



Het probleem:

Veel Nederlanders kennen de risico's en willen veilig handelen, maar kennis (weten) is niet voldoende om veilig online te handelen (doen). Dit maakt ze kwetsbaar voor onder andere oplichting en datalekken.



Belangrijkste gedragsinzichten

Ondanks dat consumenten en werknemers wél weten wat veilig online gedrag is, passen ze slechts een derde van alle **veilige handelingen** toe.



20%

consumenten

Gebruikt altijd wachtwoordmanagers.

13%

werknemers

33%

werknemers

Meldt altijd een gemaakt fout direct bij IT.

31%

consumenten

Navigeert altijd handmatig naar de website of app.

21%

werknemers

49%

werknemers

Gebruikt weleens privé AI-accounts voor werk.

Onveilig AI-gebruik

Onveilig AI-gebruik heeft grote gevolgen voor cyberveiligheid. Dit zijn belangrijke inzichten om rekening mee te houden:

→ **35%** van de werknemers en **46%** van de consumenten deelt inhoudelijke problemen met AI-tools voor advies.

→ Mensen die AI empathisch of kwalitatief goed vinden, zijn bereid meer privacy in te leveren.

→ Werknemers die bang zijn dat ze hun baan of reputatie schaden als ze géén AI gebruiken, delen vaker persoonlijke informatie met AI.

Hoe lossen we het op?

Pas deze vier gedragstechnieken toe om het cyberveilig gedrag te stimuleren.

1. Maak het makkelijk

Neem de moeite weg en leer hoe het moet: automatische 2FA, wachtwoordmanagers en opvallende meldknoppen.

2. Maak het aantrekkelijk

Laat zien wat veilig gedrag oplevert, zoals het gemak van een wachtwoordmanager: nooit meer wachtwoorden onthouden.

3. Maak het sociaal

Laat zien dat steeds meer mensen en rolmodellen het al doen, geef complimenten en laat gebruikers anderen op weg helpen.

4. Kies het juiste moment

Stuur herinneringen, haak aan bij nieuws zoals een datalek en spreek vaste als-dan-regels af, zoals: "Als ik een inloglink krijg, open ik zelf de app."

Vier belemmeringen voor gedragsverandering



Inertia: Gedrag wordt uitgesteld of vermeden als het als veel moeite of gedoe voelt, zoals bij 2FA.



Gebrek aan procedurele kennis: Mensen weten vaak wel wat ze moeten doen, maar niet hoe ze dit moeten doen.



Overmoed: Mensen overschatten hun eigen kennis, waardoor extra maatregelen overbodig voelen, zoals bij phishing.



Andermans gedrag is onzichtbaar: Online gedrag is onzichtbaar waardoor we minder snel veilig gedrag van anderen nadoen.

Vier kansrijke cybergedragingen

Op de achterzijde vind je vier kansrijke cybergedragingen om op in te zetten.



Toepassing op vier kansrijke cybergedragingen

Bekijk hier de volledige rapportage:



Een aantal cybergedragingen is kansrijker om op in te zetten. Hieronder lees je hoe je vier kansrijke gedragingen kunt stimuleren.



Twefactorauthenticatie instellen en gebruiken

- Laat stap voor stap zien hoe je 2FA aanzet, en wat je doet als je je telefoon kwijt bent. Dat kan met korte uitleg of een oefenomgeving.
- Laat zien dat steeds meer mensen 2FA gebruiken. Laat collega's, leidinggevenden en bekenden het goede voorbeeld geven.
- Zet 2FA waar het kan standaard aan. Help mensen klein te beginnen, bijvoorbeeld eerst alleen met hun e-mail.
- Kies slimme momenten, zoals na een datalek. Geef werknemers tijd op het werk om 2FA in te stellen.
- Maak duidelijk dat voorzichtig zijn niet genoeg is. Als een webshop je wachtwoord lekt, houdt alleen 2FA criminelen nog tegen.



Wachtwoordmanager instellen en gebruiken

- Maak gebruik zichtbaar: laat collega's het voordoen en nodig gebruikers uit om hun gezin mee te laten doen.
- Laat zien dat een wachtwoordmanager veiliger is dan overal hetzelfde wachtwoord gebruiken. Laat betrouwbare partijen dat bevestigen.
- Breng de wachtwoordmanager als iets wat rust geeft: nooit meer wachtwoorden onthouden en inloggen met je vingerafdruk.
- Maak beginnen makkelijk. Wijs op de wachtwoordmanager die al op je telefoon of in je browser zit, en laat de ICT-afdeling dit op werkapparaten klaarzetten.
- Laat collega's elkaar helpen door de wachtwoordmanager samen in te stellen.



Zelf naar officiële website/app gaan

- Laat organisaties zoals banken en de overheid geen inloglinks meer in e-mails sturen, en communiceer dat ook duidelijk.
- Maak zelf naar de website gaan net zo makkelijk als op een link klikken, met een bladwijzer voor bijvoorbeeld de bank, PostNL of MijnOverheid.
- Leer mensen een vaste regel: "Als een mail vraagt om in te loggen, sluit ik de mail en open ik zelf de website of app."
- Laat mensen zelf ervaren dat ze nepmails niet altijd herkennen, bijvoorbeeld met een quiz met echte mails en nepmails die met AI zijn gemaakt.
- Maak voor consumenten duidelijk wat er op het spel staat: één haastige klik kan je bankrekening leeghalen.



Fout melden binnen de organisatie

- Maak duidelijk dat fouten maken menselijk is en dat melden altijd wordt gewaardeerd, ook als er al schade is.
- Bedank mensen direct na een melding, bijvoorbeeld met: "Scherp opgemerkt, dankzij jou konden we snel ingrijpen."
- Laat leidinggevenden en collega's openlijk vertellen over hun eigen fouten, en zeg hardop dat melden spannend kan voelen.
- Maak melden zo makkelijk mogelijk, met één meldknop in het mailprogramma en eenvoudige stappen zonder jargon.
- Spreek vooraf een vaste regel af: "Als ik op een verdachte link heb geklikt, meld ik dat meteen bij ICT."