Samen aanjagen van vernieuwing

Security- en privacy-awareness in onderwijs en onderzoek

Een sectorrapportage over het bewustzijn bij medewerkers

Auteur(s): Marijke Stokkel, Albert Hankel

Versie: 1.0
Datum: 8 juli 2021

Deze publicatie is gelicenseerd onder een Creative Commons Naamsvermelding 4.0 Internationaal.

Inleiding

Onderwijs- en onderzoeksinstellingen zijn een aantrekkelijk doelwit voor cybercriminelen. Enerzijds werken ze met veel gevoelige en waardevolle informatie (denk aan persoonlijke gegevens van studenten, toetsgegevens, vertrouwelijke onderzoeksdata en technische ontwerpen), anderzijds zijn ze open van karakter en gebruiken ze allerlei soorten tooling en werken ze veel samen met partners. Dit zorgt voor een verhoogde kans op security-incidenten.

Veel cyberaanvallen en security-incidenten zijn gerelateerd aan handelingen van medewerkers. Denk aan klikken op een phishing e-mail, een harde schijf met onderzoeksgegevens verliezen, in een gevoelige mail per ongeluk alle ontvangers in de cc zetten in plaats van bcc.

Bij digitaal weerbare organisaties werken medewerkers informatieveilig en privacybewust. Deze organisaties besteden structurele aandacht aan privacy- en security-awareness. Medewerkers volgen sessies en trainingen om goed te kunnen handelen bij relevante risico's, ze worden voldoende gefaciliteerd om veilig te kunnen werken en leidinggevenden geven het juiste voorbeeld.

Voor een organisatie is het nuttig om te weten hoe het ervoor staat op het gebied van privacy- en security-awareness. Met een duidelijk overzicht van de positieve en leerpunten, kan de organisatie gericht verbeteringen doorvoeren. Vanuit deze gedachte hebben SURF en BDO gezamenlijk awarenessmetingen aangeboden aan de aan SURF verbonden onderwijs- en onderzoeksinstellingen. De metingen vallen onder de SURF Cybersave Yourself (CSY) Awarenesscampagne en hebben tot doel om naast feedback aan de instellingen, tevens een beeld van de sector te krijgen. Er hebben 26 instellingen deelgenomen. Elke instelling heeft een eigen rapportage ontvangen. We hebben de resultaten van alle metingen geanalyseerd. In dit rapport staan naar aanleiding hiervan de belangrijkste bevindingen en conclusies.

Over de auteurs
SURF heeft 'Cybersave Yourself' ontwikkeld, een beveiligingsawarenesscampagne voor onderwijs en onderzoek. Deze bevat beveiligingstips, filmpjes en games over beveiligings- en privacybewustzijn. Voor instellingen biedt Cybersave Yourself een toolkit met materialen waarmee ze zelf bewustwordingsprogramma's kunnen opzetten.

BDO ondersteunt organisaties bij het versterken van hun digitale weerbaarheid. Hiervoor heeft de organisatie een integrale aanpak ontwikkeld, die bestaat uit het uitvoeren van assessments naar kwetsbaarheden en risico's, het implementeren van cybersecurity- en privacy-standaarden, het testen en monitoren van de IT-infrastructuur en het ondersteunen bij een cyberincident. Daarnaast heeft BDO zich gespecialiseerd in het ontwikkelen van een aanpak om gedragsveranderingen bij medewerkers te realiseren.

Opzet van de meting en analyse

Dit hoofdstuk bestaat uit onze visie op gedragsverandering en gedragsonderzoek, de aanpak van de awarenessmetingen bij de instellingen en de opzet van de analyse in dit rapport.

Visie op gedragsverandering en gedragsonderzoek

Menselijk gedrag is complex. Mensen vertonen het gedrag dat securityprofessionals als risicovol zien vaak al jaren en tal van onbewuste processen en omgevingsfactoren houden het in stand. Dat is niet makkelijk te veranderen. Zeker gewenst gedrag rondom privacy en security, wat vaak als lastig of ingewikkeld ervaren wordt, is moeilijk te realiseren. Veel awarenessprogramma's richten zich op het overbrengen van kennis. De medewerkers krijgen een e-learning, presentatie of leaflet, gebaseerd op de privacy- en securityrichtlijnen van de organisatie, die weer gebaseerd zijn op het privacy- en securitybeleid. Deze aanpak is (impliciet) gebaseerd op de gedachte dat menselijk gedrag is gebaseerd op rationele overwegingen en dat mensen hun gedrag aanpassen als zij overtuigende argumenten en kennis aangedragen krijgen. Dit is achterhaald. Mensen laten zich in hun dagelijkse gedrag niet alleen leiden door rationele overwegingen.[1] Andere factoren spelen ook een rol, zoals persoonlijke drijfveren en praktische barrières. [2]

Gedragsmodel COM-B

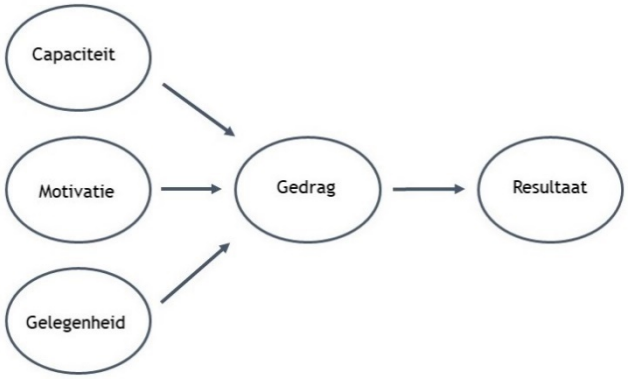
Om te veranderen, is het nodig dat mensen kunnen (capaciteit), willen (motivatie) en gefaciliteerd worden (gelegenheid). Dit is kortgezegd onze visie op privacy- en security-awareness, gebaseerd op het COM-B model van Susan Michie.[3] Vaak zijn deze componenten ook met elkaar verweven. Als mensen de 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.

- **Capaciteit** heeft betrekking op de juiste kennis en vaardigheden om de verandering te kunnen uitvoeren. Bijvoorbeeld: kunnen medewerkers risicovolle situaties herkennen? Weten ze wat ze moeten doen bij een datalek? Weten ze wat een sterk wachtwoord is? Hebben leidinggevenden de juiste vaardigheden om medewerkers aan te spreken op onveilig gedrag?
- Bij **motivatie** draait het om de intrinsieke motivatie van de medewerkers: wat vinden zij belangrijk? Sluiten privacy en security aan bij hun persoonlijke drijfveren en willen zij zich daar vanuit eigen overtuiging voor inzetten?

[1] 'Hoe mensen keuzen maken. De psychologie van het beslissen.' W.L. Tiemijer, 2010. p10-11
[2] 'Using behavioural insights to improve the public's use of cybersecurity best practices.' Government Office for Science, 2014,
[3] 'Het gedragsveranderingswiel. 8 Stappen naar succesvolle interventies.' Susan Michie, Lou Atkins & Robert West, 2018

- **Gelegenheid** gaat over het faciliteren van medewerkers om veilig gedrag te vertonen. Hebben medewerkers de juiste middelen, zoals ICT-tooling, om veilig te kunnen werken? Wordt veilig werken makkelijk gemaakt, of moeten er juist veel extra handelingen voor verricht worden? Geven leidinggevenden het juiste voorbeeld? Zijn privacy- en security-onderwerpen van gesprek op de afdeling?

De awarenessmetingen zijn gebaseerd op het COM-B gedragsmodel.



Figuur 1. COM-B gedragsmodel

Gedragsonderzoek

De meting is uitgevoerd via een online vragenlijst en betreft dus een kwantitatief onderzoek. Deze methode is geschikt om een globaal inzicht te krijgen in het (zelfgerapporteerde) gedrag en de kennis, de mening en ervaringen van de doelgroep. Vooral de componenten 'capaciteit' en 'gelegenheid' zijn goed vast te stellen via een online vragenlijst. De component 'motivatie' is wat lastiger, omdat de materie minder eenduidig is en daardoor minder gemakkelijk te vangen in een vragenlijst. Ook gaat deze component over het eigen handelen en de eigen intenties. Door de methode van zelfrapportage kan een vertekening van het werkelijke gedrag of de intentie optreden. Mogelijk heeft men geen scherp beeld van het feitelijke eigen gedrag, omdat het om onbewust gedrag gaat of men het zich niet zo goed kan herinneren. Ook kan men er, bewust of onbewust, minder eerlijk over zijn omdat bepaald gedrag of bepaalde intenties niet sociaal wenselijk zijn.[4] Ondanks deze bezwaren geeft de meting wel een globale indicatie van de motivatie van respondenten. Het zegt iets over hoe de respondenten zichzelf zien en zichzelf willen presenteren op dit onderwerp. In de rapportages adviseren we dat als de instelling behoefte heeft aan dieper inzicht in de relatie tussen persoonlijke drijfveren en privacybewust en informatieveilig gedrag, men separaat een aantal (diepte-)interviews houdt met medewerkers van de instelling.

Aanpak awarenessmetingen

In het najaar van 2020 hebben we een oproep naar de leden van SURF voor deelname aan de 'CSY privacy- en security-awarenessmeting'. Tientallen instellingen hebben zich aangemeld. Tussen januari en maart 2021 is de meting uitgezet bij 26 instellingen. De deelnemende instellingen ontvangen daarvoor een instellingsspecifieke url die ze zelf kunnen verspreiden in hun organisatie. Achter de url zit een vragenlijst, die medewerkers anoniem kunnen invullen. De doelgroep van de meting bestaat uit medewerkers van de instelling.

In de metingen staan de volgende vragen centraal:

[4] 'Hoe is gedrag te onderzoeken? Overzicht van 18 onderzoeksmethodieken voor effectief beleid.' Behavioral Insights Netwerk Nederland. Ministerie van Economische Zaken en Klimaat, november 2019

In hoeverre willen en kunnen medewerkers privacybewust en informatieveilig** werken? En in hoeverre worden zij hiertoe gefaciliteerd?*

*Met privacybewust werken bedoelen we dat medewerkers tijdens hun werk zorgvuldig omgaan met gegevens van studenten, respondenten, medewerkers of andere betrokkenen. Bijvoorbeeld: voor een onderzoeks- of onderwijsproject 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.

Vraagsoorten
De meting bevat twee soorten vragen: meningvragen en quizvragen. De meningvragen zijn om te achterhalen hoe de respondenten privacy en security (awareness) in hun instelling ervaren. 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.
Er zijn 4.916 vragenlijsten ingevuld. Naast de score van elke afzonderlijke instelling, is ook een benchmarkscore vastgesteld. Dit is de gemiddelde score van alle deelnemende instellingen. Zo kunnen de deelnemers hun eigen resultaat vergelijken met die van hun peers. Elke deelnemende instelling ontvangt een eigen rapportage met bevindingen, conclusies en advies om privacy & security awareness structureel en gericht te verbeteren.

Scoringsmethode
De totaalscore per instelling (cijfer 1-10) is vastgesteld door het gemiddelde van de drie componentscores te nemen. Elk component (motivatie, gelegenheid, capaciteit) telt even zwaar mee.
De componenten 'gelegenheid' en 'motivatie' bestaan uit de eerder genoemde meningvragen. De respondenten beantwoorden deze vragen door een cijfer van 1 tot en met 5 te geven (bijvoorbeeld van 'zeer belangrijk' tot 'zeer onbelangrijk'). Voor de component 'capaciteit' is de score opgebouwd uit de acht toetsvragen. We hebben het aantal goede antwoorden geteld en het gemiddelde daarvan genomen als score.

We hebben de volgende scoringsmethodes toegepast.

Component Motivatie & Gelegenheid		Component Capaciteit	
Antwoord	**Score**	**Aantal goed**	**Score**
1	1	0	0
2	3,25	1	1,25
3	5,5	2	2,50
4	7,75	3	3,75
5	10	4	5
		5	6,25
		6	7,5
		7	8,75
		8	10

Tabel 1. Scoringsmethode

Opzet analyse

De reden dat we een analyse maken van de 26 rapportages van de awareness-metingen is dat we benieuwd zijn of dit nieuwe gezichtspunten oplevert die relevant zijn voor de hele sector. We willen weten wat de overall resultaten zijn van de instellingen samen, en of er grote verschillen zijn:

- Tussen de functiegroepen (onderwijs/onderzoek, ondersteuning, bibliotheek en overig)
- Tussen de typen organisaties (mbo, hbo, universiteit, overig)
- Tussen de componenten (motivatie, gelegenheid, capaciteit)

En we willen weten of er nog andere zaken opvallen. Hiervoor vergelijken we de scores van de verschillende instellingen, de functiegroepen, typen organisaties en de componenten. Ook analyseren we de losse opmerkingen die respondenten hebben geplaatst.

Uiteindelijk geven de CSY-awarenessmetingen op drie niveaus inzicht:

- De individuele medewerker die deelneemt. Die krijgt tijdens en direct na het invullen van de vragenlijst terugkoppeling over zijn of haar antwoorden op de toetsvragen.
- De deelnemende instelling. Die ontvangt een rapport met bevindingen, conclusies en aanbevelingen.
- En tot slot de hele sector, middels dit rapport. Op basis van de rapportages onderzoeken we welke conclusies kunnen trekken die voor onderwijs- en onderzoekinstellingen relevant kunnen zijn.

Bevindingen

Dit hoofdstuk beschrijft de belangrijkste bevindingen van de awarenessmetingen. Het start met de awarenessmeting in aantallen. Vervolgens bespreken we de scores: de totaalscore en de scores per functiegroepen, sectoren en componenten. Tot slot bespreken we verbeterpunten die respondenten hebben aangedragen.

Aantallen

Er hebben 26 instellingen deelgenomen aan de metingen, met in totaal 4.916 ingevulde vragenlijsten. We gaan ervan uit dat één ingevulde vragenlijst gelijk staat aan één respondent. Per instelling zijn er gemiddeld 189 respondenten, maar de verschillen tussen de instellingen zijn aardig hoog. Er zijn instellingen met 20-30 respondenten, en (enkele) instellingen met meer dan 500 respondenten.

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

- onderwijs/onderzoek
- ondersteunend
- bibliotheek
- anders

Wat opvalt (zie tabel 1) is dat er relatief veel respondenten vallen in de functiegroep ‘ondersteunend’. Sommige instellingen hebben alleen maar onderzoek gedaan naar de awareness bij ondersteunende diensten, maar alsnog lijkt er sprake van een oververtegenwoordiging van respondenten in ondersteunende functies.

We hebben ook onderscheid gemaakt tussen de verschillende sectoren in het onderwijs, dat zijn:

- mbo
- hbo
- universiteit
- overig

De sector ‘overig’ bestaat uit instellingen die niet in de eerste drie categorieën vallen. Dit betreft onder andere onderzoeksinstituten en bibliotheken.

De CSY awarenessmetingen in aantallen		
Categorie	**Sub-categorie**	**Resultaat**
Aantal ingevulde vragenlijsten		4.916
Aantal deelnemende instellingen		26
Gemiddeld aantal respondenten[5] per instelling		189
Aantal respondenten per functiegroep	onderwijs/onderzoek	2.030

[5] We gaan ervan uit dat één ingevulde vragenlijst gelijk staat aan één respondent.

	ondersteunend	2.478
	bibliotheek	167
	anders	214
Aantal instellingen per sector	mbo	6
	hbo	9
	wo	4
	overig	7

Tabel 2. De CSY awarenessmetingen in aantallen

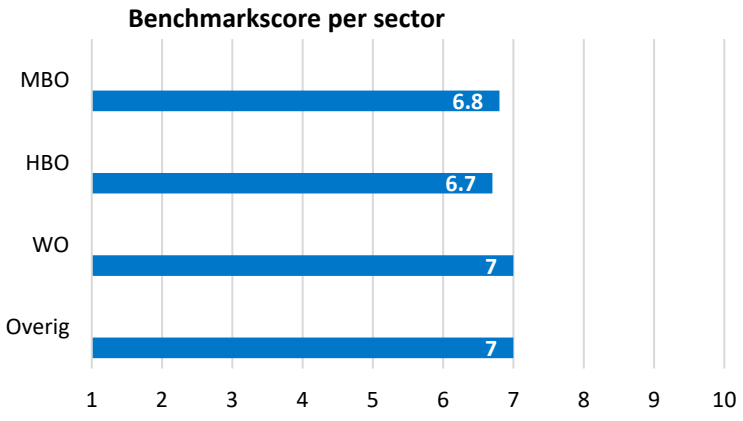
Totaalscore

Op basis van de ingevulde vragenlijsten ontvangt elke deelnemende instelling een totaalscore (1-10). Het gemiddelde van alle instellingen, de benchmark totaalscore, is 6,8. Wat opvalt, is dat de totaalscores van de deelnemende instellingen heel dicht bij elkaar liggen. Alle instellingen scoren tussen de 6,5 en 7,6. Maar liefst 17 instellingen hebben een totaalscore tussen 6,6 en 7,0. De standaarddeviatie, de gemiddelde afwijking van het gemiddelde, is met 0,28 klein te noemen.

In onze optiek heeft de instelling bij een totaalscore van 7 of hoger voldoende basis om privacybewust en informatieveilig te werken. Je zou kunnen zeggen dat de medewerkers dan gemiddeld redelijk weerbaar zijn tegen mensgerichte cyberaanvallen en security incidenten. Aangezien cyberaanvallers maar een kleine kans nodig hebben – één medewerker die klikt op een phishing e-mail – om flinke schade aan te richten, raden wij aan om een minimale awareness score van 7,5 na te streven.

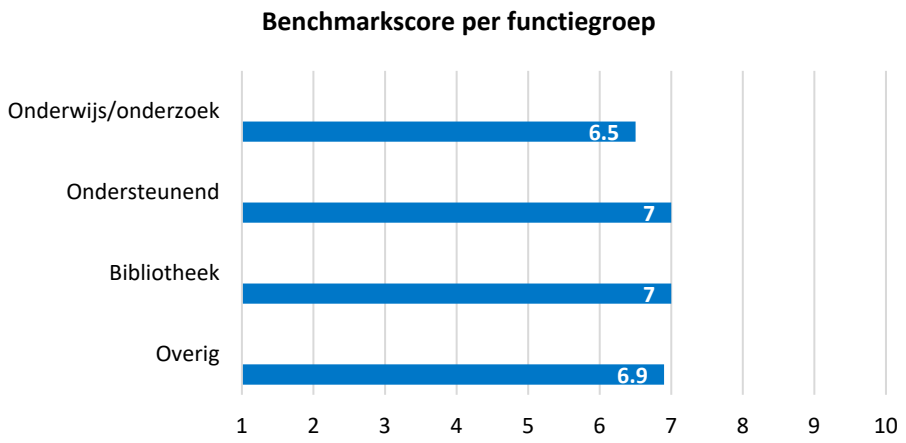
Scores sectoren en functiegroepen

Als we kijken naar de benchmarkscore per sector, valt op dat ook hier de scores niet ver uit elkaar liggen. Universiteiten en ‘overige’ instellingen scoren iets hoger dan mbo-scholen, die het weer iets beter doen dan hbo-instellingen.



Figuur 2. Benchmarkscore per sector

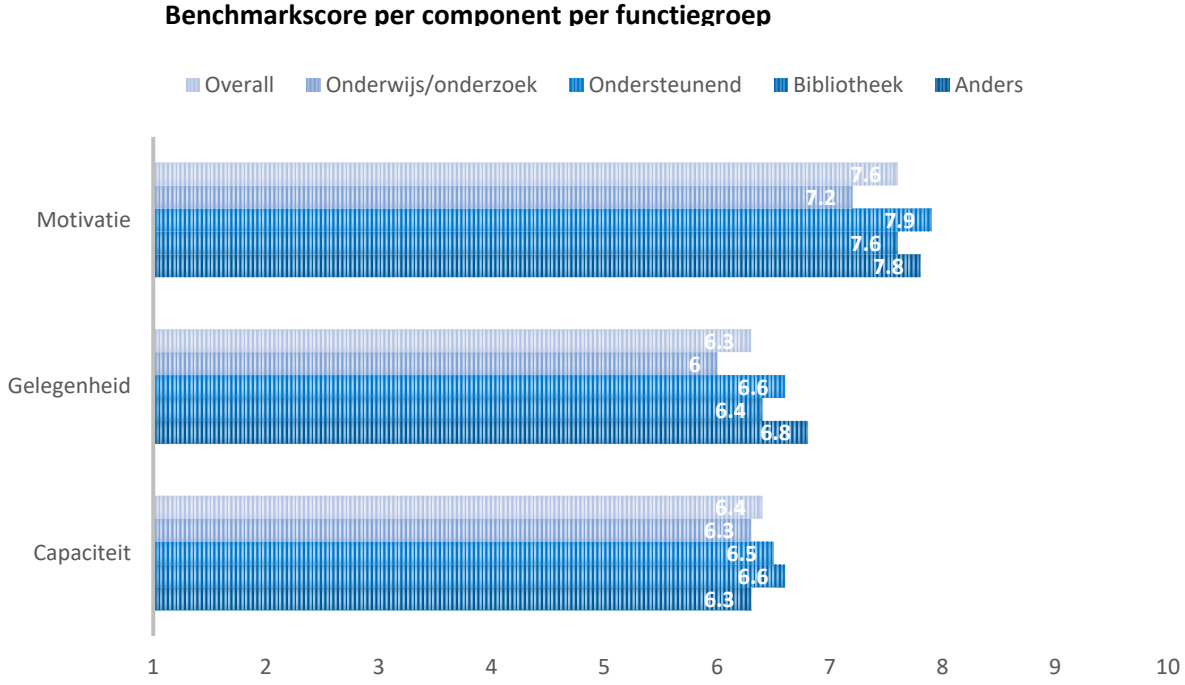
Bij de functiegroepen zien we wel duidelijk verschil. De functiegroep onderwijs/onderzoek scoort beduidend lager dan de andere functiegroepen.



Figuur 3. Benchmarkscore per functiegroep

Componentscores

De totaalscores van de instellingen worden vastgesteld door het gemiddelde van de drie componentscores. Elk component (motivatie, gelegenheid, capaciteit) telt even zwaar mee. In deze paragraaf kijken we naar de scores per component (per functiegroep) en binnen de componenten. Als we de scores van de drie componenten naast elkaar leggen, valt op dat ‘motivatie’ een stuk hoger (7,6) scoort dan ‘gelegenheid’ (6,3) en ‘capaciteit’ (6,4). Onderwijs/onderzoek loopt achter op de andere functiegroepen, vooral met betrekking tot ‘motivatie’ en ‘gelegenheid’.



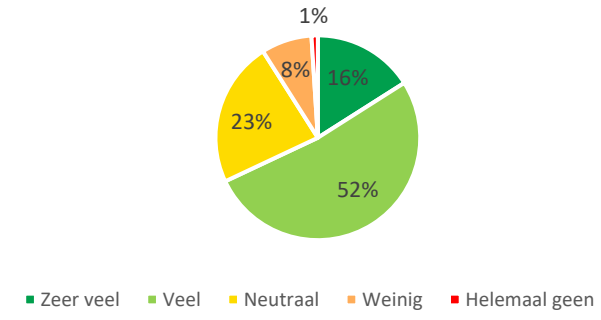
Figuur 4. Benchmarkscore per component per functiegroep

Component 'motivatie'

De antwoorden van de vragen voor de component 'motivatie' kleuren grotendeels (diep)groen. Deze component bestaat uit twee vragen:

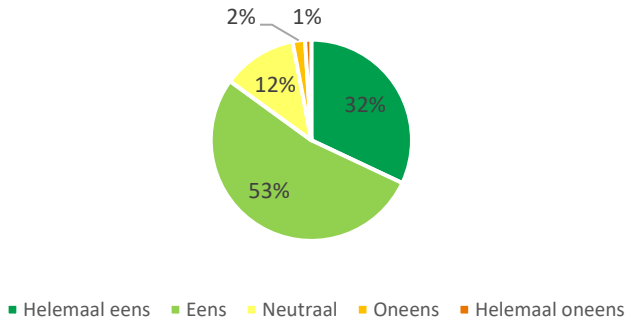
- 'Hoeveel aandacht besteed jij over het algemeen tijdens je werk aan privacy en informatiebeveiliging?' 75% zegt (zeer) veel aandacht.
- 'Ik ben bereid om extra moeite te doen om privacybewust en informatieveilig te werken.' 85% is het (helemaal) eens met deze stelling.

Hoeveel aandacht besteed jij over het algemeen tijdens je werk aan privacy en informatiebeveiliging?



Figuur 5. Antwoorden op vraag 1 Motivatie

'Ik ben bereid om extra moeite te doen om privacybewust en informatieveilig te werken'



Figuur 6. Antwoorden op vraag 2 Motivatie

Deze antwoorden duiden op een hoge motivatie om informatieveilig en privacybewust te werken. Bij navraag naar de redenen waarom men (zeer) veel aandacht besteedt aan privacy en informatiebeveiliging, antwoorden velen het simpelweg een belangrijk thema te vinden. Een ander veel gegeven antwoord is dat men werkt met vertrouwelijke (persoons)gegevens, en daarom zeer zorgvuldig met de gegevens omgaat. Respondenten die minder aandacht zeggen te besteden aan privacy en informatiebeveiliging, zeggen veelal dat deze thema's voor hen niet relevant zijn en dat ze ervan uitgaan dat de systemen al veilig zijn en dat de afdeling ICT daar zorg voor draagt. Ook noemen sommigen de hoge werkdruk als reden om privacy en security geen prioriteit te kunnen geven.

'Hou zelf niet van mijn data op straat. Dus dan zorg ik ook voor privacy voor anderen.'

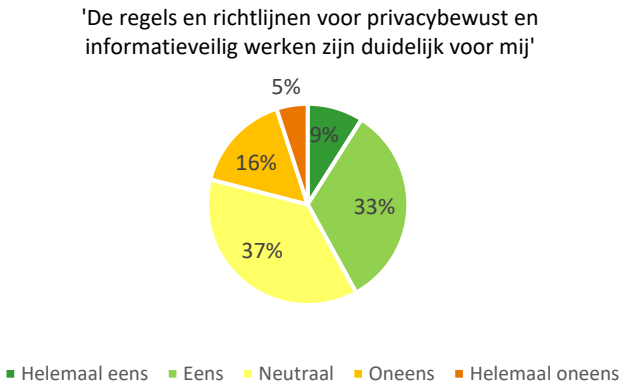
'Bij het online lesgeven is de focus op de les, niet op de privacy. Sterker nog, dat staat me vaak in de weg. Daarnaast houd ik me er gewoon niet zo erg mee bezig in mijn werk, maar wel privé.'

Component 'gelegenheid'

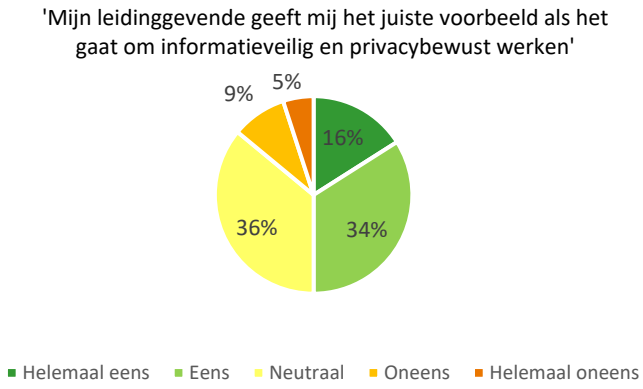
Met een gemiddelde score van 6,3 voor de component 'gelegenheid' zijn respondenten redelijk tevreden over de manier waarop zij gefaciliteerd worden om privacybewust en informatieveilig te kunnen werken. Echter, voor geen enkele stelling van deze component geldt dat een meerderheid van de respondenten het er (helemaal) mee eens is.

Het minst positief is men over de regels en richtlijnen met betrekking tot privacybewust en informatieveilig werken. Slechts 41% van de respondenten is het (helemaal) eens met de stelling dat deze duidelijk voor hen zijn. Als toelichting stellen veel respondenten dat ze niet op de hoogte zijn van het bestaan van regels of richtlijnen, of dat ze niet weten waar ze deze kunnen vinden. Anderen stellen dat de regels en richtlijnen te algemeen geformuleerd zijn en niet van toepassing op hun eigen werksituatie. Zo zegt een respondent: 'Dit hele proces moet echt grootser aangepakt worden en er moet samen met de onderzoeker gewerkt worden, in plaats van een formulier over de schutting te gooien dat maar half begrepen wordt.' Wat ook veel gezegd wordt: 'ik weet niet precies wat de regels zijn', 'ik doe het meer op gevoel' of 'ik volg mijn boerenverstand'. Sommigen steken hun hand in eigen boezem: 'Ik weet niet waar ik de info/instructies kan vinden (maar heb er waarschijnlijk ook niet goed genoeg naar gezocht).'

'Ik heb er wel een gevoel bij en weet er ook wel wat van, maar de precieze regels en richtlijnen ken ik niet.'



Figuur 7. Antwoorden op vraag 1 Capaciteit



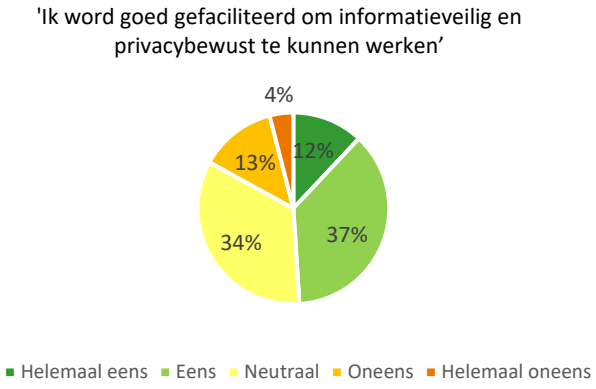
Figuur 8. Antwoorden op vraag 2 Capaciteit

'Onderwijs is vaak improviseren en pragmatisch. (…) We merken nu al dat studenten het moeilijk vinden om (…) gemotiveerd te blijven of überhaupt iets op te steken tijdens een les. Een activerende quiz, doodle, creative break of whiteboardsessie kan dan niet zonder externe tools. Regels en richtlijnen staan ver weg van deze noden.'

Met de stelling 'Mijn leidinggevende geeft mij het juiste voorbeeld als het gaat om privacybewust en informatieveilig werken' is de helft van de respondenten het (helemaal) eens. Uit de opmerkingen van medewerkers blijkt dat privacy en security vaak geen onderwerp van gesprek zijn tussen medewerkers en hun leidinggevende. Met de laatste stelling van deze component, 'ik word goed gefaciliteerd om informatieveilig en privacybewust te kunnen werken', is 49% van de respondenten het (helemaal) eens. Velen zeggen dat ze eigenlijk niet weten of ze goed gefaciliteerd worden, en ook niet wat ze op dat vlak kunnen verwachten van hun instelling. Ze hebben zelf geen beeld bij de tooling of andere

'Ik heb geen idee hoe mijn leidinggevende het doet. We praten hier nooit over.'

ondersteuning die ze nodig hebben om privacybewust en informatieveilig te kunnen werken. Ook zeggen veel respondenten (nogmaals) dat ze heldere en concrete richtlijnen missen. Een aantal respondenten noemt SURFdrive als privacyvriendelijke tool, of tooling die specifiek door hun eigen instelling wordt gebruikt. Meerdere respondenten zeggen dat ze graag ondersteuning op het gebied van privacy en security willen die aansluit bij hun dagelijkse werkpraktijk. Zij ervaren de in hun instelling bestaande regels, richtlijnen en tooling als te star. Deze staan te ver af van hun wensen en behoeften en conflicteren met hun werkzaamheden. En, tot slot, sommigen zijn ronduit content met de wijze waarop ze gefaciliteerd worden: ‘De laptop waarmee ik werk is goed beveiligd, ICT-hulpdiensten zijn goed bereikbaar, er is een duidelijk bedrijfshandboek, er is geregeld aandacht voor op intranet.’



Figuur 9. Antwoorden op vraag 3 Capaciteit

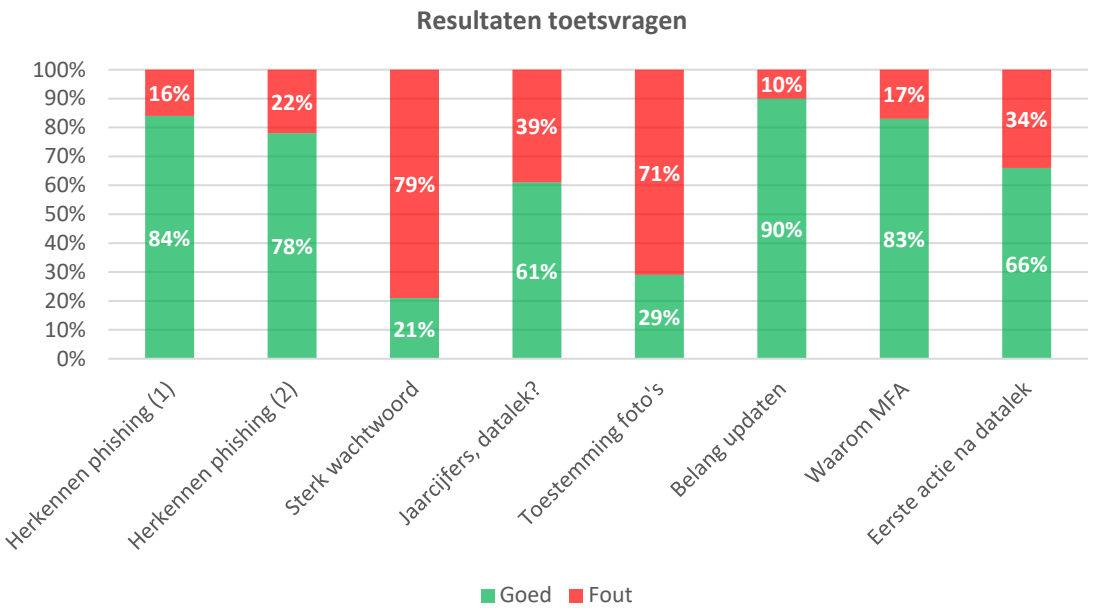
Component ‘capaciteit’

Deze component bestaat uit acht toetsvragen en een vraag over welke inhoudelijke onderwerpen men meer kennis zou willen hebben om privacybewust en informatieveilig te kunnen werken.

Dit zijn de toetsvragen (zie bijlage 1 voor de vragenlijst):

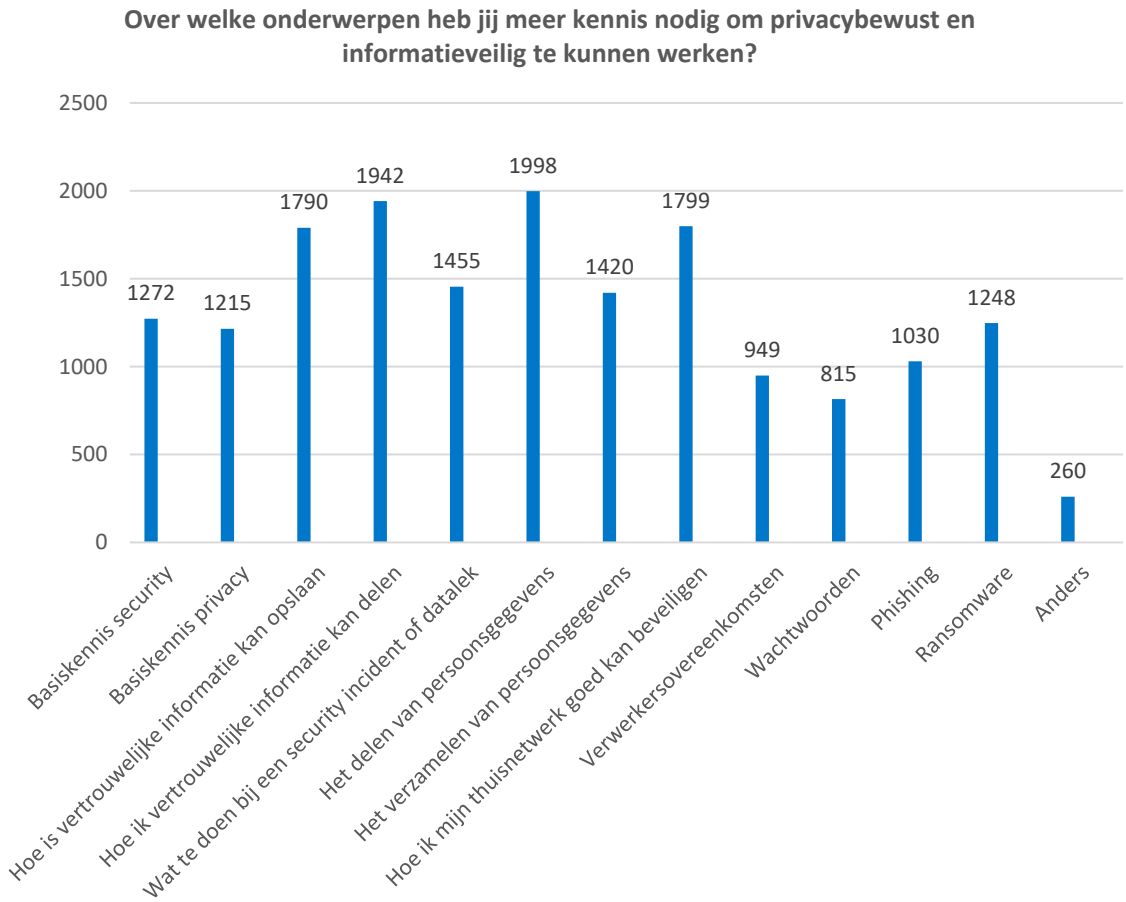
1. Het herkennen van een phishing e-mail (1)
2. Het herkennen van een phishing e-mail (2)
3. Het herkennen van het sterkste wachtwoord
4. De jaarcijfers van de instelling lekken voortijdig uit. Is dit een datalek?
5. Bij een open dag van de instelling worden foto’s gemaakt voor op de website. Is het nodig om aan iedereen die op de foto staat, expliciete toestemming te vragen?
6. Waarom is het belangrijk om je ICT-systemen geregeld te updaten?
7. Wat is het voordeel van multi-factorauthenticatie?
8. Je verliest je laptop met gegevens van respondenten van een vertrouwelijk onderzoek. Een datalek! Wat doe je als eerst?

In de resultaten valt op dat men moeite heeft om een sterk wachtwoord te kunnen herkennen. Ook ontbreekt het bij de meesten aan de juiste kennis over toestemming en beeldmateriaal. Men is wél goed op de hoogte van het belang van updaten en van multi-factorauthenticatie (MFA).



Figuur 10. Resultaten toetsvragen

De respondenten willen vooral meer weten over het delen van vertrouwelijke informatie en van persoonsgegevens. Dit blijkt uit de vraag naar onderwerpen waarover men meer kennis nodig heeft om privacybewust en informatieveilig te kunnen werken. Ook het beveiligen van het thuisnetwerk en het opslaan van vertrouwelijke gegevens worden vaak genoemd. Het minst genoemde onderwerp is wachtwoorden. Dat is opvallend, omdat bij de toetsvragen bleek dat men hier het minst over wist.



Figuur 11. Genoemde thema's waarvan men zegt meer kennis nodig te hebben

Verbeterpunten van respondenten

In de meting is aan de respondenten gevraagd of zij opmerkingen of verbeterpunten hebben voor de instelling. Er zijn vele opmerkingen en verbeterpunten gegeven. Sommige gingen heel specifiek over de eigen instelling (‘onze informatiemanager is altijd goed bereikbaar voor vragen, dat vind ik prettig’), maar de meeste waren ook voor een breder publiek relevant. In deze paragraaf hebben we de verbeterpunten onder de loep genomen. We hebben een aantal categorieën onderscheiden, waar het overgrote deel van de verbeterpunten onder geschaard kan worden.

De gebruiker centraal

’Ga langs bij de afdelingen. Alles digitaal, per mail of intranet communiceren werkt

Een veel gehoord verzoek is om niet alleen te ‘zenden’ maar ook het gesprek aan te gaan met de eindgebruiker. Respondenten willen graag dat er iemand meedenkt om privacybewust en informatieveilig werken in te bedden in de manier van werken. Dit betekent dus ook dat er verschillende boodschappen zijn voor verschillende doelgroepen.

Persoonlijke ondersteuning

Er is bij respondenten behoefte aan een toegankelijke contactpersoon op het gebied van privacy en security. Iemand die ze even kunnen bellen als ze vastlopen. Een aantal zegt ook dat ze graag willen dat er iemand meekijkt om te zien of hun thuisnetwerk wel veilig is om te werken.

‘Hoe geweldig zou een thuisbezoek zijn, door iemand die de veiligheid echt checkt.’

Aandacht en herhaling

Veel respondenten onderschrijven het belang van privacy en security en zeggen dat hun instelling er meer aandacht aan mag besteden, en dat de boodschap regelmatig herhaald dient te worden, zodat het gaat beklijven.

Duidelijke regels

Het is niet voor iedereen helder wat is toegestaan op het gebied van privacy en security. Hierdoor ontstaat willekeur. Welke gegevens mogen gedeeld worden, intern en extern? Welke tooling mag gebruikt worden om (zeer) vertrouwelijke gegevens op te slaan en te delen? Men heeft behoefte aan concrete adviezen.

Hapklare brokken

Maak geen ellenlange stukken in jargon, maar verpak de boodschap in korte en heldere documenten, is het verzoek. ‘Ik wil hier alleen informatie van als het een kort stappenplan/beslisboom is, want als het allemaal documenten worden van een paar pagina's ga ik ze niet lezen. Daar heb ik geen tijd voor en ik onthoud dan ook niet wat de strategie is. Het is niet dat ik niet aan privacy/veiligheid wil doen (ik doe het namelijk naar mijn beste

kunnen/inzicht en waarschijnlijk is dat vrij netjes) maar ik heb geen tijd om documenten door te spitten om te kijken of het nog beter kan.'

'De instelling heeft het onderwerp serieus opgepakt, maar we draaien soms ook helemaal door (ineens zijn de verjaardagslijstjes taboe, mogen we geen adres hebben van een collega om een kaartje te sturen omdat hij/zij ziek is. Dit vloeit voort uit het feit dat iedereen het anders interpreteert of het niet weet en dan extreem voorzichtig wordt.'

Expertinstructies

Meerdere respondenten verzoeken om niet alleen basiskennis over te dragen, maar ook expertinstructies te geven. 'Er is vaak alleen maar uitleg op 'dummies'-niveau. Dat is niet gepast op de universiteit. Regels zijn er, uitleg over resultaten ook. Uitleg over redenen of mechanismen zelden of nooit. "Heldere" regels of uitleg betekent regels of uitleg op het niveau van de toehoorder.'

Inwerkprogramma

Zorg ervoor dat nieuwe medewerkers bij binnenkomst direct informatie ontvangen over wat er van hen verwacht wordt en wat zij zelf kunnen doen om veilig te werken, is een advies van meerdere respondenten.

Verplichte training

Een aantal respondenten pleit voor een verplichte training. Zij verwijzen naar het bedrijfsleven, waar dat meer gangbaar is dan binnen het onderwijs. 'Bij de bank hadden we maandelijks en 'toets' die we over deze onderwerpen moesten maken. Daarbij moest je 100% scoren. Bij fouten kreeg je meer vragen en werden vragen net zo lang herhaald tot je alles goed had. Dit zorgde er wel voor dat dit echt ging leven in de bewustwording van alle medewerkers en niet slechts bij een select groepje zoals nu het geval is. Door het onderwerp maandelijks terug te laten komen, kan de informatie ook niet wegzakken.'

Eenvoudig en werkbaar

Veel respondenten zeggen dat ze best veilig willen werken, maar dat dit niet ten koste mag gaan van de uitvoerbaarheid van het werk. 'Probeer het niet te ingewikkeld te maken. De behoefte is: hoe kunnen we zo simpel en effectief ons aan de privacywetgeving houden. Bij voorkeur met zo weinig mogelijk extra systemen, handelingen en procedures bovenop de vele systemen, handelingen en procedures die al bestaan binnen een grote en ambtelijke organisatie als de universiteit.' En als het éven kan, zorg er dan voor dat de organisatie preventief, al dan niet geautomatiseerd, veiligheidsmaatregelen uitvoert, zodat de medewerker daar zelf niet mee bezig hoeft te zijn.

'Als tools niet óók gebruiksvriendelijk zijn worden ze niet gebruikt.'

Actieve leidinggevenden

Leidinggevenden zijn vaak onzichtbaar bij het ontwikkelen en uitvoeren van privacy- en security-awareness-interventies voor medewerkers. Sommige respondenten stellen dat leidinggevenden hier actiever in kunnen opereren. Dat kunnen ze doen door hun medewerkers hier op aan te

spreken, dit onderwerp op de agenda te zetten bij werkoverleggen en management-overleggen en actief de boodschap uit te dragen. En niet alleen mailtjes doorsturen, zoals een van de respondenten opmerkt.

Conclusies

Op basis van de bevindingen van de awarenessmetingen bij 26 instellingen, concluderen we het volgende.

1. **De awarenessniveaus van de instellingen komen redelijk met elkaar overeen**
   Een opvallend resultaat is dat de scoreverschillen tussen de instellingen relatief klein zijn. De totaalscores kennen weinig variëteit en ook de scoreverdeling van de componenten komt bij de meeste instellingen overeen. De respondenten bij verschillende instellingen zeggen ongeveer even gemotiveerd te zijn en ongeveer even goed gefaciliteerd. En ze hebben ongeveer hetzelfde kennisniveau van privacy- en securitythema's. Mogelijk kunnen we dit deels verklaren door de sectorbrede samenwerkingsinitiatieven op het gebied van privacy en security, zoals de CSY-campagne en ontwikkeling en implementatie van informatieveilige en privacyvriendelijke ICT-tooling (zoals bijvoorbeeld SURFdrive en SURFfilesender).
   Het enige grotere verschil is dat de functiegroep onderwijs/onderzoek achterblijft bij de andere functiegroepen, zowel in deelname aan de metingen als in resultaten. Vooral de componenten 'motivatie' en 'gelegenheid' blijven achter vergeleken met andere functiegroepen. De score bij 'capaciteit' wijkt bijna niet af.
   Een mogelijke verklaring is de hoge werkdruk die vooral medewerkers in deze functiegroep ervaren.[6] Dit is ook door een aantal respondenten zo genoemd. Privacybewust en informatieveilig werken krijgt daardoor wellicht minder prioriteit. Een andere oorzaak kan zijn dat de werksituatie bij deze functiegroep, vooral bij onderzoekers, minder eenduidig is te vatten in een set regels of richtlijnen. Onderzoekers werken vaak in (internationale) samenwerkingsverbanden, waarin de regels en richtlijnen van de instelling niet zonder meer opgevolgd kunnen worden. Bijvoorbeeld: een instelling kan verbieden om Google Docs te gebruiken voor werkzaamheden, maar als het consortium waar een onderzoeker deel van uitmaakt heeft besloten om dit te gebruiken om samen te werken, heeft de onderzoeker soms geen keus. Deze situatie zorgt er mogelijk ook voor dat deze functiegroep lager scoort op 'motivatie' en 'gelegenheid'.

2. **De motivatie om privacybewust en informatieveilig te werken is - naar eigen zeggen - hoog**
   Van de drie componenten steekt 'motivatie' er qua score met kop en schouders bovenuit. Respondenten zeggen veel tijd te besteden aan privacy en informatieveiligheid, en daar ook extra moeite voor te willen doen. We moeten er rekening mee houden dat de gebruikte onderzoeksmethode, zelfrapportage, een vertekening van de werkelijkheid kan geven. Maar het is alsnog een positief signaal. Er is

[66] https://www.vsnu.nl/2020-werkdruk-ictu.html

een goede voedingsbodem aanwezig om het privacybewustzijn en informatieveilige gedrag bij instellingen (nog verder) te verbeteren.

3. **De instellingen maken onvoldoende helder wat ze verwachten van medewerkers wat betreft privacy en security**
   Slechts een minderheid van de respondenten vindt de regels en richtlijnen voor privacybewust en informatieveilig werken van hun instelling duidelijk. De punten van kritiek: de regels en richtlijnen zijn niet bekend, niet vindbaar, onvoldoende gecommuniceerd of ze zijn zó algemeen geformuleerd dat ze in de praktijk niet bruikbaar zijn. Dit is een essentieel punt. Als een instelling niet duidelijk en concreet maakt wat ze verstaat onder privacybewust en informatieveilig werken, dan kan ze ook niet verwachten dat medewerkers veilig en zorgvuldig met vertrouwelijke gegevens omgaan. Voor medewerkers is het belangrijk dat de regels en richtlijnen concreet zijn en dat ze deze direct kunnen toepassen. Dus: welke tooling is toegestaan in welke situaties? Hoe kunnen ze grote bestanden veilig opslaan en delen? En hoe zit dat met zeer vertrouwelijke gegevens, met welke tools kunnen ze die verwerken? In welke situaties mogen gegevens van studenten, respondenten en medewerkers verzameld en gedeeld worden? Welke onderwijsondersteunende tools zijn toegestaan? Waar dient een onderzoeker in een internationaal samenwerkingsverband rekening mee te houden qua privacy en security? Welke gegevens mogen HR-medewerkers verzamelen bij langdurige ziekte van een werknemer? Maak het zo concreet mogelijk. Zoals gesteld in de eerste conclusie, is dit voor – bijvoorbeeld – onderzoekers complexer dan voor medewerkers in ondersteunende functies. Het is wellicht niet mogelijk om regels te beschrijven die alle werksituaties bevatten. Voor functiegroepen die zelfstandig navigeren in complexe situaties is het dan zinvoller om, in plaats van sets met richtlijnen op te stellen, aan te leren hoe men zelf risico's kan herkennen, gefundeerd keuzes kan maken en risico's kan mitigeren.

4. **Voor het kennisniveau over privacy en informatiebeveiliging krijgen instellingen een krappe voldoende.**
   De meting bevat acht toetsvragen. Twee ervan worden door de overgrote meerderheid van de respondenten fout beantwoord. Dit betreft het kunnen herkennen van een sterk wachtwoord (uit drie wachtwoorden) en de vraag of het nodig is om expliciete toestemming te vragen aan mensen die tijdens een open dag worden gefotografeerd voor de website. En op twee andere vragen geeft ruim een derde van de respondenten een fout antwoord. De kennis over privacy en informatiebeveiliging is dus voor verbetering vatbaar.
   Het is opmerkelijk dat de vraag over wachtwoorden het slechtst gemaakt is. Bij de vraag naar onderwerpen waar men meer kennis over nodig heeft om privacybewust en informatieveilig te kunnen werken, eindigt het onderwerp 'wachtwoorden' namelijk als laatste. Mogelijk overschatten de respondenten hun eigen kennis over dit onderwerp. Dit fenomeen, dat mensen cybersecurity-risico's onderschatten en hun eigen kennis

overschatten is ook een van de conclusies in de laatste versie van het jaarlijkse onderzoek naar het bewustzijn van Nederlanders rondom cybersecurity in opdracht van het ministerie van EZK.[7]

[7] Veilig online 2020, Ministerie van Economische Zaken en Klimaat, 1 oktober 2020
https://www.rijksoverheid.nl/documenten/rapporten/2020/09/30/veilig-online-2020

Aanbevelingen

Op basis van de resultaten en conclusies uit de metingen, komen we tot de volgende aanbevelingen.

1. **Blijf samenwerken en van elkaar leren**
   Onderwijs- en onderzoeksinstellingen werken op veel terreinen met elkaar samen. We denken dat dit (mede) de oorzaak is van de geringe verschillen tussen de instellingen op het gebied van privacy- en security-awareness. Naar aanleiding van de metingen heeft een aantal instellingen al het initiatief genomen om de resultaten onderling te bespreken om van elkaar te leren. We adviseren om dit te blijven doen. Zo kunnen de instellingen samen (nog) beter worden.

2. **Stel vast wat privacybewust en informatieveilig werken inhoudt**
   Wees duidelijk richting medewerkers wat je van hen verwacht. Stel concrete richtlijnen op en doe dit bij voorkeur in overleg met medewerkers. Verdiep je in hun werksituatie en zorg ervoor dat de richtlijnen aansluiten bij hun werksituatie. Stel indien nodig verschillende (sub)richtlijnen op voor verschillende doelgroepen. Wees realistisch: ga geen tools of activiteiten verbieden als er geen redelijke alternatieven zijn. Zorg ervoor dat het werkbaar blijft. Laat informatieveilig werken niet onnodig van medewerkers afhangen.

3. **Zorg voor heldere communicatie van de regels en richtlijnen**
   Medewerkers hebben geen behoefte aan lange documenten, ze willen liever korte en bondige richtlijnen, opgesteld in heldere taal. Stel bruikbare richtlijnen op en deel die actief met medewerkers. Zorg er ook voor dat de richtlijnen goed vindbaar zijn. Attendeer de medewerkers geregeld op de richtlijnen.
   Stel indien mogelijk ook richtlijnen voor experts op, met meer duiding en uitgebreider inhoudelijk advies.

4. **Maak een afwisselend awarenessprogramma**
   Stel een awarenessprogramma op waarbij medewerkers via verschillende kanalen en in meerdere vormen de boodschap tot zich kunnen nemen. Bijvoorbeeld quizjes, trainingen, artikelen in de nieuwsbrief, een game of een dilemma-sessie. Beperk het programma niet alleen tot digitale communicatie, maar organiseer ook ‘live’ sessies, (fysieke) trainingen of ga langs bij afdelingen.
   Probeer aan te sluiten bij bestaande gremia. Verzorg een presentatie bij het inwerkprogramma van nieuwe medewerkers, deel webcamcovers uit bij een event over informatiemanagement, verzorg een quiz bij de introductieweek van nieuwe studenten.
   Kijk naar de behoefte van de doelgroep. Professoren in de geesteswetenschap, functioneel beheerders en communicatieadviseurs hebben waarschijnlijk allemaal verschillende voorkeuren. Probeer je bij het ontwikkelen en implementeren van de awareness-interventies in te leven in de belevingswereld van de doelgroep.

5. **Geef leidinggevenden een actieve rol**
   Bied leidinggevenden een training waarin hun verantwoordelijkheden met betrekking tot privacybewust en informatieveilig werken centraal staan. Het goede voorbeeld geven, mensen aanspreken op onveilig gedrag, het onderwerp bespreekbaar maken binnen het team zijn zaken die tijdens zo'n training behandeld kunnen worden. Idealiter is privacybewust en informatieveilig werken een vast en terugkerend gespreksonderwerp tussen leidinggevende en medewerker en wordt het zo geborgd binnen de instelling.

6. **Behandel minimaal de volgende thema's**
   De richtlijnen, en ook de overige awareness-interventies, bevatten idealiter minimaal de volgende informatie:
   - hoe men zijn/haar accountgegevens kan beschermen (waaronder wachtwoorden)
   - welke ICT-tools gebruikt mogen worden, voor welke doeleinden en soorten gegevens
   - welke persoonsgegevens verzameld en vastgelegd mogen worden, onder welke voorwaarden
   - welke (persoons) gegevens gedeeld mogen worden met welke partijen, onder welke voorwaarden
   - onder welke voorwaarden en grondslagen persoonsgegevens gepubliceerd mogen worden
   - in welke situaties verwerkersovereenkomsten gesloten moeten worden en hoe men dat concreet kan doen
   - welke acties en beveiligingsmaatregelen men dient uit te voeren bij nieuwe (onderzoeks)projecten
   - hoe en waar men veilig (zeer) vertrouwelijke informatie kan opslaan en delen
   - hoe men zijn/haar thuisnetwerk kan beveiligen
   - hoe men een datalek kan herkennen en welke acties men vervolgens dient te nemen
   - wat men kan doen en met wie men kan overleggen, als het niet mogelijk is om te voldoen aan de richtlijnen

7. **Focus op medewerkers onderwijs en onderzoek**
   De meting heeft vooral medewerkers in ondersteunende processen en bij bibliotheken bereikt. De deelname van medewerkers die werken in het onderwijs- en onderzoeksproces was lager, en dat gold ook voor hun score. Het is dus zaak om in het vervolg deze medewerkers actief te betrekken bij awareness-initiatieven. Aangezien zij te maken hebben met grote werkdruk, moeten de awareness-interventies goed aansluiten bij hun dagelijkse werkzaamheden, zodat zij direct zien wat de relevantie is voor hen.

Bijlage 1 Vragenlijst CSY Awarenessmeting

maart 2021

Dit document bevat de vragenlijst zoals deze is voorgelegd aan de respondenten van de CSY Awarenessmeting. Deze meting is uitgevoerd bij 26 onderwijs- en onderzoeksinstellingen.

Introductie

Test hier hoe privacybewust en informatieveilig[8] jij werkt!
Dit onderzoek bestaat uit twee delen: 1) Jouw ervaringen en meningen en 2) Quizvragen

Aan het eind ontvang je je score plus advies om nog veiliger en privacybewuster te werken.

Succes!

Introductievraag

Welke functiecategorie is voor jou van toepassing?

- ❍ Onderwijs en onderzoek
- ❍ Bibliotheek
- ❍ Ondersteunend personeel
- ❍ Anders

[8] (met een link) Met informatieveilig en privacybewust werken bedoelen we dat je tijdens je werk:

- informatie beschermt tegen onbevoegden (informatieveilig)
- zorgvuldig omgaat met gegevens van studenten, respondenten, medewerkers of andere betrokkenen (privacybewust)

Deel 1: jouw ervaring

1. **Hoeveel aandacht besteed jij over het algemeen tijdens je werk aan privacy en informatiebeveiliging?**
   Geef een score, waarbij 1 staat voor 'helemaal geen aandacht' en 5 staat voor 'zeer veel aandacht'.

O	O	O	O	O
1	2	3	4	5

1a **Waarom besteed jij tijdens je werk (een beetje) weinig aandacht aan privacy en informatiebeveiliging?**
   Open tekstvak:

   Waar past jouw antwoord het beste bij?
   - ❍ Andere zaken vind ik belangrijker
   - ❍ Ik vind het te complex en tijdrovend
   - ❍ Ik weet niet goed wat er van me verwacht wordt
   - ❍ Ik word onvoldoende ondersteund vanuit de organisatie
   - ❍ Anders

1b Waarom besteed jij tijdens je werk (zeer) veel aandacht aan privacy en informatiebeveiliging?
   Open tekstvak:

   Waar past jouw antwoord het beste bij?
   - ❍ Ik vind het heel belangrijk
   - ❍ Het is eenvoudig en niet te tijdrovend om dit te doen
   - ❍ Het is duidelijk wat er van me verwacht wordt
   - ❍ Ik wordt goed ondersteund vanuit de organisatie
   - ❍ Iets anders

In hoeverre ben je het eens met de volgende stellingen?

2. **Ik ben bereid om extra moeite te doen om privacybewust en informatieveilig te werken.**
   Geef een score, waarbij 1 staat voor 'helemaal mee oneens en 5 staat voor 'helemaal mee eens'.

O	O	O	O	O
1	2	3	4	5

3. **De regels en richtlijnen van <instelling> voor privacybewust en informatieveilig werken. zijn duidelijk voor mij**
   Geef een score, waarbij 1 staat voor 'helemaal mee oneens en 5 staat voor 'helemaal mee eens'.

O	O	O	O	O
1	2	3	4	5

3a Waarom ben jij het (een beetje) oneens eens met deze stelling?
Open tekstvak:

Waar past jouw antwoord het beste bij?
- ❍ Ik wist niet dat er regels en richtlijnen zijn
- ❍ Ik vind de regels en richtlijnen niet helder beschreven
- ❍ Ik vind de regels en richtlijnen lastig vindbaar
- ❍ Iets anders

3b Waarom ben jij het (helemaal) eens met deze stelling?
Open tekstvak:

Waar past jouw antwoord het beste bij?
- ❍ Ik vind de regels en richtlijnen helder beschreven
- ❍ Ik vind de regels en richtlijnen goed vindbaar
- ❍ Iets anders

4. Ik word goed gefaciliteerd door <instelling> om privacybewust en informatieveilig te kunnen werken (bijvoorbeeld door tools, ICT-middelen, instructies, en andere middelen)
Geef een score, waarbij 1 staat voor 'helemaal mee oneens en 5 staat voor 'helemaal mee eens'

O	O	O	O	O
1	2	3	4	5

4a Waarom ben jij het (een beetje) oneens met deze stelling?
Open tekstvak:

Waar past jouw antwoord het beste bij?
- ❍ Ik mis goede, veilige en goed beheerde software/ICT tools
- ❍ Ik mis heldere instructies en richtlijnen
- ❍ Ik krijg geen trainingen om mijn kennis te verhogen
- ❍ Het onderwerp 'leeft' niet bij ons, komt nooit ter sprake bij collega's of leidinggevenden
- ❍ Iets anders

4b Waarom ben jij het (helemaal) eens met deze stelling?
Open tekstvak:

Waar past jouw antwoord het beste bij?
- ❍ De organisatie voorziet mij van goede, veilige en goede beheerde software/ICT tools

- De organisatie voorziet mij van heldere instructies en richtlijnen
- De organisatie voorziet mij van de juiste trainingen
- Het onderwerp 'leeft' en is onderwerp van gesprek bij collega's en mijn leidinggevende
- Iets anders

5. **Mijn leidinggevende geeft mij het juiste voorbeeld als het gaat om privacybewust en informatieveilig werken.**
   Geef een score, waarbij 1 staat voor 'helemaal mee oneens en 5 staat voor 'helemaal mee eens'

O	O	O	O	O
1	2	3	4	5

6. **Over welke onderwerpen heb jij meer kennis nodig om privacybewust en informatieveilig te kunnen werken?** *Meerdere antwoorden mogelijk*
   - Over basiskennis security
   - Over basiskennis privacy
   - Hoe ik vertrouwelijke informatie veilig kan opslaan (welke ICT middelen)
   - Hoe ik vertrouwelijke informatie veilig kan delen (welke ICT middelen)
   - Wat te doen bij een security incident of datalek
   - Over het delen van persoonsgegevens (intern of extern): wanneer toegestaan
   - Over het verzamelen persoonsgegevens: wanneer toegestaan
   - Hoe ik mijn thuisnetwerk goed kan beveiligen
   - Wanneer en hoe ik verwerkersovereenkomsten moet afsluiten
   - Hoe ik zorgvuldig wachtwoorden kan maken en beheren
   - Wat ik kan doen om phishing te voorkomen en te bestrijden
   - Wat ik kan doen om ransomware te voorkomen en te bestrijden
   - (zelf invullen)

7. **Heb jij nog opmerkingen of verbeterpunten voor <lidwoord instelling> over privacybewust en informatieveilig werken?**
   - ….

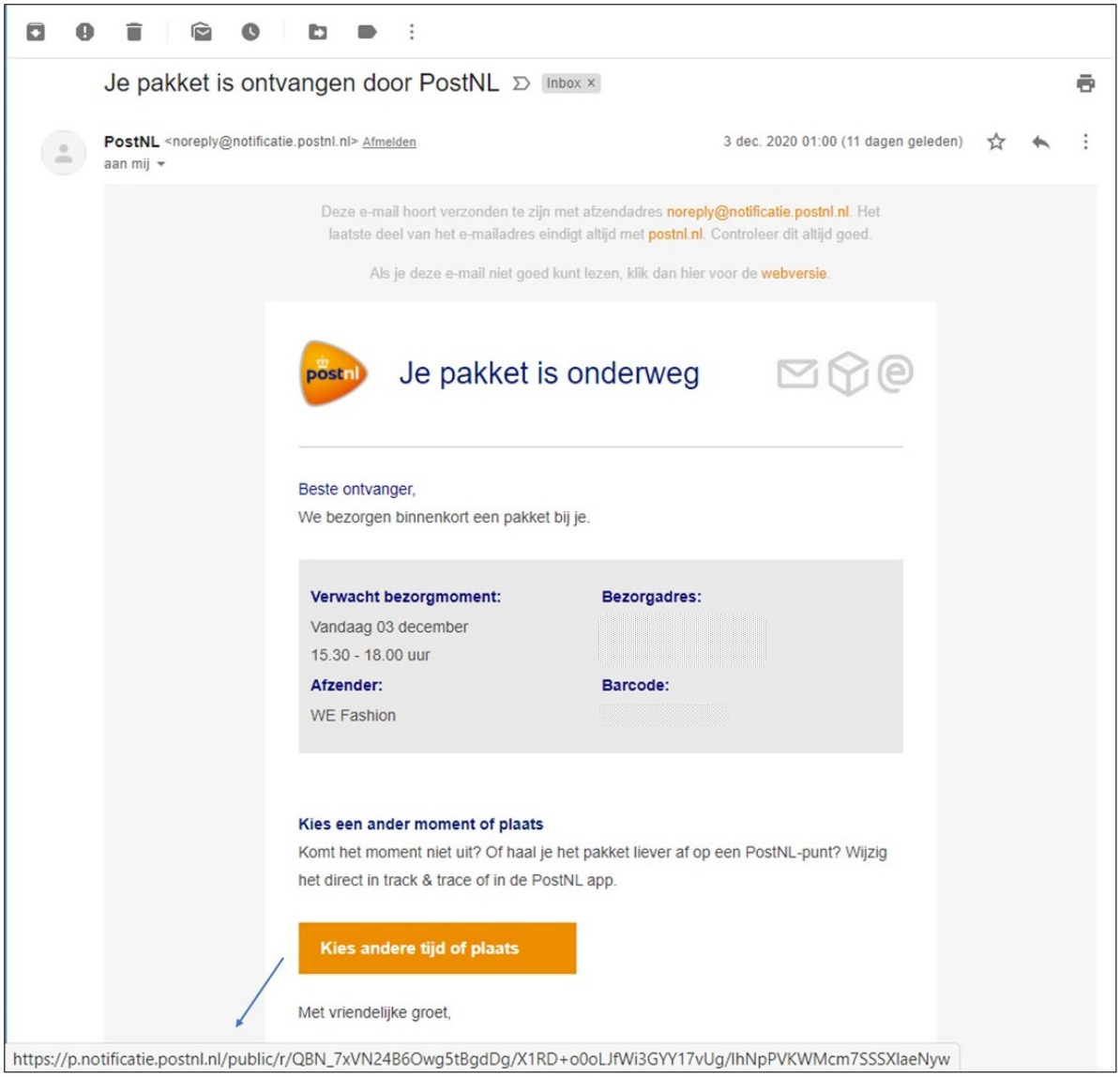
Deel 2: QUIZ

1. Bekijk deze sms-berichten. Is het onderste bericht phishing?

- ❍ Ja
- ❍ Nee

Antwoord: ja.
Het is phishing. Dit is te zien aan de url, deze verwijst naar de domeinnaam *geldovermaken.ni*, dat is geen legitieme Rabobank url. Je wordt misleid omdat eerste sms wél legitiem is. Een aanvaller kan de afzender in een sms nabootsen, dat heet spoofing.

2. Bekijk deze e-mail. Is dit phishing?



- ❍ Ja
- ❍ Nee

Antwoord: nee
Dit is geen phishing. De url en het afzendadres horen bij PostNL. Ook is de aard van de boodschap niet afwijkend voor PostNL.

3. Welke van deze wachtwoorden is het sterkst?
   - ❍ CapibaraTrampolineSchaatsen
   - ❍ *6tR2&)
   - ❍ qqwwee112233

   Antwoord: 1
   Hoe langer het wachtwoord, hoe sterker. Langere wachtwoorden zijn moeilijker te kraken. Het aantal verschillende soorten tekens is van minder groot belang.

4. De jaarcijfers van de instelling lekken voortijdig uit. Is dit een datalek?
   - ❍ Ja
   - ❍ Nee
   - ❍

   Antwoord: nee
   Dit is geen datalek, maar wel een security incident.

   - Een security incident is een situatie waarin (vertrouwelijke) informatie foutief is aangepast, niet beschikbaar is, of beschikbaar is voor ongeautoriseerde personen.
   - Een datalek is een security incident waarbij persoonsgegevens betrokken zijn (denk aan foto's, adresgegevens, medische gegevens, gegevens over personeel).

   Jaarcijfers zijn wel vertrouwelijke gegevens, maar geen persoonsgegevens. Er is dus wel sprake van een security incident, maar geen datalek.

5. Bij een open dag van de instelling worden foto’s gemaakt voor op de website. Is het nodig om aan iedereen die op de foto’s staat, expliciete toestemming te vragen?
   - ❍ Ja
   - ❍ Nee

   Antwoord: nee
   Het is niet nodig om toestemming aan iedereen te vragen. Je kunt je bij het maken van sfeerbeelden op evenementen beroepen op de 'journalistieke exceptie' of jouw 'gerechtvaardigd belang'. Wel dien je maatregelen te treffen om de privacy van de aanwezigen te waarborgen.

   - Kondig op tijd aan, bijvoorbeeld bij inschrijving voor het evenement, dat er een fotograaf aanwezig zal zijn
   - Geef aanwezigen de mogelijkheid om niet gefotografeerd te worden
   - Houd rekening met het type evenement en de doelgroep. Als het kwetsbare mensen betreft, of er zijn bijzondere persoonsgegevens uit af te leiden (zoals een bijeenkomst voor een politieke partij of patiëntenvereniging), 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.

6. Waarom is het belangrijk om je ICT-systemen en programma's geregeld te updaten?
   - ❍ Omdat je dan altijd de laatste versie van je documenten hebt
   - ❍ De systemen bevatten dan minder kwetsbaarheden en daardoor heeft een eventuele hackaanval minder kans van slagen
   - ❍ Omdat de netwerkverbinding dan beveiligd is en kwaadwillenden geen toegang kunnen krijgen tot jouw data

   Antwoord: B
   Door te updaten, zorg je ervoor dat je systemen en programma's de nieuwste versie software hebben draaien. In oudere versies zitten kwetsbaarheden waarmee kwaadwillenden makkelijker toegang kunnen krijgen tot jouw systemen. De updates zorgen ervoor dat die kwetsbaarheden worden gedicht.

7. Wat is het voordeel van MFA (Multi Factor Authenticatie)?
   - ❍ Je hoeft je wachtwoorden niet meer te onthouden
   - ❍ Je netwerkverbinding is extra beveiligd
   - ❍ Je account is beter beschermd tegen aanvallers

   Antwoord: C
   MFA voegt een extra beveiligingslaag toe bovenop de gebruikersnaam en het wachtwoord. Dit kan een sms-code, een vingerafdruk of een tokengenerator zijn. Daarmee is je account beter beschermd tegen aanvallers. Want stel je hebt MFA en een aanvaller heeft jouw gebruikersnaam en wachtwoord in handen, bijvoorbeeld via phishing. Dan is de aanval nog niet succesvol want de aanvaller moet ook toegang hebben tot de extra beveiligingsmaatregel.

8. Je verliest een laptop met gegevens van respondenten van een vertrouwelijk onderzoek. Een datalek! Wat doe je als eerst?
   a. Dit melden bij de Autoriteit Persoonsgegevens
   b. Een mailtje naar de respondenten sturen met je excuus
   c. Dit melden bij de ICT helpdesk

   Antwoord: C
   Je dient de procedure datalekken in de juiste volgorde te doorlopen:

   - Interne melding (bij ICT helpdesk, privacy officer of Functionaris Gegevensbescherming, afhankelijk van het proces datalekken in jouw instelling
   - In het geval van een datalek met risico's voor betrokkenen (de respondenten): verplichte melding bij de Autoriteit Persoonsgegevens. Hierover besluit de directie/ het CvB.
   - Indien de risico's voor betrokkenen ernstig zijn: melding aan betrokkenen.

Als je direct de betrokkenen informeert, sla je een aantal cruciale stappen over. Stel dat in die situatie een van de betrokkenen naar de pers stapt. Of dat het datalek gerelateerd is aan andere incidenten, dan haal je je mogelijk veel extra problemen op je hals. Je kunt de verantwoordelijkheid voor een externe melding beter laten waar die formeel ligt: bij de FG en directie.

Individuele terugkoppeling:

4-8 vragen fout: Helaas, onvoldoende!

Oh nee, je hebt minimaal de helft van de vragen fout beantwoord! Je weet onvoldoende hoe je informatieveilig en privacybewust werkt. Dat maakt jou -en [naam instelling]!- heel kwetsbaar voor cybersecurity incidenten en datalekken.

Om je weerbaarheid te verhogen, raden we aan om de Cybersave Yourself- adviezen[9] van SURF te lezen.

Hartelijk dank voor je deelname. Met jouw input kan je instelling gericht (verder) werken aan privacy en security awareness.

2-3 vragen fout: Gaat de goede kant op!

Je bent aardig bezig! Je hebt de meeste vragen goed beantwoord. Je weet redelijk goed hoe je informatieveilig en privacybewust moet werken.

Maar een aanvaller hoeft maar één kwetsbaarheid te ontdekken om een slag te slaan, dus we raden je aan om de Cybersave Yourself- adviezen van SURF te lezen.

[9] https://cybersaveyourself.nl/tips/

Hartelijk dank voor je deelname. Met jouw input kan je instelling gericht (verder) werken aan privacy en security awareness.

0-1 vragen fout: Fantastisch!

Je hebt (bijna) alle vragen goed beantwoord! Je weet precies hoe je informatieveilig en privacybewust moet werken.

Mocht je toch nog meer kennis willen opdoen, lees dan de Cybersave Yourself- adviezen van SURF.

Hartelijk dank voor je deelname. Met jouw input kan je instelling gericht (verder) werken aan privacy en security awareness.