GIDS

De complete gids voor security awareness training

Trainingsvormen, kosten, effectiviteit, NIS2-verplichtingen en selectiecriteria. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Security awareness training is geen luxe meer -- het is een zakelijke noodzaak. Hieronder de feiten voor Nederlandse organisaties.

33,1%
van ongetrainde medewerkers klikt op een phishing link -- 1 op 3
KnowBe4 Phishing Benchmark 2025 [1]

86%
reductie in phishing-klikken na 12 maanden doorlopende training
KnowBe4 Phishing Benchmark 2025 [1]

43%
van het Nederlandse MKB meldde een cyberincident in 2024
MKB Servicedesk [2]

EUR 270K
gemiddelde schade per cyberincident voor MKB in Nederland
Hallo.eu / Cybercrimebeeld NL [3]

70%
van organisaties vindt dat medewerkers fundamentele security awareness missen
Fortinet 2024 Report [4]

50%
van bedrijven (10+ medewerkers) maakt geen risicoanalyse
CBS Cybersecuritymonitor 2024 [5]

Q2 2026
Verwachte inwerkingtreding Cyberbeveiligingswet (NIS2) -- awareness training wordt verplicht
Digitale Overheid [6]

80%
van nieuwe kennis vergeten binnen 4 weken zonder herhaling
Diverse onderzoeken [7]

1. Wat is security awareness training?

Security awareness training is een doorlopend programma dat medewerkers leert om cyberdreigingen te herkennen, veilig te handelen en incidenten te melden. Het doel is niet alleen kennis overdragen -- het gaat om gedragsverandering.

Traditioneel bestond security awareness uit een jaarlijkse presentatie of e-learning module. Die aanpak is achterhaald. Moderne programma's combineren meerdere methoden: korte online modules, gesimuleerde phishing-aanvallen, interactieve quizzes en rapportages die laten zien hoe je organisatie presteert.

Het verschil met pure IT-beveiliging is belangrijk. Firewalls, antivirus en endpoint protection beschermen je systemen. Awareness training beschermt de mens -- en de mens is in 60% van alle datalekken de zwakste schakel [8].

> **In de kern:** Security awareness training maakt van je medewerkers een actieve verdedigingslinie in plaats van je grootste kwetsbaarheid. Het gaat niet om IT-kennis, maar om dagelijkse gewoontes: wachtwoorden, links, bijlagen, meldgedrag.

WAAR GAAT HET OVER?

Een volledig awareness programma omvat minimaal deze onderwerpen:

- **Phishing herkenning** -- verdachte e-mails, links en bijlagen identificeren
- **Wachtwoordbeleid** -- sterke wachtwoorden, wachtwoordmanagers, geen hergebruik
- **Social engineering** -- manipulatietechnieken herkennen (telefoon, e-mail, fysiek)
- **Veilig werken op afstand** -- VPN, openbare wifi, schermvergrendeling
- **Incidentmelding** -- wat doe je als je iets verdachts ziet?
- **Clean desk en fysieke beveiliging** -- documenten, USB-sticks, tailgating
- **Privacybewustzijn (AVG)** -- persoonsgegevens herkennen en beschermen

2. Waarom is het belangrijk?

Cyberaanvallen richten zich steeds vaker op mensen in plaats van systemen. De cijfers laten zien waarom awareness training geen optionele investering is.

DE MENSELIJKE FACTOR

Volgens het Verizon DBIR 2025 is bij circa 60% van alle datalekken een menselijke actie betrokken -- een verkeerde klik, een zwak wachtwoord, of een onoplettend moment [8]. IBM becijfert dat 26% van alle datalekken direct veroorzaakt wordt door menselijke fouten, met een gemiddelde schade van USD 3,62 miljoen per incident [9].

NEDERLANDS MKB ONDER DRUK

De cijfers voor het Nederlandse MKB zijn alarmerend:

- **43%** van mkb-bedrijven meldde een cyberincident in 2024 -- een stijging van 18% ten opzichte van 2023 [2]
- **77%** van het MKB had in de afgelopen twee jaar minstens een keer te maken met cybercrime [10]
- **60%** van kleine bedrijven gaat failliet binnen 6 maanden na een ernstige cyberaanval [10]
- De gemiddelde schade per cyberincident bedraagt **EUR 270.000** [3]

SOCIAL ENGINEERING DOMINEERT

Social engineering -- waarvan phishing de meest voorkomende vorm is -- is verantwoordelijk voor het overgrote deel van succesvolle aanvallen. 33,1% van ongetrainde medewerkers klikt op een phishing link [1]. Dat is 1 op 3. Bij een organisatie van 100 medewerkers betekent dat 33 potentiele ingangen voor aanvallers.

WAAROM TECHNISCHE BEVEILIGING ALLEEN NIET GENOEG IS

- Social engineering omzeilt technische maatregelen door de mens te manipuleren
- Phishing e-mails worden steeds geavanceerder -- AI maakt ze nauwelijks te onderscheiden van echte berichten
- 50% van bedrijven met 10+ medewerkers maakt geen risicoanalyse [5]
- Technische maatregelen vangen niet alles -- de laatste verdedigingslinie is altijd de medewerker

REKENSOM

Gemiddelde kosten phishing-incident in Nederland: EUR 70.000 [11]. Jaarlijkse kosten awareness platform (100 users): EUR 3.000--10.000. Een voorkomen incident betaalt 7--23 jaar training terug.

3. Hoe werkt het?

Moderne security awareness training combineert meerdere methoden in een doorlopend programma. Hieronder de belangrijkste vormen en hoe ze samenwerken.

E-LEARNING MODULES

Online cursussen die medewerkers in eigen tempo doorlopen. Onderwerpen varieren van phishing herkenning tot wachtwoordbeheer. Modules duren doorgaans 10--20 minuten en bevatten quizzes om begrip te toetsen. Schaalbaar en consistent, maar als enige methode te passief voor echte gedragsverandering.

PHISHING SIMULATIES

Gesimuleerde phishing e-mails die naar medewerkers worden gestuurd om hun reactie te meten. Wie klikt, krijgt direct feedback en een korte uitleg. Dit is de krachtigste methode voor gedragsverandering: het creëert een realistisch leermoment zonder risico. Na 12 maanden doorlopende simulaties daalt het klikpercentage van 33,1% naar 4,1% -- een reductie van 86% [1].

MICRO-LEARNINGS

Korte modules van 3--5 minuten, wekelijks of maandelijks. Dit model levert de beste kennisretentie op: kleine hapklare lessen die in de werkdag passen. Ideaal als basis voor een doorlopend programma.

GAMIFICATION

Punten, badges, leaderboards en challenges die training aantrekkelijker maken. Competitieve elementen verhogen de betrokkenheid, vooral bij teams die van nature competitief zijn. Niet voor iedere organisatie geschikt, maar effectief als aanvulling.

OPTIMALE CADANS

FREQUENTIE	EFFECT	AANBEVELING
Jaarlijks	Minimaal effect -- 80% vergeten binnen 4 weken [7]	Onvoldoende
Kwartaal	47% van organisaties kiest dit [4]	Basisniveau
Maandelijks	Tot 60% reductie phishing in 12 maanden [4]	Aanbevolen
Wekelijks (micro)	Beste kennisretentie, 3--5 min per sessie	Optimaal

Best practice: Maandelijkse korte modules (5--10 min) gecombineerd met kwartaal phishing simulaties en een jaarlijkse verdiepingssessie. 89% van organisaties rapporteert verbetering na implementatie van deze aanpak [4].

4. Wat kost het?

De kosten van security awareness training varieren sterk -- van EUR 28 per medewerker per jaar voor een doorlopend platform tot EUR 500 per persoon voor een eenmalige klassikale training.

KOSTEN PER MODEL

MODEL	KOSTEN PER MEDEWERKER	EFFECTIVITEIT
Doorlopend SaaS-platform	EUR 28--39/jaar	86% reductie phishing clicks na 12 maanden [1]
Standaard e-learning	EUR 100--200/jaar	Goed -- interactieve modules, simulaties, assessments
Premium blended	EUR 200--350/jaar	Online + live sessies, uitgebreide rapportages
Klassikaal (eenmalig)	EUR 200--500/deelnemer	Kennis vervaagt binnen 4 weken (80% vergeten) [7]
Volledig gepersonaliseerd	EUR 350--500/jaar	Sector-specifiek, individuele coaching

JAARKOSTEN VOOR MKB

ORGANISATIEGROOTTE	BUDGET (SAAS)	STANDAARD	PREMIUM
25 medewerkers	EUR 700--975	EUR 2.500--5.000	EUR 5.000--8.750
50 medewerkers	EUR 1.400--1.950	EUR 5.000--10.000	EUR 10.000--17.500
100 medewerkers	EUR 2.800--3.900	EUR 5.000--10.000	EUR 15.000--30.000
250 medewerkers	EUR 7.000--9.750	EUR 10.000--20.000	EUR 25.000--50.000

Volumekortingen zijn gebruikelijk bij 50+ medewerkers. Bij meerjarige contracten liggen onderhandelde prijzen doorgaans 22--55% onder de lijstprijs [12].

DOORLOPEND IS GOEDKOPER EN EFFECTIEVER

Een eenmalige klassikale training kost EUR 200--500 per persoon en het effect verdwijnt snel. Een doorlopend platform kost EUR 28--39 per persoon per jaar en levert aantoonbaar betere resultaten op. Over 3 jaar betaal je minder en bereik je meer.

5. Waar moet je op letten?

Niet elk awareness platform is geschikt voor elke organisatie. Hieronder de selectiecriteria die je helpen een onderbouwde keuze te maken.

SELECTIECRITERIA

CRITERIUM	WAAROM BELANGRIJK
Nederlandse taalondersteuning	Content moet in correct Nederlands beschikbaar zijn -- inclusief actuele dreigingsscenario's
Phishing simulaties inbegrepen	Gedragsverandering vereist realistische oefeningen, niet alleen theorie
Rapportage en compliance dashboard	Je moet kunnen aantonen dat medewerkers getraind zijn (NIS2-eis)
Rolgebaseerde content	Financiele medewerkers hebben andere training nodig dan receptie
Automatisering	Automatische campagnes, herinneringen en escalaties besparen IT-uren
Integratie	Koppeling met je e-mailplatform, SSO en HR-systeem
Frequentie en micro-learnings	Wekelijkse of maandelijkse korte modules leveren betere resultaten dan kwartaalmodules
Gamification	Verhoogt engagement -- niet essentieel, maar een pluspunt
Sector-specifieke scenario's	Relevante content voor jouw branche verhoogt betrokkenheid
Support en onboarding	Hoe snel ben je operationeel? SaaS-platforms: 1--5 werkdagen [13]

10 VRAGEN AAN EEN LEVERANCIER

1. Welke talen worden ondersteund, en hoe actueel is de Nederlandse content?
2. Zijn phishing simulaties inbegrepen of een aparte module?
3. Hoe ziet de rapportage eruit -- kan ik per afdeling en per medewerker filteren?
4. Ondersteunen jullie rolgebaseerde trainingsprofielen?
5. Hoe vaak wordt de content bijgewerkt met nieuwe dreigingsscenario's?
6. Welke integraties bieden jullie (SSO, e-mailplatform, HR-systeem)?
7. Wat is de gemiddelde opstarttijd en wie begeleidt de implementatie?

8. Bieden jullie NIS2-compliance rapportages?
9. Wat is jullie aanpak bij medewerkers die herhaaldelijk op simulaties klikken?
10. Wat zijn de contractvoorwaarden -- looptijd, opzegtermijn, volumekortingen?

6. Veelgemaakte fouten

De meeste awareness programma's falen niet door de technologie, maar door de aanpak. Hieronder de acht fouten die je moet vermijden.

#	FOUT	IMPACT
1	**Eenmalige jaarlijkse training**	80% van nieuwe kennis vergeten binnen 4 weken [7]. Geen meetbare gedragsverandering.
2	**Compliance-first mindset**	"Death by PowerPoint" -- checkbox-mentaliteit zonder echte gedragsverandering. Medewerkers zien het als verplicht nummer.
3	**Geen baseline meting**	Zonder nulmeting kun je geen voortgang aantonen en geen ROI berekenen.
4	**Strafcultuur bij falen**	Medewerkers melden incidenten niet meer uit angst voor consequenties. Het tegenovergestelde van wat je wilt bereiken.
5	**Geen management buy-in**	Geen budget, geen tijd in werkroosters, medewerkers nemen het niet serieus als de directie het zelf niet doet [14].
6	**Te agressieve phishing simulaties**	Wantrouwen richting IT/security team. Ondermijnt het programma in plaats van het te versterken [14].
7	**Information overload**	Te veel content in een keer = niets onthouden. Micro-learnings (3--5 minuten) werken aantoonbaar beter.
8	**One-size-fits-all content**	Niet relevant voor de functie = lage engagement. Financiele afdeling heeft andere risico's dan productie.

WAT WERKT WEL

- **Doorlopend, niet eenmalig** -- minimaal maandelijks contact
- **Positieve bekrachtiging** -- beloon goed gedrag, publiceer successen
- **Meten en rapporteren** -- phishing click rate, completion rate, incident reports
- **Management doet mee** -- C-level volgt dezelfde training
- **Relevante content** -- afgestemd op sector, functie en actuele dreigingen
- **Laagdrempelig** -- korte modules die in de werkdag passen

7. NIS2: wat wordt verplicht?

De Cyberbeveiligingswet (de Nederlandse implementatie van NIS2) gaat naar verwachting in het tweede kwartaal van 2026 in werking. Awareness training wordt daarin expliciet verplicht.

WETTELIJK KADER

De NIS2-richtlijn stelt in Artikel 21(2)(g) expliciete eisen aan cyberhygiene en awareness training. De Cyberbeveiligingswet vertaalt deze eisen naar Nederlands recht [6].

CONCRETE VERPLICHTINGEN

VERPLICHTING	DETAIL
Alle medewerkers	Regelmatig cybersecurity training -- niet alleen IT-personeel
Bestuurders (Art. 20(2))	Moeten binnen 2 jaar na inwerkingtreding training volgen [15]
Rolgebaseerd	Training afgestemd op functie, risiconiveau en verantwoordelijkheden
Frequentie	Regelmatig en doorlopend -- maandelijks of kwartaal wordt aanbevolen
Cyberhygiene (Art. 21(2)(g))	Wachtwoordbeleid, software-updates, phishing herkenning [15]
Documentatieplicht	Het weglaten van enige groep medewerkers geldt als bevinding bij audit
Scope	Vast personeel, tijdelijk personeel, remote/onsite, contractors -- iedereen [16]

> **LET OP: KETENVERANTWOORDELIJKHEID**
> Niet alleen "essentiële" entiteiten vallen onder NIS2. Voor MKB-bedrijven die leveren aan NIS2-plichtige organisaties wordt awareness training een keten-eis -- ook als je zelf niet direct onder de wet valt [15].

PRAKTISCHE IMPLICATIES VOOR MKB

Als jouw organisatie onder NIS2 valt of levert aan partijen die eronder vallen, moet je:

1. Een doorlopend awareness programma implementeren dat alle medewerkers bereikt
2. Trainingsdeelname documenteren en kunnen overleggen bij audit
3. Bestuurders apart trainen op cybersecurity-risico's en verantwoordelijkheden
4. Bewijs kunnen leveren van regelmatige updates en actuele content

8. Awareness vs phishing simulatie vs e-learning

De termen worden vaak door elkaar gebruikt, maar er zijn belangrijke verschillen. Hieronder een heldere vergelijking.

ASPECT	PURE AWARENESS TRAINING	PHISHING SIMULATIE	E-LEARNING PLATFORM	GECOMBINEERD
Doel	Kennis overdragen	Gedrag testen en trainen	Gestructureerd leren	Kennis + gedrag + meting
Aanpak	Informatief, passief	Praktisch, actief	Interactief, self-paced	Multi-channel
Effectiviteit	Matig (alleen kennis)	Hoog (gedragsverandering)	Matig--goed	Hoogst
Meetbaarheid	Laag (completion rates)	Hoog (click rates, report rates)	Gemiddeld (scores)	Volledig beeld
NIS2-compliant	Deels	Deels	Deels	Ja
Kosten (100 users)	EUR 5.000--20.000 eenmalig	EUR 2.000--6.000/jaar	EUR 5.000--15.000/jaar	EUR 5.000--20.000/jaar
Engagement	Laag--gemiddeld	Hoog (real-world)	Afhankelijk van platform	Hoog

> **Aanbeveling:** De marktstandaard verschuift naar geintegreerde platforms die alle drie combineren: phishing simulaties voor baseline en voortgangsmeting, e-learning modules voor kennisoverdracht, micro-learnings en gamification voor retentie, en dashboards voor NIS2-compliance bewijs [17].

9. Trends 2025--2026

De awareness markt verandert snel. Hieronder de vier trends die bepalen hoe training er in 2026 uitziet.

AI-GEGENEREERDE CONTENT EN DREIGINGEN

Meer dan 60% van organisaties verwacht dat medewerkers vaker slachtoffer worden van AI-aangedreven aanvallen [4]. AI maakt phishing e-mails hyperpersoonlijk en nauwelijks te onderscheiden van echte berichten. De keerzijde: AI wordt ook ingezet in training platforms om content te personaliseren en simulaties realistischer te maken.

ADAPTIVE LEARNING

Platforms passen de moeilijkheidsgraad en onderwerpen automatisch aan op basis van het gedrag van de individuele medewerker. Wie goed scoort op phishing simulaties krijgt geavanceerdere scenario's. Wie herhaaldelijk klikt krijgt extra basismodules. Dit verhoogt de effectiviteit zonder dat IT-beheerders handmatig moeten bijsturen.

GAMIFICATION ALS STANDAARD

Punten, badges, leaderboards en team-challenges worden steeds meer standaard in awareness platforms. Het verhoogt betrokkenheid en maakt training minder "verplicht" en meer "uitdagend". 86% van medewerkers staat positief tegenover awareness training wanneer gamification-elementen aanwezig zijn [4].

MICRO-LEARNINGS EN CONTINUOUS TRAINING

De shift van kwartaal- naar wekelijkse micro-learnings van 3--5 minuten zet door. 81% van organisaties vindt minimaal 3 uur training per medewerker per jaar nodig [4]. Korte, frequente sessies leveren aantoonbaar betere retentie dan lange, sporadische trainingen.

MARKTGROEI

De wereldwijde security awareness trainingsmarkt groeit van USD 5,77 miljard (2025) naar een verwachte USD 14,66 miljard in 2031 -- een jaarlijkse groei van 16,82% [18]. De groei wordt gedreven door NIS2-verplichtingen, toenemende AI-dreigingen en de verschuiving naar doorlopende programma's.

10. Aan de slag

Je weet nu wat security awareness training inhoudt, wat het kost en waarom het noodzakelijk is. De volgende stap: een programma kiezen dat past bij jouw organisatie.

IN VIJF STAPPEN NAAR EEN AWARENESS PROGRAMMA

1. **Baseline meting**

   Start met een phishing simulatie zonder waarschuwing. Meet het klikpercentage. Dit is je nulmeting en je belangrijkste argument richting management.

2. **Selectie en implementatie**

   Kies een platform op basis van de selectiecriteria in hoofdstuk 5. Opstarttijd bij SaaS-platforms: 1--5 werkdagen [13].

3. **Rollout en communicatie**

   Lanceer het programma met steun van management. Communiceer het doel: medewerkers beschermen, niet controleren. Vermijd een strafcultuur.

4. **Doorlopend programma**

   Combineer maandelijkse micro-learnings met kwartaal phishing simulaties. Plan een jaarlijkse verdiepingssessie over actuele dreigingen.

5. **Meten en bijsturen**

   Monitor phishing click rates, completion rates en incident reports. Rapporteer kwartaallijks aan management. Documenteer alles voor NIS2-compliance.

Bronnenlijst

[1] **KnowBe4 -- 2025 Phishing by Industry Benchmarking Report.** 67,7 miljoen simulaties bij 14,5 miljoen gebruikers. https://www.knowbe4.com/press/knowbe4-report-reveals-security-training-reduces-global-phishing-click-rates-by-86

[2] **MKB Servicedesk -- 1 op 5 ondernemers schade door cyberaanvallen (2024).** https://www.mkbservicedesk.nl/nieuws/ondernemersnieuws/1-op-de-5-ondernemers-had-in-2024-schade-door-cyberaanvallen

[3] **Hallo.eu -- Cybercriminaliteit kost MKB EUR 270.000 per incident.** https://hallo.eu/kennis/blogs/cybercriminaliteit-kost-mkb-euro-270-000-per-incident/

[4] **Fortinet -- 2024 Security Awareness and Training Report.** https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2024-security-awareness-and-training.pdf

[5] **CBS -- Cybersecuritymonitor 2024.** https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[6] **Digitale Overheid -- Cyberbeveiligingswet (NIS2).** https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[7] **Diverse onderzoeken -- Ebbinghaus vergeetcurve.** 80% van nieuwe kennis vergeten binnen 4 weken zonder herhaling.

[8] **Verizon -- Data Breach Investigations Report 2025.** ~60% van breaches betreft menselijke actie. https://www.verizon.com/business/resources/reports/dbir/

[9] **IBM -- Cost of a Data Breach Report 2024.** 26% van datalekken door menselijke fout, USD 3,62 miljoen gemiddeld. https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

[10] **Vodafone Business -- Driekwart MKB doelwit cybercrime.** https://www.vodafone.nl/zakelijk/inspiratie/mkb-doelwit-cybercrime-onderzoeken

[11] **Verzeker Cyber -- Gemiddelde kosten cyberaanval Nederland.** https://verzekercyber.nl/wat-zijn-de-gemiddelde-kosten-van-een-cyberaanval/

[12] **Vendr -- KnowBe4 Pricing.** Onderhandelde prijzen 22--55% onder lijstprijs. https://www.vendr.com/marketplace/knowbe4

[13] **StackAware -- Security Awareness Programma Opzetten.** https://www.stack-aware.com/security-awareness-programma-opzetten/

[14] **Brightside AI -- 8 Security Awareness Training Mistakes to Avoid in 2025.** https://www.brside.com/blog/8-security-awareness-training-mistakes-to-avoid-in-2025

[15] **CertificeringsAdvies Nederland -- NIS2 training eisen.** https://certificeringsadvies.nl/zo-voldoe-je-aan-de-eisen-nis2-training-voor-bestuur-cyberhygiene-en-bewustzijn-medewerkers-verhogen/

[16] **ISMS.online -- NIS2 Cyber Hygiene and Training.** https://www.isms.online/nis-2/requirements/cyber-hygiene-and-training/

[17] **Guardey -- Security Awareness Training Software.** https://www.guardey.com/security-awareness-training-software/

[18] **Mordor Intelligence -- Security Awareness Training Market.** CAGR 16,82%, USD 5,77 miljard (2025) naar USD 14,66 miljard (2031). https://www.mordorintelligence.com/industry-reports/security-awareness-training-market