Sectorrapport
Security en privacy awareness 2024

Kennis over cybersecurity groeit, maar praktijk blijft achter

BDO

SURF

Managementsamenvatting

Introductie

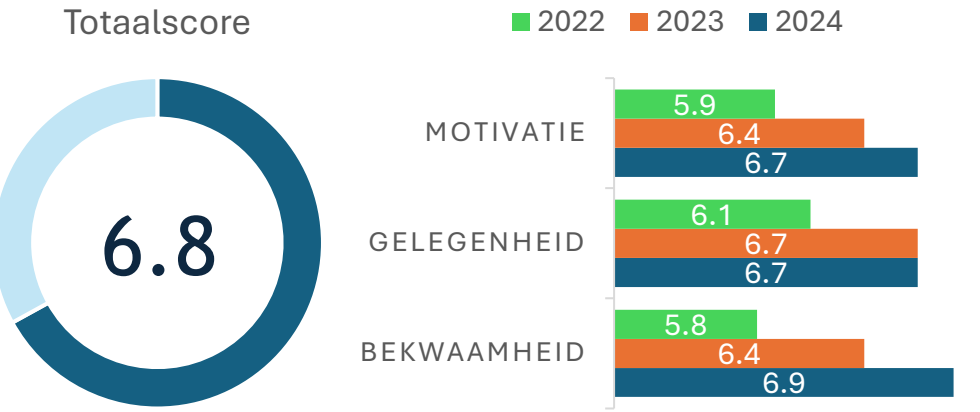
- In opdracht van SURF heeft BDO voor het vierde jaar op rij security- en privacy awarenessmetingen uitgevoerd bij onderwijs- en onderzoeksinstellingen;
- De metingen bestaan uit online vragenlijsten voor de medewerkers, daarnaast zijn voor de sectorrapportage 6 interviews gehouden;
- Deelnemende instellingen: 27, aantal respondenten: 6.391.

Conclusies

- De resultaten tonen een stijgende lijn, maar de meeste instellingen hebben nog niet het minimale, door BDO opgestelde, streefdoel, gehaald;
- De kennis over informatieveiligheid is flink verbeterd. Men heeft nu meer behoefte aan duidelijkheid rondom het verwerken van gevoelige gegevens en welke tools gebruikt mogen worden;
- Veel respondenten weten nog niet hoe security-incidenten en datalekken te melden;
- Hoewel men nog steeds overtuigd is van het belang, is de motivatie om aandacht te besteden aan security en privacy beperkt;
- Er is een afname van tevredenheid over faciliteiten en richtlijnen;
- Men wil minder vrijblijvendheid rond security en privacy gedragsregels;
- Sterke security-cultuurontbreekt.

Aanbevelingen

1. Stem awareness-uitingen af op het dagelijkse werk;
2. Neem belemmeringen voor informatieveilig werken weg, waaronder voor het melden van incidenten;
3. Focus op specifieke thema's (zoals het omgaan met persoonsgegevens);
4. Investeer in een sterke security-cultuur;
5. Maak security en privacy vast onderdeel van onboarding;
6. Houd rekening met sceptici.



Inhoudsopgave

Inleiding

Inleiding

Uit het gezaghebbende Data Breach Investigations Report van Verizon (een datagestuurd rapport over de belangrijkste risico's waarmee organisaties over de hele wereld worden geconfronteerd) blijkt dat de onderwijssector het afgelopen jaar het hoogste aantal cyberincidenten had waarbij organisatie-data in handen kwam van onbevoegden (bron: 2024 Data Breach Investigations Report | Verizon). In het SURF dreigingsbeeld van 2023 wordt benoemd dat de meerderheid van cyberincidenten in de onderwijssector plaatsvindt als gevolg van onbedoeld onveilig handelen door mensen.

Bewustwording van informatiebeveiligings- en privacyrisico's en het correct omgaan met (privacy)gevoelige informatie zijn cruciale factoren in het voorkomen van datalekken en andere cyberincidenten. Door het niveau van awareness te meten kunnen zwakke punten in de kennis en het gedrag worden geïdentificeerd en door het implementeren van gerichte maatregelen kan de algehele informatiebeveiligings- en privacycultuur worden verbeterd. Voldoende reden voor SURF om, na de afgelopen drie jaar, ook dit jaar awarenessmetingen uit te voeren bij instellingen in de sector onderwijs en onderzoek.

Dit rapport presenteert de resultaten van een security en privacy awarenessmeting uitgevoerd bij meerdere onderwijs- en onderzoeksinstellingen. Deze meting geeft inzicht in de huidige stand van zaken op het gebied van informatieveilig en privacybewust gedrag en doet aanbevelingen voor het verhogen van de weerbaarheid tegen cyberdreigingen.

Inleiding (2)

Over de auteurs

Dit rapport is tot stand gekomen in samenwerking tussen SURF en BDO.

SURF

SURF ondersteunt onderwijs- en onderzoeksinstellingen op het gebied van awareness door het stimuleren van kennisdeling tussen instellingen en door 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.

Inge Pronk is als adviseur werkzaam binnen het team Cybersecurity.

Donna Moens is als adviseur werkzaam binnen het team Cybersecurity.

Aanpak

Aanpak awarenessmeting (1)

Het afgelopen voorjaar heeft BDO bij in totaal 27 instellingen security en privacy-awarenessmetingen uitgevoerd. Deze zijn geïnitieerd via SURF.

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

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

Opbouw metingen

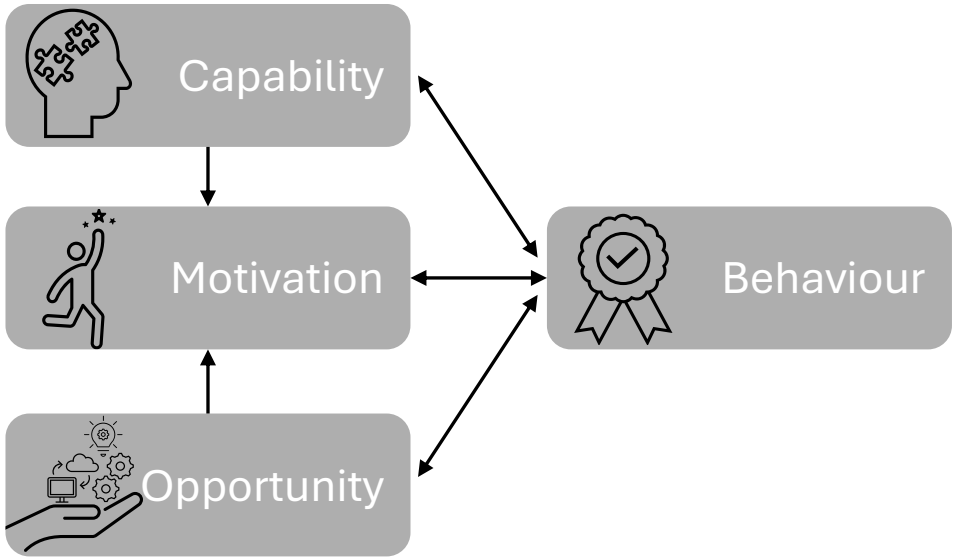
De metingen geven op drie niveaus inzicht:

- 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 zes interviews hebben we deze sectorrapportage opgesteld.

Aanpak awarenessmeting (2)

Gedragsmodel COM-B

Om informatieveilig en privacybewust gedrag in kaart te brengen is net als in 2021, 2022 en 2023 gebruikgemaakt van het COM-B gedragsmodel van Susan Michie. Het COM-B gedragsmodel is een hulpmiddel om gedrag te begrijpen en verklaren. Het model stelt dat gedrag en gedragsverandering beïnvloed wordt door drie componenten: bekwaamheid (capability), gelegenheid (opportunity) en motivatie (motivation).



- Capability (Bekwaamheid): 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 en zijn in staat om de juiste handelingen uit te voeren.
- Opportunity (Gelegenheid): 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.
- Motivation (Motivatie): 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.

Dit COM-B model helpt om gedrag te analyseren en strategieën te ontwikkelen om gedragsverandering te bevorderen.

Vorig jaar werd als onderdeel van de awarenessmeting tevens een gedragsmeting uitgevoerd. Hieruit bleek dat het COM-B model mogelijk geen optimale voorspeller is van daadwerkelijk informatieveilig gedrag. Dit jaar hebben we een aantal vragen aan de meting toegevoegd die dieper ingaan op gedragsaspecten van informatieveiligheid. Dit heeft als doel om de vragenlijst een betere voorspeller van informatieveilig gedrag te maken.

Aanpak awarenessmeting (3)

Onderzoeksvragen

De vragen uit 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 middels een online vragenlijst en interviews. De vragenlijst is geschikt om een globaal inzicht te krijgen in het (zelf gerapporteerde) gedrag en de kennis, mening en ervaringen van de respondenten. De interviews zorgen voor extra duiding en diepgang. De interviews zijn specifiek voor de sectorrapportage gehouden.

De online vragenlijst bevat zogenaamde meningvragen en quizvragen. De meningvragen zijn bedoeld om de motivatie en gelegenheid te onderzoeken. Met de quizvragen wordt de bekwaamheid getoetst.

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

De vragenlijsten zijn in maart en april uitgezet bij ruim 30 instellingen. Hiervan hebben 27 instellingen actief deelgenomen aan de meting. In totaal zijn er 6.391 vragenlijsten ingevuld en we hebben zes interviews gehouden met medewerkers van verschillende instellingen. De interviews vonden plaats in april en mei.

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 awarenessmeting (4)

Doelgroepen

De metingen bestaan uit de volgende doelgroepen:

Type functie:

- Leidinggevend
- Uitvoerend

Type werkzaamheden:

- Onderwijs/onderzoek
- Ondersteuning
- IT ondersteuning
- Overig

In dit rapport wordt per doelgroep bekeken of er verschil is in de resultaten.

Resultaten

Resultaten – Motivatie (1)

Dit hoofdstuk beschrijft de resultaten van de awarenessmeting per component (bekwaamheid, motivatie, gelegenheid). We starten met het component ‘motivatie’.

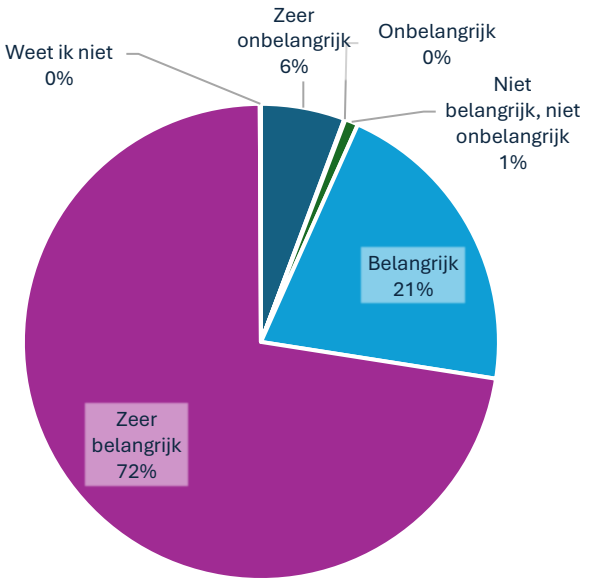
Voor het component motivatie zijn meerdere vragen gesteld aan de respondenten om in kaart te brengen in hoeverre zij (intrinsiek) gemotiveerd zijn om informatieveilig te werken.

> “*Het is een blijk van verantwoordelijkheid nemen richting studenten en collega’s*”.

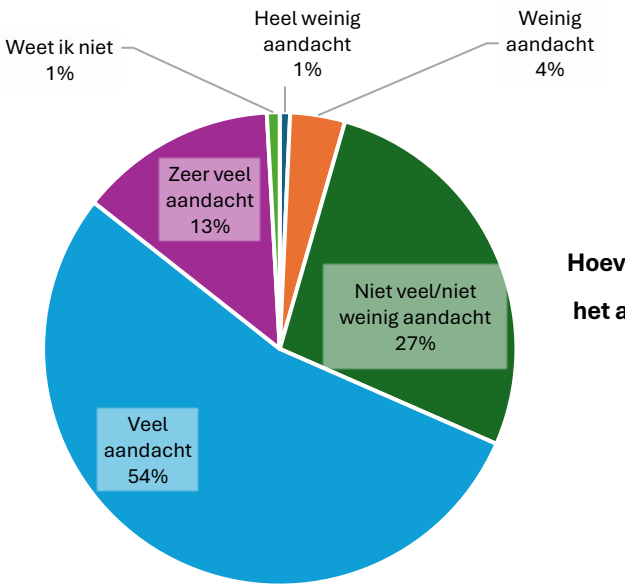
Belangrijk en aandacht

De respondenten hebben aangegeven veel belang te hechten aan informatieveiligheid, waarbij maar liefst 93% het onderwerp als ‘belangrijk’ of als ‘zeer belangrijk’ beschouwt voor hun instelling. En 67% van de respondenten zegt ‘veel aandacht’ of ‘zeer veel aandacht’ te besteden aan informatieveiligheid tijdens hun werk. Deze resultaten laten duidelijk zien dat informatieveiligheid serieus wordt genomen door de respondenten.

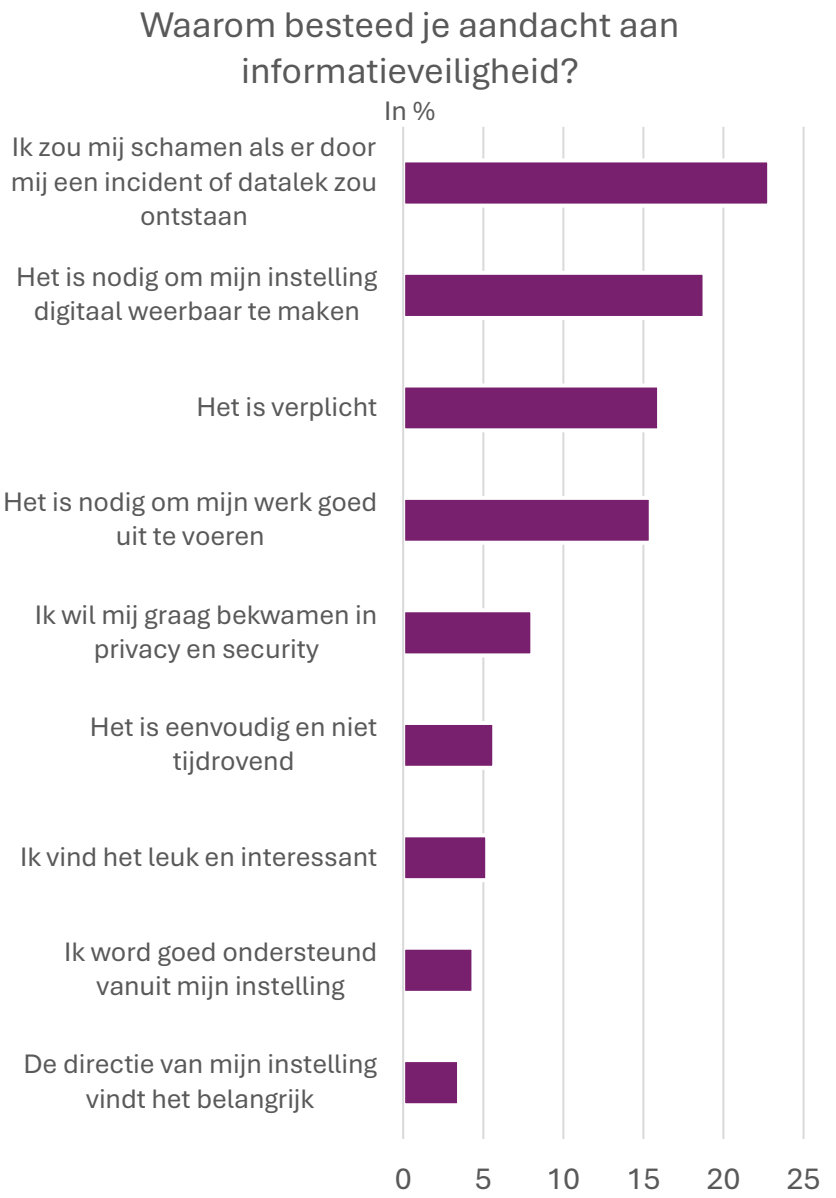
Hoe belangrijk vind jij informatieveiligheid voor jouw instelling?



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



Resultaten – Motivatie (2)



Drijfveren voor informatieveiligheid

Zoals hiervoor is aangeduid, zegt 67% van de respondenten dat ze ‘veel aandacht’ of ‘zeer veel aandacht’ besteden aan informatieveiligheid tijdens hun werk. Als we hier verder op ingaan is te zien dat de voornaamste reden hiervoor is dat men zich zou schamen als er door hen een incident of datalek zou ontstaan.

Naast de hiernaast getoonde antwoordopties, was er ook de mogelijkheid om een open antwoord te geven. Veel van deze antwoorden hebben betrekking op:

- **Moraal**
  - *“Vanuit ethisch perspectief vind ik het belangrijk om toevertrouwde informatie vertrouwelijk te houden”.*
  - *“Het is een morele verplichting tegenover mijn studenten en collega’s”.*
  - *“Ik draai mijn voordeur ook op slot als ik wegga. Digitaal moet je net zo goed nadenken over veiligheid”.*
- **Verwachtingen**
  - *“Ik wil dat andere organisaties zorgvuldig met mijn gegevens omgaan, dus vind ik het belangrijk om zelf ook zorgvuldig met andermans gegevens om te gaan”.*
  - *“Ik zou het zelf ook niet leuk vinden als er met mijn persoonsgegevens onzorgvuldig wordt omgegaan”.*
- **Verantwoordelijkheidsgevoel**
  - *“Ik voel me er verantwoordelijk voor dat ik het goed doe”.*
  - *“Je hebt de verantwoordelijkheid de privacy van degene die jou vertrouwelijke, persoonlijke, informatie geeft te waarborgen”.*

Resultaten – Motivatie (3)

Persoonlijke interesses

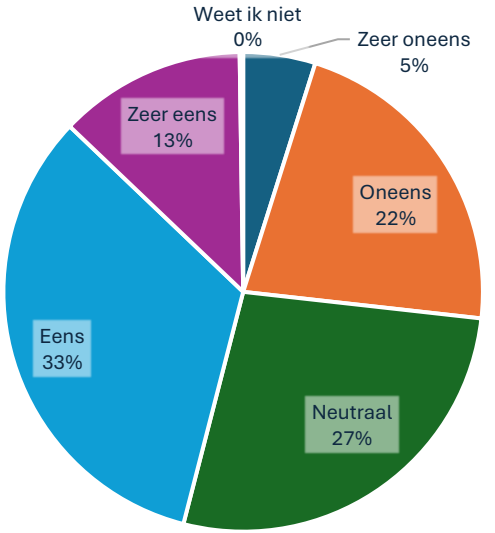
Een van de drijfveren voor het besteden van aandacht aan informatieveiligheid die nader is onderzocht, is persoonlijke interesse. Op de vorige pagina is te zien dat de antwoordoptie ‘Ik vind het leuk en interessant’ door veel respondenten niet als reden wordt gezien waarom ze aandacht besteden aan informatieveiligheid.

> “*Digitale veiligheid is voor mij (en 90% van mijn collega's) over het algemeen echt geen interessant -maar wel heel noodzakelijk- thema*”.

Als we kijken naar de stelling ‘Uit persoonlijke interesse volg ik nieuwe ontwikkelingen op het gebied van informatieveiligheid’ blijkt dat een minderheid van de respondenten (46%) het (zeer) eens is met deze stelling. Hierbij is wel een groot verschil te zien tussen de respondenten die werkzaam zijn in de IT ondersteuning en de respondenten die in een van de andere drie groepen werkzaam zijn. Bij de medewerkers uit de IT ondersteuning betrof dit namelijk 71% en bij de andere groepen varieerde dit van 41% tot en met 50%.

Stelling:

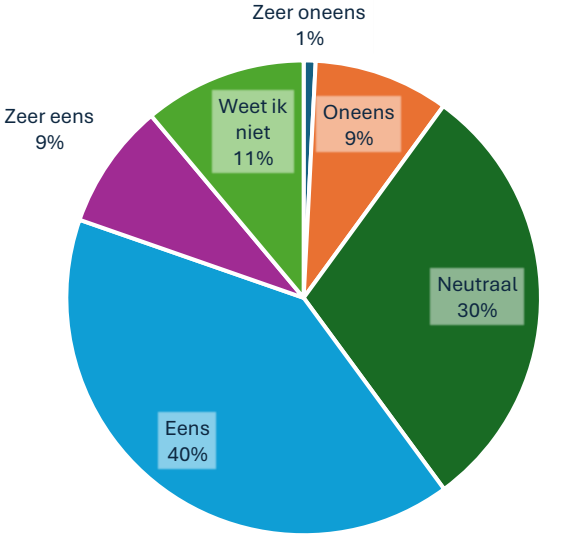
Uit persoonlijke interesse volg ik nieuwe ontwikkelingen op het gebied van informatieveiligheid.



Belang bij collega’s

Bijna alle respondenten (94%) vinden informatieveiligheid belangrijk voor de instelling, maar als er gekeken wordt naar de stelling ‘Binnen mijn instelling hechten medewerkers veel belang aan informatieveiligheid’ is te zien dat slechts een krappe minderheid (49%) het hier (zeer) mee eens is.

- *“Ik merk dat ík het wel belangrijk vind maar ik zie ook dat sommige collega's het maar een gedoe vinden, en extra werk…”.*
- *“Niet alleen awareness is belangrijk, maar dat medewerkers ook echter ander gedrag vertonen”.*
- *“Ik denk dat dit een onderwerp is waarvan iedereen het belang wel inziet, maar wat ook als "gedoe" voelt om hier actief rekening mee te houden”.*



Stelling:

Binnen mijn instelling hechten medewerkers veel belang aan informatieveiligheid.

Resultaten – Gelegenheid (1)

Gelegenheid

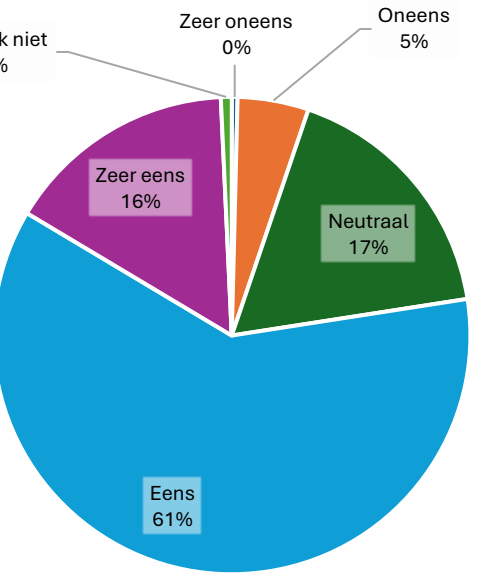
Voor het component gelegenheid zijn meerdere stellingen voorgelegd aan de respondenten om in kaart te brengen in hoeverre zij gefaciliteerd worden om informatieveilig te werken. Daarnaast zijn er in aanvulling op de stellingen van voorgaande jaren, drie nieuwe stellingen toegevoegd die inzicht geven of respondenten een incident durven te melden.

Informatieveilig werken en gedragsregels

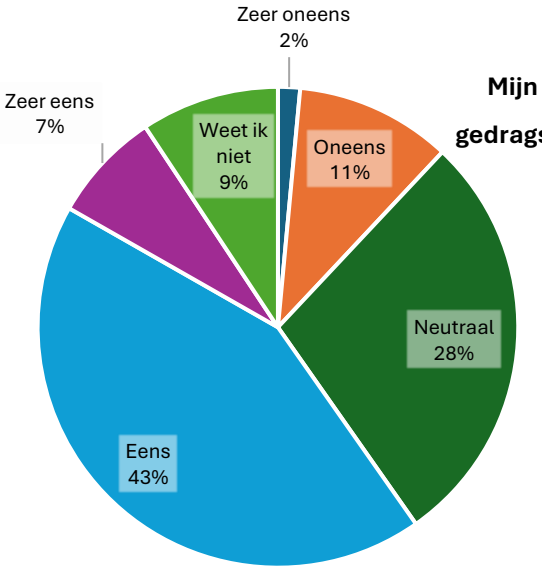
Enerzijds zegt slechts 50% van de respondenten het (zeer) eens te zijn met de stelling dat hun instelling duidelijke gedragsregels heeft voor informatieveilig werken. Anderzijds weet 77% van de respondenten naar eigen zeggen hoe ze hier tijdens hun dagelijkse werk invulling aan moeten geven. Alhoewel we ernaar streven dat **alle** medewerkers dit weten, is dit een redelijk hoog percentage. Mogelijk komt dat omdat respondenten door eigen ervaring weten hoe ze informatieveilig moeten werken zonder dat ze de gedragsregels van de instelling precies kennen. Het kan natuurlijk ook dat sommigen denken te weten hoe het moet, maar dat ze niet volgens de richtlijnen van de instelling werken.

- *"Veilig omgaan met de gegevens van studenten doe ik automatisch wegens jarenlange ervaring".*
- *"Volgens mij werken we nu op basis van gezond verstand hoe we met privacy gevoelige gegevens omgaan. Hierdoor kan de werkwijze tussen de afdelingen verschillen. Een protocol is wellicht handig. En als die er al is deze breder communiceren".*

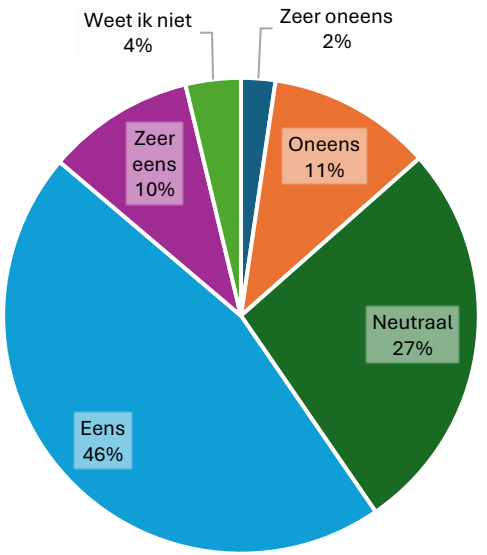
Stelling:
Ik weet hoe ik in mijn dagelijkse werk invulling moet geven aan informatieveilig werken.



Stelling:
Mijn instelling heeft duidelijke gedragsregels voor informatieveilig werken.



Resultaten – Gelegenheid (2)

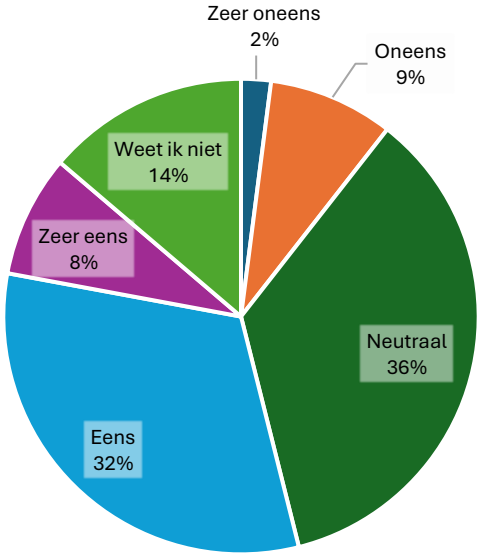


Stelling:

Ik word goed gefaciliteerd door mijn instelling om informatieveilig te kunnen werken.

Stelling:

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



Drijfveren voor informatieveiligheid

Van de respondenten is 56% het (zeer) eens met de stelling dat zij goed worden gefaciliteerd door hun instelling om informatieveilig te werken.

In de open antwoorden hebben veel respondenten aangegeven behoefte te hebben aan een goede wachtwoordmanager en instructies hierover. Daarnaast willen meerdere respondenten dat een VPN wordt aangeboden en zegt men dat het ontbreekt aan "*de juiste tools voor het doen van onderzoek*" of een "*overzicht met ondersteunde tools, en ondersteunde alternatieve voor niet-ondersteunde tools*".

Voorbeeldgedrag

Vorig jaar was 39% van de respondenten positief over de voorbeeldrol van hun leidinggevende ten aanzien van privacy en informatiebeveiliging. Met een percentage van 40% is dit jaar nauwelijks een verandering te zien. Deze minderheid is ook terug te zien in de antwoorden die zijn gegeven op de vraag "Heb jij nog opmerkingen of verbeterpunten voor jouw instelling over informatieveilig werken?":

> *"In ons instituut leeft informatieveilig werken niet en dat vind ik hinderlijk. Het gaat ook over het geven van goed voorbeeld aan elkaar & studenten. Het wordt vaker als administratieve last gezien. Het management & directie geeft er weinig urgentie aan. Zonde!"*.

Resultaten – Gelegenheid (3)

Remmende factor

Slechts 20% van de respondenten zegt de security en privacy gedragsregels als remmende factor te ervaren tijdens hun dagelijkse werkzaamheden. Dit is een kleine minderheid, maar dit geluid komt wel geregeld terug in de open antwoorden:

- *"Veiligheid staat voorop, maar efficiëntie komt op 2. Deze 2 gaan hand in hand en zouden niet in elkaars weg moeten staan. maak het makkelijker (ook inhoudelijker) voor de medewerker om deze security regels te volgen en handhaven waarbij we ook gewoon goed en makkelijk ons werk kunnen blijven doen. (Referentie: sms authenticatie, waardeloos)".*
- *"Zorg dat al die veiligheidsregels niet belemmerend werken. Door allerlei dingen heen klikken, formulieren invullen, extra devices checken: je wordt er moe van. Op een dag gaan we weer terug naar pen en papier, vrees ik, omdat al die regels niet werkbaar zijn".*
- *"Ik merk regelmatig op dat [collega's] denken dat door regels niks meer mag, waardoor privacy als remmende factor ervaren wordt. 'Dan doen we het maar niet, want dan kan het niet fout gaan'" .*

Afgaande op de open antwoorden zijn er ook veel respondenten die de gedragsregels juist te vrijblijvend vinden. Men heeft behoefte aan meer duidelijkheid en vindt dat er consequenties moeten zijn als mensen de regels niet naleven.

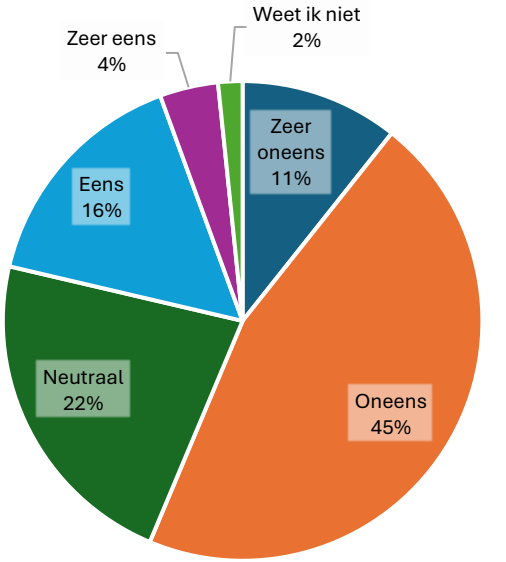
Open antwoorden:

- *"Ik ervaar (te) grote vrijheid m.b.t. het (niet) volgen van de door privacy & security opgestelde richtlijnen en gedragsregels".*
- *"Geef duidelijkheid en maak zaken soms ook gewoon verplicht. Laat de keuze niet vrijblijvend aan de medewerker. Er moet een cultuur komen waarbij we elkaar aanspreken want afspraken maken is één, doen is twee en elkaar aanspreken, corrigeren en handhaven is drie. Het schort bij HR vooral aan elkaar aanspreken, corrigeren en handhaven".*
- *"Alle medewerkers (verplicht) een digitale training laten volgen over de risico's en gevolgen van niet informatieveilig werken en wat wat jij als medewerker hier aan kan doen. Na de training (verplicht) een toets afnemen om te controleren of bewustwording en kennis voldoende is".*
- *"Ik vind ons als organisatie nog best 'lief'. Het beleid mag van mij best wat strakker en dwingender, zoals ik dit vanuit commerciële organisaties gewend ben. De 'volwassenheid' van de gemiddelde medewerker op het gebied van informatieveilig werken kan ook nog wel een boost gebruiken".*

Stelling:

Ik ervaar de security en privacy gedragsregels als een remmende factor tijdens mijn dagelijkse werkzaamheden.

(nieuwe vraag t.o.v. vorige jaren)



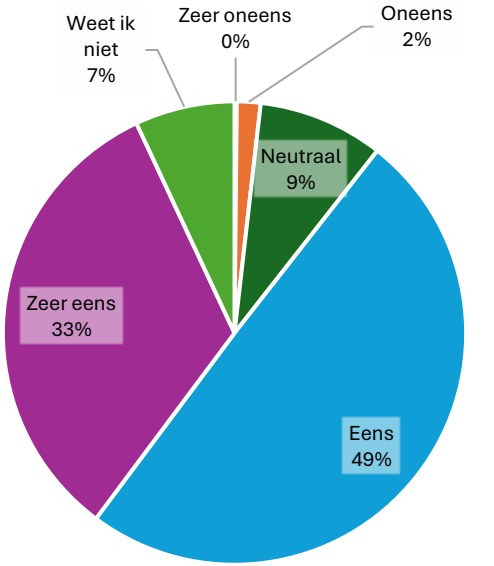
Resultaten – Gelegenheid (4)

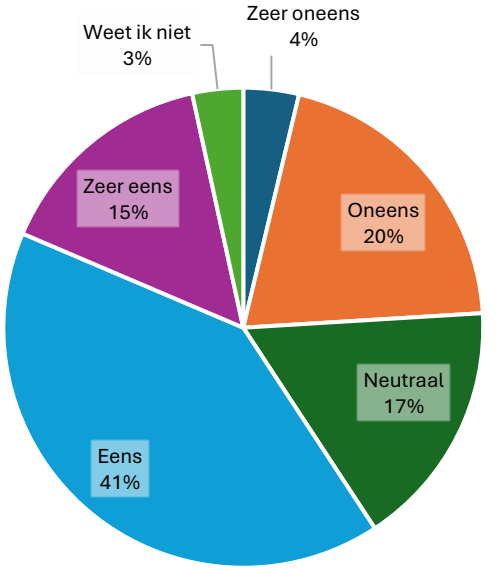
Melden van incidenten

Als we kijken naar het melden van incidenten, dan blijkt dat 82% van de respondenten het (zeer) eens is met de stelling ‘Ik durf een security- of privacy incident altijd te melden, ook als ik die zelf heb veroorzaakt’. Anderzijds zegt slechts 56% van de respondenten het (zeer) eens te zijn met de stelling ‘Ik weet wanneer en hoe ik een security- of privacy incident moet melden’. De wil is er dus wel, maar de kennis nog niet voldoende. Een aantal respondenten heeft tips gegeven om dit onder de aandacht te brengen bij de medewerkers:

- *“Door bij of op werkplekken informatie korte instructies te plaatsen waar je op moet letten, hoe je een incident kunt herkennen en wat je moet doen wanneer je een incident hebt ontdekt. Moet je bijvoorbeeld direct ook je laptop uitzetten, of juist niet?”*
- *“Er is een hoop informatie en ondersteuning beschikbaar, echter veel medewerkers kiezen er bewust voor deze niet te gebruiken. Als daar iets van gezegd wordt, komt een negatieve reactie. "Ik doe het altijd zo" of "Waar bemoei je je mee". Daarnaast voel ik mij niet veilig om een melding te maken als ik bijvoorbeeld een datalek zou melden. Zeer grote kans dat de melder dit terug krijgt en er hinder van zal ondervinden. Je bent al gauw een verklikker. Op dit vlak is er echt een cultuuromslag nodig”.*
- *“CISO office en security team en privacy teams, waarom zijn zij zo onzichtbaar? Kunnen zij een demo geven over wat zij doen en belangrijk vinden?”*

Stelling:
Ik durf een security- of privacy incident altijd te melden, ook als ik die zelf heb veroorzaakt.
(nieuwe vraag t.o.v. vorige jaren)





Stelling:
Ik weet wanneer en hoe ik een security- of privacy incident moet melden.
(nieuwe vraag t.o.v. vorige jaren)

Resultaten – Bekwaamheid (1)

Bekwaamheid

Voor het component bekwaamheid zijn acht toetsvragen (zie bijlage A) voorgelegd aan de respondenten om in kaart te brengen in hoeverre zij de juiste kennis hebben om informatieveilig te werken.

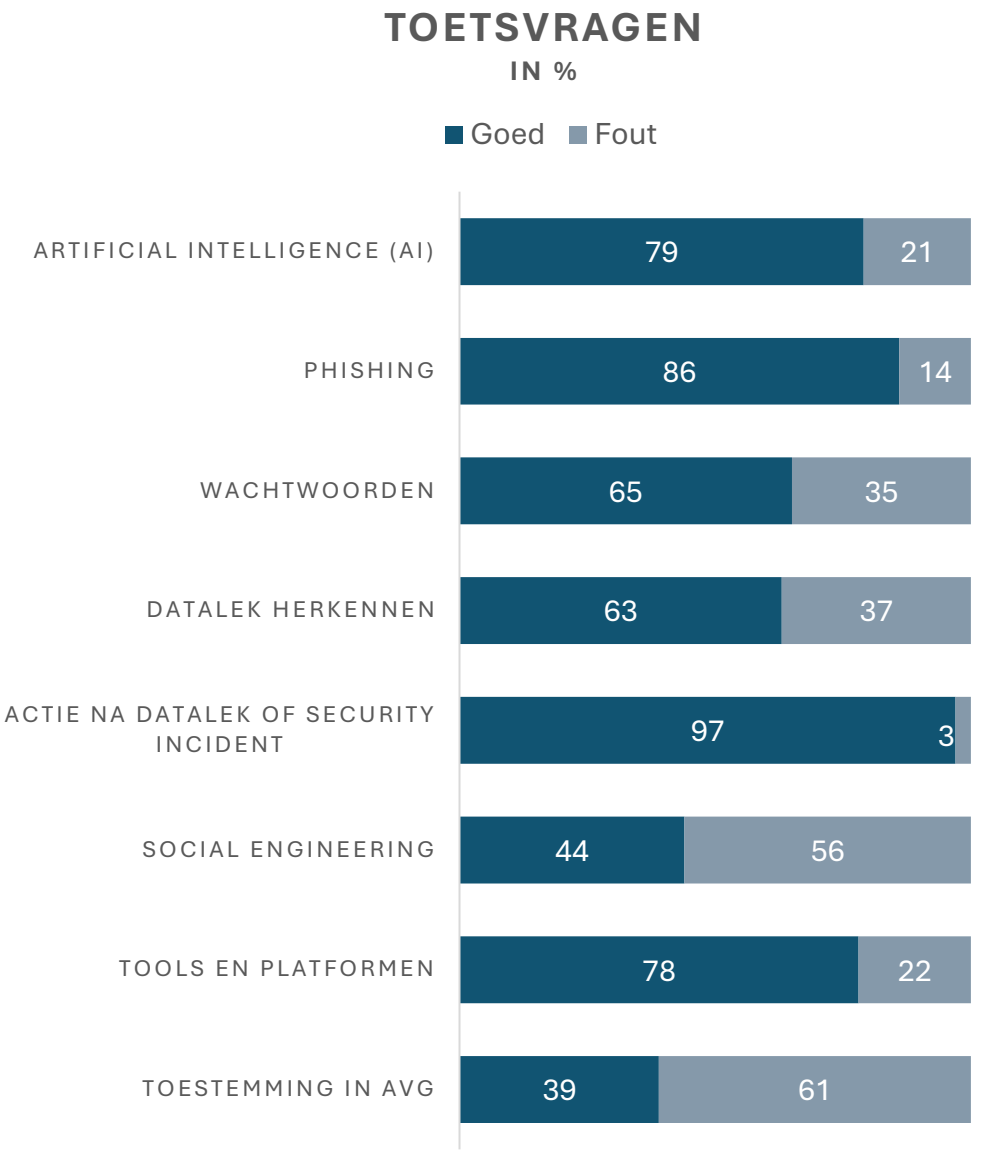
Quiz resultaten

In de meting is op twee van de acht toetsvragen door het merendeel van de respondenten een foutief antwoord gegeven:

- Toestemming in AVG
- Social engineering

Vragen waar goed op werd gescoord zijn:

- Je vergeet een stapel gemaakte toetsen in de trein. Wat doe je als eerste? (97% goed);
- Waaraan kun je zien dat onderstaand bericht phishing is? (86% goed);
- Welke stelling(en) over het gebruik van AI, zoals ChatGPT, is/zijn waar? (79% goed);
- Studenten vragen aan een docent om een Whatsapp-groep aan te maken om toetsresultaten en verdiepende artikelen op de lesstof te delen. Waarom is dit onwenselijk? (78% goed).



Resultaten – Bekwaamheid (2)

Toestemming in AVG – 61% fout

Bij de feestelijke opening van een nieuw onderwijsgebouw worden foto's gemaakt voor de website van de instelling. Is het nodig om aan iedereen die op de foto's staat expliciete toestemming te vragen?

a) Ja, maar alleen als ze herkenbaar in beeld komen (47.5%)
b) Ja, ook als ze niet herkenbaar in beeld komen (13.7%)
c) Nee, onder bepaalde voorwaarden hoeft dit niet ← (38.9%)

Het juiste antwoord is C. Je kunt je bij het maken van sfeerbeelden op evenementen beroepen op een gerechtvaardigd belang. Als je maatregelen treft om de privacy van de aanwezigen te waarborgen is het niet nodig om individueel toestemming te vragen. Maatregelen zijn bijvoorbeeld:

- Op tijd aankondigen dat er een fotograaf aanwezig zal zijn, bijvoorbeeld bij de inschrijving van het evenement;
- Geef aanwezigen de mogelijkheid om niet gefotografeerd te worden, bijvoorbeeld door een badge of keycord in een opvallende kleur te dragen;
- Houd rekening met het type evenement en de doelgroep. Als het kwetsbare mensen betreft, of er zijn bijzondere persoonsgegevens uit af te leiden, wees dan extra zorgvuldig;
- Als je op het evenement portretfoto's maakt en wilt publiceren, gaat het niet meer om sfeerbeelden. Je dient dan wel expliciete toestemming te hebben van de geportretteerde.

Social engineering – 56% fout

Welk van onderstaande situaties zijn voorbeelden van social engineering?

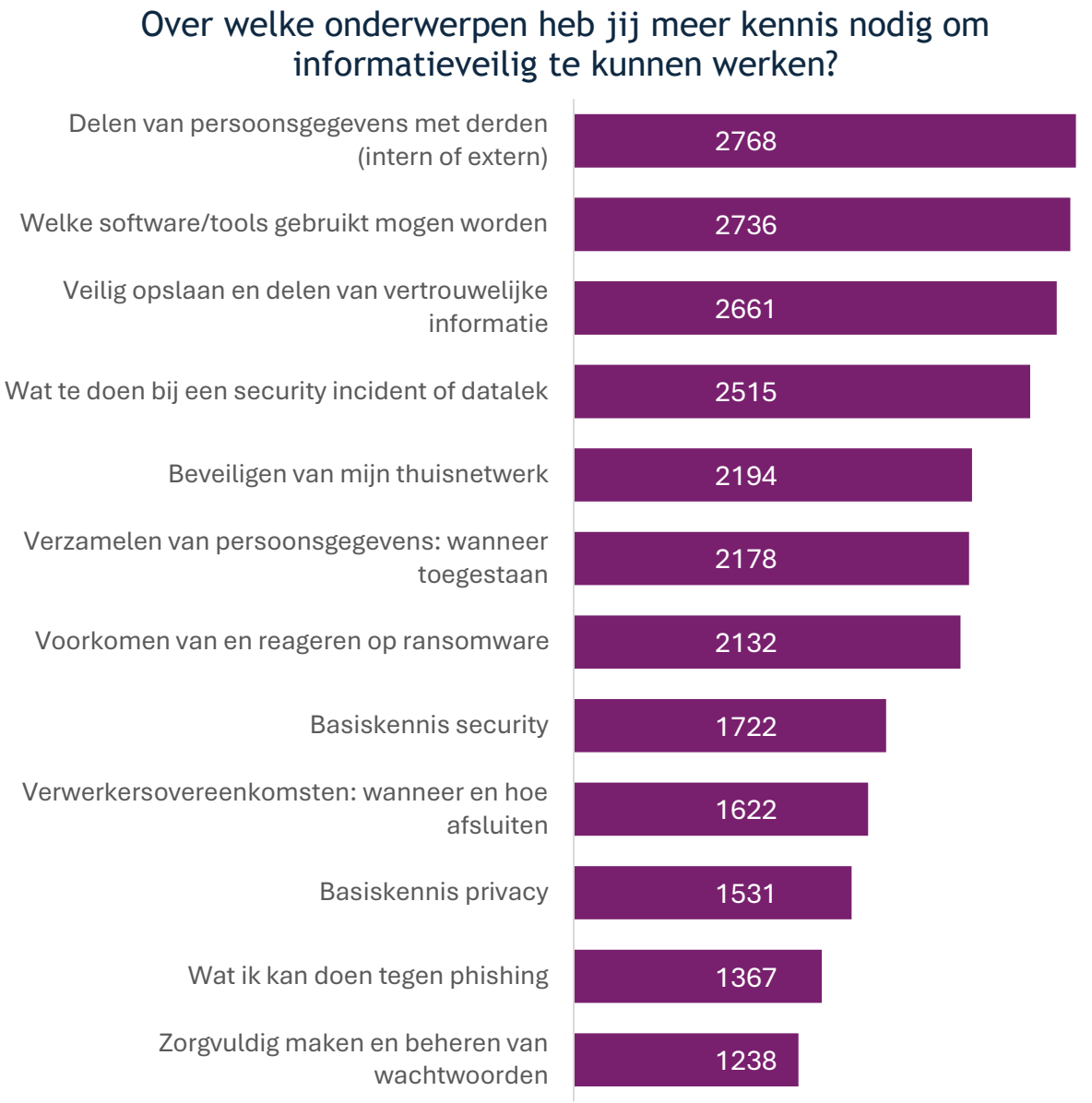
1. Iemand doet zich voor als een medewerker en vraagt aan de financiële afdeling om zijn/haar bankrekeningnummer aan te passen.
2. Er wordt een phishing e-mail gestuurd naar alle medewerkers van de instelling vanuit een e-mail adres dat afkomstig lijkt van de IT-afdeling. Hierin wordt gevraagd om een wachtwoord via een link te resetten.
3. Iemand kijkt mee over je schouder terwijl jij je wachtwoord intypt en/of met gevoelige informatie werkt.

a) Situatie 1 en 2 (36.3%)
b) Alleen situatie 1 (19.5%)
c) Situatie 1, 2 en 3 ← (44.2%)

Het juiste antwoord is C.

Al deze situaties zijn voorbeelden van social engineering. Bij social engineering maken internetcriminelen misbruik van menselijke eigenschappen zoals angst, hebzucht, nieuwsgierigheid, vertrouwen en onwetendheid voor hun eigen voordeel. Voorbeelden zijn phishing, whatsapp-fraude, shoulder surfing (over iemands schouder meekijken terwijl diegene werkt met gevoelige informatie) en impersonatie. Let op met wat je deelt op sociale media. Hoe meer informatie je openbaar op internet deelt, hoe makkelijker het is voor cybercriminelen om succesvol een social engineering-aanval uit te voeren.

Resultaten – Bekwaamheid (3)



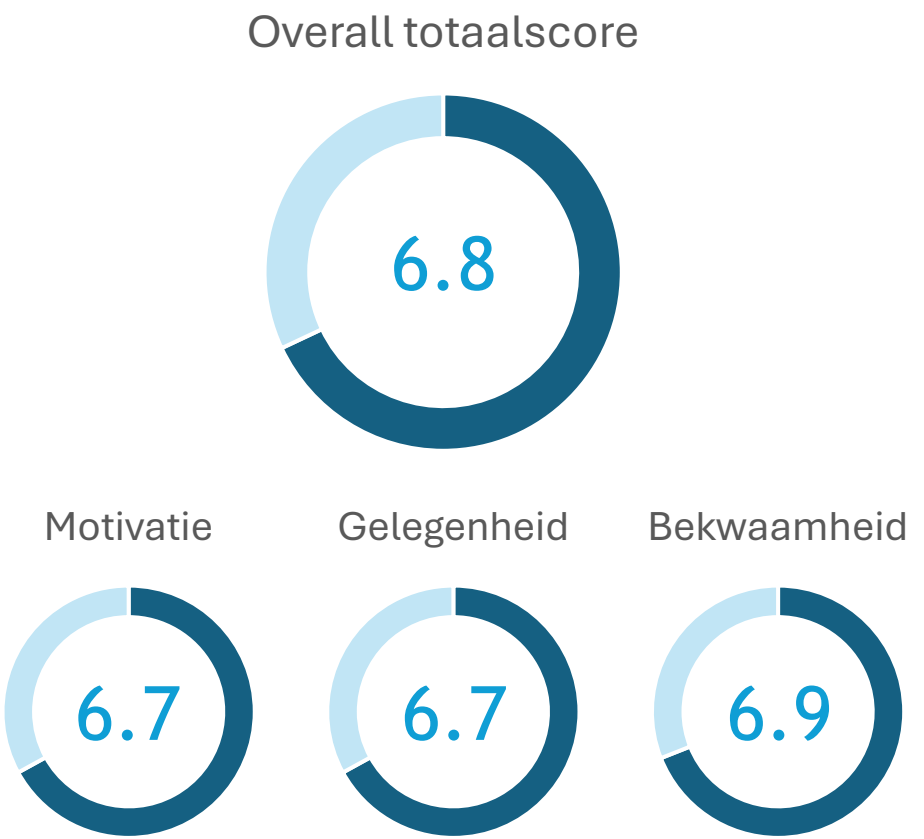
Meer kennis nodig

Tot slot is aan de respondenten gevraagd op welke thema's zij nog meer kennis nodig hebben om informatieveilig te kunnen werken. Hiernaast is te zien hoe vaak de gegeven thema's zijn gekozen. De respondenten konden hierbij meerdere antwoorden selecteren en een open antwoord geven. In de open antwoorden is onder meer het volgende gezegd:

- "*ons Ib-beleid*"
- "*data-archiving/ opschoning en bewaartermijnen*"
- "*Hoe om te gaan met beeldmateriaal van personen*"
- "*waar ik (anoniem) terecht kan als ik zie dat een collega niet veilig met privacygevoelige info omgaat*"
- "*Hoe ik beschermd ben als melder van een incident*"
- "*Hoe je in je dagelijkse werkzaamheden herkent wanneer het privacy / informatieveiligheid raakt. En hoe maak je het werkbaar voor jezelf en je collega's?*"
- "*alle onderwerpen zal ik opzoeken op sharepoint als ik hiermee te maken krijg, ik heb het dus nodig dat daar de juiste informatie staat*"

Resultaten in cijfers (1)

In dit hoofdstuk zijn de resultaten van de awarenessmeting in cijfers uitgewerkt. Op basis van de ingevulde vragenlijsten heeft iedere deelnemende instelling een totaalscore op een schaal van 1-10 ontvangen voor hun instelling inclusief de score per component. Hieronder zijn de gemiddelde totaalscore (‘overall totaalscore’) en de gemiddelde score per component te zien van de 6.931 respondenten.



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)

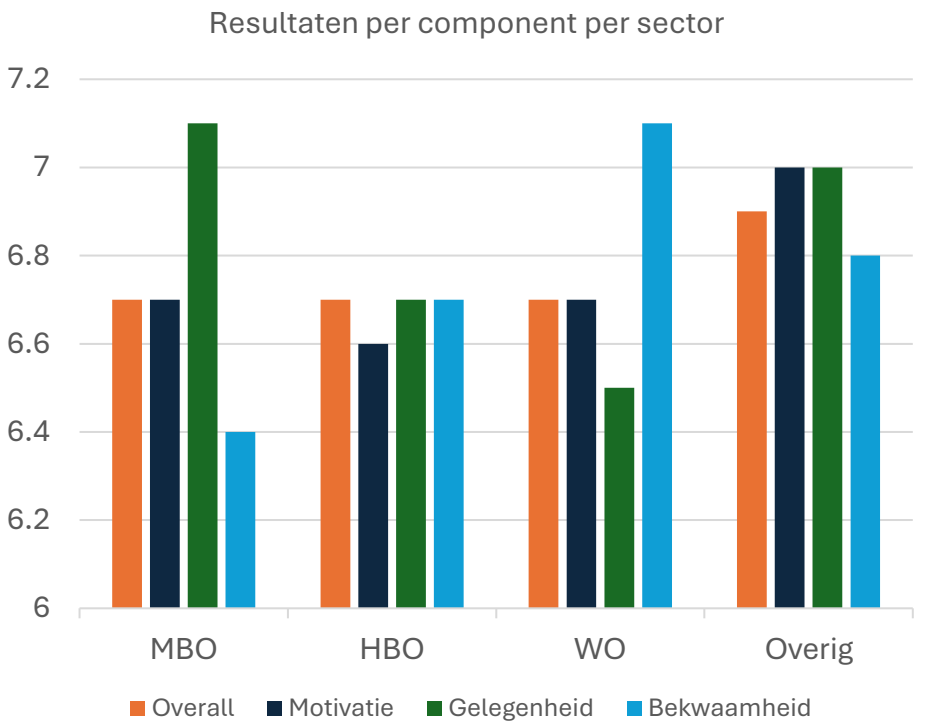
Resultaten per sector

Uit de resultaten per sector blijkt dat de sector ‘overig’ het hoogst scoort met een totaalscore van 6,9 en dat de sectoren MBO, HBO en WO alle drie een totaalscore van 6,7 hebben behaald. Wat hierbij opvalt is dat er per component redelijk grote verschillen te zien zijn.

	MBO	HBO	WO	Overig*	Totaal
Aantal instellingen	3	11	8	5	27
Aantal respondenten	232	3.062	2.585	512	6.391

Tabel 1: Aantal deelnemers in 2024

* Overig betreft onderzoeks- en kennisinstellingen

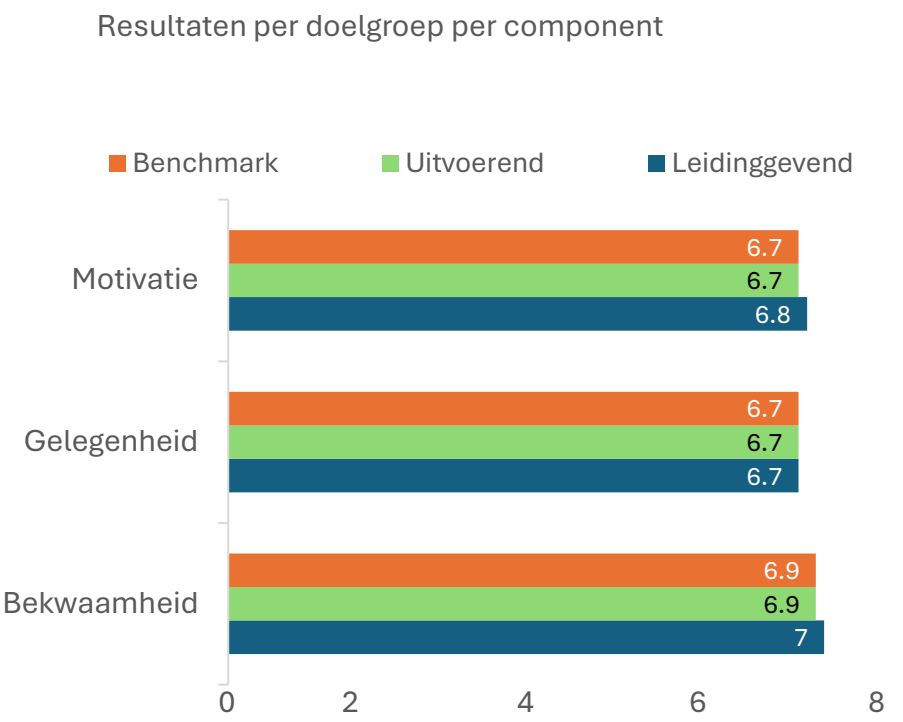


Resultaten in cijfers (3)

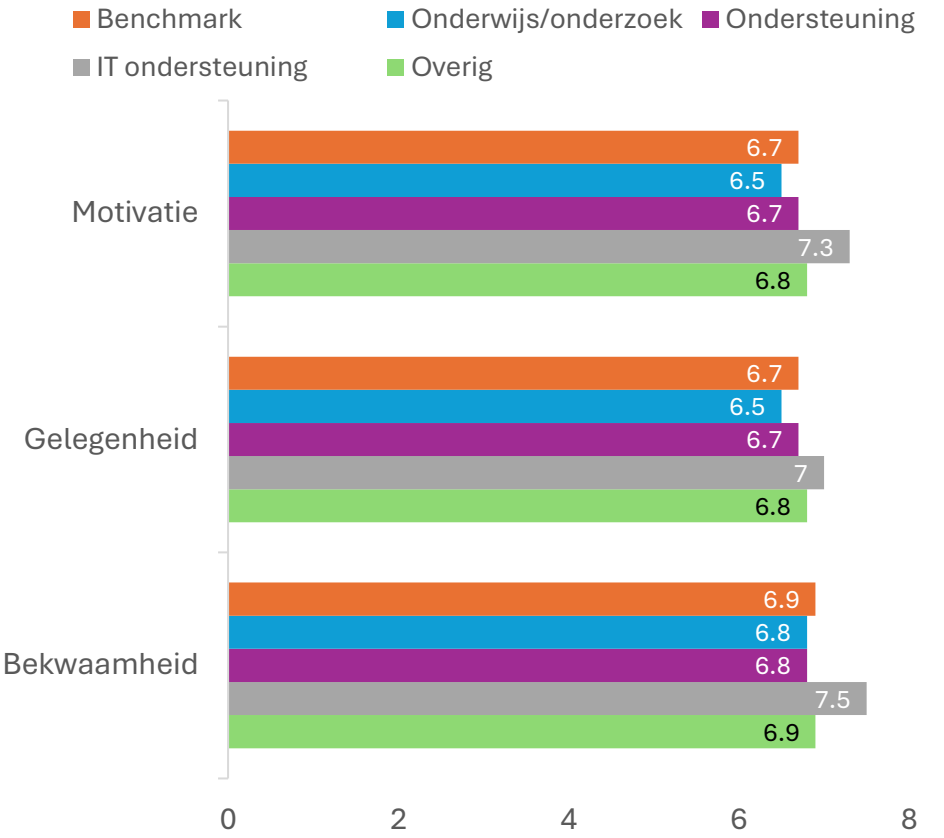
Resultaten per doelgroep

Hieronder is een analyse gemaakt op basis van 2 groepen:

1. Leidinggevend vs uitvoerend
   Leidinggevenden scoren zowel op het component motivatie als op het component bekwaamheid 0,1 hoger dan uitvoerenden. Op gelegenheid scoren ze beide hetzelfde.



2. Per functiegroep
   Voor de meting zijn 4 functiegroepen gehanteerd: onderwijs/onderzoek, ondersteuning, IT ondersteuning en overig. Uit de resultaten komt naar voren dat de groep onderwijs/onderzoek lager scoren dan de overige functiegroepen en dat IT ondersteuning op alle drie de componenten het hoogste scoort.



Verbeterpunten respondenten

Verbeterpunten respondenten (1)

Verbeterpunten

In de vragenlijst en tijdens de interviews is aan de respondenten gevraagd welke opmerkingen of verbeterpunten zij hebben voor hun instelling zodat zij beter privacybewust en informatieveilig kunnen werken. Op basis van de 6 interviews en de duizenden reacties zijn tien veel voorkomende thema's geselecteerd die in dit hoofdstuk worden toegelicht.

Betere informatievoorziening

Een flink aantal respondenten vindt dat de informatievoorziening over informatiebeveiliging en privacy verbeterd moet worden. Ze willen graag één centrale plek waar de informatie makkelijk terug te vinden is. De informatie moet zo eenvoudig, kort en bondig mogelijk worden geformuleerd en gecommuniceerd.

- *"Als we het belang van bewustwording en de toepassing van informatiebeveiliging willen benadrukken (en dat is essentieel), moeten we ervoor zorgen dat relevante informatie gemakkelijker en effectiever toegankelijk is dan op dit moment het geval is"*.
- *"Ik merk dat mensen nu vaak niet veilig werken omdat ze niet weten hoe en de uitleg te moeilijk/langdradig is, wat hun afschrikt"*.

Continue aandacht

In aanvulling op de hiervoor benoemde informatievoorziening, vinden meerdere respondenten dat er blijvende aandacht moet worden besteed aan informatiebeveiliging en privacy door het continu te herhalen en regelmatig updates te geven.

> *"Goede voorbeelden verspreiden, herhalen van de boodschap en van het belang van informatieveiligheid. Het moet meer in onze werkwijzen komen, we moeten het automatisch(er) goed gaan doen. Het is voor mij nu nog teveel mijn eigen gezonde verstand, en eigen aannames, waarop ik me baseer"*.

Gebruik van password manager

In de reacties is vaak terug te lezen dat de respondenten vinden dat de instelling als werkgever het personeel van een password manager moet voorzien voor het veilig bewaren van wachtwoorden. Hierbij zijn sommige ook op zoek naar ondersteuning bij het gebruik ervan.

> *"Het zou fijn zijn als er een heldere instructie komt voor het starten met en het onderhouden van een wachtwoordmanager. Ik ben er nu mee gestart (door de [e-learning tool]), maar ik heb het gevoel dat ik nog aan het pionieren ben, en dat ik zelf dingen moet uitzoeken waarvan ik de consequenties nog niet volledig overzie (wat gebeurt er als ik mijn telefoon verlies, welke opties zijn noodzakelijk en/of handig)"*.

Verbeterpunten respondenten (2)

Introductieprogramma

Meerdere respondenten, waarvan sommigen nog maar kort in dienst zijn, hebben benadrukt dat ze tijdens hun indiensttreding geen informatie hebben gekregen over informatiebeveiliging en/of privacy, maar vinden wel dat dit een vast onderdeel moet uitmaken van het introductieprogramma.

> "*Wat mij opviel is dat er geen goede onboarding proces was waar ook dit onderdeel goed werd uitgelegd. Manier van werken of een moment dat ik met een collega dit onderwerp even besprak. Het lijkt mij handig, op je eerste dag bij de [naam instelling], dat je in ieder geval naar de juiste pagina gestuurd wordt en dat je de informatie hierover doorneemt*".

Centraal & gecommuniceerd meldpunt

Veel respondenten hebben aangegeven dat ze niet weten waar en/of hoe ze een incident kunnen melden of dat ze hier na lang zoeken op het intranet pas achter waren gekomen. Ze zijn op zoek naar 1 centraal, goed gecommuniceerd, meldpunt voor incidenten en naar:

> "*Een (makkelijke) manier om binnengekomen spammails ergens te rapporteren, zonder voor ieder wissewasje een ticket bij [de helpdesk] aan te maken. Ik mis in Outlook, en wellicht ligt dit aan de mogelijkheden binnen Outlook, een 'delete and report'-achtige optie. Mails die clearly (of voor sommigen minder duidelijk) phishing of erger zijn moet ik op een makkelijke wijze kunnen melden, zonder dat het al te veel moeite kost*"

Clear screen

Er wordt opgemerkt dat veel medewerkers weglopen van hun device zonder deze te vergrendelen.

> "*Herinner medewerkers eraan dat het belangrijk is om hun scherm te locken wanneer zij hun plek verlaten, hoe kort ook. Ik zie nog veel om mij heen dat collega's dit niet doen. Bij mijn vorige werkgever had ik een collega die ons er altijd op wees, waardoor ik er nu zelf heel alert op ben*".

Echter blijkt uit onderstaande opmerking dat bewustwording alleen het probleem niet zal oplossen:

> "*Door het omslachtige aanmeldproces betrap ik mezelf erop dat ik mijn werkstation niet vergrendel als ik wegloop. Dat scheelt een hoop gedoe als ik weer wil gaan werken. Wat mij betreft zou een gebruikersvriendelijker aanmeldproces uiteindelijk veiliger zijn*".

Aanbod van tools/software

Veel respondenten erkennen het belang van privacy en informatiebeveiliging, maar vinden het lastig dat ze beperkt worden in het gebruik van tools/software:

> "*Als het te lastig wordt om mee te werken, gaan medewerkers iets anders gebruiken. waardoor de drang naar meer veiligheid zorgt voor minder veiligheid*".

Ze zijn ten aanzien van tools en software vooral op zoek naar "*...duidelijke communicatie over & toegankelijkheid van het aanbod van tools & materialen om veilig te werken*".

Verbeterpunten respondenten (3)

Multifactorauthenticatie (MFA)

Veel respondenten hebben hun frustraties geuit over het gebruik van multifactorauthenticatie (MFA). Deze frustraties hebben met name betrekking op het volgende:

- Ze moeten zich meerdere keren per dag opnieuw authenticeren;
- Ze moeten twee verschillende soorten MFA-oplossingen gebruiken;
- Ze moeten hun privételefoon hiervoor gebruiken.

Tone at the top

Er wordt opgemerkt dat de leidinggevenden niet altijd het juiste voorbeeld geven en/of onvoldoende het belang van informatieveilig gedrag uitdragen.

> "*Ik zou er vanuit de leiding meer over communiceren. Dat kan laagdrempelig en vooral om het on top of mind te houden*".

Echter zijn er ook medewerkers die juist vinden dat het niet alleen vanuit de top van de organisatie moet komen:

- "*Overweeg ook een bottom-up approach. Hoe korter de lijntjes, hoe effectiever de campagne*".
- "*Medewerkers betrekken door ambassadeurs per afdeling verplicht te stellen*".

Zichtbaarheid privacy & security officers

Meerdere respondenten vinden dat de privacy en security officers een meer zichtbare rol moeten hebben binnen de instelling:

> "*Naar mijn mening is het goed als de privacy officer periodiek met afdelingen in gesprek gaat en onderzoek doet naar de verwerking van data etc. Pas dan (aan de hand van concrete voorbeelden, toegespitst op hun praktijk) zullen mensen naar mijn mening zich realiseren of ze goed of minder goed daarmee bezig zijn*".

Vergelijking voorgaande jaren

Vergelijking met voorgaande jaren (1)

Hoe zijn de resultaten van nu in vergelijking met de resultaten van 2021 t/m 2023?

Aantal deelnemers

Allereerst is er een verschil in het aantal deelnemers. Dit jaar zijn er bijna de helft minder respondenten dan vorig jaar. Dit komt doordat er vorig jaar een aparte benchmarkmeting was die alleen voor mbo-instellingen via MBO Digitaal werd gehouden. Deze meting is dit jaar niet gehouden, wat het lagere aantal respondenten kan verklaren. Wel is er een positief verschil ten opzichte van 2021 en 2022: ondanks dat er bijna evenveel instellingen hebben deelgenomen, zijn er meer respondenten in 2024.

Aantal	2021	2022	2023	2024
Respondenten	4.916	4.524	12.343	6.391
Instellingen	26	26	70	27
• **MBO**	6	6	41	3
• **HBO**	9	8	9	11
• **WO**	4	9	10	8
• **Overig**	7	3	10	5

Tabel 2: Aantal deelnemers in 2022, 2023, 2024

Resultaten

Dit jaar presteren de instellingen over het algemeen beter dan vorig jaar, maar de toename is minder groot dan tussen 2022 en 2023. Op het component gelegenheid is de score gelijk gebleven.

Zijn de verschillen per vraag ook gelijk verdeeld? Om deze vraag te beantwoorden, hebben we één vraag en vier stellingen geëvalueerd die precies hetzelfde waren en waarvan het resultaat goed vergeleken kan worden. De toetsvragen (bekwaamheid) vielen af, want die zijn elk jaar verschillend. Ook de nieuwe meningvragen die dit jaar zijn toegevoegd kunnen niet vergeleken worden met voorgaande jaren.

Score	2021	2022	2023	2024
Totaalscore	6,8*	5.9	6.5	6.8
Motivatie	7,6*	5.9	6.5	6.7
Gelegenheid	6,3	6.1	6.7	6.7
Bekwaamheid	6,4	5.8	6.4	6.9

Tabel 3: Benchmarkscores 2022, 2023, 2024

* Na 2021 zijn de vragen over het component motivatie aangescherpt, waardoor deze en de totaalscore niet goed te vergelijken is met de andere jaren.

Vergelijking met voorgaande jaren (2)

Vergelijking vragen 2021, 2022, 2023 en 2024

De volgende vraag en stellingen worden vergeleken:

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

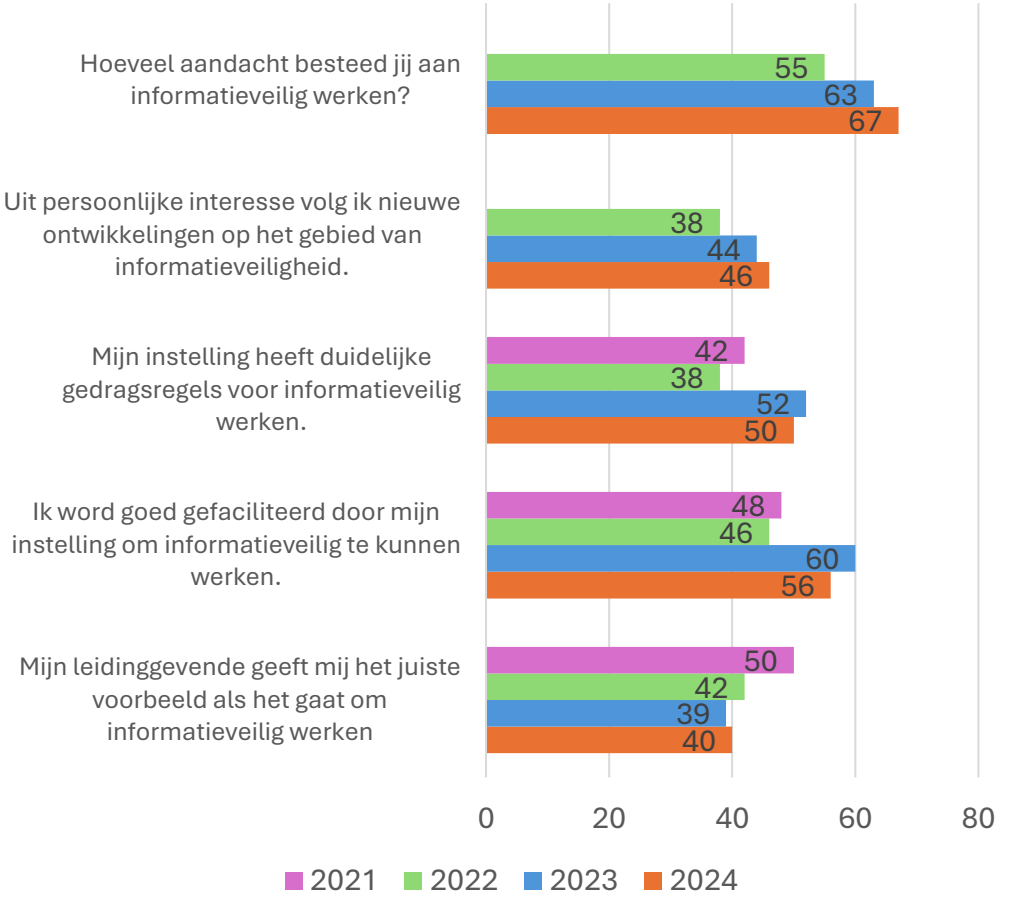
Per vraag berekenden we het opgetelde percentage respondenten dat de twee meest positieve antwoordopties heeft gegeven. Bij vraag 1 zijn dat: ‘veel aandacht’ of ‘zeer veel aandacht’ en bij de 4 stellingen zijn dat ‘eens’ of ‘zeer eens’.

Conclusie

De respondenten hebben dit jaar op twee van de vijf informatieveiligheids-vragen hoger gescoord dan voorgaande jaren. Over het hebben van duidelijke gedragsregels en het goed gefaciliteerd worden denken de respondenten (iets) minder positief dan in 2023, maar wel positiever dan in 2021 en 2022.

Conclusie (vervolg)

Ten opzichte van vorig jaar is men wel iets positiever over de voorbeeldrol van leidinggevenden, maar dit is alsnog een lagere score dan in 2022.



Conclusie

Conclusies

Dit rapport bevat een analyse van de 27 security- en privacy-awarenessmetingen die BDO in opdracht van SURF heeft uitgevoerd in het voorjaar van 2024. Op basis van de bevindingen in de voorgaande hoofdstukken, concluderen we het volgende.

De resultaten tonen een stijgende lijn, maar de meeste instellingen hebben nog niet het minimale streefdoel gehaald

Uit de meting blijkt dat de respondenten beter bekwaam en gemotiveerd zijn om veilig te werken ten opzichte van voorgaande jaren. De meeste instellingen voldoen echter nog niet aan het minimale streefdoel (zie ook pagina 23). De mate waarin respondenten zich goed gefaciliteerd voelen is iets afgenomen, net als de gepercipieerde duidelijkheid van richtlijnen en gedragsregels.

Aan de start van de awarenessmeting zijn drie onderzoeksvragen geformuleerd:

1) In hoeverre kunnen medewerkers informatieveilig en privacybewust werken (bekwaamheid)?
2) In hoeverre willen zij dat (motivatie)?
3) In hoeverre worden zij hiertoe in staat gesteld (gelegenheid)?

De volgende conclusies geven antwoord op deze vragen.

De kennis over informatieveiligheid is flink verbeterd. Men heeft nu meer behoefte aan duidelijkheid rondom het verwerken van gevoelige gegevens en welke tools gebruikt mogen worden

De quizvragen in de awarenessmeting zijn redelijk goed gemaakt. Gemiddeld heeft 69% van de respondenten een juist antwoord gegeven. Dit is een verbetering ten opzichte van 2022 en 2023, waarin respectievelijk gemiddeld 57,5% en 64% een juist antwoord heeft gegeven. Uit de open antwoorden is naar voren gekomen dat respondenten vooral behoefte hebben aan helderheid over welke tools zijn toegestaan in hun eigen werksituatie. Daarnaast zeggen de respondenten dat ze duidelijke richtlijnen nodig hebben rondom het verwerken van persoonsgegevens en vertrouwelijke gegevens die gerelateerd zijn aan hun functie. Algemene richtlijnen bieden niet genoeg handvatten.

Veel respondenten weten nog niet hoe security-incidenten en datalekken te melden

Het herkennen en melden van security-incidenten is een van de belangrijkste aspecten van informatieveilig werken. Alerte medewerkers kunnen ervoor zorgen dat incidenten in de kiem gesmoord worden. Een grote meerderheid van de respondenten zegt dat ze altijd een incident durven te melden. Maar slechts een krappe meerderheid zegt precies te weten hoe ze dat moeten doen.

Conclusies

Hoewel men nog steeds overtuigd is van het belang, is de motivatie om aandacht te besteden aan security en privacy beperkt

Net als voorgaande jaren is het merendeel van de respondenten overtuigd van het belang van informatieveiligheid en de rol van werknemers daarin, maar hebben zij beperkte (intrinsieke) motivatie om hier actief mee aan de slag te gaan. Veel respondenten richten zich vooral op informatieveiligheid om de eventuele negatieve consequenties te voorkomen. Ook is er een kleine groep die het belang van informatieveiligheid niet inziet en hier weinig aandacht aan besteedt. Deze groep vindt de aandacht voor dit onderwerp overdreven of is van mening dat de verantwoordelijkheid voor de informatieveiligheid bij de instelling ligt en niet bij de medewerkers.

Er is een afname van tevredenheid over faciliteiten en richtlijnen

Ten opzichte van vorig jaar zijn respondenten minder tevreden over de mate waarin ze gefaciliteerd worden om informatieveilig te werken. De algemene richtlijnen en gedragsregels rondom privacy en security worden vaak te generiek gevonden, terwijl medewerkers juist behoefte hebben aan richtlijnen die specifiek betrekking hebben op hun werksituatie. Om adequaat gefaciliteerd te worden zijn er door de respondenten specifieke onderwerpen benoemd die verbetering behoeven, zoals het gebruik van een wachtwoordmanager.

Men wil minder vrijblijvendheid rond security en privacy gedragsregels

Respondenten zijn kritisch over de faciliteiten en IT-tools om informatieveilig te kunnen werken, maar slechts een kleine minderheid ervaart de security en privacy gedragsregels van hun instelling als een remmende factor tijdens dagelijkse werkzaamheden. Veel respondenten vinden juist dat informatieveiligheid een te vrijblijvend karakter heeft in hun instelling en pleiten ervoor om de gedragsregels strikter te handhaven.

Sterke security-cultuur ontbreekt

Respondenten zijn positief over hun eigen inzet op het gebied van informatieveilig werken. Minder tevreden zijn ze over de voorbeeldrol van de leidinggevende en de betrokkenheid van collega’s op dit thema. Hieruit kunnen we concluderen dat, net als vorig jaar, bij de meeste instellingen een sterke security-cultuur ontbreekt. Informatieveiligheid lijkt geen thema te zijn dat regelmatig besproken wordt en waarover breed gedeelde ideeën, gedragingen en gewoontes bestaan.

Aanbevelingen

Aanbevelingen

Op basis van de bevindingen en conclusies komen we tot de volgende aanbevelingen.

Stem awareness-uitingen af op het dagelijkse werk

Om medewerkers te stimuleren om informatieveilig te werken, adviseren we om in trainingen praktische voorbeelden en scenario's te gebruiken die aansluiten op hun dagelijkse werkzaamheden. Een awarenessboodschap die specifiek relevant is voor de doelgroep en concrete en haalbare adviezen biedt, zal beter ontvangen worden dan een algemene en abstracte benadering.

Neem belemmeringen voor informatieveilig werken weg, waaronder voor incidenten melden

Onderzoek welke hindernissen medewerkers ondervinden bij informatieveilig en privacybewust werken en probeer hier een oplossing voor te vinden. Voorbeelden: faciliteer het gebruik van een wachtwoordmanager en leg duidelijk uit hoe deze werkt. Zorg ervoor dat medewerkers veilig bestanden kunnen delen. Stel heldere gedragsregels rond het melden van incidenten op en zorg ervoor dat medewerkers eenvoudig en laagdrempelig kunnen melden.

Focus op specifieke thema's

Besteed extra aandacht aan specifieke thema's, zoals:

- Veilige software/tools;
- Omgaan met persoonsgegevens;
- Datalekken en security incidenten: hoe te herkennen en hoe te handelen.

Investeer in een sterke security-cultuur

Een sterke security cultuur bestaat uit gemeenschappelijke opvattingen, gedragingen en gewoontes die gericht zijn op het beschermen van informatie. Het veilig omgaan met informatie zou de norm moeten zijn. Om een dergelijke cultuur te ontwikkelen is het essentieel dat leidinggevenden als eerste de juiste toon zetten en het onderwerp bespreekbaar maken. Daarnaast adviseren we om informatieveiligheid regelmatig op de agenda van werkoverleggen te zetten, zodat het een vanzelfsprekend onderdeel wordt van de dagelijkse werkzaamheden. Tot slot is het belangrijk dat awarenesstrainingen en sessies minder vrijblijvend zijn zodat medewerkers merken dat de instelling waarde hecht aan privacy en security en ze vertrouwd raken met de bijbehorende boodschap.

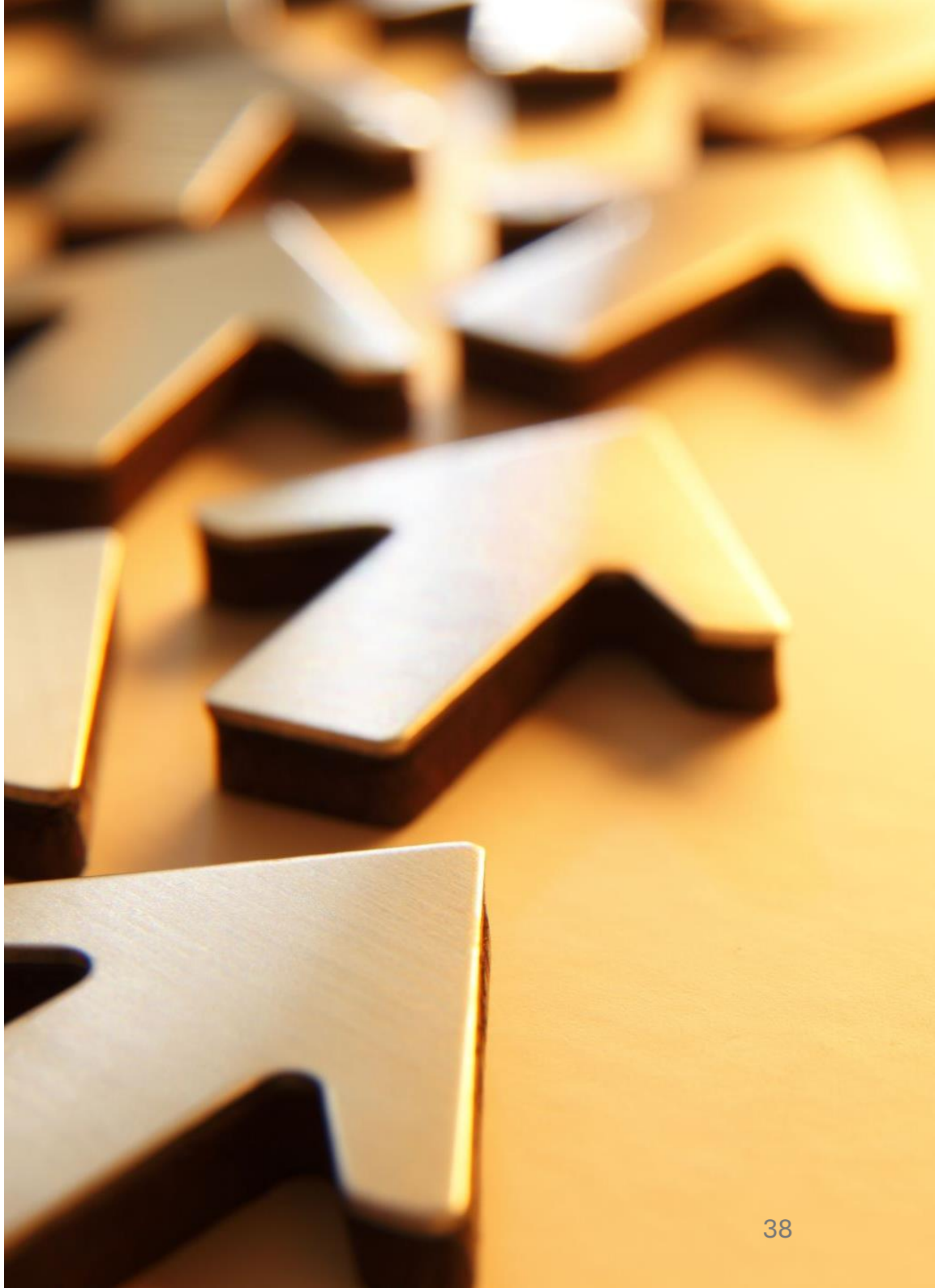
Aanbevelingen

Maak security en privacy vast onderdeel van onboarding

Zorg ervoor dat alle nieuwe medewerkers bij indiensttreding een training op het gebied van security en privacy volgen. Dit creëert helderheid over de verwachtingen en normen binnen de instelling. Aangezien nieuwe medewerkers nog niet bekend zijn met de geldende richtlijnen, en het onzeker is of ze eerder voldoende kennis over privacy en security hebben opgedaan, is dit een cruciale stap.

Houd rekening met sceptici

Hoewel medewerkers die aandacht voor privacy en security overdreven vinden een kleine minderheid vormen, kunnen zij toch een risico voor de instelling zijn. Ga met hen in gesprek en luister naar hun argumenten. Zijn zij van mening dat de risico's op het gebied van privacy en security worden overschat, of vinden ze dat sommige maatregelen te streng zijn om hun werk effectief te kunnen doen? Of speelt misschien een combinatie van beide factoren een rol?



Colofon

Sectorrapport security en privacy awareness 2024: Kennis over cybersecurity groeit, maar praktijk blijft achter.

Oktober 2024

Het rapport is opgesteld door:

- **BDO Cybersecurity**

  Donna Moens, MSc donna.moens@bdo.nl

  Inge Pronk, inge.pronk@bdo.nl

- **SURF**

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

Bijlagen

Bijlage A - Vragenlijst

‘Meningvragen’

1. Hoe belangrijk vind jij informatieveiligheid voor jouw 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 en een eventuele toelichting of opmerking geven.
4. Binnen mijn instelling hechten medewerkers veel belang aan informatieveiligheid.
5. Uit persoonlijke interesse volg ik nieuwe ontwikkelingen op het gebied van informatieveiligheid.
6. Ik weet hoe ik in mijn dagelijkse werk invulling moet geven aan informatieveilig werken.
7. Mijn instelling heeft duidelijke gedragsregels voor informatieveilig werken.
8. Ik word goed gefaciliteerd door mijn instelling om informatieveilig te kunnen werken (bijvoorbeeld door software, tools, instructies, en andere middelen).
9. Mijn leidinggevende geeft mij het juiste voorbeeld als het gaat om informatieveilig werken.
10. Ik durf een security- of privacy incident altijd te melden, ook als ik die zelf heb veroorzaakt.
11. Ik ervaar de security en privacy gedragsregels als een remmende factor tijdens mijn dagelijkse werkzaamheden.
12. Ik weet wanneer en hoe ik een security- of privacy incident moet melden.

Inventarisatie

1. Over welke onderwerpen heb jij meer kennis nodig om informatieveilig te kunnen werken? Je kunt meerdere opties kiezen.
2. Heb jij nog opmerkingen of verbeterpunten voor jouw instelling over informatieveilig werken?

Toetsvragen

1. Welke stelling(en) over het gebruik van AI, zoals ChatGPT, is/zijn waar?
    1. Via zoekvragen kun je onbedoeld gevoelige (persoons)-gegevens doorgeven aan de leverancier van de AI tool.
    2. De antwoorden van een AI zijn betrouwbaar omdat ze gebaseerd zijn op een grote hoeveelheid trainingsdata.
        A. 1 en 2 zijn beide waar
        B. 1 is waar, 2 is onwaar
        C. 1 en 2 zijn beide onwaar
2. Waaraan kun je zien dat onderstaande bericht phishing is?
    A. Het e-mailadres van de afzender klopt niet
    B. De link in de mail verwijst naar een onbekende website
    C. Beide antwoorden zijn juist
3. Welke van deze wachtwoorden is het sterkst?
    A. 8b*Q(&
    B. 051121Noah!
    C. Dek@ngoeroespeeltop1drumstel

Bijlage A - Vragenlijst

Toetsvragen (vervolg)

4. Bij welk van onderstaande situaties is er sprake van een datalek?
    1. Je stuurt het gepubliceerde jaarverslag van de instelling per ongeluk naar de verkeerde ontvanger.
    2. Je stuurt een e-mail naar studenten die interesse hebben geuit in de workshop ‘omgaan met prestatiedruk’ en zet alle ontvangers in de CC.
    3. Je laat uitgeprinte CV’s van sollicitanten per ongeluk liggen op de afdeling en kan ze nergens meer vinden.
        A. Situatie 1 en 2
        B. Situatie 2 en 3
        C. Situatie 1, 2 en 3

5. Je vergeet een stapel gemaakte toetsen in de trein. Wat doe je als eerste?
    A. Dit melden bij de Autoriteit Persoonsgegevens
    B. Een mailtje sturen naar de betreffende studenten om te zeggen dat de toets de volgende les opnieuw moet worden gemaakt
    C. Dit melden volgens de procedure van mijn instelling

6. Welk van onderstaande situaties zijn voorbeelden van social engineering?
    1. Iemand doet zich voor als een medewerker en vraagt aan de financiële afdeling om zijn/haar bankrekeningnummer aan te passen.
    2. Er wordt een phishing e-mail gestuurd naar alle medewerkers van de instelling vanuit een e-mail adres dat afkomstig lijkt van de IT-afdeling. Hierin wordt gevraagd om een wachtwoord via een link te resetten.
    3. Iemand kijkt mee over je schouder terwijl jij je wachtwoord intypt en/of met gevoelige informatie werkt.
        A. Situatie 1 en 2
        B. Alleen situatie 1
        C. Situatie 1, 2 en 3

7. Studenten vragen aan een docent om een WhatsApp-groep aan te maken om toets resultaten en verdiepende artikelen op de lesstof te delen. Waarom is dit onwenselijk?
    A. Omdat Whatsapp geen goedgekeurd communicatiemiddel is van de instelling
    B. Omdat Whatsapp een slechte reputatie heeft op het gebied van privacy
    C. Omdat de encryptie van Whatsapp van lage kwaliteit is

8. Bij de feestelijke opening van een nieuw onderwijsgebouw worden foto’s gemaakt voor de website van de instelling. Is het nodig om aan iedereen die op de foto’s staat expliciete toestemming te vragen?
    A. Ja, maar alleen als ze herkenbaar in beeld komen
    B. Ja, ook als ze niet herkenbaar in beeld komen
    C. Nee, onder bepaalde voorwaarde hoeft dit niet