Effectieve training voor medewerkers. Gemakkelijk te gebruiken door beheerders.

k-asap.nl

Kaspersky ASAP: Automated Security Awareness Platform (Geautomatiseerd platform voor beveiligingsbewustzijn)

kaspersky BRING ON THE FUTURE

Kaspersky Automated Security Awareness Platform

Kaspersky ASAP: Automated Security Platform voor bewustwording

Meer dan 80% van alle cyberincidenten wordt veroorzaakt door een menselijke fout waarbij bedrijven miljoenen verliezen als gevolg van personeelsgerelateerde incidenten. De doeltreffendheid van traditionele trainingsprogramma's ter voorkoming van deze problemen is echter beperkt. Ze slagen er zelden in om het noodzakelijke gedrag te stimuleren.

Menselijke fouten zijn het grootste cyberrisico

$ 1.315.000
per grote onderneming
De gemiddelde financiële impact van gegevenslekken als gevolg van verkeerd gebruik van IT-middelen door medewerkers*

$ 132.000
per MKB
De gemiddelde financiële impact van een gegevenslek als gevolg van het fysieke verlies van mobiele toestellen in bedrijfseigendom waardoor de organisatie aan risico's wordt blootgesteld*

50%
van bedrijven
zegt bedreigingen te ervaren die direct veroorzaakt werden door verkeerd gedrag van medewerkers, waarmee dit de meest voorkomende bedreiging van IT-veiligheid is*

43%
van kleine bedrijven
was het slachtoffer van een beveiligingsincident doordat het IT-veiligheidsbeleid geschonden werd door medewerkers*

26%
van medewerkers
zegt dat hun persoonlijke e-mail hetzelfde paswoord heeft als hun werkaccount**

Barrières voor de introductie van een efficiënt programma voor beveiligingsbewustzijn

Hoewel bedrijven staan te popelen om programma's voor beveiligingsbewustzijn te implementeren, zijn weinig ondernemingen tevreden over het proces en de resultaten. Dit is vooral een uitdaging voor kleine en middelgrote bedrijven, die meestal niet beschikken over de nodige ervaring en middelen.

Niet efficiënt voor gebruikers

Ervaren als moeilijk, saai, niet relevant.

Het gaat vooral over 'niet doen' in plaats van 'hoe'

Kennis wordt niet onthouden

Lezen en luisteren zijn niet zo effectief als doen

Een administratieve last

Zo stel je een programma op en stel je doelen

Zo beheer je trainingsopdrachten

Zo controleer je de voortgang

Zo betrek je het personeel volledig bij de training

* Rapport: Rapport "IT security economics 2021", Kaspersky

** https://www.beyondidentity.com/blog/password-sharing-work

Beheer van doeltreffendheid en opleidingsgemak voor organisaties van elke omvang

Maak kennis met het Automated Security Awareness Platform, de kern van de trainingsportfolio van Kaspersky Security Awareness.

Het platform is een online tool waarop medewerkers het hele jaar door hun praktische cyberveiligheidsvaardigheden kunnen versterken. Voor de introductie en het beheer van het platform zijn geen specifieke middelen en voorzieningen vereist, en het voorziet de organisatie van ingebouwde hulp bij alle stappen op weg naar een veilige cyberomgeving voor het bedrijf.

Zo evalueer je een bewustzijnsprogramma

Een van de belangrijkste criteria bij het kiezen van een bewustzijnsprogramma is de doeltreffendheid. ASAP integreert doeltreffendheid in de trainingsinhoud en het beheer. Het platform is gebaseerd op een competentiemodel bestaande uit 300+ praktische en essentiële cyberveiligheidsvaardigheden die alle medewerkers zouden moeten hebben.

Leer je medewerkers over cyberveiligheid om hun houding en gedrag te veranderen en je bedrijf en IT-systemen te beschermen.

Doeltreffende training

Consistent	- Goed doordachte, gestructureerde inhoud – Interactieve lessen, voortdurende herhaling, testen, gesimuleerde phishing-aanvallen om te verzekeren dat vaardigheden worden toegepast De trainingsmaterialen en hun structuur zijn gebaseerd op de kenmerken van het menselijk geheugen, ons vermogen om informatie op te nemen en te onthouden.
Praktisch en boeiend	- Relevant voor het dagelijkse beroepsleven van medewerkers - Vaardigheden die onmiddellijk gebruikt kunnen worden Voorbeelden van levensechte, herkenbare situaties dragen bij aan de betrokkenheid van de student én helpen informatie te onthouden.
Positief	- Geeft een proactieve draai aan veilig gedrag - Legt uit 'waarom' en 'hoe' in plaats van wat niet te doen Teveel regels en beperkingen kunnen ontevredenheid veroorzaken, terwijl uitleg en overtuigingen die aansluiten bij de manier waarop mensen van nature denken, bijdragen aan aanvaarding en gedragsverandering.

Eenvoudig beheer

Eenvoudig beheer	Volledig geautomatiseerd opleidingsbeheer brengt elke medewerker op het juiste niveau van veiligheidsvaardigheden, passend bij hun risicoprofiel zonder tussenkomst van de platformbeheerder
Eenvoudig te beheren	'All-in-one' dashboard en actiegerichte rapporten
Studenten raken makkelijk geboeid	Het platform verstuurd automatisch uitnodigingen en motiverende e-mails, evenals wekelijkse leerling- en beheerdersrapporten.

ASAP programmabeheer: eenvoud door volledige automatisering

Start je programma in vier eenvoudige stappen

Upload gebruikers

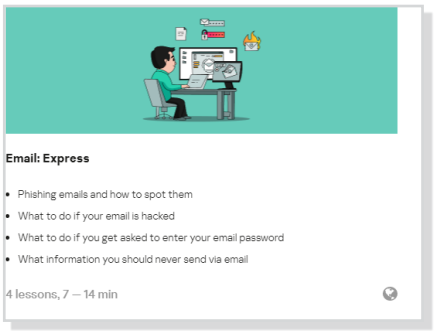
Verdeel gebruikers naar risicoprofiel en stel streefniveaus in voor elke groep

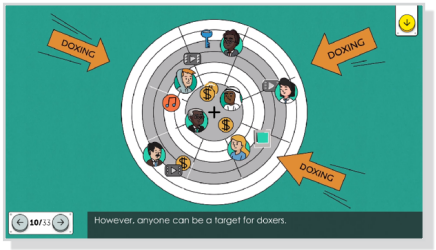
Dit is de enige stap waarbij de beheerder moet nadenken en beslissingen nemen

Start de training

Geautomatiseerd trainingsbeheer door ASAP

Het platform stelt een onderwijsschema voor elke groep samen, gebaseerd op tempo en streefniveau, en levert actiegerichte rapporten en aanbevelingen





Betere leerprincipes

Kaspersky ASAP verandert de manier waarop we cyberbeveiliging aanleren. Je kunt nu bepalen of je je medewerkers een snelle basiscursus toe wilt wijzen om hen snel op het wettige niveau voor cyberbeveiliging te brengen of hun kennis op te frissen, of kiezen voor een volledige cursus op verschillende moeilijkheidsniveaus

Snelle cursus

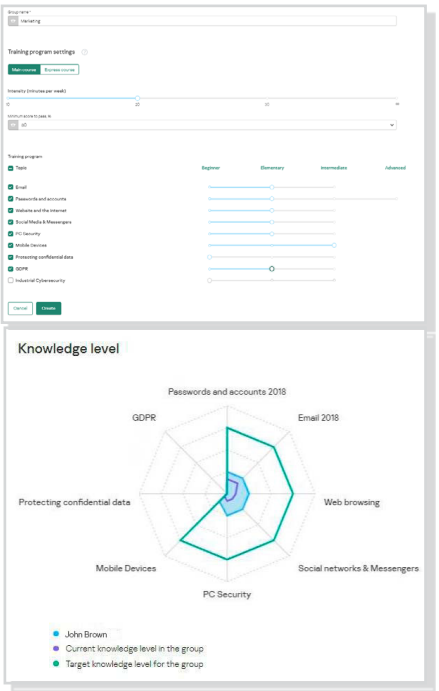
Een korte versie van de training in audio-video formaat. Elk van de zes belangrijke onderwerpen rond cyberbeveiling bevat korte lessen om de gebruiker basisvaardigheden aan te leren op het vlak van cyberbeveiliging.
- Interactieve theorie
- Video's
- Testen

Gesimuleerde phishing-aanvallen maken geen onderdeel uit van het opleidingstraject, maar kunnen door de beheerder toegevoegd worden als een phishing-aanval

Specifieke opleidingstrajecten voor elk risicoprofiel

Gebruik geautomatiseerde regels voor het toewijzen van medewerkers aan een bepaalde groep, op basis van het gewenste educatieve streefniveau. Dit streefniveau hangt af van het risico dat de specifieke rol vormt voor het bedrijf. Hoe hoger het risico, hoe hoger het educatieve streefniveau moet zijn. Een voorbeeld: IT of accountants vormen doorgaans een hoger risico dan andere kantoormedewerkers.

Flexibel opleidingstraject



Flexibel leren

- De reikwijdte van de training is volledig flexibel terwijl deze de voordelen behoudt van stapsgewijs geautomatiseerd opleidingsbeheer
- Voor elke trainingsgroep kun je nu kiezen:
  - Hoofd- of snelle cursus of de combinatie van beide
  - Onderwerpen om te leren in de hoofdcursus en/of de snelle cursus die studenten in de groep moeten kennen
  - Het streefniveau dat je studenten moeten bereiken voor elk geselecteerd onderwerp in de hoofdcursus.

Altijd actiegerichte rapporten

- Maak gebruik van dashboards met alle informatie die nodig is voor de controle en het beheer van statistische overzichten over bedrijfsgebruikers, opleidingstijden en groepstraining, met de mogelijkheid tot individueel niveau te gaan
- Krijg suggesties om resultaten te verbeteren
- Download rapporten van de hoofdpagina in een enkele klik en pas de frequentie voor de ontvangst van rapporten per e-mail aan

Vrijheid om te presteren

Medewerkers kunnen studeren op elk geschikt moment en vanaf elk apparaat. Mobiel-vriendelijk ontwerp maakt leren zelfs nog aangenamer. Gebruikers kunnen toegang tot het trainingsportaal krijgen door gepersonaliseerde links in de trainingsuitnodiging of door een enkele link voor alle gebruikers via Single Sign-On (SSO)-technologie

ASAP methode hoofdcursus

Voortdurend stapsgewijs leren

- Van eenvoudig tot meer complex, onderwerp na onderwerp en niveau na niveau: de kennis neemt toe
- Eerder aangeleerde kennis wordt uitgebreid en toegepast in nieuwe contexten

Multimodale inhoud

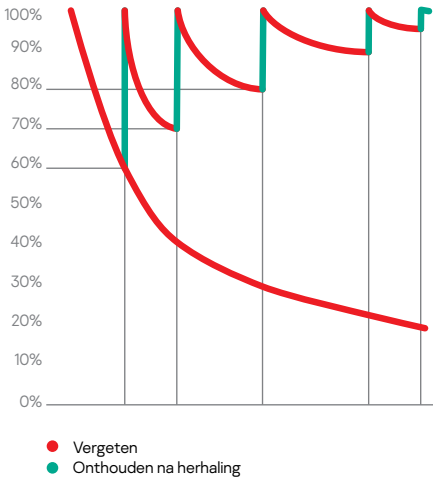
- Elk niveau omvat: evaluatie interactieve lessenherhaling (test en gesimuleerde phishing-aanval waar van toepassing)
- Alle trainingselementen ondersteunen de specifieke vaardigheid die in elke eenheid wordt aangeleerd, zodat vaardigheden werkelijk beheerst worden en deel uitmaken van het nieuwe, gewenste gedrag

Leren met tussenpozen

- De Ebbinghaus-'vergeetcurve'- leermethode gebaseerd op de kenmerken van het menselijk geheugen
- Herhaling leidt tot veilige gewoonten en voorkomt vergeten
- Herhaling in elke module

De Ebbinghaus-vergeetcurve

Herhaling draagt bij aan het opbouwen van sterke vaardigheden.



Elk onderwerp bestaat uit meerdere niveaus, waarin specifieke beveiligingsvaardigheden in detail worden behandeld.
Niveaus worden gedefinieerd op basis van de risicograad die ze helpen te voorkomen: niveau 1 is normaal gezien voldoende om tegen de gemakkelijkste en massa-aanvallen te beschermen. Om te beschermen tegen de meest geavanceerde en gerichte aanvallen moeten hogere niveaus bestudeerd worden.

Trainingsonderwerpen

- Paswoorden en accounts
- E-mail
- Websites en het internet
- Sociale media en berichtendiensten
- Pc-beveiliging
- mobiele apparaten
- Bescherming van vertrouwelijke gegevens
- AVG
- Industrial Cybersecurity

Voorbeeld: vaardigheden getraind in het onderwerp 'Websites en het internet'

Beginner Massa-aanvallen (goedkoop en eenvoudig) voorkomen	**Elementair** Massa-aanvallen op een specifiek profiel voorkomen	**Tussenniveau** Goed voorbereide, gerichte aanvallen voorkomen	**Gevorderd*** Gerichte aanvallen voorkomen
23 vaardigheden, waaronder: - Nep pop-ups herkennen - Opletten voor omleidingen - Echte download-links herkennen van nep - Uitvoerbare bestanden op het web herkennen - De authenticiteit van een browserextensie leren bepalen	**34 vaardigheden, waaronder:** - Data alleen invullen op websites met een geldig SSL-certificaat - Verschillende paswoorden voor verschillende registraties gebruiken - Nepwebsites herkennen aan verschillende kenmerken – Numerieke links vermijden - Ongeldige netwerklinkadressen van nep-subdomeinen herkennen	**12 vaardigheden, waaronder:** - Checken van links om te delen vóór verzending - Software gebruiken van betrouwbare fabrikanten voor torrents - Alleen legale inhoud downloaden via torrents - Browsercookies regelmatig verwijderen	**13 vaardigheden, waaronder:** - Verfijnde neplinks herkennen (waaronder links die eruitzien als je bedrijfswebsites, links met omleiding) - Websites checken door speciale voorzieningen te gebruiken - Herkennen of een browser aan het minen is - Zwarte SEO-websites vermijden
	+ herhaling van de elementaire vaardigheden	+ herhaling van de voorgaande vaardigheden	+ herhaling van de voorgaande vaardigheden

Belangrijke behandelde onderwerpen: links, downloads, software-installatie, registreren en inloggen, betalingen, SSL

* Wordt toegevoegd in de loop van 2022

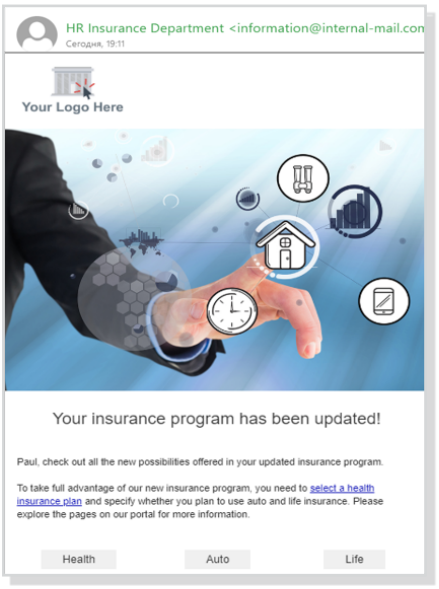
Talen

Het platform (zowel de interface voor studenten als beheer) zijn beschikbaar in de volgende talen:

- Arabisch
- Nederlands
- Engels
- Frans
- Duits
- Italiaans
- Portugees
- Russisch
- Spaans
- Tsjechisch
- Kazachs
- Pools
- Slovaaks
- Roemeens
- Turks
- Hongaars
- Deens
- Zweeds
- Grieks*
- Servisch
- Braziliaans (Portugees)*
- Portugees
- Roemeens
- Servisch
- Slovaaks
- Zweeds
- Turks
- Grieks
- Japans
- Chinees (Mandarijn)*

* worden toegevoegd in 2022

Voorbeeld van het aanpasbare gesimuleerde phishing-sjabloon en feedback



Evenwichtige, gestructureerde inhoud die relevant is voor reële situaties om doeltreffendheid te verzekeren

Leerprincipes in ASAP zijn gebaseerd op de methode die werkt met de kenmerken van menselijke natuur, ons vermogen om informatie op te nemen en te onthouden. De inhoud geeft talrijke levensechte voorbeelden en gevallen die het persoonlijke belang van cyberbeveiliging voor medewerkers benadrukken. Het platform richt zich niet alleen op kennisoverdracht maar vooral op het trainen van vaardigheden, zodat praktijkoefeningen en werknemergerelateerde taken de kern van elke module vormen.

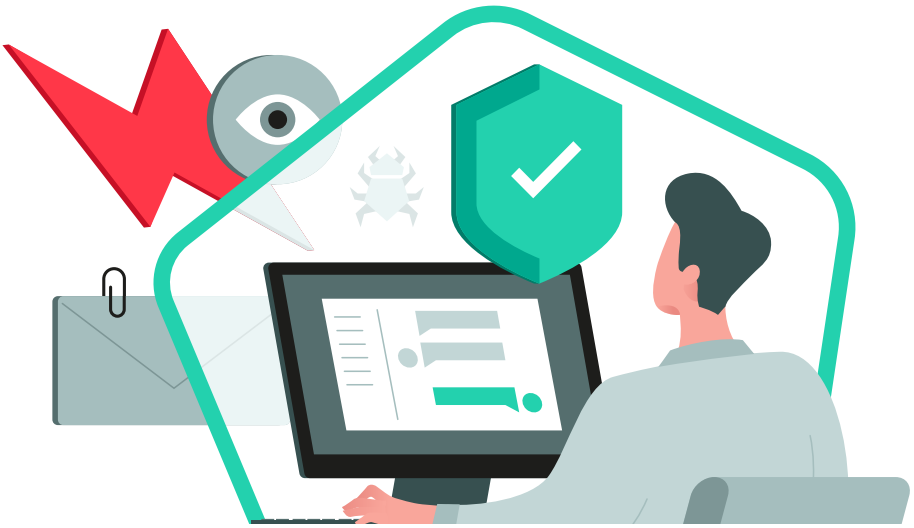
Visuele stijl en teksten worden niet alleen vertaald naar verschillende talen, maar ook aangepast aan culturen en plaatselijke gewoontes.

Gesimuleerde phishing-aanvallen

Phishing-aanvallen zijn een toevoeging aan de basistraining die de praktische vaardigheden van medewerkers test voor het voorkomen van phishing-aanvallen. Dit zal de trainingsbeheerder helpen om hiaten in de kennis van gebruikers te identificeren en studenten prikkelen om onderwerpen te bestuderen waarmee ze moeite hebben.

Het platform heeft gebruiksklare e-mailsjablonen met phishing-voorbeelden die aan gebruikers van het platform in alle beschikbare talen verstuurd kunnen worden. De beschikbare sjablonen worden regelmatig aangevuld met nieuwe. Je kunt ook aangepaste e-mails creëren op basis van voorgeprogrammeerde sjablonen.

Test de weerbaarheid van je medewerkers met een gesimuleerde phishing-aanval voordat je de training start. Het zal werknemers en management overtuigen van de voordelen van de training.



Kaspersky Security Awareness - een nieuwe aanpak voor het aanleren van IT-veiligheidsvaardigheden

Belangrijkste programmaverschillen

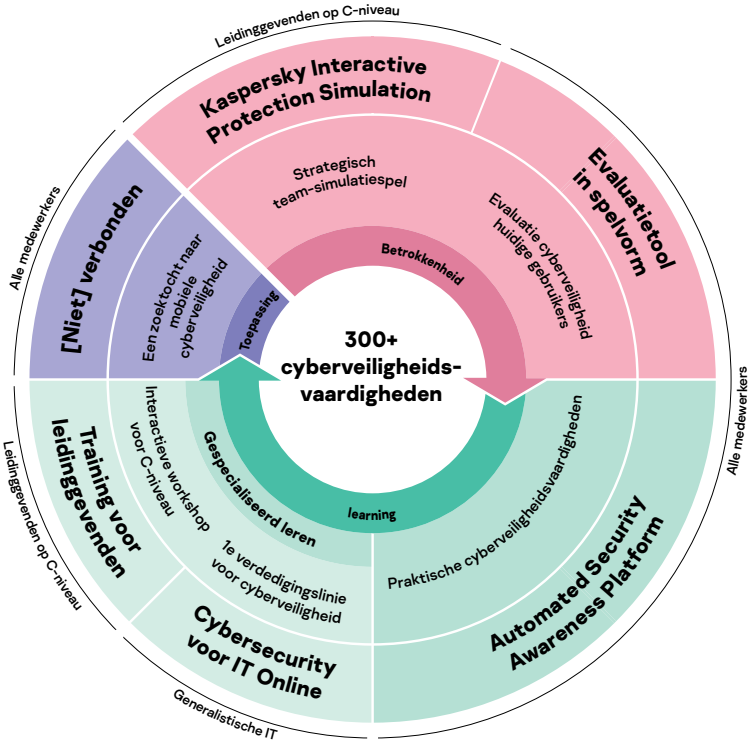
Belangrijke cyberveiligheidsexpertise
Meer dan 20 jaar ervaring in cyberveiligheid omgezet in cyberveiligheidsvaardigheden die aan de basis liggen van onze producten

Training die het gedrag verandert van medewerkers op elk niveau van je organisatie
Onze training in spelvorm zorgt voor betrokkenheid en motivatie door edutainment, terwijl de leerplatforms helpen met het zich eigenmaken van de cyberveiligheidsvaardigheden, om ze niet te vergeten.

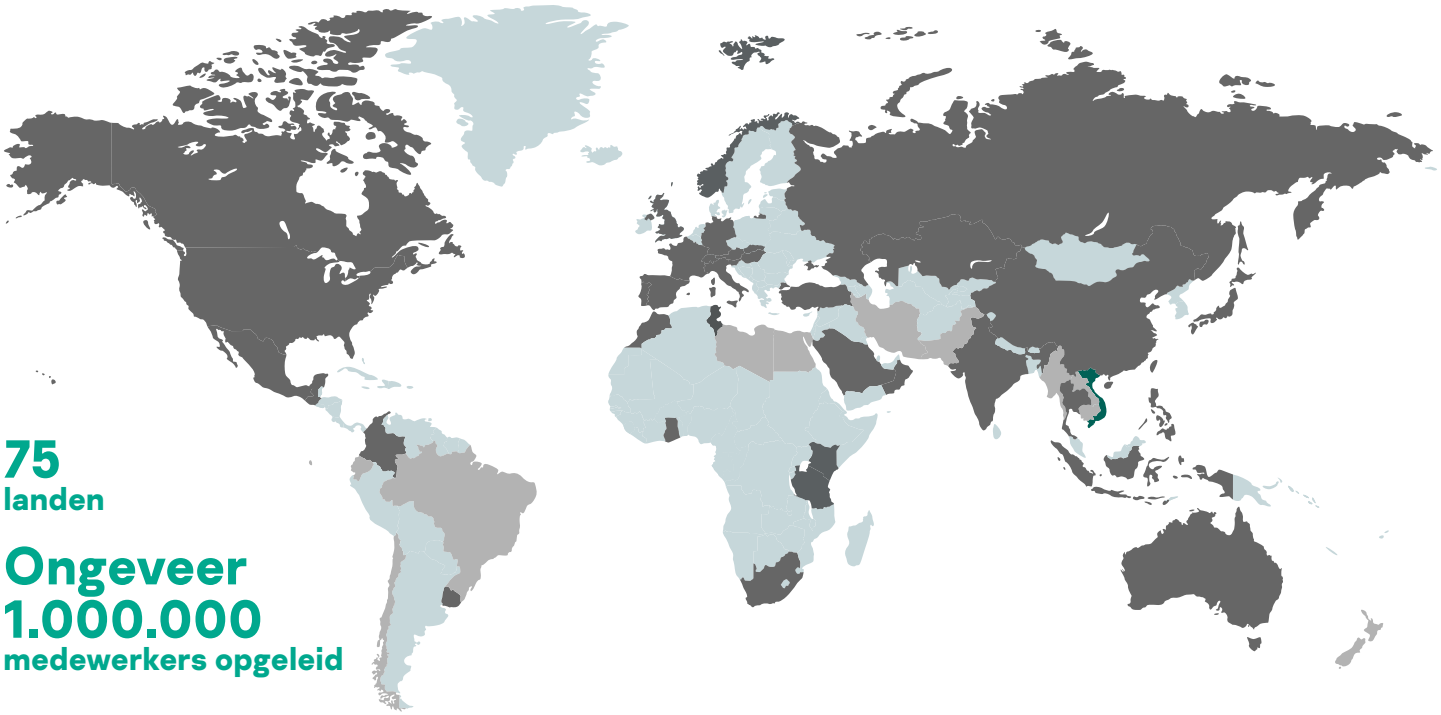
Kaspersky Security Awareness biedt een brede waaier aan oplossingen voor alle cyberveiligheidsspecifieke noden van bedrijven en leert door het gebruik van de nieuwste leertechnieken en technologie de vaardigheden aan die iedereen nodigt heeft.

Een flexibele training voor iedereen

Kies één enkele oplossing voor een specifieke beveiligingsbehoefte, of laat ons pakketten leveren waarmee u gemakkelijk trainingen kunt starten en u kunt richten op al uw behoeften en prioriteiten. Je kunt meer informatie over pakketten hier vinden: kaspersky.com/awareness



Kaspersky Security Awareness wereldwijd



75
landen

Ongeveer
1.000.000
medewerkers opgeleid

Kaspersky ASAP gratis proefversie: k-asap.nl
Enterprise Cybersecurity: www.kaspersky.nl/enterprise
Kaspersky Security Awareness: www.kaspersky.com/awareness
Nieuws over IT-beveiliging: business.kaspersky.nl/

www.kaspersky.com

kaspersky BRING ON THE FUTURE