BESLIST

WIJZER IN IT MET KNOWBE4



Leer digitale dreigingen herkennen en melden met KnowBe4.

symbis

Persoonlijk betrokken



Security awareness die verder gaat dan één training

Een phishingmail herkennen klinkt eenvoudig. Totdat die precies lijkt op een bericht van HR, een leverancier of een collega.

Met KnowBe4 oefenen medewerkers regelmatig met realistische phishingmails en korte online trainingen. Zo leren ze niet alleen waar ze op moeten letten, maar vooral welk gedrag helpt: twijfelen, controleren en verdachte berichten melden.

KnowBe4 beschermt je technische omgeving niet, het houdt geen echte phishingmail tegen en monitort je IT-omgeving niet. Het helpt juist de mensen die zo'n bericht uiteindelijk in hun inbox krijgen om er beter mee om te gaan.

WAT DOET KNOWBE4?

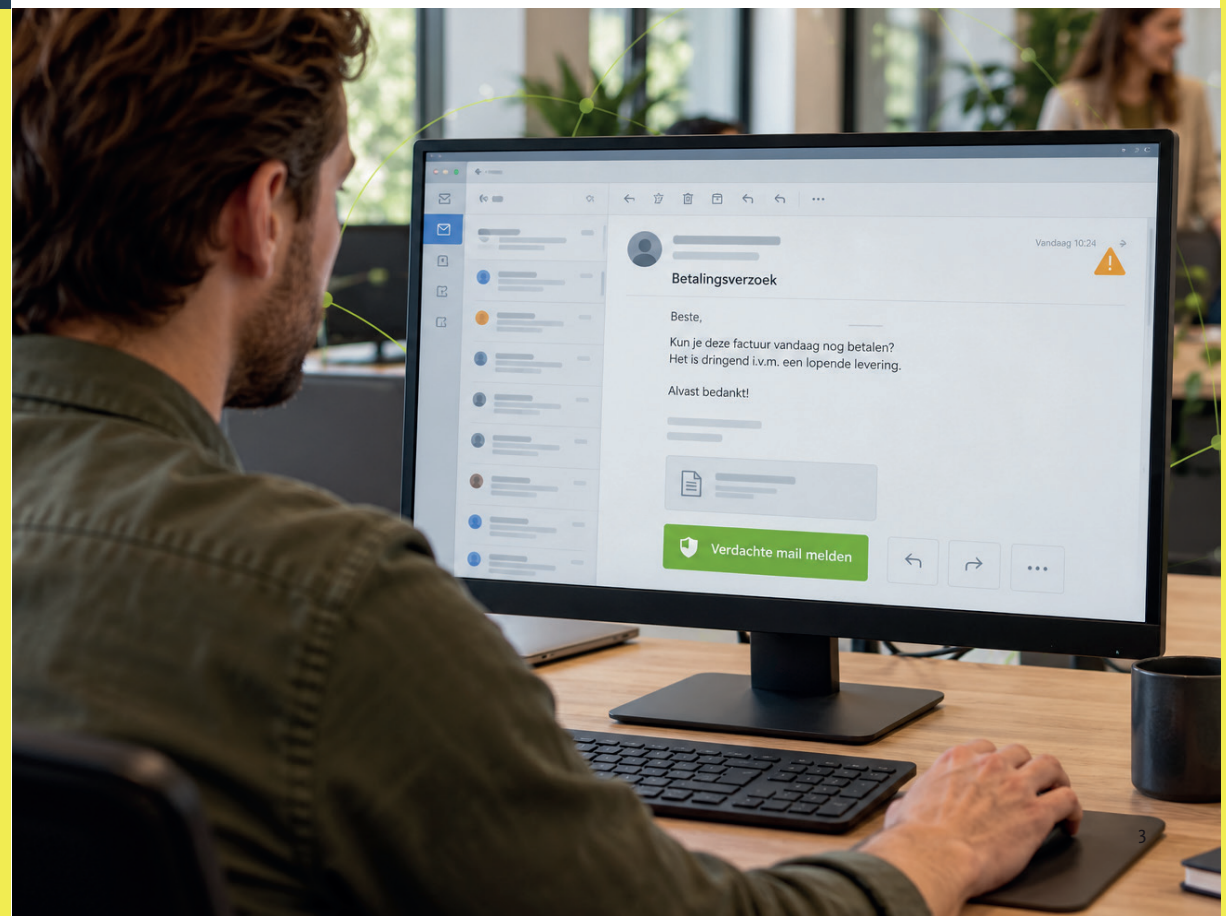
Medewerkers krijgen gesimuleerde phishingmails die lijken op berichten die ze ook in hun dagelijkse werk kunnen ontvangen.

Klikt iemand op een verdachte link? Dan kan daar een passende training op volgen. Meldt iemand de mail via de **Phish Alert Button** in Outlook? Dan wordt juist veilig gedrag geoefend en geregistreerd.

Zo krijg je steeds beter inzicht in waar medewerkers alert op zijn en waar extra aandacht nodig is.

HOE VOORKOM JE DAT IEDEREEN DEZELFDE TRAINING KRIJGT?

KnowBe4 gebruikt daarvoor AIDA: een functie die trainingen automatisch kan toewijzen op basis van wat iemand al weet en hoe iemand reageert op gesimuleerde phishingmails. Daardoor hoeft niet iedere medewerker precies hetzelfde leerprogramma te volgen.



Wat zijn de risico's en veelgemaakte fouten?

Een awarenessplatform aanschaffen is één ding.
Er vervolgens structureel mee blijven werken is iets anders.

WAT GEBEURT ER ALS ER GEEN JAARPLAN IS?

De eerste phishingtests worden enthousiast uitgezet. Maar zonder vaste planning kunnen campagnes er door drukte, vakantie of andere IT-projecten al snel bij inschieten. Dan meet je wel gedrag, maar stuur je er nauwelijks op.

BETEKENT EEN GOEDE SCORE DAT JE ORGANISATIE VEILIG IS?

Het simpele antwoord is: nee. De resultaten geven inzicht in het gedrag van medewerkers en kunnen laten zien wat je aan bewustwording doet. Maar ze bewijzen niet dat je IT-omgeving veilig is of dat niemand ooit meer op een phishingmail klikt. Awareness is onderdeel van cybersecurity, niet het hele antwoord.

WERKT DEZELFDE TRAINING VOOR IEDERE MEDEWERKER?

Niet altijd. Een medewerker van finance loopt andere risico's dan iemand in sales of management. Door trainingen en phishingtests af te stemmen op afdeling, functie en gedrag wordt het programma relevanter.

Wat we zelf terugzien

In de praktijk zien we zelf ook de positieve gevolgen van het gebruik van KnowBe4: ruim 25% lagere risicoscore in drie maanden.

Onze collega's krijgen trainingen en realistische phishingtests. Denk bijvoorbeeld aan een ogenschijnlijk normale mail over een salarisstrook, compleet met naam, deadline en een link die net niet klopt. In drie maanden daalde onze eigen risicoscore binnen KnowBe4 met ruim een kwart. Daarmee kwamen we in de laagste risicoband die het platform onderscheidt. Dat betekent niet dat een echte phishingmail nooit meer succesvol kan zijn. Het laat wel zien dat het gedrag dat KnowBe4 meet zich in de goede richting ontwikkelt.

De risicoscore is een maatstaf binnen KnowBe4 en geen formele auditnorm.
Cijfers laten zien wat er gebeurt. De waarde zit in wat je daarna verbetert.



Zelf beheren of laten doen: wat past er bij jouw organisatie?

KnowBe4 kun je prima zelf beheren wanneer security duidelijk belegd is, meerdere collega's het platform kennen en er een vaste planning ligt. Voordat je kiest, is er één praktische vraag die veel duidelijk maakt.

WIE ZORGT DAT DE CAMPAGNES BLIJVEN DRAAIEN?

Stel jezelf één vraag voordat je een prijsopgave aanvraagt:

Wie plant bij ons de campagnes en wie neemt het over als die collega drie weken weg is?

Heb je op allebei een antwoord, dan beheer je KnowBe4 zelf. Blijft het bij één antwoord of heb je er geen antwoord op, dan weet je nu al dat de licentie alleen niet genoeg is.

Wil je dat Symbis meekijkt naar wat bij jouw organisatie past, dan is dat gesprek de eerste stap.

WAAR HELPEN WIJ BIJ ALS JE HET BEHEER UIT HANDEN GEEFT?

Bij een beheerde aanpak helpen we onder andere met:

- de basisinrichting van KnowBe4;
- het inrichten van afdelingen en leerpaden op basis van de indeling die jij aanlevert;
- trainingen en leerpaden;
- phishingcampagnes;
- een jaarplanning;
- periodieke analyse van de resultaten;
- advies over vervolgstappen.

Wat er met een echte phishingmail gebeurt, blijft bij jouw eigen IT.

WAAROM SYMBIS KNOWBE4 ADVISEERT

Voor ons waren vooral drie dingen belangrijk:

1. **Training op maat**
   Een basis voor iedereen, met extra aandacht waar dat nodig is.
2. **Verschil per afdeling en functie**
   Niet ieder risico is voor iedere medewerker hetzelfde.
3. **Nederlandstalige content**
   Trainingen zijn in het Nederlands beschikbaar of ondertiteld.



Wie zorgt er binnen jouw organisatie voor dat security awareness niet na de eerste phishingtest stilvalt?

symbis

Persoonlijk betrokken

Van Hennaertweg 6,
Alblasserdam

078 - 699 58 99

www.symbis.nl

Volg ons ook op LinkedIn en blijf op de hoogte van
trends en ontwikkelingen via de artikelen op onze kennisbank.

LinkedIn Kennisbank Even sparren?