| Er is binnen mijn organisatie/bedrijf een digitale hulpverlener waar je terecht kunt | 42% | 33% |
| Er zijn adviezen/richtlijnen over het gebruikmaken van websites/of e-mail/sociale media** | 37% | 28% - |
| Er zijn regels over het gebruikmaken van websites/of e-mail/sociale media | 36% | 29% |
| De toegang tot bepaalde websites en/of socialmediakanalen is geblokkeerd | 36% | 34% |
| Er worden op willekeurige momenten testmails verstuur om medewerkers te testen op de herkenning van phishing*** | 35% | 38% + |
| Er zijn afspraken gemaakt over het gebruikmaken van opslagmedia als usb-sticks of externe harde schijven | 30% | 25% |
| Het gebruik van USB-sticks in onze organisatie is onmogelijk gemaakt | 23% | 17% |
| Er is een verzekering afgesloten tegen de financiële gevolgen van cybercrime | 3% | 4% |
| Anders | 2% - | 2% |
| In mijn bedrijf of organisatie is geen enkele actie ondernomen ten behoeve van veilig online gedrag | 1% | 1% |
| Weet ik niet | 11% | 22% |

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager). Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

*niet gevraagd in 2023
**in 2023: Er zijn adviezen/richtlijnen over het gebruikmaken van websites/of e-mail
*** in 2023: Er worden in het kader van een educatie programma op willekeurige momenten test-e-mails verstuurd om medewerkers te testen op herkenning van phishing

# Zes op tien ambtenaren vinden dat afspraken voldoende worden toegepast

- Negen op de tien ambtenaren vinden het goed als collega's hen erop aanspreken als ze zich niet aan de afspraken voor veilig gedrag houden.
- Voor vier op de vijf ambtenaren zijn de afspraken op het werk duidelijk. Voor 84 procent is het makkelijk om zich aan deze afspraken te houden.
- De helft spreekt collega's erop aan als zij zich niet aan de afspraken houden. Een derde vindt dat zijn leidinggevende het goede voorbeeld geeft. Echter geeft 42 procent aan dat van diens leidinggevende niet te weten.

**Vergelijking met 2023**

- Er zijn geen significante verschillen voor ambtenaren in vergelijking met 2023.

**Vergelijking grootbedrijf**

- Tussen medewerkers van het grootbedrijf en ambtenaren zijn geen verschillen.

| **In hoeverre bent u het eens of oneens met de volgende stellingen?** % (zeer) eens. Voorgelegd aan personen waar afspraken zijn gemaakt. | **Ambtenaren (n=416)** | **Medewerkers grootbedrijf (n=330)** |
|---|---|---|
| Ik vind het goed als collega's mij erop aanspreken als ik me niet houd aan de werkafspraken over veilig online gedrag | 88% | 85% |
| Ik krijg toegang tot goede tools en instrumenten (bijvoorbeeld twee-staps-inloggen of een wachtwoordmanager) om veilig online gedrag te bevorderen | 85% | 82% + |
| Het is gemakkelijk om mij aan de afspraken te houden over veilig online gedrag binnen mijn bedrijf of organisatie | 84% | 87% |
| De afspraken over hoe ik me online veilig moet gedragen op mijn werk vind ik duidelijk | 80% | 82% |
| De afspraken over veilig online gedrag die binnen mijn organisatie/bedrijf zijn gemaakt, worden voldoende toegepast | 61% | 68% |
| Ik spreek collega's er op aan als zij zich niet houden aan de werkafspraken over veilig online gedrag | 48% | 49% |
| Ik word er op mijn werk op aangesproken als ik me niet aan de werkafspraken houd over veilig online gedrag | 48% | 55% |
| Mijn leidinggevende geeft het goede voorbeeld als het gaat om veilig online gedrag | 36% | 43% |

Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

# Bij meeste ambtenaren maakt de werkgever automatische back-ups

- Bij negen op de tien ambtenaren worden door hun werkgever back-ups gemaakt. Bijna de helft (44%) doet dit ook thuis. Een derde (36%) maakt ook regelmatig back-ups van de werklaptop.

**Vergelijking met 2023**

- In 2024 maken minder ambtenaren thuis regelmatig back-ups van hun bestanden.
- Ook hebben ze minder vaak de privacy-instellingen van sociale media accounts verhoogd.

**Vergelijking grootbedrijf**

- Tussen ambtenaren en medewerkers van het grootbedrijf zijn geen significante verschillen voor deze stellingen.

| In hoeverre zijn de volgende uitspraken van toepassing op u? (% meestal wel + altijd) | Ambtenaren (n=473) | Medewerkers grootbedrijf (n=429) |
|---|---|---|
| Mijn werkgever maakt automatisch back-ups van alle bestanden (volledige back-ups) | 92% | 93% |
| Als ik een openbare computer heb gebruikt dan log ik na gebruik al mijn accounts uit (bank, social media en e-mail) | 87% | 87% |
| Ik heb de privacy-instellingen van mijn social media accounts verhoogd ten opzichte van de standaardinstellingen | 67% - | 65% - |
| Ik let op of er een slotje en/of https bij het webadres staat | 65% | 66% |
| Ik maak thuis regelmatig back-ups van mijn bestanden | 44% - | 45% |
| Ik maak op mijn werk regelmatig back-ups van de bestanden op mijn werklaptop | 36% | 32% - |
| Ik maak thuis gebruik van een extern opslagapparaat dat continu online is | 16% | 15% |
| Ik verstuur werkbestanden van mijn werk e-mailadres naar mijn privé e-mail | 6% | 7% |

Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

*nieuwe stelling in 2024.

# Vrijwel alle ambtenaren melden een virus

- Vrijwel alle ambtenaren melden het bij de ICT-afdeling als ze een virus downloaden.
- Twee derde van de ambtenaren zou zich schamen als blijkt dat ze in een phishingmail zijn getrapt. Vier procent zou uit schaamte niet vertellen dat ze een virus hebben gedownload.

**Vergelijking met 2023**

- Vanwege een gewijzigde vraagstelling is de ontwikkeling niet exact vast te stellen.
- Wel gaven de meeste ambtenaren ook in 2023 aan het te vertellen als ze een virus zouden downloaden. Ook het aandeel dat denkt zich te zullen schamen was vergelijkbaar.

**Vergelijking grootbedrijf**

- Tussen ambtenaren en medewerkers van het grootbedrijf zijn geen significante verschillen voor deze stellingen.

| In hoeverre zijn de volgende uitspraken van toepassing op u? (% zeer waarschijnlijk + waarschijnlijk) | Ambtenaren (n=473) | Medewerkers grootbedrijf (n=429) |
|---|---|---|
| Als ik door heb dat ik een virus heb gedownload op mijn werkcomputer waardoor ook andere computers binnen mijn bedrijf besmet (kunnen) raken, dan vertel ik de ICT-afdeling meteen wat ik heb gedaan | 97% | 96% |
| Als ik door heb dat ik een virus heb gedownload op mijn werkcomputer waardoor ook andere computers binnen mijn bedrijf besmet (kunnen) raken, dan vertel ik meteen aan iemand op mijn werk wat ik heb gedaan | 95% | 94% |
| Als ik op een link in een phishing e-mail zou klikken dan zou ik mij daarvoor schamen | 65% | 59% |
| Als ik getroffen word door ransomware (gijzelsoftware), dan zou ik betalen als ik daardoor weer toegang krijg tot mijn persoonlijke bestanden* | 8% | 6% |
| Als ik door heb dat ik een virus heb gedownload op mijn werkcomputer, dan vertel ik uit schaamte niet aan anderen wat ik heb gedaan | 4% - | 4% - |

Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).
*stelling iets anders geformuleerd in 2024 dan in eerdere jaren.

# Helft ambtenaren ervaart geen belemmering bij borgen gedragsregels

- De helft van de ambtenaren ziet geen belemmeringen voor het borgen van de gedragsregels.
- De voornaamste belemmeringen die men ervaart zijn onvoldoende communicatie of onduidelijkheid bij wie de borging van de afspraken ligt.

**Vergelijking met 2023**

- In 2023 was het niet aansprekend communiceren de meest genoemde belemmering door ambtenaren. Zestien procent noemde deze belemmering toen tegenover 7 procent nu.

**Vergelijking grootbedrijf**

- Tussen ambtenaren en medewerkers van het grootbedrijf zijn geen verschillen in de belemmeringen die zij ervaren.

| Welke van onderstaande belemmeringen ervaart u binnen uw bedrijf/organisatie bij het borgen van de afspraken voor online veilig gedrag? | Ambtenaren (n=204) | Medewerkers grootbedrijf (n=175) |
|---|---|---|
| Er wordt niet voldoende over gecommuniceerd | 12% | 7% |
| Het is niet duidelijk bij wie de borging van deze afspraken ligt | 11% | 5% |
| Er wordt geen prioriteit aan gegeven | 10% | 3% |
| Er wordt niet duidelijk over gecommuniceerd | 9% | 8% |
| Te weinig kennis binnen de organisatie | 8% | 2% |
| Te weinig tijd | 7% | 7% |
| Er wordt niet aansprekend over gecommuniceerd | 7% - | 5% |
| Er wordt niet eenduidig (door verschillende afdelingen) over gecommuniceerd | 6% | 3% |
| Er is geen duidelijk aanspreekpunt binnen de organisatie | 6% | 3% |
| Gebrek aan draagvlak vanuit het management | 4% | 3% |
| Te weinig menskracht | 3% | 5% |
| Te weinig budget | 2% | 1% |
| Ik ervaar geen belemmeringen bij het borgen van de afspraken over veilig online gedrag | 53% | 48% |
| Weet ik niet | 17% | 25% |

Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

# Vergroten kennis en cyberoefenen nog steeds meest genoemd voor verbetering borging gedragsregels

- Driekwart van de ambtenaren ziet verbeterpunten voor de borging van veilig online gedrag.
- Vier op de tien noemen dat het vergroten van kennis hieraan kan bijdragen.
- Daarna ziet men cyberoefenen, meer communicatie en periodieke audits als manieren om een veiliger online omgeving te bereiken.

**Vergelijking met 2023**

- In vergelijking met 2023 noemt men minder vaak het aantrekkelijker maken van communicatie.

**Vergelijking grootbedrijf**

- De resultaten onder medewerkers van het grootbedrijf zijn vergelijkbaar met die onder ambtenaren.

| Welke maatregelen zouden er naar uw overtuiging aan bijdragen dat veilig online gedrag (nog) beter geborgd wordt? | Ambtenaren (n=212) | Medewerkers grootbedrijf (n=155) |
|---|---|---|
| Vergroten kennis hierover binnen de organisatie | 43% | 39% |
| Cyberoefenen | 31% | 28% |
| Bedrijf (periodiek) laten doorlichten (externe audit) op cybersecurity door experts (voor ondernemers) | 22% | 26% |
| Meer communicatie | 20% | 17% |
| Een duidelijk aanspreekpunt binnen de organisatie | 19% | 12% |
| Duidelijkere communicatie | 19% | 16% |
| Hogere prioriteit | 16% | 12% |
| Een of meer ICT-experts in de organisatie | 13% | 11% |
| Beter vastleggen wie verantwoordelijk is voor welke afspraken | 12% | 9% |
| Communicatie beter op elkaar afstemmen | 11% | 4% - |
| Meer draagvlak vanuit het management | 10% | 7% |
| Meer tijd | 7% | 2% |
| Communicatie aantrekkelijker maken | 7% - | 5% |
| Meer budget | 6% | 3% |
| Meer menskracht | 5% | 5% |
| Anders | 5% | 1% |
| Ik zie geen mogelijkheden om de afspraken over veilig online gedrag beter te borgen | 6% | 10% |
| Weet ik niet | 16% | 25% |

Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

# 5. Slachtofferschap en aangiftebereidheid

# Mails met poging tot phishing meest meegemaakte vorm cybercrime op werk

- Drie op de tien ambtenaren maakten in de afgelopen 12 maanden een of meerdere pogingen tot cybercrime mee op het werk.
- Van de ambtenaren die hier wel mee te maken hadden, maakte een op de vijf een poging tot phishing mee. Zeven procent werd benaderd voor WhatsApp-fraude en ook 3 procent werd benaderd op social media met een verzoek om een onbekende link aan te klikken.

**Vergelijking met 2023**

- Ook vorig jaar was phishing het meest meegemaakte incident.
- Ambtenaren hebben nu vaker te maken met WhatsAppfraude dan een jaar eerder.

**Vergelijking grootbedrijf**

- Medewerkers van het grootbedrijf hebben vaker te maken met pogingen tot phishing

| Heeft u in de afgelopen 12 maanden zelf weleens te maken gehad met een van de onderstaande voorvallen in uw werksituatie? | Ambtenaren (n=473) | Medewerkers grootbedrijf (n=429) |
|---|---|---|
| Mails ontvangen met poging tot phishing | 22% | 29% + |
| Benaderd voor Whatsappfraude* | 7% + | 6% + |
| Benaderd op social media met een vraag om een onbekende link aan te klikken | 3% | 3% |
| Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik die echt leek | 2% | 3% |
| Gebeld door iemand die zich voordeed als bedrijf of officiële instantie (bijv. bank, belasting) om geld of gegevens te bemachtigen | 1% - | 3% |
| Een foute link ook daadwerkelijk hebben aangeklikt in de zin dat deze een virus, spam, phishing of andere ongewenste poging tot cybercrime bevatte | 0,8% | 0,7% |
| Dat iemand dreigde uw bestanden te openbaren of dit ook echt deed | 0,4% | 0,7% |
| Computer werkte tijdelijk niet door malware/virus | 0,2% | 0% - |
| Acquisitiefraude | 0,2% | 0,9% |
| Geïnfecteerde software/bestanden gedownload waardoor malware werd verspreid | 0% - | 0% |
| Identiteitsfraude** | 0% | 0% |
| Ransomware | 0% | 0,2% |
| Dat iemand in een apparaat (computer, telefoon) heeft ingelogd zonder dat u daar toestemming voor gegeven heeft | 0% | 0% |
| Dat iemand in een account heeft ingelogd zonder dat u daar toestemming voor gegeven heeft | 0% | 0% |
| Aankoopfraude | 0% | 0% |
| Geen van deze voorvallen | 71% | 67% |

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager). Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

*in 2023: Benaderd via Whatsapp door iemand die zich voordeed als een bekende die probeerde geld te ontvangen.
** in 2023: identiteitsdiefstal

# Helft van de ambtenaren doet geen aangifte of melding cybercrime

- De helft van de ambtenaren die een incident meemaakten, deed geen aangifte of melding.
- Bijna de helft van de ambtenaren die een incident meemaakten, meldde dit bij de ICT-afdeling.

**Vergelijking met 2023**

- Ambtenaren doen minder vaak aangifte of melding bij de politie dan in 2023 (toen beide 3%). Ook wordt er minder melding gemaakt bij het NCSC (2023: 4%).

**Vergelijking grootbedrijf**

- Tussen medewerkers van het grootbedrijf en ambtenaren zijn geen significante verschillen in het doen van aangifte of het maken van een melding.

| U geeft aan dat u op uw werk te maken heeft gehad met een of meerdere voorvallen van cybercrime. Heeft u of uw werkgever toen een aangifte of melding gedaan? | Ambtenaren (n=142) | Medewerkers grootbedrijf (n=143) |
|---|---|---|
| Ja, melding bij de ICT-afdeling van mijn bedrijf | 46% | 50% |
| Ja, melding bij de Fraudehelpdesk | 4% | 5% |
| Ja, bij mijn leidinggevende | 3% | 5% |
| Ja, bij een andere organisatie | 1% | 2% |
| Ja, bij de Autoriteit Persoonsgegevens | 1% | 0% |
| Ja, aangifte bij de politie | 0% - | 2% |
| Ja, melding bij de politie | 0% - | 1% |
| Ja, bij een bank | 0% | 0% |
| Ja, melding bij het Nationaal Cyber Security Centrum (NCSC) | 0% - | 1% |
| Nee, ik heb hier niks mee gedaan | 50% | 39% |

Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

# Driekwart doet aangifte of melding om veiligere online omgeving te creëren

- Driekwart noemt als belangrijkste reden voor een aangifte of melding, het creëren van een veiligere (online) omgeving. Ook wil de helft voorkomen dat de dader dit opnieuw bij een ander kan doen.
- Een derde ziet het als plicht om aangifte of melding te doen en een kwart wil voorkomen dat ze het nog eens meemaken.

**Vergelijking grootbedrijf**

- Tussen medewerkers van het grootbedrijf zijn geen significante verschillen.

| Wat zijn de belangrijkste redenen om wel aangifte of melding te doen? (maximaal 3) | Ambtenaren (n=71) | Medewerkers grootbedrijf (n=87) |
|---|---|---|
| Om een veiligere (online) omgeving te creëren | 77% + | 70% |
| Voorkomen dat de dader dit opnieuw bij een ander kan doen | 55% | 51% |
| Het voelt als een plicht om aangifte of een melding te doen | 29% | 24% |
| Voorkomen dat dit opnieuw bij mij gebeurt | 25% | 31% |
| Dat wordt door iemand anders afgehandeld/beslist | 15% | 13% |
| Ik wil dat de dader gepakt wordt | 14% | 17% |
| Om de schade vergoed te krijgen | 3% | 5% |
| Anders | 5% | 2% |
| Weet ik niet | 1% | 5% |

Significante verschillen tussen 2024 en 2023 zijn aangegeven met '+' (toename) en '-' (afname).

# Een derde deed geen aangifte vanwege weinig gevolgen van incident

- Ambtenaren die geen melding of aangifte deden, ondervonden geen of weinig schade van het incident.
- Bij een vijfde werd het door iemand anders afgehandeld of beslist.

**Vergelijking grootbedrijf**

- Er zijn geen significante verschillen tussen ambtenaren en medewerkers van het grootbedrijf.

| Wat is de belangrijkste reden om geen aangifte of melding te doen? (maximaal 3) | Ambtenaren (n=71) | Medewerkers grootbedrijf (n=56) |
|---|---|---|
| Ik ondervond geen of weinig schade | 33% | 25% |
| Dat wordt door iemand anders afgehandeld/beslist | 19% | 21% |
| Ik los het zelf op | 15% | 9% |
| Het is niet zo belangrijk | 10% | 7% |
| Het heeft geen zin, er wordt niets gedaan met de aangifte of melding | 10% | 16% |
| Ik heb weinig vertrouwen in de instanties om aangifte of een melding te doen | 6% | 11% |
| Er is niet de kennis om dit type delict aan te pakken | 3% | 4% |
| Ik weet niet bij welke instantie ik moet zijn voor het oplossen van dit type delict | 3% | 5% |
| Het kost te veel moeite | 1% | 7% |
| Ik ben bang dat de dader wraak zal nemen | 0% | 0% |
| Ik ben bang dat ik mijn baan verlies | 0% | 0% |
| Ik schaam me dat ik slachtoffer ben geworden van het delict | 0% | 0% |
| Ik vind dat het eigenlijk mijn eigen schuld is | 0% | 2% |
| Ik wilde aangifte doen maar dit werd mij afgeraden | 0% | 0% |
| Anders | 16% | 7% |
| Weet ik niet | 11% | 21% |

# 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