4 SEPTEMBER 2023

MBO Raad

Sectorrapportage

mbo digitaal

SECURITY + PRIVACY AWARENESS METING MBO

BDO

Samenvatting

Samenvatting

Sectorrapportage security- en privacyawareness MBO

Onderzoek

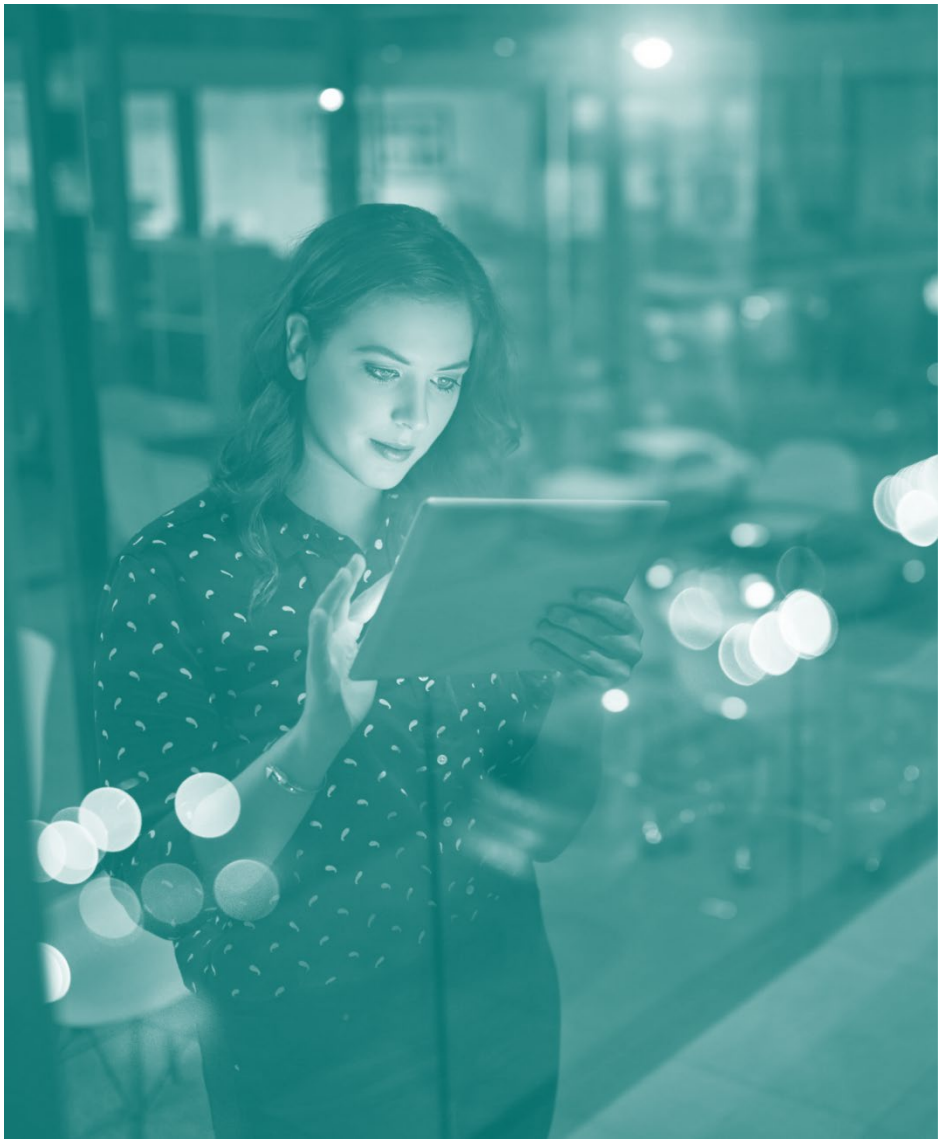
In opdracht van MBO Raad heeft BDO voor het eerst security- en privacy-awarenessmetingen uitgevoerd specifiek gericht op mbo-instellingen. De metingen bestonden uit online vragenlijsten voor de medewerkers. De vragenlijsten werden in het voorjaar van 2023 verspreid binnen de 41 deelnemende instellingen. In totaal hebben 5768 respondenten de vragenlijst volledig ingevuld. Na afloop ontvingen de instellingen met minimaal 25 respondenten een rapportage met bevindingen en aanbevelingen. Voor deze sectorrapportage, een overkoepelende analyse van de metingen, zijn tevens interviews gehouden met security- en privacyprofessionals werkzaam binnen mbo-instellingen.

De basis van de metingen is het COM-B gedragsmodel van Susan Michie. Volgens dit model is het om een gedragsverandering tot stand te brengen nodig dat mensen bekwaam en gemotiveerd zijn en gefaciliteerd worden.

Bevindingen

Het onderzoek laat zien dat medewerkers in het mbo zich bewust zijn van het belang van informatieveilig werken, maar dat ze beperkt gemotiveerd zijn, een gebrek aan duidelijke richtlijnen hebben en vaak de nodige kennis en training missen.

Respondenten geven aan vooral uit verplichting aandacht te besteden aan informatieveiligheid – ook noemt 24% schaamte bij een eventueel incident als reden om aandacht aan het onderwerp te besteden. Bestuur en leidinggevenden spelen ook een sleutelrol als rolmodellen voor hun medewerkers, maar op dit moment laten besturen en leidinggevenden relatief beperkt zien dat ze informatieveilig werken als een prioriteit zien die ieders aandacht verdient. Respondenten ervaren een disbalans tussen informatieveiligheid en gebruiksvriendelijkheid en voelen zich soms belemmerd in hun werk. Het gebrek aan bewustzijn en duidelijke richtlijnen bij medewerkers kan leiden tot onzekerheid en het nemen van risico’s.



Samenvatting

Sectorrapportage security- en privacyawareness MBO

Aanbevelingen

Creëer bewustwording die motiveert met concrete voorbeelden

- Wanneer mensen begrijpen waarom informatieveiligheid in hun werkzaamheden belangrijk is, motiveert het hen om veilig te werken omdat ze de waarde van het beschermen van gegevens voor zichzelf, hun collega's en studenten inzien.
- Maak daarom gebruik van concrete voorbeelden en scenario's die aansluiten bij de dagelijkse taken van medewerkers, dat helpt hen zien hoe hun bijdrage aan informatieveiligheid de instelling beschermt tegen cyberdreigingen en eventuele datalekken.

Ontwijk het olifantenpad

- Het is ook belangrijk om te voorkomen dat medewerkers alternatieve, minder veilige methoden gebruiken om hun werk te doen, door hen toegankelijke en effectieve beveiligingsoplossingen te bieden.

Wees duidelijk en vindbaar

- Duidelijke én vindbare gedragsregels stellen medewerkers in staat om gemakkelijk toegang te krijgen tot de juiste richtlijnen en procedures.
- Hierdoor kunnen zij de vereiste beveiligingsmaatregelen begrijpen en naleven, waardoor het risico op incidenten en datalekken wordt verminderd.

Meet gedrag

- Het meten van gedrag op het gebied van informatieveiligheid geeft inzicht in de effectiviteit van beveiligingsmaatregelen en bewustwordingsprogramma's.
- Denk hierbij aan beoordelingen, vragenlijsten, mystery guests, monitoring van beveiligingsactiviteiten en phishingsimulaties.

Geef uitleg

- Training en uitleg over lastige onderwerpen blijft van belang. Onderwerpen die extra aandacht verdienen zijn:
  - Datalekherkenning,
  - Risico's social media,
  - Sterke wachtwoorden
  - Opslaan en delen van vertrouwelijke (persoons)gegevens

Lead by example

- Schoolbesturen en leidinggevenden moeten het goede voorbeeld geven en zelf het belang van informatieveilig werken benadrukken. Als rolmodellen hebben zij een unieke kans om de bewustwording te vergroten en een positieve veiligheidscultuur te bevorderen.
- Hun goede voorbeeld moedigt medewerkers aan om beveiligingsbeleid na te leven en bij te dragen aan een veilige werkomgeving.

Inhoudsopgave

Inleiding

Inleiding

Sectorrapportage security- en privacyawareness MBO

Introductie

Het mbo is, zoals heel veel sectoren tegenwoordig, kwetsbaar voor datalekken, hackaanvallen en andere security incidenten. Vanwege zijn maatschappelijke functie is bij een verstoring in het onderwijs de ontwrichting heel zichtbaar. Dit maakt de sector een aantrekkelijk doelwit voor criminele hackers. Veel incidenten zijn gerelateerd aan menselijk handelen, zoals klikken op phishing e-mails of onbedoeld gevoelige informatie delen. De digitale weerbaarheid hangt dus sterk af van het gedrag van docenten, HR-adviseurs, secretaresses en andere medewerkers tijdens hun dagelijkse werkzaamheden.

Primeur voor het MBO

BDO heeft voor de eerste keer in opdracht van de MBO Raad security- en privacy-awarenessmetingen uitgevoerd bij 41 mbo-instellingen. Met deze metingen willen we op drie niveaus inzicht bieden: De respondent krijgt feedback; de instelling ontvangt een rapport met bevindingen en aanbevelingen; en deze sectorrapportage geeft een mbo-breed beeld.

Over de auteur

- BDO ondersteunt organisaties bij het versterken van hun digitale weerbaarheid. De aanpak bestaat uit het uitvoeren van assessments rond kwetsbaarheden en risico's, het implementeren van cybersecurity- en privacy-standaarden, het testen en monitoren van de IT-infrastructuur en het ondersteunen bij cyberincidenten. Daarnaast is BDO gespecialiseerd in het realiseren van gedragsveranderingen bij medewerkers.
  - Linda van Liempt is werkzaam binnen het team Cybersecurity met als expertise security & privacy awareness.

MBO Digitaal heeft ondersteund bij de totstandkoming van dit rapport.

Aanpak metingen

Aanpak metingen

Sectorrapportage security- en privacyawareness MBO

In het voorjaar van 2023 hebben we security- en privacy-awarenessmetingen uitgevoerd bij 41 mbo-instellingen. De uitgevoerde security- en privacy-awarenessmeting is onderdeel van het programma Cyberveiligheid mbo. De meting wordt gebruikt als nulmeting om te kunnen bepalen welke activiteiten er vanuit het programma kunnen worden opgestart om de instellingen te ondersteunen bij het verhogen van de awareness op dit gebied. De MBO Raad en MBO Digitaal hebben de instellingen opgeroepen deel te nemen aan deze meting met als resultaat dat zich 51 instellingen hebben aangemeld. Daarvan hebben er 41 daadwerkelijk deelgenomen aan de meting.

Respondenten kregen tijdens het invullen van de vragenlijst direct feedback op hun antwoorden op de quizvragen, en ontvingen hun score voor de quiz aan het einde.

Op 30 juni hebben de instellingen met meer dan 25 respondenten hun eigen awarenessrapport ontvangen, vergezeld van een vergelijking met benchmarkscore voor het hele mbo.

De resultaten die uit meting naar voren zijn gekomen, zijn de basis voor deze sectorrapportage voor het middelbaar beroepsonderwijs. Daarnaast dienen de resultaten als input voor de sectorrapportage voor het onderwijs en onderzoek, opgesteld door BDO in samenwerking met SURF.

In dit hoofdstuk beschrijven we de aanpak van de metingen. We behandelen het gedragsmodel dat als basis van de metingen fungeerde, de centrale onderzoeksvragen en de werkwijze.

Aanpak metingen

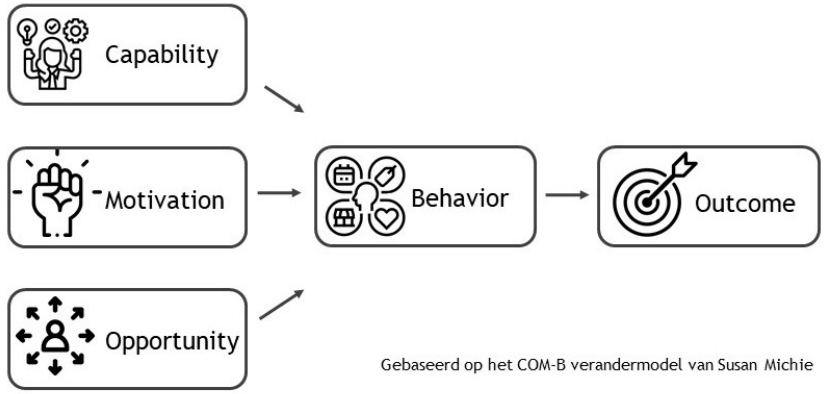
Sectorrapportage security- en privacyawareness MBO

Gedragsmodel

Om informatieveilig en privacybewust gedrag in kaart te brengen maakten we gebruik van het COM-B gedragsmodel van Susan Michie. Dit model stelt dat bekwaamheid (capability), gelegenheid (opportunity) en motivatie (motivation) aanwezig moeten zijn om gedrag (behavior) te laten plaatsvinden.

Vaak zijn deze componenten met elkaar verweven. Als mensen de juiste competenties hebben en goed gefaciliteerd worden, is de kans groot dat zij ook meer gemotiveerd raken om zorgvuldig met vertrouwelijke gegevens om te gaan. Door deze componenten alle drie te adresseren, en oog te hebben voor hun onderlinge afhankelijkheid, verhoog je de kans op een succesvolle gedragsinterventie.

- Bekwaamheid heeft betrekking op de juiste kennis en vaardigheden om de verandering te kunnen uitvoeren. Dit gaat bijvoorbeeld over het herkennen van risicovolle situaties, weten wat te doen bij een datalek, een sterk wachtwoord kunnen opstellen en in staat zijn op phishing e-mails te herkennen.
- Bij motivatie draait het om de (intrinsieke) motivatie van de medewerkers om informatieveilig en privacybewust te werken. Willen zij zich daar uit eigen overtuiging voor inzetten, of doen ze dat vooral omdat ze bang zijn voor negatieve consequenties?
- Gelegenheid gaat over het faciliteren van medewerkers om veilig te werken. Medewerkers hebben de juiste middelen, zoals software/tooling, heldere richtlijnen en ondersteuning van de leidinggevende nodig. Veilig werken dient zo makkelijk mogelijk te worden gemaakt, zonder veel extra handelingen en andere barrières.



Gebaseerd op het COM-B verandermodel van Susan Michie

Vraagstelling

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

- In hoeverre kunnen medewerkers informatieveilig en privacybewust werken?
- In hoeverre willen medewerkers informatieveilig en privacybewust werken?
- In hoeverre worden medewerkers in staat gesteld om informatieveilig en privacybewust te werken?

We hebben ervoor gekozen om zowel security als privacy te adresseren in de metingen. Dit omdat er een grote overlap tussen beide thema's is met betrekking tot het wenselijke gedrag van medewerkers.

Aanpak metingen

Sectorrapportage security- en privacyawareness MBO

Begrippen

- Met privacybewust werken bedoelen we dat medewerkers tijdens hun werk zorgvuldig omgaan met gegevens van studenten, respondenten, medewerkers of andere betrokkenen.
  - Bijvoorbeeld: voor het uitvoeren van onderwijs verzamelen medewerkers alleen persoonsgegevens als ze hier een grondslag en specifiek doel voor hebben. Ook verwerken ze niet méér gegevens dan strikt noodzakelijk. Ze delen uitsluitend persoonsgegevens met partijen die deze mogen ontvangen, doen dat via veilige kanalen en zorgen ervoor dat de gegevens niet bij de verkeerde ontvanger terecht komen. Mocht er toch een fout zijn gemaakt, dan weten ze waar ze dat kunnen melden en doen dat ook direct.
- Informatieveilig werken betekent dat medewerkers tijdens hun werk (vertrouwelijke) informatie beschermen tegen toegang of ontregeling door onbevoegden. Het houdt in dat medewerkers alert zijn op informatiebeveiligingsrisico's en volgens een minimale beveiligingsstandaard werken.
  - Voorbeelden zijn: sterke wachtwoorden creëren en voor elk account een ander wachtwoord instellen, alert zijn op phishing bij het openen van mails en sms'jes, veilige kanalen gebruiken om informatie op te slaan en te delen met anderen, via een veilige (wifi-)verbinding het internet op gaan, extra alert zijn met zeer vertrouwelijke gegevens en beveiligingsincidenten en datalekken herkennen en direct melden.

Doelgroepen

Binnen de metingen hebben we gekeken naar de verschillende functiegroepen, waarbij we de volgende onderverdeling hebben gemaakt:

- Onderwijs
- Ondersteunend
- Leidinggevend
- Uitvoerend

Aanpak metingen

Sectorrapportage security- en privacyawareness MBO

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 van een grote groep mensen. De interviews zorgen voor extra duiding en diepgang.

De online vragenlijst, die is opgesteld in afstemming met een door MBO Digitaal samengestelde commissie van awarenessprofessionals binnen het mbo, bevat meningvragen en quizvragen. De meningvragen zijn om te achterhalen hoe gemotiveerd de medewerkers zijn om veilig te werken, en hoe goed ze daartoe worden gefaciliteerd. De quizvragen toetsen privacy- en securitykennis van de respondenten. De respondenten krijgen 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 mei en juni uitgezet bij 51 instellingen, waarvan er 41 daadwerkelijk hebben deelgenomen.. In totaal zijn er 5768 vragenlijsten ingevuld. Er zijn 9 interviews gehouden met medewerkers van verschillende instellingen die allen betrokken zijn het stimuleren van informatieveilig werken binnen hun instelling. De interviews vonden plaats in juli.

Maatstaf

In onze optiek dienen instellingen een minimale awareness-totaalscore van 7 of hoger te ambiëren. Je zou kunnen zeggen dat de medewerkers dan gemiddeld redelijk weerbaar zijn tegen mensgerichte cyberaanvallen en security incidenten. Aangezien cyberaanvallers maar een enkele mogelijkheid nodig hebben – één medewerker die klikt op een phishing e-mail – om flinke schade aan te richten, raden wij aan om een awareness score van 7,5 na te streven (wenselijke score). Hierbij moet wel opgemerkt worden dat de scores slechts een globale indicatie geven. Ze zijn een vertaling van een aantal meetpunten en geven geen context of duiding over het gehele thema security & privacy awareness. Het is verstandig om de scores in samenhang met de (overige) bevindingen en conclusies te bekijken.

Alternatieve aanpak SURF

De resultaten die de basis vormen voor dit rapport, dienen ook als input voor de sectorrapportage voor het onderwijs en onderzoek, opgesteld door BDO in samenwerking met SURF. De awarenessmeting van SURF bevatte dit jaar een extra component, namelijk een gedragsmeting. De gedragsmeting had als doel om daadwerkelijk (in plaats van alleen zelfgerapporteerd) gedrag te onderzoeken, en om te analyseren wat de relatie was tussen basismeting (COM-B) en gedragsmeting. Inhoudelijk bestond de gedragsmeting uit een test voor het maken van een sterk wachtwoord en een test voor het niet onnodig delen van persoonsgegevens.

Er is één mbo-instelling die heeft meegedaan aan de awarenessmeting van SURF in plaats van die van de MBO Raad. De quizvragen van deze meting waren net anders geformuleerd, en de resultaten van deze instelling zijn om die reden niet meegenomen in dit rapport, maar zullen meegenomen worden in het rapport voor het onderwijs en onderzoek van SURF.

Leeswijzer

Deze rapportage bevat vier onderdelen. Het eerste onderdeel bestaat uit bevindingen. Dit zijn de resultaten per component, per doelgroep en in cijfers, en verbeterpunten die respondenten aandragen. Het tweede onderdeel betreft de ervaringen en bevindingen van de security- en privacyprofessionals die voor dit onderzoek geïnterviewd zijn. Het derde onderdeel bestaat uit conclusies en het vierde onderdeel, tot slot, bevat aanbevelingen.

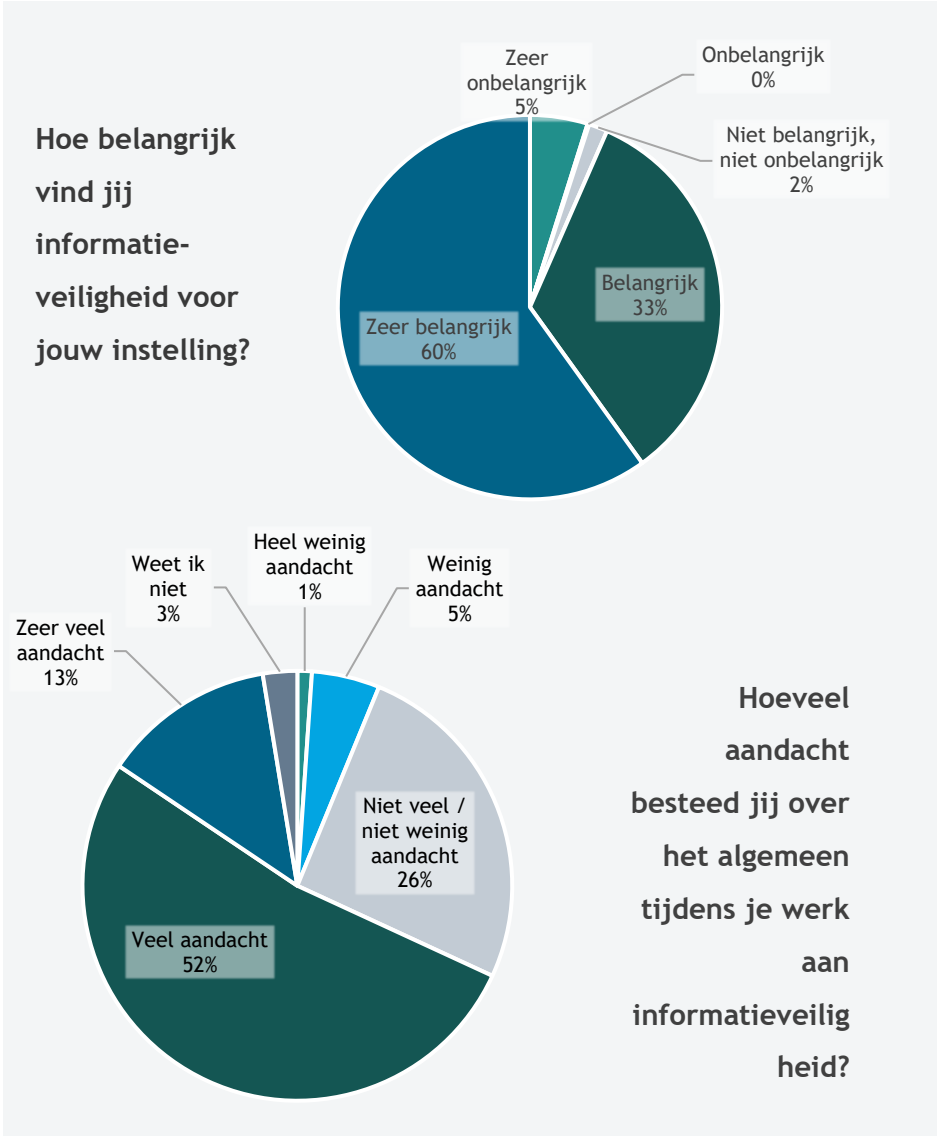
Citaten van respondenten worden als volgt gepresenteerd:

“Heel goed dat jullie dit uitvragen. Ik ga meer en meer twijfelen of mijn manier van veilig werken wel zo goed is... Ik vermoed dat er nog veel te leren valt.”

Resultaten

Resultaten - Motivatie

Sectorrapportage security- en privacyawareness MBO



Dit hoofdstuk bespreekt de resultaten die uit de online vragenlijsten naar voren zijn gekomen. We beginnen met motivatie, vervolgen met gelegenheid en daarna bekwaamheid. Tot slot worden in dit hoofdstuk de resultaten per doelgroep besproken.

Uit de ingevulde vragenlijsten blijkt dat bijna alle respondenten het belang van informatieveilig werken voor hun onderwijsinstelling ten zeerste inzien. Deze bevindingen werpen een positief licht op de bewustwording en betrokkenheid van medewerkers met betrekking tot de bescherming van vertrouwelijke gegevens en digitale informatie.

De erkenning van het belang van informatieveiligheid toont aan dat medewerkers in het onderwijs zich bewust zijn van de gevaren en risico's die digitaal werken met zich meebrengt. Het feit dat vrijwel alle medewerkers het belang van informatieveilig werken onderstrepen vormt een stevige basis om verder te bouwen aan robuuste informatieveiligheidsmaatregelen, waarbij een gezamenlijke inspanning wordt geleverd om de gegevens van studenten, medewerkers en de instelling als geheel te beschermen tegen digitale dreigingen.

Meer dan de helft van de respondenten geeft aan (zeer) veel aandacht aan informatieveiligheid te besteden. Ook deze bevindingen zijn bemoedigend en suggereren dat een aanzienlijk deel van het onderwijspersoneel zich bewust is van de cruciale rol die informatieveiligheid speelt in het beschermen van gevoelige gegevens en vertrouwelijke informatie. Dit duidt op een redelijk bewustzijn binnen de onderwijsinstellingen over de toenemende cyberdreigingen en de impact van datalekken.

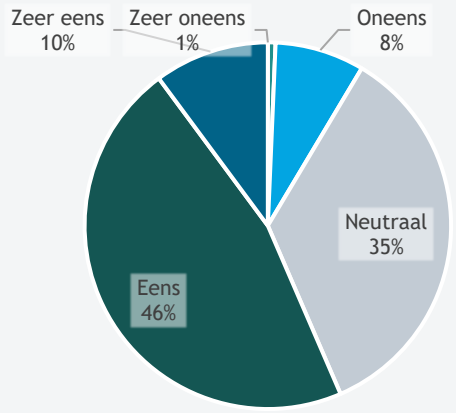
Resultaten - Motivatie

Sectorrapportage security- en privacyawareness MBO

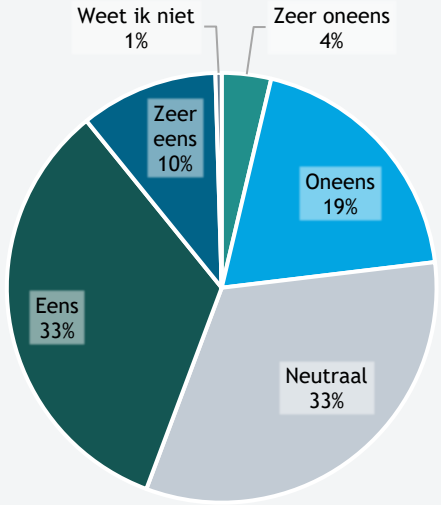
Medewerkers zijn ook bevraagd over het gedrag van hun collega's. In vergelijking met de beantwoording op de vraag hoeveel belang men zelf aan informatieveiligheid hecht, doen we een opmerkelijke bevinding: het merendeel van de respondenten is van mening dat zij zelf aanzienlijk meer aandacht besteden aan informatieveiligheid dan hun collega's. Deze waarneming werpt een interessant licht op het bewustzijn en de betrokkenheid van het onderwijspersoneel met betrekking tot de bescherming van vertrouwelijke gegevens en digitale informatie. De vraag rijst dan ook of men de veiligheid van het gedrag van collega's onderschat, of wellicht het eigen gedrag overschat.

Het gevoel dat respondenten zelf meer betrokken zijn bij informatieveiligheid dan hun collega's suggereert dat er binnen het onderwijs een aanzienlijke variatie bestaat in de mate waarin medewerkers zich bewust zijn van de dreigingen op het gebied van cybersecurity. Het creëren van een gedeelde visie op informatieveiligheid zal bijdragen aan een sterker en uniformer informatieveiligheidsbeleid dat de gehele instelling beschermt.

De deelnemers aan het onderzoek lijken vooral veilig te werken omdat het moet, niet omdat men interesse heeft in het thema cybersecurity. Met de stelling: 'uit persoonlijke interesse volg ik nieuwe ontwikkelingen op het gebied van privacy en informatiebeveiliging' is slechts 43% van de respondenten het eens of helemaal eens. Een minderheid gaat dus uit zichzelf actief aan de slag met dit thema.



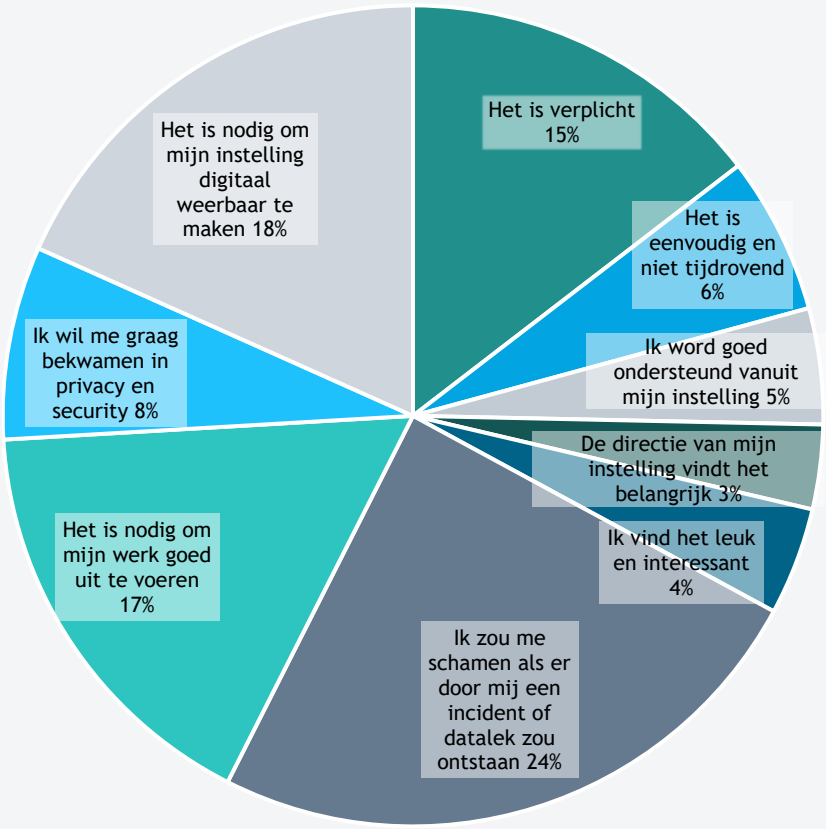
Stelling: binnen mijn instelling hechten medewerkers veel belang aan informatieveilig heid.



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

Resultaten - Motivatie

Sectorrapportage security- en privacyawareness MBO



Informatieveiligheid vereist een positieve en proactieve benadering om medewerkers te betrekken en bewust te maken van de risico's en de waarde van veilig gedrag. Toch blijkt dat wel 24% schaamte bij een eventueel incident als reden noemt om aandacht te besteden aan informatieveiligheid. Schaamte kan leiden tot een gevoel van vernedering en demotivatie, waardoor medewerkers terughoudend kunnen zijn om hun fouten te melden of vragen te stellen, wat de kans op veiligheidsincidenten vergroot.

Het feit dat medewerkers aandacht besteden aan informatieveiligheid uit verplichting, is ook minder positief. Verplichting kan leiden tot weerstand en afkeer bij medewerkers. Als veilig werken wordt opgelegd zonder uitleg over het belang ervan, kan het als een last worden ervaren en een negatieve invloed hebben op de werkcultuur.

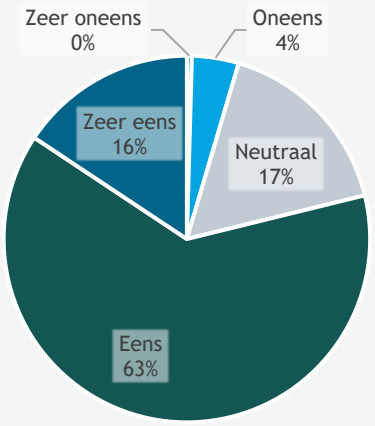
In plaats daarvan is het wenselijk om een cultuur van positieve bekrachtiging en intrinsieke motivatie te bevorderen. Medewerkers moeten worden aangemoedigd om veilig gedrag te vertonen door hen te laten zien hoe het bijdraagt aan de bescherming van gegevens, privacy en de reputatie van de instelling. Het verstrekken van trainingen die aansluiten bij het werk van de medewerker, het belonen van veilig gedrag en het bieden van ondersteuning bij eventuele twijfels zijn effectievere manieren om medewerkers te motiveren om informatieveilig te werken.

“Ik denk dat de gemiddelde collega de dwingende noodzaak niet voelt. Als je het uitlegt snapt men het heus, maar in de waan van de dag is het uitdraaien van een cijferlijst bijvoorbeeld wel heel handig. Nu weet ik dat we vorig jaar verplicht een AVG training moesten volgen, maar die heb ík 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.”

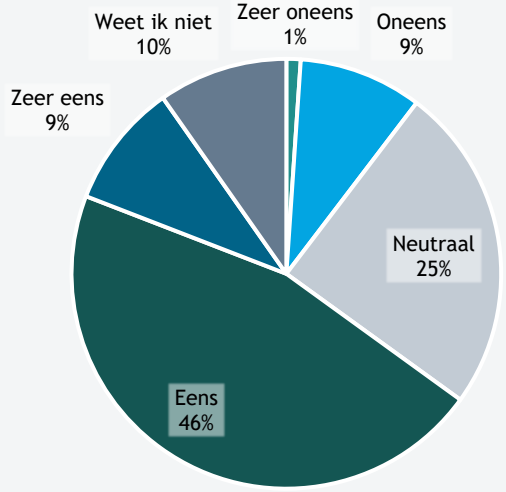
Resultaten - Gelegenheid

Sectorrapportage security- en privacyawareness MBO

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



Mijn instelling heeft duidelijke gedragsregels voor informatieveilig werken



Meer dan driekwart van de respondenten geeft aan te weten hoe ze invulling moeten geven aan informatieveilig werken. Het feit dat een aanzienlijk deel van het personeel aangeeft te weten hoe ze informatieveiligheid moeten waarborgen, suggereert dat er mogelijk al inspanningen zijn geleverd om medewerkers te informeren en te trainen over de het gewenste gedrag op dit gebied.

Hier staat tegenover dat een minder groot deel van de respondenten vindt dat er vanuit de instelling duidelijke gedragsregels zijn. Er is een groep medewerkers die zelf zegt te weten hoe er invulling aan te geven, maar vindt dat er vanuit hun instelling niet voldoende duidelijke ondersteuning is. Ook in de open antwoorden word vaak gezegd dat kennis meegenomen is vanuit vorige werkgevers, en er binnen de onderwijsinstelling waar ze nu voor werken weinig aandacht besteed wordt aan dit onderwerp.

Een onderwijsinstelling moet duidelijk zijn over wat er van medewerkers verwacht wordt met betrekking tot informatiebeveiliging. Heldere communicatie bevordert een uniforme en consistente aanpak van informatieveiligheid binnen de instelling, waardoor het risico op misverstanden en onopzettelijke incidenten wordt verminderd. Daarnaast vergroot duidelijkheid het bewustzijn van medewerkers over de potentiële risico's en hun individuele verantwoordelijkheid om vertrouwelijke gegevens te beschermen. Het helpt ook bij het bevorderen van een positieve veiligheidscultuur, waarin medewerkers zich gesteund voelen om vragen te stellen en eventuele zorgen te delen. Bovendien draagt een heldere richtlijn bij aan het versterken van de algehele informatieveiligheid van de instelling, waarbij iedereen een actieve rol speelt in het beschermen van waardevolle gegevens tegen cyberdreigingen.

“Het zou handig zijn dat er algemeen geldende afspraken komen. Ook ten aanzien van appen met leerlingen, jouw privénummer aan ouders geven etc. “

Resultaten - Gelegenheid

Sectorrapportage security- en privacyawareness MBO

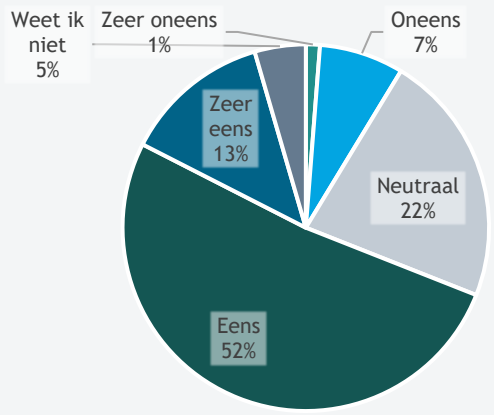
Een meerderheid (65%) voelt zich (zeer) goed gefaciliteerd door zijn of haar onderwijsinstelling om informatieveilig te werken. Deze positieve respons suggereert dat een aanzienlijk deel van het personeel de nodige middelen en ondersteuning krijgt om veilig met informatie om te gaan. Dat er nog 35% over is die het niet (zeer) eens is met die stelling, onderstreept het belang van voortdurende inspanningen van onderwijsinstellingen om te blijven investeren in het aanbieden van dan wel kenbaar maken van bestaande faciliteiten. Om deze groep te bereiken blijft het van belang om in contact met hen te treden, en awarenessinspanningen zoveel mogelijk aan te laten sluiten op de dagelijkse werkzaamheden van medewerkers.

Meer dan de helft van de respondenten is neutraal of weet niet of hun leidinggevende het goede voorbeeld geeft op het gebied van informatieveilig werken. Dat zou kunnen betekenen dat informatieveilig werken geen onderwerp van gesprek is.

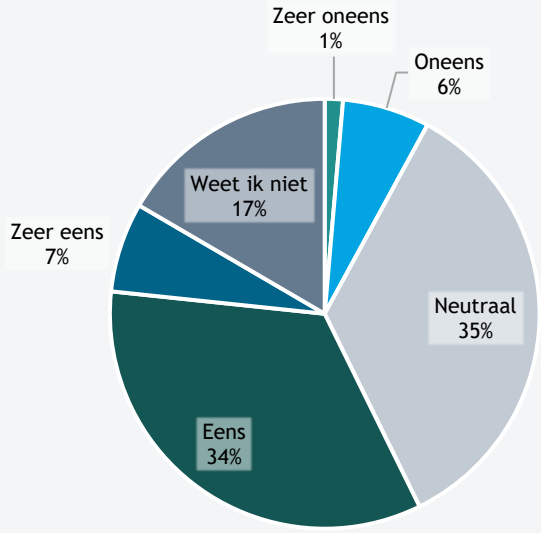
"Teamleiders doen (op mijn locatie) lang niet altijd hun werkruimte op slot als ze weglopen, dat vind ik een risico voor examinering."

Leidinggevenden spelen een essentiële rol in het juiste voorbeeld geven bij informatieveilig werken. Als leidinggevenden actief en consequent informatieveilig gedrag vertonen, moedigen ze hun team aan om dit gedrag na te volgen en het als een integraal onderdeel van hun dagelijkse werkzaamheden te zien. Bovendien hebben leidinggevenden vaak toegang tot gevoelige informatie (zoals gegevens in HR-systemen) en kunnen hun veiligheidspraktijken een directe impact hebben op de bescherming van vertrouwelijke gegevens van de medewerkers en studenten.

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 - Bekwaamheid

Sectorrapportage security- en privacyawareness MBO

De vragenlijst van de awarenessmeting bevat acht toetsvragen. Vijf van de acht vragen werden door de meeste mensen goed beantwoord. Op drie van de acht vragen werd door het merendeel van de respondenten een foutief antwoord gegeven. Deze onderwerpen lichten we in het bijzonder uit:

- Datalekherkenning
- Risico's social media
- Sterke wachtwoorden

Datalekherkenning

Wat is een datalek? Meerdere antwoorden mogelijk

a) Een email 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

Deze vraag is door 87% van de respondenten onjuist beantwoord. Alle drie de voorbeelden zijn datalekken.

De meeste medewerkers zijn zich er niet van bewust dat het onbedoeld wissen van persoonsgegevens ook een datalek is. Het is een lastige vraag, maar het is wel belangrijk dat medewerkers weten welke situaties datalekken zijn. Het vroegtijdig identificeren van datalekken stelt hen in staat om snel te handelen. Hierdoor kunnen tijdig de juiste maatregelen worden getroffen om de impact van het incident te minimaliseren, waardoor de instelling en de personen wiens gegevens het betreft beter beschermd worden tegen verdere schade. Door medewerkers bewust te maken van de tekenen van een datalek en hen te voorzien van de juiste training, kunnen instellingen de reactietijd verbeteren en de gevolgen van datalekken tot een minimum beperken.

Resultaten - Bekwaamheid

Sectorrapportage security- en privacyawareness MBO

Risico's social media

Waarom is LinkedIn een security risico? Meerdere antwoorden mogelijk

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

Medewerkers herkennen de risico's van social media zoals LinkedIn onvoldoende. Hoewel LinkedIn multifactorauthenticatie aanbiedt, worden accounts niet geverifieerd. Het is dus mogelijk dat connecties die er betrouwbaar uitzien, in werkelijkheid oplichters zijn. Daarnaast wordt bij het opstellen van een gerichte phishingaanval vaak gebruik gemaakt van door medewerkers geplaatste informatie over een instelling. Terughoudendheid is daarom van belang. Zorg dat dat medewerkers zich bewust zijn van deze risico's en verantwoordelijk omgaan met sociale media-activiteiten.

Sterk wachtwoord herkennen

Welke van deze wachtwoorden is het sterkst?

A) EenBroodjeKroketEnEenKaassouffle
B) Welkom2023
C) (6Yh$r#

Deze vraag bleek voor meer dan driekwart van de respondenten te moeilijk. Ze veronderstelden waarschijnlijk dat het belangrijkste kenmerk van een sterk wachtwoord de mate van complexiteit is. Dus: hoe meer verschillende leestekens, hoe beter. En dit terwijl het vooral om de lengte gaat. Het juiste antwoord was dus *A) EenBroodjeKroketEnEenKaassouffle*

Volgens de wachtwoordkraaktest op de website van VeiligInternetten.nl is *(6Yh$r#* binnen 2 seconden gekraakt, en *EenBroodjeKroketEnEenKaassouffle* pas na '221 quadriljoen jaar'. Aangezien wachtwoorden, ondanks securitybezwaren, nog steeds een noodzakelijk authenticatiemiddel zijn voor de meeste digitale diensten, is kennis over het creëren van sterke wachtwoorden onontbeerlijk voor cyberbewuste medewerkers.

Phishing

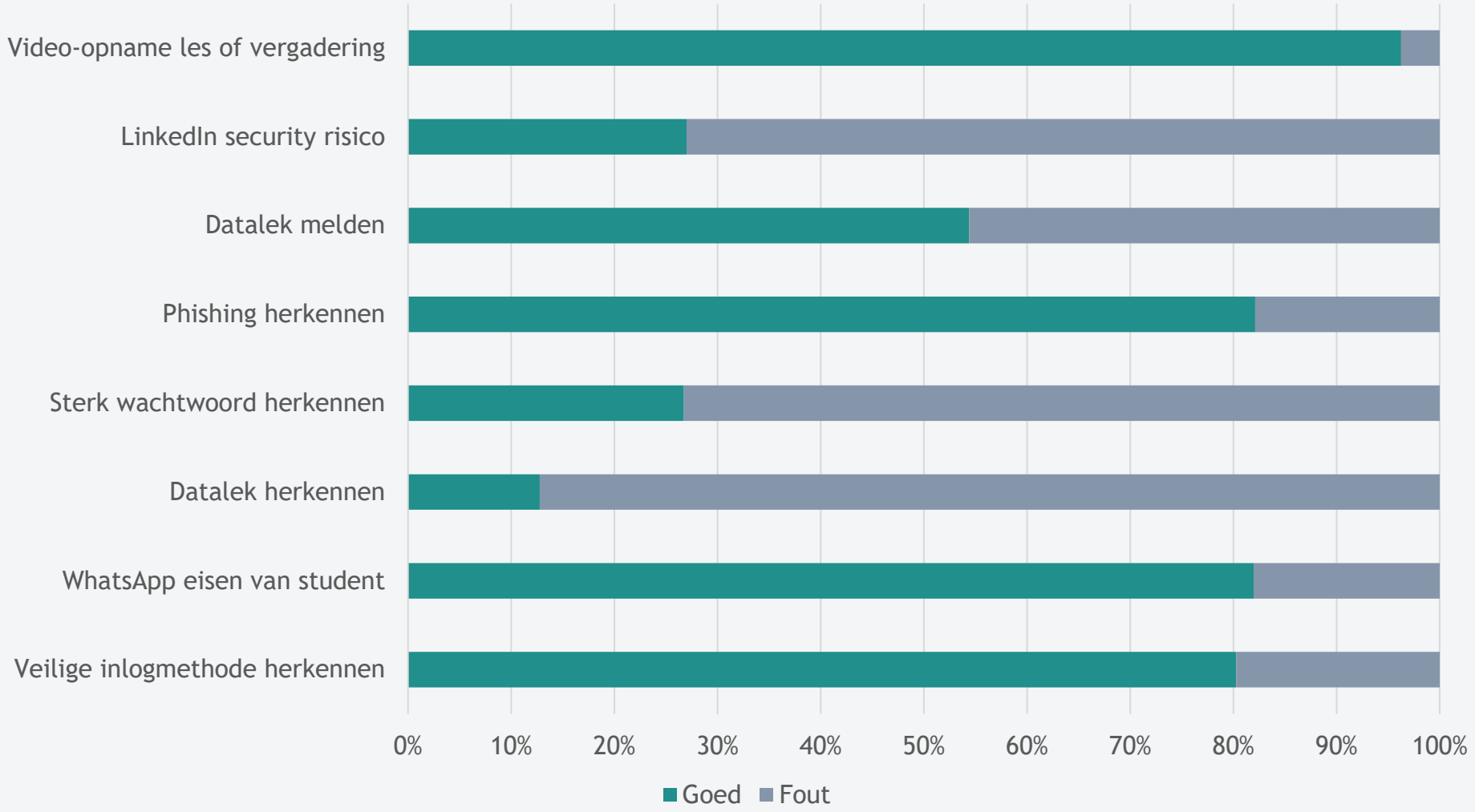
De toets bevatten een aparte vraag over phishing waarbij we een mail toonden, met de vraag of dit phishing was. Deze vraag is door ongeveer een op de vijf respondenten fout beantwoord. Dit vinden we een matige score, omdat phishing zo'n groot risico is voor instellingen: phishing is de meest gebruikte eerste stap voor een cyberaanval - en medewerkers kunnen dit risico verminderen door malafide berichten te herkennen. Daarnaast is het relatief eenvoudig om medewerkers te trainen door middel van phishingsimulaties.

Relatief goed beantwoorde onderwerpen

- Opnamen videovergadering
- WhatsApp
- Veilige inlogmethode herkennen

Resultaten - Bekwaamheid - Toetsvragen

Sectorrapportage security- en privacyawareness MBO



Resultaten - Bekwaamheid

Sectorrapportage security- en privacyawareness MBO

Tot slot hebben we gevraagd op welke thema's zich nog niet (geheel) bekwaam achten. Hierbij mochten zij meerdere antwoorden aankruisen. Het aantal respondenten dat een antwoord aankruiste staat in witte cijfers in de balken.

Het valt op dat medewerkers vooral hulp kunnen gebruiken bij de 'hoe' in het werk: "Hoe mag ik delen, hoe mag ik opslaan, hoe ga ik om met."

Medewerkers zijn gebaat bij duidelijke richtlijnen voor informatieveilig gedrag, omdat dit hen de nodige houvast en kaders biedt om vertrouwelijke gegevens effectief te beschermen. Heldere richtlijnen verminderen onzekerheid én vergroten het bewustzijn over de risico's. Medewerkers kunnen zo beter begrijpen welke praktijken essentieel zijn om datalekken en beveiligingsinbreuken te voorkomen. Een eenduidig beleid zorgt ervoor dat medewerkers op dezelfde wijze met gevoelige informatie omgaan, ongeacht hun functie of afdeling. Dit bevordert een cultuur van veiligheidsbewustzijn en teamwork, waarbij alle medewerkers samenwerken om de digitale weerbaarheid van de instelling te versterken.

"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"

Daarnaast is ook het aanbieden van een duidelijke set tools erg belangrijk voor medewerkers. Als medewerkers weten welke tools er beschikbaar zijn om hun werk mee te kunnen doen, wordt informatiebeveiliging minder als een belemmering gezien. Dit leidt direct tot een grotere naleving van beleid en vermindert het risico op datalekken en andere incidenten.

"Ik mis een VPN om buiten mijn instelling te kunnen werken"

"Kom met werkbare oplossingen en duidelijke uitleg en onderbouwing waarom bepaalde dingen soms ineens niet meer mogen."

Resultaten per doelgroep

Sectorrapportage security- en privacyawareness MBO

Voorafgaand aan de vragenlijst, hebben we respondenten gevraagd om aan te geven of hun werk leidinggevend of uitvoerend is, en of zij zich primair bezig houden met het onderwijs zelf, of daaraan ondersteunend zijn.

Aantal respondenten	Ondersteuning	Onderwijs	Totaal
Leidinggevend	344	228	572
Uitvoerend	2662	2534	5196
Totaal	3006	2762	5768

Motivatiescore	Ondersteuning	Onderwijs	Totaal
Leidinggevend	6.7	6.3	6.6
Uitvoerend	6.4	6.2	6.3
Totaal	6.5	6.2	6.3

Gelegenheidsscore	Ondersteuning	Onderwijs	Totaal
Leidinggevend	7.3	7.1	7.2
Uitvoerend	6.9	6.7	6.8
Totaal	7.0	6.7	6.8

Bekwaamheidsscore	Ondersteuning	Onderwijs	Totaal
Leidinggevend	5.9	5.8	5.9
Uitvoerend	5.8	5.7	5.8
Totaal	5.8	5.7	5.8

Totaalscore	Ondersteuning	Onderwijs	Totaal
Leidinggevend	6.6	6.4	6.6
Uitvoerend	6.4	6.2	6.3
Totaal	6.4	6.2	6.3

Resultaten per doelgroep

Sectorrapportage security- en privacyawareness MBO

Uit de metingen blijkt dat de respondenten in de doelgroep *ondersteuning* op alle componenten hoger scoren (6,4) dan de doelgroep *onderwijs* (6,2). Ze zijn gemotiveerder om informatieveilig en privacybewust te werken, ze scoren beter op de quizvragen en ze worden naar eigen zeggen beter in staat gesteld om veilig te werken.

Mogelijke oorzaken van lagere scores onder op het gebied van informatieveilig werken zijn werkdruk, perspectief en aard van de werkzaamheden. Docenten ervaren doorgaans een hoge werkdruk, terwijl ondersteunend personeel gemiddeld minder druk voelt.[1] Ook het perspectief van medewerkers zou een rol kunnen spelen, waarbij *ondersteuning* security en privacy als kerntaken ziet, terwijl docenten deze taken mogelijk als secundair beschouwen. Daarnaast spelen de aard van de werkzaamheden en de beschikbare IT-tools een rol in de mate waarin medewerkers informatieveilig en privacybewust werken. Medewerkers met afgebakende taken en passende IT-ondersteuning kunnen veiliger werken, terwijl anderen, zoals docenten die via vernieuwende manieren proberen hun onderwijsaanbod aantrekkelijk te houden, mogelijk olifantenpaadjes gebruiken vanwege beperkingen in de aangeboden tooling.

Opvallend is ook het verschil tussen de doelgroep *leidinggevend* en *uitvoerend*. Waar leidinggevenden zich beter in de gelegenheid gesteld voelen om informatieveilig te werken, en ook een significant hogere motivatiescore noteren, blijkt dat er in bekwaamheid amper verschil zit tussen deze groepen.

[1] Medewerkersonderzoek MBO Raad 2023, pagina 22: https://www.mboraad.nl/sites/default/files/publications/31-05-2023_definitief_sectorrapportage_-_ronde_v_sectoraal_medewerkersonderzoek_mbo.pdf

Verbeterpunten respondenten

Verbeterpunten respondenten

Sectorrapportage security- en privacyawareness MBO

Onderdeel van de vragenlijst waren ook 4 open vragen. Deze waren niet verplicht, maar er is desondanks door een groot aantal respondenten gebruik gemaakt van deze mogelijkheid.

Hoewel de antwoorden uiteenlopen, zowel in inhoud als sentiment, hebben we met hulp van een AI-tool (in een veilige omgeving) per vraag toch een rode draad van de gegeven antwoorden weten te vinden.

Waarom besteed je aandacht aan informatiebeveiliging?

Uit de antwoorden blijkt dat de respondenten het belangrijk vinden om zorgvuldig om te gaan met privacygevoelige informatie van studenten en medewerkers. Ze voelen zich verantwoordelijk voor de veiligheid van deze informatie en willen een betrouwbaar en integer imago uitstralen. Sommigen hebben meer kennis nodig en anderen zijn zich er minder bewust van, maar over het algemeen vinden ze het belangrijk om te handelen volgens de normen en waarden van informatieveiligheid. Het is onderdeel van hun werk en noodzakelijk in de huidige maatschappij.

Uitleg bij de stelling: Ik word goed gefaciliteerd door mijn instelling om informatieveilig te werken.

Uit de antwoorden blijkt dat er een gemengd sentiment is over hoe goed respondenten gefaciliteerd worden door hun onderwijsinstelling om informatieveilig te werken. Sommigen zijn tevreden en denken dat er wel genoeg tools zijn, terwijl anderen vinden dat er meer instructies en trainingen nodig zijn en dat de balans tussen veiligheid en werkbaarheid beter kan. Er wordt ook opgemerkt dat er soms te weinig aandacht is voor privacy en dat informatie beter vindbaar en korter/bondiger gecommuniceerd kan worden. Over het algemeen lijkt er behoefte te zijn aan meer duidelijkheid en ondersteuning op dit gebied.

“Ik mis mogelijkheden om studenten op veilige wijze filmpjes in te laten leveren.”

Verbeterpunten respondenten

Sectorrapportage security- en privacyawareness MBO

Over welke onderwerpen heb jij meer kennis nodig om informatieveilig te kunnen werken?

Respondenten geven aan dat ze behoefte hebben aan meer duidelijkheid over welke informatie als privacygevoelig wordt beschouwd en hoe hiermee om te gaan. Sommigen zeggen dat ze al voldoende kennis hebben, terwijl anderen behoefte hebben aan meer ondersteuning en tools om veilig te werken. Respondenten vinden het belangrijk om op de hoogte te blijven van recente ontwikkelingen en om regelmatig opgefrist te worden met trainingen. Duidelijke communicatie en onderbouwing waarom bepaalde maatregelen worden genomen worden als belangrijk gezien. Er lijkt behoefte te zijn aan meer praktische oplossingen en ondersteuning om veilig te kunnen werken zonder belemmeringen.

"[Ik wil graag weten h]oe studenten vertrouwelijke informatie veilig kunnen opslaan en delen (welke software/tools) met mij!"

Heb jij nog opmerkingen of verbeterpunten voor jouw instelling over informatieveilig werken?

Uit de antwoorden blijkt dat er over het algemeen behoefte is aan meer aandacht voor privacy en security in het onderwijs. Respondenten geven aan dat er meer trainingen en instructies nodig zijn, vooral voor nieuwe medewerkers en medewerkers met weinig kennis van ICT. Ook vraagt men om meer eenduidigheid en controle binnen de instellingen. Er wordt opgemerkt dat de communicatie over dit onderwerp vaak droog en onpersoonlijk is, en dat het laagdrempeliger en begrijpelijker moet worden gemaakt. Respondenten vinden het belangrijk dat er geen onnodige restricties worden opgelegd.

Er is behoefte aan meer duidelijkheid over wat wel en niet mag wat betreft informatie uitwisselen via de mail. Respondenten vinden het belangrijk dat er regelmatig een (online) opfristraining wordt aangeboden over het veilig verwerken en delen van persoonsgegevens of ander gevoelige informatie. Ook wordt er gevraagd naar meer aandacht voor het voorkomen van spam.

Verder wordt er gevraagd om meer bewustwording en communicatie over dit onderwerp, bijvoorbeeld door middel van posters en instructiesheets. Respondenten vinden het belangrijk dat er regelmatig informatie wordt aangeboden over dit onderwerp en dat er meer bekendheid wordt gegeven aan de regels omtrent informatieveiligheid. Er wordt opgemerkt dat er een groot gat zit tussen het beleid op managementniveau en wat er op de werkvloer mee wordt gedaan.

"Nog steeds worden er op een beamer leerlingeresultaten getoond van alle leerlingen aan alle leerlingen."

Over het algemeen lijkt er behoefte te zijn aan meer duidelijkheid, trainingen en bewustwording op het gebied van privacy en security in het onderwijs. Respondenten vinden het belangrijk dat gebruiksgemak niet ondergeschikt mag zijn aan veiligheid en dat er meer eenduidigheid en controle moet komen binnen de instellingen.

"Kijk met mensen van de werkvloer wat er nodig is en voor wie en hoe we dan in ons LVS AVG proof kunnen werken. Ook het verzenden van mails etc is niet eenduidig afgesproken met welke tool we extern info kunnen delen."

"Er is vast veel info te vinden op het intranet. Maar in de dagelijkse woeste werkelijkheid van alledag heeft het niet altijd een 1e prioriteit"

Bevindingen security- en privacyprofessionals

Bevindingen security- en privacyprofessionals

Sectorrapportage security- en privacyawareness MBO

De gesprekken die zijn gehouden met diverse privacy- en securityprofessionals van instellingen geven een gemixt beeld. Sommige instellingen hebben al een groot volwassenheidsniveau, waar awareness bij andere instellingen nog in de kinderschoenen staat. De hierna benoemde onderwerpen zijn een greep uit deze gesprekken.

Schoolbestuur zet de toon

De voorbeeldfunctie van het schoolbestuur is van cruciaal belang bij het bevorderen van cyberveilig gedrag bij medewerkers. Wanneer het bestuur er geen prioriteit aan geeft, wordt informatieveilig werken nooit de norm; je kunt niet van medewerkers verwachten dat ze zich inzetten voor iets waar het bestuur ambivalent over is.

De meeste geïnterviewden kwamen tot de conclusie dat het bestuur van hun instelling nog onvoldoende *on board* is om bij te dragen aan een informatieveilige cultuur. Dit zien we ook terug bij de vragenlijstrespondenten; slechts 3% zegt aandacht te besteden aan informatiebeveiliging omdat de directie het belangrijk vindt.

Schoolbesturen moeten zich ervan bewust zijn dat zij de toon zetten in de instelling. Door het belang van informatiebeveiliging expliciet te benadrukken, creëert het bestuur bewustwording en prioriteit, wat medewerkers stimuleert om actief bij te dragen aan informatieveilig werken.

Het wiel uitvinden

Iedere instelling geeft invulling aan informatieveilig werken op zijn eigen manier. Dit heeft als voordeel dat een instelling waar veel ruimte aan het onderwerp wordt gegeven dit helemaal op maat kan maken, maar een nadeel is dat bij instellingen waar minder prioriteit is, het een ondergeschoven kind kan worden. Waar de ene instelling dus vrijheid ervaart, heeft de andere instelling het gevoel het wiel te moeten uitvinden.

Bevindingen security- en privacyprofessionals

Sectorrapportage security- en privacyawareness MBO

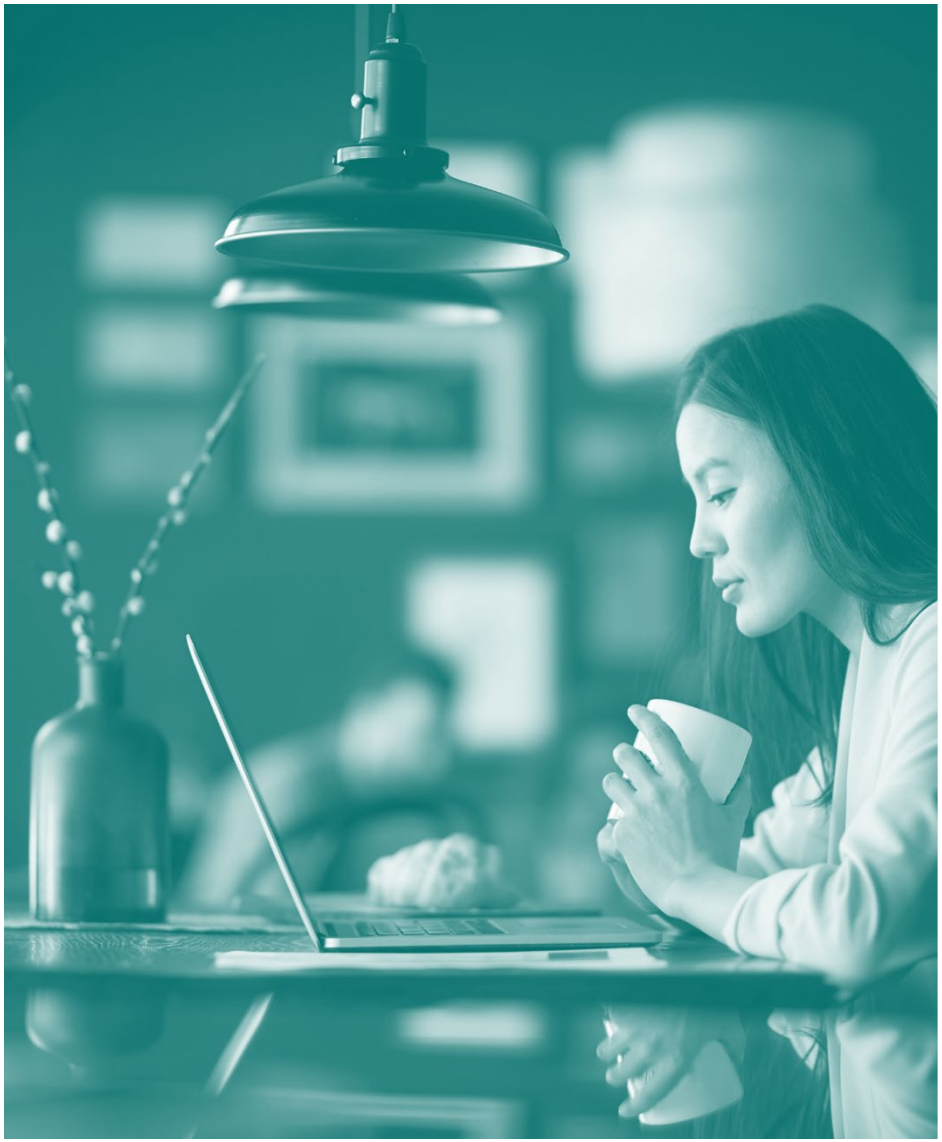
Er zijn talloze initiatieven vanuit allerlei organisaties om awareness te verhogen, maar men kan niet op één plek terecht voor een totaaloplossing. Een kant-en-klaar awarenesspakket voor mbo-instellingen zou verwelkomd worden. Hierin zou bijvoorbeeld MBO Digitaal kunnen voorzien.

Een startklaar awarenesspakket kan instellingen helpen door hen een gestructureerde aanpak te bieden om awareness toegankelijk te maken. Een dergelijk pakket bevat trainingsmaterialen, bewustmakingscampagnes en communicatiemiddelen die eenvoudig kunnen worden geïmplementeerd.

Een kant-en-klaar pakket scheelt tijd en moeite voor instellingen, omdat ze niet zelf alle awareness-content hoeven te ontwikkelen. Hierdoor kunnen ze snel en efficiënt starten met het vergroten van het bewustzijn van medewerkers over beveiligingsrisico's en de juiste procedures, en zo het informatieveilig gedrag van deze medewerkers te verhogen.

Ambassadeurs

Geïnterviewde privacy- en security-professionals benoemden dat het hebben van ambassadeurs van informatieveilig werken een positieve invloed had op de cultuur binnen hun instelling. Als voorstanders van informatieveilig werken fungeren ambassadeurs als rolmodellen en verspreiders van het belang van informatieveiligheid. Ze kunnen medewerkers motiveren om veiligheidspraktijken te omarmen, bewustwordingscampagnes bevorderen en best practices delen. Ambassadeurs kunnen ook als aanspreekpunt fungeren voor vragen en twijfels over beveiligingskwesties. Door actief bij te dragen aan het bevorderen van een positieve veiligheidscultuur, dragen ambassadeurs bij aan het creëren van een instellingsbrede inzet voor informatiebeveiliging.



Bevindingen security- en privacyprofessionals

Sectorrapportage security- en privacyawareness MBO

Olifantenpaadjes

Als mensen teveel belemmeringen ondervinden in hun werkzaamheden, gaan ze deze belemmeringen omzeilen. Wanneer instellingen te strikte en complexe beveiligingsmaatregelen implementeren, kunnen medewerkers geneigd zijn om alternatieve, minder veilige methoden te zoeken om hun werk te doen. Dit kan leiden tot het omzeilen van beveiligingsprocedures, zoals het delen van wachtwoorden of het gebruik van onveilige apparaten of software. Met dergelijke praktijken worden de geïnterviewden regelmatig geconfronteerd. Soms trekken medewerkers die beseffen dat er buiten de gebaande paden wordt gegaan zelf aan de bel, soms komen de professionals er bij toeval achter, en soms komen dergelijke praktijken aan het licht bij een incident.

Alle geïnterviewden geven aan dat zij zoeken naar een balans tussen informatieveiligheid en gebruiksvriendelijkheid. Door medewerkers te voorzien van gebruiksvriendelijke, maar veilige tools en procedures, kunnen zij efficiënter werken zonder de noodzaak om veiligheidsmaatregelen te omzeilen. Het bieden van adequate training en bewustwording kan ook bijdragen aan het begrip van medewerkers over de redenen achter de veiligheidsmaatregelen, waardoor ze meer geneigd zijn om deze te volgen.

Kortom, het begrijpen van de redenen waarom mensen olifantenpaadjes nemen, en het bieden van effectieve en gebruikersvriendelijke beveiligingsoplossingen, kan informatieveilig gedrag bevorderen en het risico op incidenten verminderen.

Conclusie

Conclusie

Sectorrapportage security- en privacyawareness MBO

Overtuigd van belang

Vrijwel alle respondenten zien het belang van informatieveilig werken voor hun onderwijsinstelling ten zeerste in. De erkenning van het belang van informatieveiligheid toont aan dat medewerkers in het onderwijs zich bewust zijn van de gevaren en risico's die bij hu werk komen kijken.

Ondersteuning bereikt medewerkers niet voldoende

Er is een relatief positieve intentie om informatieveilig te werken, maar men mist vaak de nodige kennis en training. Medewerkers willen graag bijdragen aan de bescherming van gegevens, maar weten niet altijd hoe ze dit in de praktijk moeten brengen. Het gebrek aan bewustzijn en duidelijke richtlijnen kan leiden tot onzekerheid en het nemen van risico's.

"Gewoon hun werk doen"

Instellingen moeten een balans vinden tussen informatieveiligheid en gebruiksvriendelijkheid. Door medewerkers te voorzien van gebruiksvriendelijke, maar veilige tools en procedures, kunnen zij *gewoon hun werk doen* zonder de noodzaak om veiligheidsmaatregelen te omzeilen. Het bieden van adequate training en bewustwording kan ook bijdragen aan het begrip van medewerkers over de redenen achter de veiligheidsmaatregelen, waardoor ze meer geneigd zijn om deze te volgen.

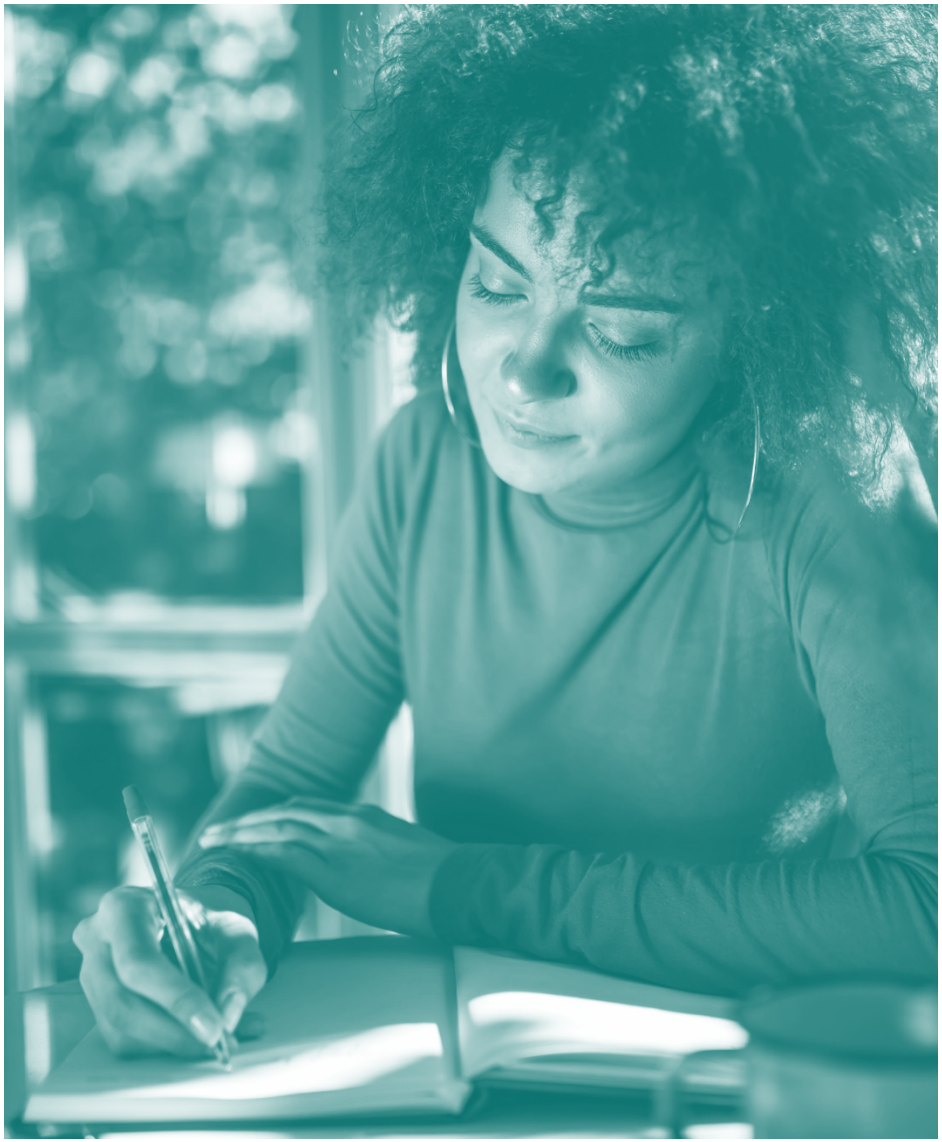
Sleutelrol voor bestuur en leidinggevenden

Meer dan de helft van de respondenten is neutraal of weet niet of hun leidinggevende het goede voorbeeld geeft op het gebied van informatieveilig werken. Ook schoolbesturen zijn over het algemeen niet proactief in het benadrukken van het belang van informatieveilig werken. Bestuur en leidinggevenden fungeren als rolmodellen voor hun medewerkers, en hun acties en gedragingen hebben een directe invloed op de instellingscultuur.

Aanbevelingen

Aanbevelingen

Sectorrapportage security- en privacyawareness MBO



Creëer bewustwording die motiveert met concrete voorbeelden

Wanneer mensen begrijpen waarom informatieveiligheid in hun werkzaamheden belangrijk is, motiveert het hen om veilig te werken omdat ze de waarde van het beschermen van gegevens voor zichzelf, hun collega's en studenten inzien. Dit besef creëert een gevoel van verantwoordelijkheid en zorg voor de beveiliging van informatie.

Om medewerkers bewust te maken van het belang van informatiebeveiliging in hun werk, is het aan te raden om concrete voorbeelden en scenario's te delen die aansluiten bij hun dagelijkse taken. Laat zien hoe het beschermen van vertrouwelijke gegevens hen en de instelling beschermt tegen cyberdreigingen en eventuele datalekken. Benadruk dat een veilige digitale omgeving hun professionele integriteit en de privacy van studenten en collega's waarborgt. Door een praktische en persoonlijke benadering te hanteren, begrijpen medewerkers beter hoe hun individuele bijdrage van belang is voor het versterken van de algehele informatieveiligheid binnen hun instelling.

Ontwijk het olifantenpad

Het belemmeren van medewerkers met te strenge informatiebeveiligingsmaatregelen kan leiden tot het zoeken van olifantenpaadjes, waarbij ze alternatieve, minder veilige methoden gebruiken om hun werk te doen. Dit kan variëren van het delen van wachtwoorden tot het omzeilen van beveiligingsprocedures om efficiëntie te bevorderen. Het is essentieel om een evenwicht te vinden tussen beveiliging en gebruikersgemak, door medewerkers te voorzien van toegankelijke en effectieve beveiligingsoplossingen. Dit zal hen aanmoedigen om veilig gedrag te vertonen, terwijl ze ook productief kunnen blijven zonder de noodzaak te voelen om veiligheidsmaatregelen te omzeilen.

Aanbevelingen

Sectorrapportage security- en privacyawareness MBO

Wees duidelijk en vindbaar

Duidelijke én vindbare gedragsregels stellen medewerkers in staat om gemakkelijk toegang te krijgen tot de juiste richtlijnen en procedures. Hierdoor kunnen zij de vereiste beveiligingsmaatregelen begrijpen en naleven, waardoor het risico op incidenten en datalekken wordt verminderd. Een toegankelijk beleid vergroot ook het bewustzijn van het belang van informatieveiligheid binnen de instelling. Bovendien draagt het bij aan de transparantie van de instelling, wat het vertrouwen van zowel interne als externe belanghebbenden versterkt in de bescherming van gevoelige gegevens en vertrouwelijke informatie.

Meet gedrag

Het meten van het gedrag van mensen op het gebied van informatiebeveiliging geeft inzicht in de effectiviteit van beveiligingsmaatregelen en bewustwordingsprogramma's. Door te evalueren hoe medewerkers omgaan met vertrouwelijke gegevens en de mate waarin zij veiligheidsprotocollen volgen, kunnen zwakke punten en risico's worden geïdentificeerd. Deze metingen bieden waardevolle gegevens om gerichte verbeteringen aan te brengen in training en bewustwording, en om passende maatregelen te nemen om de algehele informatieveiligheid te versterken. Bovendien helpt het meten van gedrag bij het creëren van een cultuur waarin informatieveilig werken en naleving van beleid een integraal onderdeel zijn van het dagelijkse werk van medewerkers.

Het gedrag van mensen kan worden gemeten door middel van beoordelingen, vragenlijsten (zoals die de basis is voor dit rapport), mystery guests en monitoring van beveiligingsactiviteiten. Ook kunnen simulaties van phishingaanvallen worden uitgevoerd om te zien hoe medewerkers reageren op potentiële dreigingen, en kunnen beveiligingsincidenten worden geanalyseerd om eventuele patronen van onveilig gedrag te identificeren.

Aanbevelingen

Sectorrapportage security- en privacyawareness MBO

Geef uitleg

Training en uitleg over lastige onderwerpen blijft van belang; wilskracht en motivatie alleen zijn niet voldoende voor een medewerker om informatieveilig te kunnen werken. Alleen met de juiste kennis kunnen ze proactief bijdragen aan de bescherming van vertrouwelijke gegevens en beveiligingsincidenten verminderen. We raden aan om hierbij te focussen op de volgende onderwerpen: datalekherkenning, risico's social media, sterke wachtwoorden, opslaan en delen van vertrouwelijke (persoons)gegevens.

Lead by example

Het is van essentieel belang dat schoolbesturen en leidinggevenden actief en consequent het belang van informatieveilig werken benadrukken en hun medewerkers inspireren door zelf het goede voorbeeld te geven. Als rolmodellen hebben zij een unieke kans om de bewustwording te vergroten en een positieve veiligheidscultuur te bevorderen.

Door het goede voorbeeld te geven en veiligheidspraktijken consequent toe te passen, laten leidinggevenden zien dat informatieveiligheid een integraal onderdeel is van hun werk. Hierbij kan worden gedacht aan het bespreken van het onderwerp in werkoverleggen, bijvoorbeeld een incident uit het nieuws of een interne *near miss*. Dit schept vertrouwen en moedigt medewerkers aan om beveiligingsbeleid na te leven en bij te dragen aan een veilige werkomgeving.

Schoolbesturen moeten zich ervan bewust zijn dat zij zelf de toon zetten in de instelling. Door het belang van informatiebeveiliging expliciet te benadrukken, creëert het bestuur bewustwording en prioriteit, wat medewerkers stimuleert om actief bij te dragen aan informatieveilig werken.

Linda van Liempt
BDO
linda.van.liempt@bdo.nl

bdo.nl

Opdrachtgever
MBO Raad
mboraad.nl

Organisator
MBO Digitaal
Martijn Bijleveld
m.bijleveld@mbodigitaal.nl
mbodigitaal.nl