Cybersecurity onderzoek Alert Online 2023

Deelrapport overheid

i&O research

Ministerie van Economische Zaken en Klimaat

Colofon

Uitgave
I&O Research
Piet Heinkade 55
1019 GM Amsterdam

Rapportnummer
2023/170

Datum
september 2023

Opdrachtgever
Ministerie van Economische Zaken en Klimaat

Auteurs
Melle Conradie
Bram Doms

Inhoudsopgave

1. Managementsamenvatting

Samenvatting | 1/2

Driekwart ambtenaren vindt kennis online veiligheid redelijk tot goed

Ruim driekwart (78%) van de ambtenaren beoordeelt de eigen kennis over online veiligheid als redelijk tot zeer goed. Een kwart vindt het eigen kennisniveau matig of nog minder (17% matig, 4% slecht, 1% zeer slecht). Dat is vergelijkbaar met 2022. Medewerkers van het grootbedrijf beoordelen de eigen kennis vaker dan ambtenaren als matig.

Met de meeste voorgelegde vormen van cybercriminaliteit is de meerderheid van de ambtenaren bekend. Alleen social engineering is bij 70 procent onbekend. Het kennisniveau is vergelijkbaar met 2022. Wel dachten ambtenaren in 2022 meer te maken te kunnen krijgen met verschillende vormen van cybercriminaliteit op het werk. Het risico op DDoS-aanvallen schat men het hoogst in (71%). Zes op de tien medewerkers van het grootbedrijf (60%) denken hier op het werk mee te maken te kunnen krijgen.

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

Driekwart van de ambtenaren (74%) maakt zich weinig zorgen over de digitale veiligheid in de werksituatie. Drie procent maakt zich veel zorgen. Minder ambtenaren maken zich zorgen dan in 2022. Het beeld onder medewerkers van het grootbedrijf is vergelijkbaar. Dat geldt ook voor het cijfer dat men zichzelf geeft voor de veilige omgang met online risico's. Zowel ambtenaren als medewerkers van het grootbedrijf beoordelen zichzelf gemiddeld met een 6,8. Twaalf procent van de ambtenaren geeft zichzelf een onvoldoende. Uit de toelichting blijkt dat deze groep vindt dat ze weinig kennis hebben of te laks zijn in hun omgang met de 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 naar eigen zeggen verplicht dit te doen (2022: 54%). Daarnaast hebben ambtenaren adviezen/richtlijnen en/of regels over verschillende zaken. 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%).

Samenvatting | 2/2

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 (82%).

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 vier procent werd zogenaamd gebeld door een bekende of officiële instantie met als doel om geld te ontvangen. Ambtenaren krijgen vaker neptelefoontjes dan in 2022. De situatie is vergelijkbaar met die van medewerkers van het grootbedrijf.

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. Ambtenaren doen minder vaak iets met het meegemaakte voorval dan medewerkers van het grootbedrijf, die vaker een melding bij de ICT-afdeling of bij de politie maken. 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 een 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. Waar relevant worden verschillen tussen medewerkers van de Rijksoverheid en medewerkers van de semioverheid in tekst beschreven.

In dit rapport worden de resultaten van ambtenaren 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.

Methode en respons

In totaal vulden 371 ambtenaren een online vragenlijst in. Het gaat om 168 ambtenaren werkzaam bij de overheid (Rijk, provincie, gemeente) en 203 die werkzaam zijn bij de semioverheid.[1] Een klein deel van de respondenten is afkomstig uit de steekproef voor het algemeen publiek. Respondenten zijn afkomstig uit het I&O Research Panel. Het online veldwerk vond plaats van 10 t/m 24 juli 2023.

[1] *Dit is op basis van zelfopgave. Men kon in de vragenlijst de optie "Ik ben werkzaam bij de semioverheid (Waterschappen, Politie, etc.)" selecteren.*

3. Kennis en ervaring online risico’s

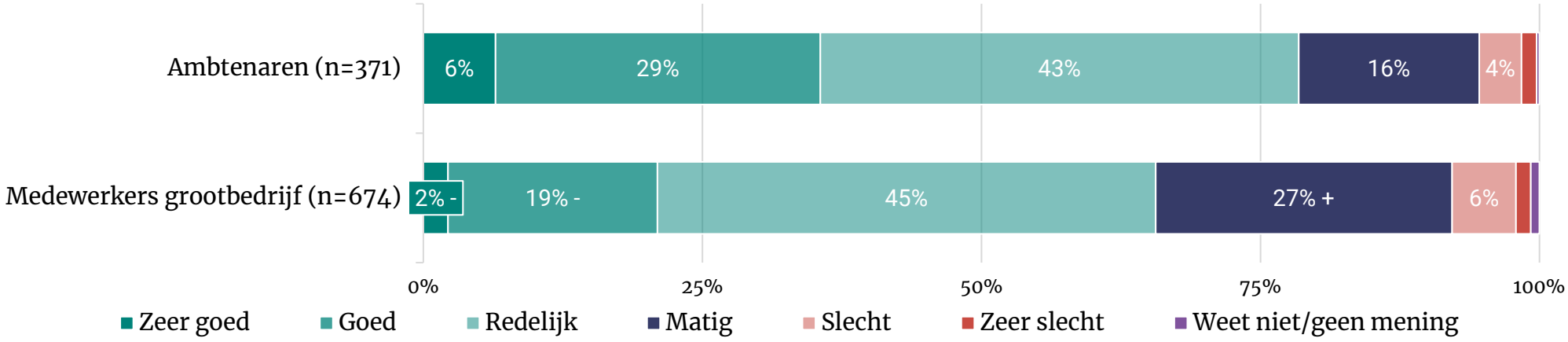
Driekwart ambtenaren vindt eigen kennis digitale veiligheid redelijk tot goed

Ruim driekwart (78%) van de ambtenaren beoordeelt de eigen kennis over digitale veiligheid als redelijk tot zeer goed. Een kwart vindt het eigen kennisniveau matig of nog minder (16% matig, 4% slecht, 1% zeer slecht). Ambtenaren bij de semioverheid beschouwen hun kennis vaker als matig.

Vergelijking met 2022
Het oordeel van de ambtenaren is vergelijkbaar met 2022. Ook medewerkers van het grootbedrijf vinden hun kennis nu minder dan een jaar eerder.

Vergelijking grootbedrijf
Medewerkers van het grootbedrijf schatten hun kennis minder vaak dan ambtenaren als goed of zeer goed in, en beoordelen hun kennis vaker als matig.

Hoe schat u uw eigen kennis over digitale veiligheid in?



Significante verschillen tussen 2023 en 2022 zijn aangegeven met '+' (toename) en '-' (afname).

Meerderheid ambtenaren denkt phishing, hacking en malware op werk mee te kunnen maken

- Zeven van de acht voorgelegde vormen van cybercrime zijn bij een meerderheid van de ambtenaren bekend.
- Twee derde denkt op het werk met phishing en hacking te maken te kunnen krijgen.

Vergelijking met 2022

- Veel vormen van cybercrime acht men waarschijnlijker om mee te maken dan in 2022.

Vergelijking grootbedrijf

- De resultaten van het grootbedrijf lijken op die van de overheid. Ambtenaren zijn iets beter bekend met DDoS-aanvallen en verwachten hier ook vaker mee te maken te krijgen op het werk.

In deze tabel staan 8 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=371)	Medewerkers grootbedrijf (n=674)	Ambtenaren		Medewerkers grootbedrijf	
Phishing	97%	95%	63%	n=360	61%	n=641
Hacking	97%	95%	64%	n=360	61% +	n=642
Malware	82%	78%	54% +	n=305	53% +	n=524
Helpdeskfraude	82%	80%	32% +	n=304	33% +	n=542
DDoS-aanval	82%	75%	71% +	n=303	60% +	n=507
Ransomware	75%	71% -	59% +	n=279	59% +	n=477
QR-codefraude	65%	60%	24% +	n=241	25% +	n=404
Social engineering	31%	30%	44% +	n=114	46% +	n=202

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager).
Significante verschillen tussen 2023 en 2022 zijn aangegeven met '+' (toename) en '-' (afname).
*Alle begrippen voorgelegd waarvan men de betekenis zegt te kennen | percentage zeker + waarschijnlijk wel.

4. Zorgen en online gedrag op het werk

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

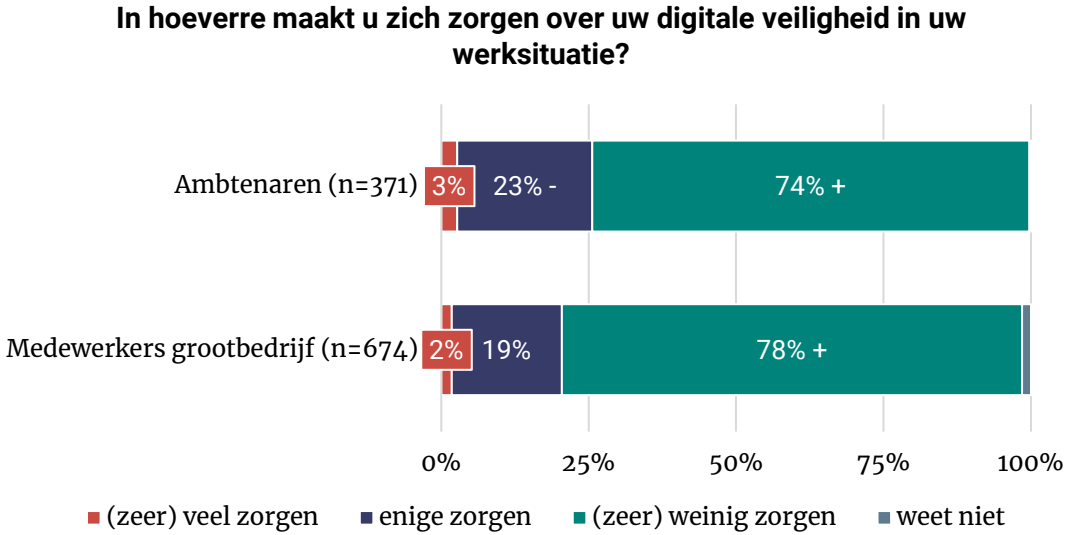
- Een kwart van de ambtenaren maakt zich wel eens zorgen over de digitale veiligheid op het werk. Drie procent maakt zich veel zorgen.

Vergelijking met 2022

- Ambtenaren maken zich minder zorgen dan in 2022 (toen 6% veel zorgen en 28% enige zorgen).

Vergelijking grootbedrijf

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



Ambtenaren geven zichzelf gemiddeld ruime voldoende voor omgang online risico's

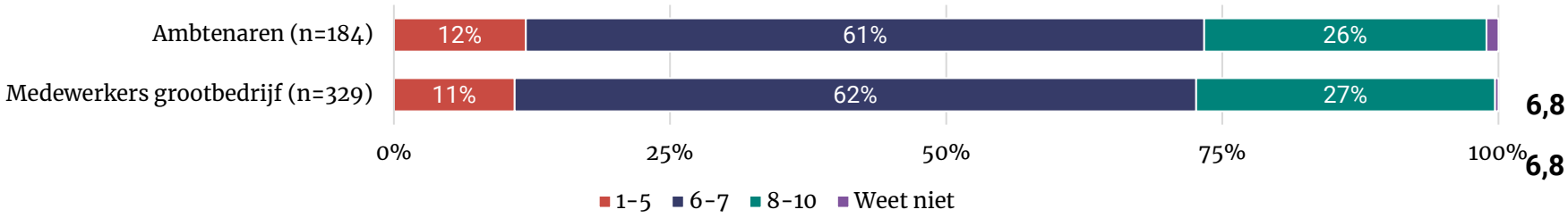
Een kwart van de ambtenaren geeft zichzelf een 8 of hoger als het gaat om het veilig omgaan met online risico's. Twaalf procent geeft zichzelf een onvoldoende. De meerderheid beoordeelt de omgang met online risico's als redelijk en geeft zichzelf een 6 of een 7. Dit resulteert in een 6,8 gemiddeld.

Gevraagd om het rapportcijfer toe te lichten noemen ambtenaren dat ze best het een en ander weten en voorzichtig zijn. Tegelijkertijd geven ze aan dat het altijd beter kan. Ambtenaren die zichzelf een lager cijfer geven, zeggen weinig kennis te hebben of laks te zijn in de omgang met de risico's die hun bekend zijn.

Vergelijking met 2022
De uitkomsten zijn vergelijkbaar met een jaar eerder.

Vergelijking grootbedrijf
Medewerkers van het grootbedrijf beoordelen hun omgang met online risico's hetzelfde als ambtenaren.

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.

Twee-staps-inloggen bij ambtenaren vaker verplicht

- Bij 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 2022

- Ambtenaren zijn vaker verplicht tot twee-staps-inloggen dan in 2022.
- Verder zijn ambtenaren minder vaak bekend met adviezen en richtlijnen die er zijn voor online veilig gedrag.

Vergelijking grootbedrijf

- Medewerkers van het grootbedrijf hebben minder te maken (of zijn minder bekend) met acties voor online veilig gedrag binnen het bedrijf.
- Wel geven ze vaker aan dat toegang tot bepaalde verzendplatforms zoals WeTransfer is geblokkeerd.

Welke acties zijn er binnen uw bedrijf/organisatie ondernomen ten behoeve van online veilig gedrag?	Ambtenaren (n=371)	Medewerkers grootbedrijf (n=674)
Er is twee-staps-inloggen verplicht voor toegang	64% +	47%
Alleen de systeembeheerders kunnen software installeren	60%	49%
Er zijn adviezen/richtlijnen over hoe je veilig online thuiswerkt	47%	39%
Er zijn afspraken gemaakt over het versturen/uitwisselen van bestanden en/of persoonsgegevens	45% -	39% -
Er zijn afspraken gemaakt over het gebruik van zakelijke smartphones, laptops en/of tablets voor privé en/of zakelijk gebruik	43% -	35% -
Er zijn regels over hoe je veilig online thuiswerkt	41%	38%
Er is binnen mijn organisatie/bedrijf een digitale hulpverlener waar je terecht kunt	39%	33%
Er zijn adviezen/richtlijnen over het gebruikmaken van websites/of e-mail	37% -	36% -
Er worden in het kader van een educatie programma op willekeurige momenten test-emails verstuurd om medewerkers te testen op herkenning van phishing	34%	32%
De toegang tot bepaalde websites en/of socialmediakanalen is geblokkeerd	34%	33% -
Er zijn regels over het gebruikmaken van websites/of e-mail	31% -	33% -
Er zijn adviezen/richtlijnen over het gebruikmaken van sociale media	29% -	27%
Er zijn afspraken gemaakt over het gebruikmaken van opslagmedia als usb-sticks of externe harde schijven	27% -	26% -
Er zijn regels over het gebruikmaken van sociale media	26%	24% -
Het gebruik van USB-sticks in onze organisatie is onmogelijk gemaakt	22%	19%
De toegang tot bepaalde verzendplatforms (zoals WeTransfer) is geblokkeerd	15%	20%
Er is een verzekering afgesloten tegen de financiële gevolgen van cybercrime	4%	5%
Anders	4%	2%
In mijn bedrijf of organisatie is geen enkele actie ondernomen ten behoeve van veilig online gedrag	0%	1%
Weet ik niet	15% +	18%

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager). Significante verschillen tussen 2023 en 2022 zijn aangegeven met '+' (toename) en '-' (afname).

Afspraken naleven is voor vier op vijf ambtenaren makkelijk

- Vier op de vijf ambtenaren vinden het goed als collega's hen erop aanspreken als ze zich niet aan de afspraken voor veilig gedrag houden.
- Ook vier op de vijf ambtenaren vinden het makkelijk om zich aan de afspraken te houden en krijgt naar eigen zeggen toegang tot goede tools voor veilig online gedrag.
- Een derde vindt dat zijn leidinggevende het goede voorbeeld geeft, maar ook een derde weet dat niet.

Vergelijking met 2022

- Er zijn geen verschillen in vergelijking met vorig jaar.

Vergelijking grootbedrijf

- Medewerkers van het grootbedrijf vinden minder vaak dan ambtenaren dat ze toegang hebben tot goede tools voor veilig online gedrag. Wel zijn de afspraken voor hen duidelijker en worden deze volgens hen ook beter toegepast.

In hoeverre bent u het eens of oneens met de volgende stellingen? % (zeer) eens. Voorgelegd aan personen waar afspraken zijn gemaakt.	**Ambtenaren (n=317)**	**Medewerkers grootbedrijf (n=543)**
Ik vind het goed als collega's mij erop aanspreken als ik me niet houd aan de werkafspraken over veilig online gedrag	83%	80%
Ik krijg toegang tot goede tools en instrumenten (bijvoorbeeld twee-staps-inloggen of een wachtwoordmanager) om veilig online gedrag te bevorderen	83%	76%
Het is gemakkelijk om mij aan de afspraken te houden over veilig online gedrag binnen mijn bedrijf of organisatie	83%	86%
De afspraken over hoe ik me online veilig moet gedragen op mijn werk vind ik duidelijk	76%	82%
De afspraken over veilig online gedrag die binnen mijn organisatie/bedrijf zijn gemaakt, worden voldoende toegepast	63%	73%
Ik word er op mijn werk op aangesproken als ik me niet aan de werkafspraken houd over veilig online gedrag	45%	51%
Ik spreek collega's er op aan als zij zich niet houden aan de werkafspraken over veilig online gedrag	45%	46%
Mijn leidinggevende geeft het goede voorbeeld als het gaat om veilig online gedrag	38%	44%

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager).

Vrijwel alle ambtenaren melden het als ze een virus downloaden

- Vrijwel alle ambtenaren melden het bij de ICT-afdeling als ze een virus downloaden.
- Daarnaast loggen vier op de vijf uit na gebruik van een openbare computer en heeft driekwart de privacy-instellingen van sociale media aangepast.
- Zes op de tien ambtenaren zouden zich schamen om in phishing te trappen en 10 procent zou het niet aan anderen vertellen als ze per ongeluk een virus downloaden.

Vergelijking met 2022

- In 2023 maken ambtenaren en hun werkgevers vaker back-ups. Ook hebben ze vaker dan vorig jaar een externe opslag thuis die continu online is.

Vergelijking grootbedrijf

- Medewerkers in het grootbedrijf hebben minder vaak de privacy-instellingen van hun sociale media aangepast.

In hoeverre zijn de volgende uitspraken van toepassing op uw gedrag?	Ambtenaren (n=371)	Medewerkers grootbedrijf (n=674)
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%	97%
Mijn werkgever maakt automatisch back-ups van alle bestanden (volledige back-ups)	93% +	95% +
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 anderen wat ik heb gedaan	92%	92%
Als ik een openbare computer heb gebruikt dan log ik na gebruik al mijn accounts uit (bank, social media en e-mail)	85%	87%
Ik heb de privacy instellingen van mijn social media accounts aangepast ten opzichte van de standaardinstellingen	78% +	72%
Ik let op of er een slotje en/of https bij het webadres staat	66%	69%
Als ik op een link in een phishing e-mail zou klikken dan zou ik mij daarvoor schamen	62%	56%
Ik maak thuis regelmatig back-ups van mijn bestanden	52%	50%
Ik maak op mijn werk regelmatig back-ups van de bestanden op mijn werklaptop	39% +	40%
Ik maak thuis gebruik van een extern opslagapparaat dat continu online is	19% +	19% +
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 uit schaamte niet aan anderen wat ik heb gedaan	10%	12%
Ik verstuur werkbestanden van mijn werk e-mailadres naar mijn privé e-mail	7%	7%
Als ik getroffen zou worden door ransomware (gijzelsoftware) en gevraagd wordt om te betalen om weer toegang tot mijn persoonlijke bestanden te krijgen, dan zou ik daarvoor betalen	3%	4%

* Nieuwe stelling in 2023.
Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager). Significante verschillen tussen 2023 en 2022 zijn aangegeven met '+' (toename) en '-' (afname).

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 weinig aansprekende communicatie of onvoldoende communicatie.
- Daarna noemt men vooral dat de afspraken en de borging ervan onduidelijk zijn.

Vergelijking grootbedrijf

- Medewerkers van het grootbedrijf ervaren weinig aansprekende communicatie en gebrek aan tijd minder als belemmering.

Welke van onderstaande belemmeringen ervaart u binnen uw bedrijf/organisatie bij het borgen van de afspraken voor online veilig gedrag?	Ambtenaren (n=160)	Medewerkers grootbedrijf (n=277)
Er wordt niet aansprekend over gecommuniceerd	16%	5%
Er wordt niet voldoende over gecommuniceerd	12%	9%
Het is niet duidelijk bij wie de borging van deze afspraken ligt	11%	8%
Er wordt niet duidelijk over gecommuniceerd	10%	8%
Te weinig tijd	9%	4%
Er wordt geen prioriteit aan gegeven	9%	6% -
Er is geen duidelijk aanspreekpunt binnen de organisatie	8%	5%
Er wordt niet eenduidig (door verschillende afdelingen) over gecommuniceerd	6%	4%
Te weinig menskracht	4%	4%
Te weinig kennis binnen de organisatie	4%	4%
Gebrek aan draagvlak vanuit het management	4%	3%
Te weinig budget	3%	2%
Ik ervaar geen belemmeringen bij het borgen van de afspraken over veilig online gedrag	46%	52%
Weet ik niet	21%	23% +

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager). Significante verschillen tussen 2023 en 2022 zijn aangegeven met '+' (toename) en '-' (afname).

Vergroten kennis kan borging gedragsregels verbeteren, maar winst gemaakt ten opzichte van 2022

- 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 2022

- Men noemt het vergroten van de kennis, een hogere prioriteit, meer draagvlak en beter afgestemde communicatie minder dan in 2022. Hieruit blijkt impliciet dat men vindt dat deze maatregelen beter worden toegepast dan destijds.

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=160)	Medewerkers grootbedrijf (n=277)
Vergroten kennis hierover binnen de organisatie	41% -	33% -
Cyberoefenen	28%	31%
Meer communicatie	24%	17%
Bedrijf (periodiek) laten doorlichten (externe audit) op cybersecurity door experts (voor ondernemers)	23%	20%
Een duidelijk aanspreekpunt binnen de organisatie	20%	17%
Duidelijkere communicatie	19% -	18% -
Een of meer ICT experts in de organisatie	17%	14%
Communicatie aantrekkelijker maken	14%	10%
Beter vastleggen wie verantwoordelijk is voor welke afspraken	13%	8%
Hogere prioriteit	10% -	8% -
Meer draagvlak vanuit het management	8% -	7%
Communicatie beter op elkaar afstemmen	7% -	11%
Meer tijd	6%	5%
Anders	5%	2%
Meer budget	4%	4%
Meer menskracht	4%	3%
Ik zie geen mogelijkheden om de afspraken over veilig online gedrag beter te borgen	11%	11%
Weet ik niet	12%	18%

Significante verschillen tussen 2023 en 2022 zijn aangegeven met '+' (toename) en '-' (afname).

5. Slachtofferschap en aangiftebereidheid

Phishing meest meegemaakte vorm van cybercrime op het werk

- Drie op de tien van de ambtenaren maakten in de afgelopen 12 maanden een poging tot cybercrime mee op het werk.
- Een kwart maakte een poging tot phishing mee. Vier procent werd benaderd voor WhatsApp-fraude en ook vier procent kreeg een neptelefoontje.

Vergelijking met 2022

- Ook in 2022 was phishing het meest meegemaakte incident.
- Ambtenaren hebben nu iets vaker te maken met WhatsAppfraude dan een jaar eerder.

Vergelijking grootbedrijf

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

Heeft u in de afgelopen 12 maanden zelf weleens te maken gehad met een van de onderstaande voorvallen in uw werksituatie?	Ambtenaren (n=371)	Medewerkers grootbedrijf (n=674)
Mails ontvangen met poging tot phishing	24%	24%
Benaderd via WhatsApp door iemand die zich voordeed als een bekende die probeerde geld te ontvangen	4% +	2%
Gebeld door iemand die zich voordeed als bedrijf of officiële instantie om geld of gegevens te bemachtigen	4%	2% -
Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik die bijna niet van echt te onderscheiden is	3%	3%
Benaderd op social media met een vraag om een onbekende link aan te klikken	1%	2%
Dat door het downloaden van geïnfecteerde software/bestanden malware verspreid werd (o.a. via een e-mail)	1%	0,6%
Acquisitiefraude	1%	0,9%
Een foute link ook daadwerkelijk hebben aangeklikt in de zin dat deze een virus, spam, phishing of andere ongewenste poging tot cybercrime bevatte	1%	1%
Dat iemand dreigde mijn bestanden te openbaren of dit ook echt deed	0,8%	0,6%
Dat iemand in een apparaat heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	0,5%	0,0%
Ransomware	0,3%	0,3%
Identiteitsdiefstal	0,3%	0,1%
Dat een computer tijdelijk niet werkte door malware zoals bijvoorbeeld een virus	0,3%	1,0%
Dat iemand in een account heeft ingelogd zonder dat u daar toestemming voor gegeven heeft	0,0%	0,1%
Geen van deze voorvallen	69%	72%

Significante verschillen tussen 2023 en 2022 zijn aangegeven met '+' (toename) en '-' (afname).

Vier op de tien ambtenaren doen geen aangifte of melding van incident op werk

- De helft van de ambtenaren die een incident meemaakten, meldde dit bij de ICT-afdeling.
- Vier op de tien deed geen aangifte of melding
- Drie procent deed aangifte bij de politie.

Vergelijking grootbedrijf

- Medewerkers van het grootbedrijf doen vaker aangifte of melding bij een meegemaakt incident.
- Ze maken vooral vaker een melding bij de ICT-afdeling en doen ook vaker aangifte bij de politie.

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=116)	Medewerkers grootbedrijf (n=187)
Ja, melding bij de ICT-afdeling van mijn bedrijf	49%	61% +
Ja, melding bij de Fraudehelpdesk	8%	5%
Ja, melding bij het Nationaal Cyber Security Centrum (NCSC)	4%	2%
Ja, aangifte bij de politie	3%	4%
Ja, melding bij de politie	3%	3% +
Ja, melding bij mijn gemeente	3%	1%
Ja, bij een andere organisatie	3%	2%
Ja, melding bij SeniorWeb	0%	0%
Nee, ik heb hier niks mee gedaan	41%	30% -

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager). Significante verschillen tussen 2023 en 2022 zijn aangegeven met '+' (toename) en '-' (afname).

Helft doet melding om veiliger online omgeving te creëren

- De voornaamste reden van aangifte of melding is om een veiliger online omgeving te creëren en om te voorkomen dat de dader dit opnieuw kan doen.
- Een derde ziet het als plicht om aangifte of melding te doen.
- Een op de vijf noemt te willen voorkomen het opnieuw mee te maken.

Vergelijking grootbedrijf

- Medewerkers van het grootbedrijf noemen dit (voorkomen het opnieuw mee te maken) vaker dan ambtenaren en ook vaker dan in 2022.

Wat is de belangrijkste reden om wel aangifte of melding te doen? (maximaal 3)	Ambtenaren (n=68)	Medewerkers grootbedrijf (n=131)
Om een veiligere (online) omgeving te creëren	56%	61%
Voorkomen dat de dader dit opnieuw bij een ander kan doen	53%	58%
Het voelt als een plicht om aangifte of een melding te doen	32%	31%
Voorkomen dat dit opnieuw bij mij gebeurt	21%	37% +
Dat wordt door iemand anders afgehandeld/beslist	21%	18%
Ik wil dat de dader gepakt wordt	16%	22%
Om de schade vergoed te krijgen	3%	6%
Anders	3%	3%
Weet ik niet	1%	2%

Significante verschillen tussen ambtenaren en medewerkers grootbedrijf zijn aangegeven met groen (hoger) en rood (lager). Significante verschillen tussen 2023 en 2022 zijn aangegeven met '+' (toename) en '-' (afname).

Geen aangifte: twee op de vijf ondervonden weinig gevolgen van incident

- Een klein aantal ambtenaren heeft geen aangifte of melding gedaan.
- De belangrijkste reden om geen actie te ondernemen is dat men weinig of geen schade ondervond van het incident.
- Een kwart noemt dat ze zelf niet de beslissing nemen om een melding of aangifte te doen.

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=48*)	Medewerkers grootbedrijf (n=56)
Ik ondervond geen of weinig schade	40%	32%
Dat wordt door iemand anders afgehandeld/beslist	23%	29%
Het heeft geen zin, er wordt niets gedaan met de aangifte of melding	13%	16%
Ik los het zelf op	8%	4%
Het is niet zo belangrijk	8%	7%
Het kost te veel moeite	8%	9%
Ik heb weinig vertrouwen in de instanties om aangifte of een melding te doen	8%	4%
Er is niet de kennis om dit type delict aan te pakken	2%	0%
Ik weet niet bij welke instantie ik moet zijn voor het oplossen van dit type delict	2%	4%
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%	0%
Ik wilde aangifte doen maar dit werd mij afgeraden	0%	0%
Anders	15%	14%
Weet ik niet	8%	13%

*Indicatieve uitkomsten vanwege laag aantal waarnemingen.

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