# Sectorrapportage 2023

## Over security en privacy awareness in onderwijs en onderzoek

Oktober 2023

SURF

IBDO

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

# Samenvatting

## Introductie

- In opdracht van SURF heeft BDO voor het derde jaar op rij security- en privacy-awarenessmetingen uitgevoerd bij onderwijs- en onderzoeksinstellingen.
- De metingen zijn gebaseerd op het COM-B model voor gedragsverandering. Kort gezegd luidt deze: om te veranderen is het nodig dat mensen kunnen (bekwaamheid), willen (motivatie) en gefaciliteerd worden (gelegenheid).
- De metingen bestaan uit online vragenlijsten voor de medewerkers en voor de sectorrapportage zijn acht interviews gehouden.
- MBO Digitaal voerde gelijktijdig een vergelijkbare awarenessmeting uit, de resultaten zijn meegenomen in dit rapport.

## Gedragsmeting

Er is dit jaar een extra meting toegevoegd, een gedragsmeting door onderzoekers van de Haagse Hogeschool. De gedragsmeting bevat twee testen. Deze gaan over 1) het aanmaken van een veilig wachtwoord en 2) het delen van persoonlijke informatie. Het doel is om te kijken wat de relatie is tussen de resultaten van de ‘basismeting’ (op basis van COM-B) en van de gedragsmeting.

## Resultaten

- Deelnemende instellingen: 70 • Aantal respondenten: 12.343


## Conclusies

1. Over de hele linie zijn de resultaten beter dan vorig jaar, maar deze zijn nog niet voldoende en men is minder positief over de voorbeeldrol van leidinggevenden;
2. Men is nog steeds overtuigd van het belang, maar beperkt gemotiveerd om aandacht te besteden aan security en privacy;
3. Er is redelijke tevredenheid over faciliteiten, maar een sterke security-cultuur ontbreekt;
4. De kennis over informatieveiligheid is matig tot redelijk, er is vooral behoefte aan helderheid en ondersteuning;
5. Gedragsmeting: er is een zeer beperkt verband tussen COM-B en daadwerkelijk veilig gedrag;
6. De doelgroep IT-ondersteuning behaalt de hoogste resultaten.

## Aanbevelingen

1. Zorg dat awarenessinstrumenten aansluiten bij het dagelijkse werk van medewerkers;
2. Neem barrières voor veilig werken weg;
3. Investeer in een sterke security-cultuur;
4. Focus in metingen en interventies op daadwerkelijk gedrag van medewerkers;
5. Maak security en privacy een vast onderdeel van onboarding;
6. Houd rekening met de sceptici;
7. Investeer extra in docenten, onderzoekers en leidinggevenden;
8. Focus op specifieke thema’s zoals veilige software, delen en opslaan van persoonsgegevens en datalekken.

# INHOUDSOPGAVE



# Inleiding

# Inleiding

## Introductie

Het grootste deel van security incidenten en datalekken hebben te maken met menselijk gedrag [bron: DBIR 2023]. Voorbeelden zijn het afgeven van inloggegevens bij social engineering, klikken op een phishing mail, het downloaden van malware en het verliezen van een laptop met persoonsgegevens. In het SURF Cyberdreigingsbeeld 2023 is “onveilig gedrag en gebrek aan awareness” voor het eerst toegevoegd als risicocategorie. Voldoende reden voor SURF om (ook dit jaar) awarenessmetingen uit te voeren bij instellingen in de sector onderwijs en onderzoek. Dit jaar zijn er twee wijzigingen in de opzet van de metingen.

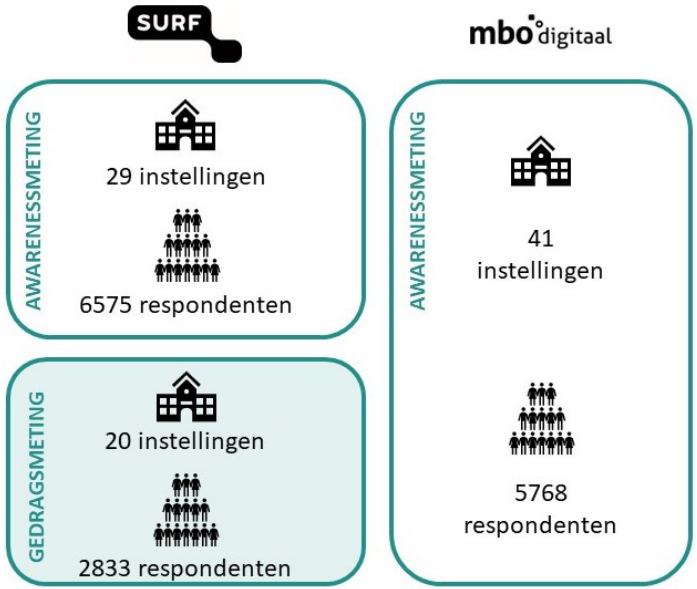
### 1. Benchmarkmetingen MBO Digitaal en SURF

Naast SURF heeft ook MBO Digitaal (MBO Raad) dit jaar een eigen benchmarkmeting uitgevoerd. Deze sectorrapportage bevat de resultaten van beide benchmarkmetingen. Voor beide benchmarkmetingen is een online vragenlijst verspreid onder de deelnemende instellingen. De vragenlijsten van SURF en MBO Digitaal verschillen op enkele onderdelen. In dit rapport worden deze verschillen duidelijk benoemd en de onderdelen apart gepresenteerd.

### 2. Awarenessmeting en gedragsmeting

De reguliere awarenessmeting is dit jaar voor een deel van de instellingen aangevuld met een gedragsmeting, met als doel om daadwerkelijk cyberveilig gedrag te meten. De gedragsmeting is onderdeel van de SURF benchmarkmeting en is uitgevoerd door onderzoekers van de Haagse Hogeschool. In hoofdstuk 8 wordt de gedragsmeting verder toegelicht.

De opzet staat schematisch weergegeven in onderstaande figuur.




*Figuur 1: Deelnemers awarenessmeting en gedragsmeting*

# Inleiding (2)

## Over de auteurs

Dit rapport is tot stand gekomen in samenwerking tussen SURF, BDO en de Haagse Hogeschool.

- **SURF**
  SURF ondersteunt onderwijs- en onderzoeksinstellingen op het gebied van awareness en training. Door het stimuleren van kennisdelen tussen instellingen en materiaal aan te bieden in de Cybersave Yourself Toolkit. De awarenessmeting helpt instellingen om zicht te krijgen op hoe bewust hun medewerkers zijn.
  Rosanne Pouw is Product Manager Awareness & Training.

- **BDO Cybersecurity**
  BDO ondersteunt organisaties bij het versterken van hun digitale weerbaarheid. Hiervoor heeft de organisatie een integrale aanpak ontwikkeld, gericht op het optimaal beheersen van risico's.
  Marijke Stokkel is als senior manager werkzaam binnen het team Cybersecurity en verantwoordelijk voor de propositie security & privacy awareness.

- **Centre of Expertise Cyber Security, de Haagse Hogeschool**
  In het Centre of Expertice Cyber Security wordt hoogwaardig toegepast wetenschappelijk onderzoek uitgevoerd, waarbij de wetenschap, praktijk en onderwijs worden samengebracht. De missie van het kenniscentrum Cyber Security is het versterken van de cyberveerkracht van publieke en private organisaties die zelf in mindere mate zijn toegerust op cyberdreigingen.
  Susanne van 't Hoff-de Goede is criminoloog en senior onderzoeker bij het Centre of Expertise Cyber Security van de Haagse Hogeschool.
  Maaike van der Wal is criminoloog en junior onderzoeker bij het Centre of Expertise  Cyber Security van de Haagse Hogeschool.

# Aanpak

# Aanpak awarenessmetingen (1)

Het afgelopen voorjaar heeft BDO bij in totaal 70 instellingen security- en privacy-awarenessmetingen uitgevoerd. Voor de hogescholen, universiteiten en overige instellingen zijn deze geïnitieerd via SURF. Voor de MBO-scholen fungeerde het platform MBO Digitaal als opdrachtgever.

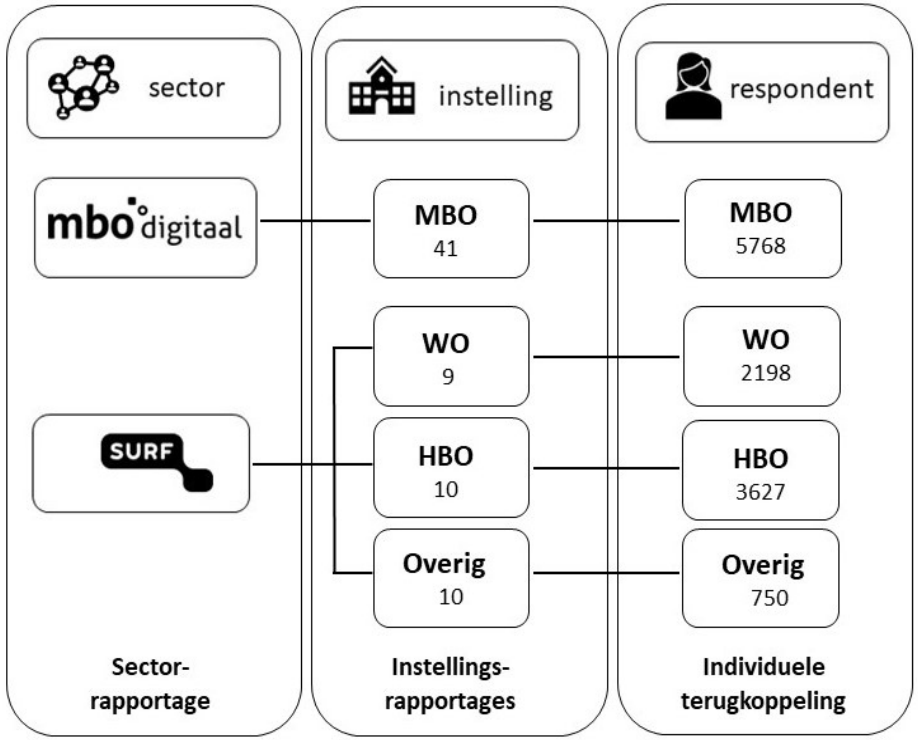
Dit hoofdstuk beschrijft de aanpak van de metingen. Het bevat:

- De opbouw van de metingen;
- Het gedragsmodel waarop de meting gebaseerd is;
- De centrale onderzoeksvragen;
- De werkwijze, inclusief terminologie en doelgroepen.

## Opbouw metingen

De metingen geven op drie niveaus inzicht:

- De ***individuele respondent*** krijgt bij het invullen van de online vragenlijst terugkoppeling over de toetsvragen, met advies over informatieveilig werken.
- De ***instelling*** ontvangt een awarenessrapport met bevindingen, conclusies en aanbevelingen voor gerichte verbeteringen.
- De ***hele sector***. Op basis van de rapportages van de deelnemende instellingen plus acht interviews hebben we deze sectorrapportage opgesteld.

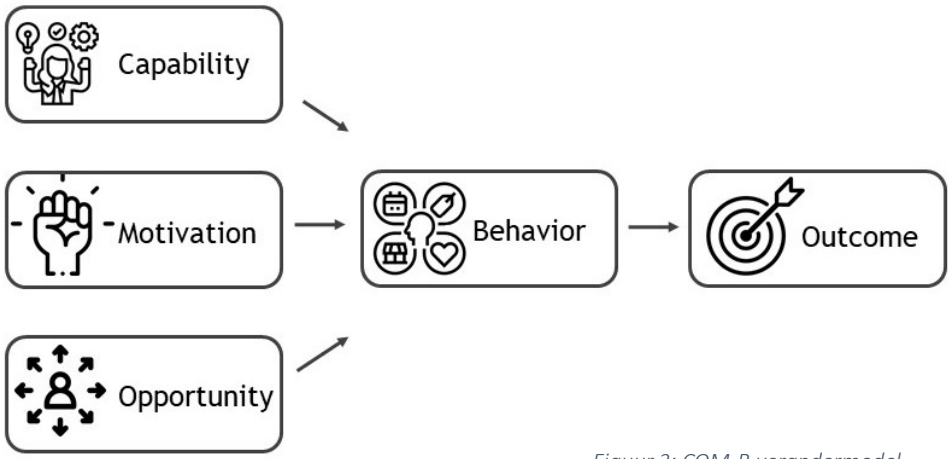



*Figuur 2: Drie niveaus van inzicht*

# Aanpak awarenessmetingen (2)

## Gedragsmodel COM-B

Om informatieveilig en privacybewust gedrag in kaart te brengen maakten we net als in 2021 en 2022 gebruik van het COM-B gedragsmodel van Susan Michie. Het COM-B gedragsmodel is een hulpmiddel om gedrag te begrijpen en te verklaren. Het model stelt dat gedrag en gedragsverandering beïnvloed wordt door drie componenten: bekwaamheid (capability), gelegenheid (opportunity) en motivatie (motivation).




*Figuur 3: COM-B verandermodel*

- **C - Capability (bekwaamheid):** dit verwijst naar de vaardigheden, kennis en fysieke mogelijkheden van een persoon om een bepaald gedrag uit te voeren. Bekwame medewerkers kunnen risico's herkennen, weten wat te doen bij een datalek zijn in staat om de juiste handelingen uit te voeren.
- **O - Opportunity (Gelegenheid):** dit heeft betrekking op de externe omstandigheden die iemand in staat stellen om het gewenste gedrag te vertonen. Medewerkers weten wat er van hen wordt verwacht, krijgen de juiste tools en middelen aangereikt en hebben een leidinggevende die informatieveilig gedrag beloont. Veilig werken wordt makkelijk gemaakt, zonder veel extra handelingen en andere barrières.
- **M - Motivation (Motivatie):** dit verwijst naar de (intrinsieke) motivatie van de medewerkers om informatieveilig en privacybewust te werken. Gemotiveerde medewerkers willen zich daar uit eigen overtuiging voor inzetten, niet omdat ze bang zijn voor negatieve consequenties.

Samen vormen deze drie componenten het COM-B model, dat helpt om gedrag te analyseren en strategieën te ontwikkelen om gedragsverandering te bevorderen.

# Aanpak awarenessmetingen (3)

## Onderzoeksvragen

De vragen van de meting sluiten aan bij het gedragsmodel dat we hanteren en luiden als volgt:

- In hoeverre willen medewerkers informatieveilig en privacybewust werken (motivatie)?
- In hoeverre worden medewerkers in staat gesteld om informatieveilig en privacybewust te werken (gelegenheid)?
- In hoeverre kunnen medewerkers informatieveilig en privacybewust werken (bekwaamheid)?

## Werkwijze

De metingen zijn uitgevoerd via een online vragenlijst en interviews. De vragenlijst is geschikt om een globaal inzicht te krijgen in het (zelfgerapporteerde) gedrag en de kennis, de mening en ervaringen. De interviews zorgen voor extra duiding en diepgang. De interviews zijn specifiek voor de sectorrapportage gehouden.
De online vragenlijst bevat zogenaamde meningvragen en quizvragen, waarbij meningvragen bedoeld zijn om motivatie en gelegenheid te onderzoeken. Met de quizvragen wordt bekwaamheid getoetst.

De respondenten ontvingen na het invullen van de meting direct terugkoppeling over hun quizresultaten, met advies voor (verdere) verbetering. Op deze wijze is de awarenessmeting een awarenessinterventie en meetinstrument in één.

De vragenlijsten zijn in april en mei uitgezet bij ruim 80 instellingen. Hiervan hebben 70 instellingen actief deelgenomen aan de meting. In totaal zijn er 12.343 vragenlijsten ingevuld en we hebben acht interviews gehouden met medewerkers van verschillende instellingen. De interviews vonden plaats in juni en juli.

## Terminologie

Security en privacy zijn separate domeinen, maar hebben veel overlap. In de meting hanteren we de term *“informatieveiligheid”*, waarbij we zowel security als privacy bedoelen. De term informatieveiligheid bestaat in de benchmarkmetingen uit:

- **privacy:** waarborgen dat de persoonsgegevens die studenten, medewerkers en andere betrokkenen ons toevertrouwen, in goede handen zijn,
- **security:** beschermen van informatie(systemen) om een digitaal weerbare organisatie te kunnen zijn.

# Aanpak awarenessmetingen (4)

## Doelgroepen

De metingen bestaan uit de volgende doelgroepen:

**MBO Digitaal**

- Leidinggevend
- Uitvoerend

- Onderwijs
- Ondersteuning

**SURF**

- Leidinggevend
- Uitvoerend

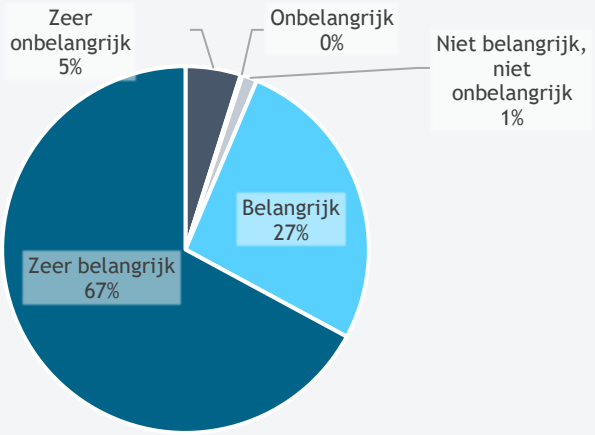
- Onderwijs/onderzoek
- Ondersteuning
- IT ondersteuning
- Overig

In het meting wordt per doelgroep gekeken of er verschil is in resultaten.

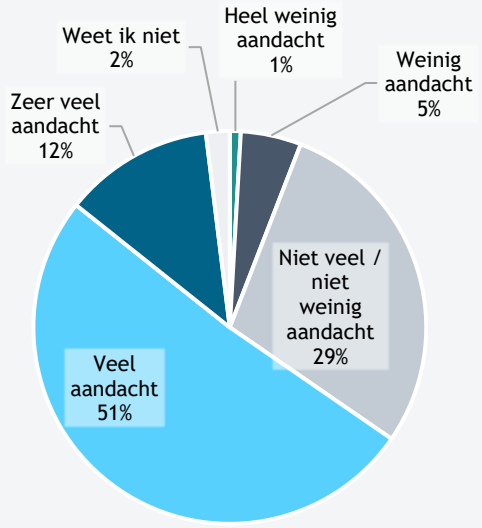

Resultaten

# Resultaten - motivatie

**Hoe belangrijk vind jij informatie-veiligheid voor jouw instelling?**




**Hoeveel aandacht besteed jij over het algemeen tijdens je werk aan informatieveiligheid?**




Dit hoofdstuk beschrijft de resultaten van de awarenessmeting per component en vervolgens in cijfers. We starten met het component ‘motivatie’.

Om de motivatie van medewerkers te onderzoeken, hebben we de respondenten meerdere vragen gesteld waarmee het thema motivatie vanuit meerdere perspectieven bekeken wordt.

> *“We zijn het de studenten verschuldigd om zorgvuldig met hun gegevens om te gaan”*

## Belangrijk en aandacht

Respondenten zeggen veel belang te hechten aan informatieveiligheid. Maar liefst 94% vindt het thema ‘belangrijk’ of ‘zeer belangrijk’ voor de eigen instelling. Ook zegt een meerderheid van de respondenten -maar wel een lager percentage- ‘zeer veel aandacht’ of ‘veel aandacht’ te besteden aan informatieveiligheid tijdens hun werk (63%). Voor instellingen die met security- en privacy awarenessprogramma’s het informatieveilig werken (verder) willen verbeteren, vormen deze resultaten een goede basis.

# Resultaten - motivatie (2)

## Belang voor collega's

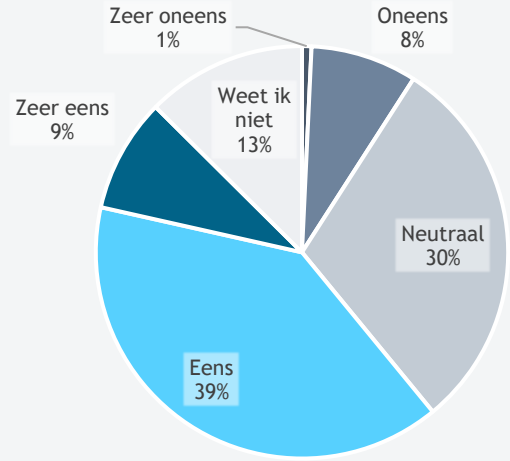
Een minderheid van de respondenten (48%) is het (zeer) eens met de stelling 'binnen mijn instelling hechten medewerkers veel belang aan informatieveiligheid'. Dat is een zeer groot verschil met belang dat zij hier zelf aan zeggen te hechten. De vraag die hierbij opkomt is of men de motivatie en het informatieveilige gedrag van collega's onderschat, of wellicht het eigen gedrag overschat.

## Waarom aandacht informatieveiligheid

De redenen dat medewerkers aandacht besteden aan informatieveilig werken zijn aardig divers. Een reden die minder speelt, is persoonlijke interesse. Op de vraag of men uit interesse nieuwe ontwikkelingen volgt op het gebied van informatieveiligheid, antwoordt een minderheid (44%) hierop bevestigend. En op de vraag waarom men aandacht besteedt aan informatieveiligheid, kiest slechts 4% (ook) het antwoord 'ik vind het leuk en interessant'.

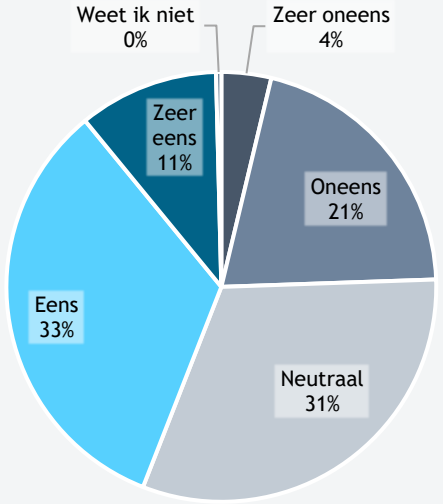
> *"Ik wil niet dat informatie van wie dan ook (studenten, collega's, externen) ongewenst bij derden belandt."*

De meestgenoemde reden is 'ik zou me schamen als er door mij een incident of datalek zou ontstaan' (24%) gevolgd door 'het is nodig om mijn instelling digitaal weerbaar te maken' (19%).

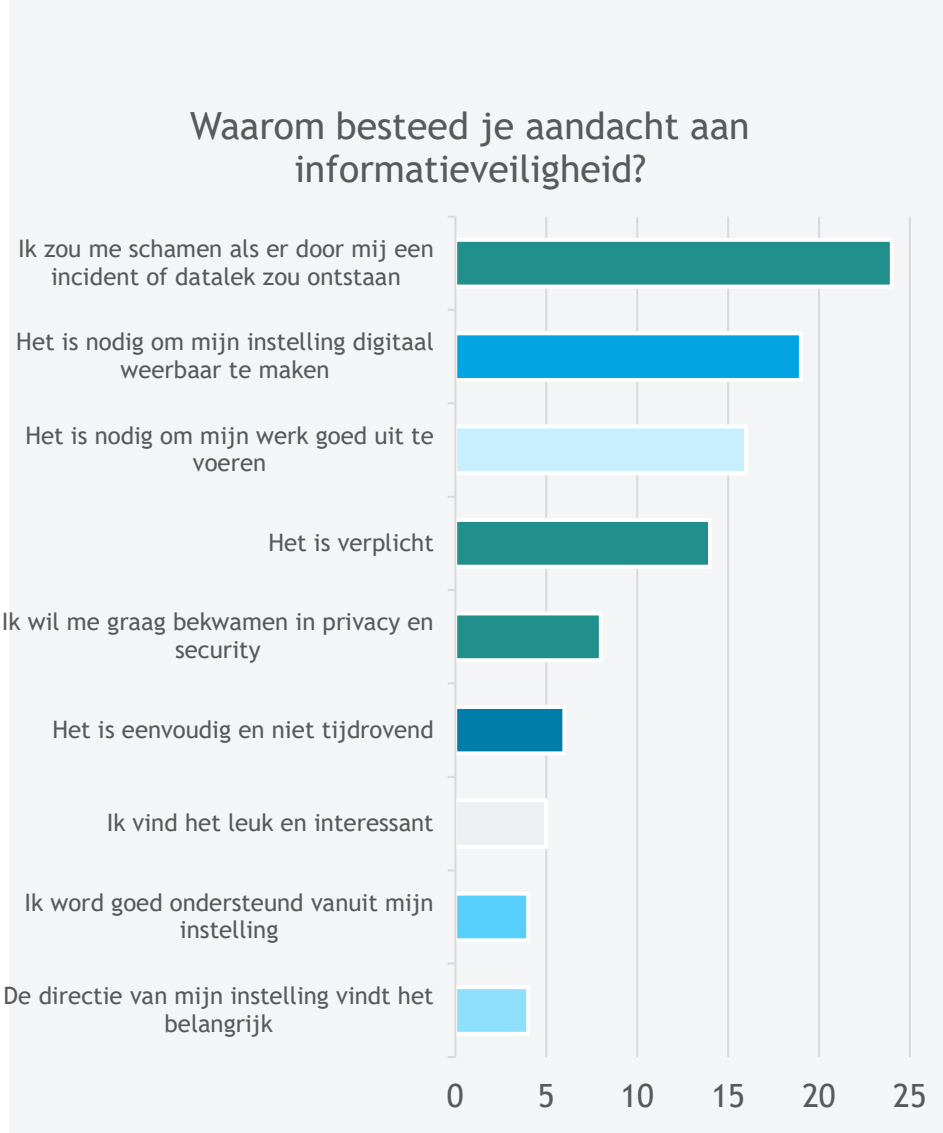



**Stelling: binnen mijn instelling hechten medewerkers veel belang aan informatieveilig heid.**

**Stelling: uit interesse volg ik nieuwe ontwikkelingen op het gebied van informatieveilig heid.**



# Resultaten - motivatie (3)




In de vragenlijst kregen respondenten de mogelijkheid om te schrijven waarom zij aandacht besteden aan informatieveiligheid. Een selectie:

- Het is onmisbaar als je met het internet werkt.

  *"Het is "good practice" net zoals je handen wassen nadat je naar de WC bent geweest"*

- Eigen ervaring met een incident.

  *"Omdat ik ooit heb meegemaakt dat er door een datalek informatie op straat gelegen had, waardoor een agressieve ex-man achter het adres van zijn ex-vrouw in het Blijf van mijn Lijf-huis kwam."*

- Begeleiden en beschermen van studenten

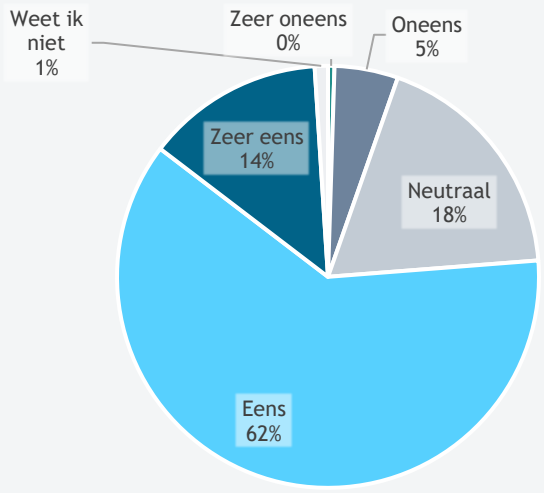
  *"Ik vind het vanuit mijn rol als docent belangrijk om vertrouwelijk met de gegevens van studenten om te gaan"*

- Reputatie instelling

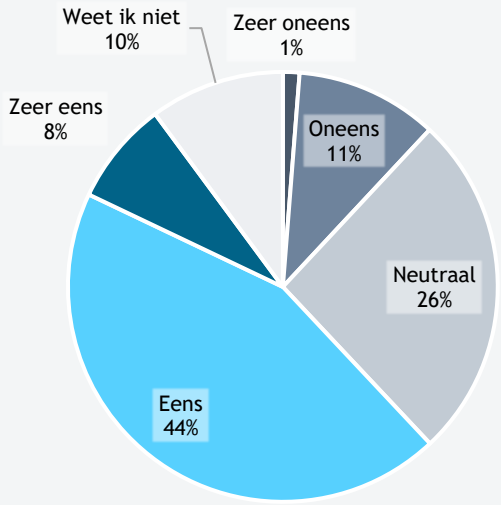
  *"Je wilt als organisatie geen onderdeel worden van een datalek, dat hierdoor privacy-gerelateerde gegevens van personen op straat komen te liggen en op een negatieve manier de landelijke media halen ivm een beveiligingslek"*

# Resultaten - gelegenheid (1)

**Ik weet hoe ik in mijn dagelijkse werk invulling moet geven aan informatieveilig werken**




**Mijn instelling heeft duidelijke gedragsregels voor informatieveilig werken**




Voor het component 'gelegenheid' hebben we de respondenten een aantal stellingen voorgelegd. Deze gaan over informatieveilig werken, over gedragsregels, over gefaciliteerd worden met software en middelen en over de voorbeeldrol van leidinggevenden.

### Dagelijkse leven en duidelijke gedragsregels

Een meerderheid van de respondenten (76%) zegt te weten hoe ze in het dagelijks leven invulling moeten geven aan informatieveilig werken. Aan de andere kant is slechts een krappe meerderheid (52%) het (zeer) eens met de stelling dat de instelling duidelijke gedragsregels heeft voor informatieveilig werken. Mogelijk weten de respondenten wat ze moeten doen, ook al zijn er geen duidelijke gedragsregels. In de open antwoorden meldden meerdere respondenten dat ze kennis hebben opgedaan bij de vorige werkgever, en dat er bij de huidige instelling weinig aandacht is voor het thema. Dat zou een verklaring kunnen zijn.

> *"Vanuit mijn vorige baan heb ik veel kennis. Binnen de [naam instelling] hoor en zie ik er weinig over."*

Een andere mogelijke verklaring is dat respondenten wel zeggen (en denken) te weten hoe ze informatieveilig moeten werken, maar dat dat in de praktijk niet of minder het geval is.

# Resultaten - gelegenheid (2)

## Goed gefaciliteerd

Een meerderheid van 60% is het (zeer) eens met de stelling ‘ik word goed gefaciliteerd door mijn instelling om informatieveilig te kunnen werken.’ Velen zeggen daarbij dat er de vooral de afgelopen paar jaar veel vooruitgang is geboekt. Sommigen vinden het lastig om de vraag te beantwoorden, omdat ze zeggen niet te weten wat een goede ondersteuning inhoudt. Anderen vinden dat het vooral een taak van de instelling is om hier inzicht in te hebben.

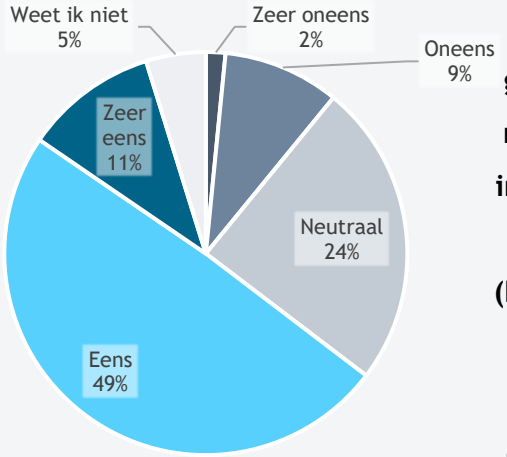
> *“Ik vertrouw erop dat als ik de soft- en hardware van mijn werkgever gebruik, ik informatieveilig werk. ik heb ook geen andere keus: mijn baan is echt te druk om dit ook nog zelf te moeten uitzoeken.”*

Daarnaast worden ook inhoudelijke aandachtspunten genoemd.

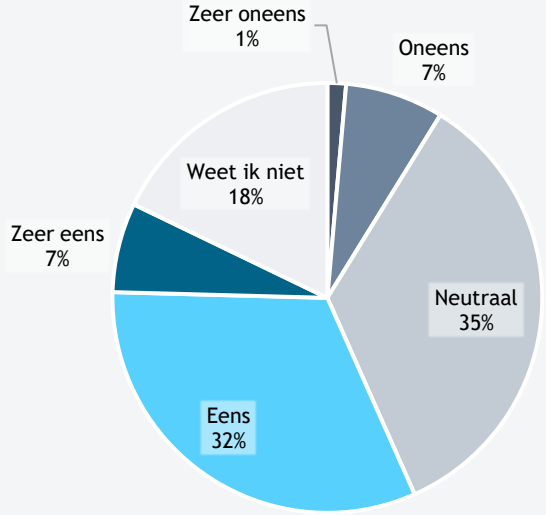
- Men heeft behoefte aan een (verplichte) door de instelling beheerder passwordmanager.
- De gedragsregels en andere richtlijnen zijn moeilijk vindbaar. Er is veel eigen initiatief nodig om informatie over informatieveiligheid te krijgen.

> *“Er zijn wel tools/instructies aanwezig, maar hier moet je wel eigenhandig naar 'op zoek.' Als je geen kennis/kunde hebt van dit onderwerp kan het dus best misgaan.”*

**Ik word goed gefaciliteerd door mijn instelling om informatieveilig te kunnen werken (bijvoorbeeld door software, tools, instructies, en andere middelen)**




**Mijn leidinggevende geeft mij het juiste voorbeeld als het gaat om informatieveilig werken.**



# Resultaten - gelegenheid (3)

Vervolg aandachtspunten:

- Men plaatst vraagtekens bij de veiligheid van MS Teams en andere Microsoft software. Respondenten vragen zich af of het wel veilig is om (o.a.) studentgegevens te delen via MS Teams.

  "*Verder werken we steeds meer met Microsoft Teams, dat vind ik zeer onaangenaam vanwege privacy gevoelige opslag in de cloud, en tracking van mijn online activity door zo'n gigant. Maar het is verplicht, wat kun je dan doen?*"

- MFA staat volgens respondenten niet altijd goed afgesteld, kost zeer veel tijd en leidt tot irritatie.

  "*Soms moet ik meer dan 10x per dag inloggen met mijn telefoon, echt vervelend*"

- Het delen van bestanden met externen ervaren sommigen als lastig, en daarom wijkt men uit naar tooling zoals WeTransfer.

- Als medewerkers binnen de instelling een andere functie krijgen, nemen ze hun autorisaties mee. Dit dient handmatig aangepast te worden en dat gebeurt veelal niet, merkt een aantal respondenten op. Zo hebben veel medewerkers toegang tot te veel informatie.

### Leidinggevenden

De respondenten zijn beperkt tevreden over de voorbeeldrol van hun leidinggevende op het gebied van informatieveiligheid. Een minderheid van 39% is het (zeer) eens met de stelling "Mijn leidinggevende geeft mij het juiste voorbeeld als het gaat om informatieveilig werken." Leidinggevenden hebben een sturende rol in het informatieveilige gedrag van medewerkers. Als het management de regels omzeilt of een lage prioriteit geeft aan informatieveiligheid, geven zij hiermee een duidelijke boodschap af aan de rest van de organisatie: het is acceptabel om gedragsregels te negeren (bron: NCSC.gov.uk).

"*Teamleiders doen (op mijn locatie) lang niet altijd hun werkruimte op slot als ze weglopen, dat vind ik een risico voor examinering.*"

"*Het onderwerp zou veel meer gaan leven als de direct leidinggevende er aandacht aan schonk. Nu komt er af en toe een mailtje over binnen van ver weg in de organisatie.*"

"*Wat te doen als leidinggevenden niet meewerken aan security / privacy, of dat nonsense vinden, bijv. je bijna verplichten om via whats-app te communiceren. Als je weigert lig je er sociaal uit*".

# Resultaten - bekwaamheid (1)

De vragenlijst van de awarenessmeting bevat acht quizvragen. De quizvragen van de MBO Raad-meting wijken enigszins af ten opzichte van de SURF-meting. De eerste quizvraag is inhoudelijk compleet anders en voor een aantal andere vragen verschillen enkele onderdelen. Daarom presenteren we voor dit component de resultaten van MBO Raad en SURF apart van elkaar. Zie bijlage A en B voor de volledige vragenlijsten.

Naast de quizvragen hebben we de respondenten ook gevraagd over welke thema's zij meer kennis nodig hebben om informatieveilig te kunnen werken.

## Quizvragen - MBO Digitaal

Vijf van de acht vragen werden door de meeste mensen goed beantwoord. Het merendeel van de respondenten gaven op drie vragen een foutief antwoord:

- Datalekherkenning
- Risico's social media
- Sterke wachtwoorden

Op de volgende pagina staat een toelichting per vraag.

# Resultaten - bekwaamheid (2)

### ➢ Datalekherkenning

**Wat is een datalek?**

a) Een e-mail met studentgegevens naar de verkeerde ontvanger sturen
b) Per ongeluk gegevens van studenten wissen in een studentvolgsysteem
c) Een lijst met huisadressen van medewerkers vergeten van de printer te halen

Het juiste antwoord: alle drie de voorbeelden zijn datalekken. Deze vraag is door 87% van de respondenten onjuist beantwoord. De meeste medewerkers hadden er slechts een of twee gekozen. Velen zijn zich er niet van bewust dat het wissen van persoonsgegevens ook een datalek is.

### ➢ Risico's social media

**Waarom is LinkedIn een security risico?**

a) Er is geen multifactorauthenticatie (MFA) mogelijk op LinkedIn accounts
a) Informatie die gebruikers op hun LinkedIn account zetten, kunnen misbruikt worden door oplichters, bijvoorbeeld voor een phishing aanval.
b) Er is geen verificatie op LinkedIn-accounts: iedereen kan zich voordoen als betrouwbare collega of interessante samenwerkings-partner en andere LinkedIn gebruikers zo informatie ontfutselen.

Het juiste antwoord: b en c. Deze vraag is door 73% van de respondenten onjuist beantwoord. Velen dachten dat alle drie de antwoorden juist waren.

### ➢ Sterk wachtwoord herkennen

**Welke van deze wachtwoorden is het sterkst?**

a) EenBroodjeKroketEnEenKaassouffle
b) Welkom2023
c) (6Yh$r#

Het juiste antwoord is a. Deze vraag is ook door 73% onjuist beantwoord. De meeste respondenten dachten c.

### Relatief goed beantwoorde vragen

De volgende vragen werden het best beantwoord.

1. Mag je video-opnamen maken van een les of een online vergadering? -> 96% geeft het juiste antwoord
2. Een docent mag van een student eisen dat deze lid wordt van een Whatsapp-groep van een bepaald vak. -> 82% geeft het juiste antwoord
3. Is deze e-mail template phishing? -> 82% geeft het juiste antwoord

# Resultaten - bekwaamheid (3)

## Quizvragen -SURF

De SURF-meting bevat onderzoek bij HBO-, WO- en 'overige' instellingen. In de meting zijn zes van de acht toetsvragen door de meeste mensen goed beantwoord. Op twee van de acht vragen werd door het merendeel van de respondenten een foutief antwoord gegeven.

- Risico's social media
- Sterke wachtwoorden

### ➢ Risico's social media

**Waarom is LinkedIn een security risico?**

Deze vraag is helemaal gelijk aan de MBO-vraag en is door 68% van de respondenten onjuist beantwoord.

### ➢ Sterk wachtwoord herkennen

**Welke van deze wachtwoorden is het sterkst?**

a) EenBroodjeKroketEnEenKaassouffle
b) Welk()m2023!
c) (6Yh$r#

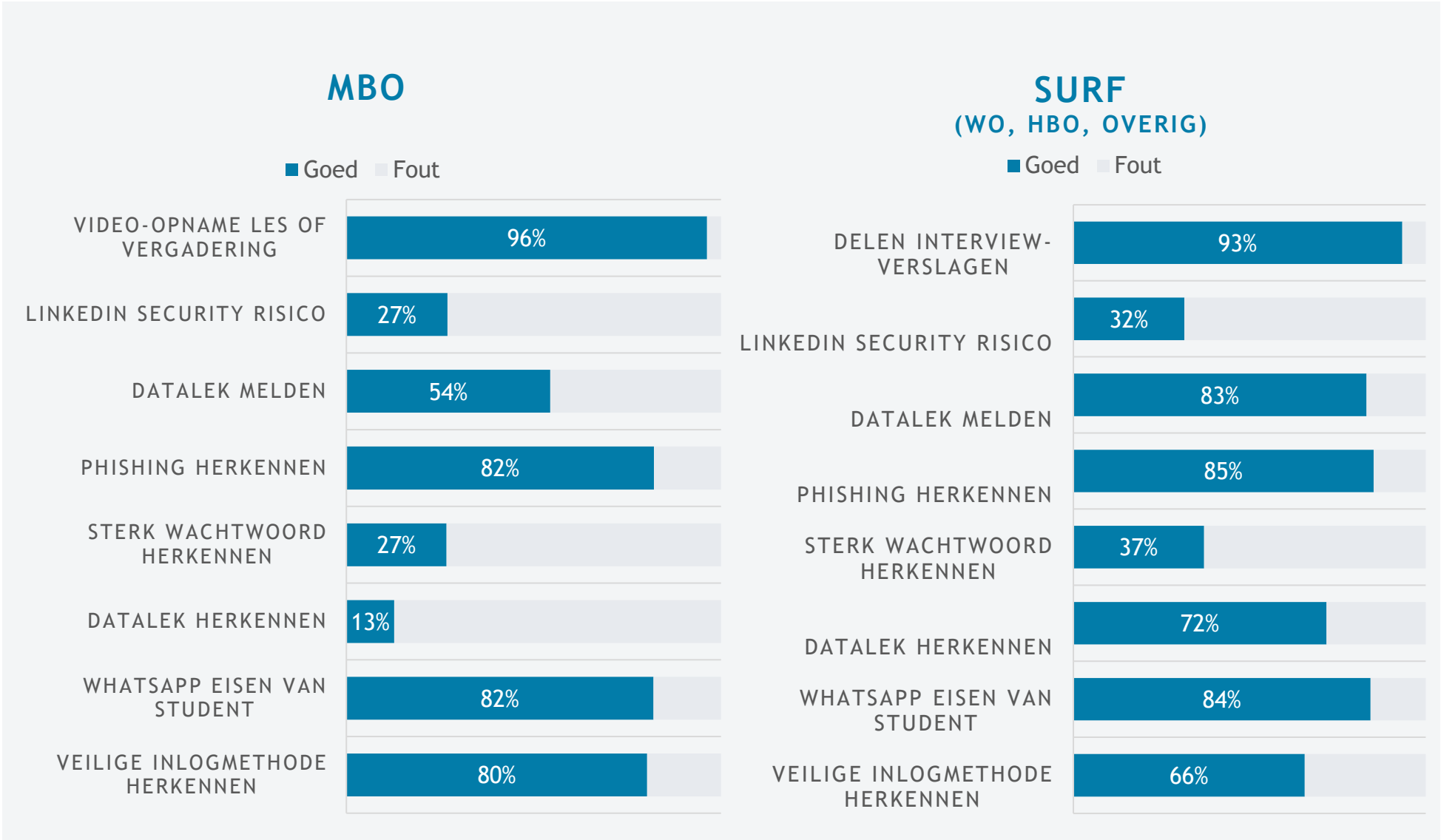
Deze vraag is bijna gelijk aan de toetsvraag van MBO Digitaal, alleen het (onjuiste) antwoord b is in de SURF-versie iets moeilijker. Het juiste antwoord is wederom a. Deze vraag is ook door 63% onjuist beantwoord.

### Relatief goed beantwoorde vragen

Deze vragen kregen de meeste goede antwoorden.

1. Je bent onderzoeker en wilt interview-verslagen delen met een externe onderzoeker. Welke van de onderstaande methoden heeft de voorkeur? -> 93% geeft het juiste antwoord
2. Is deze voorbeeld-email phishing? -> 85% geeft het juiste antwoord
3. Een docent mag van een student eisen dat deze lid wordt van een Whatsapp-groep van een bepaald vak. -> 84% geeft het juiste antwoord

# Resultaten - bekwaamheid (4)



# Resultaten - bekwaamheid (5)

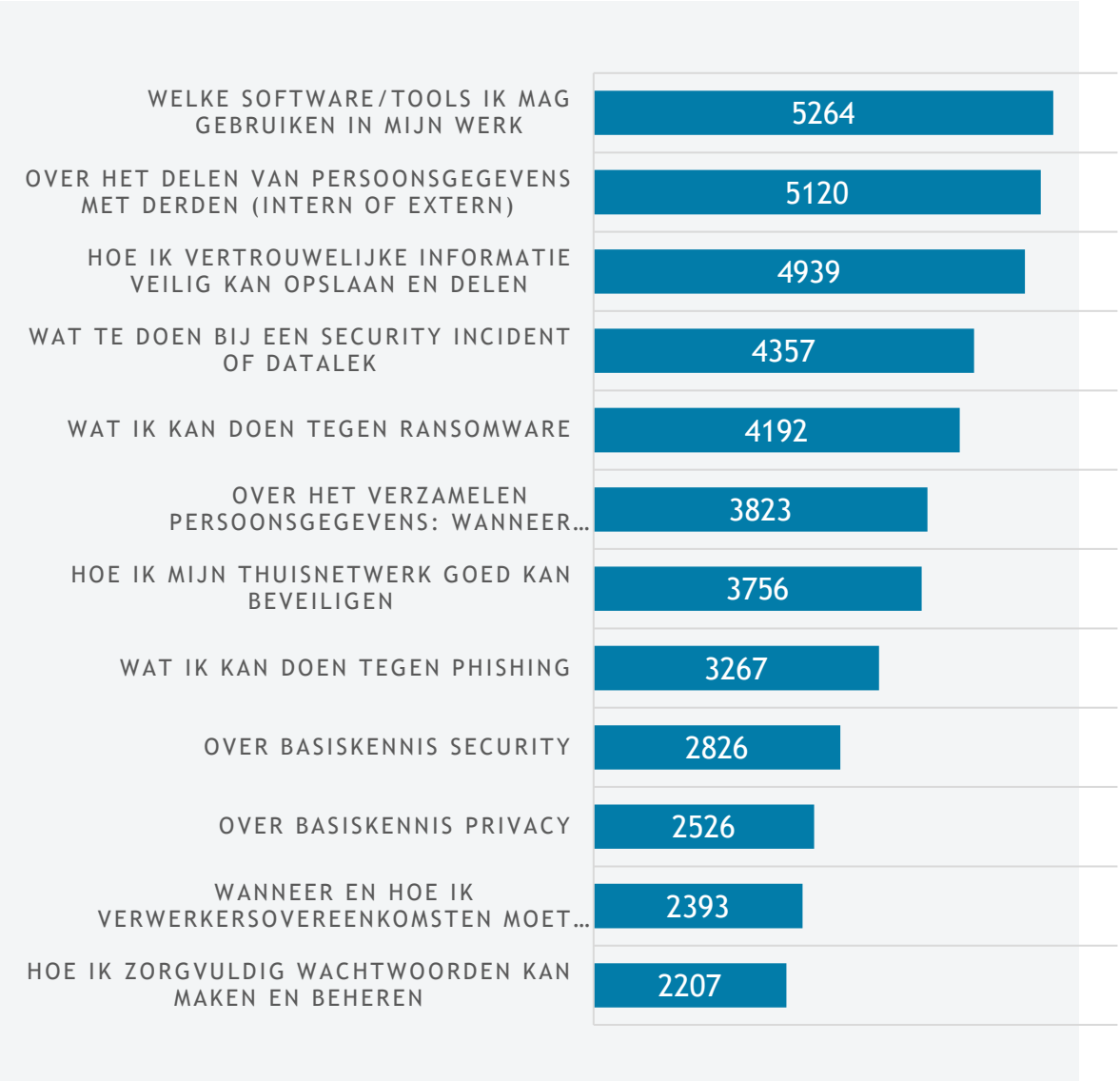
Tot slot hebben we gevraagd op welke thema's respondenten zich nog niet (geheel) bekwaam achten. Zij konden meerdere antwoorden selecteren. Hieruit komt naar voren dat men 1) vooral graag meer wil weten welke software/tools zijn toegestaan op het werk, 2) behoefte heeft aan kennis over het opslaan en delen van persoonsgegevens en andere vertrouwelijke informatie en 3) wil weten wat te doen bij een security incident of datalek.

In de open antwoorden zeggen sommige respondenten dat ze al voldoende kennis hebben. Anderen vinden de vraag lastig te beantwoorden.

> *"Ik weet niet wat ik niet weet. Ik ben een gebruiker, geen expert."*

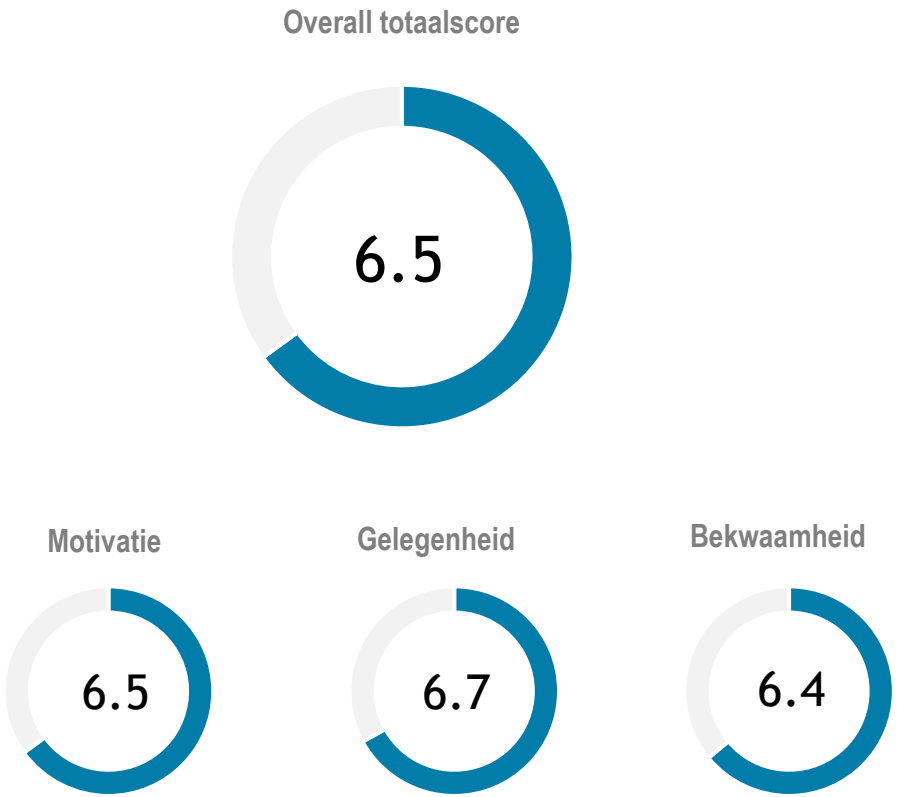
Verder benadrukt een aantal respondenten dat ze geen kennis nodig hebben, maar eerder duidelijkheid over de juiste manier van werken, en hierin goed gefaciliteerd willen worden.

> *"Het gaat niet om kennis, maar om het faciliteren van informatieveilig werken. Zo is een projectomgeving maken met externe partners nog steeds lastig en werkt dat niet altijd naar behoren."*



# Resultaten in cijfers (1)

Dit hoofdstuk bevat de resultaten van de awarenessmeting in cijfers. Deze worden middels scores (1-10) getoond. De ‘overall totaalscore’ is de score van alle respondenten samen, zowel van de MBO Digitaal-meting als de SURF-meting. Onder de ‘overall totaalscore’ staan de totaalscores per component.




In totaal hebben 12.343 respondenten de vragenlijst ingevuld. Hiervan heeft 47% deelgenomen via de MBO Raad en 53% via SURF.

### Nuancering scores

Het gebruik van scores impliceert dat we verwijzen naar een objectieve werkelijkheid, maar dat is niet het geval. Deze meting gaat over menselijke ervaringen en waarnemingen. We vragen de lezer om niet te veel waarde te hechten aan de exacte score, maar om deze te zien als globale indicatie van het awarenessniveau van de respondenten.

### Streefdoel

Wij beschouwen een score van 7 als minimaal streefdoel. Vanaf deze score is er binnen de organisatie voldoende basis op het gebied van motivatie, bekwaamheid en gelegenheid om privacybewust en informatieveilig te werken. Je zou dan kunnen zeggen dat de medewerkers dan gemiddeld redelijk weerbaar zijn tegen mensgerichte cyberaanvallen en security-incidenten. De meeste instellingen voldoen (nog) niet aan deze score.

Dit hoofdstuk bevat verder de scores per sector en die per doelgroep en functie.

# Resultaten in cijfers (2)

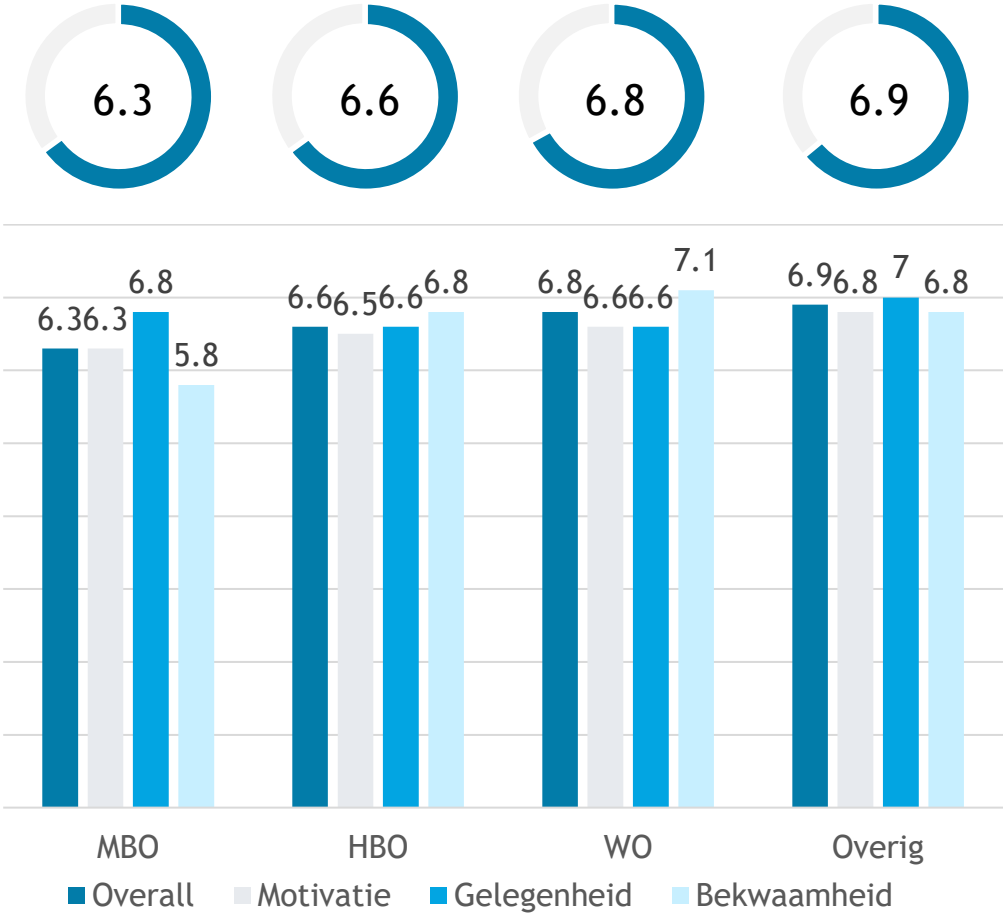
## Resultaten per sector

Uit de resultaten per sector komt naar voren dat de categorie ‘overig’ het hoogst scoort met een gemiddelde totaalscore van 6.9. De MBO behaalt de laagste score met een 6.3. Hierbij moet wel opgemerkt worden dat de vragen voor het onderdeel ‘bekwaamheid’ (de toetsvragen) gedeeltelijk anders waren voor de MBO dan voor de andere sectoren. Dit is ook het component met de grootste scoreverschillen. Mogelijk zijn deze verschillen dus (deels) te verklaren door de toetsvragen.

Verder valt op dat de overall totaalscore een 6,5 is, terwijl drie van de vier sectoren een hoger cijfer hebben. Dat is te verklaren omdat de totaalscores gebaseerd is op het gemiddelde van alle respondenten, niet het gemiddelde van de vier sectoren.

| | MBO | HBO | WO | overig | Totaal |
|---|---|---|---|---|---|
| **Aantal instellingen** | 41 | 10 | 9 | 10 | 70 |
| **Aantal respondenten** | 5.768 | 3.627 | 2.198 | 750 | 12.343 |

*Tabel 1. Deelnemers per sector*




*Tabel 2. Resultaten per component per sector*

# Resultaten in cijfers (3)

## Resultaten per doelgroep

We analyseren de doelgroepen via twee assen:

1. Leidinggevend vs uitvoerend.
   Leidinggevenden scoren iets beter dan uitvoerenden. Bij de meting van MBO Digitaal is het verschil (0.3) tussen beide doelgroepen groter dan bij de SURF-meting (0.1).

2. Per functiegroep.
   MBO Digitaal heeft alleen de functiegroepen onderwijs en ondersteuning. In de SURF meting zijn de functiegroepen IT ondersteuning en overig toegevoegd. En de functiegroep onderwijs heeft bij SURF de titel onderwijs/onderzoek.
   IT- ondersteuning haalt de hoogste score van de functiegroepen en onderwijs/onderzoek de laagste score.

| | Doelgroep | MBO | SURF | Totaal |
|---|---|---|---|---|
| 1 | Leidinggevend | 572 | 891 | 1463 |
| | Uitvoerend | 5196 | 5684 | 10880 |
| | | | | |
| 2 | Onderwijs/ onderzoek | 2762 | 2539 | 5301 |
| | Ondersteuning | 3006 | 2697 | 5703 |
| | IT ondersteuning | x | 763 | 763 |
| | Overig | x | 576 | 576 |

*Tabel 3. Deelnemers per doelgroep*

| | Doelgroep | MBO | SURF | Gemid-deld |
|---|---|---|---|---|
| 1 | Leidinggevend | 6.6 | 6.8 | 6.7 |
| | Uitvoerend | 6.3 | 6.7 | 6.5 |
| | | | | |
| 2 | Onderwijs/onderzoek | 6.2 | 6.5 | 6.3 |
| | Ondersteuning | 6.4 | 6.7 | 6.5 |
| | IT ondersteuning | x | 7.4 | 7.4 |
| | Overig | x | 6.7 | 6.7 |

*Tabel 4. Gemiddelde scores per doelgroep*

# Verbeterpunten respondenten

# Verbeterpunten respondenten (1)

In de vragenlijst en tijdens de interviews hebben we respondenten gevraagd of zij opmerkingen of verbeterpunten hebben voor hun instelling zodat zij beter privacybewust en informatieveilig kunnen werken. Op basis van de duizenden reacties, waaronder gesprekken met acht geïnterviewden, kunnen we de volgende thema's destilleren.

- **Behoefte aan duidelijkheid en ondersteuning**
  Respondenten zeggen dat ze graag helderheid willen over informatieveilig werken in hun instelling. Zoals: welke tools zijn toegestaan? Hoe kunnen we vertrouwelijke informatie verzamelen, opslaan en delen? De respondenten vragen om deze zaken goed in te richten, zodat informatieveilig werken voor hen behapbaar is.

  > *"Ik stel voor dat we niet overgaan tot meer regels, dat we de regels hanteerbaar en uitvoerbaar houden en dat een ieder ook zelf verantwoordelijk is en dat er aandacht is voor fijne ondersteuning"*

- **Aansprekende en relevante boodschappen**
  Er wordt opgemerkt dat de communicatie over informatieveiligheid vaak droog en onpersoonlijk is. De wens is dat het laagdrempeliger en begrijpelijker wordt gemaakt, en dat de boodschap aansluit bij de dagelijkse werkzaamheden van de ontvangers.

- **Vast onderdeel van onboarding**
  Respondenten die nog kort in dienst zijn bij hun instelling, zijn verbaasd dat zij geen informatie hebben ontvangen over informatieveiligheid. Zij, en veel andere respondenten, adviseren om dit thema een vast onderdeel te maken van de onboarding van nieuwe medewerkers.

  > *"Als nieuwe medewerker ben ik niet tot nauwelijks geïnformeerd over wat onze richtlijnen en regels zijn mbt informatieveilig werken. Dit moet je echt zelf uitzoeken."*

- **Gebruikersvriendelijkere security-maatregelen**
  Security-maatregelen zorgen geregeld voor frustratie bij veel respondenten. Het meest genoemde voorbeeld is MFA. Vooral de authenticator app vindt men lastig in het gebruik. Andere voorbeelden zijn het werkend krijgen en houden van een password manager en onvindbare en onuitvoerbare gedragsregels en richtlijnen. Men heeft behoefte aan meer gebruikersvriendelijkheid.

- **Duidelijkheid over AI / ChatGPT**
  Respondenten wensen heldere richtlijnen over AI. Vragen die spelen zijn: hoe kunnen we informatieveilig omgaan met ChatGPT en andere AI tooling? Maar ook: Kunnen we AI-tooling inzetten om informatieveilig(er) te werken?

# Verbeterpunten respondenten (2)

- **Verplichten van training**

  Informatieveilig werken heeft in veel instellingen een vrijblijvend karakter. Het is niet verplicht om deel te nemen aan een training, er is geen controle of handhaving. Respondenten adviseren om een verplichte training of e-learning uit te rollen voor de medewerkers, en deze op vaste momenten te herhalen.

  *"Nu weet ik dat we vorig jaar verplicht een AVG training moesten volgen, maar die heb ik nooit gehad en geen haan die er naar kraait. Managers mogen wat dat betreft wel meer verantwoordelijkheid nemen, het goede voorbeeld geven en hun teams gaan managen."*

- **Teveel aandacht voor security en privacy**

  Een –uitgesproken- minderheid vindt dat er teveel belang gehecht wordt aan security en privacy. Zij zijn van mening dat de regels te strikt worden toegepast of stellen dat de AVG wordt misbruikt om bepaalde initiatieven te blokkeren.

  *"Het onderwerp boeit me niet, en er wordt soms veel te overdreven over gedaan uit angst voor sancties. (..)Ik ben erg tegen doorgeslagen security, zeker als het de doelen van de organisatie uiteindelijk tegenwerkt (bijv. studentenbelang)."*

- **Betere ondersteuning onderzoekers**

  Veel onderzoekers zijn van mening dat ze onvoldoende ondersteund worden op het gebied van informatieveiligheid. De faciliteiten voor het opslaan en delen van onderzoeksdata schieten tekort. Ook vindt men de privacyregels bij het versturen van surveys omslachtig.

  *"Het overzetten van onderzoeksdata naar de beveiligde schijf duurt ontiegelijk lang en het proces breekt regelmatig af. Daardoor staat data helaas nogal eens op een externe harde schijf."*

- **Ondersteuning studentenonderzoekers**

  Voor studenten zijn er vaak helemaal geen voorzieningen en gedragsregels met betrekking tot het uitvoeren van onderzoek. Zij zijn hiervoor afhankelijk van hun docent of tutor. Respondenten willen graag dat dit goed geregeld wordt, dat studenten goed begeleid worden bij het veilig en zorgvuldig verzamelen van data en dat zij hun onderzoeksgegevens op een veilige plek kunnen opslaan.

- **Phishingtest**

  Respondenten adviseren om zo nu en dan een phishing test uit te voeren om medewerkers alert te houden. Ook zou er meer training moeten zijn voor het herkennen van phishing.

# Verbeterpunten respondenten (3)

- **Op orde brengen autorisaties**

  Op het gebied van autorisaties spelen meerdere informatieveiligheidszaken, zeggen respondenten die hier als stakeholder een rol in hebben. Allereerst het dilemma van autorisaties verlenen aan medewerkers die daar om vragen maar er vanuit hun rol eigenlijk geen recht op hebben. Als deze verzoeken worden toegekend, brengt dat security risico's met zich mee. Als ze worden afgewezen, gaan de medewerkers veelal op een andere manier zoeken naar toegang. Bijvoorbeeld door collega's te vragen om exports te maken. Die exports kunnen een eigen leven gaan leiden – ze worden lokaal opgeslagen, verder verrijkt en gedeeld per e-mail- ook met extra security risico's tot gevolg. Ten tweede blijven, zoals eerder genoemd, autorisaties vaak behouden als een medewerker intern wisselt van functie. Het intrekken van rechten is meestal niet (voldoende) geautomatiseerd. Dit is ook lastig, omdat veel systemen uit een tijd komen waarin dit minder relevant was. De functies moeten handmatig ingetrokken worden, maar dat gebeurt vaak niet. Het is lastig om dit waterdicht te krijgen, daar zou bij instellingen meer aandacht aan besteed kunnen worden.

# Vergelijking met 2022

# Vergelijking met 2022

Hoe zijn de resultaten van nu vergeleken met de resultaten van 2022?

### Aantal deelnemers

Allereerst is er een verschil in het aantal deelnemers. Dit jaar zijn er bijna drie keer zoveel deelnemende instellingen en ook bijna drie keer zoveel respondenten als vorig jaar. Dat is een mooi resultaat en voor een groot deel te danken aan de aparte benchmarkmeting die via MBO Digitaal voor de MBO instellingen is gehouden.

### Resultaten

Ook is er verschil in resultaten. Dit jaar scoren de instellingen gemiddeld beter dan vorig jaar. Toevallig zijn in 2023 zowel het overall resultaat als het resultaat per component precies 0.6 punt hoger dan in 2022.

Hoe zit het met de verschillen per vraag? Zijn die ook gelijk verdeeld? Om deze vraag te beantwoorden, hebben we de vragen genomen die precies hetzelfde zijn in 2022 en 2023 en waarvan het resultaat goed vergeleken kan worden. De toetsvragen (bekwaamheid) vielen af, want die zijn verschillend voor beide jaren. Ook zijn dit jaar enkele vragen toegevoegd. In totaal zijn er vijf vragen die in 2022 en 2023 precies hetzelfde en die onderling goed vergelijkbaar zijn.

| Aantal | 2022 | 2023 |
|---|---|---|
| Respondenten | 4.524 | 12.343 |
| Instellingen | 26 | 70 |
| • MBO | 6 | 41 |
| • WO | 8 | 9 |
| • HBO | 9 | 10 |
| • Overig | 3 | 10 |

*Tabel 5. Aantal deelnemers aan meting in 2022 en in 2023*

| Score | 2022 | 2023 |
|---|---|---|
| Overall | 5.9 | 6.5 |
| Motivatie | 5.9 | 6.5 |
| Gelegenheid | 6.1 | 6.7 |
| Bekwaamheid | 5.8 | 6.4 |

*Tabel 6. Scores per component in 2022 en 2023*

# Vergelijking met 2022

## Vergelijking vragen 2022 en 2023

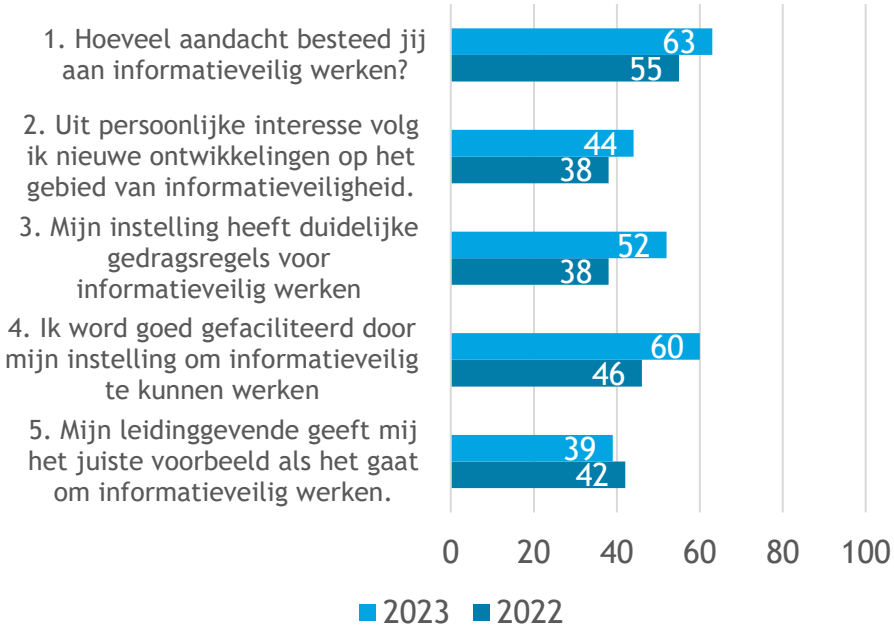
We vergelijken de volgende vragen:

1. Hoeveel aandacht besteed jij aan informatieveilig werken?
2. Stelling: uit persoonlijke interesse volg ik nieuwe ontwikkelingen op het gebied van informatieveiligheid.
3. Stelling: mijn instelling heeft duidelijke gedragsregels voor informatieveilig werken.
4. Stelling: ik word goed gefaciliteerd door mijn instelling om informatieveilig te kunnen werken.
5. Stelling: mijn leidinggevende geeft mij het juiste voorbeeld als het gaat om informatieveilig werken.

Per vraag berekenden we het opgetelde percentage respondenten dat de twee meest positieve antwoordopties gaf. Bij vraag 1 zijn dat: ‘veel aandacht’ of ‘zeer veel aandacht’. Bij vraag 2 tot en met 5 zijn dat ‘eens’ of ‘zeer eens’.
Uit de analyse blijkt dat bij vier van de vijf vragen de scores in 2023 hoger waren. Alleen op vraag 5, over de voorbeeldrol van de leidinggevende, is de score in 2023 lager. Slechts 39% van de respondenten is het eens of zeer eens met de stelling dat de leidinggevende het juiste voorbeeld geeft, ten opzichte van 42% in 2022 (wat ook al geen hoge score was).

## Conclusie

De respondenten zijn in 2023 over de meeste onderwerpen met betrekking tot informatieveilig werken positiever dan in 2022. Er is één uitzondering: de voorbeeldrol van de leidinggevende. Daarover denken respondenten nu (iets) minder positief dan in 2022.




*Tabel 7. Vergelijking antwoorden 2022 en 2023*

# Gedragsmeting

# Introductie gedragsmeting

Naast de awarenessmeting is dit jaar is een extra meting toegevoegd: een gedragsmeting die daadwerkelijk cyberveilig gedrag meet. De gedragsmeting is uitgevoerd door onderzoekers van het Lectoraat Cybercrime en Cybersecurity van de Haagse Hogeschool (HHS). De meting is uitgezet via de SURF awarenessmeting en in totaal hebben 20 instellingen met 2833 respondenten deelgenomen aan deze meting.

## Hoofdvragen

1. Wat zijn resultaten van de gedragsmeting?
2. Wat is de relatie tussen de score van de gedragsmeting tot die van de basis-awarenessmeting? In andere woorden, zeggen de kennis, motivatie en gelegenheid van de medewerkers m.b.t. veilig online werken iets over hun daadwerkelijke cyberveilige gedrag?

## Waarom een gedragsmeting

Eerder wetenschappelijk onderzoek van de Haagse Hogeschool toont aan dat de relatie tussen zelfgerapporteerd gedrag en daadwerkelijk gedrag op het gebied van cyberveiligheid mogelijk niet zo sterk is. De HHS wil onder andere met deze meting vervolgonderzoek uitvoeren om dit beeld scherper te krijgen.

## Soorten gedragsmeting

De gedragsmeting is onderdeel van de online vragenlijst van de SURF - awarenessmeting en bevat twee gedragstesten.

**1. Sterk wachtwoord maken**

Het gebruik van unieke, sterke wachtwoorden door alle medewerkers draagt bij aan de cyberweerbaarheid van een organisatie. Sterke wachtwoorden kunnen veel minder makkelijk geraden of (brute force) gehackt worden.

**2. Niet ongewenst delen persoonlijke informatie**

Ongewenst persoonlijke informatie delen kan als gevolg hebben dat deze gegevens worden uitgebuit door kwaadwillende. Met persoonsgegevens kunnen gepersonaliseerde aanvallen uitgevoerd worden, zoals spear phishing en CEO fraude.

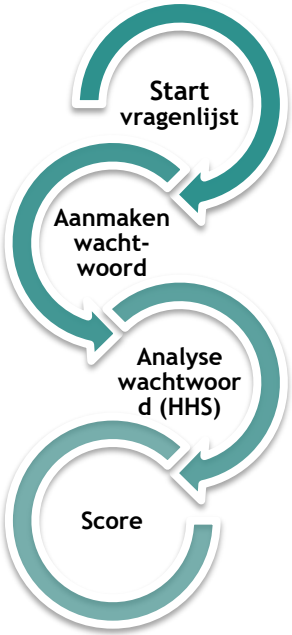
Deze testen zijn niet vooraf gecommuniceerd met de respondenten, omdat zij dan hun gedrag konden aanpassen. Op de volgende pagina's worden de testen toegelicht.

# Aanpak gedragsmeting

## 1. ‘Sterk wachtwoord maken’

**Hoe ging de gedragstest in zijn werk?**

- Aan de deelnemers van de SURF-awarenessmeting werd bij aanvang gevraagd om een account aan te maken, inclusief een wachtwoord. Zonder account was het niet mogelijk om de meting te voltooien.
- Vervolgens werd aan de hand van 20 indicatoren gemeten hoe sterk het wachtwoord was (het wachtwoord zelf werd niet opgeslagen in de onderzoekstool). Voorbeelden van indicatoren zijn het aantal karakters, aantal cijfers, hoofdletters, speciale karakters en het aantal bruteforcepogingen nodig om het wachtwoord te kraken.
- Aan de hand van deze indicatoren werd een score (0-4) vastgesteld. Wachtwoorden met score 3 of 4 hebben we als ‘sterk’ bestempeld.




*Figuur 4. proces wachtwoordtest*

## 2. ‘Niet ongewenst delen persoonsgegevens’

**Hoe ging de gedragstest in zijn werk?**

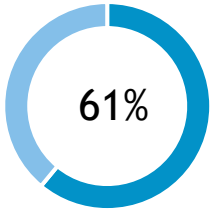
- Aan het eind van de vragenlijst van de SURF awarenessmeting kregen de respondenten het verzoek om een aantal persoonsgegevens in te vullen.
- Het betreft zeven soorten persoonsgegevens:
  - Naam
  - Adres
  - Postcode
  - Plaats
  - Telefoonnummer
  - Geboortedatum
  - Medewerkernummer
- Vervolgens werd gekeken of, en zo ja hoeveel, gegevens de respondenten delen.
- Respondenten die helemaal geen persoonsgegevens delen, kregen het stempel ‘niet ongewenst delen persoonsgegevens’.


*Figuur 5. proces test persoons-gegevens*

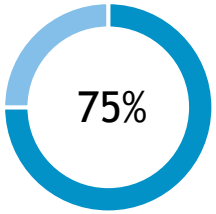
# Resultaten gedragsmeting (1)

## Resultaten gedragsmeting

Gemiddeld maakt 61% van de respondenten een sterk wachtwoord aan en vult 75% van de respondenten géén persoonsgegevens in, als daar om wordt gevraagd.




Benchmark sterk wachtwoord




Benchmark persoonsgegevens

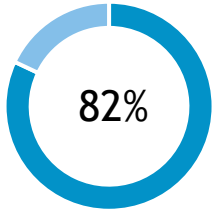
**Wachtwoordtest**

- In de wachtwoordtest is onder andere gekeken naar de lengte van het ingevoerde wachtwoord. Een overgrote meerderheid (82%) van de respondenten creëerde een wachtwoord van minimaal acht karakter. En ongeveer de helft daarvan had zelfs een wachtwoord van 12 karakters en meer.

| Karakters wachtwoord | Percentage respondenten |
|---|---|
| 1-7 karakters | 18% |
| 8-11 karakters | 43% |
| 12+ karakters | 39% |

*Tabel 8. Percentages lengte wachtwoord*

- Ook is gekeken of het ingevoerde wachtwoord al bekend is in zogenaamde password dictionaries. Dat zijn lijsten met bekende wachtwoorden die bijvoorbeeld onderdeel waren van een datalek-dump. Hackers gebruiken password dictionaries bij wachtwoordaanvallen. Een wachtwoord dat bekend is in dictionaries is in de regel minder sterk dan wachtwoorden die dat niet zijn. Uit de wachtwoordtest komt naar voren dat 18% van de wachtwoorden voorkomt in een dictionary, en 82% niet.




Wachtwoorden niet in dictionary

**Test persoonsgegevens**

In totaal heeft 75% van de respondenten helemaal geen persoonsgegevens gedeeld. De respondenten die dat wél deden, maakten veelal onderscheid per vraag. De volgende pagina toont per gevraagd persoonsgegeven het percentage respondenten dat informatie heeft gedeeld. Respondenten zijn het meest geneigd om hun eigen naam te delen (21%) en het minst hun adres (3%).

# Resultaten gedragsmeting (2)

| Persoonsgegeven | % respondenten niet gedeeld |
|---|---|
| Naam | 79% |
| Adres | 97% |
| Postcode | 96% |
| Woonplaats | 93% |
| Telefoonnummer | 93% |
| Geboortedatum | 89% |
| Medewerkernummer | 92% |

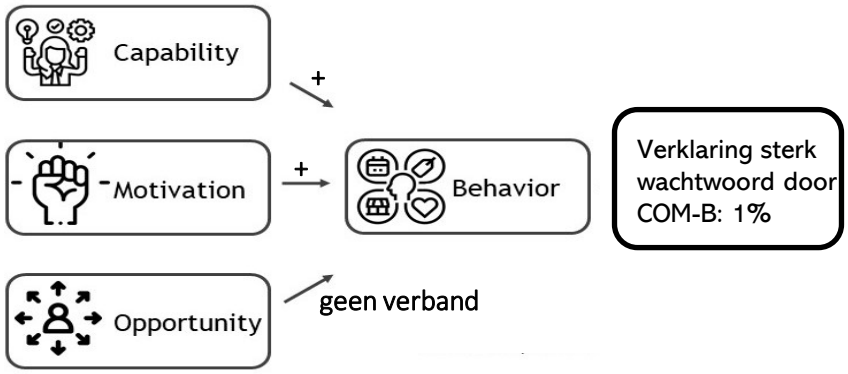
*Tabel 9. Percentages niet delen persoonsgegevens*

## Relatie score gedragsmeting en COM-B basismeting

Er is onderzocht in hoeverre de componenten van het COM-B model – bekwaamheid, gelegenheid en motivatie- gerelateerd zijn aan daadwerkelijk online gedrag onder medewerkers. Er is, zoals eerder beschreven, gekeken naar twee vormen van daadwerkelijk online gedrag: A) de sterkte van het aangemaakte wachtwoord en B) het al dan niet invullen van persoonsgegevens.

### A. Wachtwoordsterkte

Uit de gedragstest over wachtwoordsterkte is naar voren gekomen dat bekwaamheid en motivatie significant gerelateerd zijn aan de sterkte van het wachtwoord dat medewerkers hebben gekozen. Dit betekent dat medewerkers sterkere wachtwoorden aanmaken en dus veiliger omgaan met wachtwoorden naarmate zij meer kennis en motivatie hebben. Dit is in lijn met de theoretische verwachting. Het component gelegenheid laat geen significant verband zien met wachtwoordsterkte, wat niet in lijn is met de theoretische verwachting. Bekwaamheid en motivatie verklaren echter samen een zeer klein deel van de gekozen wachtwoordsterkte, namelijk zo'n 1%. Dit betekent dat zo'n 99% van de variantie tussen medewerkers in wachtwoordsterkte wordt verklaard door andere factoren die niet zijn meegenomen in dit onderzoek.



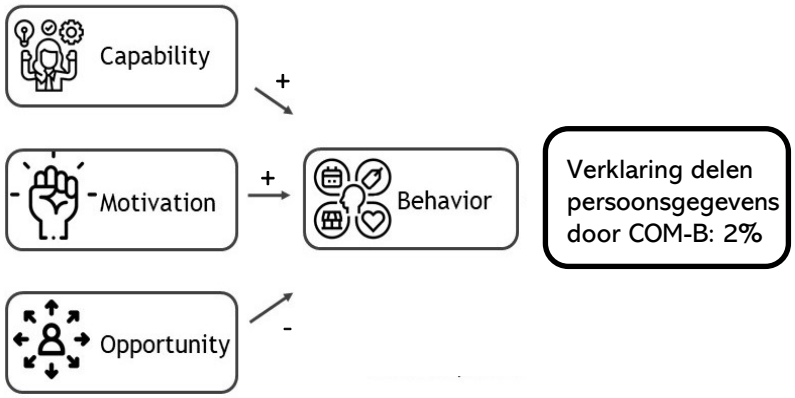

*Figuur 6: Relatie tussen COM-B en wachtwoordsterkte*

# Resultaten gedragsmeting (3)

### B. Persoonsgegevens

Vervolgens is gekeken naar de mate waarin medewerkers persoonsgegevens invullen. Hieruit is naar voren gekomen dat de componenten bekwaamheid, motivatie en gelegenheid alle drie een significant verband laten zien met het invullen van persoonsgegevens. Hoe meer kennis en motivatie medewerkers hebben met betrekking tot veilig online werken, hoe minder persoonsgegevens zij invullen, oftewel hoe veiliger zij omgaan met het delen van persoonsgegevens. Dit is in lijn met de theoretische verwachting. Het verband met gelegenheid laat echter zien dat hoe meer gelegenheid medewerkers hebben om informatieveilig te werken, hoe meer zij persoonsgegevens invullen en dit is niet in lijn met de theoretische verwachting.

Bekwaamheid, motivatie en gelegenheid verklaren slechts een zeer klein deel van de bereidheid om persoonsgegevens te delen, namelijk zo'n 2%. Dit betekent dat zo'n 98% van de variantie tussen medewerkers in de bereidheid om persoonsgegevens te delen wordt verklaard door andere factoren die niet zijn meegenomen in dit onderzoek.




*Figuur 7: Relatie tussen COM-B en het delen van persoonsgegevens*

### Conclusie

Samengenomen lijken de componenten bekwaamheid en motivatie in zeer beperkte mate een positief verband te hebben met daadwerkelijk informatieveilig gedrag. Het component gelegenheid laat in zeer beperkte mate een negatief verband zien met daadwerkelijk informatieveilig gedrag.

# Conclusie

# Conclusie (1)

Dit rapport bevat een analyse van de 70 security- en privacy-awarenessmetingen die BDO in opdracht van SURF en MBO Digitaal heeft uitgevoerd in het voorjaar van 2023. Op basis van de bevindingen in de voorgaande hoofdstukken, concluderen we het volgende.

1. **Over de hele linie zijn de resultaten beter dan vorig jaar, maar deze zijn nog niet voldoende en men is minder positief over de voorbeeldrol van leidinggevenden**
   Uit de meting komt naar voren dat de respondenten meer gemotiveerd zijn, beter bekwaam zijn en zich beter gefaciliteerd voelen om veilig te werken dan vorig jaar. Helaas voldoen de meeste instellingen nog steeds niet aan het minimale streefdoel (informatie over het streefdoel staat op pagina 24). Verder is er één onderwerp waar een afname zichtbaar is: in hoeverre men vindt dat leidinggevenden het juiste voorbeeld geven.

Aan de start van de awarenessmeting zijn drie onderzoeksvragen geformuleerd: 1) in hoeverre willen medewerkers informatieveilig en privacybewust werken (motivatie), 2) in hoeverre kunnen zij dat (bekwaamheid) en 3) in hoeverre worden zij hiertoe in staat gesteld (gelegenheid)? Conclusie 2, 3 en 4 geven antwoord op deze onderzoeksvragen.

2. **Men is nog steeds overtuigd van het belang, maar beperkt gemotiveerd om aandacht te besteden aan security en privacy**
   Net als in 2022 is de overgrote meerderheid van respondenten zich bewust van het belang van informatieveiligheid en de rol van medewerkers hier in, maar beperkt gemotiveerd om hier mee aan de slag te gaan. Respondenten besteden in de regel vooral aandacht aan informatieveiligheid omdat ze negatieve consequenties willen vermijden. Ook is er een minderheid die zegt geen belang te hechten aan informatieveiligheid en hier (zeer) weinig aandacht aan te besteden. Zij vinden de aandacht voor het thema overtrokken of zijn van mening dat de instelling verantwoordelijk is voor de informatieveiligheid en dat zij hier als medewerker geen rol in hebben.

3. **Redelijke tevredenheid over faciliteiten, maar sterke security cultuur ontbreekt**
   Een meerderheid van de respondenten is tevreden over de mate waarin ze gefaciliteerd worden om informatieveilig te werken. Toch worden er nog veel concrete onderwerpen genoemd die verbetering behoeven. Daarnaast lijkt er in de meeste instellingen geen sprake te zijn van een sterke security cultuur: ze lijken geen breed gedeelde ideeën, gedragingen en gewoontes te hebben die erop

# Conclusie (2)

gericht zijn om informatie te beschermen. De meeste respondenten denken niet dat hun collega's veel belang hechten aan informatie-veiligheid. Volgens respondenten pakken leidinggevenden hun voorbeeldrol amper op. Vanuit die invalshoek worden medewerkers maar matig gefaciliteerd om informatieveilig te werken.

4. **De kennis over informatieveiligheid is matig tot redelijk, er is vooral behoefte aan helderheid en ondersteuning**

   De quizvragen in de awarenessmeting zijn matig tot redelijk gemaakt. Van alle acht vragen gaf gemiddeld 64% van de respondenten een juist antwoord. Dat is een stuk beter dan de resultaten van vorig jaar (toen 57,5%), maar er is voldoende ruimte voor verbetering. Veel respondenten zeggen dat ze vooral behoefte hebben aan helderheid over wat wel en niet is toegestaan in hun eigen werkproces, met betrekking tot informatieveilig werken. In algemene adviezen hebben ze minder interesse. Ook willen ze goed ondersteund worden, zodat er zo weinig mogelijk barrières zijn voor het gewenste gedrag.

Naast de antwoorden op de onderzoeksvragen kunnen we enkele aanvullende conclusies trekken. Deze hebben betrekking op de gedragsmeting en op de doelgroepen van de awarenessmeting.

# Conclusie (3)


5. **Zeer beperkt verband tussen COM-B en daadwerkelijk veilig gedrag**

   Er zijn twee gedragsmetingen uitgevoerd, waarbij gekeken werd of er een relatie is tussen de resultaten van de COM-B vragenlijst en daadwerkelijk informatieveilig gedrag. Uit de analyse blijkt dat de componenten bekwaamheid (de C van capability in COM-B) en motivatie (de M) een zeer beperkt positief verband hebben met daadwerkelijk veilig gedrag. Het component gelegenheid (de O van opportunity) laat een zeer beperkt negatief verband zien met informatieveilig gedrag. Het verband is 1-2%, dat betekent dat 98-99% van de variantie tussen medewerkers in het informatieveilige gedrag wordt verklaard door andere factoren (die niet zijn meegenomen in dit onderzoek).

6. **Doelgroep ondersteuning behaalt hoogste resultaten**

   De respondenten met een ondersteunende functie hebben betere resultaten behaald (tussen 6.5 en 7.4) dan de respondenten uit het primaire werkproces (onderwijs/onderzoek) (gemiddeld 6.3). De doelgroep IT-ondersteuning behaalde de hoogste score (7.4).

# Aanbevelingen

# Aanbevelingen

Op basis van de bevindingen en conclusies komen we tot de volgende aanbevelingen voor instellingen om de security en privacy awareness van hun medewerkers te verhogen.

1. **Zorg dat awarenessuitingen aansluiten bij het dagelijkse werk**
   Om medewerkers te motiveren om informatieveilig te werken, is het raadzaam om in trainingen concrete voorbeelden en scenario's te delen die aansluiten bij hun dagelijkse taken. Men zal eerder open staan voor een awarenessboodschap die relevant is voor de eigen doelgroep en die een een concreet en haalbaar advies bevat, dan voor een algemeen en abstract verhaal.

2. **Neem barrières voor veilig werken weg**
   Net als vorig jaar adviseren we om te onderzoeken welke belemmeringen medewerkers ervaren bij informatieveilig en privacybewust werken. Uit de metingen dit jaar blijkt o.a. dat: 1) multifactor authenticatie (MFA) voor veel respondenten niet optimaal werkt, 2) men moeite heeft met het beheren van alle wachtwoorden en behoefte heeft aan een door de instelling beheerde password manager en 3) men veilig en gemakkelijk bestanden wil kunnen delen met externen. Ook ervaren onderzoekers veel barrières in het omgaan met hun onderzoeksgegevens.

Door oplossingen te bieden voor dit soort zaken, wordt het makkelijker voor medewerkers om veilig te werken.

3. **Investeer in een sterke security cultuur**
   Een sterke security cultuur heeft breed gedeelde ideeën, gedragen en gewoontes die erop gericht zijn op het beschermen van informatie. Informatieveilig werken dient de norm te zijn. Om een sterke security cultuur te ontwikkelen, zou er allereerst aandacht moeten zijn voor de leidinggevenden. Zij dienen het juiste voorbeeld te geven en het thema bespreekbaar te maken. Verder dient het onderwerp geregeld op de agenda van werkoverleggen te komen, zodat het een thema wordt dat er vanzelfsprekend bij hoort. Tot slot zou het goed zijn als awareness-trainingen en -sessies een minder vrijblijvend karakter krijgen. Zo zullen medewerkers ervaren dat de instelling belang hecht aan security en privacy en raken ze allemaal bekend met de bijbehorende boodschap.

4. **Heb aandacht voor daadwerkelijk gedrag**
   Uit de gedragsmeting blijkt dat kennis, motivatie en gelegenheid maar een klein deel van informatieveilig gedrag verklaren. Daarom is het belangrijk om -zowel metingen als interventies- te richten op daadwerkelijk gedrag, en niet alleen op vragenlijsten en trainingen.

# Aanbevelingen

Voorbeelden van gedrags*metingen* zijn 1) phishing-testen 2) meten in het mailprogramma hoe vaak gevoelige gegevens als bsn-nummers worden gemaild. Een type gedragsgerichte *interventie* is **'nudging':** mensen onbewust sturen naar het juiste gedrag. Een voorbeeld is de standaard instellingen van een tool de meest privacy-vriendelijke instellingen maken. Een ander type gedragsgerichte interventie is **'techno-regulation'.** Dit houdt in dat gebruik van software/tooling uitsluitend op een informatieveilige manier mogelijk is. Je kunt hierbij denken aan beveiligd printen: documenten worden pas uitgeprint wanneer de gebruiker zijn pas bij de printer houdt of een pincode invoert, niet direct bij het geven van de opdracht. Een ander voorbeeld is instellen dat e-mails standaard 1-2 minuten later verstuurd worden, zodat de verzender direct opgemerkte fouten, zoals een foutieve geadresseerde, nog kan herstellen.

5. **Maak security en privacy een vast onderdeel van onboarding**
   Zorg dat alle nieuwe medewerkers zodra ze in dienst komen een security/privacy training volgen. Dit zorgt voor duidelijkheid over de verwachtingen die worden gesteld. Nieuwe medewerkers zijn nog niet bekend met de geldende richtlijnen van de instellingen het is niet zeker of ze eerder al toereikende security en privacy kennis hebben opgedaan.

# Aanbevelingen

### 6. Houd rekening met de sceptici

De medewerkers die de aandacht voor privacy en security overtrokken vinden, vormen een kleine minderheid, maar kunnen mogelijk wel een risico vormen voor de organisatie. Ga in gesprek met hen, vraag naar hun argumenten. Is het probleem dat medewerkers privacy en security risico's onderschatten, of dat sommige maatregelen te strikt zijn om het werk goed te kunnen uitvoeren? Of gaat het wellicht om een combinatie van beide?

### 7. Investeer extra in docenten, onderzoekers en leidinggevenden

Net als vorig jaar adviseren we om leidinggevenden, docenten en onderzoekers extra aandacht te geven in het awarenessprogramma. Organiseer een training of workshop om leidinggevenden te ondersteunen bij het uitvoeren van hun voorbeeldrol op het gebied van cybersecurity en privacy. Doe extra moeite om docenten en onderzoekers te bereiken, bijvoorbeeld via afdelingsoverleggen en onderzoeksgroepen. Bied interventies aan die nauw aansluiten bij hun dagelijks werkproces (zie ook aanbeveling 1), zodat ze er niet  onnodig veel tijd aan kwijt zijn.

### 8. Thema's

Besteed extra aandacht aan specifieke thema's, zoals:

- Veilige software/tools
- Delen en opslaan persoonsgegevens
- Datalekken en security incidenten: hoe te herkennen en hoe te handelen
- Social engineering via sociale media
- Wachtwoorden

# Tot slot

Afgelopen voorjaar hebben SURF en BDO voor de derde jaar op rij een benchmark awarenessmeting uitgevoerd in het onderwijs. Dit jaar hebben we het op twee punten anders aangepakt.

### ▶ MBO Digitaal

Naast de SURF meting is er een eigen benchmarkmeting voor MBO instellingen uitgevoerd, geïnitieerd door MBO Digitaal. Hierdoor hebben een veelvoud aan instellingen en respondenten deelgenomen, waar we zeer verheugd over zijn. De resultaten van de MBO Digitaal benchmark zijn meegenomen in dit sectorrapport.

### ▶ Gedragsmeting

Naast de awareness meting, een (online) vragenlijst, is dit jaar ook een gedragsmeting toegevoegd, ontwikkeld en uitgevoerd door onderzoekers van de Haagse Hogeschool. Het doel was om enerzijds te meten hoe informatieveilig respondenten zich daadwerkelijk gedragen en anderzijds om te onderzoeken wat het verband is tussen de uitkomsten van de awarenessmeting en die van de gedragsmeting. Vooraf hadden we wat zorgen of de aanpak van de gedragsmeting zou leiden tot veel kritiek onder de respondenten –omdat ze zonder medeweten getest zouden worden- en of dit vervolgens tot een lage response zou leiden. Beiden bleken niet het geval.

Tijdens de meting hebben we geen klachten ontvangen van deelnemende instellingen en uit de evaluatie achteraf kwamen ook vooral positieve geluiden naar voren. Verder is het response-percentage van de instellingen met gedragsmeting ongeveer gelijk aan de instellingen die alleen de basismeting hebben gehouden.

De gedragsmeting concludeert dat er een zeer beperkt verband is tussen de awarenessmeting en daadwerkelijk gedrag. De in de awarenessmeting gemeten motivatie, gelegenheid en bekwaamheid (de basis van COM-B) zeggen volgens de gedragsmeting amper iets over het daadwerkelijke gedrag van respondenten.

Wat betekent dit voor de toekomst van awareness? Moeten we het COM-B model bij het oud vuil zetten en een compleet andere aanpak kiezen? Daarvoor is het wat ons betreft nog te vroeg. Uit de gedragsmeting blijkt dat andere factoren dan motivatie, bekwaamheid en gelegenheid -zoals gemeten in dit onderzoek- mogelijk een grotere invloed hebben op het daadwerkelijke informatieveilige gedrag. Dit dient verder onderzocht te worden. BDO, SURF en de Haagse Hogeschool gaan zich de komende periode hierover buigen, elk vanuit hun eigen expertise. We verkennen ook de mogelijkheid om gezamenlijk een vervolgonderzoek uit te voeren.

# Colofon

Sectorrapportage 2023. Over security en privacy awareness in onderwijs en onderzoek

Oktober 2023

Het rapport is opgesteld door

- **BDO Cybersecurity**
  drs. Marijke Stokkel, marijke.stokkel@bdo.nl

- **SURF**
  Rosanne Pouw, MSc, MPIM, MBA, CISM, CISSP, CIPM,
  rosanne.pouw@surf.nl

- **Centre of Expertise Cyber Security, de Haagse Hogeschool**
  dr. Susanne van ’t Hoff-de Goede, m.s.vanthoff-degoede@hhs.nl
  Maaike van der Wal, MSc, m.l.vanderwal@hhs.nl

# Bijlagen

# Bijlage A Vragenlijst SURF

**‘Meningvragen’**

1. Hoe belangrijk vind jij informatieveiligheid voor je instelling?
2. Hoeveel aandacht besteed jij over het algemeen tijdens je werk aan informatieveiligheid?
3. Waarom besteed jij tijdens je werk aandacht aan informatieveiligheid? Je kunt meerdere opties kiezen.
4. Stelling: binnen mijn instelling hechten medewerkers veel belang aan informatieveiligheid.
5. Stelling: uit persoonlijke interesse volg ik nieuwe ontwikkelingen op het gebied van informatieveiligheid.
6. Stelling: ik weet hoe ik in mijn dagelijkse werk invulling moet geven aan informatieveilig werken
7. Stelling: mijn instelling heeft duidelijke gedragsregels voor informatieveilig werken
8. Stelling: ik word goed gefaciliteerd door mijn instelling om informatieveilig te kunnen werken (bijvoorbeeld door software, tools, instructies, en andere middelen)
9. Stelling: mijn leidinggevende geeft mij het juiste voorbeeld als het gaat om informatieveilig werken.

**Quizvragen**

1. Je bent onderzoeker en wilt interview-verslagen delen met een externe onderzoeker. Welke van de onderstaande methoden heeft de voorkeur?
2. Waarom is LinkedIn een security risico?
3. Een datalek, hoe klein ook, dien je intern altijd te melden. Klopt dit?
4. Bekijk deze email. Is dit phishing?
5. Welke van deze wachtwoorden is het sterkst?
6. Wat is een datalek? Meerdere antwoorden mogelijk
7. Een docent mag van een student eisen dat deze lid wordt van een Whatsapp-groep van een bepaald vak. Klopt dit?
8. Welke inlogmethode is het veiligst?

**Inventarisatie**

- Over welke onderwerpen heb jij meer kennis nodig om privacybewust en informatieveilig te kunnen werken?
- Heb jij nog opmerkingen of verbeterpunten voor mijn instelling over informatieveilig werken?

# Bijlage B – Vragenlijst MBO Digitaal

**‘Meningvragen’**

1. Hoe belangrijk vind jij informatieveiligheid voor je instelling?
2. Hoeveel aandacht besteed jij over het algemeen tijdens je werk aan informatieveiligheid?
3. Waarom besteed jij tijdens je werk aandacht aan informatieveiligheid? Je kunt meerdere opties kiezen.
4. Stelling: binnen mijn instelling hechten medewerkers veel belang aan informatieveiligheid.
5. Stelling: uit persoonlijke interesse volg ik nieuwe ontwikkelingen op het gebied van informatieveiligheid.
6. Stelling: ik weet hoe ik in mijn dagelijkse werk invulling moet geven aan informatieveilig werken
7. Stelling: mijn instelling heeft duidelijke gedragsregels voor informatieveilig werken
8. Stelling: ik word goed gefaciliteerd door mijn instelling om informatieveilig te kunnen werken (bijvoorbeeld door software, tools, instructies, en andere middelen)
9. Stelling: mijn leidinggevende geeft mij het juiste voorbeeld als het gaat om informatieveilig werken.

**Quizvragen**

1. Mag je video-opnamen maken van een les of een online vergadering?
2. Waarom is LinkedIn een security risico? Meerdere antwoorden mogelijk
3. Een datalek, hoe klein ook, dien je intern altijd te melden. Klopt dit?
4. Bekijk deze email. De link ‘Verkrijg meer opslag’ verwijst naar de URL https://storage.onedrive2023.com. Is dit phishing?
5. Welke van deze wachtwoorden is het sterkst?
6. Wat is een datalek? Meerdere antwoorden mogelijk
7. Een docent mag van een student eisen dat deze lid wordt van een Whatsapp-groep van een bepaald vak.
8. Welke inlogmethode is het veiligst?

**Inventarisatie**

- Over welke onderwerpen heb jij meer kennis nodig om privacybewust en informatieveilig te kunnen werken?
- Heb jij nog opmerkingen of verbeterpunten voor mijn instelling over informatieveilig werken?