

Rapportage

Cybersecurity gedragsonderzoek Alert Online 2026

September 2026

Behavior
Change
Group



Inhoudsopgave

<u>Managementsamenvatting</u>	3
<u>Aanleiding en doel</u>	5
<u>1. Welke doelgedragingen en doelgroepen zijn het meest relevant om te onderzoeken?</u>	8
<u>2. Hoe gedragen de doelgroepen zich op dit moment?</u>	12
<u>3. Welke gedragsbepalers verklaren waarom mensen de gewenste gedragingen wel of niet uitvoeren?</u>	16
<u>4. Welke verandertechnieken sluiten het beste aan op de relevante gedragsbepalers?</u> <u>Hoe kunnen deze worden vertaald naar kansrijke interventies?</u>	19
• <u>Toepassing op 4 kansrijke gedragingen: 2FA, fout melden, officiële website gebruiken, wachtwoordmanager</u>	22
• <u>Resultaten en interventies rondom AI</u>	35
<u>Bijlage A: Methodologische verantwoording</u>	47
<u>Bijlage B: Toepassing op overige cybergedragingen</u>	52
<u>Bijlage C: Aanvullende resultaten</u>	70
• <u>Steekproef</u>	71
• <u>Gedragsbepalers</u>	73
• <u>Descriptives van de scenario's</u>	90

Managementsamenvatting

Uit dit vragenlijstenonderzoek (met een representatieve steekproef van 609 consumenten en 378 werknemers) blijkt dat zowel consumenten als werknemers nog relatief weinig cyberveilige gedragingen uitvoeren. **Gemiddeld voeren consumenten slechts 33% van de veilige gedragingen altijd uit en werknemers voeren 31% van de gedragingen altijd uit.** Ondanks verschillende bewustwordingscampagnes, blijft de online veiligheid dus achter.

De kloof tussen weten en doen

Er is een structurele gedragskloof: veel Nederlanders kennen de risico's en willen veilig handelen, maar dit blijft vaak steken op controleergedrag en vertaalt niet door naar actievere handelingen. Zo geeft 77-84% aan dat ze de gevolgen van online criminaliteit of digitale fraude ernstig vinden. Ook heeft 64-76% de intentie om vaker mails, links en betaalverzoeken te controleren. De daadwerkelijke uitvoering van deze basishandelingen gaat redelijk goed: 48-66% controleert bijvoorbeeld altijd of de inhoud van een e-mail logisch is en 41-50% let altijd op tijdsdruk of dringende taal, zoals 'vandaag nog', 'meteen' of 'anders gaat het mis'. Simpel controleren gebeurt dus al wat vaker, maar zodra een actievere handeling zoals verificatie of extra beveiliging nodig is, blijft de intentie achter. Zo heeft 53% de intentie om (vaker) tweefactorauthenticatie (2FA) te gebruiken en 31-34% om een wachtwoordmanager in te stellen. Ook het daadwerkelijke gedrag van deze actievere handelingen blijft achter. Slechts 21-31% navigeert altijd zelf handmatig naar de officiële website of app. Daarnaast gebruikt 13-20% altijd een wachtwoordmanager en 16-32% gebruikt altijd 2FA. Als laatste meldt slechts 33% van de werknemers een gemaakte fout (zoals een verkeerde klik) direct bij de IT-afdeling.



Gebruik van AI

Hoewel men terughoudend is met persoonlijke informatie delen met AI (13-21% heeft de intentie om informatie te delen met AI), gebruikt 49% van de werknemers weleens privé AI-accounts

voor het werk, wat kan leiden tot shadow AI. Daarnaast deelt 35-46% inhoudelijke (werk)problemen met AI-tools om advies te krijgen. Wanneer mensen vinden dat AI empathisch is en veel kwaliteit levert, zijn zij bereid meer privacy in te leveren. Ook delen werknemers vaker persoonlijke informatie met AI wanneer zij bang zijn dat geen-gebruik van AI leidt tot negatieve consequenties op werk.

Waarom veranderen we niet?

Kennis alleen is niet genoeg om gedrag te veranderen. Regressieanalyses op de vragenlijstdata tonen aan dat er vier voornaamste belemmeringen zijn voor verandering in cybergedrag:



Inertia: Gedrag wordt uitgesteld of vermeden als het als te veel moeite of gedoe voelt. Waar op een link klikken 1 klik kost, vereist handmatig navigeren naar de officiële site 5-10 handelingen. Sommige veilige gedragingen worden dan ook als meer tijdrovend ervaren: 30-33% vindt gebruik van 2FA of een wachtwoordmanager tijdrovend, versus 10-19% voor het controleren van mails.



Gebrek aan procedurele kennis: Mensen hebben vaak wel theoretische kennis (weten wat), maar missen de praktische vaardigheid (weten hoe). Zo weet maar ongeveer de helft (45-59%) hoe ze 2FA of een wachtwoordmanager moeten instellen en gebruiken.



Ervaren nut: Niet iedereen ziet het nut in van extra maatregelen. Een deelnemer: *"2FA is goed voor belangrijke accounts met veel persoonlijke gegevens zoals bank en email, maar tegenwoordig heb je voor zoveel dingen accounts nodig... Voor willekeurige webwinkels of online diensten slaat het nergens op. Wat wil een crimineel daarmee doen? Zien wat ik besteld heb, of wat voor abonnement ik heb? Succes daarmee."* Overmoed speelt hierbij ook een rol. Mensen die geloven dat ze phishingmails zelf kunnen herkennen, gebruiken minder vaak de officiële website/app. Ze vertrouwen op hun eigen vaardigheden en denken dat extra maatregelen voor hen niet nodig zijn.



Andermans gedrag is onzichtbaar: Mensen zijn sociale dieren en worden beïnvloed door het gedrag van anderen. Online gedrag is echter niet goed zichtbaar (weet jij of jouw vrienden altijd 2FA gebruiken?) waardoor we minder snel het veilige cybergedrag van anderen kopiëren. Een deelnemer illustreerde dit mooi met *"Verder weet ik ECHT niet wat anderen doen."*

Managementsamenvatting



weten

doen

Hoe stimuleren we mensen om structureel digitaal veilig gedrag te vertonen?

Om consumenten en werknemers cyber-veiliger te maken, moeten we inzetten op de vier belemmeringen: inertia, procedurele kennis, ervaren nut en sociale normen. Het EAST-model houdt rekening met deze vier belemmeringen en bestaat uit vier pijlers.

<i>Easy (makkelijk)</i>	<i>Attractive (aantrekkelijk)</i>	<i>Social (sociaal)</i>	<i>Timely (tijdsgebonden)</i>
Mensen kiezen vaak onbewust voor de weg van de minste weerstand om energie te behouden. Zodra digitaal veilig gedrag te veel tijd of gedoe kost, haken mensen af. Stimuleer gewenst gedrag door gedrag makkelijker te maken (inertia te verlagen) en te leren hoe het moet (procedurele kennis verhogen).	Een gedrag moet aantrekkelijk, opvallend en belonend zijn om het te kunnen veranderen. Gebruikers zijn vaak overmoedig ("Ik herken phishing zelf wel") en zien daardoor het nut van extra veiligheidsmaatregelen niet in. Om deze overmoed te doorbreken, moet veilig gedrag de aandacht trekken en moeten de voordelen functioneel of emotioneel voelbaar worden gemaakt.	Mensen zijn sociale wezens en laten zich beïnvloeden door wat anderen in hun omgeving doen of geloven. Omdat veilig cybergedrag vaak onzichtbaar is, denkt ons brein onbewust dat 'niemand dit doet'. We moeten deze norm zichtbaar maken. Zet het sociale netwerk in om gedrag te veranderen.	Interventies zijn het meest effectief wanneer ze worden aangeboden op het juiste moment. Stimuleer het gedrag bij transities of directe beslismomenten. Dit verlaagt namelijk ook de inertia en verhoogt het ervaren nut .
• Standaardiseer het gedrag (defaults): Maak de veilige route de weg van de minste weerstand. Schakel 2FA automatisch in waar mogelijk en installeer wachtwoordmanagers vooraf op werklaptops. Stel de belangrijkste werksystemen standaard in als browser-bladwijzer en integreer opvallende eenkliks-meldknoppen om de melddrempel te minimaliseren. • Verminder frictie: Knip complexe handelingen op in kleine, behapbare stappen. Richt trainingen en handleidingen niet in op de theorie achter een tool, maar laat kort en krachtig zien hoe een gebruiker deze stapsgewijs activeert. • Verhoog frictie op onveilige routes: Ban actiesites en directe inloglinks in e-mails volledig uit. Door de onveilige handeling te blokkeren of te bemoeilijken, stuur je gebruikers automatisch richting het veilige alternatief (zelf naar de app of website navigeren).	• Doorbreek overmoed via ervaring (gamification): Alleen waarschuwen werkt niet. Zet interactieve realitychecks in, zoals phishingsimulaties met directe feedback of "zoek de verschillen"-quizen, om mensen aan den lijve te laten ervaren hoe snel ze misleid worden. • Frame de voordelen (gevoel van rust): Positioneer veiligheidstools positief. Verkoop een wachtwoordmanager niet als een 'verplichte beveiligingstaak', maar als een persoonlijke tool die mentale rust brengt en het onthouden van talloze wachtwoorden verbodig maakt. • Loss framing bij risico's: Benadruk bij handelingen expliciet wat men te verliezen heeft als men het gedrag niet uitvoert: van het leegroven van de eigen bankrekening tot het stilleggen van de gehele organisatie.	• Maak het gewenste gedrag of de trend daarvan zichtbaar: Communiceer met duidelijke, herkenbare boodschappen dat steeds meer mensen wél veilig handelen: "Steeds meer Nederlanders beveiligen hun belangrijkste accounts extra. Al meer dan de helft gebruikt 2FA. Doe jij ook mee?". • Social modeling en injunctieve norm: Laat binnen een organisatie het management expliciet optreden als rolmodel door openlijk te vertellen over hun eigen cyberfouten en welke maatregelen zij nemen. Beloon daarnaast meldingen van werknemers direct met actieve complimenten, om te laten zien dat alertheid enorm wordt gewaardeerd. • Zet in op 'zendingswerk': Activeer de sociale netwerken van consumenten en werknemers. Moedig hen aan om als cyberambassadeur op te treden en ook vrienden of familieleden te helpen met het instellen van 2FA of een wachtwoordmanager.	• Prompts op het beslismoment: Koppel herinneringen aan de feitelijke handeling. Toon bijvoorbeeld automatische waarschuwings-banners bij inkomende externe e-mails, waardoor de werknemer letterlijk twee seconden moet pauzeren om de afzender te scannen. • Gebruik bestaand momentum: Haak in op natuurlijke triggers. Krijgt een gebruiker bijvoorbeeld een melding om een wachtwoord te wijzigen vanwege een datalek? Koppel dit momentum dan direct aan de optie om meteen 2FA te activeren of makkelijk een veilig nieuw wachtwoord te genereren via een wachtwoordmanager. • Zet in op 'als-dan' routines: Help gebruikers nieuwe gewoontes te vormen. Leer hen een simpele regel aan om de foute klik-reflex te overschrijven: "Als een bericht mij vraagt om in te loggen, sluit ik de mail direct en open ik zélf mijn app of browser."

Aanleiding en *doel*

Aanleiding en *doel*

De kloof tussen bewustwording en digitaal gedrag

Ondanks jarenlange, intensieve bewustwordingscampagnes en de periodieke monitoring van kennis, houding en gedrag, blijft een structurele verbetering van de online veiligheid in Nederland achter. De resultaten uit het Cybersecurityonderzoek Alert Online 2025 (Ipsos I&O, 2025) tonen aan dat er een hardnekkige kloof bestaat tussen zelfgerapporteerd gedrag en daadwerkelijk handelen: wat consumenten en werknemers *zeggen* te doen, komt in de praktijk vaak niet overeen met hun feitelijke acties. De impact van traditionele metingen en campagnes blijkt hierdoor beperkt.

Tegelijkertijd verandert het digitale dreigingslandschap in een hoog tempo. Door de opkomst van geavanceerde technologieën, zoals AI-gedreven misleiding en geraffineerde phishing, worden digitale dreigingen steeds frequenter, persoonlijker en taalkundig foutloos. Dit vergroot de kwetsbaarheid van zowel consumenten als het bedrijfsleven aanzienlijk.

Wat drijft cyberveilig gedrag?

De huidige context vraagt niet langer om het louter registreren van wat mensen online doen, maar om een fundamenteel begrip van waarom digitaal veilig gedrag achterblijft. Daarom is een inhoudelijke vernieuwing van het cyberonderzoek noodzakelijk. Er is diepgaand inzicht nodig in de achterliggende psychologische mechanismen, zoals motivatie, impulsiviteit en risicoperceptie, om effectievere barrières op te werpen tegen moderne cyberdreigingen.

Richting structurele gedragsverandering en impact

Met het oog op deze ontwikkelingen heeft het ECP | Platform voor de InformatieSamenleving samen met de Behavior Change Group het Cybersecurityonderzoek Alert Online doorontwikkeld. Het hoofddoel van het huidige onderzoek is het realiseren van een meetbare, structurele gedragsverandering op het gebied van online veiligheid.

Om dit hoofddoel te bereiken, richt het onderzoek zich op de volgende subdoelen:

- **Blootleggen van psychologische mechanismen:** Inzicht verkrijgen in de dieperliggende motivaties en barrières die bepalen hoe mensen omgaan met digitale risico's.
- **Bieden van concrete handelingsperspectieven:** Het formuleren van toepasbare handvatten voor zowel de consument als de zakelijke markt.
- **Vergroten van campagne-impact:** Het aanreiken van scherpe, datagedreven aanknopingspunten voor effectieve gedragsinterventies en campagnes met een grote maatschappelijke en media-impact.

Hoofdvraag: Hoe kunnen we consumenten en professionals binnen de bedrijfswereld stimuleren om structureel digitaal veilig gedrag te vertonen?

1. Welke concrete doelgedragingen en welke (sub)doelgroepen binnen het algemene publiek en de bedrijfswereld zijn het meest relevant om verder te onderzoeken?
2. Hoe gedragen deze doelgroepen zich op dit moment in situaties waarin digitaal veilig handelen belangrijk is?
3. Welke gedragsbepalers verklaren waarom mensen de gewenste gedragingen wel of niet uitvoeren?
4. Welke verandertechnieken sluiten het beste aan op de relevante gedragsbepalers?
5. Hoe kunnen de verandertechnieken worden vertaald naar kansrijke interventies of aanpassingen in communicatie, technologie of omgeving voor Alert Online en haar partners?

Onderzoeksmethoden

Bewustwording is een belangrijke voorwaarde, maar zelden voldoende om echte gedragsverandering te realiseren. Voor effectieve gedragsverandering is het daarom cruciaal om te weten waar je begint en hoe je begint. Met welke gedragingen kun je het beste starten? Welk gedrag kun je van de doelgroep nu al verwachten en welk gedrag vraagt om een langere adem? En welke gedragsmechanismen bepalen vervolgens of mensen deze gedragingen werkelijk uitvoeren? Met de volgende onderzoeksmethoden hebben we deze vragen beantwoord.



Rasch-analyse. We startten met een verdiepende analyse van de reeds beschikbare kwantitatieve data uit het Alert Online-onderzoek 2025. Met behulp van de Rasch-methodiek konden we bepalen welke cybergedragingen kansrijk zijn om op in te spelen. We analyseerden:

- hoe de cybergedragingen zich tot elkaar verhouden.
- of er een achterliggende mindset is, die voorspellend is voor meer online veilig gedrag.
- welke digitaal veilige gedragingen relatief laagdrempelig zijn en al door een groot deel van de doelgroep worden uitgevoerd.
- welke gedragingen relatief weinig worden uitgevoerd en meer inspanning, vaardigheden of motivatie vragen.



Verdiepende deskresearch. Een verdiepende deskresearch gaf ons een eerste inzicht in de belangrijkste gedragsbepalers voor elk van de kansrijke gedragingen uit de Rasch-analyse. Dit was een eerste aanzet voor het beantwoorden van de vraag: Welke gedragsmechanismen bepalen of mensen deze gedragingen werkelijk uitvoeren?



Vragenlijstonderzoek. Als laatste hebben we een selectie gemaakt van de meest kansrijke gedragingen en gedragsbepalers en een vragenlijst gemaakt. Zo konden we statistisch toetsen welke relaties er bestaan tussen de gedragingen en gedragsbepalers voor consumenten en werknemers. Hiermee konden we definitief de belangrijkste gedragsmechanismen in kaart brengen.

In juni en juli 2026 is deze vragenlijst naar cybergedragingen uitgezet onder consumenten en werknemers (thuis versus op het werk) en de achterliggende gedragsbepalers. In totaal hebben 609 mensen de consumentenvragenlijst ingevuld en 378 mensen de werknemervragenlijst*. Zie bijlage C voor een overzicht van de volledige steekproef. Aan de hand hiervan hebben we in kaart gebracht hoeveel mensen het gedrag al uitvoeren. Voor de werknemers zijn deze beschrijvende resultaten ook uitgesplitst naar type werknemers: ZZP, MKB (2-50 werknemers) of corporate (50+ werknemers). Middels regressieanalyses is vervolgens onderzocht welke gedragsbepalers invloed hebben op de verschillende cybergedragingen. Op basis van deze inzichten zijn adviezen opgesteld.

Zie bijlage A: Methodologische verantwoording voor meer details over de onderzoeksmethoden.

*De resultaten van de vragenlijst zijn gewogen. Dit betekent dat er een correctie is toegevoegd om te zorgen dat de steekproef een eerlijke spiegel is van de totale groep consumenten en werknemers. In de data zitten namelijk enkele groepen die over- en ondervetegenwoordigd zijn. Door weging toe te voegen, tellen ondervetegenwoordigde groepen zwaarder en overvetegenwoordigde groepen minder zwaar. Zo wordt de data meer representatief voor de echte doelgroep. Dit betekent ook dat de steekproefaantallen naast sommige grafieken hoger of lager zijn dan het totaal aantal geworven deelnemers dat vermeld staat op deze pagina.

1. Welke *doelgedragingen* en *doelgroepen* zijn het meest relevant om te onderzoeken?

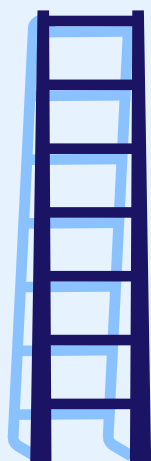
Onderzochte *doelgroepen*



In dit onderzoek focussen we specifiek op twee doelgroepen: consumenten in het algemeen en werknemers van bedrijven. Dit onderscheid is cruciaal, omdat de gedragsbepalers tussen deze twee groepen sterk kunnen verschillen. Bij werknemers spelen vaak omgevings- en systeemfactoren een rol, zoals standaardbeveiligingsinstellingen of verplichte werkwijzen binnen een organisatie. Bij consumenten is het gedrag vaker vrijwillig of incidenteel. Door beide groepen te onderzoeken, kunnen de onderliggende gedragsmechanismen per context goed worden geduid.

De afbeelding links toont de huidige positie van de doelgroepen op de veiligheidsladder. Hoe hoger een doelgroep op de ladder staat, hoe meer veilige gedragingen ze gemiddeld als groep uitvoeren. Zowel consumenten als werknemers hebben nog stappen te zetten in hun cyberveiligheid. De andere twee grafieken laten zien hoeveel procent van de doelgroep de specifieke gedragingen momenteel al altijd uitvoert. Deze resultaten komen voort uit de Rasch-analyse die is gedaan op de data van Alert Online 2025.

Voert veel
cybergedragingen uit



Consumenten voeren
gemiddeld 33% van de
gedragingen altijd uit

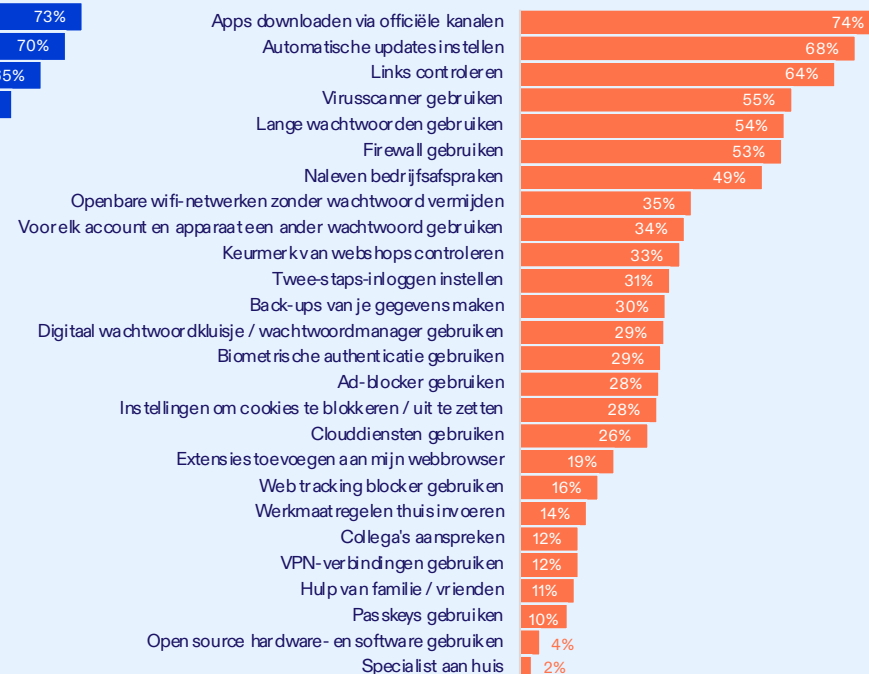
Werknemers voeren
gemiddeld 31% van de
gedragingen altijd uit

Voert weinig
cybergedragingen uit

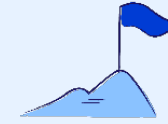
Consumenten



Werknemers



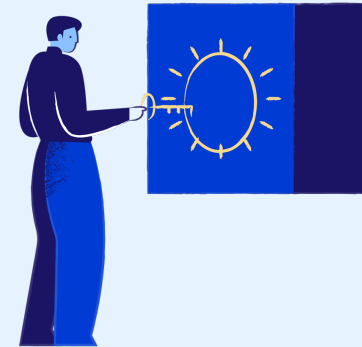
Onderzochte *doelgedragingen*



Om een gedegen gedragsstrategie te maken was het belangrijk om een selectie te maken van cybergedragingen voor het vragenlijstonderzoek. We hebben de gedragingen uit Alert Online 2025 gebruikt als basis. Deze zijn aangevuld met andere kansrijke gedragingen. Aan de hand van de Rasch-analyse, experts en deskresearch is bepaald welke doelgedragingen het meest kansrijk zijn om op in te spelen. Deze doelgedragingen kunnen geclusterd worden in drie thema's:

1. **Gedragingen die *altijd* uitgevoerd moeten worden.** Denk aan gedragingen rondom phishing en sociale manipulatie zoals links controleren of officiële kanalen gebruiken. Experts leggen de nadruk op stoppen, checken en melden. Daarom kozen we voor verschillende gedragingen binnen het checken van mails, links en betaalverzoeken en het melden van cyberfouten binnen een organisatie.
2. **Gedragingen die eenmalig ingesteld moeten worden en vervolgens gebruikt moeten blijven worden.** Denk aan tweefactorauthenticatie (2FA) en wachtwoordmanagers. Er is een grote kloof tussen mensen die 2FA soms en altijd gebruiken. Het is interessant om te onderzoeken hoe deze kloof meer gedicht kan worden. 2FA en wachtwoordmanagers kwamen ook in de Rasch-analyse naar voren als kansrijk en hebben mogelijk veel impact: nog niet iedereen doet het en ook nog niet niemand. De gedragingen zitten precies op het niveau op de ladder waar de doelgroep zich momenteel bevindt (31-33%). De gedragingen worden dus als haalbaar gezien.
3. **AI-gerelateerde gedragingen.** AI is een heel erg opkomend thema. Het is interessant om specifieke AI gedragingen mee te nemen om te zien hoeveel mensen dit al doen en wat daar voorspellers voor zijn. De AI-gedragingen werden vooral exploratief onderzocht.

Zie op de volgende pagina een overzicht van alle gedragingen per doelgroep waar we op hebben ingezoomd tijdens de vragenlijst in dit onderzoek. Daarna beschrijven we hoeveel mensen het gedrag nu uitvoeren per cluster.



Onderzochte *doelgedragingen*

Consumenten

Cluster 1: altijd uitvoeren

- Ik kijk of het e-mailadres van de afzender logisch en betrouwbaar lijkt.
- Ik controleer waar een link naartoe gaat voordat ik erop klik.
- Ik ga zelf naar de officiële website of app in plaats van dat ik een link uit de e-mail gebruik.
- Ik controleer of de inhoud van de e-mail logisch is, bijvoorbeeld of ik echt iets verwacht.
- Ik let op tijdsdruk of dringende taal, zoals “vandaag nog”, “meteen” of “anders gaat het mis”.
- Ik controleer bij betaalverzoeken het bedrag, de ontvanger en de reden van betaling.
- Ik gebruik alleen vertrouwde betaalplatforms voor betaalverzoeken.

Cluster 2: eenmalig moeite

- Ik gebruik twee-factor-authenticatie (2FA) voor mijn privé-accounts (bijvoorbeeld e-mail, bankzaken of online shoppen).
- Ik gebruik een wachtwoordmanager voor mijn persoonlijke online accounts (zoals e-mail, sociale media of bankieren).

Cluster 3: AI

In hoeverre deel jij de volgende dingen met AI:

- Persoonlijke emoties, zorgen of gevoelens.
- Persoonlijke documenten (zoals cv's of medische rapporten).
- Informatie over familieleden, vrienden of collega's.
- Persoonlijke situaties of problemen om advies te krijgen.

Werknemers

Cluster 1: altijd uitvoeren

- Ik kijk of het e-mailadres van de afzender logisch en betrouwbaar lijkt.
- Ik controleer waar een link naartoe gaat voordat ik erop klik.
- Ik ga zelf naar de officiële website of app in plaats van dat ik een link uit de e-mail gebruik.
- Ik controleer of de inhoud van de e-mail logisch is, bijvoorbeeld of ik echt iets verwacht.
- Ik let op tijdsdruk of dringende taal, zoals “vandaag nog”, “meteen” of “anders gaat het mis”.
- Als ik iets doe waar ik later over twijfel, bijvoorbeeld op een link klikken die ik achteraf niet vertrouw, meld ik dit bij mijn organisatie (zoals IT-support of security-officer).

Cluster 2: eenmalig moeite

- Ik gebruik twee-factor-authenticatie (2FA) voor werk-accounts (bijvoorbeeld e-mail of administratiesystemen).
- Ik gebruik een wachtwoordmanager voor mijn online werkaccounts (zoals e-mail, agenda of administratiesystemen).

Cluster 3: AI

- Ik gebruik AI-tools voor werk zonder toestemming of medeweten van mijn organisatie.
- Ik gebruik privé AI-accounts of apps voor werkdoeleinden.

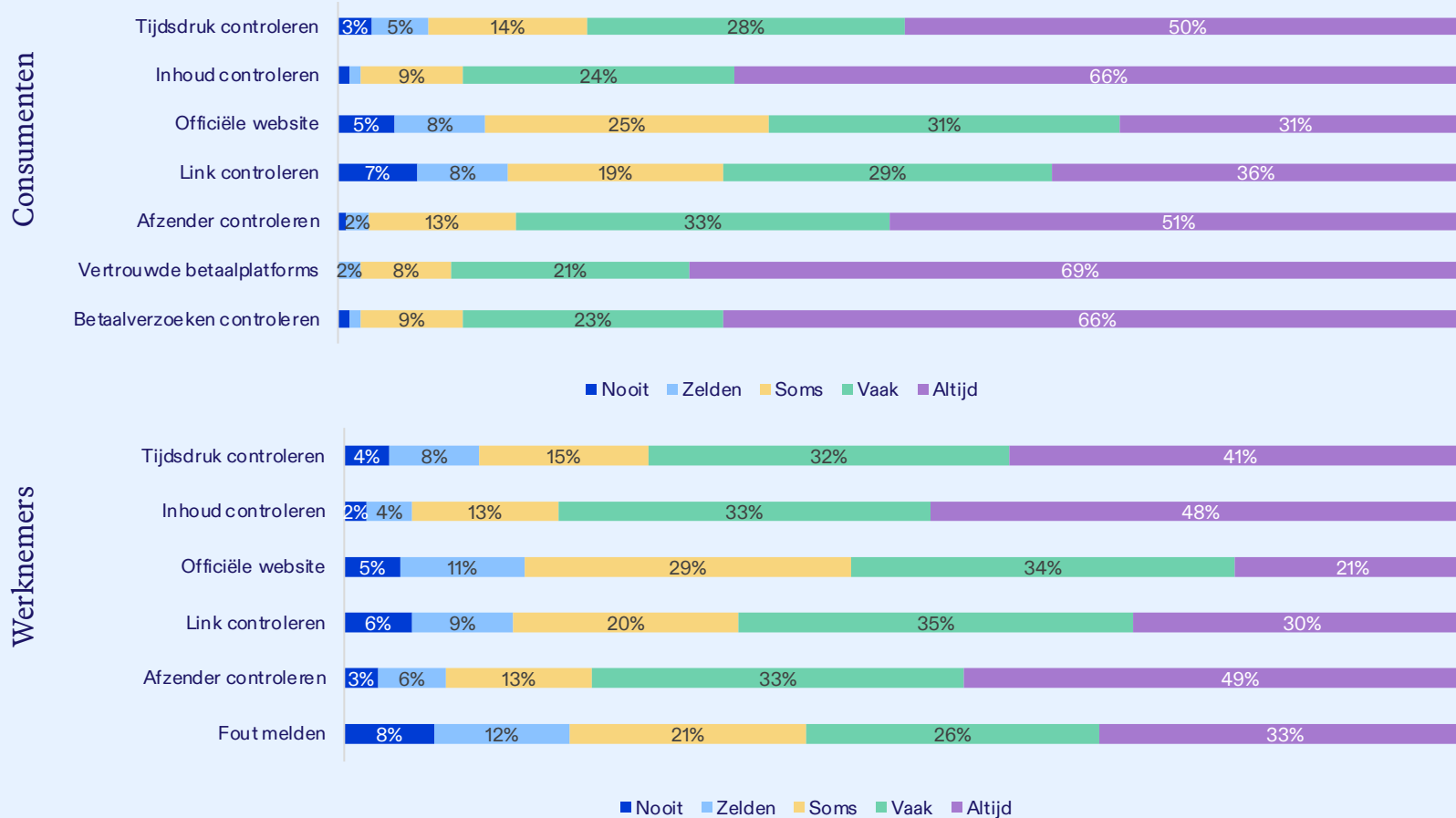
In hoeverre deel je de volgende soorten persoonlijke informatie met AI-tools:

- Persoonlijke emoties, zorgen of gevoelens.
- Persoonlijke documenten (zoals cv's of werknemergegevens).
- Informatie over collega's en leidinggevenden.
- Informatie over mijn klanten / patiënten / studenten of andere doelgroep.
- Werksituaties of -problemen om advies te krijgen.

2. *Hoe gedragen* de
doelgroepen zich op dit
moment?

Cluster 1: controleren en melden

Vooraf bij links controleren en de officiële website gebruiken is er nog winst te boeken.



Wat valt op?

In grote lijnen rapporteren consumenten en werknemers dat ze **basishandelingen rondom 'controleren' relatief vaak uitvoeren** (zoals het controleren van de inhoud van een mail (90% consumenten vaak of altijd; 81% werknemers vaak of altijd) en de afzender (84% consumenten vaak of altijd; 82% werknemers vaak of altijd).

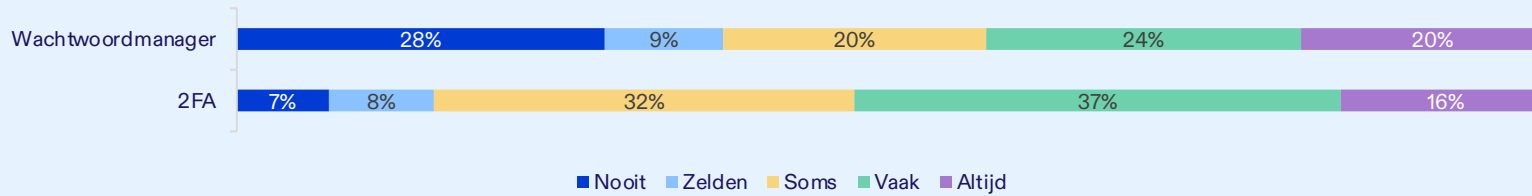
Er lijkt echter een **kloof te zijn tussen zelfgerapporteerd gedrag en daadwerkelijk veilig handelen**. Zodra actieve, specifiekere handelingen worden gevraagd, zoals het handmatig navigeren naar een officiële website (62% consumenten vaak of altijd; 51% werknemers vaak of altijd) of het controleren van de daadwerkelijke link (65% consumenten en werknemers vaak of altijd), blijft het gedrag wat meer achter.

Bij werknemers is het melden van fouten een extra knelpunt: slechts **33% meldt altijd een cyberfout** bij de organisatie.

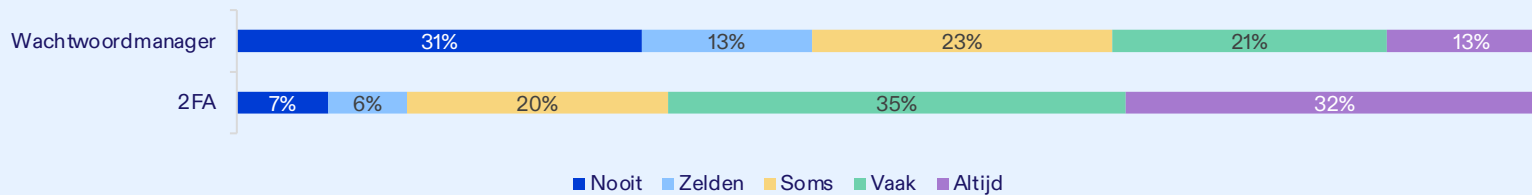
Cluster 2: 2FA en wachtwoordmanager

Bij zowel wachtwoordmanager als 2FA is er nog winst te boeken.

Consumenten



Werknemers



Wat valt op?

Bij zowel consumenten als werknemers zijn er nog maar weinig mensen die een wachtwoordmanager of 2FA gebruiken.

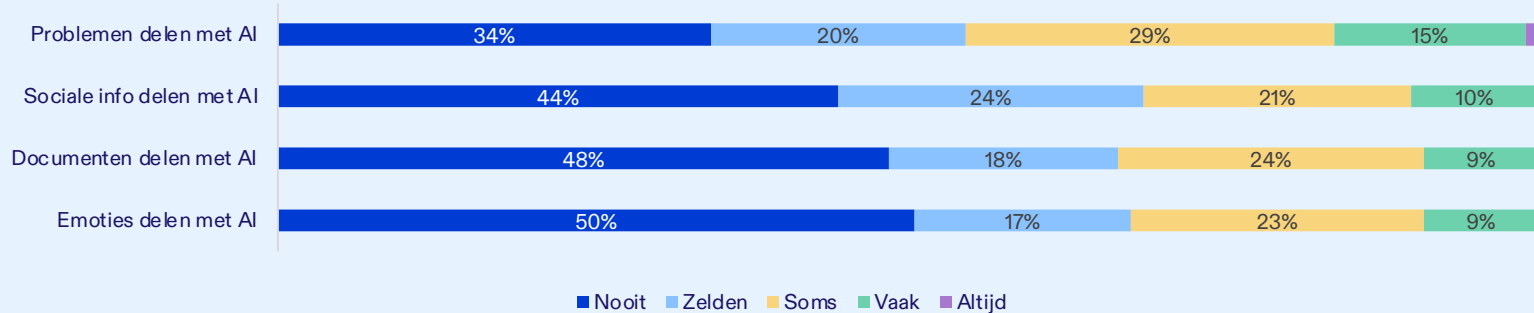
Ongeveer de helft van de consumenten gebruikt 2FA vaak of altijd (53%), maar **slechts 16% van de consumenten gebruikt het altijd** voor privé-accounts. **Bij werknemers ligt het percentage voor 2FA aanzienlijk hoger** op 67%, en 32% altijd, wat er waarschijnlijk op duidt dat veel organisaties dit inmiddels verplichten.

Het gebruik van een wachtwoordmanager blijft achter bij beide doelgroepen. Slechts 44% van de consumenten en 34% van de werknemers maakt vaak of altijd gebruik van een wachtwoordmanager. **Een grote groep gebruikt zelfs nooit een wachtwoordmanager** (28% van de consumenten en 31% van de werknemers). Slechts 20% van de consumenten en 13% van de werknemers gebruikt altijd een wachtwoordmanager.

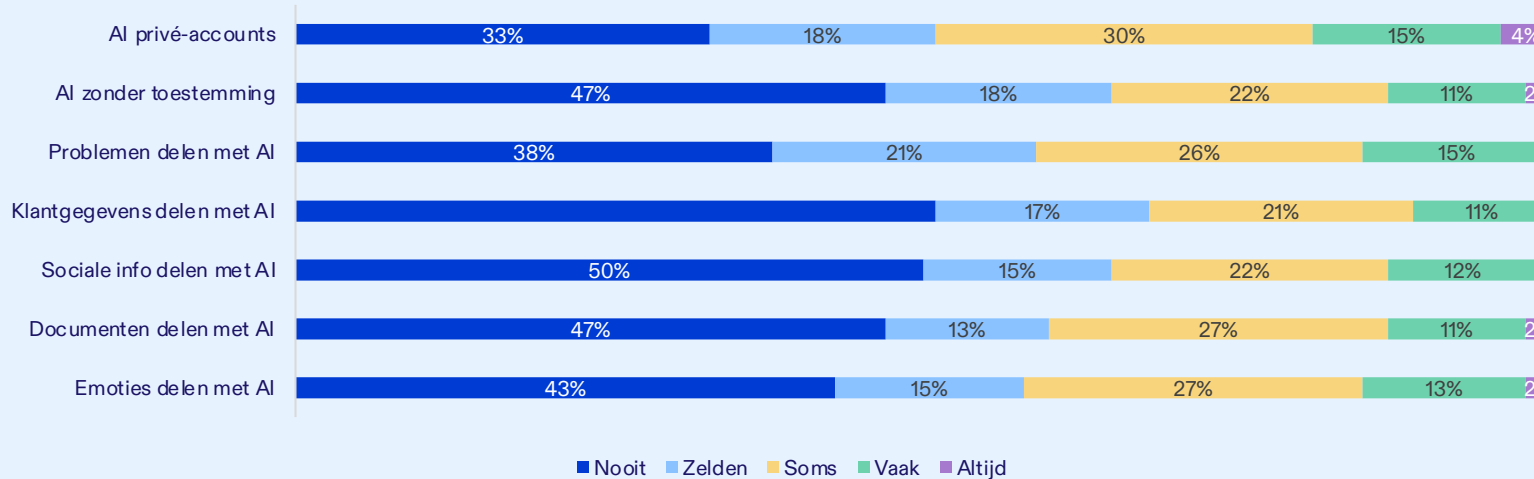
Cluster 3: AI

Voor al bij privé AI-accounts gebruiken is er nog winst te boeken.

Consumenten



Werknemers



Wat valt op?

De meeste consumenten en werknemers zijn **terughoudend met het delen van persoonlijke en gevoelige informatie (zoals emoties, documenten of sociale gegevens) met AI-tools**. De percentages van mensen die dit 'zelden' of 'nooit' doen liggen overal boven de 50%. Zo deelt 67% van de consumenten en 58% van de werknemers nooit of zelden emoties met AI. Wel **deelt een aanzienlijk deel van de doelgroep persoonlijke situaties of werksituaties met AI** om advies te krijgen: bijna de helft van de consumenten (46%) en ruim een derde van de werknemers (35%) doet dit soms, vaak of altijd.

Privé-accounts gebruiken is een belangrijk knelpunt op de werkvloer. Bijna de helft van de werknemers (49%) maakt op het werk soms, vaak of altijd gebruik van privé-AI-accounts of apps voor werkdoeleinden.

Kanttekeningen:

- Informatie delen met AI is op zichzelf niet ongewenst. Zo lang de persoonlijke gegevens bijvoorbeeld uit documenten worden gehaald, voordat een document wordt gedeeld, is het prima. *Hoe* AI precies wordt gebruikt hebben we nu niet in detail uitgevraagd. Houd hier rekening mee bij het interpreteren van de data.
- De AI gedragingen zijn nu een momentopname. Het kan zijn dat hoe meer mensen AI gaan gebruiken de komende jaren, hoe meer mensen ook ongewenste informatie gaan delen. Het is goed om deze gedragingen de komende tijd in de gaten te houden. Mensen die nu AI gebruiken zijn er mogelijk nog wat voorzichtiger mee.

3. Welke *gedragsbepalers* verklaren waarom mensen de gewenste gedragingen wel of niet uitvoeren?

Gedragbepalers cluster 1 en 2

Per gedrag zijn de belangrijkste gedragbepalers in kaart gebracht (zie pagina 23-34, en bijlage B). Gedragbepalers zijn stimulerende en belemmerende factoren die het gedrag beïnvloeden. Inspelen op deze gedragbepalers is belangrijk om gedrag echt te kunnen veranderen en verder te klimmen op de gedragsladder. Een aantal stimulerende en belemmerende gedragbepalers komen over de gedragingen van cluster 1 en 2 heen vaker terug. Deze overkoepelende gedragbepalers staan hieronder beschreven. Bij het ontwerpen van communicatie en interventies is het goed daar rekening mee te houden, hieronder geven we aan hoe dat kan. Daarnaast is het per gedrag en doelgroep belangrijk naar de specifieke gedragbepalers te kijken en daarop in te spelen.

Kennis

Kennis was bij een groot deel van de gedragingen een voorspellende gedragbepaler: hoe meer kennis iemand heeft, hoe vaker ze het cybergedrag uitvoeren. Het gaat hier niet om theoretische definities van wat bijvoorbeeld 2FA is, maar om procedurele kennis: *hoe stel ik dit concreet in op mijn telefoon?*

Wat is nodig?

Het is dus belangrijk om dit soort **procedurele kennis** te verhogen. Leg stapsgewijs uit hoe 2FA of een wachtwoordmanager ingesteld moet worden of waar iemand allemaal op moet letten als ze een mail binnenkrijgen met een linkje. Nu weet nog maar ongeveer de helft (45-59%) hoe ze dit moeten doen.



Sociale norm

Mensen kijken naar wat andere mensen in hun omgeving doen (descriptieve norm). Als zij denken dat veel mensen in hun directe omgeving (vrienden, familie, collega's) het cybergedrag uitvoeren, dan zullen ze dit zelf ook eerder doen. Specifiek voor fout melden is ook de injunctieve norm voorspellend: als werknemers denken dat het in hun organisatie gewaardeerd wordt om fouten te melden, dan wordt dit ook vaker gedaan. De meerderheid (77%) van de respondenten geeft aan dat het al gewaardeerd wordt in hun organisatie om fouten te melden.

Wat is nodig?

Laat zien dat al best veel mensen bepaalde cybergedragingen uitvoeren. Hierbij is het wel belangrijk om te letten op de geloofwaardigheid hiervan. Als nog maar zeer weinig mensen het doen, dan is het beter om een trend te benoemen: steeds meer mensen stellen 2FA in op hun apparaten bijvoorbeeld. Let op: communiceer de juiste norm, niet de norm dat iedereen zich onveilig gedraagt op het werk.



Ervaren nut

Het nut inzien van de gedragingen (waar het tegen beschermt) is cruciaal om online veiliger gedrag te vertonen. Dit nut heeft te maken met ervaren dat een cybergedrag de kans verkleint om opgelicht te worden, maar ook met overmoed. Als mensen het gevoel hebben dat ze zelf al goed opletten en bijvoorbeeld mails controleren, nemen ze niet altijd extra maatregelen zoals naar de officiële website gaan of 2FA instellen. De analyses laten zien: Hoe sterker iemand denkt de kans op oplichting te verkleinen door een e-mail goed te controleren voor actie te ondernemen, hoe *minder* vaak diegene naar de officiële website gaat. Mensen kunnen het gevoel hebben dat ze phishing en dergelijke zelf wel kunnen spotten en dus geen officiële website hoeven te gebruiken. Daarnaast denkt 16-17% dat ze geen 2FA nodig hebben, omdat ze zelf online al voorzichtig genoeg zijn. De ruime meerderheid (77-84%) is zich wel al bewust van de gevolgen en ziet ook in dat mails en betaalverzoeken controleren een effectieve methode is om de kans op phishing te verkleinen (83-90%). Alleen voor 2FA en wachtwoordmanagers zien ze het nut er nog minder van in (46-49%). Werknemers schatten de kans om slachtoffer te worden groter in dan consumenten: 73% vs. 28%.

Wat is nodig?

Verhoog het ervaren nut. Juist ook voor hen met overmoed. Zij zijn nog steeds vatbaar voor hacks. Alleen beargumenteren om te overtuigen helpt niet. Mensen moeten aan den lijve ervaren (bijvoorbeeld via simulaties) hoe makkelijk ze te misleiden zijn en dat de cybergedragingen hiertegen beschermen.

Inertia

Inertia, het gevoel dat een gedrag moeite kost, komt een aantal keer terug als weerstand: Zolang de waargenomen moeite (wachtwoorden overzetten, extra inlogstap) groter voelt dan het directe voordeel, stellen mensen het gedrag uit. Sommige gedragingen worden als tijdrovender dan andere gedragingen gezien. Zo vinden mensen 2FA en wachtwoordmanagers meer tijd en moeite kosten dan betaalverzoeken en mails controleren en fouten melden.

Wat is nodig?

Het is daarom belangrijk om de ervaren moeite te verlagen. Maak de gevraagde gedragingen zo makkelijk mogelijk. Denk bijvoorbeeld aan defaults of vooraf ingestelde toepassingen op werklaptops.



Gedragsbepalers cluster 3

Ook voor de AI gedragingen zijn de gedragsbepalers in kaart gebracht. AI-gedrag verschilt echter van de cluster 1 en 2 gedragingen, waardoor de gedragsbepalers ook niet overeenkomen met die op de vorige pagina. We beschrijven hieronder de algemene opvallendheden uit de data binnen het thema AI. In het volgende hoofdstuk beschrijven we ook voor cluster 3 per gedrag de gedragsbepalers en de bijbehorende technieken om het gedrag te veranderen, bijvoorbeeld om shadow AI tegen te gaan.

Frequentie AI-gebruik

Hoe vaker je AI gebruikt, hoe minder vaak je informatie deelt met AI, zoals emoties, documenten, sociale informatie en problemen.



Leeftijd

Leeftijd komt bij alle AI-gedragingen terug als voorspeller: oudere consumenten en werknemers delen minder vaak informatie en documenten met AI. Ook gebruiken ze minder vaak privé-AI accounts en AI-tools zonder toestemming.



Angst gevolgen loopbaan

Bij werknemers valt ook op dat angst voor gevolgen als men geen AI gebruikt vaak een significante voorspeller is. Werknemers met deze angst delen vaker informatie met AI.



AI empathisch vinden

Zowel consumenten als werknemers delen informatie en problemen met AI en werknemers gebruiken vaker privé-accounts als ze AI als empathisch ervaren. Empathie kan een vals gevoel van psychologische veiligheid en vertrouwelijkheid opwekken (*Deze AI begrijpt mij, dus ik kan dit veilig delen*). Bij generatieve AI wordt dit effect versterkt door antropomorfisme: het toeschrijven van menselijke eigenschappen aan AI zorgt ervoor dat gebruikers hun mentale 'privacy-filter' uitschakelen.



AI levert kwaliteit

Gebruikers kiezen voor kwaliteit en productiviteit boven veiligheid. Als de risico's acceptabel voelen ten opzichte van de tijdswinst, of als de kwaliteit hoog is, negeren ze de veiligheidsrisico's. Consumenten en werknemers die vinden dat AI kwaliteit levert, dat ze eerder persoonlijke of werkdoelen behalen en dat AI efficiënt is, delen vaker informatie met AI en werknemers grijpen dan ook vaker naar privé AI-accounts op werk.



4. Welke *verandertechnieken* sluiten het beste aan op de relevante gedragsbepalers? Hoe kunnen deze worden vertaald naar kansrijke *interventies*?

Gedragstrategie hoog over (*EAST*)

Zowel consumenten als werknemers staan nog relatief laag op de ladder als het gaat om cyberveiligheid. Het doel van dit onderzoek was om hier verandering in te brengen: Hoe kunnen we het algemene publiek en professionals binnen de bedrijfswereld stimuleren om structureel digitaal veilig gedrag te vertonen? Om gedrag echt te veranderen en de doelgroepen hoger op de ladder te laten klimmen, zijn effectieve interventies nodig. Volgens het EAST-framework* zijn interventies pas effectief als er aan vier voorwaarden wordt voldaan. Hieronder beschrijven we deze vier pijlers en hoe de vier overkoepelende gedragsbepalers van cluster 1 en 2 hier aan te koppelen zijn. Daarnaast beschrijven we tactieken en technieken die helpen om aan deze pijlers te voldoen.

<i>Easy (makkelijk)</i>	<i>Attractive (aantrekkelijk)</i>	<i>Social (sociaal)</i>	<i>Timely (tijdsgebonden)</i>
Mensen kiezen vaak onbewust voor de weg van de minste weerstand om energie te behouden. Zodra digitaal veilig gedrag te veel tijd of gedoe kost, haken mensen af. Stimuleer gewenst gedrag door gedrag makkelijker te maken (inertia te verlagen) en te leren hoe het moet (procedurele kennis verhogen).	Een gedrag moet aantrekkelijk, opvallend en belonend zijn om het te kunnen veranderen. Gebruikers zijn vaak overmoedig (<i>Ik herken phishing zelf wel</i>) en zien daardoor het nut van extra veiligheidsmaatregelen niet in. Om deze overmoed te doorbreken, moet veilig gedrag de aandacht trekken en moeten de voordelen functioneel of emotioneel voelbaar worden gemaakt.	Mensen zijn sociale wezens en laten zich beïnvloeden door wat anderen in hun omgeving doen of geloven. Omdat veilig cybergedrag vaak onzichtbaar is, denkt ons brein onbewust dat 'niemand dit doet'. We moeten deze norm zichtbaar maken. Zet het sociale netwerk in om gedrag te veranderen.	Interventies zijn het meest effectief wanneer ze worden aangeboden op het juiste moment. Stimuleer het gedrag bij transities of directe beslismomenten. Dit verlaagt namelijk ook de inertia en verhoogt het ervaren nut .
• Standaardiseer het gedrag (defaults): Maak de veilige route de weg van de minste weerstand. Schakel 2FA automatisch in waar mogelijk en installeer wachtwoordmanagers vooraf op werklaptops. Stel de belangrijkste werksystemen standaard in als browser-bladwijzer en integreer opvallende eenkliks-meldknoppen om de melddrempel te minimaliseren. • Verminder frictie: Knip complexe handelingen op in kleine, behapbare stappen. Richt trainingen en handleidingen niet in op de theorie achter een tool, maar laat kort en krachtig zien hoe een gebruiker deze stapsgewijs activeert. • Verhoog frictie op onveilige routes: Ban actiesites en directe inloglinks in e-mails volledig uit. Door de onveilige handeling te blokkeren of te bemoeilijken, stuur je gebruikers automatisch richting het veilige alternatief (zelf naar de app of website navigeren).	• Doorbreek overmoed via ervaring (gamification): Alleen waarschuwen werkt niet. Zet interactieve realitychecks in, zoals phishingsimulaties met directe feedback of "zoek de verschillen"-quizen, om mensen aan den lijve te laten ervaren hoe snel ze misleid worden. • Frame de voordelen (gevoel van rust): Positioneer veiligheidstools positief. Verkoop een wachtwoordmanager niet als een 'verplichte beveiligingstaak', maar als een persoonlijke tool die mentale rust brengt en het onthouden van talloze wachtwoorden overbodig maakt. • Loss framing bij risico's: Benadruk bij handelingen expliciet wat men te verliezen heeft als men het gedrag niet uitvoert: van het leegroven van de eigen bankrekening tot het stilleggen van de gehele organisatie.	• Maak het gewenste gedrag of de trend daarvan zichtbaar: Communiceer met duidelijke, herkenbare boodschappen dat steeds meer mensen wél veilig handelen: "Steeds meer Nederlanders beveiligen hun belangrijkste accounts extra. Al meer dan de helft gebruikt 2FA. Doe jij ook mee?". • Social modeling en injunctieve norm: Laat binnen een organisatie het management expliciet optreden als rolmodel door openlijk te vertellen over hun eigen cyberfouten en welke maatregelen zij nemen. Beloon daarnaast meldingen van werknemers direct met actieve complimenten, om te laten zien dat alertheid enorm wordt gewaardeerd. • Zet in op 'zendingswerk': Activeer de sociale netwerken van consumenten en werknemers. Moedig hen aan om als cyberambassadeur op te treden en ook vrienden of familieleden te helpen met het instellen van 2FA of een wachtwoordmanager.	• Prompts op het beslismoment: Koppel herinneringen aan de feitelijke handeling. Toon bijvoorbeeld automatische waarschuwings-banners bij inkomende externe e-mails, waardoor de werknemer letterlijk twee seconden moet pauzeren om de afzender te scannen. • Gebruik bestaand momentum: Haak in op natuurlijke triggers. Krijgt een gebruiker bijvoorbeeld een melding om een wachtwoord te wijzigen vanwege een datalek? Koppel dit momentum dan direct aan de optie om meteen 2FA te activeren of makkelijk een veilig nieuw wachtwoord te genereren via een wachtwoordmanager. • Zet in op 'als-dan' routines: Help gebruikers nieuwe gewoontes te vormen. Leer hen een simpele regel aan om de foute klik-reflex te overschrijven: "Als een bericht mij vraagt om in te loggen, sluit ik de mail direct en open ik zélf mijn app of browser."

*Service, O., Hallsworth, M., Halpern, D., Algate, F., Gallagher, R., Nguyen, S., Ruda, S., Sanders, M., Pelenur, M., Gyani, A., Harper, H., Reinhard, J., & Kirkman, E. (2014). *EAST: Four simple ways to apply behavioural insights*. Behavioural Insights Team. https://www.bi.team/wp-content/uploads/2015/07/BIT-Publication-EAST_FA_WEB.pdf

Overige adviezen

Naast de specifieke EAST-adviezen zijn er ook een aantal meer hoogover adviezen:

1. **Verschuiving naar passkeys.** Experts geven aan dat het gewenst is om op den duur volledig te verschuiven naar passkeys (inloggen met bijvoorbeeld biometrie/gezicht in plaats van wachtwoorden) om de wachtwoordproblemen in de toekomst volledig op te lossen.
2. **Adviezen op maat.** In het ideale geval krijgen mensen adviezen op maat: gedragingen die passend zijn voor hun eigen positie op de cyberladder. Voor het thema waterbesparing is op basis van een rasch-analyse een online tool gemaakt die precies dat doet. Zie <https://waterweter.vitens.nl/>. Zo krijgen mensen geen adviezen aangereikt die nog veel te moeilijk voor ze zijn (gedragingen die ver boven hen op de ladder staan) of die ze allang uitvoeren (gedragingen die ver onder hen op de ladder staan).
3. **Data-gestuurde campagnes.** Scan op afstand op welke grote platforms gebruikers achterblijven qua bijvoorbeeld 2FA, om hen vervolgens specifiek en gericht een campagne te sturen.
4. **Integrale samenwerking.** Het stimuleren van cybergedragingen en het effectief opvolgen van meldgedrag reikt verder dan de grenzen van één individuele consument, werknemer of organisatie. Bovendien zenden marktpartijen soms verwarrende signalen uit. Om de impact van de gedragingen te maximaliseren, is een integrale ketensamenwerking noodzakelijk tussen publieke instanties, brancheverenigingen en grote marktpartijen. Door krachten te bundelen, kennis te delen, duidelijke normen en betrouwbare tools, bouwen we aan een landelijk veilig digitaal ecosysteem. Dit uit zich in:
 - **Landelijke campagnes:** Blijf benadrukken in campagnes en bedrijfsculturen dat melden nooit een probleem of fout is, en juist essentieel is om in te kunnen grijpen.
 - **Kennisdeling door grote partijen:** Grote organisaties (zoals banken en de Belastingdienst) beschikken over geavanceerde detectiesystemen om 'copycat'-websites en logomisbruik snel op te sporen. Zij zouden deze systemen (of de lessen daaruit) beschikbaar moeten stellen aan kleinere organisaties, zodat ook zij foute websites sneller kunnen melden. Partijen als Thuiswinkel zijn ook bezig met systemen om aangesloten leden proactief te monitoren op copycats en te helpen met collectieve *notice & takedown* verzoeken, zodat meldingen directer leiden tot het verwijderen van websites.
 - **Landelijke norm stellen:** Stimuleer organisaties om de expliciete afspraak met klanten te maken en uit te dragen in landelijke campagnes: *Wij sturen u nóóit berichten of mails met directe inloglinks*. Dit maakt zelf navigeren naar de officiële website of app de universele maatschappelijke norm.
 - **Domeinvermindering:** Dwing interne samenwerking in bedrijven af tussen security en marketing om de wildgroei aan domeinnamen en losse actiesites tegen te gaan. Elke organisatie zou idealiter maar 1 (of heel weinig) hoofddomein(en) moeten gebruiken, zodat de consument exact weet waar hij aan toe is.
 - **Actieve keurmerkverificatie (Thuiswinkel Waarborg):** Consumenten moeten niet simpelweg verteld worden dat ze naar een website moeten, maar moeten de instrumenten aangereikt krijgen om de echtheid te kunnen verifiëren (bijvoorbeeld het actief controleren of een certificaat of keurmerk echt is, en niet zomaar een gekopieerd 'jpeg' plaatje).

Toepassing op 4 kansrijke gedragingen

Om gedegen interventies te ontwikkelen, is het essentieel om op een select aantal doelgedragingen in te zetten. Anders is er weinig focus en is het lastig te achterhalen wat mogelijke effecten van een interventie zijn geweest. Op basis van de resultaten uit het vragenlijstonderzoek en een sessie met relevante experts en stakeholders hebben we de eerder geselecteerde gedragingen daarom afgebakend tot een top 4. Op deze vier kansrijke gedragingen hebben we het EAST model toegepast.

1. 2FA instellen en gebruiken
2. Wachtwoordmanager gebruiken
3. Officiële website gebruiken (in plaats van op links klikken)
4. Fout melden binnen de organisatie

Op de volgende pagina's wordt per gedrag uitgelicht waarom hiervoor gekozen is, in hoeverre het gedrag wordt uitgevoerd, wat de belangrijkste gedragsbepalers* zijn en wat ervoor nodig is om dit gedrag verder te stimuleren.

Interesse in een van de andere gedragingen uit cluster 1, diens gedragsbepalers en wat er nodig is om dit verder te stimuleren? Zie bijlage B: Toepassing op overige cybergedragingen.

De gedragsbepalers en adviezen voor de AI-gedragingen zijn exploratief onderzocht en hebben daarom een andere aard dan de rest van de gedragingen. De AI-gedragingen zijn opgenomen als apart deel in dit hoofdstuk na de uitwerking van de vier kansrijke gedragingen.

*Zie bijlage C voor een overzicht van alle gedragsbepalers die zijn meegenomen in het vragenlijstonderzoek. Dit is een lijst van gedragsbepalers die theoretisch een relatie kunnen hebben met de doelgedragingen. Op de volgende pagina's staan alleen de gedragsbepalers die als significante voorspellers van het gedrag naar voren kwamen in de data-analyse. Significants betekent dat die gedragsbepaler statistisch aantoonbaar een relatie heeft met het doelgedrag. De kans is zeer klein dat die relatie door toeval komt.

Belangrijke conclusies over de gedragsbepalers die relevant zijn voor de interventies.

Conclusie 1: Grote verschillen tussen belangrijkste bepalers voor consumenten en werknemers.

Er zijn enkele gedragsbepalers die voor zowel consumenten als werknemers gelden, maar ook een aantal bepalers die alleen voor een van beide groepen gelden. Beide behoeven dus een andere aanpak: andere gedragsbepalers behoeven immers andere gedragstechnieken en interventies. In de suggesties voor tactieken en technieken van elk gedrag staat aangegeven of een tactiek of techniek specifiek voor consumenten of werknemers is. Als dit er niet bij staat, is de tactiek toepasbaar op beide doelgroepen.

Conclusie 2: Verschillen tussen subgroepen.

De analyses laten zien dat sommige achtergrondkenmerken een significante rol spelen. Dit betekent dat er verschillen tussen subgroepen zijn. De achtergrondkenmerken leeftijd, geslacht, opleidingsniveau en stedelijkheid zijn voor sommige gedragingen voorspellend. Dat zou betekenen dat er een andere aanpak nodig is voor ouderen vs. jongeren, hoogopgeleiden vs. laagopgeleiden of stedelijke gebieden vs. minder stedelijke gebieden. In enkele tactieken en technieken is hier al kort aandacht aan gegeven. Extra onderzoek is nodig om te achterhalen of de gedragsbepalers ook per subgroep verschillen.

Disclaimer

Op de volgende pagina's en in Bijlage B staan er per gedrag adviezen en suggesties voor technieken om het gedrag verder te stimuleren onder consumenten en werknemers. Deze technieken voor interventies zijn gebaseerd op de significante gedragsbepalers die naar voren kwamen in de data-analyse en op wetenschappelijke gedragskennis. Zie het als suggesties vanuit de gedragswetenschappelijke bril. De technieken zijn niet getoetst door cybersecurity experts op haalbaarheid en uitvoerbaarheid.

2FA

16% van de consumenten gebruikt altijd 2FA, 32% van de werknemers doet dit altijd.

Om 2FA te stimuleren zijn de belangrijkste gedragsbepalers voor consumenten en werknemers:

- **Kennis en self-efficacy:** Wanneer iemand weet hoe hij 2FA kan aanzetten voor zijn accounts, gebruikt hij vaker 2FA. Ook wanneer iemand erop vertrouwt dat hij eventuele problemen met inlogcodes of verificatie-apps zelf kan oplossen, gebruikt hij vaker 2FA.
- **Descriptieve norm:** Wanneer iemand mensen in zijn omgeving (familie, vrienden, collega's) heeft die hun accounts met 2FA beveiligen, gebruiken ze vaker 2FA.
- **Overmoed:** Wanneer iemand vindt dat hij geen 2FA nodig heeft, omdat hij zelf al voorzichtig genoeg is online, gebruikt hij minder vaak 2FA. Mensen kunnen ook twijfelen over het risico: "Waarom ben ik interessant om gehackt te worden?".

Voor consumenten is ook **inertia** van invloed. Wanneer consumenten vinden dat het inloggen via 2FA veel tijd en moeite kost in het dagelijks gebruik, gebruiken ze minder vaak 2FA. Voor mensen die nog geen 2FA gebruiken, kan het instellen voelen als een gigantische klus.

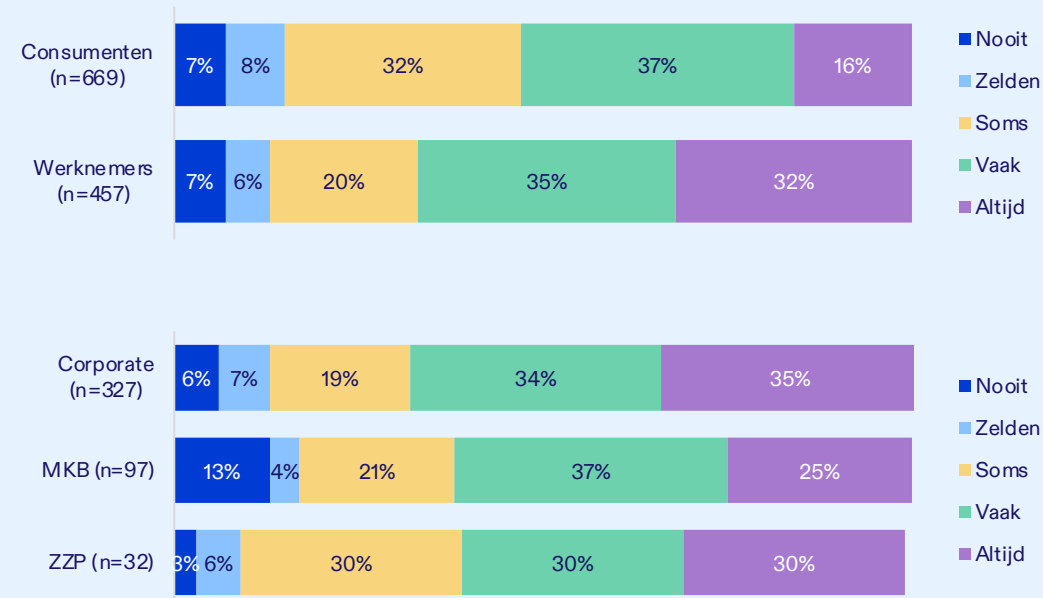
Een mogelijk technisch knelpunt is dat 2FA niet altijd ondersteund wordt door bepaalde systemen of apparaten. Een organisatie kan 2FA dus niet altijd voor iedereen verplicht stellen. Daarnaast kiezen consumenten bij webshops vaker voor (tijdelijke) gastaccounts in plaats van geregistreerde accounts, waardoor er geen ruimte is voor 2FA.

Ook speelt **leeftijd** en **opleidingsniveau** bij werknemers een rol. Oudere en hogeropgeleide werknemers gebruiken vaker 2FA dan jonge en lageropgeleide werknemers.

Daarnaast hebben werknemers die vaker 2FA gebruiken, meer **angst** om toegang tot hun werkaccounts te verliezen wanneer 2FA faalt.

Consumenten: Ik gebruik tweefactor authenticatie voor mijn privé-accounts (bijvoorbeeld e-mail, bankzaken of online shoppen).

Werknemers: Ik gebruik twee-factor authenticatie voor werk-accounts (bijvoorbeeld e-mail of administratiesystemen).



Hoe *stimuleren* we mensen om vaker *2FA* te gebruiken?

Tactiek 1: Kennis en self-efficacy verhogen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Gebruikers ontbreekt het zelden aan <i>theoretische</i> kennis over wat 2FA is, maar lopen vast op het gebrek aan <i>procedurele</i> kennis: de exacte, praktische stappen die nodig zijn om 2FA in te stellen en te gebruiken. Zo weet 59% van de consumenten en werknemers hoe ze 2FA moeten instellen en gebruiken. Daarnaast is er een gebrek aan <i>self-efficacy</i> (vertrouwen in eigen kunnen): consumenten en werknemers zijn bang dat ze het proces niet begrijpen, fouten maken of zichzelf definitief buitensluiten bij problemen (zoals een verloren telefoon). 55% van de consumenten en 52% van de werknemers twijfelt aan het eigen kunnen om problemen met 2FA op te lossen. Deze frictie en handelingsonzekerheid zorgen ervoor dat mensen afhaken voordat ze beginnen.	Er is een transitie nodig van abstracte theorie naar concrete, visuele en stapsgewijze instructies. Het handelingsperspectief moet laagdrempelig worden gemaakt en de angst voor accountblokkades moet vooraf worden weggenomen door herstelscenario's expliciet inzichtelijk te maken. Geef mensen het vertrouwen dat ze eventuele problemen zelf direct kunnen oplossen.	• Gidsen en herstelomgevingen: Bied korte walkthroughs (zoals <i>2FA op WhatsApp in 3 stappen</i>) die expliciet focussen op herstelopties (bijvoorbeeld back-upcodes). Dit verhoogt de self-efficacy door te bewijzen dat eventuele inlog- of synchronisatieproblemen eenvoudig zelf op te lossen zijn. • Simulaties: Bied een veilige, gesimuleerde testomgeving aan (bijvoorbeeld op Veiliginternetten.nl) waar gebruikers risicoloos kunnen oefenen met het invoeren van tokens. Dit bouwt zelfvertrouwen op zonder de vrees het eigen account te beschadigen. • Onboarding: Integreer korte video's of GIF's in de werk-onboarding of op het intranet. Dit visualiseert de exacte koppeling van de bedrijfsauthenticator, wat de drempel verlaagt en de procedurele kennis direct verhoogt.

Tactiek 2: Sociale norm activeren

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Mensen zijn sociale wezens en spiegelen hun gedrag aan hun directe omgeving (collega's, leidinggevendenden, familie en vrienden). Wanneer zij merken dat de norm verschuift naar 'veilig inloggen', activeren ze zelf ook eerder 2FA. Omdat de statische adoptiecijfers voor continue 2FA-gebruik momenteel nog relatief laag zijn (16% bij consumenten, 32% bij werknemers), werkt het communiceren van vaste percentages averechts omdat dit het onveilige gedrag kan normaliseren.	Het activeren van een dynamische norm (trendcommunicatie) die laat zien dat veilig inloggen de snelgroeiende standaard is. Daarnaast moet dit onzichtbare gedrag zichtbaar worden gemaakt op de werkvloer en in de privésfeer door ambassadeurs, spelelementen en rolmodellen in te zetten.	• Trendcommunicatie: Communiceer de stijgende beweging (<i>Steeds meer mensen beveiligen hun accounts extra: al meer dan de helft gebruikt 2FA</i>). Dit triggert het gevoel dat men niet achter mag blijven bij een positieve maatschappelijke trend. • Zendingswerk: Faciliteer deelmogelijkheden na activatie (<i>Ik heb mijn account extra beveiligd, help je omgeving ook</i>). Dit stimuleert actieve gebruikers om als sociale aanjager te fungeren binnen hun eigen netwerk. • Gamification: Zet een breed gedragen, interactieve checklist of spel in waarin gebruikers fysiek of digitaal kunnen aftikken voor welke applicaties ze 2FA hebben geactiveerd. Dit maakt het beveiligingsproces visueel en sociaal meetbaar. • Rolmodellen & afdelingsbenchmarks: Maak de adoptie per afdeling inzichtelijk (<i>85% van Finance logt al veilig in</i>) en laat leidinggevendenden expliciet uitdragen dat 2FA bij professioneel vakmanschap hoort. Dit activeert groepsdruk en stimuleert de sociale acceptatie.

Hoe *stimuleren* we mensen om vaker *2FA* te gebruiken?

Tactiek 3: Inertia verlagen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Inertia is een grote psychologische barrière. 30-31% van de mensen ervaren het instellen en het dagelijks herhalen van de extra inlogstap als een tijdrovende, ingewikkelde klus. Deze ervaren moeite leidt tot uitstelgedrag, waarbij het directe gemak wint van het langetermijnsrisico.	Het drastisch verlagen van de fysieke en cognitieve frictie. De veilige optie moet de weg van de minste weerstand worden gemaakt door automatische instellingen, stapsgewijze uitrol, naadloze authenticatie en het bieden van directe organisatorische hulp.	• Systeemveranderingen (defaults): Maak 2FA geen vrijwillige keuze, maar een verplichte standaardinstelling waar dit technisch mogelijk is. Denk ook aan push-notificaties of passkeys. Dit maakt inloggen met 2FA sneller en makkelijker dan een traditioneel wachtwoord. Of specifiek bij werknemers: reik tijdens onboarding hardware uit waarbij de 2FA-applicatie al is voorgeïnstalleerd en het activeringsproces de verplichte opstartstap is. • Kleine stapjes: Adviseer mensen om niet alles tegelijk te doen, maar te beginnen met de belangrijkste sleutel (<i>Start vandaag alleen met je e-mail</i>). Dit verlaagt de ervaren berg aan werk. • Aanhaken op kansrijke momenten: Koppel het instelmoment aan een al bestaande handeling of frictie, zoals een verplichte wachtwoordwijziging of datalek melding. Dit benut een actief leermoment. • Gefaciliteerde tijd op werk: Geef werknemers expliciet de tijd om 2FA in te stellen 'in de tijd van de baas' (bijvoorbeeld tijdens een weekstart). Dit neemt de frictie van ervaren werkdruk weg.

Tactiek 4: Overmoed verlagen en ervaren nut verhogen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Veel consumenten en werknemers lijden aan een controle-illusie en overmoed (<i>Ik ben online voorzichtig genoeg / Bij mij valt niets te halen</i>). Ze zien het nut van 2FA niet in, omdat ze denken dat hacks altijd het gevolg zijn van een eigen menselijke fout. Ze onderschatten de impact van datalekken bij derden en de kracht van geautomatiseerde inbraakpogingen. Zo vindt 16-17% 2FA niet nodig omdat ze zichzelf voorzichtig genoeg vinden en denkt slechts 48-49% denkt dat 2FA echt helpt tegen het voorkomen van hacks.	De controle-illusie moet worden ontkracht door aan te tonen dat risico's buiten de eigen invloedssfeer liggen. Het 'onzichtbare' nut van 2FA moet tastbaar en visueel worden gemaakt via simulaties, realtime cijfers en directe feedback na incidenten.	• Concreet maken en visualisaties: Verhoog het ervaren nut door het nut concreet te maken en te visualiseren. • Kanteling van de controle-illusie: Communiceer dat voorzichtigheid niet helpt als een externe webshop lekt (<i>Je wachtwoord ligt op straat door een datalek; 2FA is het enige slot dat je account dan nog beschermt</i>). • Laten ervaren en demonstratie van risico en nut: Toon hoe automatische bots duizenden wachtwoordcombinaties per seconde testen. Dit bewijst dat menselijke oplettendheid alleen onvoldoende is en 2FA een noodzakelijk filter. Of demonstreer hoe snel een computer een menselijk bedacht wachtwoord kraakt, afgezet tegen de ondoordringbaarheid van een 2FA-laag. Dit verlaagt de overmoed in het eigen wachtwoord. Of laat via een interactieve check de domino-impact zien van een gehackte e-mail (toegang tot webshops, financiën en overheid). Dit maakt het financiële en persoonlijke afbreukrisico voelbaar. • Visualisatie van geblokeerde inbraakpogingen: Deel maandelijks cijfers over het aantal inlogpogingen dat door 2FA succesvol is afgeweerd binnen de organisatie. Dit maakt het effect van de maatregel direct zichtbaar. • Direct advies na incidenten & phishing-simulaties: Bied slachtoffers van fraude direct 2FA aan als dé oplossing om herhaling te voorkomen. Geef na interne phishingtests de feedback dat 2FA de ultieme achtervanger is, zelfs als men per ongeluk op een link klikt.

Wachtwoordmanager

Momenteel gebruiken nog maar weinig mensen altijd een wachtwoordmanager: 20% van consumenten, 13% van werknemers. Wachtwoordmanagers kunnen een belangrijk hulpmiddel en een 'traprede' zijn naar algemeen veilig gedrag. Een manager neemt veel moeite weg bij de eindgebruiker, wat de stap om 2FA in te stellen aanzienlijk kleiner maakt. Bovendien helpt de manager de gebruiker direct als deze betrokken is bij een datalek, door te assisteren bij het genereren van een nieuw, sterk wachtwoord. Door dit te stimuleren, wordt de inspanning voor criminelen om accounts te hacken direct een stuk lastiger.

Om wachtwoordmanagers te stimuleren zijn de belangrijkste gedragsbepalers voor consumenten en werknemers:

- **Kennis:** Mensen die weten hoe ze een wachtwoordmanager moeten gebruiken, hebben vaker een wachtwoordmanager.
- **Descriptieve norm:** Wanneer iemand mensen in zijn omgeving (familie, vrienden, collega's) heeft die een wachtwoordmanager hebben, gebruiken ze vaker zelf ook een wachtwoordmanager.
- **Rust:** Wanneer iemand ervaart dat een wachtwoordmanager hem rust in zijn hoofd geeft, omdat hij niet langer tientallen unieke inloggegevens zelf hoeft te onthouden, gebruikt hij vaker een wachtwoordmanager.

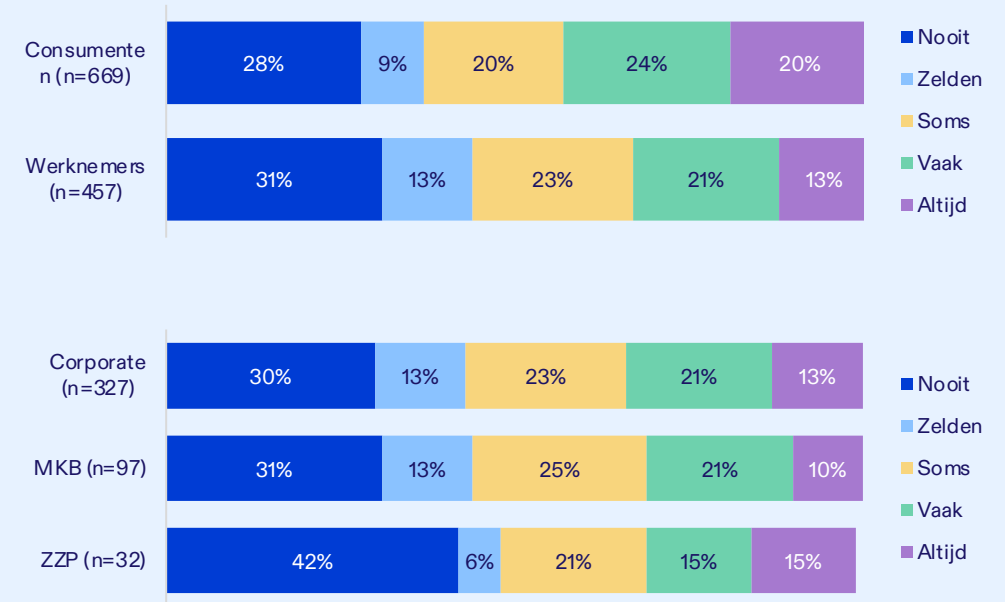
Voor consumenten spelen **angsten** ook een rol. Wanneer ze bang zijn dat ze nergens meer bij kunnen als ze het hoofdwachtwoord van de kluis vergeten of het riskant vinden om al hun wachtwoorden op één centrale plek op te slaan, gebruiken ze minder vaak een wachtwoordmanager.

Voor werknemers speelt de **default** ook een rol. Werknemers die aangeven vooral gebruik te maken van een wachtwoordmanager als deze standaard is ingebouwd in de webbrowser of werktelefoon, maken vaker gebruik van een wachtwoordmanager.

Ook speelt **stedelijkheid** bij werknemers een rol. Mensen uit stedelijke gebieden hebben minder vaak een wachtwoordmanager dan mensen uit minder stedelijke gebieden.

Consumenten: Ik gebruik een wachtwoordmanager voor mijn persoonlijke online accounts (zoals e-mail, sociale media of bankieren).

Werknemers: Ik gebruik een wachtwoordmanager voor mijn online werkaccounts (zoals e-mail, agenda of administratiesystemen).



Hoe *stimuleren* we mensen om vaker *een wachtwoordmanager* te gebruiken?

Tactiek 1: De sociale norm activeren

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Wachtwoordbeheer is van nature een 'onzichtbaar' digitaal gedrag dat zich afspeelt achter gesloten schermen. Omdat consumenten en werknemers niet zien dat hun familie, vrienden of collega's gebruikmaken van een wachtwoordmanager, ontbreekt een duidelijke sociale norm (30-31% denkt dat anderen een wachtwoordmanager gebruiken). Zonder de visuele bevestiging dat de omgeving massaal overstapt, ontbreekt de sociale stimulans en de groepsdruk om zelf het initiatief te nemen.	Het onzichtbare gebruik van wachtwoordmanagers expliciet zichtbaar en bespreekbaar maken binnen sociale netwerken, gezinnen en werkteams. Door het gebruik sociaal te normeren en actieve gebruikers in te zetten als ambassadeurs, wordt het overstappen op een wachtwoordkuis neergezet als de maatschappelijke en professionele standaard.	• Zendingswerk: Faciliteer gezins- en netwerkactivatie met een directe 1-klik uitnodiging na activatie (<i>Houd je gezin veilig: deel je digitale sleutelkuis gratis met je partner of kinderen</i>). Dit zet actieve gebruikers direct om in sociale ambassadeurs. • Gamification: Maak de adoptiegraad per team openlijk zichtbaar op het intranet (<i>85% van Marketing logt al veilig in!</i>) en beloon afdelingen die hoge scores behalen. Dit activeert een gezonde competitie en versterkt de descriptieve norm op de werkvloer. Let op: werk met trends als de huidige norm nog heel laag is, wat vaak het geval is bij wachtwoordmanagers. • Rolmodellen: Wijs binnen teams directe collega's aan (geen IT-experts) die in korte meetings van 1 minuut laten zien hoe zij een wachtwoordmanager gebruiken om sneller te werken. Dit creëert herkenbare en geloofwaardige rolmodellen.

Tactiek 2: Het gevoel van rust verhogen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Het ervaren van mentale rust (het niet langer hoeven onthouden van tientallen unieke, complexe wachtwoorden) is een positieve drijfveer voor het gebruik van een wachtwoordmanager. Veel traditionele beveiligingsmaatregelen stuiten op weerstand omdat ze extra denkwerk vragen. Als een tool wordt geassocieerd met 'meer gedoe en risico's', haken mensen af. 54% van de consumenten en 48% van de werknemers verwacht rust in het hoofd door het gebruik van een wachtwoordmanager.	De positionering van de wachtwoordmanager moet om: weg van angstige risicocommunicatie en focus op gemak, stressreductie en cognitieve ontlasting. De tool moet in de beeldvorming transformeren van een 'technisch beveiligingsinstrument' naar een 'productiviteits- en comfortool' voor een drukke werk- en privédag.	• Campagnes ('Rust in je hoofd'): Positioneer de tool in publiekscampagnes puur op mentale ontlasting (<i>Nooit meer wachtwoorden onthouden, geef je brein rust</i>), en benadruk dat een wachtwoordmanager ook direct helpt bij het zorgeloos aanmaken van een nieuw wachtwoord na een datalek. • Visualisatie van frictie vs. gemak: Zet de herkenbare frustratie van een 'wachtwoord onjuist'-melding af tegen het relaxte inloggen in 1 seconde via biometrie (vingerafdruk). Koppel dit aan een gevoel van rust (<i>Je onthoudt 150 telefoonnummers toch ook niet uit je hoofd?</i>). • Associatie met gemak: Richt interne werkcommunicatie op de directe besparing van tijd en inlogstress (<i>Begin je maandag frictieloos: log 1 keer in en al je systemen staan direct open. Geen IT-resets meer tijdens strakke deadlines</i>).

Hoe *stimuleren* we mensen om vaker *een wachtwoordmanager* te gebruiken?

Tactiek 3: Kennis verhogen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Consumenten en werknemers weten theoretisch wel dat wachtwoordmanagers bestaan, maar ze missen vaak de <i>procedurele kennis</i> (55-58% weet hoe ze een wachtwoordmanager moeten gebruiken): hoe installeer je de tool, hoe sla je een nieuw wachtwoord op, en hoe werkt het automatisch invullen van inloggegevens op een telefoon of laptop? Zonder deze praktische vaardigheden voelt de stap om te beginnen te ingewikkeld.	Er is een transitie nodig van abstracte cybersecurity-theorie naar concrete, visuele en stapsgewijze instructies. De drempel om de tool in te richten moet zo laag mogelijk worden gemaakt door de basisfunctionaliteiten (zoals opslaan en automatisch invullen) direct in de praktijk aan te leren en te faciliteren.	• Stapsgewijze interactieve gidsen: Bied korte visuele walkthroughs, GIF's of video-instructies van maximaal 1 minuut (<i>Zo sla je in 3 stappen je eerste wachtwoord op</i>). Dit bouwt de procedurele kennis stapsgewijs op zonder dat de gebruiker wordt overweldigd. • Systeemveranderingen (defaults): Zet bij werknemers de kluis-extensie standaard geïnstalleerd klaar in de browser via het IT-groepsbeleid, of wijs consumenten op reeds ingebouwde apparaat-defaults (zoals Apple Sleutelhanger of Google Wachtwoordbeheer). Dit neemt de technische installatiehorde weg. Zie ook tactiek 5. Dan is minder procedurele kennis nodig om er gebruik van te maken. • Team- en gezinsonboarding: Organiseer korte, informele momenten waarop collega's of gezinsleden samen de kluis activeren onder begeleiding van een 'buddy'. Dit maakt het aanleerkunnen van de vaardigheden een begeleide, sociale ervaring.

Tactiek 4: Angsten verkleinen en ervaren nut verhogen (voor consumenten)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Bij consumenten spelen specifieke angsten een remmende rol. Ten eerste is er de angst om buitengesloten te raken (37-41% heeft deze angst), wat wijst op een gebrek aan self-efficacy bij herstelscenario's. Ten tweede voelt het onveilig om alle wachtwoorden op één centrale plek op te slaan (44-51% heeft deze angst). Deze angsten blokkeren het gebruik, zelfs als men de voordelen van een wachtwoordkluis wel inziet.	Het expliciet wegnemen en ontcrachten van deze angsten door transparante herstelprocedures te tonen (het verhogen van de self-efficacy bij noodsituaties) en het verduidelijken dat een versleutelde kluis vele malen veiliger is dan het alternatief (hergebruikte of zwakke wachtwoorden). Het gaat dus ook om het herdefiniëren van het ervaren nut en de effectiviteit van de maatregel.	• Hersteligidsen en simulaties: Bied expliciete instructies en korte demonstraties over het herstelproces (<i>Hoofdwachtwoord vergeten? Zo werken nood-herstelcodes of familie-toegang</i>). Het vooraf inzichtelijk maken van deze opvangnetten neemt de angst voor definitieve accountblokkades weg. • Biometrische koppeling (koppelen aan gewoontes): Adviseer consumenten om de kluis direct te koppelen aan FaceID of een vingerafdruk op hun smartphone. Dit verlaagt de angst om een hoofdwachtwoord te moeten onthouden, omdat de dagelijkse toegang via vertrouwde biometrie verloopt. • Reframing: Gebruik begrijpelijke vergelijkingen in campagnes om de risicoperceptie te herkalibreren (<i>Tien accounts met hetzelfde wachtwoord is alsof je één sleutel gebruikt voor je huis, auto én kluis. Een versleutelde wachtwoordmanager is als een professionele bankkluis met unieke, onkraakbare sleutels</i>). Dit laat zien dat verspreid hergebruik in werkelijkheid het grootste risico vormt. • Veiligheids garanties: Zet onafhankelijke experts (zoals de Consumentenbond of Veiliginternetten.nl) in die expliciet garanderen dat gecertificeerde wachtwoordmanagers de veiligste keuze zijn. Dit biedt de consument het nodige externe vertrouwen om de stap te durven zetten. • Simulatie: Organiseer korte live-demonstraties waarin een ethische hacker toont hoe snel eenvoudige of hergebruikte wachtwoorden worden gekraakt, afgezet tegen de ondoordringbaarheid en automatische phishing-blokkade van de gegenereerde wachtwoorden van een wachtwoordmanager.

Hoe *stimuleren* we mensen om vaker *een wachtwoordmanager* te gebruiken?

Tactiek 5: Defaults inzetten en inertia verlagen (voor werknemers)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
31% van de werknemers ervaart inertia bij wachtwoordmanagers. Mensen kunnen het overstappen zien als een intimiderende, uren durende klus, omdat ze denken dat ze al hun bestaande wachtwoorden handmatig moeten opzoeken en invoeren. Deze opstartfrictie blokkeert het voorgenomen gedrag.	De opstartdrempel drastisch verlagen door de omgeving aan te passen, aan te haken bij bestaande defaults op apparaten, het installatieproces via IT over te nemen en het invoeren te herformuleren naar een moeiteloze, stapsgewijze en gefaciliteerde ervaring.	• Systeemveranderingen (defaults & pre-installatie): Wijs mensen op wachtwoordmanagers die al ingebouwd zijn op bepaalde apparaten (Apple Sleutelhanger, Google Wachtwoordbeheer) en geef apparaat-specifieke "2-klikken handleidingen" hiervoor. Laat IT voor werknemers de browser-extensie (bijv. 1Password of LastPass) vooraf installeren, zodat de tool direct klaarstaat in de browserbalk. • Buddysystemen (onboarding): Organiseer korte sessies waarin collega's onder het genot van koffie samen de manager activeren en hun eerste account opslaan, ondersteund door een 'onboarding buddy' of IT-collega die eventuele twijfels direct wegneemt.

Officiële website

De gemiddelde klant begrijpt niet hoe een URL is opgebouwd (bijvoorbeeld het verschil tussen rabobank.helpdesk.nl en rabobank.nl). Zelfs goed getrainde mensen zien dit soort subtiele verschillen over het hoofd. Daarnaast zorgen de verschuiving naar mobiel internetten en apps, de komst van misleidende social media advertenties, en de opkomst van AI ervoor dat het beoordelen van een link vrijwel onbegonnen werk is. Het gebruiken van de officiële website is daarom een beter alternatief. Zo'n 31% van de consumenten en 21% van de werknemers gaat al altijd naar de officiële website.

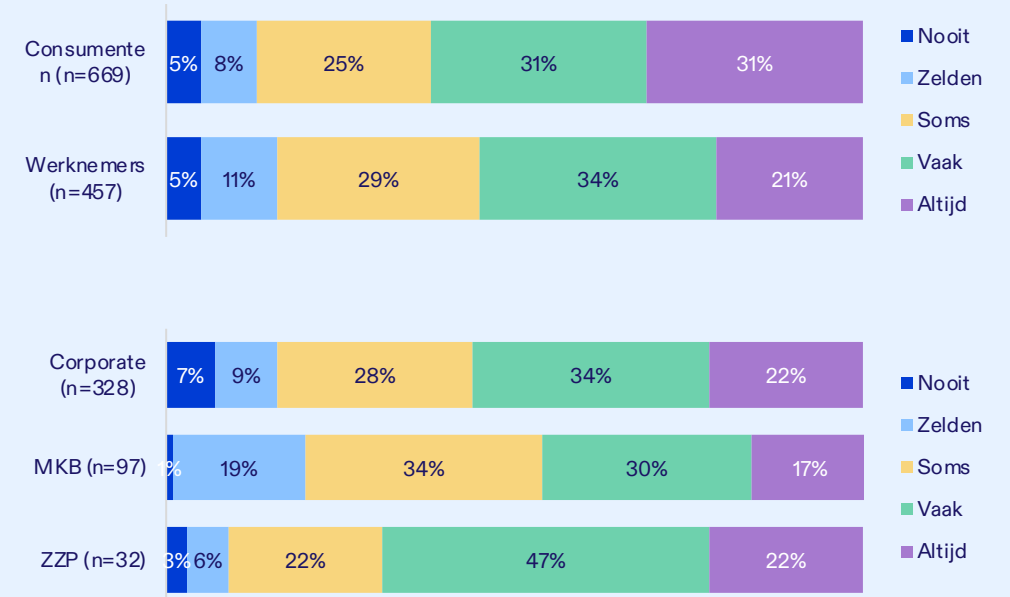
Om het gebruiken van de officiële website te stimuleren zijn de belangrijkste gedragsbepalers voor consumenten en werknemers:

- **Inertia:** Hoe meer moeite consumenten en werknemers het vinden kosten om onbekende mails goed te controleren, hoe minder vaak ze de officiële website gebruiken. Op een link in een mail klikken kost 1 klik (weinig moeite). Een nieuwe tab openen, de URL intypen, de inlogpagina zoeken en inloggen kost 5 tot 10 handelingen (veel moeite). Hoe meer moeite werknemers het vinden kosten om een cyberfout te melden via de systemen, hoe vaker ze de officiële website gebruiken. Mogelijk doen ze dit dus om de rompslomp van een foutmelding achteraf te voorkomen.

Voor consumenten is ook **ervaren nut** van invloed. Hoe sterker iemand denkt de kans op oplichting te verkleinen door een e-mail goed te controleren, hoe minder vaak diegene naar de officiële website gaat. Mogelijk denken dat ze phishingberichten zelf wel kunnen spotten, waardoor ze de officiële route onnodig vinden.

Bij consumenten speelt **leeftijd** en **opleidingsniveau** ook een rol. Oudere consumenten gebruiken officiële websites vaker dan jongere consumenten. Laagopgeleiden gebruiken minder vaak de officiële website dan anders opgeleiden.

Ik ga zelf naar de officiële website of app in plaats van dat ik een link uit de e-mail gebruik.



Hoe *stimuleren* we mensen om vaker *de officiële website* te gebruiken?

Tactiek 1: Inertia verlagen

Achtergrond

Het handmatig navigeren naar een officiële website of app (in plaats van direct doorklikken op een link) vraagt meer gedoe en kost meer moeite. Zolang het veilige alternatief meer tijd en cognitieve moeite kost dan de onveilige link, wint de luie klik-reflex het van het veilige gedrag.

Wat is er nodig?

De frictie voor de veilige route moet drastisch worden verlaagd zodat zelf navigeren even snel en moeiteloos wordt als het klikken op een link. Dit vraagt om het wegnemen van de klik-mogelijkheid bij de bron (beleid), het faciliteren van 1-klik alternatieven (zoals vooringestelde bladwijzers en mobiele apps), en het automatiseren van de besluitvorming via vaste gedragsregels.

Voorbeelden van technieken

- **Beleid “geen inloglinks in mails”:** Organisaties (zoals banken, overheid en werkgevers) zouden moeten stoppen met het opnemen van directe inloglinks in hun e-mails en communiceren hier transparant over (*Wij sturen nooit directe inloglinks*). Dit haalt de verleiding en mogelijkheid om te klikken weg, maakt het ontbreken van links de standaard (default), en stimuleert het verifiëren van alternatieve echtheidskenmerken (zoals een Thuiswinkel Waarborg).
- **Systeemveranderingen en defaults:** Maak het gedrag makkelijker door systeemveranderingen en automatiseringen.
 - **Bladwijzers en favorieten:** Vraag consumenten actief om favorieten aan te maken of vast te pinnen voor veelgebruikte diensten (zoals banken, MijnOverheid en PostNL). Bij werknemers stelt de IT-afdeling belangrijke portalen vooraf in als bladwijzer in de browser. Hierdoor kost zelf navigeren slechts 1 klik op de favorietenbalk.
 - **Open app-eerst:** Promoot het direct openen van de smartphone-app via FaceID of vingerafdruk als sneller alternatief voor doorklikken in een mail (*Krijg je een mail of SMS van PostNL, je bank of de overheid? Klik niet, maar open direct de app op je telefoon*).
 - **Automatische waarschuwingshints:** Laat bij externe e-mails met urgentiewoorden automatisch een gele waarschuwingbanner en een gerichte navigatietip verschijnen (🔔 *Open direct het interne portaal om deze factuur te controleren*), wat de luie reflex doorbreekt en direct het veilige alternatief aanreikt.
- **Als-dan plannen:** Automatiseer het besluitvormingsproces door consumenten en werknemers een vaste ‘als-dan’ regel aan te leren: *Als een e-mail mij vraagt om ergens in te loggen, dán sluit ik de mail en open ik mijn eigen browser of app*. Dit haalt de mentale risico-afweging weg en verlaagt de cognitieve inertia.

Hoe *stimuleren* we mensen om vaker *de officiële website* te gebruiken?

Tactiek 2: Ervaren nut verhogen (voor consumenten)

Achtergrond

Hoe sterker consumenten geloven dat zij nep-mails zelf kunnen herkennen (bijvoorbeeld aan het logo, de opmaak of de schrijfstijl), hoe minder snel zij uit zichzelf naar de officiële website of app navigeren. 66% van de consumenten vertrouwd erop nepmails zelf te herkennen. Deze overmoed leidt tot valse risicoperceptie: consumenten denken dat ze phishingberichten prima kunnen spotten, waardoor ze de extra beveiligingsstap van handmatig navigeren als overbodig of "onnodig gedoe" beschouwen.

Wat is er nodig?

De controle-illusie moet actief worden doorbroken. Argumenten alleen volstaan niet bij overmoedige gebruikers; zij moeten de onbetrouwbaarheid van hun eigen visuele inspectie daadwerkelijk ervaren. Er is een confrontatie nodig met de huidige werkelijkheid (waarin AI visueel identieke nep-mails genereert), gecombineerd met instrumenten die aantonen dat handmatig navigeren naar de officiële site of app de enige 100% sluitende beveiliging is.

Voorbeelden van technieken

- **Zelfovertuiging:** Ontwikkel publiciteitscampagnes die consumenten niet beleren, maar vragen stellen die hen dwingen hun eigen gedragingen in twijfel te trekken (*Als een oplichter AI gebruikt om een e-mail taalkundig foutloos en met het juiste logo te schrijven, hoe zie je dan nog het verschil met een echte mail?*). Consumenten overtuigen zichzelf dat een visuele check onbetrouwbaar is en dat zelf navigeren noodzakelijk is.
- **Gamification (laten ervaren):** Bied een korte online quiz aan waarin gebruikers binnen 3 seconden echte e-mails moeten onderscheiden van visueel identieke AI-copycats. Bij een fout volgt direct een confronterende boodschap: *Zelfs de scherpste controleurs worden door AI misleid. Kies voor 100% zekerheid: open direct de officiële app of typ zelf de URL in.*
- **Loss framing:** Benadruk in communicatie expliciet wat men te verliezen heeft als men vertrouwt op eigen visuele checks (*Eén haastige klik op een link kan je bankrekening binnen 5 seconden leegtrekken. Voorkom dit verlies: typ altijd zelf de officiële website in of open direct de app*). Dit verhoogt de gepercipieerde ernst van blind vertrouwen op e-maillinks.
- **Verificatie-instrumenten:** Bied actieve tools aan waarmee consumenten de echtheid van keurmerken (zoals het Thuiswinkel Waarborg) daadwerkelijk kunnen verifiëren, in plaats van dat zij blind vertrouwen op een statisch en makkelijk te kopiëren logo in de e-mail.

Fout melden

In het vragenlijstonderzoek kwam naar voren dat slechts 33% van de werknemers altijd een fout meldt, terwijl dit niet doen aanzienlijke gevolgen kan hebben. Idealiter wordt er niet alleen ingezet op melden binnen een organisatie, maar ook op melden door consumenten, bijvoorbeeld van frauduleuze websites. Een foutmelding van een werknemer of consument is een belangrijk signaal om direct actie te kunnen ondernemen. Zonder deze meldingen kunnen organisaties (zoals de Fraudehulpdesk of webshops) en de politie malafide domeinen niet offline halen of blokkeren.

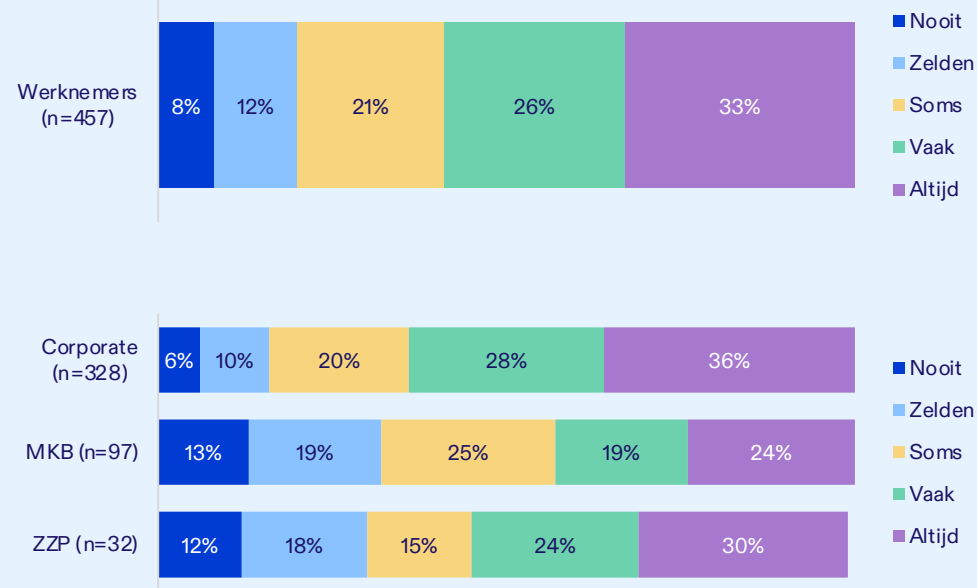
Om het melden van fouten te stimuleren zijn de belangrijkste gedragsbepalers voor werknemers:

- **Injunctieve norm:** Wanneer een werknemer denkt dat het melden van een mogelijke beveiligingsfout wordt gewaardeerd binnen de organisatie, melden zij vaker fouten.
- **Self-efficacy:** Wanneer een werknemer zich in staat voelt om een cyberfout te melden, melden zij vaker fouten.

Andere knelpunten zijn dat er in de maatschappij sprake is van 'meldmoeheid', waar in communicatie of interventies rekening mee gehouden moet worden. Mensen moeten al voor veel verschillende online of interne problemen een melding maken, waardoor het melden van een cyberfout als een extra, tijdrovende administratieve drempel wordt gezien. Daarnaast zijn werknemers soms benauwd of bang om te melden wanneer ze op een foute link hebben geklikt. Uit paniek zetten ze soms alles uit en gaan ze weg, wat de schade (bijvoorbeeld bij ransomware) juist vergroot. Er is ook een link met angst voor negatieve gevolgen in onze data: Mensen die vaker fouten hebben gemeld, zijn vaker bang dat het melden van een cyberfout negatieve gevolgen heeft voor hun loopbaan. Mogelijk komt dit door ervaring: ze hebben al eens een cyberfout gemeld en daar is negatief op gereageerd.

Ook speelt **leeftijd** en **opleidingsniveau** bij werknemers een rol. Oudere werknemers melden vaker een fout dan jongere werknemers. Laagopgeleiden melden minder vaak een fout dan anders opgeleiden.

Als ik iets doe waar ik later over twijfel, bijvoorbeeld op een link klikken die ik achteraf niet vertrouw, meld ik dit bij mijn organisatie (zoals IT-support of security-officer).



Hoe *stimuleren* we mensen om vaker *fouten te melden*?

Tactiek 1: Psychologische veiligheid en waardering cultiveren

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Het melden van een eigen gemaakte fout (zoals het doorklikken op een verdachte link) vraagt om kwetsbaarheid en het nemen van een sociaal risico. Werknemers worden hierin vaak geremd door angst voor negatieve loopbaanconsequenties, vrees voor straf of afkeuring vanuit de leiding, en schaamte over de gemaakte fout. Wanneer er binnen een organisatie geen expliciete sfeer van psychologische veiligheid heerst, wint de menselijke reflex om een incident te verzwijgen of voor zich uit te schuiven. 19% van de werknemers bang dat melden negatieve gevolgen voor ze heeft.	Er is een actieve cultuurverandering nodig waarin de spanning rondom het maken van cyberfouten proactief wordt weggenomen. De leiding moet expliciet communiceren dat fouten maken menselijk is en dat het direct melden van een fout juist als een uiting van vakmanschap en verantwoordelijkheid wordt gewaardeerd. Melden moet worden geherkaderd van een 'schuld bekentenis' naar een 'waardevolle beschermingsactie voor het bedrijf'.	• Complimenten: Beloon werknemers direct na een melding met complimenten of punten (gamification). Zorg dat de IT-servicedesk reageert met een enthousiaste reactie (<i>Scherp opgemerkt! Dankzij jouw snelle melding konden we direct ingrijpen</i>) in plaats van een droog ticketnummer. Dit versterkt het positieve zelfbeeld en bouwt vertrouwen op in het meldproces. • Social modelling: Zet leidinggevenden, ervaren collega's en ouder personeel (die al vaker melden) in als rolmodel. Laat hen openlijk vertellen over hun eigen digitale missers en hoe ze dit hebben opgelost. Dit normaliseert het maken én melden van fouten op de werkvloer. • Weerstand erkennen: Benoem als organisatie proactief de drempel en angst om te melden (<i>We weten dat het spannend kan zijn om toe te geven dat je op een verkeerde link hebt geklikt...</i>) en ontkracht deze direct. Dit neemt de schaamte en spanning op het kritieke moment weg. • Awareness-training: Zet phishing-simulaties in waarbij het rapporteren van verdachte mails actief in gang wordt gezet. Benadruk tijdens deze trainingen dat melden altijd wordt gewaardeerd, zelfs als er per ongeluk al schade (zoals ransomware) is veroorzaakt.

Tactiek 2: Self-efficacy verhogen en moeite minimaliseren

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Het niet-melden van cyberfouten wordt gedreven door een lage self-efficacy (33% twijfelt over het eigen kunnen om een fout goed te melden). Dit kan samenhangen met inertia (19% vindt het melden van fouten moeite kosten). Daarnaast kan acute paniek op het moment dat een fout optreedt zorgen voor handelingsverlamming, terwijl ingewikkelde formulieren leiden tot meldmoeite.	Het meldproces moet volledig worden gestript van bureaucratie, lange formulieren en ingewikkelde stappen. Instructies moeten voor iedereen toegankelijk zijn door het hanteren van B1-taalniveau en visuele ondersteuning. Daarnaast moet het handelingsperspectief op het moment van de fout vooraf zijn geautomatiseerd, zodat werknemers zonder frictie direct kunnen handelen.	• Makkelijk maken: Integreer een opvallende rapportageknop direct in de e-mailomgeving (zoals Outlook). Dit brengt de handeling terug tot exact één klik, omzeilt ingewikkelde IT-procedures en minimaliseert de fysieke en cognitieve drempel voor de gehele werkvloer. • Duidelijke stappen (B1-niveau & visuele gidsen): Schrijf alle instructies, beleidsteksten en e-learnings op eenvoudig taalniveau B1 en vermijd technisch jargon. Ondersteun dit met visuele stappenplannen, zodat iedere werknemer precies weet welke actie verwacht wordt en de self-efficacy toeneemt. • Als-dan plannen: Formuleer concrete 'als-dan' regels voor werknemers om het juiste gedrag bij paniek te automatiseren (<i>Als ik merk dat ik op een link heb geklikt die ik achteraf niet vertrouw, dán klik ik direct op de meldknop in Outlook</i>). Dit neemt besluitfrictie op het moment van de fout weg en zet voorgenomen gedrag om in een automatische reactie.

Resultaten en interventies *rondom AI*

Voor de vier kansrijke gedragingen kon het EAST-model direct worden toegepast: er is één veilige route en de vraag is alleen hoe we mensen daarheen krijgen. Bij AI ligt dat anders. Daarom staan de AI-resultaten apart van cluster 1 en 2.

Er is geen eenduidig gewenst gedrag bij AI

Informatie delen met AI is niet per definitie onveilig. Of het risicovol is, hangt af van wát iemand deelt, met welke tool en in welke context, en dat hebben we niet in detail uitgevraagd (zie de kanttekeningen op pagina 15). Bij 2FA instellen of een melding maken is de veilige handeling wel eenduidig. De vier kansrijke gedragingen zijn bovendien geselecteerd via de Rasch-analyse op de Alert Online 2025 data: ze staan op de gedragsladder, op het niveau waar de doelgroep zich bevindt. De AI-gedragingen waren eerder nog niet meegenomen in het jaarlijkse Alert Online onderzoek en werden in het huidige onderzoek dus vooral exploratief meegenomen.

De gedragsbepalers voor AI wijzen een andere kant op

Bij cluster 1 en 2 verklaren kennis, sociale norm, ervaren nut en inertia waarom veilig gedrag uitblijft: het kost moeite en levert niets zichtbaars op. Bij AI is het gedrag juist aantrekkelijk. Hier zijn leeftijd, de frequentie van AI-gebruik, het ervaren van AI als empathisch en de ervaren kwaliteit en tijdwinst de voorspellers, en bij werknemers de angst voor negatieve loopbaangevolgen als ze géén AI gebruiken. Waar we bij cluster 1 en 2 een drempel moeten wegnemen, moeten we bij AI juist een rem inbouwen. Dat vraagt andere technieken.

Op de volgende slides laten we per AI-gedraging zien hoeveel mensen het doen en welke gedragsbepalers opvallen. We geven hier geen tactieken per gedrag, maar hoog-over adviezen voor veilig AI-gebruik en het tegengaan van shadow AI.



Emoties delen met AI

50% van de consumenten deelt nooit emoties met AI, 43% van de werknemers doet dit nooit.

De belangrijkste gedragsbepalers die het delen van emoties met AI voorspellen bij consumenten en werknemers zijn:

- **AI empathisch vinden:** Hoe empathischer iemand AI vindt, hoe vaker diegene emoties deelt met AI.

Daarnaast is voor consumenten de volgende gedragsbepaler van invloed:

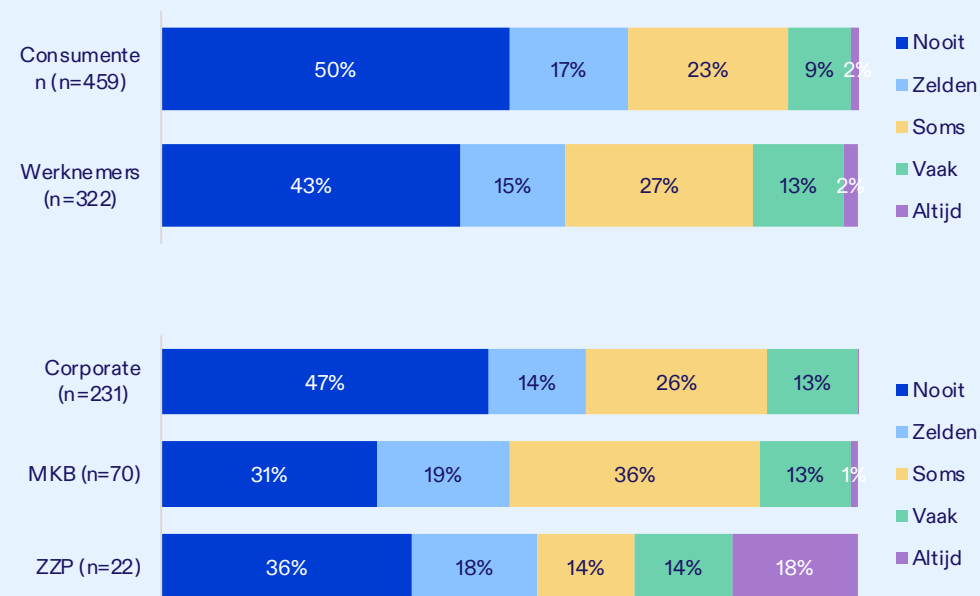
- **Afhankelijkheid:** Wanneer consumenten niet meer zonder AI zouden kunnen in het dagelijkse leven, delen zij vaker emoties met AI.

Voor werknemers zijn de volgende gedragsbepalers ook van invloed:

- **Kwaliteit:** Wanneer werknemers de productiviteitsverhoging door AI zo groot vinden dat ze eventuele risico's voor de organisatie acceptabel vinden, delen ze vaker emoties met AI.
- **Aanbieder vertrouwen:** Werknemers die erop vertrouwen dat de aanbieder van de AI-tool eerlijk en oprecht is over hoe de data van de organisatie wordt gebruikt, delen vaker emoties met AI.
- **Veilig:** Werknemers die er alle vertrouwen in hebben dat ze AI-tools veilig kunnen gebruiken zonder de veiligheidsregels van hun organisatie te overtreden, delen vaker emoties met AI.
- **Angst gevolgen als geen AI:** Werknemers die bang zijn hun baan of reputatie in gevaar te brengen als ze geen AI gebruiken, delen vaker emoties met AI.
- **Bestaande tools zijn voldoende:** Werknemers die vinden dat de officiële AI-tools binnen hun organisatie voldoen aan hun behoeften, delen minder vaak emoties met AI.

Bij consumenten en werknemers spelen **leeftijd** en **frequentie** ook een rol en bij werknemers ook **opleidingsniveau**. Oudere mensen delen minder vaak emoties met AI dan jongere. Hoe vaker iemand AI gebruikt, hoe minder vaak ze emoties delen met AI. Laagopgeleide werknemers delen vaker emoties met AI dan anders opgeleide werknemers.

In hoeverre deel jij de volgende soorten persoonlijke informatie met AI: Persoonlijke emoties, zorgen of gevoelens.



Documenten delen met AI

48% van de consumenten deelt nooit documenten met AI, 47% van de werknemers doet dit nooit.

De belangrijkste gedragsbepalers die het delen van documenten met AI voorspellen bij consumenten en werknemers zijn:

- **Kennis privacybeleid en richtlijnen:** Wanneer consumenten goed op de hoogte zijn van het privacybeleid van de AI-tools die ze gebruiken, delen ze vaker documenten met AI. Werknemers die goed op de hoogte zijn van de AI-richtlijnen en het veiligheidsbeleid van hun organisatie, delen ook vaker documenten met AI.
- **Kwaliteit:** Consumenten die de kwaliteit van AI zo hoog vinden dat ze bereid zijn wat privacy op te offeren, delen vaker documenten met AI. Hoe meer werknemers vinden dat AI helpt om werkdoelen veel sneller te bereiken, hoe vaker ze documenten delen met AI.

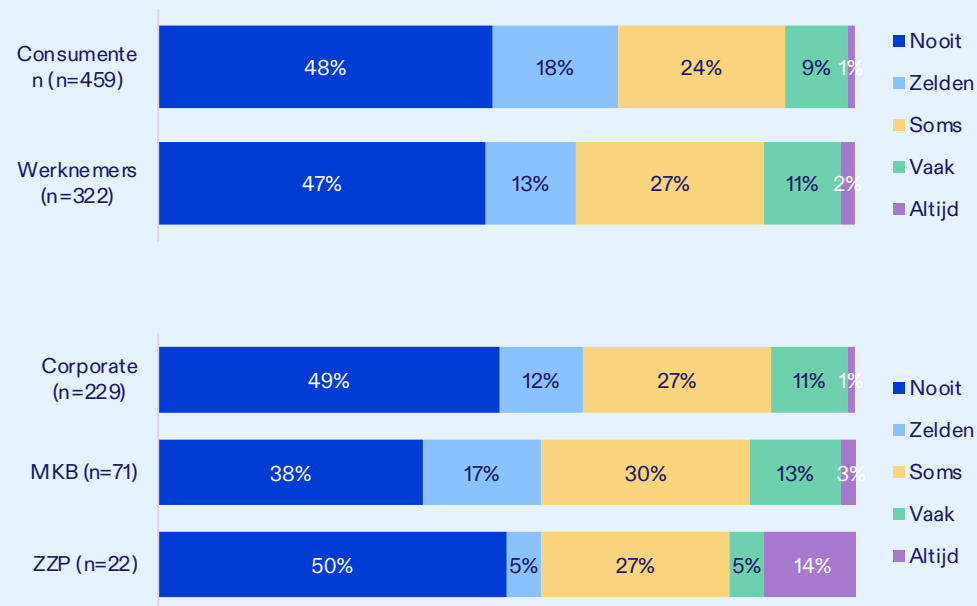
Daarnaast zijn voor werknemers de volgende gedragsbepalers van invloed:

- **Aanbieder vertrouwen:** Werknemers die erop vertrouwen dat de aanbieder van de AI-tool eerlijk en oprecht is over hoe de data van de organisatie wordt gebruikt, delen vaker emoties met AI.
- **AI empathisch vinden:** Hoe empathischer werknemers AI vinden, hoe vaker ze documenten delen met AI.
- **Angst gevolgen als geen AI:** Werknemers die bang zijn hun baan of reputatie in gevaar te brengen als ze geen AI gebruiken, delen vaker emoties met AI.

Bij consumenten en werknemers spelen **leeftijd** en **frequentie** ook een rol en bij consumenten ook **opleidingsniveau** en **stedelijkheid**. Oudere mensen delen minder vaak documenten met AI dan jongere. Hoe vaker iemand AI gebruikt, hoe minder vaak ze documenten delen met AI. Laagopgeleide en stedelijke consumenten delen vaker documenten met AI dan anders opgeleide en minder stedelijke consumenten.

Consumenten: In hoeverre deel jij de volgende soorten persoonlijke informatie met AI: Persoonlijke documenten (zoals cv's of medische rapporten).

Werknemers: In hoeverre deel jij de volgende soorten persoonlijke informatie met AI: Persoonlijke documenten (zoals cv's of werknemergegevens).



Sociale informatie delen met AI

44% van de consumenten deelt nooit sociale informatie met AI, 50% van de werknemers doet dit nooit.

De belangrijkste gedragbepalers die het delen van sociale informatie met AI voorspellen bij consumenten en werknemers zijn:

- **AI empathisch vinden:** Hoe empathischer mensen AI vinden, hoe vaker ze documenten delen met AI.

Daarnaast zijn voor consumenten de volgende gedragbepalers van invloed:

- **Kwaliteit:** Consumenten die de kwaliteit van AI zo hoog vinden dat ze bereid zijn wat privacy op te offeren, delen vaker sociale informatie met AI.
- **Angst dat anderen informatie inzien:** Hoe vaker consumenten sociale informatie delen, hoe bang er is dat de informatie die ze delen met AI ingezien kan worden door andere mensen. Mogelijk wordt men zich meer bewust van de risico's naarmate ze AI vaker gebruiken.

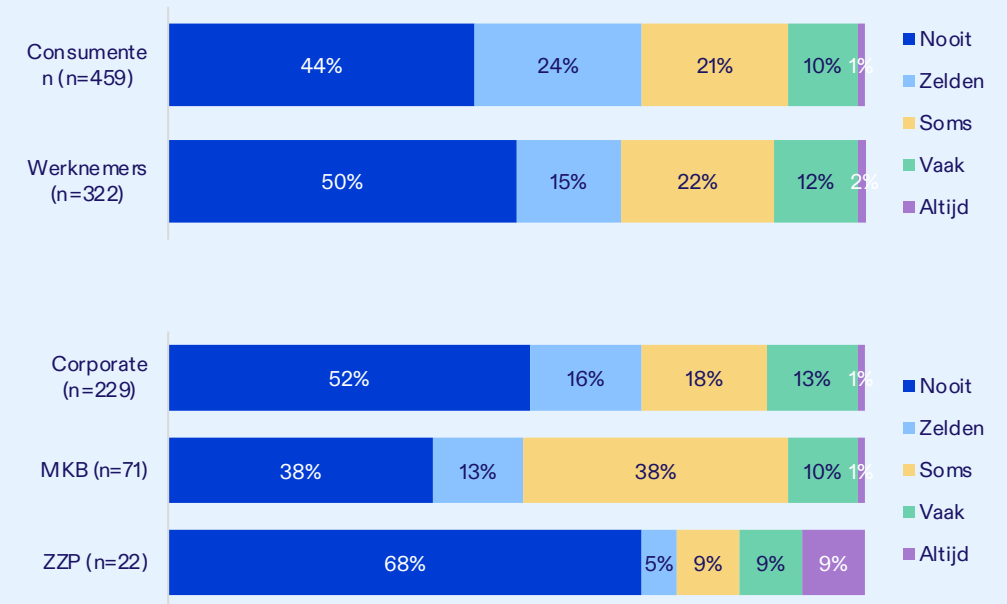
Voor werknemers zijn ook de volgende gedragbepalers belangrijk:

- **Descriptieve norm:** Werknemers met collega's die gebruikmaken van AI, delen minder vaak sociale informatie met AI.
- **Angst gevolgen als geen AI:** Werknemers die bang zijn hun baan of reputatie in gevaar te brengen als ze geen AI gebruiken, delen vaker sociale informatie.

Bij consumenten en werknemers speelt **leeftijd** ook een rol en bij consumenten ook **opleidingsniveau**, **geslacht** en **frequentie**. Oudere mensen delen minder vaak sociale informatie met AI dan jongere. Hoe vaker consumenten AI gebruiken, hoe minder vaak ze sociale informatie delen met AI. Laagopgeleide consumenten delen vaker sociale informatie met AI dan anders opgeleide consumenten. Mannelijke consumenten delen minder vaak sociale informatie met AI dan vrouwen.

Consumenten: In hoeverre deel jij de volgende soorten persoonlijke informatie met AI: Informatie over familieleden, vrienden of collega's.

Werknemers: In hoeverre deel jij de volgende soorten persoonlijke informatie met AI: Informatie over collega's en leidinggevenden.



Problemen delen met AI

34% van de consumenten deelt nooit problemen met AI, 38% van de werknemers doet dit nooit.

De belangrijkste gedragsbepalers die het delen van problemen met AI voorspellen bij consumenten en werknemers zijn:

- **AI empathisch vinden:** Hoe empathischer mensen AI vinden, hoe vaker ze documenten delen met AI.

Daarnaast zijn voor consumenten de volgende gedragsbepalers van invloed:

- **Kwaliteit:** Consumenten die de kwaliteit van AI zo hoog vinden dat ze bereid zijn wat privacy op te offeren, delen vaker problemen met AI. Hoe meer consumenten vinden dat AI helpt om persoonlijker doelen veel sneller te bereiken, hoe vaker ze problemen delen met AI.

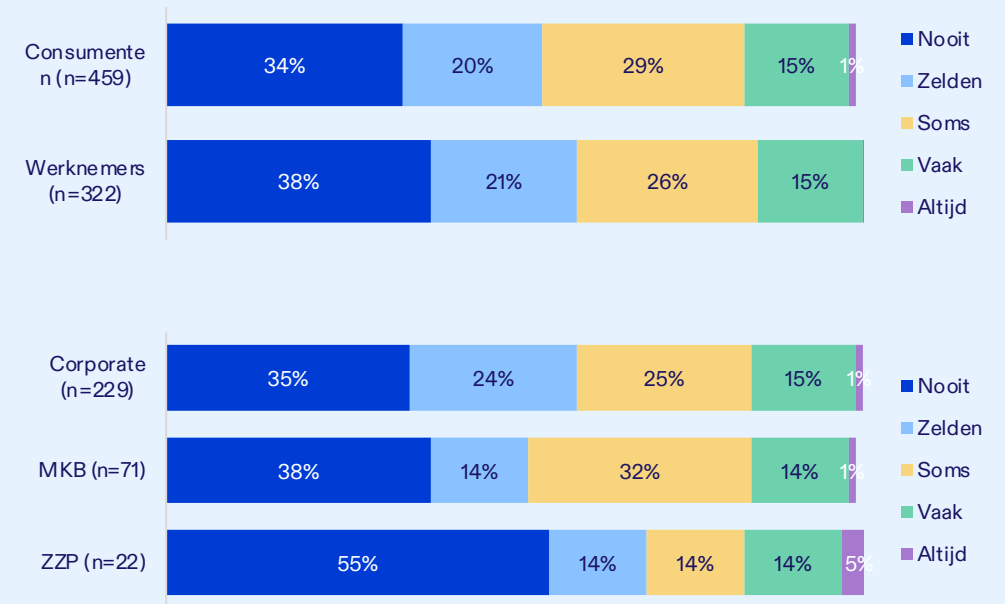
Voor werknemers zijn ook de volgende gedragsbepalers belangrijk:

- **Angst gevolgen als geen AI:** Werknemers die bang zijn hun baan of reputatie in gevaar te brengen als ze geen AI gebruiken, delen vaker problemen met AI.

Bij consumenten en werknemers spelen **leeftijd** en **frequentie** ook een rol en bij consumenten ook **geslacht**. Oudere mensen delen minder vaak problemen met AI dan jongere. Hoe vaker iemand AI gebruikt, hoe minder vaak ze problemen delen met AI. Mannelijke consumenten delen minder vaak problemen met AI dan vrouwelijke consumenten.

Consumenten: In hoeverre deel jij de volgende soorten persoonlijke informatie met AI: Persoonlijke situaties of problemen om advies te krijgen.

Werknemers: In hoeverre deel jij de volgende soorten persoonlijke informatie met AI: Werksituaties of -problemen om advies te krijgen.



Doelgroepinformatie delen met AI

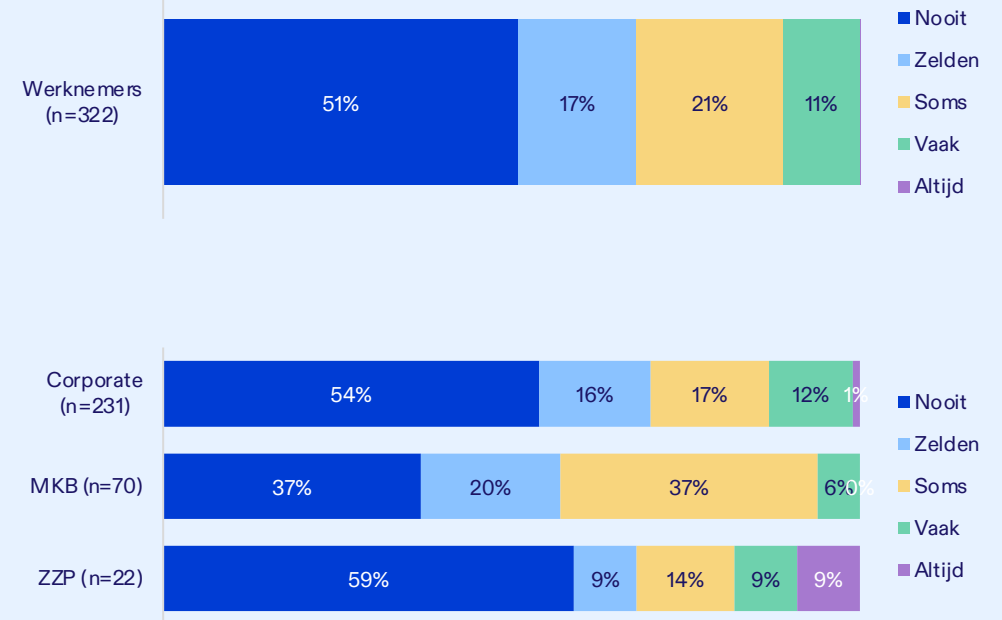
51% van de werknemers deelt nooit doelgroepinformatie met AI.

De belangrijkste gedragsbepalers die het delen van problemen met AI voorspellen bij werknemers zijn:

- **Descriptieve norm:** Werknemers met collega's die gebruikmaken van AI, delen minder vaak doelgroepinformatie met AI.
- **Aanbieder vertrouwen:** Werknemers die erop vertrouwen dat de aanbieder van de AI-tool eerlijk en oprecht is over hoe de data van de organisatie wordt gebruikt, delen vaker doelgroepinformatie met AI.
- **AI empathisch vinden:** Hoe empathischer werknemers AI vinden, hoe vaker ze doelgroepinformatie delen met AI.
- **Angst gevolgen als geen AI:** Werknemers die bang zijn hun baan of reputatie in gevaar te brengen als ze geen AI gebruiken, delen vaker doelgroepinformatie met AI.

Leeftijd speelt ook een rol. Oudere werknemers delen minder vaak doelgroepinformatie met AI dan jongere werknemers.

In hoeverre deel jij de volgende soorten persoonlijke informatie met AI: Informatie over mijn klanten / patiënten / studenten of andere doelgroep.



Hoe *stimuleren* we mensen om *correct informatie met AI te delen*?

Zoals eerder aangegeven, is het niet mogelijk om in de data te achterhalen op welke manier mensen informatie delen met AI en of dit gewenst is of niet. Aan de hand van de analyses kunnen we dus ook niet vaststellen op welke gedragsbepalers ingezet moet worden om meer van het gewenste gedrag te stimuleren. Het is goed dat verder te onderzoeken. Hieronder staan enkele algemene tactieken en technieken.

Tactiek 1: Inertia verlagen		
Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Het handmatig anonimiseren of 'schoonmaken' van documenten en prompts (zoals het opsporen en verwijderen van namen, adressen, BSN's of financiële gegevens) kost tijd, cognitieve energie en moeite. In de praktijk wint de drang naar snelheid en productiviteit het vaak van de zorgvuldigheid. Wanneer het veilig delen van informatie veel extra handmatige stappen vereist, haken gebruikers af en uploaden ze ruwe, gevoelige bestanden rechtstreeks in AI-tools.	De frictie voor de veilige route moet naar nul worden gebracht. Het verwijderen van persoonsgegevens en bedrijfsgevoelige informatie moet geautomatiseerd of verregaand gefaciliteerd worden, zodat het veilige gedrag automatisch de makkelijkste en snelste optie wordt.	• Systeemveranderingen en defaults: Stimuleer de integratie van browserextensies of interne software die persoonsgegevens (zoals namen, adressen en BSN's) automatisch uit documenten en teksten filtert of anonimiseert voordat de prompt naar de AI-server wordt verzonden. Dit neemt het handmatige opschoonwerk volledig weg. • Goedgekeurde AI-tools: Bied als organisatie vooraf geconfigureerde, afgeschermdes AI-omgevingen aan (waarin gegevenstracking en modeltraining standaard uitstaan). Hierdoor hoeft de werknemer niet zelf privacy-instellingen uit te zoeken, maar is de standaardomgeving per definitie veilig.
Tactiek 2: Risicoperceptie & de-antropomorfisering		
Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Gebruikers neigen ernaar AI-systemen te antropomorfiseren: ze schrijven de AI menselijke eigenschappen toe en behandelen de chat-interface als een vertrouwelijk gesprek met een behulpzame collega (12-16% vindt AI empathisch). Dit schakelt het natuurlijke 'privacy-filter' uit. Gebruikers staan er niet bij stil dat ingevoerde gegevens worden opgeslagen op externe servers, ingezien kunnen worden door model-reviewers, of hergebruikt worden om het AI-model verder te trainen.	De illusie van een 'besloten, vertrouwelijke chatbot' moet worden doorbroken. Er is een nieuw, helder mentaal model nodig dat gebruikers op een laagdrempelige manier herinnert aan het openbare en externe karakter van gegevensverwerking door AI.	• Vuistregels: Introduceer een simpele, visuele vuistregel in publieks- en interne campagnes: <i>Typ of upload niets in een AI-tool wat je niet hardop zou voorlezen in een overvolle trein</i>. Dit de-antropomorfiseert de AI en herinnert de gebruiker direct aan de externe opslag van data. • Visualisatie: Toon via korte demonstraties hoe ingevoerde bedrijfsgeheimen of broncodes in de praktijk weer boven water kunnen komen in antwoorden aan derden als datatraining niet is uitgeschakeld. Dit verhoogt de gepercipieerde ernst en ontkracht het idee dat ingevoerde prompts onzichtbaar verdwijnen.

Hoe *stimuleren* we mensen om *correct informatie met AI te delen*?

Tactiek 3: Prompts op het schakelmoment

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Tekst invoeren of documenten slepen naar een AI-invoerveld gebeurt vaak op de automatische piloot. Gebruikers kopiëren snel een hele e-mail of een compleet klantrapport en plakken dit direct in het venster. Algemene cybersecurity-trainingen die weken geleden zijn gevolgd, worden op het moment van de handeling vaak niet geactiveerd.	Het automatische typ- en plakgedrag moet precies op het moment van de beslissing (bij het invoerveld zelf) kort worden onderbroken om het analytische brein te activeren en een bewust leermoment te creëren.	• Prompts: Moedig ontwikkelaars en IT-afdelingen aan om visuele triggers (zoals een oranje waarschuwingsbadge of subtiele pop-up) te integreren direct bij het invoerveld. Zodra de software gevoelige termen herkent (zoals BSN, salaris, IBAN, medisch of het woord vertrouwelijk), verschijnt de herinnering:  <i>Let op: Bevat dit document persoonsgegevens? Anonimiseer deze eerst.</i> • Als-dan regels: Train gebruikers in een vaste routine vóór het plakken van tekst: <i>Als ik een document of tekst wil uploaden naar AI, dán doe ik eerst een scan op namen, adressen en nummers.</i>

Tactiek 4: Kennis van beleid verhogen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Het niet-veilig delen van informatie wordt mede veroorzaakt door een gebrek aan procedurele kennis: werknemers en consumenten weten vaak simpelweg niet welke gegevens wel of niet gedeeld mogen worden en hoe ze een document snel kunnen opschonen. Vage richtlijnen (<i>ga zorgvuldig om met data</i>) kunnen leiden tot handelingsonzekerheid, waardoor mensen op goed geluk handelen. Van de werknemers weet 39% welke AI tools mogen van de organisatie en 35% kent de richtlijnen. Van de consumenten weet slechts 14% wat het privacybeleid is van de AI tools die ze gebruiken.	Het bieden van eenduidige, visuele beslisbomen en eenvoudige 'hoe-te-handelen' protocollen die in één oogopslag verduidelijken welke datacategorieën geschikt zijn voor AI-invoer.	• Vuistregels: Bied een overzichtelijke visualisatie. Bijvoorbeeld: een poster bij de werkplek of een widget in de browser met drie heldere kleurencategorieën. •  Groen (vrij te gebruiken): Openbare teksten, algemene concepten, niet-gevoelige brainstorms. •  Oranje (eerst opschonen): Interne werkmethode of conceptverslagen (alleen toegestaan ná verwijdering van namen en bedrijfsdetails). •  Rood (strikt verboden): Persoonsgegevens, medische data, wachtwoorden, ongepubliceerde financiële cijfers. • Stapsgewijze gidsen: Bied korte 1-minuut video's die exact laten zien hoe je in veelgebruikte programma's (zoals Word of PDF-readers) met functies zoals 'Zoek & Vervang' of automatische zwartlakt-tools in 10 seconden alle persoonsgegevens verwijdert alvorens een tekst in AI te plaatsen.

AI zonder toestemming gebruiken

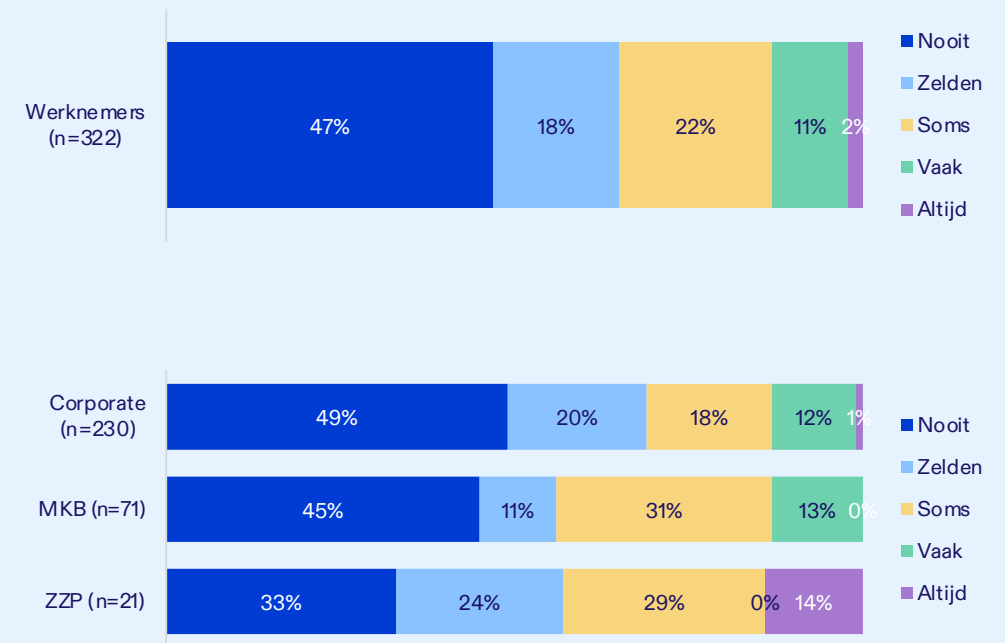
35% van de werknemers gebruikt soms, vaak of altijd AI-tools zonder toestemming van de organisatie.

De belangrijkste gedragsbepalers die het delen van problemen met AI voorspellen bij werknemers zijn:

- **Descriptieve norm:** Werknemers met collega's die gebruikmaken van AI, gebruiken minder vaak AI zonder toestemming.
- **AI empathisch vinden:** Hoe empathischer werknemers AI vinden, hoe vaker ze AI zonder toestemming gebruiken.

Leeftijd en frequentie spelen ook een rol. Oudere werknemers gebruiken minder vaak AI zonder toestemming dan jongere werknemers. Hoe vaker werknemers AI gebruiken, hoe minder vaak ze AI zonder toestemming gebruiken.

Ik gebruik AI-tools voor werk zonder toestemming of medeweten van mijn organisatie.



Privé AI-accounts gebruiken voor werk

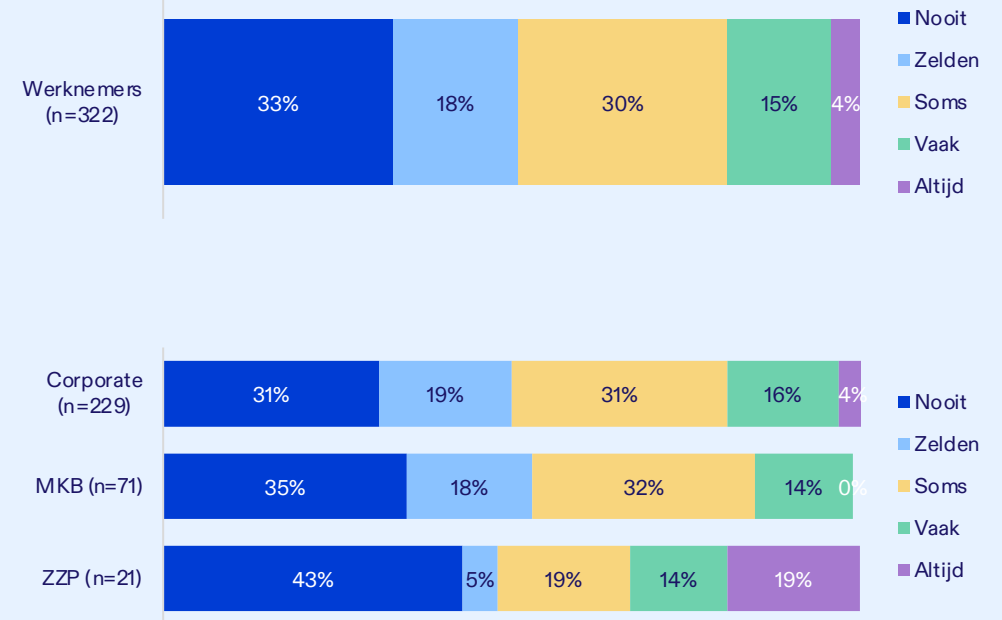
49% van de werknemers gebruikt soms, vaak of altijd privé AI-account voor werk.

De belangrijkste gedragsbepalers die het delen van problemen met AI voorspellen bij werknemers zijn:

- **Kwaliteit:** Wanneer iemand de productiviteitsverhoging door AI zo groot vindt dat ze eventuele risico's voor de organisatie acceptabel vinden, gebruiken ze vaker privé AI-accounts voor werk. Hoe meer iemand vindt dat AI helpt om werkdoelen veel sneller te bereiken, hoe minder vaak diegene privé AI-accounts voor werk gebruikt.
- **AI empathisch vinden:** Hoe empathischer werknemers AI vinden, hoe vaker ze privé AI-accounts voor werk gebruiken.
- **Angst dat anderen informatie inzien:** Hoe banger werknemers zijn dat informatie die ze delen met AI ingezien kan worden door andere mensen en organisaties, hoe vaker ze privé AI-accounts voor werk gebruiken.
- **Veilig:** Werknemers die er alle vertrouwen in hebben dat ze AI-tools veilig kunnen gebruiken zonder de veiligheidsregels van hun organisatie te overtreden, gebruiken vaker privé AI-accounts voor werk.
- **Kennis welke mogen:** Werknemers die weten welke AI-tools wel of niet gebruikt mogen worden, gebruiken minder vaak privé AI-accounts voor werk. Over het algemeen weet ook maar 39% welke AI-tools gebruikt mogen worden op werk (zie Bijlage C).

Leeftijd en frequentie spelen ook een rol. Oudere werknemers gebruiken minder vaak privé AI-accounts voor werk dan jongere werknemers. Hoe vaker werknemers AI gebruiken, hoe minder vaak ze privé AI-accounts voor werk gebruiken.

Ik gebruik privé AI-accounts of apps voor werkdoeleinden.



Hoe *stimuleren* we werknemers om *geen privé-accounts* en *AI-tools* zonder *toestemming* van werkgever te gebruiken?

Deze twee gedragingen zijn wel duidelijk ongewenst. De gedragsbepalers die hiervoor genoemd worden zijn ook voor deze twee gedragingen relevant. We delen hier adviezen die kunnen helpen om mensen minder vaak shadow AI te laten gebruiken.

Tactiek 1: Antropomorfisme doorbreken en risicoperceptie verhogen (voor werknemers)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Wanneer werknemers communiceren met AI-systemen treedt er snel antropomorfisme op: het toeschrijven van menselijke eigenschappen aan de machine (empathie-illusie). De chat-interface voelt als een veilige, begripvolle coach of luisterend oor. Zolang de interactie lief en begripvol aanvoelt (wat voor 16% van de werknemers geldt), schakelt het natuurlijke privacy-filter uit. Werknemers staan er niet bij stil dat hun invoer (zoals gevoelige dossierinformatie, zakelijke conflicten of klantgegevens) niet vertrouwelijk blijft, maar als data wordt opgeslagen op externe servers van commerciële techbedrijven om modellen verder te trainen. Ook vindt 20% de risico's van AI acceptabel, waardoor ze mogelijk minder veilig met hun gegevens omgaan.	Het mentale model van de werknemer moet worden gewijzigd: weg van de begripvolle gesprekspartner en naar een externe, statistische dataverwerker. De illusie van vertrouwelijkheid moet worden verbroken door de-anthropomorfisering, real-time privacy triggers bij gevoelige invoer en memorabele vuistregels die de externe opslag visueel maken.	• Herkadering: Verander de perceptie van AI in alle interne communicatie: <i>AI voelt als een begripvolle coach, maar is een statistische dataspons. Alles wat je typt is geen geheim gesprek, maar data die wordt opgeslagen op externe servers van een techbedrijf.</i> • Prompts: Bouw bij de invoervelden van AI-systemen automatische disclaimers in die verschijnen zodra gevoelige of emotionele woorden (zoals conflict, salaris, ziekte, ontslag) worden getypt. Waarschuwing: ⚠️ <i>Let op: Deze AI klinkt empathisch, maar garandeert geen vertrouwelijkheid van jouw persoonsgegevens. Data wordt extern opgeslagen.</i> • Vuistregels: Leer werknemers een simpele, memorabele vergelijkingsregel aan wanneer ze gevoelige situaties of documenten aan AI willen voorgeven. <i>Zou je deze beschrijving of foto ook op het raam van een volle trein plakken of hardop voorlezen in de sprinter naar Utrecht? Zo nee, typ of upload het dan niet in AI.</i>

Hoe *stimuleren* we werknemers om *geen privé-accounts* en *AI-tools* zonder *toestemming* van werkgever te gebruiken?

Tactiek 2: Inertia verlagen (voor werknemers)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Het gebruik van privé-accounts en niet-geautoriseerde AI-tools wordt gedreven door productiviteitsdrang en tijdsbesparing. Werknemers kiezen vaak voor het resultaat (20% vindt de risico's acceptabel, 29% vindt dat AI helpt om hun werkdoelen te bereiken). Als het officiële, door de werkgever goedgekeurde alternatief trager is, minder functionaliteiten biedt of simpelweg niet bestaat, wint de drang naar snelheid en kwaliteit het van een abstract risico op de lange termijn. Direct gemak verslaat abstracte veiligheid.	De balans tussen productiviteit en veiligheid moet hersteld worden. De veilige optie moet de weg van de minste weerstand worden. De organisatie moet goedgekeurde, volwaardige AI-tools aanbieden die qua gebruiksgemak en snelheid niet onderdoen voor privé-accounts, én het begrip 'kwaliteit van werk' herdefiniëren binnen de organisatiecultuur.	• Herdefinieer kwaliteit als accuraat + veilig: Pas de normering binnen organisaties aan. Kwalitatief werk = accurate output én dataveiligheid. Output van een niet-geautoriseerd privé-account is per definitie slechte kwaliteit vanwege het datalekrisico. Neem de angst weg dat werknemers worden afgestraft als ze geen privé-AI gebruiken en beloon verantwoord gebruik in plaats van blinde snelheid. • Veilige alternatieven: Bied vanuit de IT-afdeling goedgekeurde AI-varianten aan (waarin gegevenstracking en training uitstaan) die even snel en toegankelijk werken als privé-tools. Zorg dat inloggen via single sign-on verloopt, zodat de drempel om het officiële kanaal te gebruiken minimaal is. • Systeemaanpassing: Maak een laagdrempelig loket waar werknemers functionaliteiten kunnen aanvragen die ze momenteel missen op het werk. Boodschap: <i>Gebruik je een privé-tool omdat het je 3 uur per week bespaart? Meld het bij het innovatieloket, dan regelen we een veilige variant.</i> Dit zet productiviteitsdrang om in veilige innovatie.

Tactiek 3: Kennis van toegestane tools verhogen & risico's zichtbaar maken (voor werknemers)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Het gebruik van ongeautoriseerde tools ontstaat vaak door een gebrek aan duidelijke procedurele kennis: 39% van de werknemers weet niet welke AI-tools en accounts wel of niet zijn toegestaan door de werkgever. Daarnaast zijn de risico's van het voeden van data aan privé-accounts (zoals intellectueel eigendomsverlies, AVG-boetes of imagoschade) voor de individuele werknemer onzichtbaar en te abstract op het moment dat ze snel een taak willen afronden. Slechts 35% is op de hoogte van alle richtlijnen.	Het bieden van eenduidige kennis over goedgekeurde scenario's (focus op wat wél mag in plaats van alleen een lijst met verboden), gecombineerd met het direct zichtbaar en concreet maken van het organisatierisico op het moment dat een privé-account wordt gebruikt.	• Beleid (de groene lijst): Bied een duidelijke, visuele beslisboom of lijst die werknemers direct laat zien welke tools en scenario's groen licht hebben. Focus op het faciliteren van toegestane functionaliteiten in plaats van alleen te zwaaien met verbodsbepalingen. • Visualisatie: Maak op het moment van keuzestress direct de negatieve consequentie inzichtelijk om de risicoperceptie te verhogen. <i>Het gebruik van dit privé-account bespaart je 10 minuten, maar stelt onze klantdata direct bloot aan derden en kan de organisatie een AVG-boete opleveren.</i> • Rolmodellen en onboarding: Integreer korte instructies in de onboarding en teamoverleggen waarin leidinggevend expliciet het goede voorbeeld geven: zij tonen hoe ze de officiële IT-tools inzetten en benoemen openlijk dat privé-accounts niet worden getolereerd binnen het vakmanschap van de afdeling.

Bijlage A: *Methodologische verantwoording*

De *Rasch*-methodiek

De Rasch-methodiek is een wetenschappelijke methode waarmee we statistisch kunnen bepalen welke vormen van digitaal veilig gedrag het meest kansrijk zijn om op in te zetten. Hiervoor hebben we de data van het Alert Online 2025 onderzoek gebruikt. De methodiek bouwt voort op universele gedragsmechanismen.

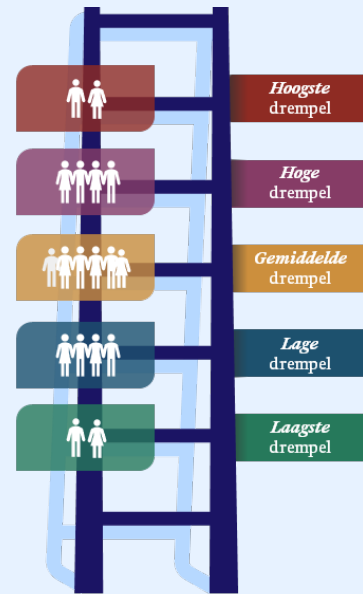
De mindset en de gedragsladder

Een *mindset* is een mentaal construct. Een mindset bestaat uit concrete gedragingen die uiting geven aan de mindset. Met het Rasch-model wordt getoetst of een lijst aan gedragingen samen één hiërarchische structuur vormen, namelijk een *gedragsladder*. Een gedragsladder representeert zo'n onderliggende mindset.

Binnen digitale veiligheid bestaan bijvoorbeeld gedragingen die relatief makkelijk zijn om uit te voeren en gedragingen die meer tijd, moeite of vaardigheden vragen. Sommige handelingen hebben een grote drempel waardoor ze minder snel worden uitgevoerd. Andere hebben een kleine drempel en worden juist vaker opgepakt door consumenten en werknemers. Op de gedragsladder worden de gedragingen gerangschikt van een lage drempel (al veel mensen vertonen dit gedrag) naar een hoge drempel (slechts enkele personen vertonen dit gedrag).

De doelgroep

Hoe belangrijker iemand digitale veiligheid en weerbaarheid daartegen vindt (hoe sterker hun mindset), hoe hoger diegene op de ladder klimt. Bovenaan de ladder staan consumenten en werknemers die veel waarde hechten aan digitale veiligheid. Zij voeren zowel eenvoudige als complexere gedragingen uit. Onderaan de ladder staan mensen die het onderwerp minder belangrijk vinden en vooral de laagdrempelige stappen zetten.



Het Rasch-model als ladder: Hoe sterker iemands mindset, des te hoger staat diegene op de ladder.

Uitkomst

Door de Rasch-methodiek toe te passen op digitaal veilig gedrag van consumenten en werknemers kunnen we een gedragsladder binnen digitale veiligheid statistisch toetsen. Hierdoor ontstaat een helder visueel overzicht van kansrijke cybergedragingen voor een specifieke doelgroep:

- inzichtelijke relatie tussen verschillende doelgedragingen
- zichtbaar waar verschillende doelgroepen zich bevinden op de ladder
- duidelijk welke doelgedragingen kansrijk zijn vanuit de huidige positie en vaardigheden van een doelgroep.

Kansrijke gedragingen zijn met name:

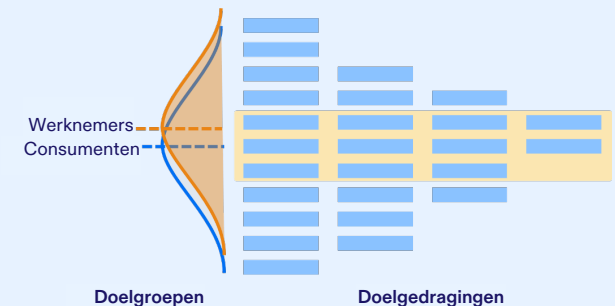
- gedragingen in het midden van de ladder: deze sluiten aan bij de vaardigheden van een groot deel van de doelgroep en zijn daardoor geschikt voor brede campagnes gericht op het stimuleren van meer online veilig gedrag.
- gedragingen die specifiek aansluiten bij de positie van een afgebakende doelgroep (bijvoorbeeld koplopers of achterblijvers).

Weinig mensen doen dit



Veel mensen doen dit

Met het Rasch-model zijn de meest kansrijke gedragingen te identificeren.



Met het Rasch-model is inzichtelijk te maken waar doelgroepen zich bevinden op de ladder.

Verdiepende *deskresearch*

Voor de kansrijke doelgedragingen ontwikkelden we visuele gedragsmodellen. Deze modellen werden gebaseerd op verdiepend deskresearch, aanvullende analyses op de Alert Online 2025 data en inhoudelijke expertise uit eerder uitgevoerd onderzoek.

Deskresearch gaf inzicht in bestaande kennis over de gedragsbepalers die een rol spelen bij online veilig gedrag. Denk aan zelfoverschatting en risicoperceptie. We brachten in kaart welke gedragsbepalers relevant zijn voor de gekozen doelgedragingen. Daarnaast bepaalden we ook welke kennis er nog miste. Deze inzichten vormden de inhoudelijke basis voor de volgende onderzoeksfase: de vragenlijst.

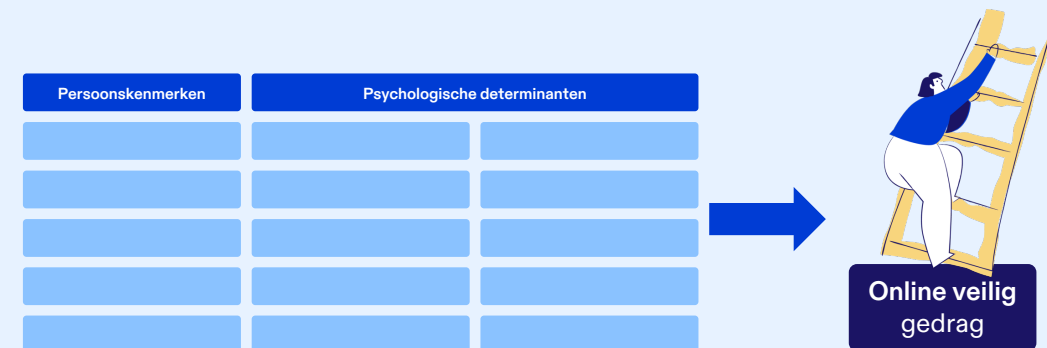
Hieronder beschrijven we de stappen die we doorliepen.

1. **Reeds beschikbare publicaties verzamelen.** We vroegen de opdrachtgever om relevante publicaties en onderzoeksrapporten aan te leveren. We gebruikten de aangeleverde literatuur en eerder door ons verworven kennis als input voor het huidige onderzoek.
2. **Zoektermen bepalen.** We stelden een lijst op met Nederlandse en Engelse zoektermen, gebaseerd op de onderzoeksvragen en de eerder gevonden literatuur. Deze termen gingen over het doelgedrag, de doelgroepen en relevante situaties. We hielden hierbij ook rekening met vakjargon in wetenschappelijke publicaties.
3. **Literatuur zoeken en prioriteren.** Met de zoektermen zochten we systematisch in databases zoals PsycINFO, Web of Science en Google Scholar. We verzamelden relevante publicaties in een overzicht en beoordeelden deze op geschiktheid aan de hand van:
 - de overeenkomst met de huidige doelgroep en het doelgedrag;
 - het soort publicatie (wetenschappelijk/niet wetenschappelijk);
 - het onderzoeksdesign (metastudie, randomized controlled trial, case study);
 - de eventuele statistische effectgroottes.

4. **Literatuur lezen en inzichten bijhouden.** Tijdens het lezen van de publicaties hielden we alle relevante informatie voor het huidige onderzoek bij. We verzamelden inzichten over doelgedragingen, gedragsbepalers en doelgroepen. Bij wetenschappelijke studies namen we daarbij ook de specifieke onderzoeksmethoden en statistische effectgroottes in overweging. We rangschikten de inzichten op basis van relevantie, statistische betrouwbaarheid en geschiktheid voor het huidige onderzoek.

Betrouwbaarheid en validiteit

De betrouwbaarheid en validiteit van een deskresearch hangen af van de beschikbare (wetenschappelijke) literatuur. We waarborgden de betrouwbaarheid en validiteit door effectgroottes en statistische kenmerken nauwkeurig te documenteren en de literatuur te filteren op de meest belangrijke en relevante publicaties.



Door middel van deskresearch hebben we achterhaald wat belangrijke persoonskenmerken en psychologische determinanten online veilig gedrag beïnvloeden.

Vragenlijst

Op basis van de Rasch-analyse, deskresearch en in overleg met experts hebben we een selectie gemaakt van de meest kansrijke gedragingen en gedragsbepalers. Via een vragenlijst konden we statistisch toetsen welke relaties er bestaan tussen de gedragingen en gedragsbepalers voor consumenten en werknemers.

Hieronder beschrijven we de stappen die we doorliepen.

1. **Doelgroepen bepalen.** We richtten ons op twee doelgroepen: consumenten en werknemers. Binnen de doelgroep werknemers onderscheidden we 3 subgroepen: ZZP'ers, MKB'ers (bedrijf tot 50 werknemers) en corporate werknemers (bedrijf met 50+ werknemers).
2. **Inhoud vragenlijst bepalen.** We beperkten de lengte van de vragenlijst voor een zo hoog mogelijke respons. Het invullen van de vragenlijst duurde maximaal 15 minuten. We bepaalden de specifieke inhoud van de vragenlijst op basis van de uitkomsten van de Rasch-analyse, deskresearch en experts. De volgende onderdelen kwamen aan bod:
 - **Individuele kenmerken:** leeftijd, geslacht, regio waarin ze wonen, werksituatie en opleiding.
 - **Doelgedraging(en):** zie de doelgedragingen op pagina 11. We hebben gedrag op twee manieren uitgevraagd.
 - We vroegen de doelgroepen om zelf te rapporteren in hoeverre ze de doelgedragingen al vertonen. Elk doelgedrag werd omgezet in concrete, eenvoudig te beantwoorden vragen. Het voordeel van deze route is dat we een brede lijst van gedragingen aan de doelgroep konden voorleggen. De beperking is dat de kloof tussen zelfgerapporteerd en daadwerkelijk gedrag lastig te bepalen is, waardoor de externe validiteit lager ligt dan bij andere routes.
 - Daarom legden we ook een scenario voor aan de doelgroepen. We vroegen wat ze in deze situaties zouden laten zien. We vroegen de doelgroep zich in te leven in situatie die een mix vormde van risicovolle en niet-risicovolle momenten. Hiermee toetsten we of het gerapporteerde gedrag zowel veilig als realistisch is en scheiden we realistische antwoorden van sociaal wenselijke antwoorden. Het voordeel van deze route was dat we dichtbij

daadwerkelijke situaties en gedrag konden komen. Het nadeel was dat elk scenario meer tijd vroeg, waardoor het aantal gedragingen en scenario's dat we konden uitvragen beperkter was.

- **Motieven en barrières:** We vroegen ook naar motieven en barrières rondom de doelgedragingen. We stelden de doelgroepen per doelgedrag vragen over de mate waarin zij mogelijk relevante omgevingsfactoren, capaciteiten en competenties en psychologische weerstanden en drijfveren hebben of ervaren. We bepaalden welke factoren het sterkst met de doelgedragingen samenhangen, door de mate waarin de doelgroepsleden deze gedragsbepalers ervaren te relateren aan de mate waarin ze het doelgedrag vertonen.
3. **Vragenlijstitems ontwerpen.** We maakten gebruik van een vragenlijst met schaalvragen. Dit zijn vragen waarbij mensen aangeven hoe ze iets vinden of voelen door een cijfer te kiezen op een lijn van bijvoorbeeld 1 tot 5. Op deze manier kregen we een gedetailleerd inzicht in de mate waarin de gedragsbepalers samenhangen met het doelgedrag/de doelgedragingen.
 4. **Doelgroep werven.** Voor het werven van de respondenten maakten we gebruik van een panelbureau. Zij werven de respondenten vanuit hun eigen panel, legden contact met de doelgroep en verstuurden de vragenlijst. De panelleden kregen een vergoeding van het panelbureau. Uiteindelijk deden 987 deelnemers mee aan het onderzoek, waarvan 609 consumenten en 378 werknemers.

Selectiebias verkleinen

Bij het invullen van vragenlijsten was sprake van zelfselectie. Dit betekent dat de consumenten en werknemers die de vragenlijst invulden mogelijk verschilden van consumenten en werknemers die de vragenlijst niet invulden. We reduceerden de selectiebias zo sterk mogelijk, door:

- de anonimiteit van respondenten te benadrukken;
- de vragenlijst kort te houden zodat het invullen maximaal 10 minuten duurde;
- rekening te houden met praktische zaken, zoals de mogelijkheid om de vragenlijst ook in te kunnen vullen op een smartphone.

Vragenlijst

- 5. Antwoorden analyseren & inzichten delen.** Bij schaalvragen gebruikten we regressiemodellen die gangbaar zijn in de wetenschap. Hiermee is in kaart gebracht welke gedragsbepalers invloed hebben op de cybergedragingen. De hoeveelheid statistische toetsen was hierbij afhankelijk van de hoeveelheid doelgedragingen en subgroepen. We hebben een gestructureerd analyseplan uitgevoerd. Na het opschonen van de dataset en het excluderen van onbetrouwbare respondenten, zoals straightliners en deelnemers met een te korte doorlooptijd, zijn de data gecontroleerd op statistische assumpties. Beschrijvende analyses geven extra inzicht in verschillende subgroepen.

Betrouwbaarheid en validiteit

Bij digitale vragenlijsten streven we naar een hoge betrouwbaarheid en validiteit van de onderzoeksresultaten door zorgvuldig ontworpen meetinstrumenten en processen. We maakten zo mogelijk gebruik van gevalideerde schalen en vragen die eerder in wetenschappelijk onderzoek zijn getest. Op die manier waarborgden we de betrouwbaarheid van de resultaten zo goed mogelijk.

Beperkingen van het onderzoek

Digitale vragenlijsten zijn efficiënt en bieden toegang tot een grote steekproef. Toch kennen ze ook enkele beperkingen. Een mogelijke beperking is de afhankelijkheid van zelfrapportage, wat kan leiden tot bias door sociale wenselijkheid of incorrecte zelfperceptie. Dit kan de nauwkeurigheid van de antwoorden beïnvloeden. Daarnaast kan de representativiteit van de steekproef een uitdaging zijn. Deelnemers zijn vaak afhankelijk van hun toegang tot technologie en hun bereidheid om deel te nemen, wat kan leiden tot een selectieve steekproef. Dit kan vooral problematisch zijn bij onderzoek met doelgroepen die minder digitaal vaardig zijn.

Ethiek en privacy

We sloegen de data op in een beveiligde map die alleen toegankelijk is voor projectleden van het onderzoek en we verwijderden eventuele bijzondere persoonsgegevens zes maanden na afronding van het project uit de dataset. In de uitwerkingen die we maakten van de vragenlijst en in rapportages, noemden we geen direct identificeerbare persoonsgegevens. Wel benoemden we subgroepskenmerken van respondenten als deze relevant waren voor het interpreteren van de inzichten. We voorkwamen zo dat respondenten op basis van de combinatie van verschillende kenmerken alsnog geïdentificeerd konden worden.

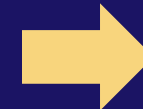


Bijlage B: Toepassing op *overige cybergedragingen*

Op de volgende pagina's tonen we net als in het hoofdrapport per gedrag in hoeverre het gedrag wordt uitgevoerd, wat de belangrijkste gedragsbepalers zijn en wat ervoor nodig is om dit gedrag verder te stimuleren. De technieken die worden genoemd zijn voorbeelden en suggesties.

Zie in bijlage C sectie "Gedragsbepalers" de precieze stellingen van de psychologische determinanten per gedrag.

Persoonskenmerken	Psychologische determinanten	
+	+	
		-
		-
	+	
		+



Online veilig
gedrag

Tijdsdruk controleren

50% van de consumenten let altijd op tijdsdruk-taal, 41% van de werknemers doet dit altijd.

Om het controleren van de tijdsdruk te stimuleren zijn de belangrijkste gedragsbepalers voor consumenten:

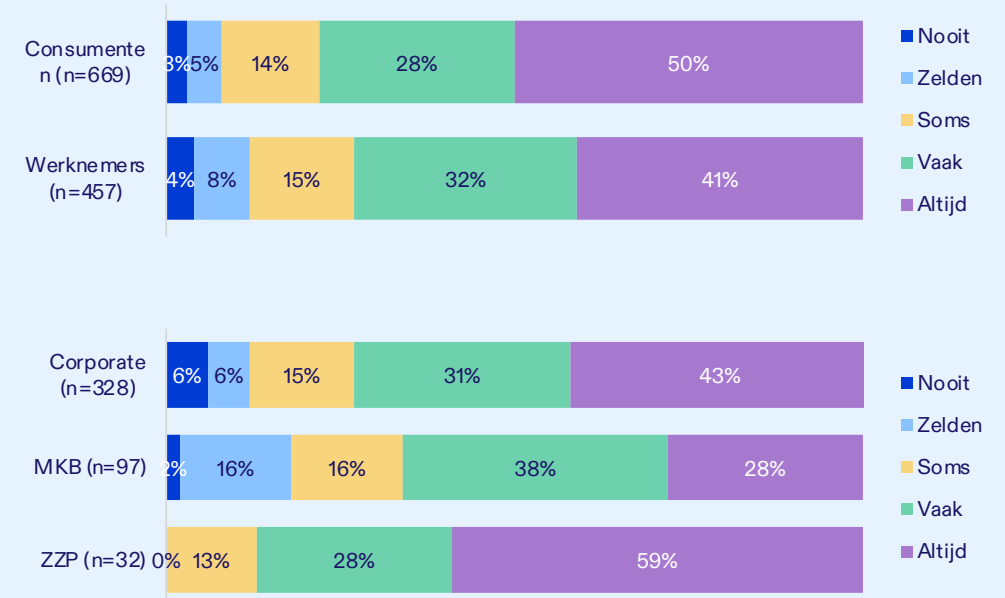
- **Risicoperceptie:** Wanneer iemand ervan overtuigd is dat de gevolgen ernstig kunnen zijn, controleren zij vaker op tijdsdruk-taal.

De belangrijkste gedragsbepalers voor werknemers zijn:

- **Kennis:** Wanneer werknemers weten waar zij op moet letten om te beoordelen of een e-mail, link of QR-code betrouwbaar is, controleren zij vaker op tijdsdruk-taal.
- **Descriptieve norm:** Hoe sterker de norm bij collega's en leidinggevenden, hoe vaker werknemers letten op tijdsdruk-taal.
- **Tijdsdrukgevoelig:** Wanneer werknemers ervaren dat zij snel moeten reageren op een e-mail, zijn ze sneller geneigd om te klikken, scannen of gegevens te delen. En letten zij minder vaak op tijdsdruk-taal.

Bij consumenten speelt **stedelijkheid** ook een rol en bij werknemers **opleidingsniveau**. Consumenten die uit een van de 3 grote steden komen of randgemeenten, controleren minder vaak op tijdsdruk-taal. Laagopgeleide werknemers letten minder vaak op tijdsdruk-taal dan anders opgeleide werknemers.

Ik let op tijdsdruk of dringende taal, zoals 'vandaag nog', 'meteen' of 'anders gaat het mis'.



Hoe *stimuleren* we mensen om vaker *tijdsdruk te controleren*?

Tactiek 1: Risicoperceptie verhogen (voor consumenten)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Consumenten die inzien dat één verkeerde klik op een spoedbericht kan leiden tot lege bankrekeningen, identiteitsfraude of het kwijtraken van persoonlijke bestanden, zijn aanzienlijk alerter op alarmerende taal. Zodra de gepercipieerde ernst van de gevolgen echter laag is, treedt een laconieke houding op (<i>het zal wel</i>). Consumenten klikken dan mogelijk sneller op een e-mail of sms om van het 'gezeur' of de dreigende blokkade af te zijn. De meeste consumenten zien de gevaren in, maar zo'n 14-23% niet of minder.	Het abstracte digitale gevaar moet concreet, voelbaar en emotioneel geladen worden gemaakt. Dit vraagt om het inzetten van een fear appeal (angstaanjaging) die direct wordt gekoppeld aan een haalbaar handelingsperspectief, gecombineerd met heldere vuistregels en menselijke impactverhalen.	• Fear appeal (met handelingsperspectief): Toon de directe, ingrijpende gevolgen van een overhaaste klik, maar koppel deze angst direct aan een simpel en moeiteloos uit te voeren alternatief (<i>Eén haastige klik op een sms-link kan je bankrekening binnen 5 seconden leegtrekken. Voorkom dit: controleer het bericht op dringende taal, sluit de sms direct en open zelf de officiële app van je bank</i>). • Vuistregels: Koppel 'kunstmatige paniek' in de communicatie direct aan het hoogste risiconiveau (<i>Echte bedrijven, banken of overheidsinstanties geven je nooit een deadline van een paar uur via e-mail, SMS of QR-code. Druk = Fraude</i>). • Visualisatie: Laat in korte video's of ervaringsverhalen de werkelijke menselijke ernst van een geslaagde hack zien (<i>Binnen 10 minuten waren al haar spaarcenten weg doordat ze dacht dat haar pakketje anders geretourneerd werd</i>). Dit verhoogt de gepercipieerde ernst op emotioneel niveau in plaats van op een abstract niveau.

Tactiek 2: Kennis verhogen (voor werknemers)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Tijdsdruk is een teken van online criminaliteit, omdat er misbruik wordt gemaakt van de eerste reflex die mensen hebben. Phishingaanvallen maken namelijk misbruik van snel, emotioneel handelen. Werknemers die precies weten hoe tijdsdruk er in een valse e-mail uitziet, herkennen de psychologische manipulatie sneller en trappen er minder snel in. Kennis zorgt ervoor dat het analytische brein tijdig inschakelt om de signaalwoorden te herkennen.	Het vergroten van de procedurele kennis over specifieke tijdsdrukindicatoren. Werknemers moeten via heldere frameworks, simulaties en formele garanties van instanties worden uitgerust om dringende taal direct te identificeren als een beveiligingsrisico. Benadruk dat criminelen tijdsdruk en urgente situaties expres/bewust inzetten omdat het mensen een paniekerig gevoel geeft, waardoor er minder rationeel gehandeld wordt.	• Vuistregels: Train werknemers om e-mails te scannen op de combinatie van drie specifieke factoren: (1) 📧 Grote emotie/druk (<i>Meteen actie vereist</i>), (2) ⏰ Korte deadline (<i>Binnen 4 uur</i>), en (3) 🔗 Directe actielink of QR-code. De vuistregel: <i>Zie je deze 3 samen? Dan is het 99% zeker phishing</i>. • Simulaties: Voer periodiek phishingtests uit die specifiek gericht zijn op werkgerelateerde spoed (bijvoorbeeld: <i>Factuur vandaag nog betalen, anders boete</i>). Werknemers die doorklikken, krijgen direct een korte leermodule waarin getoond wordt welke specifieke tijdsdruk-signalen ze over het hoofd zagen. • Garanties: Communiceer de harde garantie dat banken, de overheid en de eigen werkgever werknemers nooit onder tijdsdruk zullen zetten of direct dreigen met acute blokkades. Dit versterkt de instelling dat dringende taal per definitie duidt op fraude.

Hoe *stimuleren* we mensen om vaker *tijdsdruk te controleren*?

Tactiek 3: De descriptieve norm activeren (voor werknemers)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Mensen spiegelen hun gedrag aan hun directe werkomgeving. Als collega's en leidinggevenden laten zien dat zij gehaast op spoedberichten reageren, neemt het gehele team dat onveilige gedrag over. Als de heersende norm binnen de organisatie echter is dat spoedmails rustig en kritisch worden bekeken, past iedereen zijn werkwijze hierop aan.	Het onzichtbare gedrag van het bewust 'vertragen' en controleren van spoedmails zichtbaar maken. Dit gebeurt door het actief communiceren van de statistische groepsnorm en door leidinggevenden in te zetten als cultuurdragers en rolmodellen.	• Descriptieve norm communiceren: Deel de positieve cijfers uit onderzoek over de werkelijke alertheid op de werkvloer via intranet of posters bij de koffieautomaat (<i>Wist je dat 73% van de werknemers e-mails altijd controleert op tijdsdruk? Neem gerust de tijd, dat doet de rest ook.</i>). • Leidinggevenden als rolmodel: Laat managers in teamoverleggen expliciet benoemen wanneer ze een spoedmail wantrouwden en bewust niet direct handelden (<i>Ik kreeg vanmorgen een mail dat een leverancier 'vandaag nog' een wijziging wilde doorvoeren. Ik heb bewust niet geklikt maar even opgebeld. Bleek nep te zijn. Neem die tijd altijd!</i>).

Tactiek 4: Tijdsdrukgevoeligheid verlagen (voor werknemers)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Hoge werkdruk en de verwerkingssnelheid van e-mails (x mails per uur) maken werknemers extreem kwetsbaar. Wanneer een organisatie een cultuur kent waarin snel reageren wordt beloond, wint snelheid het van veiligheid. Tijdsdruk blokkeert rationeel nadenken, waardoor waarschuwingssignalen massaal over het hoofd worden gezien.	Het fysiek doorbreken van de automatische klikreflex op het moment van de reactie (disrupt-then-reframe), gecombineerd met organisatorische kaders en protocollen die werknemers de expliciete 'toestemming' geven om te vertragen.	• Disrupt-then-reframe: Richt de e-mailomgeving zo in dat bij externe mails met urgentiewoorden (<i>meteen, speed, direct</i>) automatisch een opvallende gele waarschuwingsbanner verschijnt. Dit onderbreekt het automatische typ- en klikgedrag en zet het bewuste brein aan. • Facilitering: Zorg voor kaders en protocollen. • De pauzevergunning: Neem de tijdsdrukgevoeligheid weg door werknemers vanuit het management formeel toestemming te geven om te vertragen (<i>Binnen ons bedrijf gaat veiligheid áltijd boven snelheid. Geen enkele legitieme spoedeisende zaak stort in als jij 2 minuten neemt om de afzender of link te controleren.</i>). • De 4-ogen-regel: Stel een vast werkprotocol in bij spoedverzoeken (<i>Bij e-mails die vragen om directe betaling, accountwijzigingen of spoedacties, bellen we áltijd eerst even met de afzender of een collega via een bekend nummer.</i>). Dit haalt de individuele druk van de ketel.

Inhoud controleren

66% van de consumenten controleert de inhoud van een e-mail altijd, 48% van de werknemers doet dit altijd.

Om het controleren van de inhoud te stimuleren zijn de belangrijkste gedragbepalers voor consumenten en werknemers:

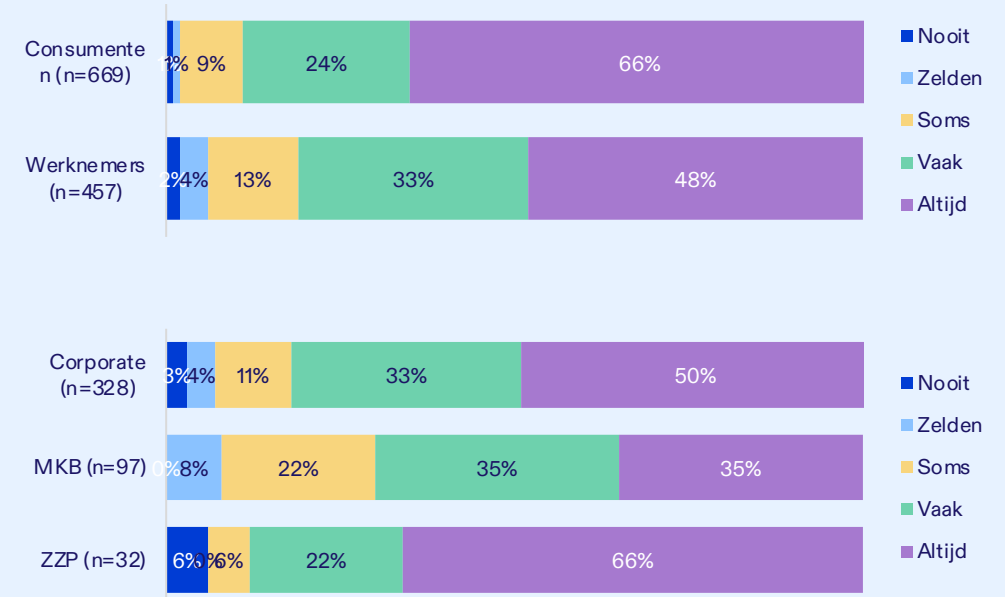
- **Risicoperceptie:** Hoe hoger consumenten en werknemers de kans schatten slachtoffer te worden (of hun organisatie) van online criminaliteit of fraude, online oplichting of phishing, hoe vaker ze de inhoud van hun e-mail controleren. Wanneer consumenten ervan overtuigd zijn dat de gevolgen ernstig kunnen zijn (bijvoorbeeld financiële gevolgen na het betalen van een vals betaalverzoek), controleren zij vaker de inhoud.
- **Kennis:** Wanneer consumenten weten waar zij op moeten letten om te controleren of een betaalverzoek betrouwbaar is, controleren ze vaker de inhoud van mails. Wanneer werknemers weten waar zij op moeten letten om te beoordelen of een e-mail, link of QR-code betrouwbaar is, controleren zij vaker de inhoud.
- **Inertia:** Wanneer mensen ervan overtuigd zijn dat het teveel tijd en moeite kost om onbekende of onverwachte e-mails goed te controleren, controleren zij minder vaak ze de inhoud.

Daarnaast zijn voor werknemers ook de volgende gedragbepalers van invloed:

- **Injunctieve norm:** Wanneer werknemers ervan overtuigd zijn dat een melding van een mogelijke beveiligingsfout wordt gewaardeerd binnen de organisatie, controleren zij vaker de inhoud.
- **Tijdsdrukgevoeligheid:** Wanneer werknemers ervaren dat zij snel moeten reageren op een e-mail, zijn zij sneller geneigd om te klikken, scannen of gegevens te delen en controleren zij minder vaak de inhoud.

Bij consumenten en werknemers speelt **geslacht** ook een rol en bij werknemers **stedelijkheid**. Vrouwen controleren de inhoud van een e-mail vaker dan mannen. Werknemers uit een van de 3 grote steden komt of randgemeenten controleren minder vaak de inhoud van een e-mail.

Ik controleer of de inhoud van de e-mail logisch is, bijvoorbeeld of ik echt iets verwacht.



Hoe *stimuleren* we mensen om vaker de *inhoud te controleren*?

Tactiek 1: Gepercipieerde kans en ernst van de gevolgen verhogen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Consumenten en werknemers zijn vaak overmoedig: zo gelooft 66-69% dat ze nepberichten kunnen herkennen aan spelfouten of dat hun e-mailfilters al het gevaar al afweren. Door de opkomst van AI zijn phishingmails tegenwoordig echter taalkundig en visueel foutloos, waardoor een louter visuele check onbetrouwbaar is geworden. Daarnaast heerst bij een deel de gedachte dat er 'bij hen niets te halen valt'. Zo schat 11-25% de kans op slachtofferschap laag in. Pas wanneer de gepercipieerde kans op misleiding én de financiële of organisatorische ernst realistisch en voelbaar worden gemaakt, stijgt de bereidheid om de inhoud te verifiëren.	De overtuiging doorbreken dat visuele inspectie of technologie voldoende bescherming biedt. Gebruikers moeten inzien dat de inhoudelijke logica (<i>Verwacht ik dit wel echt?</i>) een veel betrouwbaardere verdedigingslinie is. Dit vraagt om het concreet maken van de financiële en operationele impact bij misleiding.	• Zelfovertuiging: Stel consumenten de vraag '<i>Als een oplichter AI gebruikt om een e-mail taalkundig foutloos te maken, hoe zie je dan het verschil?</i>' of houd werknemers een spiegel voor '<i>IT filtert 95%, jij bent de laatste 5%</i>'. Doordat mensen hier zelf over nadenken, overtuigen ze zichzelf dat de inhoudelijke logica de enige betrouwbare controle is. • Fear appeal en loss aversion: Koppel de directe ernst van financieel of persoonlijk verlies (<i>Binnen 30 seconden je spaarrekening leeg via een nep-betaallink</i>) aan een concreet en direct uitvoerbaar handelingsperspectief (<i>Check bij elke e-mail of je echt een bericht of pakket verwacht voor je klikt</i>). • Storytelling: Gebruik gerichte scenario's voor specifieke functies om te tonen dat alleen een inhoudelijke check schade kan voorkomen. Bijvoorbeeld: de financiële administratie waarschuwen voor nagemaakte facturen of gewijzigde IBAN-nummers van bestaande leveranciers.

Tactiek 2: Kennis verhogen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Een deel van de mensen mist de praktische, procedurele kennis over hoe ze binnen enkele seconden de inhoud van een bericht effectief kunnen beoordelen (67% consumenten en 72% werknemers weet hoe ze een mail goed moeten controleren).	Het bieden van eenvoudige vuistregels, visuele gidsen en bindende protocollen die precies voorschrijven welke inhoudelijke vragen gesteld moeten worden en via welk alternatief kanaal verificatie moet plaatsvinden.	• Vuistregels: Train consumenten op twee vaststaande basisvragen voordat ze naar een betaalpagina gaan: (1) <i>Verwacht ik dit?</i> en (2) <i>Klopt de afzender met de context?</i> • Visuele gidsen: Bied duidelijke visuele vergelijkingen tussen officiële betaalomgevingen (iDEAL/Tikkie) en nepschermen die vragen om gevoelige inloggegevens. • Als-dan regels: Geef administratief personeel een bindend stappenplan bij betalings- of IBAN-wijzigingen: voer een context-check uit, open geen bijlagen in de mail, en verifieer het verzoek altijd mondeling via een reeds bekend telefoonnummer uit het CRM/ERP-systeem. • Default: Richt IT-systemen zo in dat elke IBAN-wijziging of betaling boven een bepaalde drempel automatisch wordt geblokkeerd totdat een tweede collega de wijziging handmatig accordeert.

Hoe *stimuleren* we mensen om vaker de *inhoud te controleren*?

Tactiek 3: Inertia verlagen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Als werknemers of consumenten het gevoel hebben dat het te veel tijd en moeite kost om een onbekende e-mail inhoudelijk uit te pluizen, haakt men af. De neiging om snel door te klikken wint het dan van een grondige inhoudelijke controle. Zo'n 15-18% van de mensen vindt mails controleren veel tijd en moeite kosten.	De cognitieve belasting drastisch verlagen door de inhoudelijke controle te versimpelen, de leesmoeite te minimaliseren en het verifiëren over te laten nemen door handige tools of geautomatiseerde gewoontes.	• Maak het makkelijk: Integreer een rapportageknop in Outlook waarmee werknemers een twijfelmail met 1 klik ter verificatie naar IT sturen, of toon automatische hints bij externe mails met woorden zoals 'factuur' of 'spoed' (💡 <i>Check de inhoud: Verwacht jij deze factuur?</i>). • Minimaliseer de leesmoeite: Leer werknemers de gewoonte aan om e-mails niet van A tot Z door te spitten, maar alleen te scannen op 3 ruis-factoren: (1) geen logische aanleiding, (2) een ongewoon verzoek, of (3) een mismatch tussen het verhaal en het bestandstype (bijvoorbeeld een .zip-bestand bij een factuur). • Als-dan regels: Train een vaste automatische reactie: <i>Als ik een e-mail of sms krijg met een betaallink of pakketstatus, dán sluit ik het bericht en check ik direct in mijn eigen app of bestelgeschiedenis of ik wel echt iets verwacht.</i>

Tactiek 4: Tijdsdrukgevoeligheid verlagen (voor werknemers)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Werkdruk, gehaast werken en stress zorgen ervoor dat werknemers terugvallen op snelle, automatische klikbeslissingen. Hierdoor wordt de inhoudelijke logica van een e-mail volledig over het hoofd gezien om de mail snel 'af te handelen'.	Het onderbreken van de gehaaste workflow op het moment dat een externe e-mail binnenkomt, gecombineerd met een heldere organisatienorm dat zorgvuldigheid áltijd boven snelheid gaat.	• Disrupt-then-reframe: Stel via IT in dat externe e-mails automatisch een opvallende gele waarschuwingsbanner krijgen. Dit verstoort de automatische klikreflex en dwingt tot een kort pauzemoment. • Injunctieve norm neerzetten: Management draagt expliciet uit dat later antwoorden vanwege een inhoudelijke controle wordt gezien als professioneel werk (<i>Een mail 10 minuten later beantwoorden omdat je de inhoud moest verifiëren is uitstekend. Ondoordacht handelen om van je mail af te zijn is een risico</i>).

Tactiek 5: Waardering van controleren verhogen (voor werknemers)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Werknemers schrikken soms terug voor inhoudelijke checks, omdat ze bang zijn collega's of leveranciers lastig te vallen, de voortgang te vertragen, of belachelijk te worden gemaakt. Wanneer er geen expliciete positieve bekrachtiging is voor het stellen van kritische vragen, blijft het melden of dubbelchecken van de inhoud achter.	Een werkklimaat scheppen waarin het inhoudelijk verifiëren van onduidelijke e-mails actief gewaardeerd, openlijk beloond en sociaal gecultiveerd wordt door de leidinggevenden en IT.	• Injunctieve norm communiceren en social modeling: Zorg voor directe positieve bekrachtiging vanuit IT of het management bij een inhoudelijke melding (<i>Scherp opgemerkt dat het rekeningnummer afweek, dankzij jou voorkomen we fraude!</i>). Laat managers vertellen (in korte video's) hoe zij onverwachte e-mails eerst telefonisch checken voordat ze actie ondernemen. • Interne 'phishing catchers' in het zonnetje zetten: Deel geanonimiseerde voorbeelden van echte, slimme e-mails die door werknemers zijn opgemerkt op basis van inhoudelijke inconsistenties. Dit maakt de waardering voor oplettendheid visueel en tastbaar voor de gehele organisatie.

Link *controleren*

36% van de consumenten controleert links altijd, 30% van de werknemers doet dit altijd.

Om het controleren van links te stimuleren zijn de belangrijkste gedragsbepalers voor consumenten en werknemers:

- **Kennis:** Hoe meer kennis iemand heeft over waar ze op moeten letten bij een mail of link, hoe vaker ze links controleren.

Daarnaast zijn voor consumenten de volgende gedragsbepalers van invloed:

- **Risicoperceptie:** Hoe ernstiger consumenten denken dat de financiële gevolgen zijn van een vals betaalverzoek betalen, hoe vaker ze links controleren.

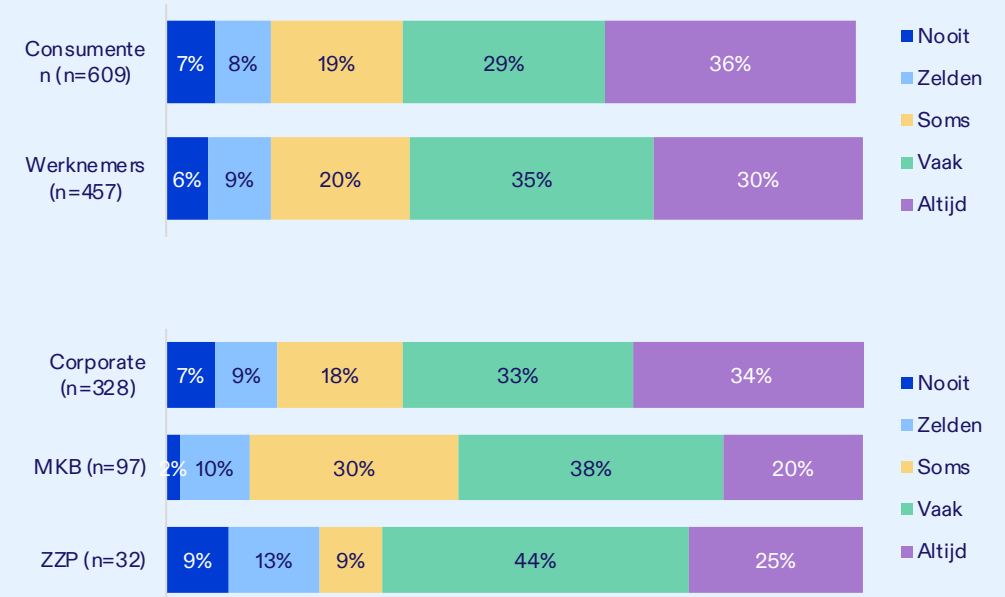
Voor werknemers zijn de volgende gedragsbepalers ook van invloed:

- **Descriptieve norm:** Hoe sterker de norm bij collega's, hoe vaker mensen links controleren of de intentie hebben om dit te doen.

Bij werknemers speelt **stedelijkheid** ook een rol en bij consumenten **leeftijd**. Iemand die uit een van de 3 grote steden komt of randgemeenten controleert minder vaak links dan iemand uit minder stedelijke gebieden. Oudere consumenten controleren vaker links controleert dan jongere consumenten.

Let op: zelfs met de tactieken en technieken op de volgende pagina is het erg moeilijk om links goed te kunnen controleren. Idealiter wordt dit gedrag dus niet gestimuleerd, maar worden alternatieve gedragingen gestimuleerd zoals naar de officiële website of app gaan.

Ik controleer waar een link naartoe gaat voordat ik erop klik.



Hoe *stimuleren* we mensen om vaker *links te controleren*?

Tactiek 1: Kennis verhogen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Mensen weten vaak wel dat phishinglinks bestaan en gevaarlijk zijn, maar ze missen de procedurele kennis: hoe lees je een URL exact, waar moet je op letten en hoe voer je een link-check uit op een smartphone? Mensen kijken uit gewoonte vaak alleen naar het begin van een link (bijv. [https://paypal.veilig-inloggen.nl] en nemen aan dat het klopt omdat ze een bekende merknaam zien staan. Gebrek aan deze praktische vaardigheid leidt ertoe dat men op het automatische gevoel afgaat.	Het aanreiken van eenvoudige, direct toepasbare vuistregels voor zowel pc als mobiel. Daarnaast moet het herkenningsvermogen worden getraind via gamification, zodat het brein leert om valse domeinnamen van leveranciers, IT-afdelingen of partners binnen enkele seconden te doorzien.	• Vuistregels: Leer gebruikers via korte visuals de vaste vuistregel aan om een domein van rechts naar links te lezen (zoek de .nl of .com en kijk welk woord er dáár direct voor staat). Dit ontmaskert misleidende merknamen aan het begin van de URL. • Instructievideo's: Train specifiek mobiel gedrag via korte video's waarin wordt voorgedaan hoe je de long-press (het lang ingedrukt houden van een link op een touchscreen) gebruikt. Hierdoor wordt de werkelijke bestemming zichtbaar gemaakt zonder de link direct te openen. • Gamification (zoek-de-verschillen): Bied korte, visuele quizen aan waarin consumenten en werknemers twee URL's naast elkaar zien en binnen 3 seconden de nep-variant moeten aanwijzen. Directe feedback helpt het brein om patronen sneller en automatisch te herkennen.

Tactiek 2: Gepercipieerde ernst en ervaren nut verhogen (voor consumenten)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Consumenten en werknemers controleren pas consequent links wanneer zij overtuigd zijn van de ernstige financiële gevolgen van een misleidende klik (bijvoorbeeld bij een vals betaalverzoek). De meeste consumenten zien het risico al sterk in, maar 21% niet of minder. Wanneer het nut van de controleactie of de ernst van de mogelijke schade als laag wordt ingeschat, wint het snelle gemak het van de alertheid.	Het rechtstreeks verbinden van de handeling 'links controleren' aan het beschermen van de eigen bankrekening of organisatie. Maak het directe verband tussen de controleactie en het voorkomen van materiële schade expliciet en voelbaar.	• Concreet maken van de schade: Koppel het controleren van de URL direct aan de financiële impact op de spaarrekening (<i>Eén onbedachtzame klik op een vals betaalverzoek of nep-iDEAL pagina kan je spaarrekening leegtrekken. Controleer altijd de URL in de adresbalk vóór je inlogt bij je bank</i>). Dit verhoogt het besef van de ernst en toont de directe effectiviteit van de controle aan.

Hoe *stimuleren* we mensen om vaker *links te controleren*?

Tactiek 3: Sociale norm activeren (voor werknemers)

Achtergrond

Links controleren is 'onzichtbaar gedrag': niemand ziet het fysiek als een collega of gezinslid met de muis boven een link zweeft. Daardoor denkt ons brein onbewust dat 'niemand dit doet'. Daarnaast heerst er soms schaamte of terughoudendheid om bij twijfel vragen te stellen of te verifiëren, uit angst om als achterdochtig of zeurderig gezien te worden. 53% van de werknemers ziet anderen dit niet doen.

Wat is er nodig?

Het onzichtbare checkgedrag zichtbaar maken door positieve trends te communiceren (zonder onveilig gedrag te normaliseren). Daarnaast moet het stellen van vragen sociaal geaccepteerd worden gemaakt en moeten leidinggevenden worden ingezet als openlijke rolmodellen.

Voorbeelden van technieken

- **Norm communiceren:** Wat doet de meerderheid? Deel positieve cijfers uit phishingtests of enquêtes via interne kanalen (*92% van onze collega's controleert inmiddels de URL van externe mails. 8 op de 10 collega's zweeft eerst met de muis over een link*). Dit zet de juiste sociale standaard neer.
- **Normaliseren van het 'dubbelchecken' en navragen:** Creëer een open werkklimaat waarin verifiëren wordt gewaardeerd (*Bij ons geldt: beter één keer te veel vragen of een link klopt, dan één keer te snel geklikt*). Dit haalt de schaamte rondom achterdocht weg.
- **Rolmodellen & zichtbare gedragsregels:** Laat leidinggevenden in korte video's of overleggen expliciet benoemen hoe zij zelf twijfelachtige links inspecteren en verifiëren voordat ze actie ondernemen.
- **Prompts:** Gebruik opvallende waarschuwingsbanners bij externe e-mails (⚠ Externe mail: Blijf 2 seconden met je muis op links staan om het adres te controleren). Dit onderbreekt de automatische klikreflex en dient als een directe trigger in het werkproces.

Afzender *controleren*

51% van de consumenten controleert de afzender altijd, 49% van de werknemers doet dit altijd.

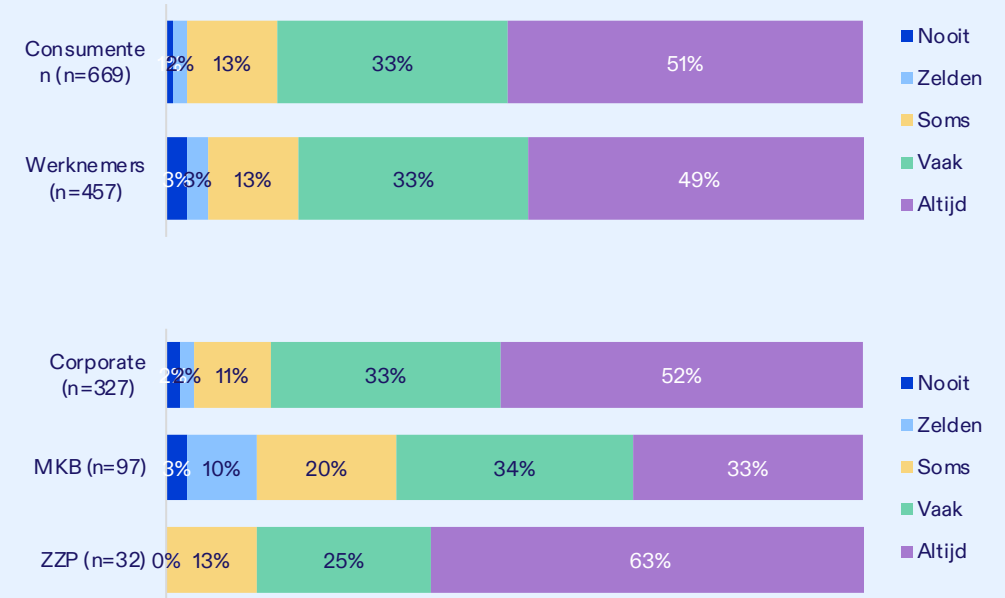
Om het controleren van de afzender te stimuleren zijn de belangrijkste gedragsbepalers voor consumenten en werknemers:

- **Kennis:** Mensen die weten waar zij op moeten letten om te beoordelen of een e-mail, link of QR-code betrouwbaar is, doen dit vaker. Consumenten die weten waar zij op moeten letten om te beoordelen of een betaalverzoek betrouwbaar is, doen dit vaker.

Voor consumenten is ook **risicoperceptie** (ernst van de gevolgen) van invloed en voor werknemers ook **inertia**. Consumenten die aangeven dat als zij een vals betaalverzoek betalen, de financiële gevolgen ernstig kunnen zijn, controleren vaker de afzender. Werknemers die het veel tijd en moeite vinden kosten om afzenders te controleren, doen dit minder vaak.

Bij werknemers spelen **geslacht** en **opleidingsniveau** ook een rol. Mannelijke en lageropgeleide werknemers controleren de afzender minder vaak dan vrouwelijke en anders opgeleide werknemers.

Ik kijk of het e-mailadres van de afzender logisch en betrouwbaar lijkt.



Hoe *stimuleren* we mensen om vaker de *afzender te controleren*?

Tactiek 1: Kennis verhogen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Een deel van de consumenten en werknemers mist de procedurele kennis om effectief achter het masker van de weergavenaam van de afzender te kijken. E-mailprogramma's tonen vaak alleen een vriendelijke of vertrouwde naam (bijvoorbeeld ING Bank of IT Desk), terwijl het werkelijke e-mailadres daaronder verborgen zit. Zonder praktische kennis over hoe men dit e-mailadres te voorschijn haalt en beoordeelt, gaan mensen af op de misleidende weergavenaam. 67% van de consumenten en 72% van de werknemers weet al wel hoe ze een mail controleren.	Het aanleren van concrete, eenvoudige controlehandelingen, het trainen van herkenning van typefouten in domeinnamen, en het leren matchen van automatische externe tags en banners met het werkelijke e-mailadres.	• Informeren via campagnes: Leer consumenten via korte instructievideo's of GIFs de vaste handeling aan om op de afzendernaam te tikken/klikken en specifiek het domein achter het @-teken te controleren op de exacte websitenaam van het bedrijf. • Beleid van instanties: Grote publieksorganisaties en banken communiceren transparant en expliciet vanaf welke specifieke e-maildomeinen zij uitsluitend communiceren, zodat afwijkingen voor de consument direct opvallen. • Trainen: • Train werknemers via korte modules in het herkennen van subtiele typefouten in bekende domeinen (zoals microsoft.com) en het spotten van externe e-mailadressen bij berichten die beweren intern te zijn. • Bied procedurele kennis om automatische systeembladen (zoals [EXTERN] of gele waarschuwingbalken) direct te verifiëren met het werkelijke e-mailadres van de afzender. • De hover-gewoonte: Leer werknemers via korte GIFs de 'zweef-reflex' aan (het op een pc of laptop met de muis over de afzendernaam bewegen zonder te klikken om het echte e-mailadres direct in een pop-up te controleren).

Tactiek 2: Gepercipieerde ernst van de gevolgen verhogen (voor consumenten)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Gebruikers die de ernst van de gevolgen inzien van een verkeerde klik, controleren vaker de afzender. Wanneer het niet-controleren van de afzender echter wordt gezien als een 'klein foutje', blijft alertheid achterwege. Pas als men doorziet dat een onbedachtzame klik kan leiden tot acute financiële schade of het uitvallen van de gehele organisatie, wordt het verifiëren van de afzender een prioriteit.	Het herframen van de consequenties van een verkeerde klik via loss framing, storytelling en het benadrukken van de verantwoordelijkheid richting collega's. De handeling 'afzender controleren' moet rechtstreeks worden gekoppeld aan het voorkomen van ingrijpende materiële of operationele schade.	• Loss framing: Benadruk wat men verliest bij het negeren van de afzendercheck (van het leegroven van de eigen bankrekening bij consumenten tot het stilleggen van de gehele organisatie via ransomware bij werknemers). • Storytelling: Deel realistische, geanonimiseerde praktijkvoorbeelden (zoals CEO-fraude of spear phishing) op het intranet of in teamoverleggen om te tonen hoe het manipuleren van afzendernamen leidde tot grote financiële en operationele schade. • Altercasting: Plaats mensen in een beschermende rol. Haak in op sociale loyaliteit op de werkvloer door te benadrukken dat het niet-controleren van de afzender kan leiden tot accountkaping, waarna de hacker onder jouw naam malware-mails stuurt naar je directe teamleden.

Hoe *stimuleren* we mensen om vaker de *afzender te controleren*?

Tactiek 3: Inertia verlagen (voor werknemers)

Achtergrond

Het controleren van het e-mailadres wordt dwarsgezeten door inertia (18% van de werknemers vindt het controleren van mails tijdrovend). Omdat e-mailprogramma's het echte e-mailadres standaard verbergen achter de weergavenaam, kan het handmatig opzoeken en verifiëren van het adres voelen als een vertragende, extra handeling in het werkproces.

Wat is er nodig?

Het technisch wegnemen van de frictie door e-mailadressen en waarschuwingen automatisch zichtbaar te maken via IT-instellingen, gecombineerd met het inslijpen van een geautomatiseerde, moeiteloze scan-gewoonte.

Voorbeelden van technieken

- **Systeemveranderingen en defaults:** Pas de instellingen in Outlook/Gmail organisatiebreed zo aan dat het volledige e-mailadres standaard zichtbaar is in de inbox, gecombineerd met automatische visuele waarschuwingslabels bij externe afzenders of mismatches met de weergavenaam.
- **Als-dan regels:** Leer werknemers een gewoonte aan via een simpele regel: *Als ik een nieuwe mail open, dán negeer ik de naam en trek ik in 1 seconde mijn oog direct naar het domein achter het @-teken.*

Vertrouwde betaalplatforms

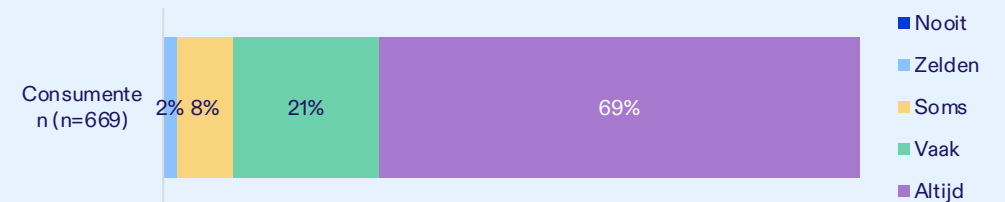
69% van de consumenten geeft aan dat zij altijd vertrouwde betaalplatforms gebruiken voor betaalverzoeken.

Om het gebruik van vertrouwde betaalplatforms te stimuleren zijn de belangrijkste gedragsbepalers voor consumenten:

- **Risicoperceptie:** Wanneer consumenten ervan overtuigd zijn dat de gevolgen ernstig kunnen zijn, gebruiken zij vaker vertrouwde betaalplatforms.

Leeftijd speelt ook een rol. Oudere mensen geven vaker aan dat zij altijd alleen vertrouwde betaalplatforms gebruiken voor betaalverzoeken.

Ik gebruik alleen vertrouwde betaalplatforms voor betaalverzoeken.



Hoe *stimuleren* we mensen om vaker *vertrouwde betaalplatforms* te gebruiken?

Tactiek 1: Gepercipieerde ernst van de gevolgen verhogen (voor consumenten)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Consumenten handelen bij digitale betalingen vaak op de automatische piloot of reageren impulsief op aantrekkelijke nep-marktplaatsdeals en emotionele situaties (zogenaamde 'vrienden in nood'). Ze staan daardoor op het afrekenmoment niet stil bij het reële risico dat hun complete bankrekening geplunderd kan worden via nagemaakte betaalomgevingen (zoals neppe iDEAL- of Tikkie-pagina's). Doordat het gevarieerde risico op de achtergrond abstract aanvoelt, is voor sommigen (21%) de gepercipieerde ernst van foutieve betaalverzoeken betalen laag en wint de snelle klikreflex het van het veiligheidsoverweging.	De reële financiële en persoonlijke schade moet direct, voelbaar en emotioneel geladen worden gemaakt. Tegelijkertijd moet de automatische klikreflex fysiek of mentaal worden onderbroken (disruptie) en direct gekoppeld worden aan een helder, moeiteeloos en herkenbaar handelingsperspectief: het handmatig betalen via de eigen, vertrouwde bank-app of -omgeving.	• Fear appeal en loss framing: Ontwikkel communicatie die het abstracte gevaar van neppe betaallinks tastbaar maakt door het potentiële verlies centraal te stellen (<i>Eén haastige klik op een betaallink van een onbekende partij kan je binnen 30 seconden al je spaargeld kosten</i>). De dreiging van gestolen bankgegevens wordt direct gekoppeld aan de actieve oplossing: uitsluitend betalen via de eigen vertrouwde bankomgeving. • Storytelling: Deel korte, herkenbare video's of persoonlijke verhalen van gewone Nederlanders (<i>Ik dacht dat ik 1 cent overmaakte om mijn Marktplaats-account te verifiëren. Binnen 5 minuten was mijn spaarrekening leeg</i>). Dit verhoogt de gepercipieerde ernst op een emotioneel en herkenbaar niveau, waarna direct de verlossende veilige gedragsregel wordt geboden. • Disrupt-then-reframe: Integreer in samenwerking met telefoonfabrikanten, browsers en e-mailproviders een automatische pop-up zodra een gebruiker op een onbekende of niet-gecertificeerde betaallink klikt. De pop-up onderbreekt de automatische klikreflex (🛑 <i>STOP: Je staat op het punt om te betalen via een onbekend platform</i>), herkadert de situatie door te dwingen stil te staan bij het risico, en biedt direct een knop voor de veilige route (<i>Breng me veilig naar mijn eigen bank-app</i>). • Als-dan regels & vuistregels: Leer consumenten via infographics en campagnes een 'als-dan' gewoonte aan om het besluitvormingsproces te automatiseren (<i>Als ik via sms, WhatsApp of e-mail een betaalverzoek of QR-code ontvang van een onbekende partij, dán sluit ik direct het bericht en open ik handmatig mijn eigen bank-app</i>). Koppel dringende spoed of druk direct aan het hoogste risiconiveau via de vuistregel: <i>Dringende toon = Fraude</i>.

Betaalverzoeken controleren

66% van de consumenten geeft aan dat zij altijd het bedrag, de ontvanger en de reden van betaling controleren bij betaalverzoeken.

Om het controleren van betaalverzoeken te stimuleren zijn de belangrijkste gedragsbepalers voor consumenten:

- **Risicoperceptie:** Wanneer iemand denkt dat de kans groot is dat hij ooit slachtoffer wordt van online criminaliteit of digitale fraude, controleren zij minder vaak betaalverzoeken. Wanneer consumenten ervan overtuigd zijn dat de gevolgen ernstig kunnen zijn (bijvoorbeeld financiële gevolgen na het betalen van een vals betaalverzoek), controleren zij vaker betaalverzoeken.
- **Inertia:** Wanneer iemand vindt dat het teveel tijd en moeite kost om betaalverzoeken goed te controleren, controleren zij minder vaak betaalverzoeken.

Stedelijkheid speelt ook een rol. Mensen in grote steden controleren minder vaak het bedrag, de ontvanger en de reden van betaling.

Ik controleer bij betaalverzoeken het bedrag, de ontvanger en de reden van betaling.



Hoe *stimuleren* we mensen om vaker *betalverzoeken te controleren*?

Tactiek 1: Gevoel van hulpeloosheid verlagen (voor consumenten)

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Wanneer consumenten de kans op slachtofferschap hoog inschatten, treedt er vaak angstverlamming en defensieve vermijding op. Het gevoel dat cybercriminaliteit overal is en dat men er 'toch wel een keer in trapt', leidt tot een ervaren verlies van controle. Consumenten stoppen vervolgens met actieve controle (<i>laat maar zitten, het helpt toch niet</i>). Deze hulpeloosheid zorgt ervoor dat zelfs simpele beveiligingsstappen bij betaalverzoeken achterwege blijven. 35% van de consumenten denkt dat ze slachtoffer kunnen worden van een foutief betaalverzoek.	De focus in de communicatie moet verschuiven van de onvermijdelijkheid van het gevaar naar de hoge effectiviteit en eenvoud van het controlegedrag. Consumenten moeten het inzicht krijgen dat zij zélf de regie hebben en dat een simpele handeling hen 100% beschermt.	• Empowerment: Ontwikkel communicatie die de consument niet benadert met dreigende taal, maar transformeert van passief slachtoffer naar actieve poortwachter: • Weerstand erkennen: <i>We snappen het. Online oplichters worden steeds slimmer en berichten lijken perfect. Het voelt soms alsof je er niks tegen kunt doen.</i> • Self-efficacy verhogen: <i>Maar jij hebt de regie over jouw geld. Oplichters proberen via misleidende berichten binnen te dringen, maar met één vaste reflex zet jij de deur stevig op slot. Je hoeft geen IT-expert te zijn om je spaargeld te beschermen: jouw eigen controle is de meest effectieve verdedigingslinie. Met één simpele reflex bouw je een ondoordringbaar schild om je spaargeld.</i> • De actie: <i>Oplichters zijn slim, maar jouw schild is sterker. Neem de controle: controleer het betaalverzoek.</i> Idealiter is dit handelingsperspectief zo concreet mogelijk.

Tactiek 2: Ernst van de gevolgen verhogen

Achtergrond	Wat is er nodig?	Voorbeelden van technieken
Enkele consumenten onderschatten de directe ernst van een enkele klik op een link, of de risico's van het overmaken van een schijnbaar klein bedrag (zoals € 0,01 ter verificatie). Ze verkeren in de veronderstelling dat 'even snel klikken' geen kwaad kan zolang er uiteindelijk niets betaald wordt, of dat kleine bedragen geen groot financieel risico dragen.	Het visueel en voelbaar maken dat een enkele klik of een klein verificatiebedrag in werkelijkheid de directe katalysator is voor het leegroven van de gehele spaarrekening. De psychologische drempelverlaging van kleine bedragen moet actief worden doorbroken.	• Visualisatie: Ontwikkel een korte animatie die toont dat klikken nooit zonder risico is. Bijvoorbeeld: Vergelijk een ondoordachte klik met een kettingbotsing. Een vinger tikt een link aan, waarna direct zichtbaar wordt hoe schadelijke software (malware) op de achtergrond meeleest met inlogpogingen of sessies kaapt. Boodschap: <i>Denk je dat even snel klikken geen kwaad kan zolang je niet betaalt? Criminelen gebruiken valse links om direct toegang te krijgen tot je telefoon. Klik nooit om 'even te checken', maar open altijd zelf de app.</i> • Disrupt-then-reframe: Doorbreek de drempelverlaging van 1 cent overmaken. Bijvoorbeeld: • Disrupt: Een commercial toont een bekende Marktplaats-situatie met een iDEAL-knop van € 0,01 (Maak 1 cent over om te verifiëren). • Reframe: Zodra de vinger de knop raakt, verandert deze in een gigantische magneet die met een luid metaalgeluid de bankpas, portemonnee, laptop en spaarpot het scherm in zuigt. • Boodschap: <i>Een vals betaalverzoek gaat nooit om die ene cent. Het is een magneet om je inloggegevens te stelen en je rekening leeg te roven. Controleer de ontvanger en het bedrag altijd op je eigen bank-app.</i>

Hoe *stimuleren* we mensen om vaker *betalaverzoeken te controleren*?

Tactiek 3: Inertia verlagen (voor consumenten)

Achtergrond

Betalingen worden door consumenten vaak snel en op de automatische piloot uitgevoerd. Als het inhoudelijk controleren van een betaalverzoek aanvoelt als een ingewikkelde, tijdrovende administratieve taak, haken consumenten af. 13% vindt betaalverzoeken controleren tijdrovend.

Wat is er nodig?

Het reduceren van de cognitieve belasting door het controleproces te vertalen naar een simpele, gestandaardiseerde routine die snel uitgevoerd kan worden.

Voorbeelden van technieken

- **Vuistregels:** Ontlast het brein door de controle terug te brengen tot een routine op 3 vaste punten vóór elke betaling:
 - **Bedrag:** Is dit op de cent nauwkeurig het afgesproken bedrag?
 - **Ontvanger:** Staat hier de exacte, echte naam van de persoon/het bedrijf, of zie ik een vreemde code?
 - **Reden:** Klopt de omschrijving met wat we hebben afgesproken?
 - **IBAN:** Komt het rekeningnummer overeen met de gegevens op de officiële website?
- **Prompts:** Verspreid opvallende stickers (3-seconden check) bij postpakketjes, banken of bibliotheken die consumenten op hun laptop of koelkast kunnen plakken als visuele herinnering.

Bijlage C:

Aanvullende resultaten

Op de volgende pagina's staan een aantal aanvullende resultaten van het vragenlijstonderzoek, zoals:

- Een beschrijving van de steekproef
- Beschrijvende resultaten van de gedragsbepalers
- Beschrijvende resultaten van de onderzochte scenario's.

Steekproef

In juni en juli 2026 is onder consumenten en werknemers de vragenlijst uitgezet naar cybergedragingen (privé en op het werk) en de achterliggende gedragsbepalers. Van de in totaal 987 deelnemers hebben 609 deelnemers de consumentenvragenlijst ingevuld en 378 deelnemers de werknemervragenlijst (mits zij werkend waren). Deze twee groepen zijn meegenomen in de analyses.

Daarnaast is voor werknemers de groep verder uitgesplitst in werksituatie: ZZP, MKB (werkzaam bij een bedrijf met 50 of minder werknemers) en corporate (werkzaam bij een bedrijf met meer dan 50 werknemers). De verdeling van groepen naar werksituatie heeft te kleine subgroepen om statistisch te vergelijken. Daarom zijn die resultaten alleen beschrijvend weergegeven in het rapport.

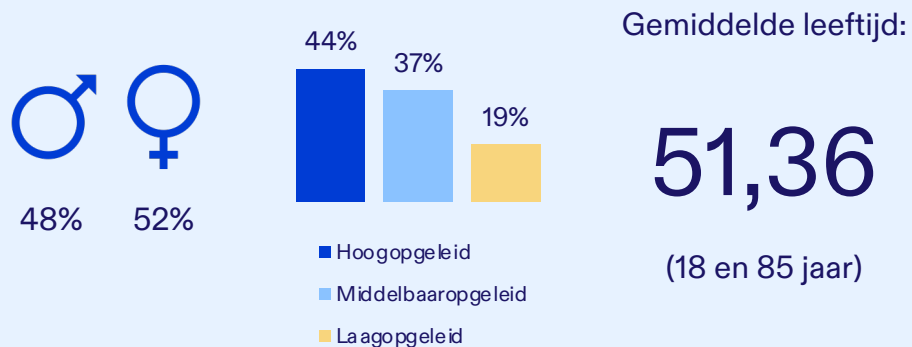
*De resultaten van de vragenlijst zijn gewogen. Dit betekent dat er een correctie is toegevoegd om te zorgen dat de steekproef een eerlijke spiegel is van de totale groep consumenten en werknemers. In de data zitten namelijk enkele groepen die over- en ondervertegenwoordigd zijn. Door weging toe te voegen, tellen ondervertegenwoordigde groepen zwaarder en oververtegenwoordigde groepen minder zwaar. Zo wordt de data meer representatief voor de echte doelgroep. Dit betekent ook dat de steekproefaantallen naast sommige grafieken hoger of lager zijn dan het totaal aantal geworven deelnemers dat vermeld staat op deze pagina.



Steekproef

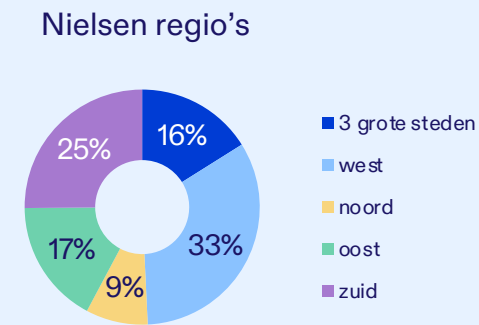
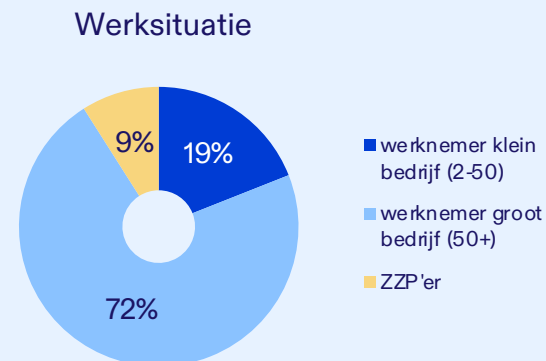
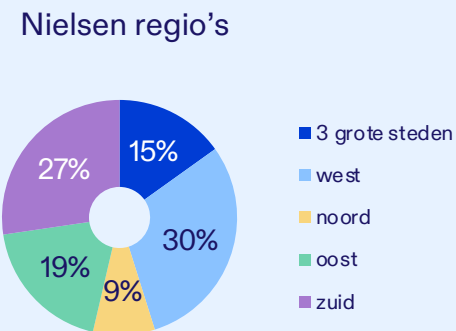
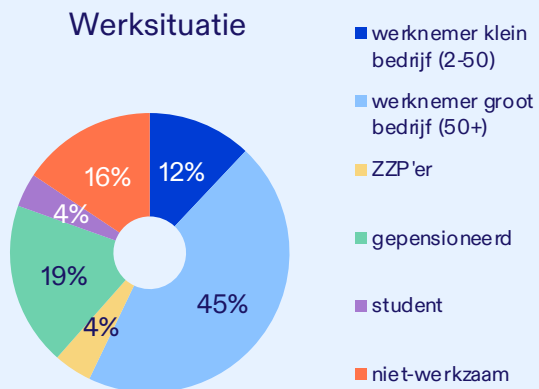
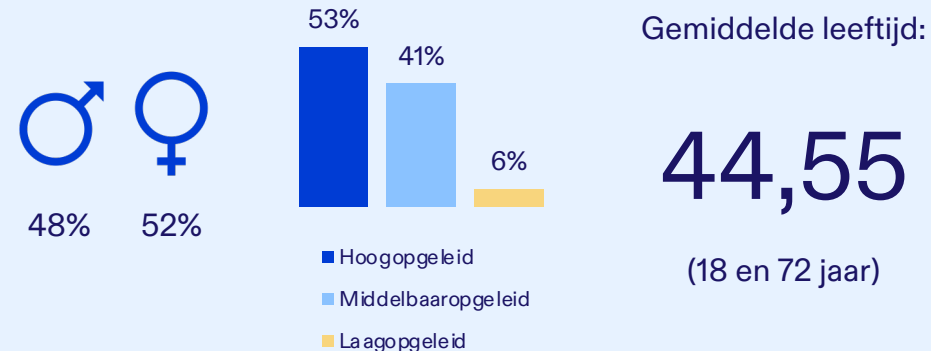
Consumenten (N = 609)

- Van de respondenten is 48,3% man en 51,7% vrouw. De gemiddelde leeftijd is 51,36 jaar, met een spreiding tussen 18 en 85 jaar.
- 44,2% van de deelnemers is hoogopgeleid, 36,9% middenopgeleid en 18,9% laagopgeleid. In totaal is 61,6% werkzaam.



Werknemers (N = 378)

- Van de respondenten is 48,1% man en 51,9% vrouw. De gemiddelde leeftijd is 44,55 jaar, met een spreiding tussen 18 en 72 jaar.
- 52,9% van de deelnemers is hoogopgeleid, 41,0% middenopgeleid en 6,1% laagopgeleid. In totaal is 72,2% werkzaam in een corporate bedrijf, 19,3% in het MKB en 8,5% is ZZP'er.



Gedragsebepalers

Op de volgende pagina's is meer informatie te vinden over de gedragsebepalers uitgevraagd bij het vragenlijstonderzoek. Eerst volgt een overzicht van de stellingen van de bepalers. Daarna wordt per gedragsebepaler de verdeling weergegeven van hoe consumenten en werknemers hier gemiddeld op scoren. Dit geeft bijvoorbeeld een beeld van hoeveel kennis deze doelgroepen zeggen te hebben of in hoeverre zij inschatten dat ze slachtoffer kunnen worden van een cyberaanval.

Opvallende gedragsebepalers

- Veel mensen staan open voor meer cyberveilig gedrag. Alleen voor 2FA en wachtwoordmanager blijft de intentie nog wat achter.
- Kennis en self-efficacy is bij de meesten aanwezig. Vooral AI-richtlijnen zijn minder bekend.
- Risicoperceptie is hoog. Mensen denken dat de gevolgen van online criminaliteit ernstig kunnen zijn. De kans om zelf slachtoffer te worden van online criminaliteit ligt bij werknemers een stuk hoger dan bij consumenten. Mails en betaalverzoeken controleren wordt gezien als een zeer effectieve methode om de kans op phishing en oplichting te verkleinen. 2FA en wachtwoordmanagers worden echter nog minder vaak als effectief gezien.
- Ook voor AI zien mensen risico's. Een redelijk deel vertrouwt de AI-aanbieder niet en is bang dat de aanbieder misbruik maakt van hun data. Ook zijn ze het er meestal niet mee eens om veiligheid in te leveren voor meer efficiëntie.
- Wachtwoordmanagers en 2FA gebruiken worden het vaakst als tijdrovend gezien, in vergelijking met betaalverzoeken en mails controleren en fouten melden.



Stellingen *intenties*

Voor een aantal gedragingen is ook de intentie uitgevraagd. Deze intenties zijn uitgevraagd op een 5-puntschaal: zeker niet t/m zeker wel.

Consumenten

Gedragsebepaler	Stelling
Intentie emails controleren	Ben je van plan om in de toekomst (vaker) het e-mailadres te controleren?
Intentie links controleren	Ben je van plan om in de toekomst (vaker) een link te controleren?
Intentie betaalverzoek controleren	Ben je van plan om in de toekomst (vaker) een betaalverzoek te controleren?
Intentie 2FA	Ben je van plan om in de toekomst (vaker) 2FA te gebruiken voor jouw persoonlijke accounts?
Intentie wachtwoordmanager	Ben je van plan om in de toekomst (vaker) een wachtwoordmanager te gebruiken voor jouw persoonlijke online accounts?
Intentie informatie delen met AI	Ben je van plan om in de toekomst (vaker) persoonlijke informatie met AI-tools te delen?

Werknemers

Gedragsebepaler	Stelling
Intentie emails controleren	Ben je van plan om in de toekomst (vaker) het e-mailadres te controleren?
Intentie links controleren	Ben je van plan om in de toekomst (vaker) een link te controleren?
Intentie fout melden	Ben je van plan om in de toekomst (vaker) een cyberfout te melden bij jouw organisatie ?
Intentie 2FA	Ben je van plan om in de toekomst (vaker) 2FA te gebruiken voor jouw werk-accounts
Intentie wachtwoordmanager	Ben je van plan om in de toekomst (vaker) een wachtwoordmanager te gebruiken voor jouw online werkaccounts
Intentie informatie delen met AI	Ben je van plan om in de toekomst (vaker) werk-gerelateerde informatie met AI-tools te delen?

Stellingen *gedragsbepalers* – Controleren

De gedragsbepalers voor consumenten zijn eveneens uitgevraagd op een 5-puntschaal: helemaal mee oneens t/m helemaal mee eens.

Gedragsbepaler	Stelling
Kans op slachtofferschap algemeen	Ik denk dat de kans groot is dat ik ooit slachtoffer word van online criminaliteit of digitale fraude.
Gevolgen ernstig algemeen	De gevolgen van online criminaliteit of digitale fraude kunnen voor mij ernstig zijn.
Kans op slachtofferschap mails	Ik denk dat ik zelf slachtoffer kan worden van phishing of online oplichting via e-mail.
Gevolgen ernstig mails	Als ik op een verkeerde link klik of QR-code scan kunnen de gevolgen ernstig zijn.
Response-efficacy mails	Door een e-mail goed te controleren voordat ik klik, scan of betaal, kan ik de kans op phishing of oplichting verkleinen.
Self-efficacy mails	Ik vertrouw erop dat ik een verdachte e-mail kan herkennen.
Inertia mails	Het kost mij te veel tijd en moeite om onbekende of onverwachte e-mails goed te controleren.
Kennis mails	Ik weet waar ik op moet letten om te beoordelen of een e-mail, link of QR-code betrouwbaar is.

Gedragsbepaler	Stelling
Attitude mails controleren	Ik vind het belangrijk om onbekende of onverwachte e-mails goed te controleren voordat ik iets doe.
Hulpeloosheid	Als internetcriminelen mij echt willen misleiden, kan ik daar weinig tegen doen.
Kans op slachtofferschap betaalverzoek	Ik denk dat ik zelf slachtoffer kan worden van fraude via een nep betaalverzoek.
Gevolgen ernstig betaalverzoek	Als ik een vals betaalverzoek betaal, kunnen de financiële gevolgen ernstig zijn.
Response-efficacy betaalverzoek	Door een betaalverzoek goed te controleren voordat ik betaal, kan ik de kans op fraude verkleinen.
Self-efficacy betaalverzoek	Ik vertrouw erop dat ik een verdacht of nep betaalverzoek kan herkennen.
Inertia betaalverzoeken	Het kost mij te veel tijd en moeite om betaalverzoeken goed te controleren voordat ik betaal.
Kennis betaalverzoeken	Ik weet waar ik op moet letten om te beoordelen of een betaalverzoek betrouwbaar is.
Attitude betaalverzoek	Ik vind het belangrijk om betaalverzoeken goed te controleren voordat ik betaal.

Stellingen *gedragsbepalers* – Controleren

De gedragsbepalers voor werknemers zijn eveneens uitgevraagd op een 5-puntschaal: helemaal mee oneens t/m helemaal mee eens.

Gedragsbepaler	Stelling
Kans op slachtofferschap algemeen	Ik denk dat mijn organisatie slachtoffer kan worden van phishing of online oplichting via mijn werk-mail.
Gevolgen ernstig algemeen	Als ik op een verkeerde link klik, een QR-code scan of gegevens verkeerd deel, kunnen de gevolgen voor mijn organisatie ernstig zijn.
Response-efficacy mails	Door een e-mail goed te controleren voordat ik klik, scan of gegevens deel, kan ik de kans op phishing of oplichting verkleinen voor mijn organisatie.
Self-efficacy mails	Ik vertrouw erop dat ik een verdachte werk-mail kan herkennen.
Inertia mails	Het kost mij te veel tijd en moeite om onbekende of onverwachte e-mails goed te controleren.
Kennis mails	Ik weet waar ik op moet letten om te beoordelen of een e-mail, link of QR-code betrouwbaar is.
Attitude mails	Ik vind het belangrijk om onbekende of onverwachte e-mails goed te controleren voordat ik iets doe.
Descriptieve norm mails	Collega's en leidinggevendenden controleren onbekende of onverwachte e-mails voordat zij op een link klikken, een QR-code scannen of gegevens delen.

Gedragsbepaler	Stelling
Hulpeloosheid mails	Als internetcriminelen mij echt willen misleiden, kan ik daar weinig tegen doen.
Tijdsdruk-gevoeligheid	Als een e-mail zegt dat ik snel moet reageren, ben ik sneller geneigd om te klikken, scannen of gegevens te delen.
Injunctie norm fout melden	Het melden van een mogelijke beveiligingsfout wordt binnen onze organisatie gewaardeerd.
Angst baanverlies	Ik ben bang dat melden dat ik een cyberfout heb gemaakt, negatieve gevolgen heeft voor mijn loopbaan binnen deze organisatie.
Self-efficacy melden	Ik voel mij volledig in staat om een cyberfout of beveiligingsincident op de juiste manier te melden.
Inertia melden	Het melden van een cyberfout via onze systemen kost mij veel tijd.

Stellingen *gedragsebepalers* – 2FA

De gedragsebepalers voor consumenten zijn eveneens uitgevraagd op een 5-puntschaal: helemaal mee oneens t/m helemaal mee eens.

Gedragsebepaler	Stelling
Systeemdwang	Ik gebruik twee-factor-authenticatie voor mijn accounts alleen wanneer dit verplicht is. <i>*Als je zelf geen 2FA gebruikt, probeer de vraag dan te beantwoorden vanuit de gedachte: "Als ik 2FA zou gebruiken, dan gebruik ik twee-factor-authenticatie voor mijn accounts alleen wanneer dit verplicht is."</i>
Default	Ik gebruik twee-factor-authenticatie voor mijn accounts alleen wanneer dit automatisch aan staat. <i>*Als je zelf geen 2FA gebruikt, probeer de vraag dan te beantwoorden vanuit de gedachte: "Als ik 2FA zou gebruiken, dan gebruik ik twee-factor-authenticatie voor mijn accounts alleen wanneer dit automatisch aan staat."</i>
Kennis	Ik weet hoe ik twee-factor-authenticatie kan aanzetten voor mijn accounts.
Sociale norm	Mensen in mijn omgeving (familie, vrienden, collega's) beveiligen hun accounts met tweestapsverificatie.
Self-efficacy	Ik vertrouw erop dat ik eventuele problemen met inlogcodes of verificatie-apps zelf kan oplossen.
Angst toegangsverlies	Ik ben bang dat ik toegang tot accounts verlies wanneer mijn twee-factor-authenticatie faalt, bijvoorbeeld als ik mijn telefoon kwijtraak.

Gedragsebepaler	Stelling
Inertia	Het extra inloggen via twee-factor-authenticatie kost mij te veel tijd en moeite in het dagelijks gebruik.
Response-efficacy	Ik ben ervan overtuigd dat twee-factor-authenticatie het risico dat mijn accounts gehackt worden wegneemt.
Optimisme	Ik heb geen twee-factor-authenticatie nodig, omdat ik zelf al voorzichtig genoeg ben online.
Reactance	Ik ervaar de controles via tweestapsverificatie als een belemmering van mijn digitale vrijheid.

Stellingen *gedragsbepalers* – 2FA

De gedragsbepalers voor werknemers zijn eveneens uitgevraagd op een 5-puntschaal: helemaal mee oneens t/m helemaal mee eens.

Gedragsbepaler	Stelling
Systeem-dwang	Ik gebruik twee-factor-authenticatie voor mijn werkaccounts alleen wanneer dit verplicht is. <i>*Als je zelf geen 2FA gebruikt, probeer de vraag dan te beantwoorden vanuit de gedachte: "Als ik 2FA zou gebruiken, dan gebruik ik twee-factor-authenticatie voor mijn werkaccounts alleen wanneer dit verplicht is."</i>
Default	Ik gebruik twee-factor-authenticatie voor mijn werkaccounts alleen wanneer dit automatisch aan staat. <i>*Als je zelf geen 2FA gebruikt, probeer de vraag dan te beantwoorden vanuit de gedachte: "Als ik 2FA zou gebruiken, dan gebruik ik twee-factor-authenticatie voor mijn werkaccounts alleen wanneer dit automatisch aan staat."</i>
Kennis	Ik weet hoe ik twee-factor-authenticatie kan aanzetten voor mijn accounts.
Sociale norm	Mijn collega's beveiligen hun accounts met tweestapsverificatie.
Self-efficacy	Ik vertrouw erop dat ik eventuele problemen met inlogcodes of verificatie-apps zelf kan oplossen.
Angst toegangsverlies	Ik ben bang dat ik toegang tot werkaccounts verlies wanneer mijn twee-factor-authenticatie faalt, bijvoorbeeld als ik mijn telefoon of token kwijtraak.

Gedragsbepaler	Stelling
Authenticatie-moeheid	Het extra inloggen via twee-factor-authenticatie kost mij te veel tijd en moeite in mijn werk.
Response-efficacy	Ik ben ervan overtuigd dat twee-factor-authenticatie het risico dat mijn werkaccounts gehackt worden wegneemt.
Optimisme	Ik heb geen twee-factor-authenticatie nodig, omdat ik zelf al voorzichtig genoeg ben online.
Reactance	Ik ervaar de controles via tweestapsverificatie als een belemmering van mijn digitale vrijheid.

Stellingen *gedragsbepalers* – Wachtwoord

De gedragsbepalers voor consumenten zijn eveneens uitgevraagd op een 5-puntschaal: helemaal mee oneens t/m helemaal mee eens.

Gedragsbepaler	Stelling
Default	Ik maak alleen gebruik van een wachtwoordmanager als deze standaard is ingebouwd in mijn webbrowser (zoals Chrome/Safari) of smartphone. <i>*Als je zelf geen wachtwoordmanager gebruikt, probeer de vraag dan te beantwoorden vanuit de gedachte: "Als ik een wachtwoordmanager zou gebruiken, dan maak ik alleen gebruik van een wachtwoordmanager als deze standaard is ingebouwd in mijn webbrowser (zoals Chrome/Safari) of smartphone."</i>
Kennis	Ik weet hoe ik een wachtwoordmanager kan gebruiken voor mijn accounts.
Sociale norm	Mensen in mijn omgeving (familie, vrienden, collega's) maken gebruik van een wachtwoordmanager.
Self-efficacy	Ik vertrouw erop dat ik eventuele problemen met een wachtwoordmanager zelf kan oplossen.
Angst voor lockout	Ik ben bang dat ik nergens meer bij kan als ik het hoofdwachtwoord van mijn wachtwoordkluis vergeet.
Moeite	Ik vind de tijd en moeite die het kost om al mijn bestaande accounts over te zetten naar een wachtwoordmanager een veel te grote drempel.
Response-efficacy	Ik geloof dat het gebruik van een wachtwoordmanager effectief helpt om te voorkomen dat mijn accounts gehackt worden.

Gedragsbepaler	Stelling
Cognitieve belasting	Het gebruik van een wachtwoordmanager geeft mij rust in mijn hoofd, omdat ik niet langer tientallen unieke inloggegevens zelf hoeft te onthouden.
Wantrouwen	Ik vind het riskant om al mijn wachtwoorden op één centrale plek op te slaan.
Alternatief	Ik vind het veiliger om mijn wachtwoorden op papier op te schrijven dan om ze digitaal op te slaan.

Overige stelling:

- Wat voor soort wachtwoordmanager gebruik je? Meerdere antwoorden mogelijk
 - Ingebouwd in mijn browser of telefoon (zoals Chrome, Safari, Apple of Google)
 - Via een aparte app of dienst (zoals Bitwarden, 1Password of LastPass)
 - Anders, namelijk: _____

Stellingen *gedragsbepalers* – Wachtwoord

De gedragsbepalers voor werknemers zijn eveneens uitgevraagd op een 5-puntschaal: helemaal mee oneens t/m helemaal mee eens.

Gedragsbepaler	Stelling
Default	Ik maak alleen gebruik van een wachtwoordmanager als deze standaard is ingebouwd in mijn webbrowser (zoals Chrome/Safari) of werktelefoon (bijvoorbeeld omdat de IT-afdeling dit standaard installeert). <i>*Als je zelf geen wachtwoordmanager gebruikt, probeer de vraag dan te beantwoorden vanuit de gedachte: "Als ik een wachtwoordmanager zou gebruiken, dan maak ik alleen gebruik van een wachtwoordmanager als deze standaard is ingebouwd in mijn webbrowser (zoals Chrome/Safari) of werktelefoon (bijvoorbeeld omdat de IT-afdeling dit standaard installeert)."</i>
Kennis	Ik weet hoe ik een wachtwoordmanager kan gebruiken voor mijn werkaccounts.
Sociale norm	Mijn collega's maken gebruik van een wachtwoordmanager.
Self-efficacy	Ik vertrouw erop dat ik eventuele problemen met een wachtwoordmanager zelf kan oplossen.
Angst voor lockout	Ik ben bang dat ik nergens meer bij kan als ik het hoofdwachtwoord van mijn wachtwoordkluis vergeet.
Moeite	Ik vind de tijd en moeite die het kost om al mijn bestaande werkaccounts over te zetten naar een wachtwoordmanager een veel te grote drempel.
Response-efficacy	Ik geloof dat het gebruik van een wachtwoordmanager effectief helpt om te voorkomen dat mijn werkaccounts gehackt worden.

Gedragsbepaler	Stelling
Cognitieve belasting	Het gebruik van een wachtwoordmanager geeft mij rust in mijn hoofd, omdat ik niet langer tientallen unieke inloggegevens zelf hoeft te onthouden.
Risikant	Ik vind het riskant om al mijn wachtwoorden op één centrale plek op te slaan.
Alternatief	Ik vind het veiliger om mijn wachtwoorden op papier op te schrijven dan om ze digitaal op te slaan.

Overige stelling:

- Wat voor soort wachtwoordmanager gebruik je? Meerdere antwoorden mogelijk
 - Ingebouwd in mijn browser of telefoon (zoals Chrome, Safari, Apple of Google)
 - Via een aparte app of dienst (zoals Bitwarden, 1Password of LastPass)
 - Anders, namelijk: _____

Stellingen *gedragsbepalers* – AI

De gedragsbepalers voor consumenten zijn eveneens uitgevraagd op een 5-puntschaal: helemaal mee oneens t/m helemaal mee eens.

Gedragsbepaler	Stelling
Doelen bereiken	Het gebruik van AI helpt mij om mijn persoonlijke doelen veel sneller te bereiken.
Kwaliteit boven veiligheid	De kwaliteit van de AI-antwoorden is zo hoog dat ik bereid ben om wat privacy op te offeren.
Descriptieve norm	Mensen in mijn omgeving (familie, vrienden, collega's) maken gebruik van AI.
Aanbieder misbruikt	Ik maak me grote zorgen dat de informatie die ik deel door de AI-aanbieder kan worden misbruikt.
Aanbieder vertrouwen	Ik vertrouw erop dat de aanbieder van de AI-tool eerlijk en oprecht is over hoe mijn data wordt gebruikt
AI is empathisch	Ik heb het gevoel dat de AI-chatbot mij echt begrijpt en op een empathische manier reageert
Angst data inzien	Ik ben bang dat andere mensen de informatie die ik met AI deel kunnen inzien.
Self-efficacy	Ik heb er alle vertrouwen in dat ik de AI-tool veilig kan gebruiken zonder mijn privacy te schenden.
Niet zonder kunnen	Ik zou niet meer zonder AI kunnen in mijn dagelijkse leven.
Kennis privacybeleid	Ik ben goed op de hoogte van het privacybeleid van de AI-tools die ik gebruik.

Overige stellingen:

- Van welk type AI-tools maak je vooral gebruik voor werk?
 - Europese AI-tools (zoals Mistral AI - Le Chat, Proton Lumo, GreenPT, Aleph Alpha)
 - Niet-Europese AI-tools (zoals ChatGPT, Claude, Gemini, Microsoft Copilot)
 - Beide
- Hoe vaak precies maak je gebruik van AI-tools voor werk?
 - Meerdere keren per dag
 - Dagelijks
 - Wekelijks
 - Maandelijks
 - Minder dan één keer per maand

Stellingen *gedragsbepalers* – AI

De gedragsbepalers voor werknemers zijn eveneens uitgevraagd op een 5-puntschaal: helemaal mee oneens t/m helemaal mee eens.

Gedragsbepaler	Stelling
Doelen bereiken	Het gebruik van AI helpt mij om mijn werkdoelen aanzienlijk te verbeteren.
Kwaliteit boven veiligheid	De productiviteitsverhoging door AI is zo groot dat eventuele risico's voor mijn organisatie acceptabel zijn.
Descriptieve norm	Collega's en leidinggevendenden maken gebruik van AI.
Risico datalek	Ik maak me grote zorgen dat het invoeren van bedrijfsdata in een AI-tool kan leiden tot een datalek.
Aanbieder vertrouwen	Ik vertrouw erop dat de aanbieder van de AI-tool eerlijk en oprecht is over hoe de data van mijn organisatie wordt gebruikt.
AI is empathisch	Ik heb het gevoel dat de AI-chatbot mij echt begrijpt en op een empathische manier reageert.
Angst data inzien	Ik ben bang dat andere mensen en organisaties de informatie die ik met AI deel kunnen inzien.
Self-efficacy	Ik heb er alle vertrouwen in dat ik de AI-tool veilig kan gebruiken zonder de veiligheidsregels van mijn organisatie te overtreden.
Niet zonder kunnen	Ik zou niet meer zonder AI kunnen in mijn werkleven.
Kennis AI-richtlijnen	Ik ben goed op de hoogte van de AI-richtlijnen en het veiligheidsbeleid van mijn organisatie.

Gedragsbepaler	Stelling
Angst baanverlies	Ik ben bang mijn baan of reputatie in gevaar te brengen als ik geen AI gebruik.
Duidelijke regels	Mijn organisatie heeft duidelijke regels over het gebruik van AI-tools.
Kennis welke mogen	Ik weet welke AI-tools ik wel of niet mag gebruiken voor werk.
Tools organisatie	De officiële AI-tools binnen mijn organisatie voldoen aan mijn behoeften.

Overige stellingen:

- Van welk type AI-tools maak je vooral gebruik voor werk?
 - Europese AI-tools (zoals Mistral AI - Le Chat, Proton Lumo, GreenPT, Aleph Alpha)
 - Niet-Europese AI-tools (zoals ChatGPT, Claude, Gemini, Microsoft Copilot)
 - Beide
- Hoe vaak precies maak je gebruik van AI-tools voor werk?
 - Meerdere keren per dag
 - Dagelijks
 - Wekelijks
 - Maandelijks
 - Minder dan één keer per maand

Intentie

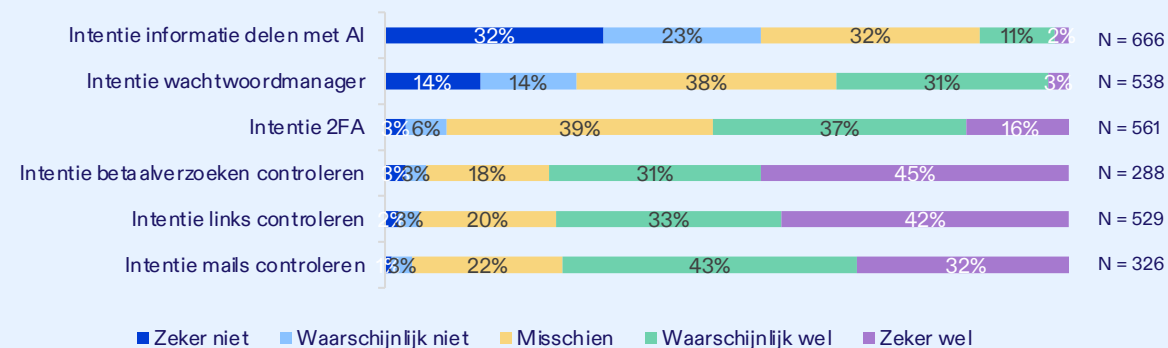
Intentie

- De intentie om betaalverzoeken (76%) en links te controleren is het hoogste (75% voor consumenten, 69% voor werknemers).
- De intentie om een wachtwoordmanager te gebruiken is het laagste (34% voor consumenten, 31% voor werknemers). Er is zelfs een aanzienlijke groep dat het waarschijnlijk of zeker niet van plan is (28% voor consumenten, 33% voor werknemers).
- De intentie om informatie te delen met AI is laag. 55% van de consumenten en 44% van de werknemers zou dit zeker niet of waarschijnlijk niet doen.

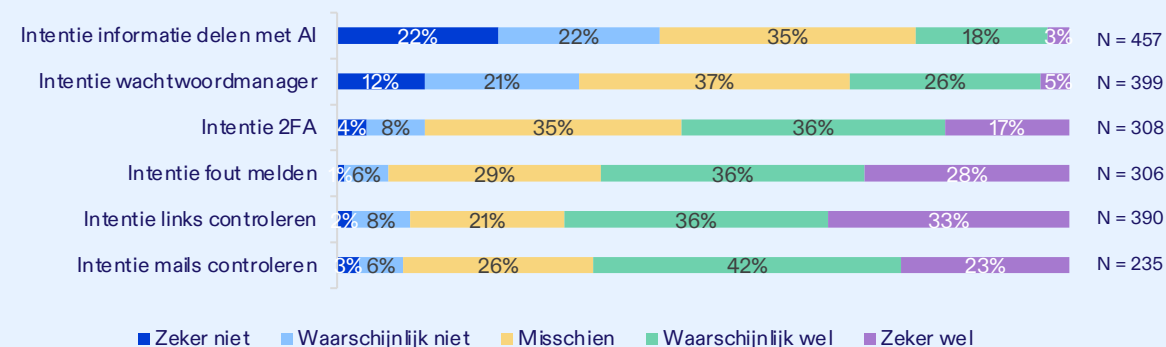
Leeswijzer: Op deze en de volgende pagina's staan de resultaten per gedragsebepaler, steeds boven voor consumenten en onder voor werknemers. De genoemde percentages zijn het aandeel respondenten dat het (helemaal) (on)eens is met de stelling.

De steekproefgrootte (N) verschilt per stelling, omdat niet elke vraag aan iedereen is voorgelegd en de data gewogen zijn. Zo is de intentievraag is alleen gesteld aan wie het gedrag nog niet altijd vertoont. De intentiecijfers zijn dus niet direct naast de andere gedragsebepalers te leggen.

Consumenten



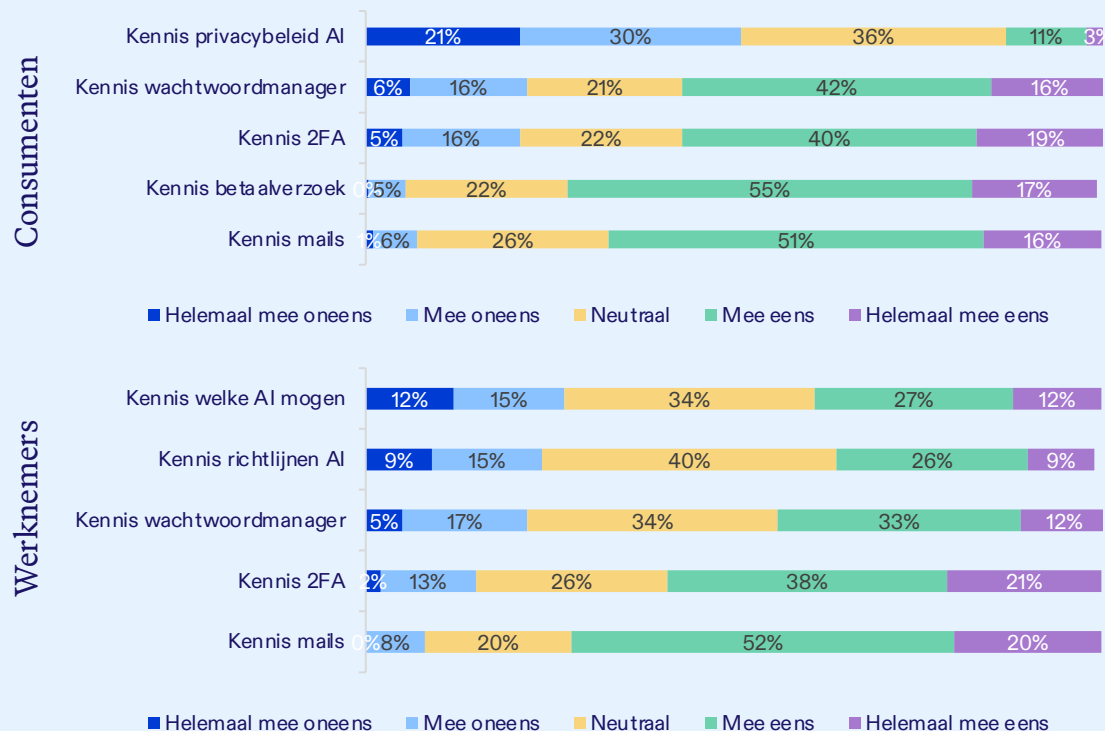
Werknemers



Kennis en kunde

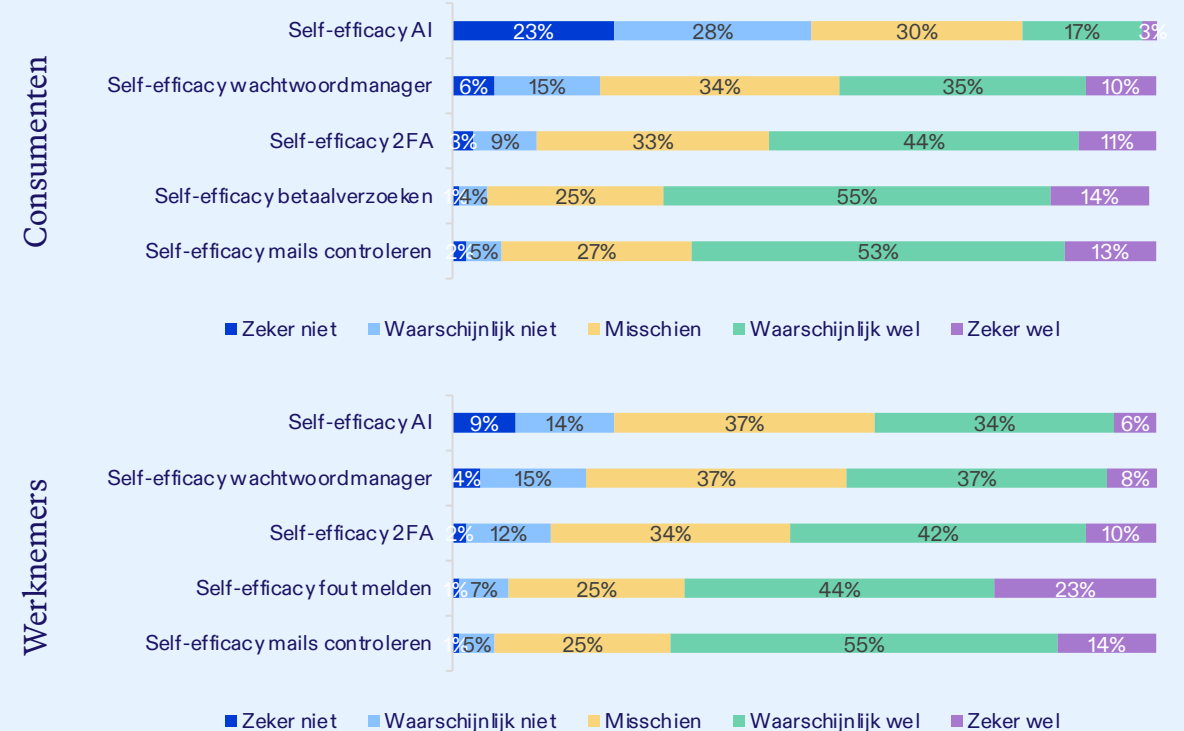
Kennis

- De meesten weten hoe ze mails (67% consumenten, 72% werknemers) en betaalverzoeken (72%) moeten controleren. Ongeveer de helft van de consumenten en werknemers weet hoe ze 2FA of een wachtwoordmanager moeten gebruiken (45-59%). Maar weinig mensen weten echter wat de richtlijnen en het beleid is rondom AI. Bij consumenten weet 14% wat het AI-privacybeleid is. Bij werknemers weet 39% welke AI mogen en weet 35% welke richtlijnen hun organisatie hanteert.



Self-efficacy

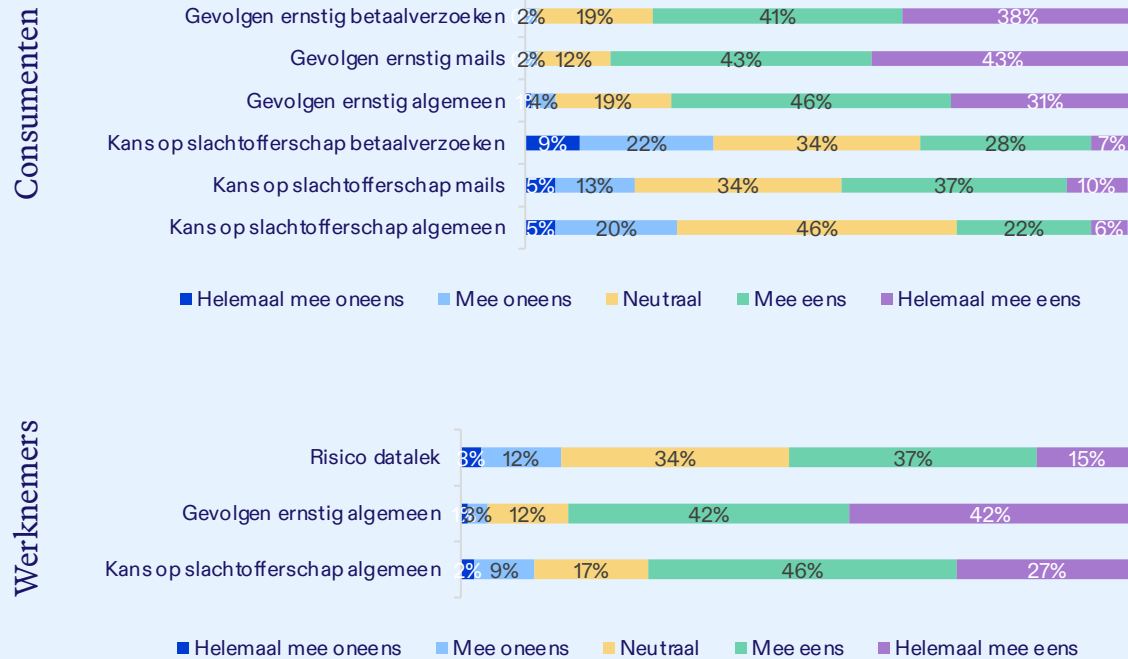
- De meeste mensen hebben er vertrouwen in dat ze malafide mails (66-69%) en betaalverzoeken kunnen herkennen (59%). Vertrouwen hebben in het kunnen gebruiken van 2FA en een wachtwoordmanager ligt iets lager (45-55%). Werknemers hebben er meer vertrouwen in om AI-tools veilig te kunnen gebruiken zonder hun privacy te schenden (40% v s. 20% bij consumenten). Mogelijk komt dit, omdat er op werk vaker wordt gewerkt met AI-tools, waar organisatie brede richtlijnen voor zijn, dan thuis.



Risicoperceptie, inertia en reactance

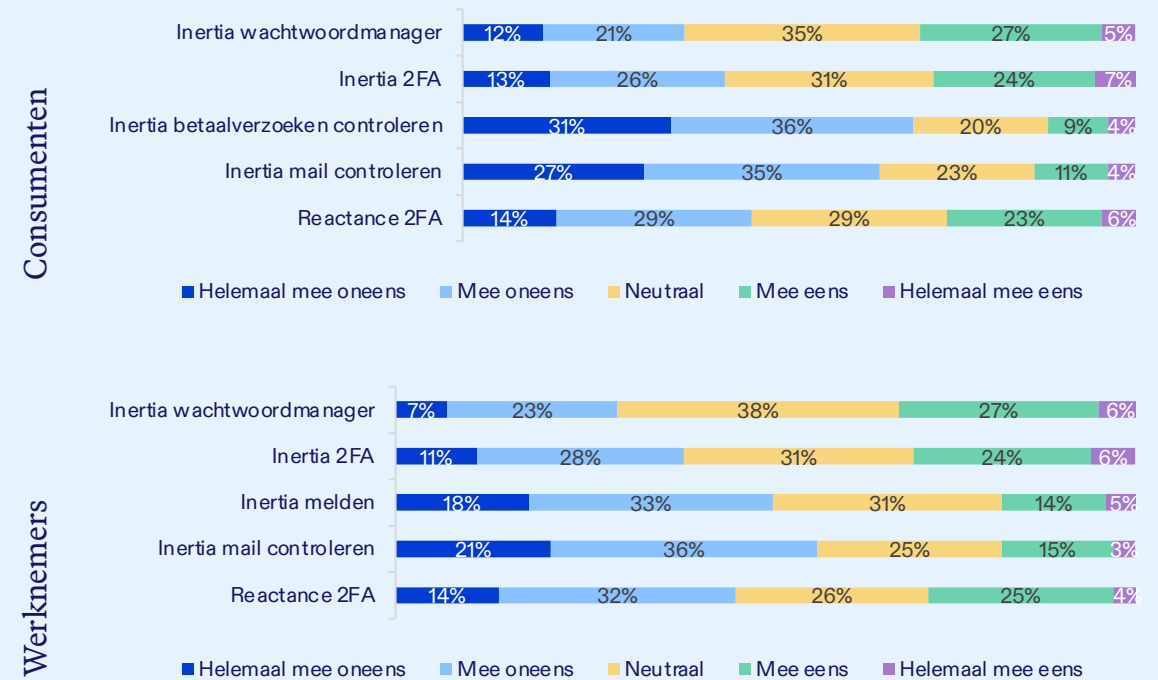
Ervaren risico

- 77-84% van de consumenten denkt dat de gevolgen van online criminaliteit ernstig zullen zijn. Bij werknemers is dit percentage ongeveer gelijk. De kans om zelf slachtoffer te worden van online criminaliteit ligt bij werknemers een stuk hoger dan bij consumenten: 73% vs. 28-47% bij consumenten.



Inertia en reactance

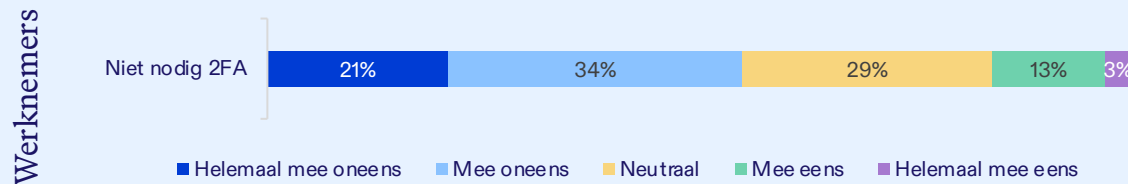
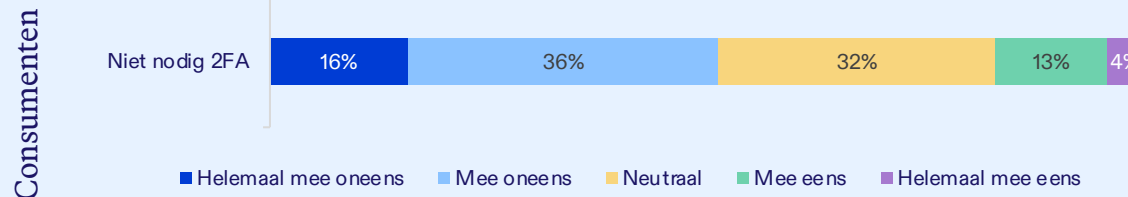
- Of mensen de veilige gedragingen veel moeite en tijd vinden kosten is verdeeld. Sommige mensen vinden het erg veel tijd en moeite kosten en anderen helemaal niet. Wachtwoordmanagers (32-33%) en 2FA (30-31%) gebruiken worden het vaakst als tijdrovend gezien.



Ervaren *nut*

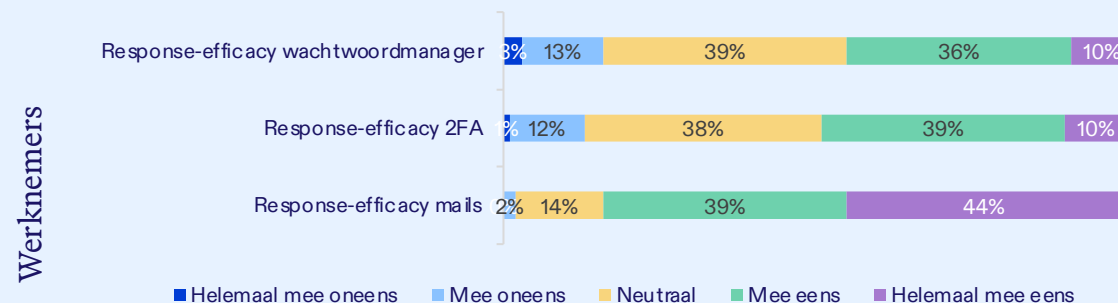
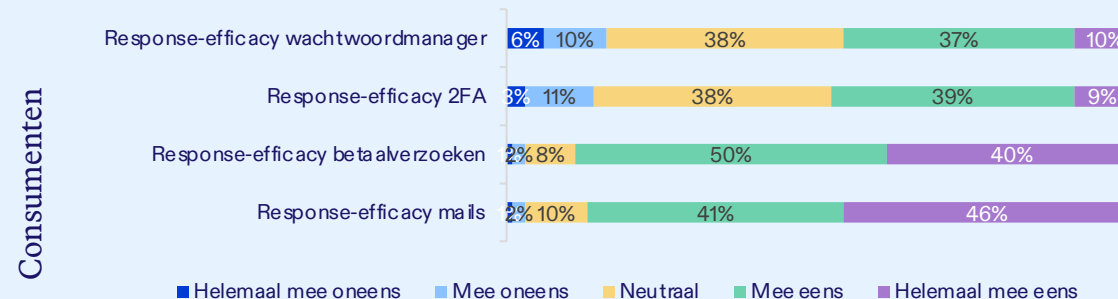
Niet nodig

- Een aantal consumenten (17%) en werknemers (16%) vindt dat ze al voorzichtig genoeg zijn online, en daarmee geen 2FA nodig hebben.



Response-efficacy

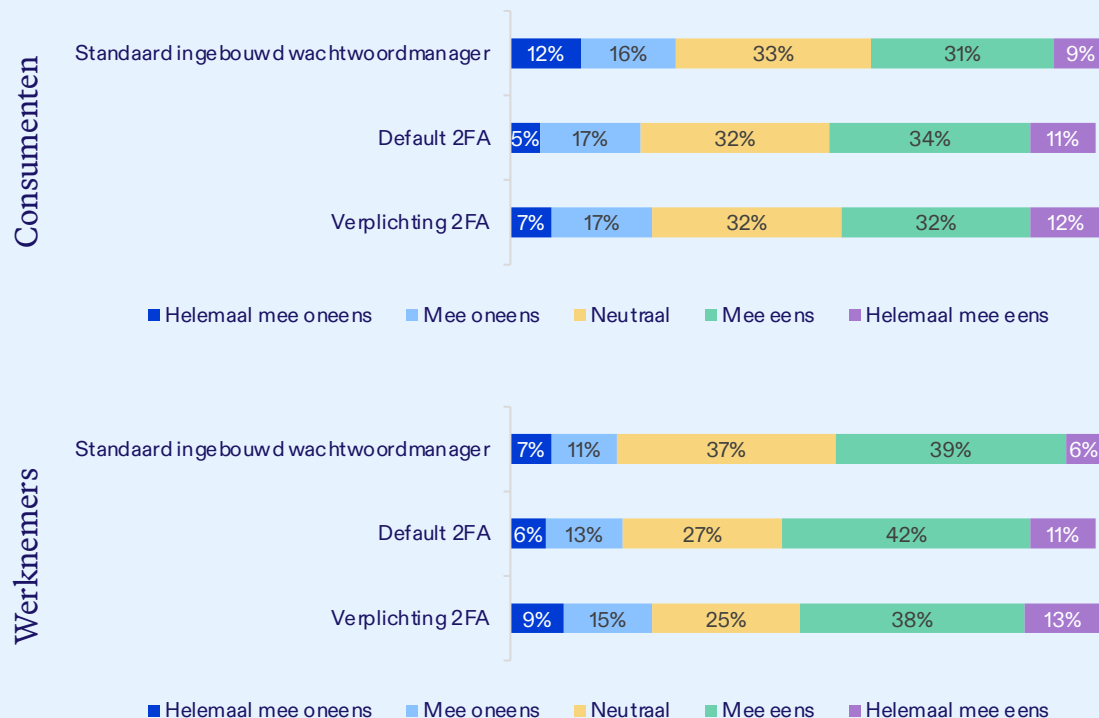
- Mails en betaalverzoeken controleren wordt gezien als een zeer effectieve methode om de kans op phishing en oplichting te verkleinen (83-90%). Een veel kleiner deel vindt echter dat 2FA en wachtwoordmanagers gebruiken helpt om hacks te voorkomen (46-49%). Deze cijfers zijn nagenoeg hetzelfde voor consumenten en werknemers.



Inrichting omgeving

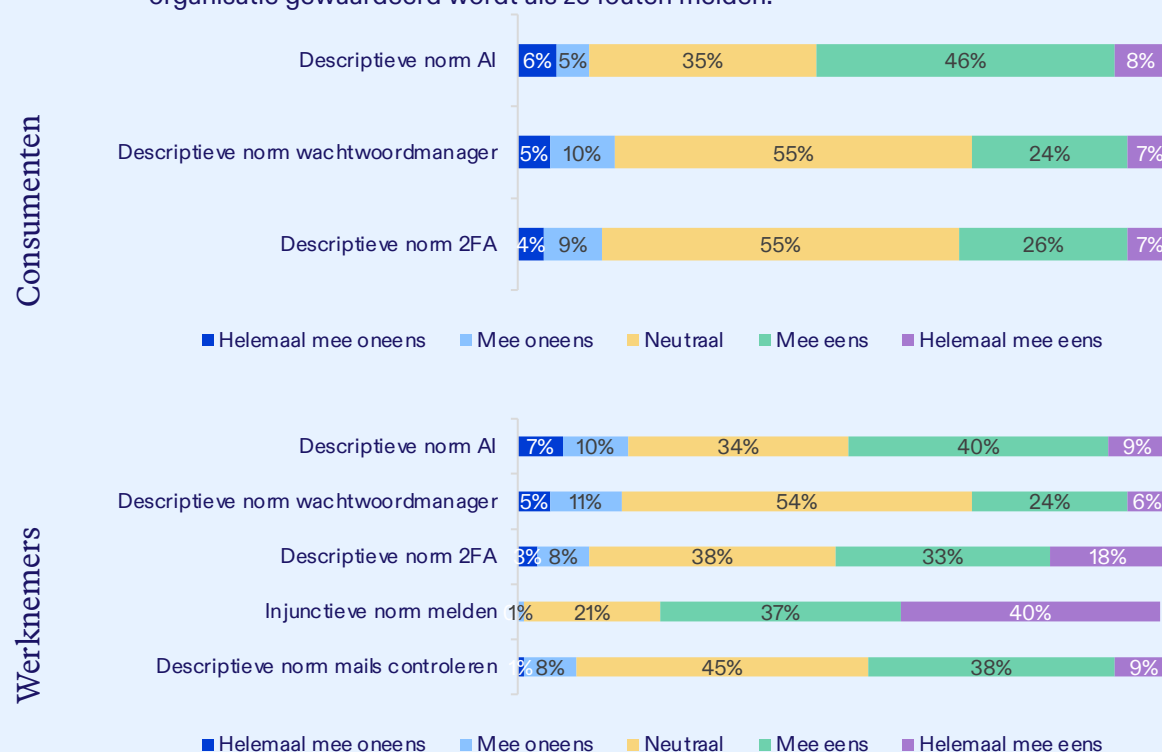
Architectuur

- Mensen zijn heel erg verdeeld over of ze 2FA alleen zouden gebruiken wanneer dit verplicht is of wanneer dit standaard aanstaat. Hetzelfde geldt voor wachtwoordmanagers.



Sociale normen

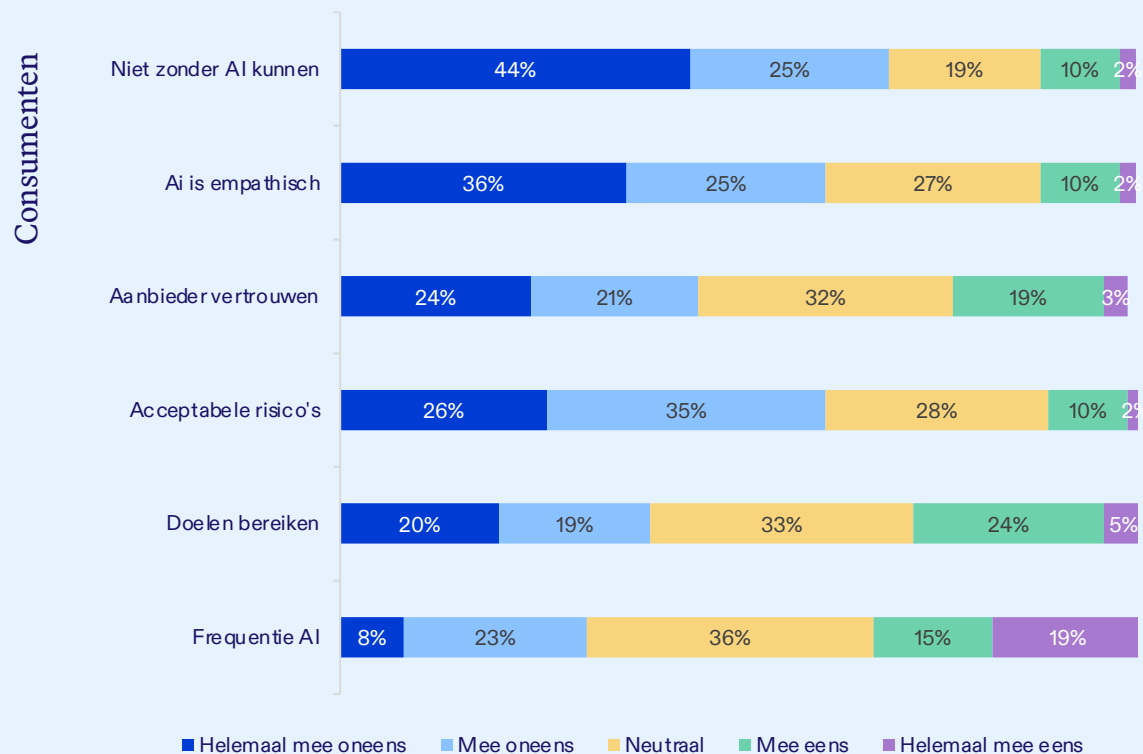
- Consumenten en werknemers zien niet heel veel en ook niet heel weinig vrienden, familie of collega's cyberveilig gedrag vertonen. Alleen bij AI zien ze dat meer mensen het gebruiken (54% voor consumenten, 49% voor werknemers). Bij werknemers is wel een sterke injunctieve norm om fouten te melden: 77% geeft aan dat het binnen hun organisatie gewaardeerd wordt als ze fouten melden.



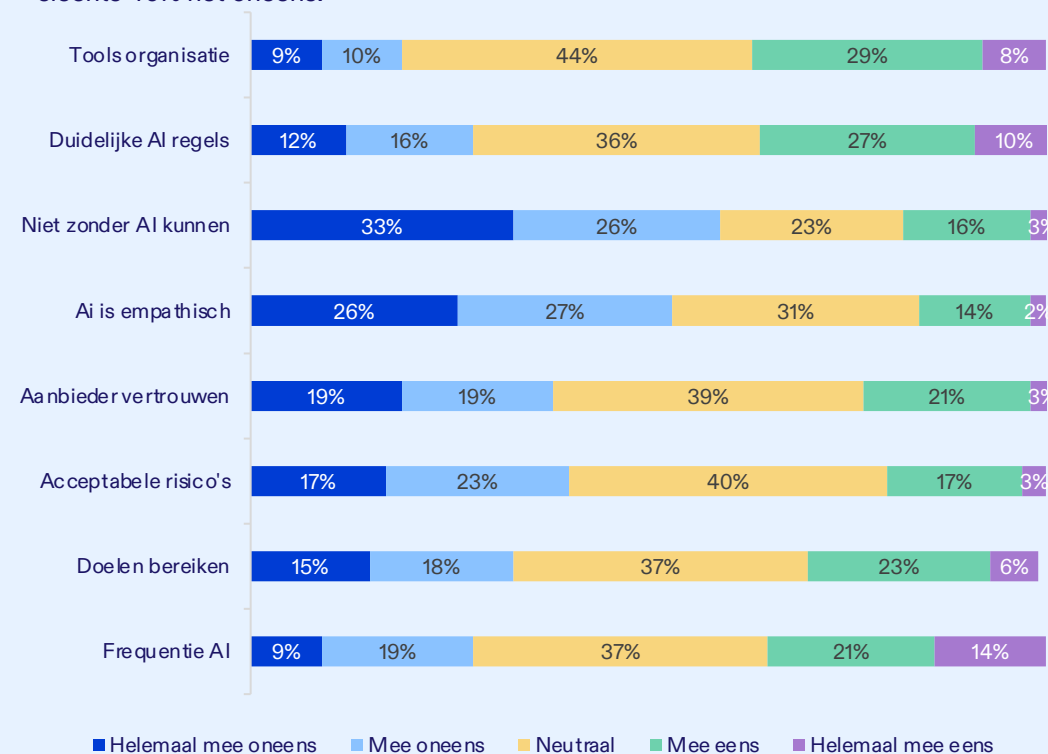
AI specifiek

AI specifiek

- Mensen gebruiken thuis ongeveer even vaak AI-tools als op het werk. De meeste mensen gebruiken AI wekelijks of dagelijks.
- De meeste mensen geven aan prima zonder AI te kunnen: 69% consumenten en 59% werknemers. Een deel vindt AI empathisch: 12% consumenten en 16% werknemers.



- Mensen vinden dat er wel wat risico's verbonden zijn aan AI-gebruik. Zo vertrouwt 45% van de consumenten de aanbieder niet en 38% van de werknemers. Ook zijn ze het er meestal niet mee eens om veiligheid in te leveren voor meer efficiëntie. 61% van consumenten is het hier niet mee eens. Werknemers zijn het er vaker mee eens, daar is slechts 40% het oneens.

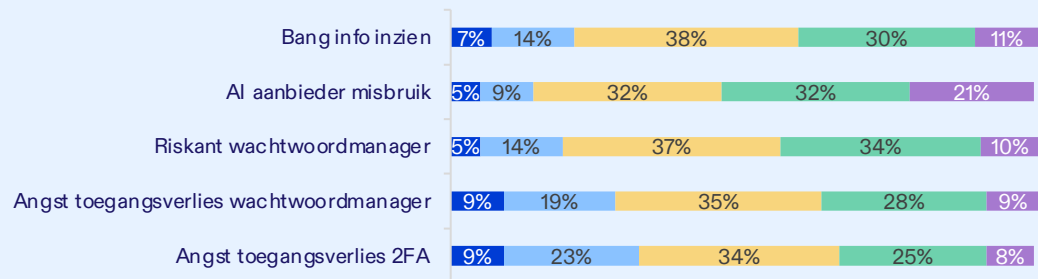


Angsten en overig

Angsten

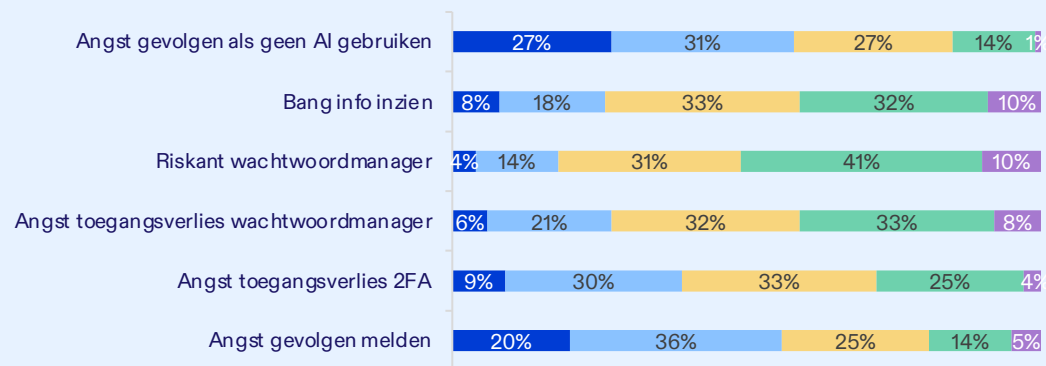
- Voor alle gedragingen is er een deel dat bang is dat er iets fout gaat met hun gegevens of het inloggen. Deze angst is bij consumenten het grootste voor AI gebruik. 53% is bang dat de AI-aanbieder misbruik maakt van hun data. Bij werknemers vinden ze het vooral riskant om alle wachtwoorden op één centrale plek op te slaan (51%). Een redelijk deel van beide groepen is bang dat anderen hun gegevens kunnen inzien (41% consumenten, 42% werknemers).

Consumenten



■ Helemaal mee oneens ■ Mee oneens ■ Neutraal ■ Mee eens ■ Helemaal mee eens

Werknemers

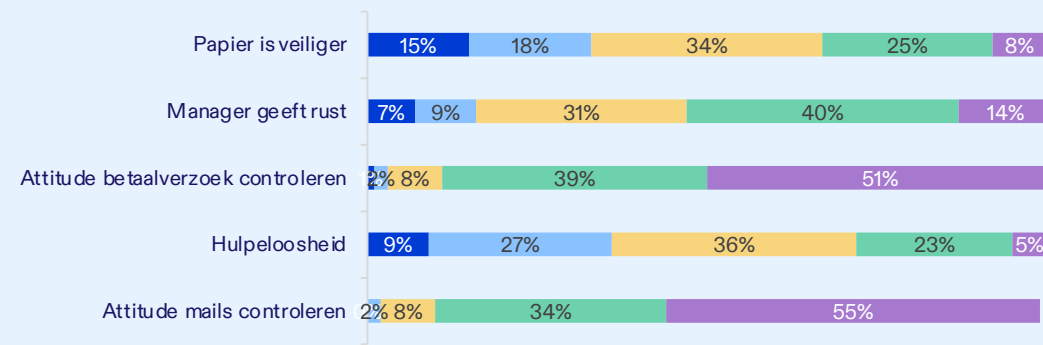


■ Helemaal mee oneens ■ Mee oneens ■ Neutraal ■ Mee eens ■ Helemaal mee eens

Overig

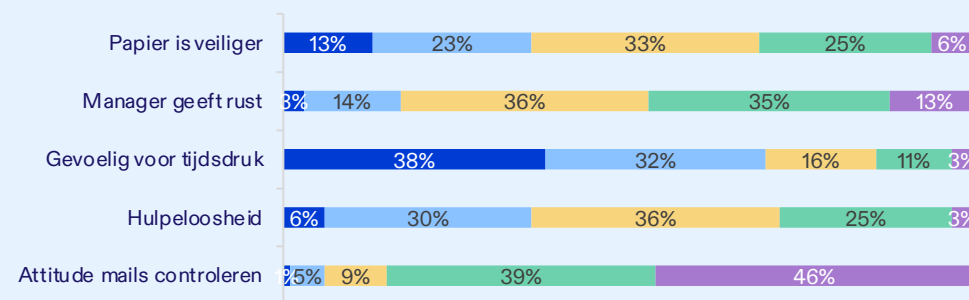
- Veruit de meeste mensen vinden het belangrijk om mails en betaalverzoeken te controleren (85-91%). Ook vindt de helft dat een wachtwoordmanager rust in het hoofd zou geven (54% en 48%).

Consumenten



■ Helemaal mee oneens ■ Mee oneens ■ Neutraal ■ Mee eens ■ Helemaal mee eens

Werknemers



■ Helemaal mee oneens ■ Mee oneens ■ Neutraal ■ Mee eens ■ Helemaal mee eens

Descriptives van *de scenario's*

We legden de deelnemers van de vragenlijst ook een scenario in een digitale omgeving voor. We vroegen de deelnemers zich in te leven in de situatie. Hiermee toetsen we of het gerapporteerde gedrag zou overeenkomen met een realistische weergave van de werkelijkheid en niet enkel sociaal wenselijke antwoorden zou opleveren. We komen zo dichterbij daadwerkelijke situaties en gedrag dan alleen zelfrapportage. Op de volgende pagina staat een overzicht van de scenario's en de resultaten.

De belangrijkste inzichten

Zowel consumenten als werknemers tonen in de scenario's alertheid: bij verdachte elementen (zoals een spoed-betalverzoek of QR-code) herkent de meerderheid een e-mail als phishing. Waar een neutrale statusupdate voornamelijk twijfel oproept, zorgen gevraagde acties of betaalverzoeken direct voor emoties zoals irritatie, verwarring en onrust. Beide groepen beoordelen e-mails op vergelijkbare punten: de inhoud van de tekst, het exacte mailadres van de afzender en de herkenbaarheid van de leveranciers.

Bij de verdachte betaalmail kiest het merendeel van de consumenten voor direct verwijderen, terwijl werknemers het bericht vooral zouden rapporteren of melden bij de IT-afdeling. Risicovol handelen (zoals daadwerkelijk op knoppen klikken of QR-codes scannen) blijft in de scenario's minimaal.

Deze resultaten weerspiegelen wat er verder in de vragenlijst terugkwam: mensen weten vaak wel waar ze op moeten letten en passieve controles vinden regelmatig plaats. Toch blijft actief gedrag, zoals het melden van een fout, achter. Slechts 41% van de werknemers zou een fout melden binnen de organisatie.



De scenario's

De twee linker afbeeldingen tonen het scenario van de consumenten, de rechter afbeelding en tekst het scenario van de werknemers.

We beginnen met een fictief scenario. Dit scenario lijkt op een situatie die je in het dagelijks leven kunt tegenkomen.

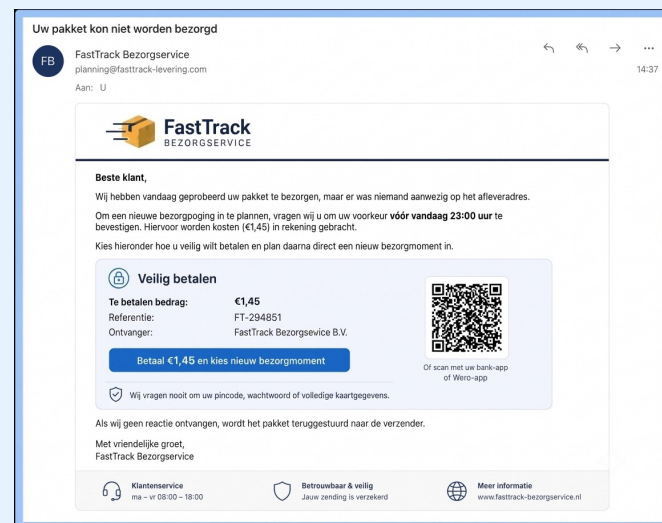
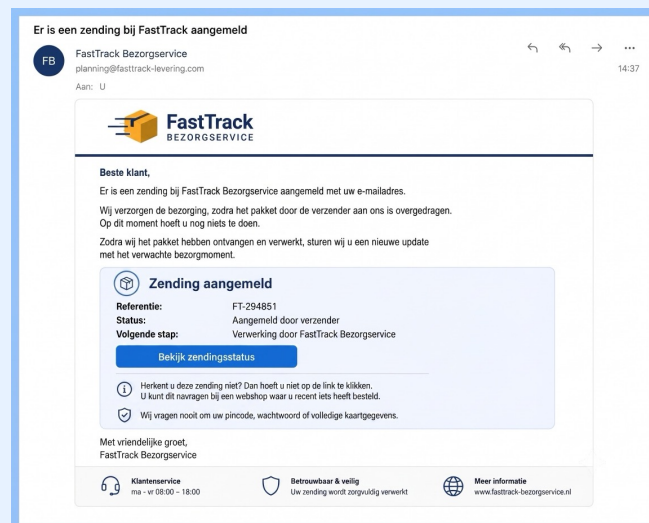
Stel je voor: het is een gewone weekdag en je bent thuis. Je kijkt op je mobiel en ziet dat je een e-mail hebt ontvangen van bezorgservice FastTrack.

Lees de e-mail rustig en aandachtig door. Daarna stellen we je een paar vragen.

Na een paar dagen zie je dat je een tweede e-mail hebt ontvangen van FastTrack.

Eerder kreeg je van FastTrack het bericht dat er een zending was aangemeld met jouw e-mailadres. Nu ontvang je een update over deze zending.

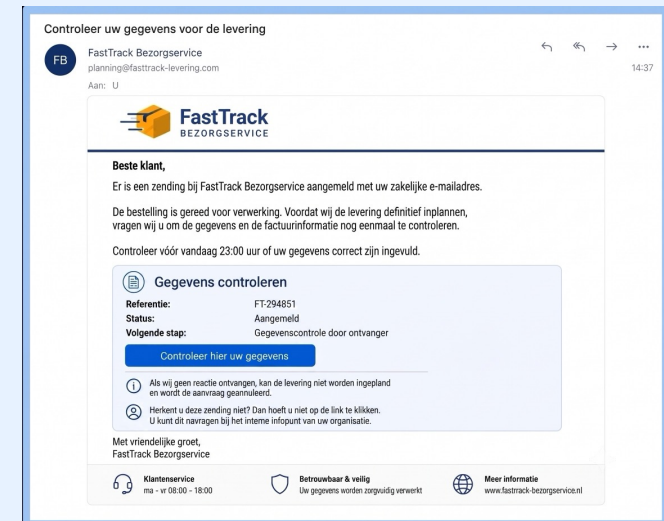
Lees de e-mail rustig door. Daarna stellen we je een paar vragen over deze tweede situatie.



We beginnen met een fictief scenario. Dit scenario lijkt op een situatie die je op je werk kunt tegenkomen.

Stel je voor: het is een gewone werkdag en je bent op kantoor. Je kijkt op je werklaptop en ziet dat je een e-mail hebt ontvangen van leverancier FastTrack.

Lees de e-mail rustig en aandachtig door. Daarna stellen we je een paar vragen.

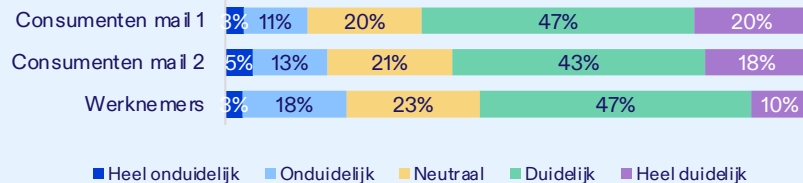


Je hebt op de knop geklikt om jouw gegevens te controleren. De gegevens waren onvolledig en je hebt enkele open velden aangevuld.

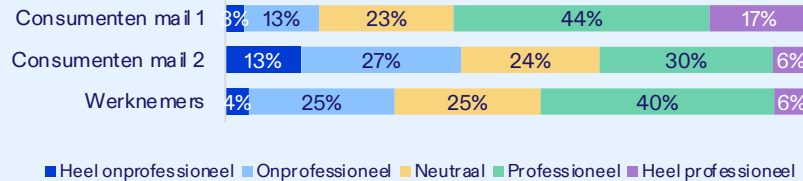
Na een week is er geen bericht meer gekomen over de levering. Je bent aan het twijfelen of de mail wel klopte.

Manipulatiecheck

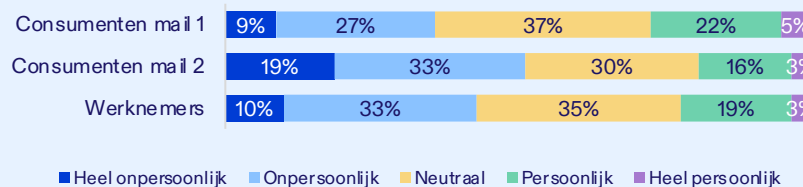
Hoe duidelijk vond je de mail?



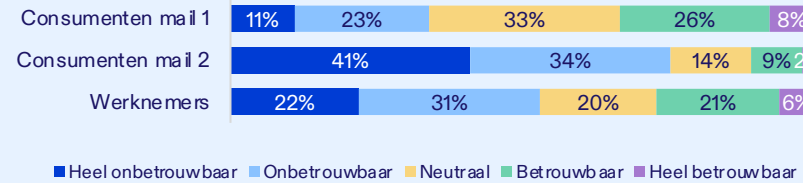
Hoe professioneel vond je de mail?



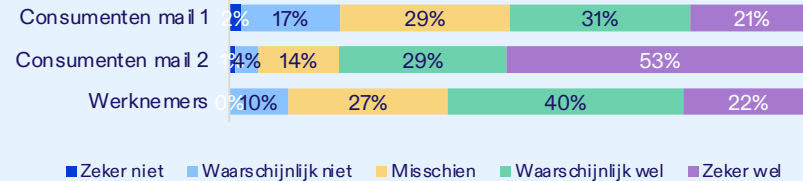
Hoe persoonlijk vond je de mail?



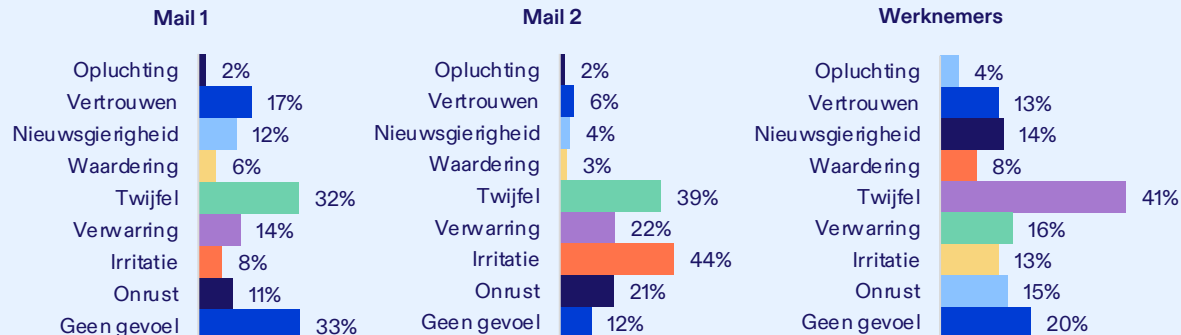
Hoe betrouwbaar vond je de mail?



In hoeverre heb je het idee dat de mail phishing of oplichting was?



Welk gevoel roept de mail vooral bij je op?



Wat valt op?

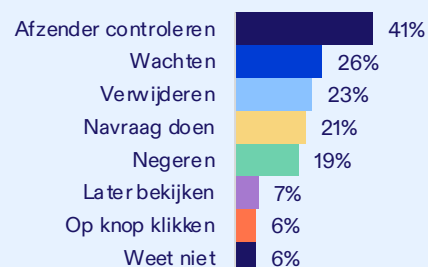
De eerste e-mail in het scenario werd door consumenten voornamelijk beoordeeld als duidelijk (67%) en professioneel (61%). Deze e-mail werd door de doelgroep niet meteen als onbetrouwbaar of als phishing bestempeld (52%). Bij de tweede e-mail was dit beeld anders: deze werd door een ruime meerderheid (75%) als (zeer) onbetrouwbaar ervaren. Ook werd dit vaker als phishing herkend (81%).

De e-mail uit het scenario voor werknemers werd door ongeveer de helft gezien als duidelijk (57%) en professioneel (46%). Toch werd het bericht door een aanzienlijk deel als onbetrouwbaar ervaren (53%), waarbij maar liefst 62% van de werknemers inschat dat het (waarschijnlijk) om een phishingbericht gaat.

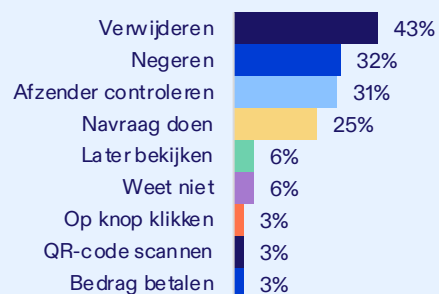
Waar de eerste mail voor consumenten voornamelijk twijfel of geen gevoel opwerkte, kwam bij de tweede mail een gevoel van twijfel, irritatie, onrust en verwarring naar boven. Het bericht roept bij werknemers voornamelijk een gevoel van twijfel (41%) op, gevolgd door geen gevoel (20%), verwarring (16%), onrust (15%) en nieuwsgierigheid (14%).

Resultaten

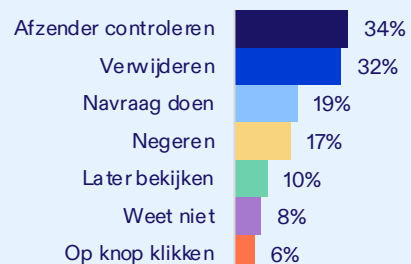
Wat zou je waarschijnlijk doen als je deze mail ontvangt (mail 1)?



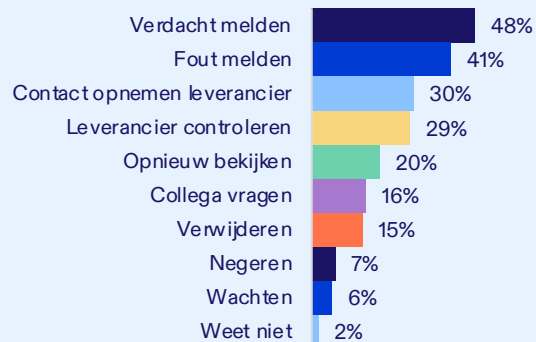
Wat zou je waarschijnlijk doen als je deze mail ontvangt (mail 2)?



Wat zou je waarschijnlijk doen als je deze mail ontvangt? (werknemers)

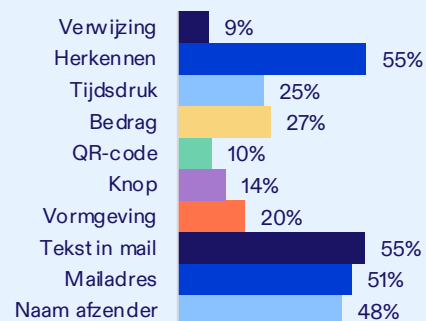


Wat zou je waarschijnlijk doen in deze situatie (na geen reactie)? (werknemers)

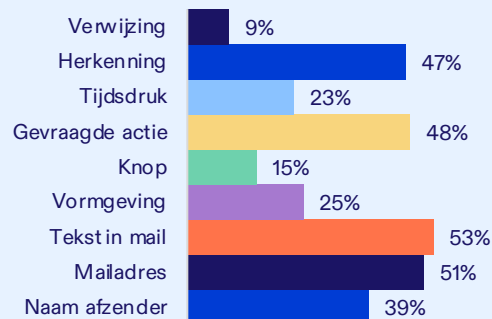


Waar vooral op gelet bij het beoordelen?

Consumenten



Werknemers



Het gedrag van consumenten laat een duidelijke verandering zien bij de tweede mail ten opzichte van de eerste. Bij mail 1 controleert het merendeel de afzender (41%), kiest voor afwachten (26%) of het verwijderen van de mail (23%), of doet actief navraag (21%). Bij mail 2 kiest het merendeel ervoor om de mail direct te verwijderen (43%). *"Ik heb er niets besteld!!!!!!!!!! Dus blokkeren en negeren."*

Andere gekozen acties zijn het controleren van de afzender (31%) of het doen van navraag over de zending (25%). Het risicovolle gedrag blijft hierbij minimaal: slechts 3% zou klikken op de knop en 3% zou de QR-code scannen.

Bij werknemers kiest het merendeel voor verifiëren of verwijderen: 34% controleert eerst de afzender en 32% kiest ervoor de mail direct te verwijderen. Andere frequente vervolgstappen zijn het doen van navraag (19%) of het negeren van de e-mail (17%). Slechts 6% geeft aan direct op de knop te klikken.

Wanneer er na verloop van tijd geen reactie of levering volgt, ondernemen werknemers actieve vervolgstappen binnen hun organisatie. De grootste groep kiest voor melden: 48% meldt het bericht als verdacht en 41% meldt het specifiek als een fout. *"Op de knop check phishing klikken die in mijn e-mail programma zit, waarna de de e-mail door de IT afdeling wordt beoordeeld op echtheid."*

Daarnaast verifieert een groot deel het bericht extern: 30% neemt contact op met de leverancier en 29% controleert de leverancier zelf. 16% vraagt een collega om advies. *"Controleren of dit een leverancier is van ons, welke bestellingen er eventueel uitstaan, welke case correspondeert met deze zending."*

Bij het beoordelen van een e-mail vertrouwen consumenten en werknemers voornamelijk op de volgende punten:

- het herkennen van de leverancier;
- de inhoud en logica van de tekst;
- het exacte mailadres van de afzender;
- de naam van de afzender.

Sommige consumenten letten ook op andere dingen: *"Of mijn naam persoonlijk genoemd word ipv klant."* *"Het feit dat er spontaan om geld gevraagd wordt, zelfs een klein bedrag."*

Always *one move* ahead

Behavior
Change
Group

Dominik Simler: dominik@behaviorchange.group

Lobke de Bruin: lobke@behaviorchange.group

Leonie Venhoeven: leonie@behaviorchange.group

Gea Schonewille: gea@behaviorchange.group