Trendrapport 2024

De mens, risico of sterkste troef?

Ontwikkelingen en patronen in beeld

AWARE WAYS

De kracht van mensen in een digitale wereld.

Van tech naar talent.

Nu, maar nog meer naar de toekomst toe is de **weerbaarheid** van organisaties en hun medewerkers van cruciaal belang in de wereld van informatieveiligheid en privacy. Weerbaarheid is de mate van aanpassingsvermogen van een organisatie of medewerker ten opzichte van een bedreiging (Hollnagel et al., 2015). Deze weerbaarheid vormt de ruggengraat van een veilige en veerkrachtige samenleving.

Hoewel technische oplossingen belangrijk blijven, is het gedrag van medewerkers een onmisbare schakel in het versterken van de weerbaarheid rondom informatieveiligheid en privacy. Medewerkers spelen immers een sleutelrol in het herkennen en voorkomen van incidenten en in het reageren op dreigingen. Met het veranderende dreigingslandschap (waaronder toenemende activiteit van statelijke actoren (AIV, 2024), veranderende wet en regelgeving (AVG, NIS2 en Dora) en de digitale transformatie van de samenleving (digitalisering, AI en hybride werken), is het versterken van de menselijke weerbaarheid urgenter dan ooit.

AWAREWAYS

Ontdek waar medewerkers excelleren en waar ze versterking nodig hebben.

Het doel van dit trendrapport van Awareways is om expliciet de menselijke factor centraal te stellen in de analyse van trends en ontwikkelingen. Door trends te onderzoeken en psychologische inzichten uit diverse jaren samen te brengen, biedt dit rapport een helder en praktisch overzicht van de vaardigheden waarin medewerkers excelleren én de gebieden waar zij nog uitdagingen ervaren. Dit rapport is bedoeld om organisaties te helpen begrijpen hoe zij het potentieel van hun medewerkers kunnen versterken en gerichte verbeteringen kunnen aanbrengen.

Een essentieel rapport voor professionals in security en privacy.

Dit trendrapport is een absolute must-read voor professionals die de weerbaarheid van hun organisatie willen versterken in een steeds complexer wordend landschap van informatieveiligheid en privacy. Ben jij verantwoordelijk voor security, privacy, talentontwikkeling, compliance, of bijvoorbeeld digitale transformatie? Werk je aan strategische vraagstukken rondom risicobeheer, gedrags- en cultuurverandering, en het trainen van medewerkers? Of ben je simpelweg op zoek naar concrete handvatten om je organisatie veiliger en veerkrachtiger te maken? Dan is dit rapport voor jou.

“Menselijke weerbaarheid is geen kwestie van risico’s vermijden, maar van kracht versterken.”

Awareways,
Sjoerd van Veldhuizen
MSc, Sociaal Psycholoog

Samenvatting

Dit trendrapport toont duidelijke ontwikkelingen in de menselijke weerbaarheid op het gebied van informatieveiligheid en privacy, gebaseerd op de antwoorden uit startmetingen van 28.215 medewerkers uit 32 organisaties tussen 2022-2024. De startmetingen laten zien hoe de initiële cultuur rond informatieveiligheid en privacy over organisaties in de tijd is veranderd.

Het onderzoeksmodel, Theory of Planned Behavior, stelt dat intenties je gedrag vormen. Deze intenties worden weer gevormd door: de sociale normen om je heen, je eigen attitude tegenover bepaald gedrag, en de controle die je over je eigen gedrag ervaart. Per construct zien we verschillende trends:

- **Gedrag**: Het gedrag rondom veilig omgaan met informatie laat een stabiel beeld zien sinds 2022.
- **Intentie**: De intentie om veilig te werken met informatie die medewerkers rapporteren laat sinds 2022 een licht toenemende trend zien.
- **Sociale norm**: Sinds 2022 zien we dat de sociale norm is toegenomen ten aanzien van verschillende informatieveiligheid en privacy thema's.
- **Attitude**: Bij de attitude zien we dat medewerkers veilig werken met informatie consistent belangrijk vinden sinds 2022.
- **Ervaren controle**: Sinds 2022 geloven medewerkers consistent dat ze in staat zijn om veilig te werken met informatie.
- **Kennis**: Op het gebied van kennis is een toename te zien sinds 2022 op de meeste informatieveiligheid en privacy thema's.
- **Gelegenheid**: Sinds 2022 wisselt het voor medewerkers hoe gemakkelijk of moeilijk ze veilig met informatie kunnen werken.

Algemene bevindingen

Hoewel we op veel gebieden mooie vooruitgang zien, zijn er ook een aantal zorgpunten. Zo lijkt er een groeiend gevoel van 'wachtwoordmoeheid', afnemende aandacht en kennis over veilig thuiswerken, en een verslechterende naleving van de AVG-richtlijnen. Deze trends weerspiegelen de uitdagingen van digitalisering, de versnelde adoptie van nieuwe technologieën, en de toenemende complexiteit van wet- en regelgeving in het kader van informatieveiligheid en privacy.

Focus op resilience

Er is een groeiende focus op de mens als risicofactor: human risk. Bij Awareways geloven we echter dat juist het versterken van menselijke weerbaarheid een krachtige bijdrage levert aan effectieve informatieveiligheid en privacy. Een robuuste weerbaarheidscultuur is daarbij onmisbaar en vraagt om continue aandacht, kennis en flexibiliteit in een snel veranderende digitale wereld.

Dit rapport biedt inzichten en kansen om deze menselijke weerbaarheid verder te versterken.

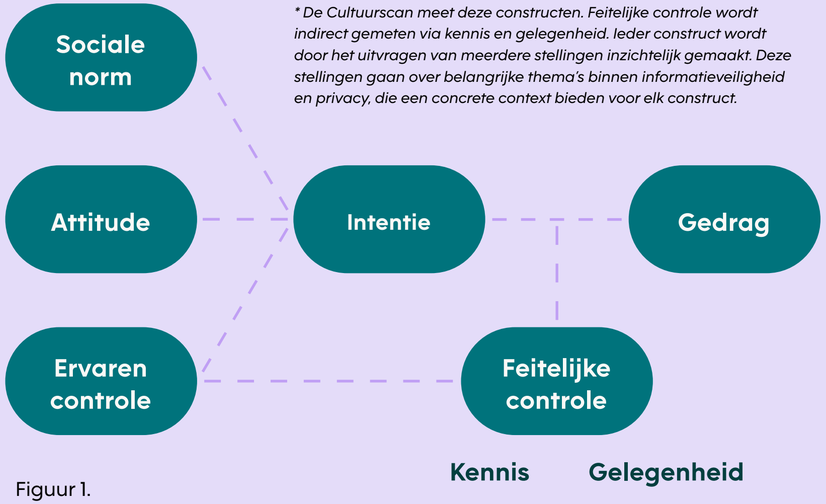
Over de Cultuurscan

De Cultuurscan is een vragenlijst die verschillende onderdelen van informatieveiligheid en privacy meet. Deze onderdelen, ook wel psychologische constructen genoemd, zijn gebaseerd op het bekende psychologische 'Theory of Planned Behavior' model (Ajzen & Schmidt, 2020).

Op basis van alle startmetingen, de eerste meting die gedaan wordt bij de klanten van Awareways voor aanvang van een Security Awareness programma, is een groot trendonderzoek uitgevoerd om belangrijke inzichten te vinden. In dit onderzoek zijn de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties bekeken over de periode 2022-2024. Deze antwoorden zijn anoniem verzameld en verwerkt, zodat de privacy van de medewerkers en organisaties beschermd is.

Onderzoeksmodel: Theory of Planned Behavior

Het Theory of Planned Behavior model is gericht op het voorspellen en begrijpen van menselijk gedrag en biedt inzichten in cognitieve en sociale factoren die menselijk gedrag sturen. Het model stelt dat intenties je gedrag vormen. Deze intenties worden weer gevormd door: de sociale normen om je heen, je eigen attitude tegenover bepaald gedrag, en de controle die je over je eigen gedrag ervaart.



** De Cultuurscan meet deze constructen. Feitelijke controle wordt indirect gemeten via kennis en gelegenheid. Ieder construct wordt door het uitvragen van meerdere stellingen inzichtelijk gemaakt. Deze stellingen gaan over belangrijke thema's binnen informatieveiligheid en privacy, die een concrete context bieden voor elk construct.*

Figuur 1.

AWAREWAYS

Ter illustratie een voorbeeld over sporten:

- **Intentie**: Je bent van plan om vaak te sporten. Dit wordt beïnvloed door:
  - **Sociale norm**: Je vrienden gaan vaak naar de sportschool, dus is de kans groter dat jij ook wilt gaan.
  - **Attitude**: Je vindt het belangrijk om fit te zijn, dus is de kans groter dat je vaker wilt gaan sporten.
  - **Ervaren controle**: Je gelooft goed te zijn in sporten, dus is de kans groter dat je dit wilt gaan doen.

Een intentie is echter niet alles. Of intenties ook echt tot gedrag leiden, wordt ook sterk beïnvloed door je feitelijke controle over het gedrag. De feitelijke controle verwijst naar de middelen die je nodig hebt om bepaald gedrag te vertonen. Deze middelen kunnen intern zijn voor de persoon, zoals kennis, vaardigheden of intelligentie, of extern voor de persoon, zoals de juiste faciliteiten en genoeg tijd (gelegenheid). Bijvoorbeeld:

- **Feitelijke controle**: Je kan vaak sporten. Dit bestaat uit:
  - **Kennis** (intern): Je kijkt veel filmpjes over sporten, dus je weet welke oefeningen je in de sportschool kunt doen.
  - **Gelegenheid** (extern): Er is een sportschool op 5 minuten lopen, dus is het makkelijk om vaak te sporten.

Als deze constructen allemaal in hoge mate aanwezig zijn, dan is de kans groter dat je vaak in de sportschool te vinden zal zijn.

Onderzoeksthema's

Binnen de cultuurscan maken we gebruik van zeven thema's die gezamenlijk inzicht bieden in de constructen rondom informatieveiligheid en privacy.

AVG	AVG richt zich op de kennis van medewerkers over de AVG-richtlijnen en hun verantwoordelijkheid bij het verwerken van persoonsgegevens.
E-mailen	E-mailen gaat over veilig e-mailgebruik en bewustzijn van de risico's, zoals het per ongeluk verzenden van gevoelige informatie naar een verkeerd adres.
Incidenten melden	Het melden van incidenten beslaat de motivatie en het vermogen van medewerkers om incidenten te melden als er iets misgaat bij het werken met informatie.
Phishing	Phishing onderzoekt of medewerkers phishing kunnen herkennen en of ze weten welke stappen er genomen moeten worden wanneer ze vermoeden dat ze met phishing te maken hebben.
Regels	Het regels thema omschrijft in hoeverre medewerkers op de hoogte zijn van de regels die gelden binnen een organisatie voor informatieveiligheid en privacy en of ze deze ook toepassen.
Thuiswerken	Thuiswerken beschrijft of medewerkers veilig willen en kunnen werken met informatie op afstand, meestal vanuit huis.
Wachtwoorden	Wachtwoorden gaat in op de werkwijzen rondom wachtwoordbeheer en hoe medewerkers hiermee omgaan.

7-punts Likert Schaal

De Cultuurscan maakt gebruik van 7-punts Likert-schalen. Deelnemers geven aan in hoeverre zij het met de stellingen eens zijn. Hierbij staat 1 voor "Helemaal mee oneens", 4 voor "Neutraal" en 7 voor "Helemaal mee eens".

Onderzoeksvragen

In dit rapport is er gekeken naar hoe de constructen, de thema's en de individuele vragen zich in de loop van de tijd hebben ontwikkeld. Er wordt ingegaan op vragen als "Hoe goed passen medewerkers de AVG-richtlijnen toe sinds 2022", "Hoe verandert de aandacht en kennis ten opzichte van thuiswerken?" en "Hoe verandert de houding van medewerkers ten opzichte van wachtwoorden?".

Inzicht in constructen

Ontwikkelingen en patronen in beeld.

Sinds 2012 werkt Awareways aan het versterken van de menselijke weerbaarheid in organisaties, variërend van lokale gemeenten tot wereldwijde commerciële spelers. Wat ons uniek maakt, is de combinatie van ons multidisciplinaire team, onze innovatieve aanpak, en een schat aan ervaring die we in meer dan een decennium hebben opgebouwd.
Met diensten zoals onze beproefde Cultuurscan vragenlijst, phishing-simulaties, communicatiecampagnes en ons gamified leerplatform, helpen we organisaties niet alleen om medewerkers bewuster en veerkrachtiger te maken, maar verzamelen we ook waardevolle inzichten. Deze gegevens geven ons een helder beeld van de sterke punten en groeimogelijkheden binnen organisaties. Voor dit trendrapport hebben we ons gericht op anonieme data uit onze Cultuurscan vragenlijst. Door inzichten vanuit deze data te analyseren, hebben we trends in menselijke weerbaarheid geïdentificeerd en nieuwe kansen ontdekt.

In de volgende hoofdstukken nemen we je mee in onze interpretatie van de ontwikkeling van elk construct over tijd. Voor elk construct volgen we een vaste opbouw: eerst schetsen we de algemene ontwikkeling, waarna we inzoomen op specifieke vragen of een opvallend patroon.

Om deze ontwikkelingen te visualiseren, hebben we per construct drie zorgvuldig geselecteerde grafieken opgenomen. Elke grafiek laat de antwoorden over de jaren zien op de gepresenteerde stelling met een 95%-betrouwbaarheidsinterval. Deze grafieken illustreren trends en ondersteunen de interpretaties die in de tekst worden gepresenteerd. Samen bieden de tekst en grafieken een samenhangend beeld van de veranderingen en de onderliggende factoren die deze bewegingen verklaren.

Gedrag laat zien hoe vaak medewerkers zeggen veilig te werken met informatie.

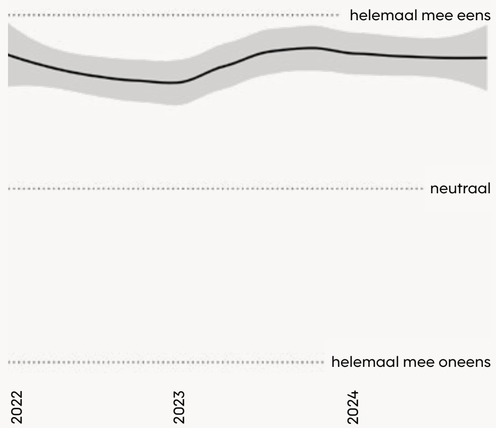
Het gedrag rondom veilig omgaan met informatie laat een consistent en stabiel beeld zien sinds 2022.

In het gedrag van medewerkers is voor de meeste thema's een stabiel beeld te zien sinds 2022. Dit is terug te zien in een aantal concrete gedragingen die van grote invloed zijn op informatieveiligheid en privacy. Eén van deze concrete gedragingen is de mate waarin medewerkers aangeven de **regels te volgen** voor veilig omgaan met informatie. Hierin zien we dat dit gedrag afnam bij medewerkers tot aan 2023, maar vervolgens weer is toegenomen en sindsdien stabiel is (Figuur 2). Daarnaast geven medewerkers over de jaren consistent aan **op te letten** voordat ze op **links klikken** (Figuur 3).

AWARE WAYS

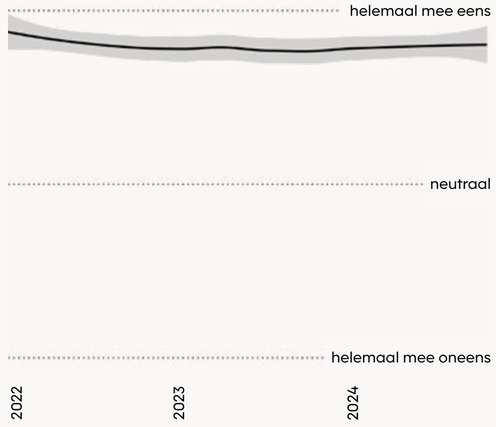
Figuur 2.

"Ik volg de regels voor het veilig werken met informatie tijdens mijn werk."



Figuur 3.

"Ik let goed op voordat ik klik op een link in een bericht."



Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

Afnemende aandacht voor AVG: Van prioriteit naar achtergrond?

Een opvallende verandering is te zien binnen het thema **AVG.** De mate waarin medewerkers persoonsgegevens volgens de AVG-richtlijnen bewaren **daalt** over de jaren (Figuur 4). Dit figuur past in een groter beeld wat Awareways ziet, waarin het toepassen van de AVG-richtlijnen naar de achtergrond lijkt te verdwijnen. Een mogelijke verklaring ligt in de afgenomen aandacht binnen organisaties voor de AVG. Na het invoeren van de AVG in 2018, was de aandacht voor implementatie en adoptie van de nieuwe regels binnen organisaties hoog. Nu de meeste organisaties de AVG geïntegreerd hebben in hun standaard werkprocessen, lijkt de aandacht binnen organisaties afgenomen. Daarnaast is er met de komst van nieuwe wetgeving 'concurrentie' voor de AVG. Wetgeving zoals de NIS2 en Dora zijn een actueler gespreksonderwerp voor beleid en regelgeving. Dit kan bijdragen aan een verminderde aandacht voor de correcte opvolging van de AVG bij medewerkers, wat leidt tot de uitdoving van eerder aangeleerd gedrag.

AWAREWAYS

Figuur 4.

"Ik bewaar persoonsgegevens volgens de AVG (privacyrichtlijnen)."

Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

Gedrag | Intentie | Sociale norm | Attitude | Ervaren controle | Kennis | Gelegenheid

Intentie laat zien in welke mate medewerkers van plan zijn om veilig te werken met informatie.

De intentie om veilig te werken met informatie die medewerkers rapporteren laat sinds 2022 een licht toenemende trend zien.

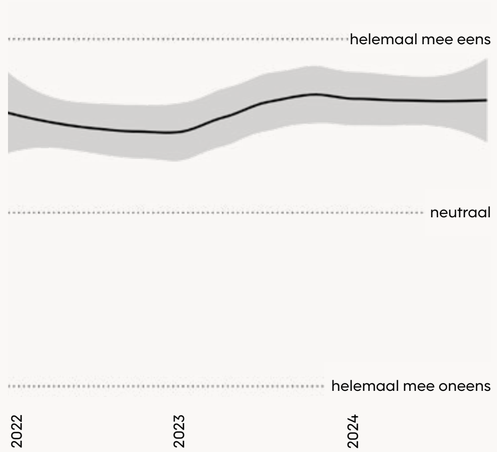
In de intentie van medewerkers om veilig te werken met informatie is voor de meeste thema's een lichte toename te zien sinds 2022. Dit wordt duidelijk aan de hand van enkele concrete intenties die van belang zijn op informatieveiligheid en privacy. Een dergelijke concrete intentie is de mate waarin medewerkers van plan zijn om **collega's aan te moedigen** om **verdachte situaties te melden**, wat licht is toegenomen (Figuur 5). Hetzelfde geldt voor de intentie om **meer te leren** over informatieveiligheid (Figuur 6). Medewerkers staan dus steeds meer welwillend tegenover informatieveiligheid en dit samen oppakken met hun collega's.

Gedrag | **Intentie** | Sociale norm | Attitude | Ervaren controle | Kennis | Gelegenheid

AWARE WAYS

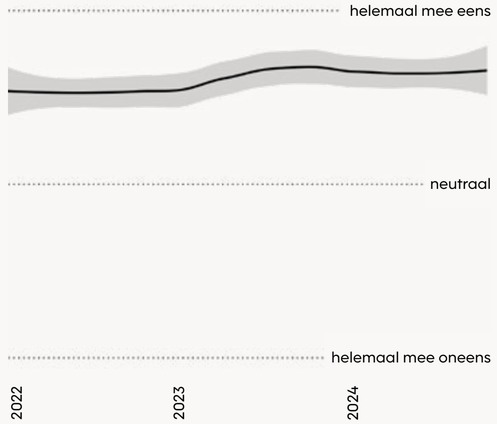
Figuur 5.

"Als collega's twijfelen over een verdachte situatie, dan moedig ik ze aan hier melding van te maken."



Figuur 6.

"Als ik meer kan leren over veilig werken met informatie, dan wil ik dat doen."



Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

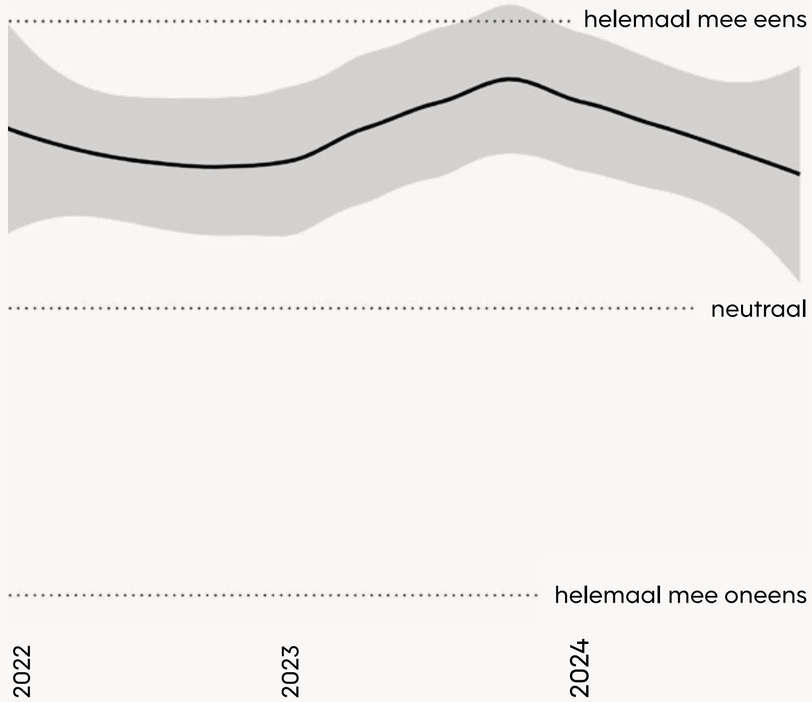
Zijn we massaal wachtwoordmoe?

Wachtwoorden is een thema waar een grote verandering te zien is. De mate waarin medewerkers van plan zijn om unieke en sterke wachtwoorden te maken is gestegen tot eind 2023, maar laat sindsdien een **daling** zien (Figuur 7). Dit patroon zien we ook terug bij de attitude ten opzichte van wachtwoorden. Deze afname is in lijn met het gevoel van 'wachtwoordmoeheid' wat Awareways steeds vaker terugziet in organisaties.

Een mogelijke verklaring is de toegenomen vraag van organisaties aan hun medewerkers rondom preventieve toegangsmaatregelen. Zo ziet Awareways dat wachtwoordbeleid steeds intensiever wordt, authenticatieprocessen steeds complexer worden en de hoeveelheid wachtwoorden die onthouden moet worden alleen maar toeneemt. Deze veeleisende en cognitief belastende taak werkt **demotiverend** voor medewerkers.

Figuur 7.

"Als ik een nieuw wachtwoord moet bedenken, dan zorg ik dat dit uniek, sterk en goed te onthouden is."



Gedrag | **Intentie** | Sociale norm | Attitude | Ervaren controle | Kennis | Gelegenheid

Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

Sociale norm laat zien in hoeverre medewerkers ervaren dat anderen, zoals collega's of leidinggevenden, bezig zijn met informatieveiligheid en privacy.

Sinds 2022 zien we dat de sociale norm is toegenomen ten aanzien van verschillende informatieveiligheid en privacy thema's.

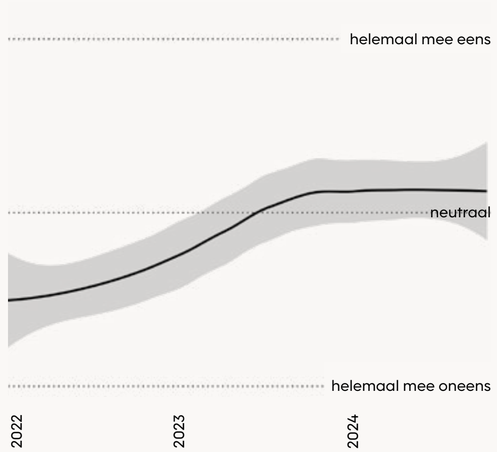
De sociale norm die medewerkers ervaren rondom informatieveiligheid en privacy is op alle thema's toegenomen sinds 2022. Een aantal specifieke normen, die van belang zijn voor informatieveiligheid en privacy, laten dit goed zien. Een van deze belangrijke normen, de **risico's van phishing**, wordt **steeds meer benadrukt door leidinggevenden** (Figuur 8). Ook het snel melden van incidenten krijgt steeds **meer aandacht** door **leidinggevenden en management** (Figuur 9 en 10). De aandacht op deze thema's werd in 2022 door de meeste medewerkers nog niet of nauwelijks ervaren, maar lijkt te zijn toegenomen tot eind 2023, waarna deze toename is afgevlakt.

Gedrag | Intentie | **Sociale norm** | Attitude | Ervaren controle | Kennis | Gelegenheid

AWARE WAYS

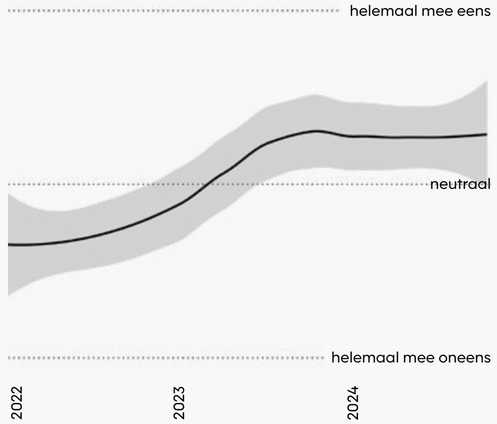
Figuur 8.

"Mijn leidinggevende benadrukt regelmatig het risico van phishing."



Figuur 9.

"Mijn leidinggevende benadrukt regelmatig het belang van het snel melden van (mogelijke) informatiebeveiligings-incidenten."



Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

Heeft de thuiswerken-trend de sociale norm beïnvloed?

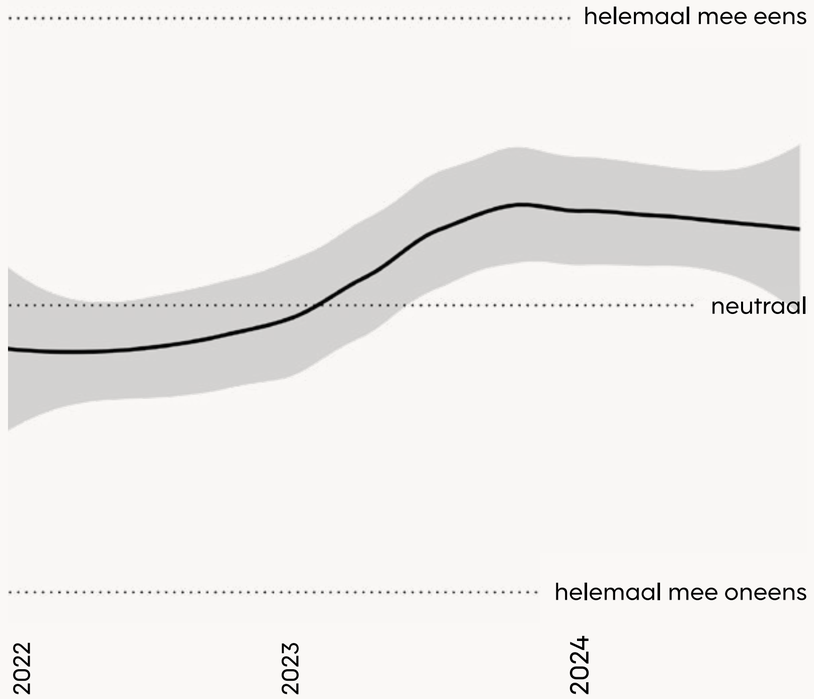
Zoals te zien in de trends, is de aandacht voor de thema's afgevlakt en sinds eind 2023 stabiel gebleven. Waar medewerkers in 2022 nog vonden dat leidinggevenden en het management deze thema's niet of nauwelijks benadrukten, neigen de meeste medewerkers het nu eens te zijn met dat deze sociale normen worden benadrukt. Dit valt mogelijk te verklaren door de toename van **thuiswerken** als gevolg van de COVID-pandemie. Toen het thuiswerken de norm werd, zijn de bijkomende uitdagingen serieus aangepakt in organisaties, ook vanuit leidinggevenden en management. Dit heeft geleid tot een omslagpunt in de norm die medewerkers ervaren rondom de aandacht voor de risico's en de regels die komen kijken bij thuiswerken. Deze toegenomen aandacht is sinds een jaar echter afgevlakt, wat ook samen lijkt te hangen met de verdere terugloop van thuiswerken in Nederland (CBS, 2024).

Gedrag | Intentie | **Sociale norm** | Attitude | Ervaren controle | Kennis | Gelegenheid

AWARE WAYS

Figuur 10.

"Het management benadrukt regelmatig het belang van het snel melden van (mogelijke) informatiebeveiligingsincidenten."



Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

Attitude laat zien hoe belangrijk medewerkers informatieveiligheid en privacy vinden.

Bij de attitude zien we dat medewerkers veilig werken met informatie consistent **belangrijk vinden sinds 2022.**

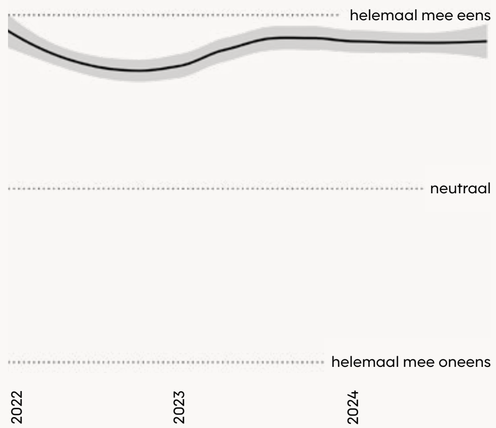
De attitude van medewerkers tegenover de meeste informatieveiligheid en privacy thema's laat een stabiel beeld zien sinds 2023, na een eerdere dip in 2022. Een paar houdingen die kenmerkend zijn voor informatieveiligheid en privacy, illustreren dit beeld het best. Zo vinden medewerkers het **direct melden** van onveilige situaties bij het werken met informatie sinds 2023 consistent **erg belangrijk** (Figuur 11). Ook zeggen medewerkers consistent sinds 2023 dat **informatieveiligheid een prioriteit moet zijn** in hun organisatie (Figuur 12). Voor de meeste medewerkers is het belang van veilig omgaan met informatie dus een duidelijk gegeven.

Gedrag | Intentie | Sociale norm | **Attitude** | Ervaren controle | Kennis | Gelegenheid

AWARE WAYS

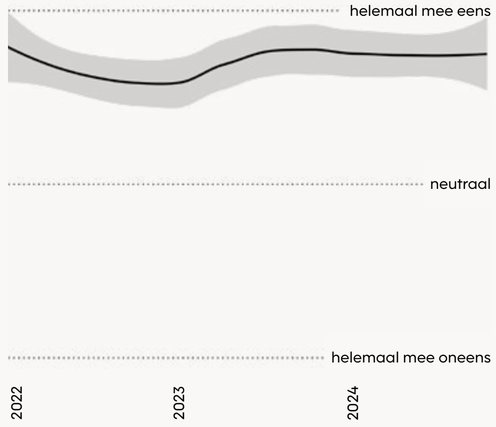
Figuur 11.

"Het direct melden van onveilige situaties met betrekking tot informatie is erg belangrijk."



Figuur 12.

"Ik vind dat informatieveiligheid een prioriteit moet zijn binnen mijn organisatie."



Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

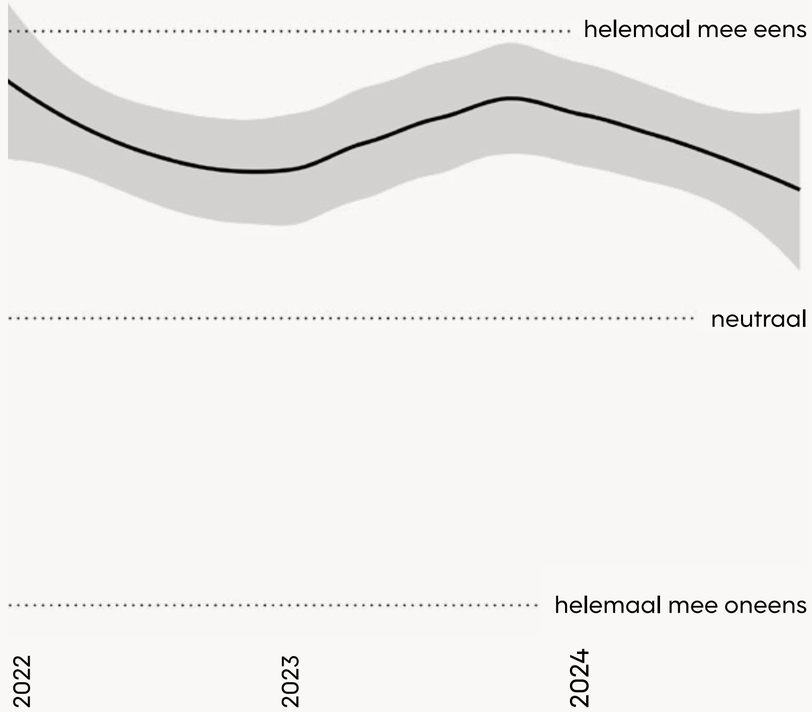
Preventieve toegangs-maatregelen: Mogelijke druk die wachtwoord-moeheid bevordert.

Er is een ander beeld te zien bij één thema: wachtwoorden. Hoe belangrijk medewerkers het vinden om unieke en sterke wachtwoorden te maken is gestegen tot het einde van 2023, maar **daalt** sindsdien (Figuur 13). Dit is hetzelfde patroon dat we terugzien bij de intentie om goed met wachtwoorden om te gaan. Ook dit is in lijn met het gevoel van 'wachtwoordmoeheid' wat Awareways steeds vaker terugziet in organisaties. Ook voor attitude is de toegenomen vraag van organisaties aan hun medewerkers rondom preventieve toegangsmaatregelen een mogelijke verklaring. Zoals bij intentie besproken wordt wachtwoordbeleid steeds intensiever, authenticatieprocessen worden steeds complexer en de hoeveelheid wachtwoorden die onthouden moet worden neemt alleen maar toe. Deze veeleisende en cognitief belastende taak werkt demotiverend en frustrerend voor medewerkers. Dit kan ertoe leiden dat medewerkers het ook **minder belangrijk** gaan vinden om hun wachtwoorden zelf goed te regelen.

Gedrag | Intentie | Sociale norm | **Attitude** | Ervaren controle | Kennis | Gelegenheid

Figuur 13.

"Ik vind het belangrijk om mijn best te doen bij het bedenken van een uniek en sterk wachtwoord."



Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

Ervaren controle laat zien in hoeverre medewerkers geloven dat ze goed in staat zijn om veilig te werken met informatie en dat ze invloed hebben op de informatieveiligheid en privacy in hun organisatie.

Sinds 2022 geloven medewerkers consistent dat ze in staat zijn om veilig te werken met informatie.

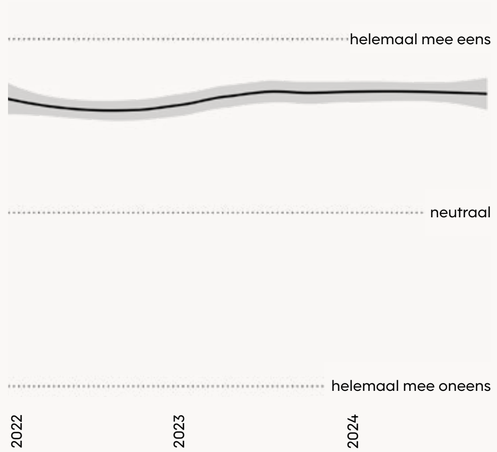
De controle die medewerkers ervaren in het veilig omgaan met informatie laat voor de meeste thema's een stabiel beeld zien sinds 2022. Een paar kenmerkende stellingen tonen dit duidelijk. Bijvoorbeeld als het gaat om het kunnen herkennen van een phishingbericht, waar medewerkers consistent van **aangeven dit te kunnen** (Figuur 14). Ook zien medewerkers consistent in dat **hun acties invloed hebben** op de informatieveiligheid van hun organisatie. Dit inzicht begint zelfs licht toe te nemen (Figuur 15). Het omzetten van deze inzichten naar dagelijks gedrag gebeurt niet altijd, omdat medewerkers hiervoor ook de feitelijke controle (kennis en gelegenheid) nodig hebben.

Gedrag | Intentie | Sociale norm | Attitude | **Ervaren controle** | Kennis | Gelegenheid

AWARE WAYS

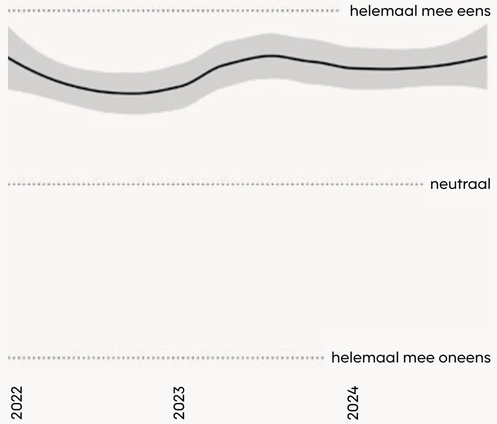
Figuur 14.

"Ik ben in staat om een phishingbericht te herkennen."



Figuur 15.

"Mijn gedrag heeft invloed op de informatieveiligheid binnen mijn organisatie."



Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

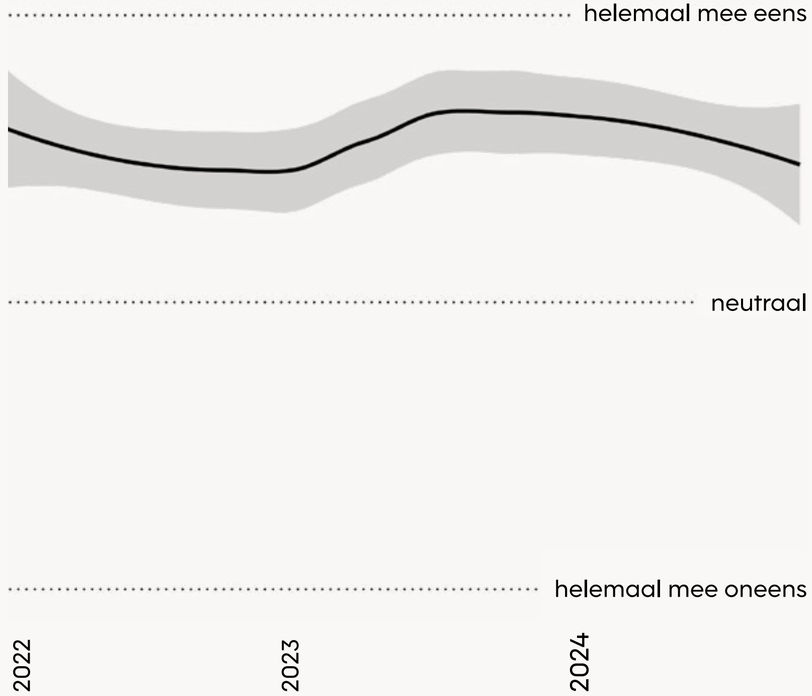
Kunnen we classificeren binnen classificatie?

Medewerkers laten een andere ervaring zien bij het herkennen van **gevoelige informatie.** Na een korte toename sinds 2022, hebben medewerkers vanaf het einde van 2023 het idee dat ze steeds **minder** goed in staat zijn om gevoelige, geheime of vertrouwelijke informatie te herkennen (Figuur 16). Deze afname kan samenhangen met de trend waarin persoonsgegevens steeds lastiger worden gevonden om te herkennen. Nu de aandacht binnen organisaties voor de **AVG** steeds meer afneemt, vinden medewerkers het lastiger om persoonsgegevens, maar ook andere soorten informatie te onderscheiden. Ook bij gevoelige informatie voelen medewerkers zich vervolgens **minder** in staat om dit te kunnen herkennen.

AWARE WAYS

Figuur 16.

“Ik kan goed herkennen welke informatie gevoelig/geheim/vertrouwelijk is.”



Gedrag | Intentie | Sociale norm | Attitude | **Ervaren controle** | Kennis | Gelegenheid

Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

Gedrag laat zien hoe vaak medewerkers zeggen veilig te werken met informatie.

Op het gebied van kennis is een toename te zien sinds 2022 op de meeste informatieveiligheid en privacy thema's.

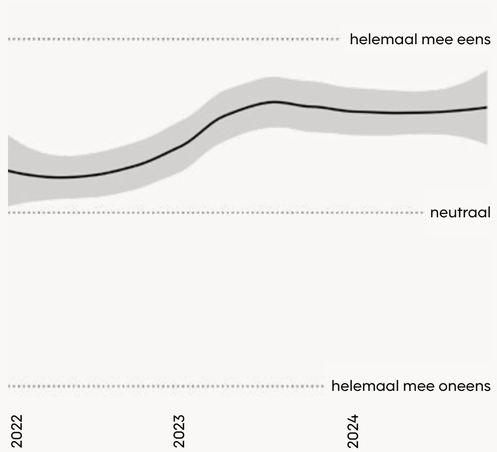
De kennis die medewerkers hebben over de meeste informatieveiligheid en privacy thema's is gestegen sinds 2022. Enkele concrete onderwerpen laten dit beeld duidelijk zien. Een goed voorbeeld is het **kennen van de regels** die gelden binnen een organisatie, waar medewerkers steeds meer over weten (Figuur 17). Ook weten medewerkers meer over **welke informatie** ze via **e-mail mogen delen** dan in 2022 (Figuur 18). Het kennisniveau over veilig omgaan met informatie bij medewerkers is gegroeid.

Gedrag | Intentie | Sociale norm | Attitude | Ervaren controle | **Kennis** | Gelegenheid

AWARENWAYS

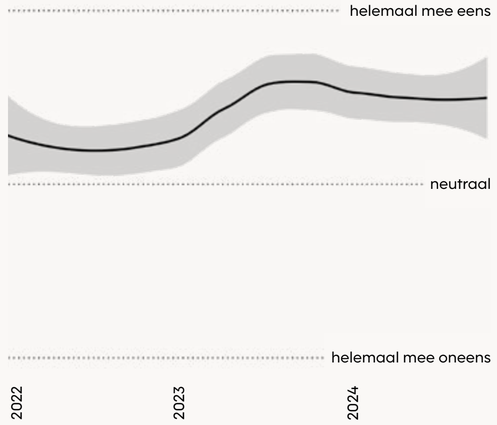
Figuur 17.

"Ik ken de regels voor het veilig werken met informatie die gelden binnen mijn organisatie."



Figuur 18.

"Ik weet welke informatie ik via e-mail mag delen."



Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

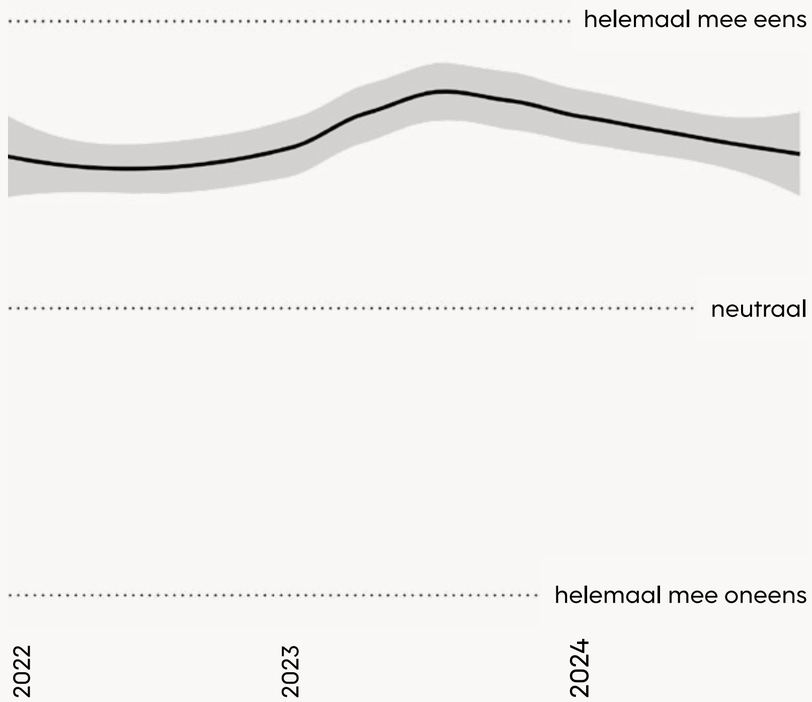
Hoe veilig werken we nog thuis?

Opvallend is dat er een uitzondering is te zien op de thema's **wachtwoorden** en **thuiswerken**, waarbij vooral de laatste opvalt. Hoewel de kennis op deze thema's eerder steeg, laten deze twee een daling zien sinds medio 2023. Zo weten medewerkers steeds minder goed hoe ze veilig kunnen werken buiten hun vaste werkplek (Figuur 19).

De verminderde kennis rondom thuiswerken lijkt, net als de afvlakking van de sociale norm, gerelateerd aan de COVID-pandemie. Nu medewerkers weer steeds vaker terug naar kantoor gaan en minder thuiswerken (CBS, 2024), lijkt de behoefte om meer te leren over veilig thuiswerken, evenals de kennis daarover, te zijn afgenomen. Het toegenomen werken op kantoor kan het gevoel van verantwoordelijkheid voor de informatieveiligheid en privacy ook verleggen. Waar bij thuiswerken de medewerker zich meer verantwoordelijk kan voelen, voelt de medewerker dat op kantoor de organisatie verantwoordelijk is voor het verzorgen van de veiligheid. Dit hangt mogelijk samen met de afvlakking van de aandacht voor het veilig omgaan met informatie vanuit de organisatie, die naar voren komt bij de trend die we observeren bij de sociale norm.

Figuur 19.

"Ik weet hoe ik veilig met informatie kan werken buiten mijn vaste werkplek."



Gedrag | Intentie | Sociale norm | Attitude | Ervaren controle | **Kennis** | Gelegenheid

Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

Gelegenheid is een onderdeel van feitelijke gedragscontrole en verwijst naar de externe factoren (middelen, tijd, processen) die de medewerkers in staat stellen om veilig met informatie te werken.

Sinds 2022 wisselt het voor medewerkers hoe gemakkelijk of moeilijk ze veilig met informatie kunnen werken.

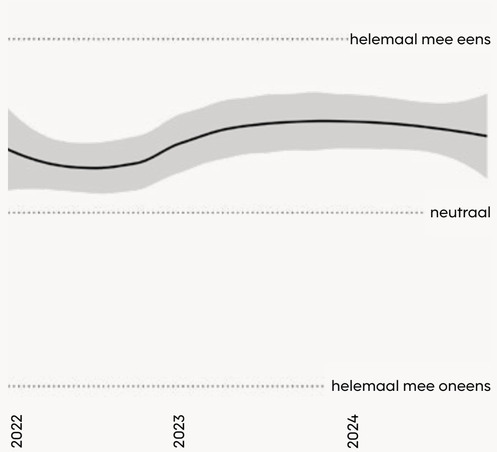
De gelegenheid die medewerkers ervaren om veilig om te gaan met informatie, varieert over de meeste thema's sinds 2022. Een paar specifieke ervaringen laten dit het beste zien. Zo zijn medewerkers het in verschillende mate eens over de jaren met de vraag of ze **genoeg tijd hebben** om hun **berichten te controleren op phishing** kenmerken (Figuur 20). Hoewel deze trend licht steeg in 2023, is het eind 2024 weer op hetzelfde niveau als het begin van 2022. Ook zijn medewerkers het afwisselend eens met hoe **gemakkelijk** het is om **nieuwe wachtwoorden** aan te maken (Figuur 21). Op alle thema's lijken er dus nog kansen te liggen om het makkelijker te maken om veilig te werken met informatie voor medewerkers.

Gedrag | Intentie | Sociale norm | Attitude | Ervaren controle | Kennis | **Gelegenheid**

AWARE WAYS

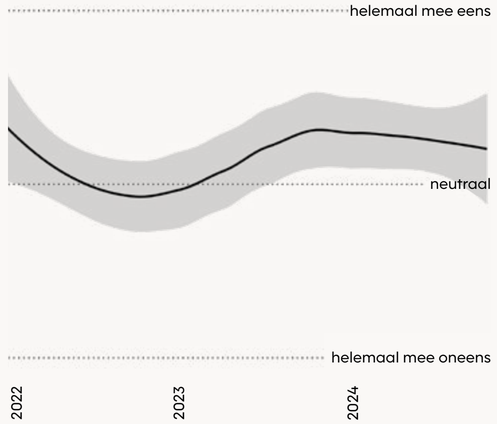
Figuur 20.

"Ik heb voldoende tijd om mijn berichten goed te controleren op (mogelijke) phishing kenmerken."



Figuur 21.

"Ik vind het makkelijk om voor ieder account een uniek en sterk wachtwoord te maken."



Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

Wat zijn ook alweer die persoonsgegevens?

Het meest opvallende thema is **AVG**. Het herkennen van (bijzondere) persoonsgegevens is zelfs **moeilijker** geworden over de jaren (Figuur 22). In 2024 antwoorden medewerkers gemiddeld “Neutraal” op de vraag of ze het makkelijk vinden om (bijzondere) persoonsgegevens te herkennen.

De toegenomen moeilijkheid van het herkennen van persoonsgegevens valt samen met de ontwikkeling die terug is te zien bij het gedrag, waar de aandacht voor de AVG naar de achtergrond lijkt te schuiven. Een verminderde aandacht voor de correcte opvolging van de AVG bij medewerkers, lijkt te leiden tot de uitdoving van eerder aangeleerd gedrag. Dit maakt het vervolgens voor medewerkers ook lastiger om dit gedrag nog uit te voeren, omdat ze het minder gewend zijn om te doen. Deze moeite om verschillende soorten gegevens te herkennen uit zich ook in de afgenomen ervaren controle van medewerkers om vertrouwelijke informatie te herkennen.

Figuur 22.

“Het werken met (bijzondere) persoonsgegevens is makkelijk.”

Gedrag | Intentie | Sociale norm | Attitude | Ervaren controle | Kennis | Gelegenheid

Gebaseerd op de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties.

Conclusie

AWARE WAYS

In dit trendrapport is de menselijke weerbaarheid onderzocht op het gebied van informatieveiligheid en privacy. Hiervoor zijn de antwoorden van 28.215 medewerkers uit 32 verschillende organisaties bekeken over de periode 2022-2024. Op verschillende psychologische constructen en over belangrijke informatieveiligheid en privacy thema's komen er duidelijke ontwikkelingen naar voren.

AVG

Allereerst laat de vraag "Hoe goed passen medewerkers de AVG-richtlijnen toe sinds 2022?" zien dat medewerkers dit steeds slechter doen sinds 2022. Ook ervaren medewerkers steeds meer moeite met het herkennen van verschillende soorten informatie, zoals persoonsgegevens en vertrouwelijke informatie.

Thuiswerken

Voor de vraag "Hoe verandert de aandacht en kennis ten opzichte van **thuiswerken**?" is te zien dat de kennis van medewerkers en de aandacht die wordt gegeven vanuit leidinggevenden en management is gegroeid tot 2023. Dit is sindsdien echter afgevlakt en de kennis van medewerkers over veilig thuiswerken begint zelfs af te nemen.

Wachtwoorden

Tenslotte wordt het antwoord op de vraag "Hoe verandert de houding van medewerkers ten opzichte van **wachtwoorden**?" duidelijk door de bevinding dat er onder medewerkers een gevoel groeit van 'wachtwoordmoeheid'. Dit uit zich in dat medewerkers het regelen van wachtwoorden minder belangrijk beginnen te vinden en dit ook steeds minder willen doen.

Conclusie

De trends die naar voren komen in dit trendrapport zijn relevant om te beschouwen binnen een groter beeld van digitalisering van de huidige samenleving en de toename van wet- en regelgeving in de wereld van informatieveiligheid en privacy.

Digitalisering brengt naast kansen op het gebied van automatisering en efficiëntie ook uitdagingen met zich mee, zoals nieuwe technologieën, veranderende omstandigheden en een hogere noodzaak voor informatieveiligheid en privacy. Deze uitdagingen kunnen leiden tot frustraties, zoals 'wachtwoordmoeheid', waardoor de potentiële voordelen van digitalisering niet optimaal benut worden in organisaties.
De uitdagingen van digitalisering vereisen voortdurende aandacht. Zo versnelde de COVID-19-pandemie de focus op veilig thuiswerken, maar neemt sinds 2023 hierover af doordat er minder aandacht voor is en meer gewenning. Ook met het toenemende gebruik van artificial intelligence in organisaties, bijvoorbeeld ChatGPT, Co-pilot en Gemini, is het steeds relevanter om de menselijke factor mee te nemen bij de (verdere) implementatie van nieuwe technologie.

Ook wet- en regelgeving op het gebied van informatieveiligheid en privacy vereist constante aandacht en uitleg, vooral nu het steeds uitgebreider en ingewikkelder wordt (zoals NIS2 en Dora). Bij nieuwe wet- en regelgeving, zoals de AVG in 2018 was, is er tijdens de invoering veel aandacht voor de implementatie, maar die neemt vaak af na de beginfase. Nu we aan de vooravond staan van de implementatie van wederom nieuwe wet- en regelgeving, is het van belang om rekening te houden met dit risico.

Er is een groeiende focus op de mens als risicofactor: human risk. Bij Awareways geloven we echter dat juist het versterken van menselijke weerbaarheid een krachtige bijdrage levert aan effectieve informatieveiligheid en privacy. Een robuuste weerbaarheidscultuur is daarbij onmisbaar en vraagt om continue aandacht, kennis en flexibiliteit in een snel veranderende digitale wereld.

Dit rapport biedt inzichten en kansen om deze menselijke weerbaarheid verder te versterken.

Definitielijst

Attitude	Attitude laat zien hoe belangrijk medewerkers informatieveiligheid vinden.
Constructen	Psychologisch begrip om menselijke gedachten, ervaringen en handelingen te omschrijven.
Cultuurscan	Gevalideerde vragenlijst die de psychologische constructen van de Theory of Planned Behavior meet.
Ervaren controle	Ervaren controle laat zien in hoeverre medewerkers geloven dat ze goed in staat zijn om veilig te werken met informatie én dat ze invloed hebben op de informatieveiligheid in hun organisatie.
Feitelijke controle	De middelen die medewerkers nodig hebben om bepaald gedrag te vertonen. Deze middelen kunnen intern zijn voor de persoon, zoals kennis, vaardigheden of intelligentie, of extern voor de persoon, zoals de juiste faciliteiten en genoeg tijd (gelegenheid).
Gedrag	Gedrag laat zien hoe vaak medewerkers zeggen veilig te werken met informatie.
Gelegenheid	Gelegenheid een onderdeel van feitelijke gedragscontrole en verwijst naar de externe factoren (middelen, tijd, processen) die de medewerkers in staat stellen om veilig met informatie te werken. Intentie laat zien in welke mate medewerkers van plan zijn om veilig te werken met informatie.
Intentie	Intentie laat zien in welke mate medewerkers van plan zijn om veilig te werken met informatie.
Kennis	Kennis is een onderdeel van feitelijke controle en laat zien hoeveel medewerkers weten over informatieveiligheid.
Sociale norm	Sociale norm laat zien in hoeverre medewerkers ervaren dat anderen, zoals collega's of leidinggevenden, bezig zijn met informatieveiligheid.
Startmeting	Startmeting is de eerste meting die gedaan wordt bij de klanten van Awareways voor aanvang van een Security Awareness programma.
Theory of Planned Behavior	Psychologisch model dat gepland gedrag in kaart brengt door onder andere te kijken naar de intentie tot gedrag en de feitelijke controle over het gedrag.

Referentielijst

AIV. (2024, 4 juni). Hybride dreigingen en maatschappelijke weerbaarheid. *Adviesraad Internationale Vraagstukken.* geraadpleegd op 9 december 2024, van https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2024/06/04/hybride-dreigingen-en-maatschappelijke-weerbaarheid

CBS. (2024, 15 maart). Ruim helft Nederlanders werkt weleens thuis. *Centraal Bureau voor de Statistiek.* Geraadpleegd op 2 december 2024, van https://www.cbs.nl/nl-nl/nieuws/2024/11/ ruim-helft-nederlanders-werkt-weleens-thuis

Ajzen, I., & Schmidt, P. (2020). Changing Behavior using the Theory of Planned Behavior. In M. S. Hagger, L. Cameron, K. Hamilton, N. Hankoren, & T. Lintunen (Eds.), *The handbook of Behavior Change,* 17-31. Cambridge, UK: Cambridge University Press. https://doi.org/10.1017/9781108677318.002

Hollnagel E., Wears R.L. and Braithwaite J. (2015). From Safety-I to Safety-II: A White Paper. *The Resilient Health Care Net: Published simultaneously by the University of Southern Denmark, University of Florida, USA, and Macquarie University, Australia.* https://doi.org/10.13140/RG.2.1.4051.5282

AWAREWAYS

Colofon

Titel:
Trendrapport 2024: De mens, risico of sterkste troef?

Uitgegeven door: Awareways
www.awareways.com

Auteur: Sjoerd van Veldhuizen, MSc
Redactie en eindredactie: Geertje Veenbergen
Ontwerp en vormgeving: Maureen Rademakers
Opmaak & vormgeving: Julia van den Tweel

Publicatiedatum: December 2024

Contact:
E-mail: info@awareways.com
Telefoon: 030 227 14 67

Menselijke weerbaarheid is geen kwestie van risico's vermijden, **maar van kracht versterken.**

Contactgegevens
www.awareways.com
info@awareways.com
030 227 14 67