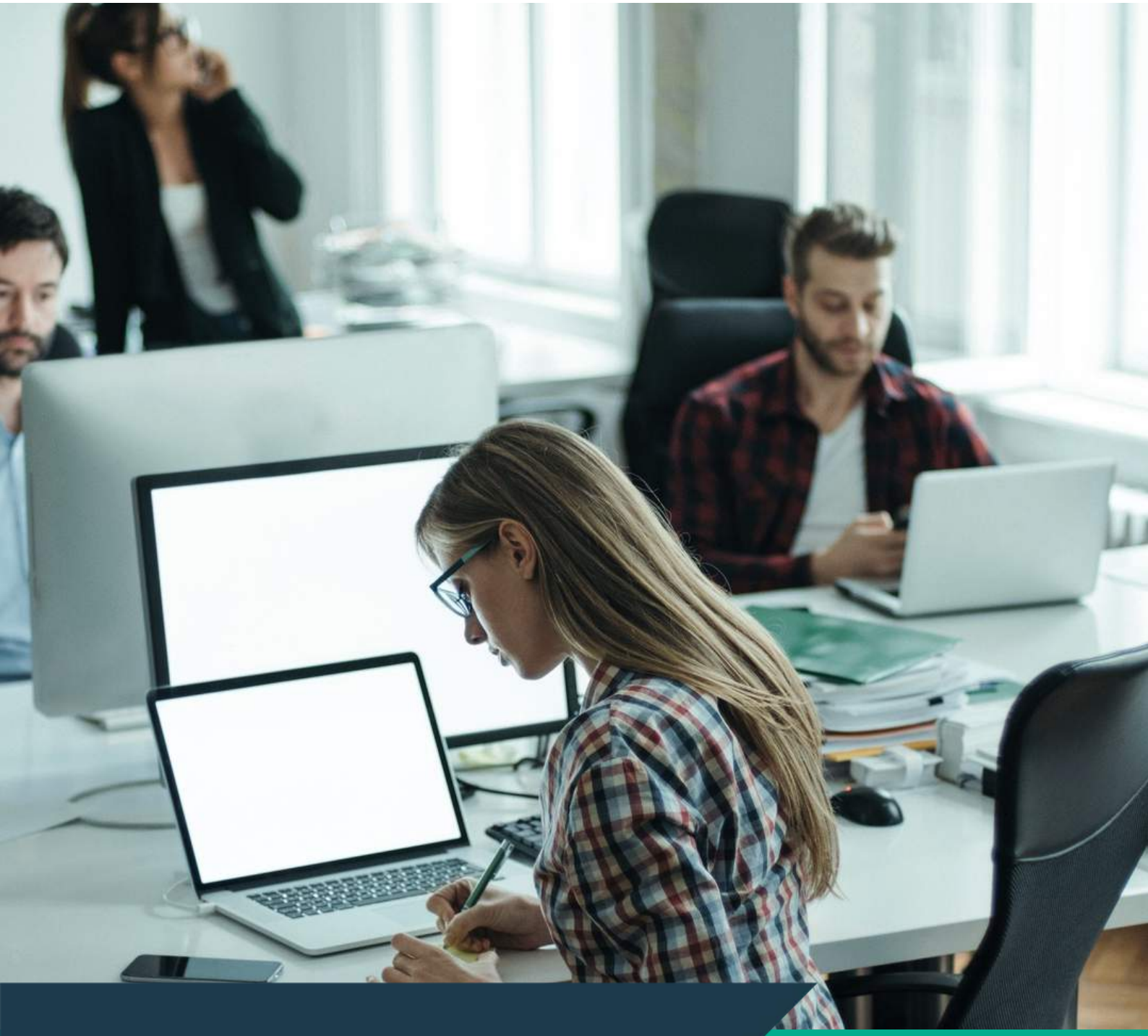
The Trusted Third Party



TT3P Phishing Simulatie

Cyberbewustzijn onderhouden is een continu proces.

Hoe gaan uw medewerkers om met phishing mails?

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

De Phishing Simulatie van TT3P bootst een aanval middels een phishing e-mail na. In de simulatie wordt getest of medewerkers in staat zijn om phishing e-mails te herkennen en of ze adequaat handelen na het ontvangen van een dergelijke phishing e-mail.

"91% van alle cyberaanvallen start met phishing" - Gartner

Praktisch

Medewerkers leren phishing e-mails herkennen en blijven daar-door alert. Dat is precies wat u wilt en het is hoognodig met alle cyberdreigingen van nu. Uw organisatie krijgt een goed beeld van welke medewerkers scherp zijn en wie er mogelijk extra training nodig hebben. Door medewerkers regelmatig te testen en te trainen verkleint uw organisatie de kans dat ze slachtoffer wordt van een ransomware-aanval.

Waarom een phishing simulatie uitvoeren?

- ☑ Cyberrisico's verkleinen;
- ☑ Cyberbewust worden;
- ☑ Meten en sturen op cyberbewustzijn.

Uit het Phishing Benchmark Global Report van Terranova Security in samenwerking met Microsoft blijkt dat uit 1.000.000 phishing simulatie e-mails 19,8% van de participanten op een phishing link heeft geklikt, 14,4% van het totale aantal participanten heeft zelfs een document gedownload van de simulatie webpagina.

Terranova Security en Microsoft, 2021

The Trusted Third Party

Hoe gaan we te werk?

Om tot een zo effectief mogelijke training te komen gaan we stapsgewijs te werk. Zo haalt uw organisatie het meeste rendement uit onze Phishing Simulatie:

- ☑ Stap 1: Wij stemmen met u af of we een standaard phishing template gebruiken (van bijvoorbeeld een bank of Microsoft) of dat we een maatwerk phishing template maken;
- ☑ Stap 2: Natuurlijk stellen we onze contactpersoon binnen uw ogranisatie op de hoogte van de simulate. Daarna versturen wij de phishing mail en registreren we de resultaten;
- ☑ Stap3: U ontvangt een gedetailleerde rapportage met de resultaten. In een persoonlijke sessie bespreken we de resultaten en geven we onze aanbevelingen.

Deskundige informatiebeveiliging

TT3P biedt onafhankelijke analyse en praktisch advies op het gebied van cybersecurity, waarmee voor elk type organisatie het risico op gijzeling van bedrijfssystemen, bedrijfsgegevens en het onrechtmatig toegang verkrijgen tot data door onbevoegde derden aanmerkelijk kan worden verkleind.

Cyberveiligheid begint bij alerte medewerkers!

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

Hofplein 20 | 3022 AC Rotterdam | 088 38 38 38 3 | info@tt3p.nl | www.tt3p.nl