Phishing simulatie

Wat doet jouw medewerker als er een nep-e-mail binnenkomt?

DOCUMENT
Phishing simulatie

DATUM
Juni 2026

CLASSIFICATIE
Openbaar

VERSIE
V1.1 - Definitief

WAT DOET JOUW MEDEWERKER ALS ER EEN NEP-E-MAIL BINNENKOMT?

Eén nep-e-mail is genoeg. Een aanvaller stuurt een bericht dat lijkt te komen van Microsoft, een pakketdienst of een collega. Het doel: iemand laten klikken of inloggegevens laten invullen.

Onderzoek over 11,9 miljoen medewerkers in 57.000 organisaties laat zien dat 34% klikt op een nep e-mail wanneer zij geen training hebben gehad (bron: KnowBe4 Phishing Benchmarking Report 2024).

Met een phishing-simulatie testen we hoe jouw medewerkers reageren op nep e-mails. Zo zie je precies waar het risico zit en wat er beter kan. Na een jaar regelmatige simulaties en training daalt het percentage dat klikt naar 4,6% (zelfde bron).

Wat levert het jouw organisatie op

Phishing-simulaties maken de kwetsbaarheid van jouw organisatie zichtbaar en helpen die te verkleinen. Je krijgt:

- Inzicht in hoe vatbaar jouw organisatie is voor oplichting via e-mail.
- Medewerkers die nep-e-mails sneller herkennen en melden.
- Minder kans dat een aanvaller via een medewerker binnenkomt.

Wat zit erin

We voeren 2 tot 3 phishing-simulaties per jaar uit. Medewerkers ontvangen realistische nep-e-mails die lijken op veelvoorkomende aanvallen, zoals:

- Een melding van Microsoft over een wachtwoord of account.
- Een pakketbezorgingsbericht.
- Een factuur van een leverancier.

De simulaties zijn volledig veilig. Er worden geen echte gegevens verzameld of opgeslagen. Het doel is niet om medewerkers te betrappen, maar om medewerkers te leren herkennen.

Zo werkt een simulatie

Elke phishing-simulatie doorloopt drie vaste stappen. Na afloop ontvang je een helder rapport.

STAP 1

Voorbereiding

We stemmen de scenario's af en zorgen dat de testmails niet worden geblokkeerd. Daarna sturen we een realistische nep-e-mail naar jouw medewerkers.

STAP 2

Meting

We meten hoe medewerkers reageren: hoeveel openden de mail, hoeveel klikten op een link en hoeveel meldden het als verdacht.

STAP 3

Rapportage

Je ontvangt een helder overzicht met resultaten en trends per simulatie. Zo zie je hoe het bewustzijn zich ontwikkelt en waar extra aandacht nodig is.

Rapportage en inzicht

Na elke simulatie ontvang je een overzicht van de resultaten: hoeveel medewerkers de nep-e-mail openden, hoeveel op een link klikten en hoeveel de mail als verdacht meldden. Deze cijfers laten zien hoe het bewustzijn zich ontwikkelt over tijd. Zo kun je gericht bijsturen met extra training of een gerichte aanpak voor teams die meer aandacht nodig hebben.

Wat wij afspreken

Een paar dingen vragen wij van jou.

- Een actuele lijst van e-mailadressen van deelnemende medewerkers.
- Aangeven welke medewerkers of afdelingen deelnemen aan de simulaties.

Wat wij niet doen

Individuele medewerker-resultaten

Onze phishing-simulaties meten gedrag op organisatieniveau. Individuele resultaten per medewerker delen we niet buiten de direct leidinggevende.

Security awareness training

Security awareness training maakt geen onderdeel uit van deze dienst, maar is eenvoudig te combineren. Zie hieronder.

Wat het kost

De prijs voor Phishing Simulatie staat in de bijbehorende offerte, per medewerker per jaar of als jaarbundel. Bij combinatie met Security Awareness Training geldt een pakketkorting; de hoogte staat in de offerte.

Combineer met security awareness training

Een simulatie laat zien hoe medewerkers reageren. Training leert hun wat ze moeten doen. Simulatie meet, training leert. Combineer phishing-simulaties met onze Online Security Awareness Training en ontvang een pakketkorting.

CONTRACTUELE BASIS

Op deze dienst zijn de **Hoofdovereenkomst, Algemene Voorwaarden en Service Level Agreement (SLA)** van Dynamic ICT van toepassing. Voor deze dienst geldt **SLA B.**

Standaard looptijd is **12 maanden.** Daarna loopt de overeenkomst door voor onbepaalde tijd, met **1 maand opzegtermijn.** Opzeggen doe je schriftelijk via **INFO@DYNAMICICT.NL.**