

Wave voor de zorg

AWAREWAYS

Je zorginstelling digitaal veilig houden. **Hoe pak jij dat aan?**

Cyberaanvallen en datalekken kunnen ernstige gevolgen hebben voor jouw organisatie en de privacy van je cliënten. Een effectief security awareness programma is essentieel om deze risico's te minimaliseren. Zorginstellingen moeten voldoen aan strikte regelgeving zoals de NEN7510. Training zorgt ervoor dat medewerkers op de hoogte zijn van deze verplichtingen en compliant blijven. Dit helpt bij de bescherming van grote hoeveelheden medische dossiers en persoonlijke informatie, aangezien onbewuste medewerkers per ongeluk deze gegevens kunnen blootstellen of verliezen.

Investeer in een op maat gemaakt trainingsprogramma dat voldoet aan de hoogste normen en zorg voor een proactieve aanpak in risicobeheer en aansprakelijkheid.

Awareways
ontzorgt CISO's
in de zorg!



Micro-leren voor maximale efficiëntie

Versterk je security awareness programma met Wave

Awareways biedt een op maat gemaakte benadering speciaal ontwikkeld voor de zorgsector, van zorgmedewerkers, ondersteunende medewerkers tot management. Onze methode richt zich zowel op basisvaardigheden als diepgaande kennis, afgestemd op de volwassenheid van jouw organisatie. In plaats van lange, traditionele e-learning modules, biedt onze training een interactieve en effectieve kennismaking met informatieveiligheid.

Micro-leren voor maximale efficiëntie

Wave volgt het principe van micro-leren, waarbij je in overzichtelijke en behapbare hoeveelheden leert. Geen onnodige tijdverspilling, maar een efficiënte en prettige leerervaring. Onze training is aanpasbaar aan verschillende leerniveaus en -behoeften, ideaal voor zowel onboarding als doorlopende training.



Onze vier-fasen aanpak voor de zorgsector



Fase 1 – de basis

Leer de essentiële omgangsregels met informatie, de AVG en het elektronisch patiëntendossier. Fase 1 is relevant voor alle medewerkers en is daarnaast een effectieve onboarding voor nieuwe collega's.



Fase 2 – de waarde

In fase 2 ligt de focus op de waarde van informatie, classificeren van informatie en het vaststellen van veilig gedrag via quizzes, video's en vaardigheidsspellen.



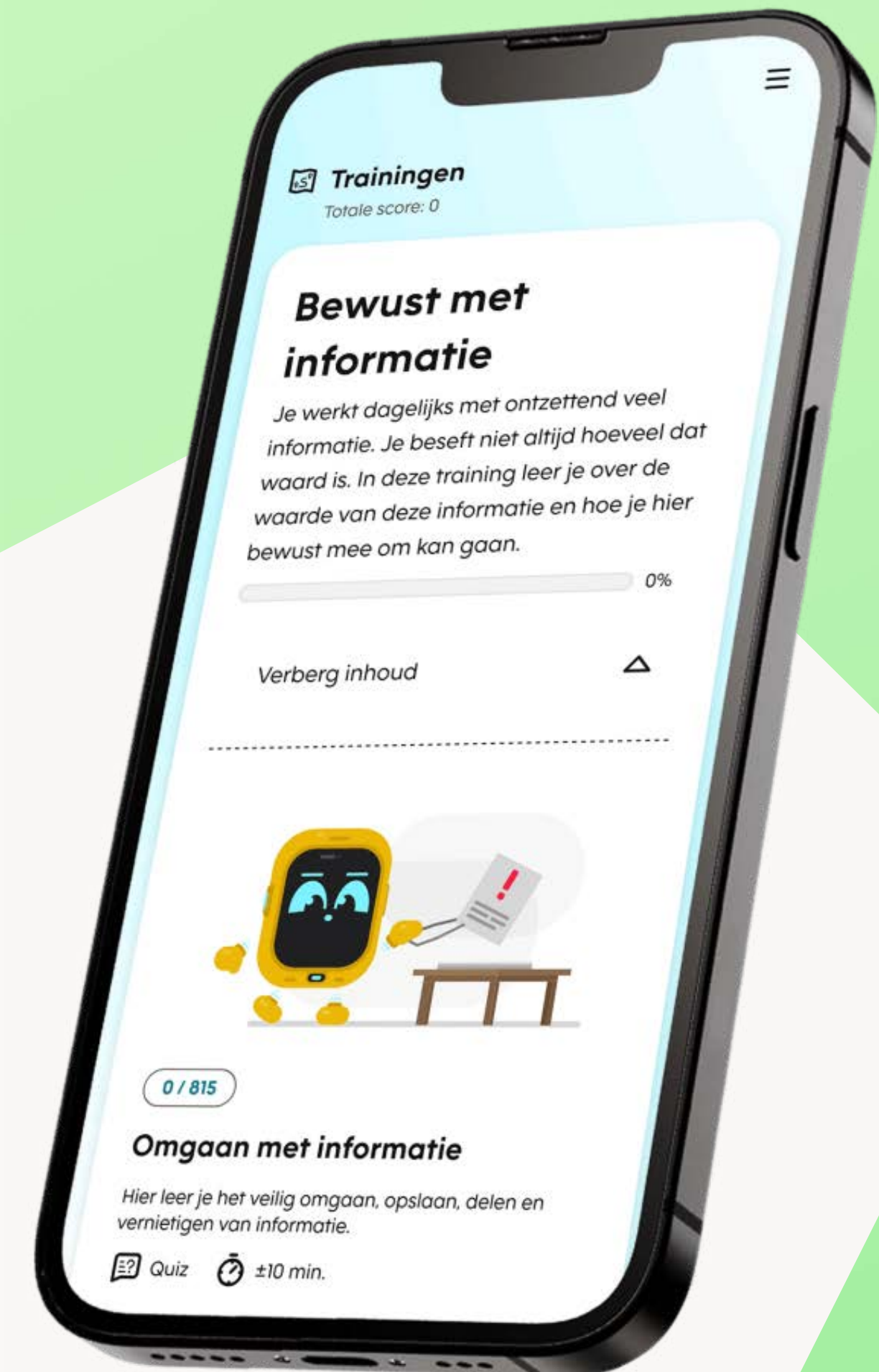
Fase 3 – de risico's

Vergroot de weerbaarheid van je medewerkers tegen social engineering met micro-leermodules over phishing, smishing en vishing. Verhoog de weerbaarheid van medewerkers tegen gerichte aanvallen.



Fase 4 – het gedrag

In fase 4 is alles gericht op actie, oftewel hoe moet je reageren. Je wordt geactiveerd om proactief te handelen en te vertrouwen op het niet-pluis gevoel om potentieel gevaar te herkennen.

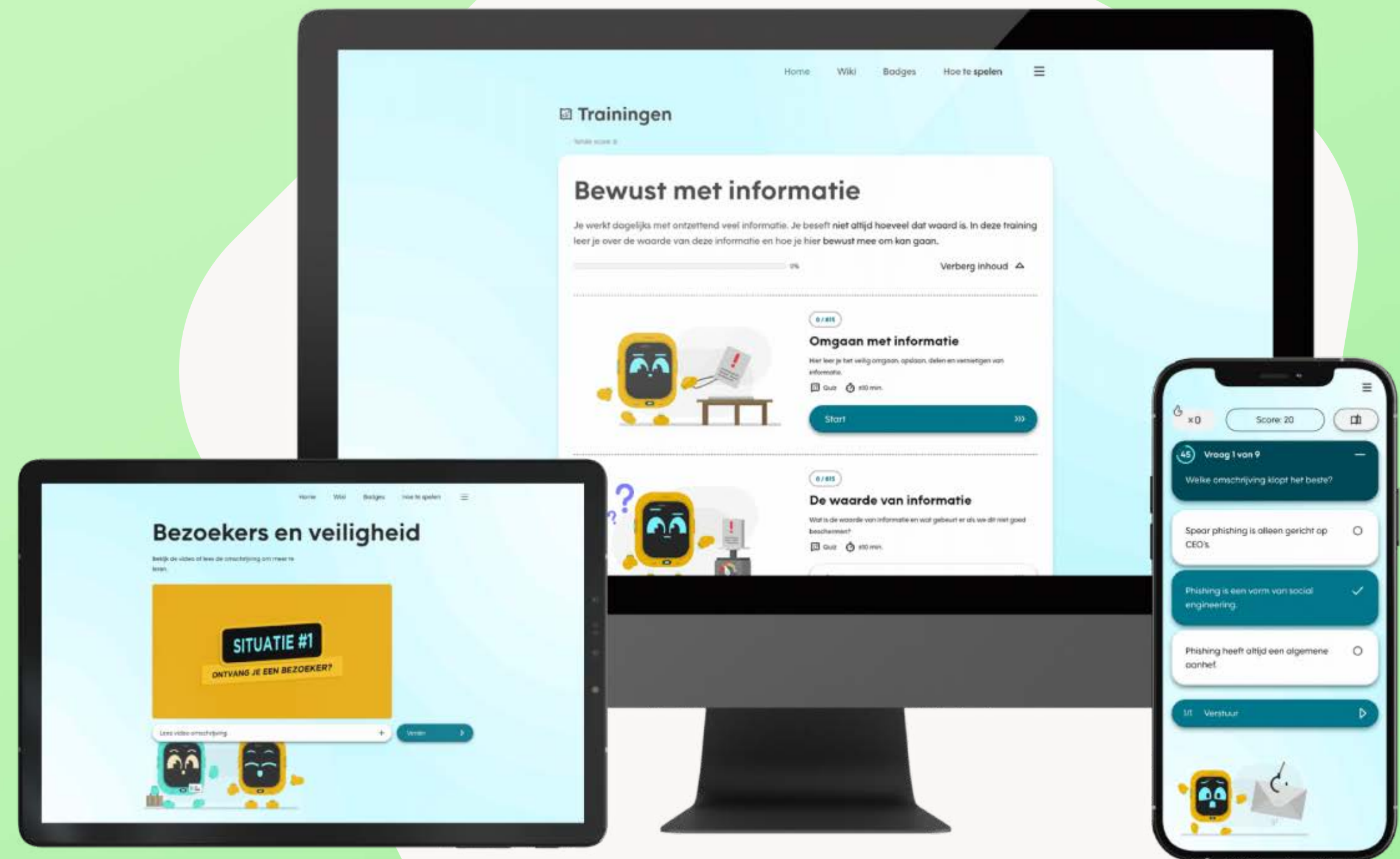


Over Wave

Wave combineert quizzen, video's en skillgames (serious gaming) om effectieve training en gedragsverandering te realiseren. Veilig gedrag begint met kennis, begrip van de toepassing en de vaardigheden om dit uit te voeren.

Wat Wave biedt

- **Herkenbare content:** Gebaseerd op het Cybersecurity Dreigingsbeeld Zorg 2022 van ZCERT en aanvullend onderzoek.
- **Conform NEN7510:** Voldoet aan alle relevante normen.
- **Naadloze integratie:** Te koppelen met jouw bestaande leermanagementoplossing, inclusief SAP.
- **Meertaligheid:** Beschikbaar in meerdere talen, standaard in Nederlands.
- **Inclusief en toegankelijk:** WCAG 2.2 goedgekeurd.



Wave voor de zorg

Waarom kiezen voor Awareways

- **Expertise en kennis:** Ons team van ervaren professionals is goed op de hoogte van de laatste trends en best practices.
- **Praktische aanpak:** We bieden praktische tools en strategieën die direct toepasbaar zijn.
- **Slim maatwerk:** Onze programma's worden aangepast aan de specifieke behoeften en cultuur van jouw organisatie.
- **Ondersteuning bij implementatie:** Onze programmamanagers begeleiden je organisatie van start tot resultaat om de beheerlast te beperken.

Op zoek naar andere interventies?

Zoek je metingen, communicatie, phishing simulaties of een volledig programma?

Neem contact op met één van onze accountmanagers.

✉ sales@awareways.com

☎ +31 (0)30 227 14 67

🌐 awareways.com/indezorg

