CYBER SECURITY AWARENESS

voor medewerkers om cyberdreigingen te herkennen

OBI Hét ICT Team

ZORGT DAT ICT WERKT. ALTIJD. OVERAL.

CYBER SECURITY AWARENESS

Voor organisaties die hun medewerkers willen trainen om cyber dreigingen te herkennen en te voorkomen.

INHOUD

OBI Automatisering | www.obi.nl | support@obi.nl

Tel. +31 (0)88 9008100 | Insulindelaan 111, 5642 CV Eindhoven

KVK nr. 17130973 | BTW nr. NL 8093.61.048.B01 | IBAN NL73ABNA0588512311

VOORKOM EEN CYBERAANVAL MET CYBER SECURITY AWARENESS

DE RISICO'S VAN CYBER AANVALLEN IN CIJFERS

In 2024 jaar was het percentage bedrijven dat te maken kreeg met een cyber event flink meer dan een jaar eerder. Het Amerikaanse verzekeringsbedrijf Hiscox[1] onderzocht bijna 5.000 organisaties die te maken hebben gehad met cyberincidenten en lekken. Hieronder een samenvatting van de statistieken over phishing en cybercrime uit het Hiscox Cyber Readiness Report 2024:

> ***"13 % van de onderzochte organisaties schatte hun financiële verlies door een cyberaanval tussen $100.000 en $499.000."***
>
> *- Hiscox*

- **Cyberaanvallen nemen toe**
  Bedrijven krijgen steeds vaker te maken met digitale aanvallen. Gemiddeld werd een bedrijf vorig jaar **66 keer aangevallen**.
- **Schade is groot**
  Aanvallen kosten niet alleen geld (13% van de organisaties verloor tussen $100-$499k), maar ook klanten en reputatie. Bijna de helft van de getroffen bedrijven verloor klanten of kreeg een slechte naam.
- **Hoe criminelen binnenkomen**
  De meeste aanvallen beginnen via **nep-e-mails**, **kwetsbare cloudservers**, of door medewerkers te misleiden (**phishing/social engineering**).
- **Fraude is grootste dreiging**
  Vooral **betalingsfraude** (bijvoorbeeld dat geld naar de verkeerde rekening gaat) wordt gezien als het grootste risico.
- **Nieuwe technologie zoals AI**
  Ongeveer **70% van de bedrijven gebruikt kunstmatige intelligentie (AI)**. Dit brengt kansen, maar ook nieuwe risico's.

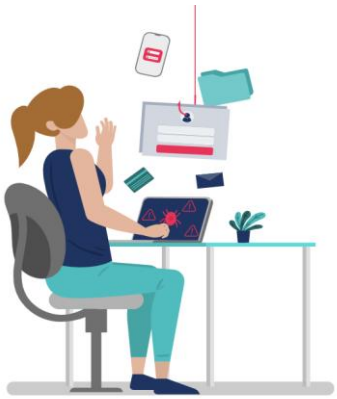
CREËER EEN MENSELIJKE FIREWALL

Vandaag de dag heeft het grootste gedeelte van alle cyberaanvallen een menselijke interactie nodig. Een medewerker klikt onbedoeld op een link in een nep e-mail (phishing), waardoor ransomware het bedrijf overneemt, waarna een hacker losgeld zal eisen om de gegijzelde (versleutelde) bestanden weer vrij te geven. Het gebeurt vaker dan je zou vermoeden. Daarom is er het besef nodig dat een investering in een 'menselijke firewall' even noodzakelijk is als investeren in technische infrastructuur.

OBI helpt organisaties een eigen Menselijke Firewall te bouwen, maar wat betekent dat en waarom is het belangrijk? De traditionele cyber security awareness training met een Powerpoint presentatie voldoet niet langer aan de vereisten om de kwetsbare groep medewerkers weerbaar te maken tegen een cyberaanval. Er

[1] Bron: https://www.hiscoxgroup.com/cyber-readiness

ontbreken namelijk enkele basisingrediënten: Het regelmatig ‘updaten’ van het kennisniveau, het controleren en ‘monitoren’ van eventuele zwakke schakels of lekken in de beveiliging.



“Meer dan 99 procent van de waargenomen aanvallen vereiste menselijke interactie om te werken”

“Microsoft-gerelateerde aanvallen bleven het populairst”

- Proofpoint

OBI heeft in samenwerking met haar software partner ‘KnowBe4’ een programma opgezet waarbij er **continu wordt gemeten waar de zwakste schakel zit in de menselijke firewall door het simuleren van cyberaanvallen met nep e-mails.**

ALLEEN DAAR TRAINEN WAAR NODIG

Medewerkers zijn al druk genoeg en trainen is goed, maar liever niet ten koste van de productiviteit van de organisatie. Daarom meet OBI eerst wíe er behoefte heeft aan cyber security trainingen door middel van een 0-meting met een phishing aanval simulatie met nep e-mail, gevolgd door een bewustwording sessie (Cyber Security Awareness training) voor de medewerkers die het nodig hebben.

> ***“Medewerkers zijn al druk genoeg en trainen is goed,***
> ***maar liever niet ten koste van de productiviteit van de organisatie.”***

Continue awareness binnen uw organisatie wordt gecreerd door continue simulatie van nep e-mail trainingen met dezelfde phishing aanval simulaties.
Medewerkers die onverhoopt op links blijven klikken tijdens de gesimuleerde phishing aanvallen kunnen extra getraind worden door middel van begeleiding, een workshop via Teams, of bij u op locatie door uw persoonlijke Security Officer van OBI.

HET CYBER SECURITY AWARENESS PROGRAMMA VAN OBI

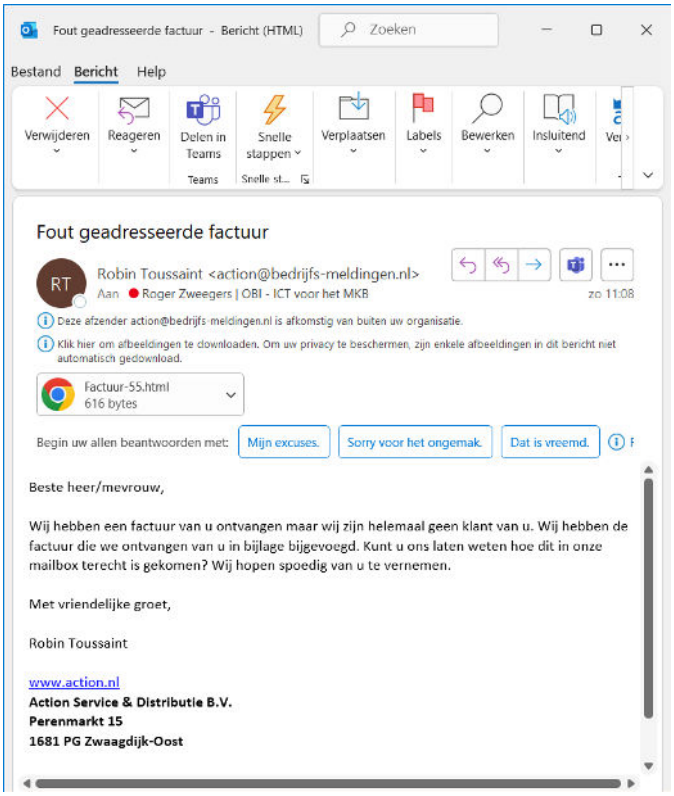
GEAUTOMATISEERDE AANVAL MET NEP E-MAIL (PHISHING) SIMULATIES

Cyber security awareness voor medewerkers door middel van een gesimuleerde aanval met nep e-mail betekent dat OBI nep e-mails simuleert en deze verstuurt naar de medewerkers, zonder de gevaren van echte hackers.

Door medewerkers in contact te laten komen met alle mogelijke phishingvarianten, in een veilige en gecontroleerde omgeving, herkennen zij de echte gevaren wanneer die zich voordoen.

De phishing simulator is ingebouwd met een zelflerende module die rekening houdt met het gedrag van elk individu en daarmee zijn aanpak aanpast bij elke simulatie op basis van klikgedrag van de gebruiker.

De simulator verstuurt periodiek geautomatiseerde phishingsimulaties, die zowel qua timing als qua inhoud zijn afgestemd op de ontvanger.



MAATWERK SPEAR-PHISHING AANVAL MET NEP E-MAIL SIMULATIES

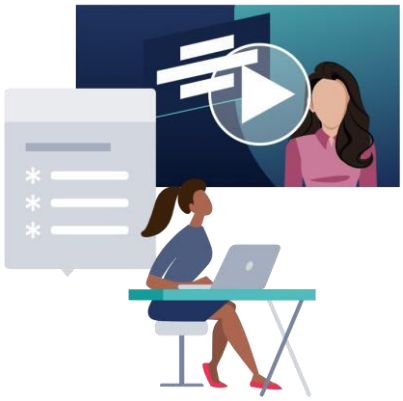
Hackers gebruiken vaak publiekelijk beschikbare informatie, zoals details over een aanstaande bedrijfsverhuizing of de oprichtingsdatum van het bedrijf, om hun spear-phishing aanvallen een schijn van legitimiteit te geven. Zo kan een aanvaller zich voordoen als de secretaresse van het bedrijf en medewerkers benaderen met een verzoek om suggesties voor een origineel cadeau voor de eigenaar, ter ere van een speciale gelegenheid. Deze schijnbaar onschuldige verzoeken zijn in werkelijkheid verkapte pogingen om medewerkers te misleiden tot het delen van gevoelige informatie of het ondernemen van acties die het bedrijf kunnen schaden, zoals het overmaken van geld of het klikken op een link die leidt naar een kwaadaardige website.

Deze vorm van spear-phishing simulaties met nep e-mail worden handmatig door OBI uitgevoerd in overleg met de centrale contactpersoon van de opdrachtgever en zijn standaard onderdeel van de dienstverlening.

BEWUSTWORDING WORKSHOPS

Tijdens de workshop Cyber Security Awareness worden verschillende groepen medewerkers binnen een organisatie bewuster gemaakt van cybercrime. Een aanvulling op de online training waar nodig. Dit kan via Teams of bij opdrachtgever op locatie.

"Het online Cyber Security Awareness training programma kan worden uitgebreid met maatwerk workshops op locatie"



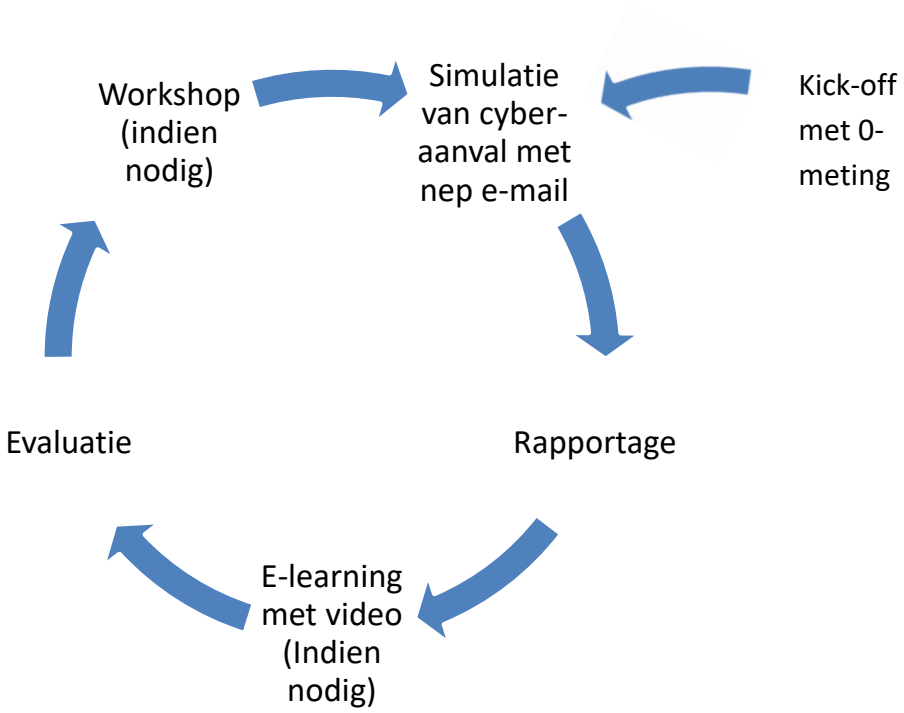
ONLINE CYBER SECURITY AWARENESS TRAINING PLATFORM

Het online Security Awareness Training platform van KnowBe4 helpt organisaties hun medewerkers te beschermen tegen cyberdreigingen door middel van gesimuleerde phishing-tests en een uitgebreide bibliotheek met interactieve leermiddelen. Gebruikers leren verdachte e-mails te herkennen en rapporteren, terwijl organisaties met gedetailleerde rapportages hun beveiligingsniveau kunnen monitoren en verbeteren.

WERKWIJZE EN PLANNING

Kick-off en onboarding van organisatie met simulatie van nep e-mail

1. Inrichten simulatie software t.b.v. Cyber Security Awareness campagne.
   De gebruikers worden gekoppeld aan het KnowBe4 platform, de phishing mailings worden ingesteld inclusief sjablonen en handtekeningen van de organisatie en de rapportages worden ingericht.
2. 0-meting met eerste simulatie van een nep e-mail aanval
   Hierbij wordt het kennisniveau van de eindgebruikers in kaart gebracht via een eerste simulatie. Indien gewenst kan dit met een maatwerk spear-phishing campagne.
3. Evaluatie 0-meting met rapportage naar centrale contactpersoon (via Teams)
4. Kick-off Cyber Security Awareness campagne naar eindgebruikers
   (Introductie naar eindgebruikers per e-mail via centrale contactpersoon opdrachtgever)
5. Periodieke simulatie van aanval met nep e-mail (geautomatiseerd), gemiddeld 1 mail per week per medewerker
6. Periodieke rapportage
7. Persoonlijke begeleiding “Cyber Security en nep e-mails” voor mensen die vaker ‘in de val trappen’



RAPPORTAGE EN COMPLIANCY

RAPPORTAGE EN EVALUATIE

Periodiek zal er door OBI uitgebreide rapportering plaatsvinden op basis van gedragsanalyses per afdeling, ontvanger, functie en locatie. Op deze manier kan met de opdrachtgever worden afgestemd of er extra begeleiding nodig is voor een kwetsbare groep gebruikers of afdeling binnen de organisatie.
Daarnaast kan de rapportage gebruikt worden om externe audits van de klant te ondersteunen als bewijslast.

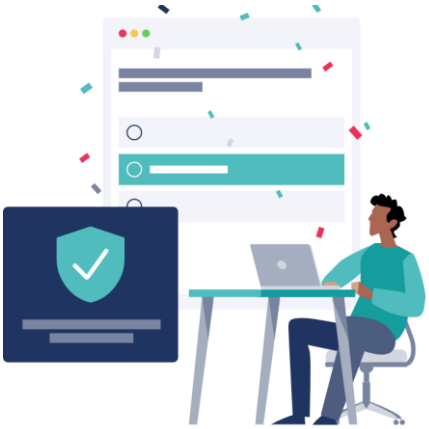
ISO 27001

OBI helpt organisaties voldoen aan cyber security certificeringen, zoals de ISO 27001-normen. Anti-phishingtraining vormt een belangrijke manier om de staat en evolutie van cyber security awareness maatregelen te evalueren en te verbeteren (PDCA). Bovendien draagt de online trainingmodule bij tot het behalen van de ISO-norm rond permanente bijscholing over informatiebeveiliging en maakt deze het makkelijk om de stand van zaken te meten, bij te houden, te documenteren en te verbeteren binnen de organisatie.

VOLDOEN AAN DE AVG/GDPR PRIVACY & NIS2 WETGEVING

De AVG privacy wetgeving én de NIS2 wetgeving stellen dat organisaties technische en organisatorische maatregelen moeten nemen om de kans op datalekken te verkleinen. Dit Cyber Security Awareness programma valt onder deze categorie organisatorische maatregelen.

“Een Cyber Security Awareness programma helpt je organisatie te voldoen aan de NIS2 wetgeving”



TARIEVEN

Licentie KnowBe4 phishing platform	**Eenmalig tarief**	**Jaarlijks tarief**
Een licentie voor toegang tot het online phishing platform waarmee uw medewerkers continue worden getest via een geautomatiseerde aanval met nep e-mail simulaties. Dit online software platform wordt door OBI voor opdrachtgever beheerd. **Inclusief:** • Setup en inrichting nep e-mail simulatie software • **Simulatie met nep e-mail**, 1x per week per medewerker • Beheer platform + aanmaken / wisselen van gebruikers • **Rapportage** en statistieken per e-mail • **Online Cyber Security Awareness trainingen**	**€ 600,00** Eenmalig setup	**€ 46,80** per gebruiker
Voorwaarden: • Tarieven zijn exclusief btw • Facturatie is jaarlijks en vooruit • Jaarlijks opzegbaar, één maand voor afloop abonnement • Minimum afname van 25 licenties, koppeling van gebruikers via Active Directory / Entra ID • Meerprijs voor uitgebreide online Security Awareness Trainingen, AI-driven phishing en Password vulnerability monitoring in de Active Directory: € 22,00 per gebruiker per jaar		

Maatwerk spear-phishing simulatie met nep e-mail	**Eenmalig tarief**
<u>Maatwerk simulatie van cyber-aanval met nep e-mail</u> Uw medewerkers worden getest door een aanval via 'spear phishing'. Hierbij wordt het scenario gesimuleerd dat een hacker probeert binnen te komen door een maatwerk geschreven e-mail met handtekening en contactgegevens van de organisatie. **Inclusief:** • Maatwerk geschreven nep e-mail specifiek gericht op opdrachtgever • Inrichting spear phishing campagne en versturen van nep e-mail simulatie • Rapportage en statistieken • Evalueren en bespreken van rapportage (via Teams)	**€ 800,00**
Voorwaarden: • Tarieven zijn exclusief btw • Exclusief maatwerk workshop in navolging van deze spear-phishing campagne (zie volgende pagina)	

Maatwerk Workshops	
Workshop categorie	**Tarieven**
Cyber Security en nep e-mail : • Hoe werken hackers • Risico's voor organisatie en medewerkers (ook privé) • Wat kun jij doen? Veilige wachtwoorden en 2-stap verificatie Hoe herken je een nep e-mail (globaal) Hoe herken je een nep helpdesk • Spookfacturen • CEO mail	**€ 135,00 per uur** max. 10 gebruikers per sessie, max. 4 sessies per dag
Cyber Security voor directie en MT: • Bewustwording bij medewerkers • Periodieke interne audits op ICT • Cyber Security risico inventarisatie • De voordelen van een IT beleid met gedragscode	**€ 135,00 per uur** max. 10 gebruikers per sessie, max. 4 sessies per dag
AVG / GDPR privacy wetgeving Categorie keuze: • AVG/GDPR privacy bewustwording voor directie en het MT • AVG/GDPR privacy bewustwording voor medewerkers	**€ 135,00 per uur** max. 10 gebruikers per sessie, max. 4 sessies per dag
Voorwaarden: • Tarieven zijn exclusief btw en reiskosten • Maximaal 10 eindgebruikers per sessie van één uur • Een workshop wordt op locatie gegeven	