Phishwise

SECURITY AWARENESS DIE DOORLOOPT

Aandacht voor veilig digitaal gedrag

Phishwise laat medewerkers veilig oefenen met phishing, leert ze precies wat ze nodig hebben en laat aan bestuur en auditor zien wat er verandert. Nederlandse software voor gemeenten, zorg en onderwijs.

Aandacht | Respect | Samen leren | Meetbare voortgang

Eén phishingtest per jaar bewijst dat je hebt getest. Niet dat er iets veranderd is.

De meeste organisaties doen wat de norm vraagt: een jaarlijkse e-learning en een phishingtest. Het vinkje staat, de klikratio blijft hangen. Gedrag verandert pas als oefenen normaal wordt, feedback op het moment zelf komt, en melden iets oplevert.

91%

van de cyberaanvallen begint met een phishingmail. Firewalls en filters vangen veel, maar de mail die doorkomt belandt bij een mens. Die mens is geen zwakke schakel; het is de laatste die nog nee kan zeggen. Dat lukt alleen met oefening.

Phishwise brengt alles wat daarvoor nodig is in één omgeving: realistische simulaties, korte tips en challenges tussendoor, training die past bij wat iemand net deed, een meldknop in Outlook, en een rapport dat een bestuurder in vijf minuten leest.

Gebouwd en gehost in Nederland. Ingericht op BIO, NIS2, NEN 7510 en ISO 27001, zodat de rapportage direct bruikbaar is voor ENSIA en audits.

> “Binnen zes maanden daalde onze klikratio van 23% naar 4%.”
>
> IT-manager, Wind

Wat we anders doen

- **Aandacht in plaats van angst.** Wie klikt, krijgt uitleg en een korte training, geen mail naar de leidinggevende.
- **Melden telt mee.** We meten niet alleen wie klikt, maar vooral wie een verdachte mail op tijd meldt.
- **Om de week iets kleins.** Een tip of een vraag van één minuut werkt beter dan een uur e-learning per jaar.
- **Sturen per team of locatie.** Managers zien hun eigen team, het bestuur ziet het geheel.

WAT EEN MEDEWERKER ERVAN MERKT

MAANDAG, 09:00

Een tip van één minuut

“Zo zie je of een factuur echt van je leverancier komt.” Lezen, klaar. Geen inlog, geen cursus.

TWEE WEKEN LATER

Een vraag met een keuze

Een challenge over een agenda-uitnodiging. Verkeerd gekozen? Dan volgt de uitleg meteen, en een korte training als het nodig is.

ERGENS IN HET KWARTAAL

Een mail die echt lijkt

Wie klikt, ziet een lespagina in plaats van een standje. Wie hem meldt via de Outlook-knop, krijgt een bedankje.

ELKE DAG

Eigen portaal

Score, trainingen, geschiedenis en de meldroute op één plek. Managers zien alleen hun eigen team.

VOOR WIE

Gemeenten en andere overheden die ENSIA en de BIO moeten aantonen. Zorgorganisaties die NEN 7510 volgen. Onderwijsinstellingen met honderden accounts en weinig tijd. Overal waar één ingevuld wachtwoord echte schade doet.

Start binnen 24 uur: de verzending loopt via jullie eigen Microsoft 365, medewerkers komen binnen via SCIM of een import, en de eerste nulmeting kan dezelfde week nog.

Phishwise

Zo ziet een jaar met Phishwise eruit

Geen losse test, maar een ritme. Phishwise plant het voor je en houdt bij wat het oplevert.

01 · NULMETING

Weten waar je staat

Een eerste simulatie zonder aankondiging. De uitkomst is je nulmeting: klikratio, meldgedrag en de Human Firewall Score waarmee je later vergelijkt.

02 · RITME

Om de week iets kleins

Het Awareness-jaar plant automatisch: afwisselend een Unhooked-tip en een challenge, elk kwartaal een simulatie, in oktober een Phishing Hunt.

03 · LEREN

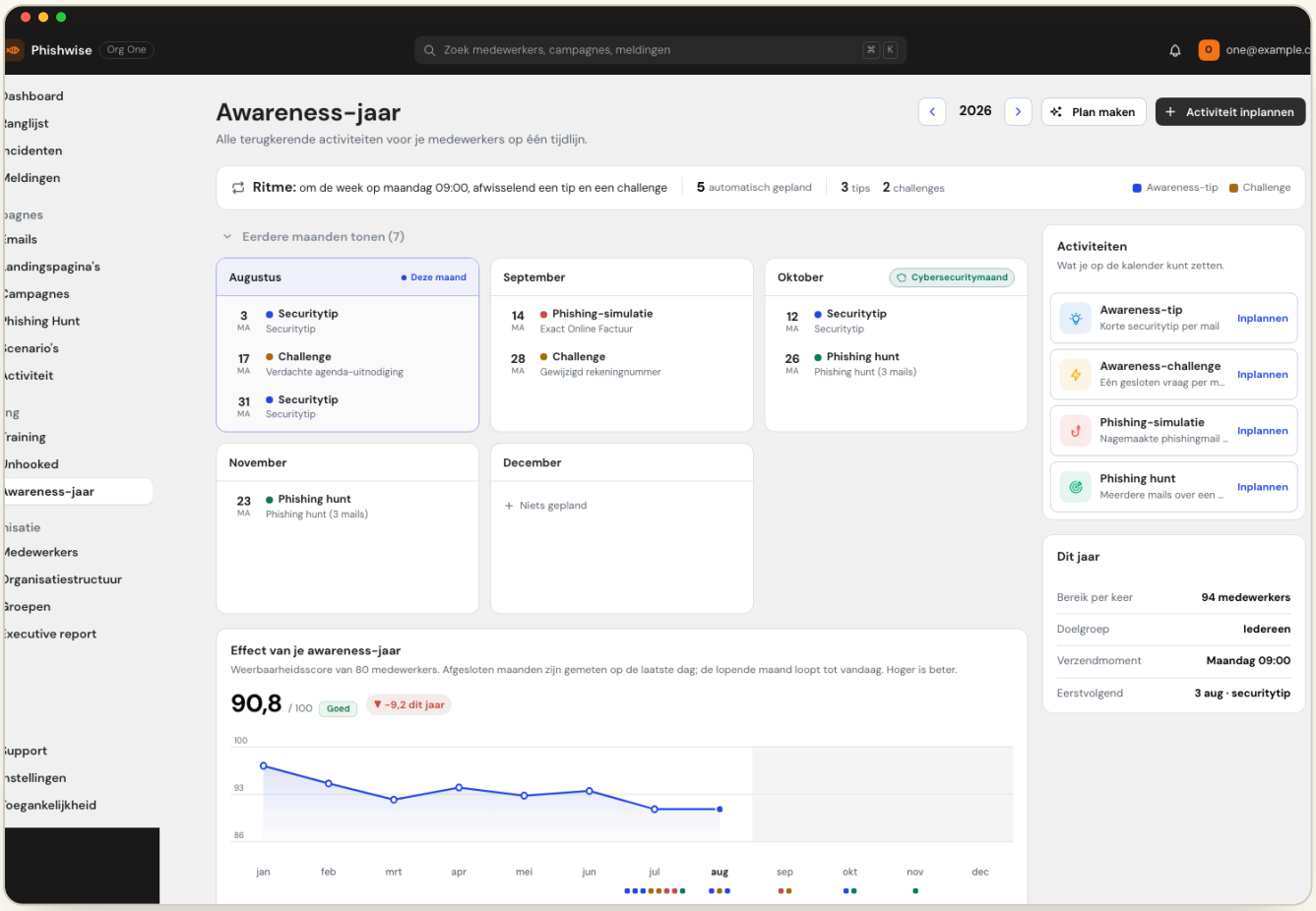
Direct na de klik

Wie klikt of gegevens invult, ziet meteen een lespagina en krijgt een korte training met deadline. Herinneringen gaan vanzelf.

04 · BIJSTUREN

Zien wat het doet

Het Executive report vergelijkt met de nulmeting en met vorig jaar, per team of locatie. Elke maand een snapshot, te delen met een link.



Het Awareness-jaar: alle activiteiten voor deze organisatie op één tijdlijn. Ritme: om de week op maandag 09:00, afwisselend een tip en een challenge; simulaties en de Phishing Hunt staan ertussen. Onderin de weerbaarheidsscore door het jaar heen.

Realistisch, niet gemeen

Scenario's lijken op de mail die jullie echt krijgen: een factuur van een leverancier, een agenda-uitnodiging, een bericht van HR. Geen valse bonus in december.

Melden is de goede afloop

Een Phishing Hunt is aangekondigd: een paar weken lang komen er nepmails en wint wie ze meldt. De Hunt telt bewust niet mee in de score.

Adaptief als je wilt

Unhooked kan tips kiezen op basis van wat iemand deed: klikken, gegevens invullen, een melding missen of een training laten liggen.

Wat erin zit

Alles werkt op dezelfde medewerkers, teams en resultaten. Een klik in een simulatie wordt een training, een melding wordt een plus in het rapport.

Simulaties

E-mails en landingspagina's uit de bibliotheek of zelf gemaakt; de AI-assistent schrijft een eerste versie in jullie huisstijl en toon. Scenario's in meerdere stappen, in acht categorieën, van urgentie tot een gekaapte mailthread. Eigen afzenderdomeinen, testverzending, doelgroepen per team, groep of persoon, gespreid en gerandomiseerd verzonden.

Unhooked en challenges

52 korte securitytips en 100 challenges (één vraag, direct feedback, zo nodig een training erachter), in het Nederlands en Engels. Wekelijks, tweewekelijks of maandelijks, op volgorde of adaptief. Eigen tips en challenges voeg je zelf toe, met jullie voorbeelden en media.

Training

Een cursusbibliotheek per sector (voor de zorg alleen al negentien cursussen), plus eigen trainingen met taalversies, quiz en herkansing. Toewijzen met de hand of automatisch na een klik, met deadline en herinneringen. Studytube-klanten starten de training vanuit hun eigen leeromgeving.

Melden en incidenten

Melden met de Outlook-meldknop, door de mail door te sturen, of via het portaal. Meldingen van simulaties herkent Phishwise vanzelf; echte meldingen beoordeel je als dreiging of vals alarm. Een klik of ingevuld wachtwoord wordt een incident met de bijbehorende training en status.

Rapportage

Dashboard met Human Firewall Score, faalpercentage, meldgedrag en trainingsstatus, per team, locatie of doelgroep en afgezet tegen de nulmeting. Executive report als PDF en Excel, automatisch een snapshot per maand, en een beveiligde deellink die 30 dagen werkt.

Portalen

Medewerkers zien hun eigen score, trainingen, simulatiegeschiedenis en meldroute. Managers zien alleen hun eigen team. De ranglijst werkt per organisatie of onderdeel en kan anoniem, met instelbare zichtbaarheid.

SECURITYTIPS	CHALLENGES	SCENARIOTYPES	ZORGCURSUSSEN
52	**100**	**8**	**19**
NL en EN, plus eigen tips	één vraag, directe feedback	van urgentie tot thread hijacking	en bibliotheken voor overheid en onderwijs

Inrichting en beheer

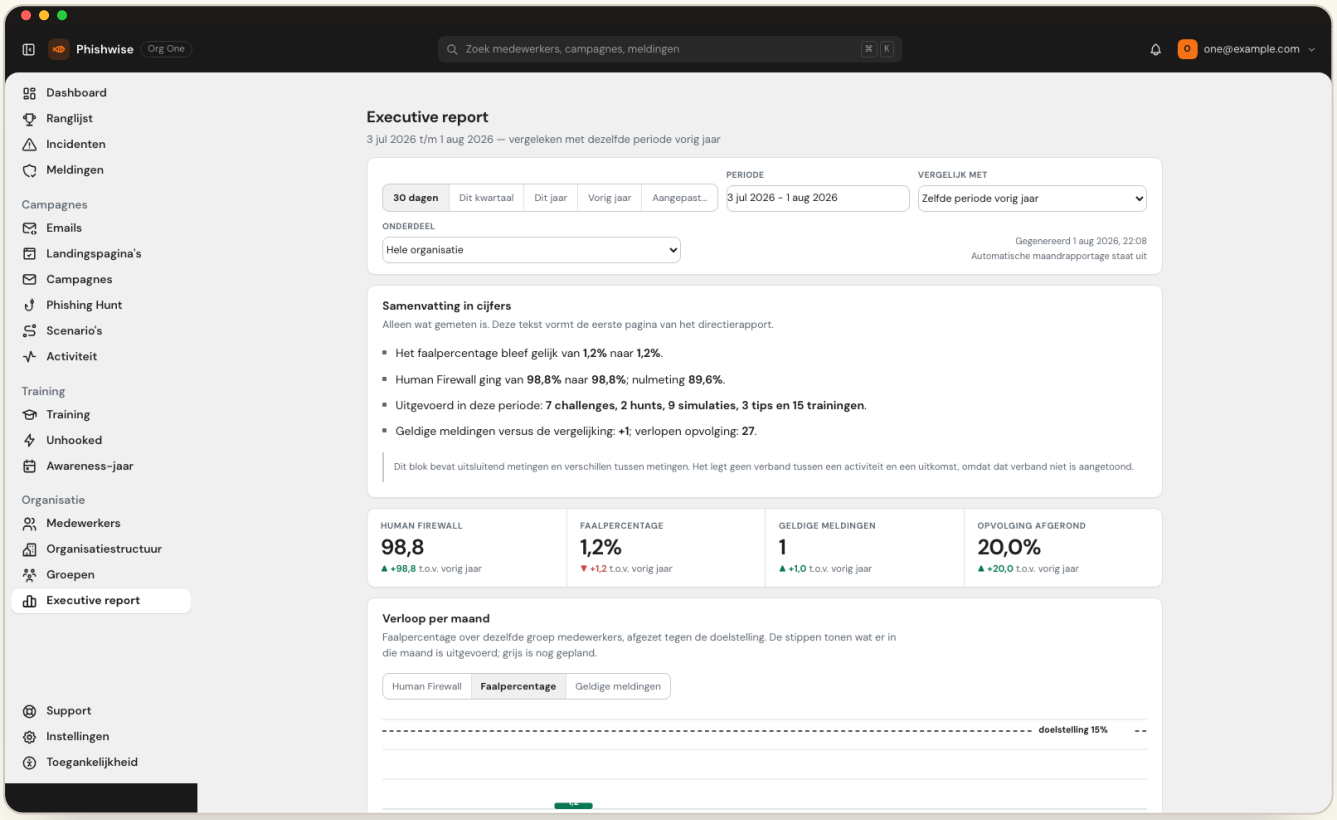
Sluit aan op wat er al is.

- Organisatiestructuur van elke diepte
- Rechten per onderdeel
- Eigen huisstijl
- Nederlands en Engels
- Mailpauze voor rustige periodes
- Terugkerende programma's
- Nulmetingen bewaren

Een rapport dat zegt wat gemeten is

Het Executive report is gemaakt om door te sturen naar een directie, een CISO of een auditor. Het begint met vier getallen en legt geen verband dat niet is aangetoond.

HUMAN FIREWALL	FAALPERCENTAGE	GELDIGE MELDINGEN	OPVOLGING AFGEROND
98,8	**1,2%**	**+1**	**20%**
nulmeting 89,6	doel 15%	t.o.v. vergelijking	trainingen na incident



Het Executive report over 30 dagen, vergeleken met dezelfde periode vorig jaar. De samenvatting in cijfers is de eerste pagina van de PDF. Cijfers uit een demo-omgeving.

Wat de Human Firewall Score is

Honderd min het percentage medewerkers dat in simulaties klikte. Geen samengestelde index met wegingen, zodat iedereen het kan narekenen. De aangekondigde Phishing Hunt telt niet mee: die meet meldgedrag, geen verrassing.

Wat je ermee doet

- Vergelijken met de nulmeting en met dezelfde periode vorig jaar.
- Per team, locatie of doelgroep kijken waar de aandacht heen moet.
- Maandelijks automatisch een snapshot, zodat de trend vaststaat.
- Exporteren als PDF of Excel, of delen met een link die 30 dagen geldig is.

Past in de omgeving die je al hebt

Verzending, inloggen, medewerkers en trainingen sluiten aan op wat er al draait. Geen aparte accounts, geen handmatige lijsten.

Microsoft 365

Simulaties worden verzonden via jullie eigen Microsoft 365 (Graph). We leveren de instellingen voor Advanced Delivery mee, zodat de mails niet in de spamfilter blijven hangen.

Outlook-meldknop

Een add-in voor Outlook op desktop, web en mobiel. Eén klik meldt de mail bij Phishwise; simulaties worden herkend, echte dreigingen komen bij jullie securityteam.

Microsoft Entra SSO

Beheerders loggen in met hun Microsoft-account. Medewerkers hebben geen wachtwoord nodig: het portaal opent met een persoonlijke link.

SCIM 2.0: HelloID, Entra

Medewerkers, groepen en de organisatiestructuur komen automatisch mee uit jullie bronsysteem. Wie uit dienst gaat, verdwijnt uit de simulaties.

Studytube (LTI 1.3)

Trainingen starten vanuit Studytube; Phishwise stuurt voortgang en score terug. Andere LTI-omgevingen in overleg.

API en webhooks

Meldingen, ranglijst en inkomende mail via de API. Voor wie zelf wil koppelen: documentatie en een sleutel per organisatie.

ZO BEGINNEN WE

Week 1 · Aansluiten

Koppelingen, huisstijl en een import of SCIM. De eerste nulmeting bij één afdeling.

Maand 1 · Ritme aan

Awareness-jaar inplannen, meldknop uitrollen, managers hun team laten zien.

Maand 3 · Eerste rapport

Executive report naast de nulmeting. Samen bijsturen waar het nodig is.

PRIJS

€ 2,50 per medewerker per maand

Onbeperkt simulaties, tips, challenges en trainingen. Eenmalige implementatie € 2.500. Jaarlijks vooruit, prijs twaalf maanden vast, volumekorting bij grotere organisaties.

Eerst zien?

Plan een proefperiode. We richten binnen 24 uur een omgeving in met jullie eigen domein en doen de eerste nulmeting bij een afdeling naar keuze. Daarna beslis je met cijfers.

hi@phishwise.nl · phishwise.nl