

PHISHING SIMULATIE

MAAK VAN DE ZWAKSTE SCHAKEL DE VOORHOEDE VAN JE VERDEDIGING.

Met onze Phishing simulatie kunnen bedrijven een completer beeld geven van de beveiligingsstatus en potentiële risico's van een bedrijf, zodat de medewerkers die misschien de zwakste schakel waren, de sterkste beschermingspunt kunnen worden.

PHISHING SIMULATIE & BEVEILIGINGSBEWUSTZIJNSTRAINING

Regelmatige en actuele cyberbeveiligingstesten en -training voor medewerkers zijn essentieel in de steeds gevaarlijker wordende online dreigingsomgeving van vandaag. Onze Phishing simulatie biedt gesimuleerde phishing-aanvallen en campagnes voor beveiligingsbewustzijnstraining om medewerkers op te leiden, waardoor zij de beste verdediging tegen cybercriminaliteit worden.

**60% VAN DE BEVEILIGINGSINBREUKEN
WORDT VEROORZAAKT DOOR
ONOPZETTELIJKE MENSELIJKE FOUTEN.**

TRAIN EN TEST MEDEWERKERS

Getrainde en bewuste medewerkers staan aan de frontlinie van de beveiliging van een organisatie. Een effectief intern programma voor beveiligingsbewustzijn versterkt alleen maar de verdedigingsstrategie.

Beveiligingsbewustzijnstraining en phishing-simulaties gaan hand in hand. Phishing is zeer geavanceerd en bijna ondetecteerbaar geworden, aangezien criminelen manieren hebben gevonden om hun e-mails zo realistisch mogelijk te maken. Phishing-simulaties testen medewerkers op hun reactie op een echte phishing-aanval. Je kunt bijhouden welke medewerkers op de phishing-e-mail hebben geklikt, wie hun wachtwoord heeft prijsgegeven, wie een bijlage heeft geopend en wie de e-mail heeft genegeerd.

VISUALISEER HET GROTERE GEHEEL

Met onze Phishing simulatie heb je een uitgebreid platform waarmee je kunt ontdekken waar het gedrag en de blootstelling van de werknemers wijzen op een behoefte aan training. Zodra er een blootstelling is gedetecteerd, worden boeiende educatieve video's geleverd aan de meest kwetsbare gebruikers. Gesimuleerde phishing-tests vullen de video-gebaseerde training aan, met volledige focus op bewustzijn van eindgebruikersbeveiliging. Je kunt vervolgens de voortgang continu monitoren en rapporteren en de statistieken op organisatieniveau analyseren om de algehele beveiligingshouding van je klanten te versterken.

**92,4% VAN DE MALWARE WORDT VIA
E-MAIL VERSPREID.**

CYBERAANVALLEN WORDEN GEWOON

Aangezien medewerkers de kern van elk bedrijf vormen, zullen zij altijd het hoofddoelwit zijn voor cybercriminelen. Het is van cruciaal belang dat eindgebruikers up-to-date blijven met hun kennis van cyberbeveiliging. Het dreigingslandschap evolueert voortdurend en een bedrijf moet zijn verdedigingsaanpak ook blijven verbeteren.

PHISHING SIMULATIE



JOUW BETROUWBARE PARTNER

Onze Phishing simulatie wordt wereldwijd vertrouwd door organisaties om eersteklas beveiligings- en trainingstools te leveren.



EENVOUDIG CAMPAGNEBEHEER

Voer verschillende campagnes uit voor meerdere groepen en plan campagnes om op willekeurige tijden te verzenden.



GEVARIEERDE E-MAILS

Varieer de inhoud van de phishing-e-mails gebaseerd op jouw behoeften en de dreigingen waarmee ze worden geconfronteerd. Gebruik vooraf geladen e-mailsjablonen of eigen e-mails vanaf een leeg sjabloon.



VIDEO-GEBASEERDE TRAINING

Gemakkelijk te begrijpen, korte en visueel aantrekkelijke trainingsvideo's in 8 talen, met een optie om je eigen trainingsinhoud te creëren. Controleer kennisbehoud van medewerkers met online quizen.



ANALYTICS

Grafische rapportage helpt de algehele cyberbeveiligingshouding te visualiseren en omvat Dark Web ID-inbreuken op inloggegevens gecombineerd met de resultaten van phishing- en trainingscampagnes.

NEEM DIRECT CONTACT MET ONS OP OM MEER TE WETEN TE KOMEN

<https://heiper.nl/contact>