Security awareness

Phishing-mails zijn nog steeds een van de meest lucratieve manieren voor cybercriminelen om in te breken. Onze combinatie van phishing awareness-campagnes en e-learnings verhoogt meetbaar de digitale weerbaarheid van uw organisatie.

ThreadStone
CYBER SECURITY

Periodieke phishing-simulaties

Wat doen we?

We controleren niet eenmalig het bewustzijn van uw medewerkers, maar in een doorlopend proces. Door periodiek phishing-campagnes uit te voeren houdt u uw medewerkers continu alert op het herkennen van malafide e-mails.

Waarom is deze dienst nodig?

Cybercriminelen zetten phishing-aanvallen in om:

- medewerkers om te leiden naar valse webpagina's om zo bijvoorbeeld inloggegevens te ontfutselen;
- malware te installeren op systemen;
- ransomware-aanvallen uit te voeren;
- CEO-fraude te plegen.

Vaak wordt een cyberaanval opgestart via phishing. Op het moment dat rechten op uw systemen van een van uw medewerkers bij cybercriminelen in handen zijn, kunnen ze proberen om meer rechten te verkrijgen en vandaaruit bijvoorbeeld malware of ransomware te installeren op uw systemen. Het is dus van het grootste belang dat medewerkers phishing-e-mails kunnen herkennen en niet zomaar op elke link klikken of software installeren.

Hoe werkt het?

De campagnes die we opzetten zijn gestandaardiseerd dankzij ons ThreadPhish-platform. Wij zorgen periodiek voor het opzetten van een campagne die inspeelt op de actualiteit. Alle medewerkers/e-mailadressen die in ons systeem zijn ingevoerd (of in een .CSV-bestand zijn aangeleverd) ontvangen deze phishing-campagnes.

Follow-up na elke campagne

U ontvangt na afloop van elke campagnemail een duidelijke, geanonimiseerde rapportage met cijfers over naar hoeveel medewerkers de mail is gestuurd, hoeveel medewerkers de mail hebben geopend, hoeveel medewerkers op de phishing-link hebben geklikt en eventueel hoeveel medewerkers gegevens hebben achtergelaten. Ook geven we aan welke e-mailadressen we hebben kunnen vinden in de database van HaveIbeenPwned. Het rapport kan bij uitstek worden gebruikt in de communicatie naar medewerkers om het bewustzijn rond phishing te verhogen en het zorgvuldige gebruik van wachtwoorden te stimuleren.

De belangrijkste voordelen van periodieke phishing-simulaties

Steeds een nieuwe, actuele campagne
We kijken naar de actualiteit en zetten op basis daarvan de campagnes op. Elke keer dus een nieuwe, actuele campagne. Juist in die actualiteit en herhaling schuilt de kracht van deze dienst.

Maakt uw medewerkers bewust van mogelijke phishing-aanvallen
De phishing-mails zijn niet van echt te onderscheiden. Klikt een medewerker, dan krijgt hij/zij direct uitleg waaraan herkend had kunnen worden dat het om een phishing-mail gaat. Na afloop ontvangt u een duidelijke rapportage.

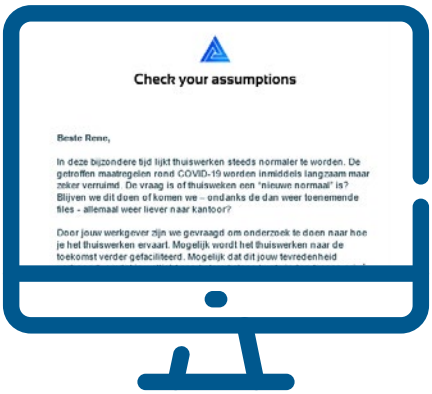
On-the-job training
Medewerkers ontvangen de mails in hun reguliere mailbox. Dit zorgt ervoor dat zij leren in hun gewone werkomgeving. Dat zorgt voor een hogere awareness.

Werkwijze periodieke phishing-simulaties

1

U levert een bestand aan met de gegevens van uw medewerkers. Vervolgens ontvangen uw medewerkers op een willekeurig moment de phishing-simulatiemails.

Vooraf wordt aan u gecommuniceerd in welke weken de simulaties zullen plaatsvinden, zodat u eventuele supportmedewerkers op de hoogte kunt brengen.

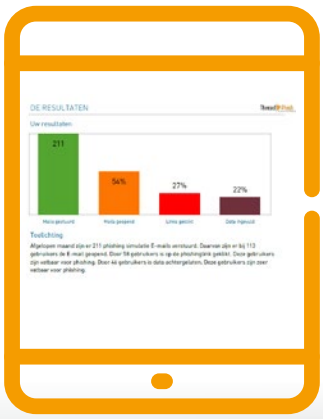


2

Na klikken op de link in de mail verschijnt een pagina waarop wordt aangegeven dat dit een phishing-simulatie betreft en wat de medewerker de volgende keer kan doen om deze te herkennen. Een andere mogelijkheid is dat we de medewerker ook werkelijk gegevens laten invullen op een zogenaamde landingspagina.

3

Na afloop van elke campagne ontvangt u een rapportage met het aantal mails dat we hebben verstuurd, het aantal e-mails dat is geopend, het aantal medewerkers dat heeft geklikt en eventueel het aantal medewerkers dat informatie heeft achtergelaten (afhankelijk van de campagne die we uitvoeren).
Bovendien rapporteren we de resultaten van de controle op HaveIBeenPwned.com waar datalekken worden bijgehouden. Medewerkers die hetzelfde wachtwoord voor meerdere applicaties en websites gebruiken, kunnen vervolgens gewezen worden op het feit dat hun wachtwoord blijkbaar gehackt is.



E-learning informatiebeveiliging

Wat doen we?

We leveren een platform waarmee uw medewerkers de theorie rond informatiebeveiliging leren. Hierdoor weten uw medewerkers wat ze moeten doen en welk gedrag u van hen verwacht op het gebied van informatiebeveiliging. Leermodules worden opgevolgd door examens om de kennis te toetsen. Zo houdt u ook inzicht in de vorderingen.

Waarom is deze dienst nodig?

Medewerkers worden nog altijd gezien als zwakste schakel in de beveiliging van organisaties. Cybercriminelen maken graag misbruik van medewerkers die de risico's van het digitale tijdperk onderschatten of niet weten wat ze precies moeten doen. In onze e-learnings bieden we uw medewerkers de juiste handvatten om risico's op het gebied van informatiebeveiliging, cybersecurity en privacy te herkennen en er goed mee om te gaan.

Hoe werkt het?

Security awareness is geen project, maar een proces. Met onze speciaal ontwikkelde en geteste programma's geeft u doorlopend invulling aan security awareness. Wij testen het gedrag van uw medewerkers, brengen kwetsbaarheden aan het licht en geven u tools om deze kwetsbaarheden aan te pakken. Leer uw medewerkers beveiligingsrisico's herkennen en creëer een (cyber)veilige werkomgeving!

U houdt zelf de regie over de awareness-programma's. Beheerders krijgen toegang tot een bibliotheek met bijna 50 trainingsmodules, games en kennistesten over de verschillende thema's rondom informatiebeveiliging, cybersecurity en privacy. Met deze content stelt u eenvoudig meerdere trainingsprogramma's samen die aansluiten bij de doelen en wensen van uw organisatie.

Gebruikers kunnen worden ingedeeld in groepen die verschillende trainingsprogramma's kunnen volgen: wellicht heeft Finance een ander programma nodig dan HR. Nadat een gebruiker heeft ingelogd, komt hij of zij direct in het leerprogramma dat voor hem of haar beschikbaar is gesteld.

Met de rapportagetool heeft u real-time inzicht in de voortgang en resultaten van gebruikers en kunt u zelf rapportages en certificaten voor gebruikers of groepen genereren. Dat vergroot de motivatie.

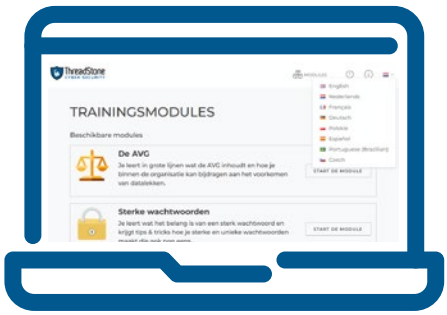
De belangrijkste voordelen van de e-learning informatie-beveiliging

- **Flexibiliteit dankzij modulaire opbouw**
  Het complete programma kan in volgorde, selectie en timing helemaal naar wens worden aangepast. Zo kunt u een trainingsprogramma samenstellen dat perfect aansluit op de wensen van de organisatie. Elk jaar lanceren we minimaal 6 nieuwe modules. Deze worden automatisch toegevoegd aan de bibliotheek.

- **Laagdrempelig interactief**
  De modules zijn kort en toegankelijk. We maken onder andere gebruik van geanimeerde bewustwordingsvideo's, interactieve games en kennistesten. Elke module is in 5 tot 15 minuten te doorlopen. Geen overdaad aan regels en theoretische verhalen, maar direct toepasbare tips aan de hand van praktijkvoorbeelden, om veiliger te werken, ook in privésituaties. Denk aan het herkennen van phishing-mails en het versturen van (gevoelige) gegevens.

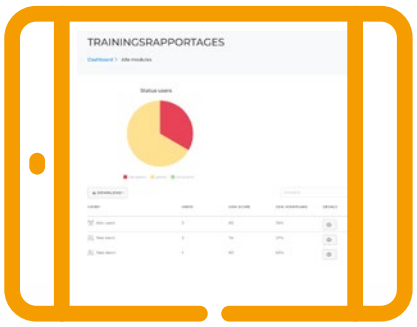
- **Meertalig**
  Onze content is beschikbaar in 8 talen: Nederlands, Engels, Duits, Frans, Spaans, Portugees, Pools en Tsjechisch.

Werkwijze Uitgebreide awareness



1 U levert een bestand aan met de gegevens van uw medewerkers, eventueel ingedeeld per afdeling. Vervolgens ontvangen uw medewerkers een inlog en maandelijks een mail waarin een nieuwe e-learning-module wordt aangekondigd. Na inloggen krijgt de medewerker de verschillende modules te zien die in 8 verschillende talen gevolgd kunnen worden.

2 In totaal zijn er bijna 50 modules die gevolgd kunnen worden. Na het starten van een module krijgt de medewerker een filmpje te zien van 5 tot 15 minuten. Na afloop volgt een toetsing van de kennis.



3 In het portaal hebben medewerkers die daarvoor gemachtigd zijn (bijvoorbeeld HR) continu inzage in de voortgang van de trainingen. Hierdoor kunt u dus controle houden over de voortgang per medewerker, afdeling of over de gehele organisatie.

De unieke propositie van ThreadStone

ThreadStone is in 2014 gestart met één belangrijke missie: het Nederlandse en Europese internet veiliger maken. Zowel voor grote als kleinere organisaties bieden we betrouwbare, praktische en betaalbare cybersecurity-oplossingen die we leveren vanuit Europa.

- Toegankelijke en effectieve cybersecurity-oplossingen.
- Een overzichtelijke Security Routekaart, waarmee we een aanbod op maat kunnen samenstellen.
- ISO 27001-gecertificeerd.
- Korte lijnen en persoonlijke manier van werken.

ThreadStone
CYBER SECURITY

Bewust veilig
www.threadstone.eu

MADE IN HOLLAND