



TT3P Phishing Simulatie

**Maak van elke medewerker  
een cybersecurity-expert**



## Bescherm uw organisatie

**Stelt u zich eens voor dat uw eigen medewerkers de eerste verdedigingslinie zijn tegen cyberaanvallen. Met TT3P's Phishing Simulatie-dienst transformeren we deze visie in realiteit.**

Phishing is de bekendste vorm van cybercriminaliteit, waarbij criminelen een e-mail naar uw medewerkers versturen om te proberen inloggegevens, financiële informatie, pincodes of andere persoonlijke gegevens te achterhalen. Phishing ligt in meer dan 90% van de gevallen aan de basis van cyberaanvallen.

Wij bieden een effectieve phishing simulatie, waarbij gebruik wordt gemaakt van namaakdomeinen en simulaties om uw team te testen en te trainen in het herkennen van verdachte e-mails.

Onze aanpak omvat niet alleen het testen, maar ook het bieden van directe educatieve feedback, door middel van interactieve quizen en concrete tips. Hierdoor zijn uw medewerkers beter voorbereid op echte phishing pogingen.

Dit alles wordt ondersteund door onze slimme technologie en expertise, waardoor uw organisatie niet alleen wordt getest, maar ook wordt versterkt tegen de steeds veranderende dreigingen van cyberaanvallen. Kies voor TT3P's Phishing Simulatie en maak van uw medewerkers een ondoordringbare muur tegen phishing.

### Wat is onze Phishing Simulatie?

Het is van cruciaal belang om goed voorbereid te zijn op cyberaanvallen. Phishing simulaties zijn hierbij een essentiële stap. Maar wat is onze Phishing Simulatie precies? Deze bestaat uit:

- Meerdere realistische phishing tests
- Een interactieve cybersecurity training
- Analyses en rapportages
- Aanpasbare phishing simulatie programma's

Door te kiezen voor TT3P's Phishing Simulatie, investeert u in de cybersecurity van uw organisatie en vermindert u het risico op datalekken en cyberaanvallen. Onze dienst is ontworpen om een cultuur van cybersecurity bewustzijn en waakzaamheid te creëren, waardoor uw medewerkers de eerste en sterkste verdedigingslinie worden tegen phishing-aanvallen.

## Hoe gaan we te werk?

De uitvoering van de Phishing Simulatie wordt gedaan met behulp van Metasploit Pro en een set van eigen gekochte domeinen. We voeren de volgende stappen uit:

- Testing: gebruik van namaakdomeinen
- Whitelisting: voorbereiding en testen van de simulatie
- Email Spoofing Controle: nagaan of er e-mails verzonden kunnen worden namens u vanuit uw eigen organisatie of vanuit derde partijen en leveranciers
- Uitvoering van simulatie: simulatie gericht op alle medewerkers met realistisch nagemaakte e-mails en inlogpagina's
- Registratie: we houden de resultaten per medewerker bij
- Quiz en educatie: we bieden een quiz na de simulatie die elementen herhaalt, met antwoorden die concrete tips geven om phishing beter te herkennen
- Optionele diensten: we bieden de mogelijkheid tot periodieke of geautomatiseerde uitvoering van de simulatie in verschillende vormen

**Neem vandaag nog contact op en zet de eerste stap naar een veiligere toekomst met onze Phishing Simulatie-dienst.**

Wilt u meer informatie,  
we staan u graag te woord.

