GIDS

De complete gids voor phishing simulatie

Klikpercentages, kosten, programma-opzet, selectiecriteria, NIS2 en AI-trends. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Phishing is verantwoordelijk voor het merendeel van alle cyberincidenten. Simulatie brengt het risico meetbaar omlaag. Hieronder de feiten.

33% > 4%

Gemiddelde klikrate daalt van 33,1% naar 4,1% na 12 maanden simulatie

KnowBe4 Benchmarking Report 2024 [1]

276%

ROI van security awareness programma's met phishing simulatie

Osterman Research / Forrester [2]

EUR 10--80

Kosten per medewerker per jaar, afhankelijk van type en omvang

Vita Magazine / AmiPhished [3]

86%

van organisaties meldde in 2024 een AI-gestuurd phishing incident

SoSafe Human Risk Review 2024 [4]

+400%

Stijging QR-code phishing (quishing) in 2023--2024

ReliaQuest / Hoxhunt [5]

$14,8M

Gemiddelde jaarlijkse kosten van phishing per organisatie

Ponemon / IBM [6]

80%

van Nederlanders weet wat phishing is -- maar klikken toch

Opgelicht?! / Gartner [7]

NIS2

Art. 20(2): bestuurders verplicht tot cyberbeveiligingsopleiding voor personeel

NIS2-richtlijn Art. 20 [8]

1. Wat is phishing simulatie?

Phishing simulatie is het gecontroleerd versturen van nep-phishingmails naar je eigen medewerkers om te meten wie klikt, wie meldt en wie kwetsbaar is -- zonder dat er daadwerkelijk schade ontstaat.

Het doel is niet om medewerkers te "betrappen", maar om gedrag meetbaar te maken en gericht te verbeteren. Een simulatie bootst realistische aanvalsscenario's na -- van pakketbezorging-mails tot CEO-fraude -- zodat medewerkers leren herkennen wat echt is en wat niet [1].

SIMULATIE VS AWARENESS TRAINING

KENMERK	PHISHING SIMULATIE	AWARENESS TRAINING
Aanpak	Praktijktest: nep-phishing versturen	Theorie: e-learning, video's, quizzes
Wat het meet	Daadwerkelijk gedrag (klikken, melden)	Kennis (scores op toetsen)
Feedback	Direct: landingspagina na klik	Uitgesteld: na afronding module
Frequentie	Maandelijks tot wekelijks	Kwartaal tot jaarlijks
Emotionele impact	Hoog -- "ik had geklikt"	Laag -- passief consumeren
Geschikt als standalone	Nee -- combineer met training	Nee -- zonder praktijk beklijft het niet

> **De combinatie werkt**
>
> Organisaties die simulatie combineren met awareness training zien de sterkste gedragsverandering. Kennis zonder praktijk beklijft niet; praktijk zonder uitleg frustreert. De meeste platforms bieden beide als geintegreerde oplossing [9].

2. Waarom werkt het?

Phishing simulatie werkt omdat het gedrag verandert -- niet alleen kennis. De data zijn overtuigend.

DE BENCHMARK: 33% NAAR 4%

Het meest geciteerde onderzoek naar phishing simulatie is het jaarlijkse benchmarking rapport gebaseerd op data van miljoenen gebruikers wereldwijd. De conclusie over 2024: organisaties die starten met simulatie hebben een gemiddelde klikrate van 33,1%. Na 90 dagen daalt dit naar 18,9%. Na 12 maanden naar 4,1% [1].

Deze daling is consistent over sectoren, regio's en bedrijfsgroottes. De verklaring: herhaalde blootstelling aan realistische scenario's bouwt een automatische herkenningsreflex op -- vergelijkbaar met hoe brandoefeningen werken.

CASE: ZIEKENHUIS 28% NAAR 4%

Een Nederlands ziekenhuis startte met een klikrate van 28% bij de eerste simulatie. Na 12 maanden maandelijkse simulaties met varierende scenario's (pakketbezorging, IT-helpdesk, HR-documenten) daalde de klikrate naar 4%. Het meldingspercentage steeg van 12% naar 67% [10].

NEDERLANDSE BENCHMARKDATA

SECTOR	STARTPERCENTAGE	NA 12 MAANDEN
Gezondheidszorg	28--35%	3--6%
Financiele dienstverlening	20--28%	2--5%
Overheid	25--32%	4--7%
Technologie	15--22%	2--4%
Onderwijs	30--40%	5--8%
MKB (gemiddeld)	25--35%	4--7%

ROI: 276%

Onderzoek berekent de ROI van security awareness met phishing simulatie op 276% over drie jaar [2]. De berekening: lagere incidentkosten, minder downtime, minder forensisch onderzoek en minder reputatieschade. Bij een gemiddelde phishing-schade van $14,8 miljoen per organisatie per jaar [6] is een investering van EUR 10--80 per medewerker verwaarloosbaar.

GEDRAGSVERANDERING IN DRIE FASES

- **Fase 1 (maand 1--3)** -- Bewustwording: medewerkers ontdekken dat ze kwetsbaar zijn. Klikrate daalt van ~33% naar ~19%
- **Fase 2 (maand 3--6)** -- Herkenning: patronen worden herkend. Medewerkers beginnen actief te melden
- **Fase 3 (maand 6--12)** -- Reflex: herkenning wordt automatisch. Klikrate stabiliseert rond 4--5%, meldingspercentage stijgt boven 60%

3. Hoe werkt het?

Een phishing simulatieprogramma opzetten vergt meer dan alleen nep-mails versturen. Hieronder het volledige proces.

PROGRAMMA OPZETTEN IN 5 STAPPEN

1 **Baseline meting**

WEEK 1--2

Verstuur een eerste simulatie zonder vooraankondiging. Meet de klikrate, rapporteerrate en wie credentials invoert. Dit is je nulmeting.

2 **Awareness kickoff**

WEEK 3--4

Communiceer de resultaten (geanonimiseerd) en start een basistraining. Leg uit waarom het programma bestaat en wat medewerkers kunnen verwachten.

3 **Doorlopende simulaties**

MAANDELIJKS

Verstuur maandelijks 1--2 simulaties met varierende scenario's. Wissel af tussen urgentie-mails, CEO-fraude, pakketbezorging, IT-support en seizoensgebonden thema's.

4 **Gerichte opvolging**

NA ELKE SIMULATIE

Medewerkers die klikken krijgen direct een educatieve landingspagina. Herhaalde klikkers krijgen extra training. Melders krijgen positieve bevestiging.

5 **Meten en rapporteren**

KWARTAAL

Rapporteer kwartaalcijfers aan management: klikrate, meldingspercentage, trend per afdeling. Stuur bij op basis van data.

FREQUENTIE

Onderzoek toont dat maandelijkse simulaties het optimum zijn. Wekelijks leidt tot "simulatie-moeheid"; kwartaal is te weinig om gedrag te veranderen. Bij maandelijkse cadans daalt de klikrate het snelst en blijft de alertheid hoog [1].

SCENARIO-VARIATIE

Gebruik minimaal 8--12 verschillende scenario's per jaar. Varieer in:

- **Type** -- urgentie, autoriteit, nieuwsgierigheid, angst, beloning
- **Kanaal** -- e-mail, SMS (smishing), QR-codes (quishing), voicemail (vishing)
- **Moeilijkheidsgraad** -- van duidelijk nep tot geavanceerd spear phishing
- **Seizoen** -- Black Friday, kerst, belastingaangifte, vakantieplanning

KPI'S

KPI	DOEL NA 12 MAANDEN	WAAROM BELANGRIJK
Klikrate	< 5%	Meet kwetsbaarheid -- hoeveel medewerkers trappen erin
Meldingspercentage	> 60%	Meet actieve verdediging -- hoeveel medewerkers melden verdachte mails
Credential invoer	< 1%	Meet ernstigste risico -- wie voert daadwerkelijk wachtwoorden in
Tijd tot melding	< 5 minuten	Meet reactiesnelheid -- hoe snel wordt een aanval gesignaleerd

TIP

Meet het meldingspercentage naast de klikrate. Een klikrate van 5% met een meldingspercentage van 70% is beter dan een klikrate van 3% met een meldingspercentage van 10%. Melden is actieve verdediging.

4. Wat kost het?

De kosten van phishing simulatie varieren van EUR 5 per medewerker voor een eenmalige test tot EUR 80 per medewerker per jaar voor een volledig managed programma.

KOSTEN PER MEDEWERKER

CATEGORIE	PRIJS PER MEDEWERKER/JAAR	WAT JE KRIJGT
Eenmalige test	EUR 5--15	Baseline meting, beperkte rapportage, geen opvolging
Doorlopend basis	EUR 10--25	Maandelijkse simulaties, standaard templates, basisrapportage
SaaS selfservice	EUR 15--40	Onbeperkte simulaties, template bibliotheek, dashboards, meldknop
Managed service	EUR 30--60	Volledig beheerde campagnes, spear phishing, uitgebreide rapportage
Enterprise (simulatie + training)	EUR 40--80	Geintegreerd awareness + simulatie, AI-gestuurd, compliance rapportage

JAARKOSTEN PER ORGANISATIEGROOTTE

ORGANISATIEGROOTTE	BASIS (EUR/JAAR)	MIDDENWEG (EUR/JAAR)	MANAGED (EUR/JAAR)
10--25 medewerkers	250--625	500--1.000	750--1.500
25--50 medewerkers	500--1.250	1.000--2.000	1.500--3.000
50--100 medewerkers	1.000--2.500	2.000--4.000	3.000--6.000
100--250 medewerkers	2.500--6.250	4.000--10.000	7.500--15.000
250--500 medewerkers	5.000--12.500	7.500--20.000	12.000--30.000

ROI-berekening

Een organisatie met 50 medewerkers investeert EUR 2.000/jaar in phishing simulatie. Gemiddelde schade per phishing incident: EUR 270.000 [11]. Als simulatie de kans op een incident met 50% verlaagt (conservatief bij een daling van 33% naar 4% klikrate), is de besparing EUR 135.000 in verwachte schade per jaar. ROI: 6.650%.

5. Waar moet je op letten?

Niet elke phishing simulatie-oplossing is gelijk. Deze selectiecriteria helpen je de juiste keuze te maken.

SELECTIECRITERIA

CRITERIUM	WAAROM BELANGRIJK
AI-gestuurde scenario's vs vaste templates	AI past scenario's aan op basis van functie, afdeling en eerder gedrag. Templates zijn voorspelbaar en verliezen na een paar rondes hun effectiviteit [12]
Nederlandse taalondersteuning	Simulaties in het Nederlands zijn realistischer voor NL-organisaties. Engelse phishing wordt sneller herkend als nep
Gamification	Leaderboards, badges en scores verhogen betrokkenheid. Medewerkers die "scoren" blijven alerter [13]
AVG/EU-hosting	Persoonsgegevens (wie klikt, wie niet) moeten binnen de EU worden verwerkt. DPIA is verplicht
SOC-integratie	Koppeling met je Security Operations Center zodat gemelde phishing direct wordt geanalyseerd
Rapportage en dashboards	Management wil trends zien. Afdelingshoofden willen hun team-scores. IT wil de risicogroepen kennen
Meldknop (report button)	Een-klik meldknop in Outlook/Gmail verlaagt de drempel om te melden en verhoogt het meldingspercentage
Multi-channel	Niet alleen e-mail, maar ook SMS (smishing), QR-codes (quishing) en voicemail (vishing)
Automatische opvolging	Klikkers krijgen direct een educatieve landingspagina en extra training -- zonder handmatige actie
NIS2-compliance rapportage	Bewijs dat je aan Art. 20(2) voldoet: documentatie van training en simulatieresultaten

10 VRAGEN AAN JE LEVERANCIER

1. Worden scenario's AI-gestuurd of gebruik je vaste templates?

2. Ondersteunen jullie Nederlandse en meertalige scenario's?
3. Waar worden mijn data gehost -- EU of daarbuiten?
4. Bieden jullie een meldknop voor Outlook en Gmail?
5. Hoe werkt de automatische opvolging na een klik?
6. Ondersteunen jullie multi-channel simulaties (SMS, QR, voice)?
7. Welke rapportages zijn beschikbaar voor management en CISO?
8. Hoe integreren jullie met onze bestaande security tooling?
9. Bieden jullie NIS2-compliance documentatie?
10. Wat is de minimale contractduur en hoe werkt opschalen?

> **LET OP: AVG EN DPIA**
>
> Phishing simulatie verwerkt persoonsgegevens (wie klikt, wie niet). Je bent verplicht een DPIA (Data Protection Impact Assessment) uit te voeren. Communiceer vooraf aan de OR en medewerkers dat er gesimuleerd wordt -- niet wanneer, maar dat het gebeurt [14].

6. Veelgemaakte fouten

Deze acht valkuilen ondermijnen de effectiviteit van je phishing simulatieprogramma.

1. Naming & shaming

Medewerkers publiekelijk aanspreken op klikgedrag creert angst, niet alertheid. Het resultaat: medewerkers melden verdachte mails niet meer uit angst voor negatieve gevolgen. Houd resultaten geanonimiseerd op teamniveau. Individuele opvolging gebeurt via extra training, niet via schaamte [15].

2. Eenmalige simulatie

Een enkele phishing test is een momentopname, geen programma. Gedragsverandering vereist herhaalde blootstelling over minimaal 12 maanden. Organisaties die stoppen na een baseline meting zien hun klikrate binnen 3 maanden terugkeren naar het oorspronkelijke niveau [1].

3. Management uitsluiten

C-level en directie worden vaker het doelwit van spear phishing en CEO-fraude. Als management niet meedoet aan simulaties, mist de organisatie het grootste risico. Bovendien ondermijnt het de geloofwaardigheid van het programma: "als het voor de directie niet hoeft, waarom dan voor ons?" [16].

4. Geen opvolging na klik

Een medewerker klikt op een simulatie en er gebeurt niets. Geen uitleg, geen training, geen feedback. De leerkans is verloren. Implementeer altijd een educatieve landingspagina die direct na de klik uitlegt wat er fout ging en hoe je het de volgende keer herkent.

5. Alleen e-mail simuleren

Phishing beperkt zich niet meer tot e-mail. QR-code phishing (quishing) steeg met 400% [5]. SMS-phishing (smishing) en voice phishing (vishing) nemen toe. Een programma dat alleen e-mail simuleert, traint medewerkers voor gisteren, niet voor morgen.

6. AVG/DPIA vergeten

Phishing simulatie registreert wie klikt en wie niet -- dat zijn persoonsgegevens. Zonder DPIA en zonder voorafgaande communicatie aan medewerkers en OR riskeer je een AVG-klacht. Informeer medewerkers dat simulaties worden uitgevoerd (niet wanneer) en voer een DPIA uit [14].

7. Meldingspercentage niet meten

De meeste organisaties focussen alleen op klikrate. Maar het meldingspercentage is minstens zo belangrijk: het meet hoeveel medewerkers actief verdachte mails rapporteren. Een hoog meldingspercentage betekent dat je organisatie een menselijke firewall heeft -- medewerkers die aanvallen signaleren voordat ze schade aanrichten.

8. Te weinig variatie

Drie keer dezelfde "pakketbezorging"-mail versturen traint medewerkers om een specifiek sjabloon te herkennen, niet om phishing in het algemeen te herkennen. Varieer in type trigger (urgentie, nieuwsgierigheid, autoriteit), kanaal, afzender en moeilijkheidsgraad. Gebruik minimaal 8--12 unieke scenario's per jaar [12].

7. Compliance: NIS2

De Cyberbeveiligingswet (NIS2-implementatie) maakt security awareness en training wettelijk verplicht voor ~10.000 Nederlandse organisaties.

ART. 20(2): BESTUURDERS VERPLICHT

NIS2 Artikel 20, lid 2 stelt dat leden van het bestuur van essentiele en belangrijke entiteiten verplicht zijn om een opleiding te volgen en dat zij vergelijkbare opleidingen op regelmatige basis aan hun personeel aanbieden. Phishing simulatie is de meest directe invulling van deze verplichting: het traint medewerkers actief in het herkennen van cyberdreigingen [8].

ART. 21(2)(G): BASISHYGIENE

Artikel 21, lid 2, sub g verplicht organisaties tot "basispraktijken op het gebied van cyberhygiene en opleiding op het gebied van cyberbeveiliging". Phishing simulatie valt hier direct onder als meetbare basishygiene-maatregel [8].

CADANS EN DOCUMENTATIE

NIS2-EIS	INVULLING MET PHISHING SIMULATIE	AANBEVOLEN CADANS
Bestuurdersopleiding (Art. 20.2)	Directie neemt deel aan simulaties	Kwartaal
Personeelsopleiding (Art. 20.2)	Alle medewerkers in simulatieprogramma	Maandelijks
Basishygiene (Art. 21.2.g)	Klikrate en meldingspercentage als KPI	Maandelijks meten, kwartaal rapporteren
Aantoonbaarheid	Dashboard met historische data en trends	Continu bijhouden
Evaluatie	Jaarlijkse review van programma-effectiviteit	Jaarlijks

TIP

Bewaar alle simulatieresultaten minimaal 3 jaar. Bij een NIS2-audit moet je kunnen aantonen dat je structureel investeert in security awareness. Een dashboard met 12+ maanden trenddata is het sterkste bewijs.

8. Verschil met verwante oplossingen

Phishing simulatie overlapt met awareness training en social engineering assessments. Hieronder de afbakening.

KENMERK	PHISHING SIMULATIE	AWARENESS TRAINING	RED TEAM SOCIAL ENGINEERING
Doel	Gedrag meten en verbeteren	Kennis overdragen	Beveiligingsniveau testen
Aanpak	Geautomatiseerde nep-phishing naar alle medewerkers	E-learning modules, video's, quizzes	Handmatige aanval door specialisten
Scope	Hele organisatie, doorlopend	Hele organisatie, periodiek	Gericht op specifieke doelwitten
Frequentie	Maandelijks	Kwartaal tot jaarlijks	Jaarlijks
Output	Klikrate, meldrate, trend per afdeling	Voltooiingspercentage, kennisscore	Rapport met bevindingen en aanbevelingen
Kosten MKB	EUR 10--40/medewerker/jaar	EUR 5--25/medewerker/jaar	EUR 5.000--25.000 per assessment
Geschikt voor	Doorlopende gedragsverandering	Kennisbasis opbouwen	Eenmalige toetsing van weerbaarheid

Wanneer wat inzetten?

Start met awareness training als basis. Voeg phishing simulatie toe voor meetbare gedragsverandering. Overweeg red team social engineering als je wilt weten hoe weerbaar je organisatie is tegen een gerichte aanval. De drie vullen elkaar aan -- het is geen of-of keuze.

9. Trends

Vier ontwikkelingen die phishing simulatie de komende jaren veranderen.

1. AI-gestuurde phishing -- 86% incident

86% van organisaties meldde in 2024 een AI-gestuurd phishing incident [4]. Generatieve AI maakt phishingmails foutloos, gepersonaliseerd en in perfect Nederlands. De traditionele herkenningspunten (spelfouten, vreemde afzender) verdwijnen. Simulatieprogramma's moeten mee-evolueren: AI-gegenereerde scenario's zijn noodzakelijk om medewerkers te trainen tegen AI-gegenereerde aanvallen [17].

2. QR-code phishing (quishing) -- +400%

Quishing steeg met 400% in 2023--2024 [5]. QR-codes omzeilen traditionele e-mail security filters omdat de URL verborgen zit in een afbeelding. Aanvallers plaatsen kwaadaardige QR-codes in parkeergarages, op posters en in e-mails. Simulatieprogramma's die alleen tekst-links testen, missen dit groeiende aanvalsvector.

3. Deepfake vishing -- +1.600%

Voice phishing met deepfake audio steeg met 1.600% [18]. Aanvallers klonen de stem van een CEO of CFO en bellen medewerkers met urgente betalingsverzoeken. Multi-channel simulatie -- inclusief voice en video -- wordt de nieuwe standaard voor security awareness programma's.

4. Multi-channel aanpak

De grens tussen e-mail phishing, smishing, vishing en quishing vervaagt. Aanvallers combineren kanalen: een e-mail met een QR-code die leidt naar een nep-inlogpagina, gevolgd door een bevestigingstelefoontje. Effectieve simulatieprogramma's trainen medewerkers op alle kanalen, niet alleen e-mail [19].

WAT BETEKENT DIT VOOR JOU?

AI maakt phishing beter; simulatie moet meegroeien. Een programma dat alleen standaard e-mail templates verstuurt, traint medewerkers voor de aanvallen van twee jaar geleden. Kies een oplossing die AI-scenario's, multi-channel en adaptieve moeilijkheidsgraden ondersteunt.

10. Aan de slag

Je weet nu wat phishing simulatie is, wat het kost, hoe je het opzet en waar je op moet letten. Tijd om te handelen.

DRIE STAPPEN OM TE STARTEN

1 Bepaal je situatie

Hoeveel medewerkers heb je? Heb je al awareness training? Is er een meldknop voor phishing? Ken je je huidige klikrate? Als je deze vragen niet kunt beantwoorden, begin dan met een baseline meting.

2 Vergelijk oplossingen

Gebruik de 10 vragen uit hoofdstuk 5 om minimaal 3 aanbieders te vergelijken. Let op Nederlandse taalondersteuning, EU-hosting, multi-channel en NIS2-rapportage.

3 Start klein, schaal op

Begin met maandelijkse e-mail simulaties voor de hele organisatie. Voeg na 3 maanden multi-channel toe. Bouw naar een volledig awareness programma met simulatie, training en rapportage.

DIRECT AAN DE SLAG?

Word vrijblijvend gematcht met phishing simulatie aanbieders die passen bij jouw sector, omvang en budget.

ibgids.nl/word-gematcht

Of neem contact op via info@ibgids.nl

Bronnenlijst

[1] **KnowBe4** -- Phishing by Industry Benchmarking Report 2024. knowbe4.com/phishing-benchmarking-report

[2] **Osterman Research / Forrester** -- ROI of Security Awareness Training: 276% over drie jaar. ostermanresearch.com/reports/roi-of-security-awareness-training

[3] **Vita Magazine** -- Phishing awareness training 2026: kosten en vergelijking. vita-magazine.nl/phishing-awareness-training/

[4] **SoSafe** -- Human Risk Review 2024: 86% AI-phishing incident. sosafe-awareness.com/resources/reports/human-risk-review/

[5] **ReliaQuest / Hoxhunt** -- QR-code phishing (quishing) stijging 400% in 2023--2024. reliaquest.com/blog/qr-code-phishing-quishing/

[6] **Ponemon Institute / IBM** -- Cost of Phishing Study: $14,8M gemiddelde jaarlijkse kosten. ibm.com/reports/cost-of-a-data-breach

[7] **Opgelicht?! / AVROTROS** -- 80% van Nederlanders weet wat phishing is. opgelicht.avrotros.nl/alerts/phishing/

[8] **NIS2-richtlijn** -- Art. 20(2) en Art. 21(2)(g): verplichting bestuurders en personeel. eur-lex.europa.eu/eli/dir/2022/2555/oj

[9] **Emerce** -- Vergelijking security awareness platforms 2025. emerce.nl/best-practices/vergelijking-security-awareness-platforms

[10] **SIDN** -- Phishing in Nederland: cijfers en trends. sidn.nl/nieuws-en-blogs/phishing-in-nederland

[11] **Verzekercyber.nl** -- Gemiddelde schade MKB per cyberincident: EUR 270K. verzekercyber.nl/wat-kost-een-cyberverzekering/

[12] **Gartner** -- Market Guide for Security Awareness Computer-Based Training 2024. gartner.com/reviews/market/security-awareness-training

[13] **Hoxhunt** -- Gamification in Security Awareness: impact op engagement. hoxhunt.com/blog/gamification-security-awareness/

[14] **Autoriteit Persoonsgegevens** -- DPIA verplicht bij verwerking persoonsgegevens met hoog risico. autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia

[15] **SANS Institute** -- Security Awareness Report 2024: naming & shaming ondermijnt programma. sans.org/security-awareness-training/reports/

[16] **NCSC** -- Basishygiene voor cyberbeveiliging: management betrokkenheid. ncsc.nl/onderwerpen/basismaatregelen

[17] **Darktrace** -- AI-generated phishing: de volgende generatie aanvallen. darktrace.com/blog/ai-generated-phishing

[18] **CrowdStrike** -- Global Threat Report 2025: vishing +1.600%. crowdstrike.com/global-threat-report/

[19] **Proofpoint** -- State of the Phish 2025: multi-channel aanpak. proofpoint.com/us/resources/threat-reports/state-of-phish

[20] **CBS** -- Cybersecuritymonitor 2024: MFA-gebruik en incidentcijfers. cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

[21] **Digital Trust Center** -- Phishing: herken en voorkom het. digitaltrustcenter.nl/informatie-advies/phishing

[22] **AmiPhished** -- Transparante tarieven phishing simulatie 2025. amiphished.nl/prijzen/

Deze gids is samengesteld door IBgids.nl op basis van openbare bronnen en marktonderzoek. Alle genoemde prijzen zijn indicatief (peildatum: maart 2026). IBgids.nl is een onafhankelijk platform en geen leverancier of adviseur.