Formazione efficace per i dipendenti. Facilità di utilizzo per i manager.

k-asap.com

Kaspersky ASAP: Automated Security Awareness Platform

kaspersky BRING ON THE FUTURE

Kaspersky Automated Security Awareness Platform

Kaspersky ASAP: Automated Security Awareness Platform

Più dell'80% degli incidenti informatici è causato da errori umani, che si traducono a livello aziendale in milioni di euro spesi per ripristinare i sistemi interessati. Tuttavia, l'efficacia dei programmi di formazione tradizionali destinati a prevenire questi problemi è limitata e di solito non riesce a motivare il comportamento desiderato.

L'errore umano è il rischio informatico più grande

1.315.000 dollari
per organizzazione aziendale
L'impatto finanziario medio delle violazioni dei dati causate dall'uso inappropriato delle risorse IT da parte dei dipendenti*

132.000 dollari
per PMI
L'impatto finanziario medio di una violazione dei dati causata dalla perdita fisica dei dispositivi mobili di proprietà dell'azienda che espone l'organizzazione al rischio*

Il 50%
delle aziende
ha riferito di aver subito minacce direttamente causate dal comportamento inappropriato del personale, fattore identificato come la minaccia più comune per la sicurezza IT*

Il 43%
delle piccole aziende
ha subito un incidente di sicurezza dovuto a una violazione dei criteri di sicurezza IT da parte dei dipendenti*

Il 26%
dei dipendenti
ha riferito di avere la stessa password per l'e-mail personale e l'account aziendale**

Fattori da considerare per un approccio efficiente a un programma formativo sulla cybersicurezza

Nonostante le aziende siano pronte a implementare i programmi di Security Awareness, non molte sono soddisfatte dei processi e risultati. Le piccole e medie imprese, invece, che di solito non hanno esperienza e risorse dedicate, sono particolarmente interessate.

Scarsa efficacia per i partecipanti

Percepito come un'attività faticosa, noiosa e di secondaria importanza.

Vengono indicate solo le cose da "non fare", anziché fornire istruzioni su "come fare" qualcosa

Le conoscenze acquisite non vengono consolidate

Lettura e ascolto non sono efficaci come l'attività pratica

Carico amministrativo elevato

Come creare un programma e definire gli obiettivi

Come gestire gli incarichi di formazione

Come controllare i progressi compiuti

Come coinvolgere pienamente le persone nel programma formativo

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

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

Efficienza e semplicità di gestione della formazione per le organizzazioni di ogni dimensione

Kaspersky introduce la piattaforma Automated Security Awareness, che costituisce il focus principale del portfolio formativo Kaspersky Security Awareness.

La piattaforma è uno strumento online per la formazione dei dipendenti sulle tematiche relative alla sicurezza informatica nell'arco di un anno. Il processo di implementazione e gestione della piattaforma non richiede risorse o configurazioni specifiche ed è in grado di offrire all'organizzazione una guida integrata per ogni passaggio del percorso verso un ambiente di cybersicurezza aziendale sicuro.

Come valutare un programma di Security Awareness

Uno dei criteri più importanti nella scelta di un simile programma formativo è rappresentato dal grado di efficienza di quest'ultimo. Con ASAP, il concetto di efficienza è profondamente integrato nei contenuti e nelle modalità di gestione del programma. I contenuti della piattaforma si basano su un modello formativo suddiviso in oltre 300 lezioni pratiche ed essenziali sulla cybersicurezza: tutti i dipendenti dovrebbero acquisire queste competenze indispensabili.

Un adeguato programma formativo sulla sicurezza informatica consentirà di modificare i modelli comportamentali e gli atteggiamenti del personale, proteggendo di conseguenza l'azienda e i sistemi IT.

Formazione efficiente

Coerenza	– Contenuti ben strutturati – Moduli interattivi, costante rafforzamento, conduzione di test, attacchi di phishing simulati, per garantire l'applicazione delle competenze acquisite Il materiale formativo e la struttura dello stesso sono organizzati in modo tale da rispecchiare le specificità della memoria umana, la nostra capacità di assorbire e conservare le informazioni.
Pratica e coinvolgente	– Pertinente alle attività lavorative quotidiane dei dipendenti – Le competenze fornite si possono utilizzare immediatamente Gli esempi concreti, relativi a situazioni ed eventi reali in cui i dipendenti si riconoscono pienamente, contribuiscono al coinvolgimento dell'utente e aiutano al contempo a memorizzare le informazioni in modo efficace.
Positività	– Imprime una decisa spinta proattiva verso l'adozione di comportamenti sicuri – Spiega "perché" e "in che modo" agire, in maniera semplice Troppe regole e restrizioni possono causare malcontento, mentre spiegazioni e strategie di convincimento perfettamente allineate al modo in cui pensano le persone contribuiscono con naturalezza all'adozione e alla modifica di determinati comportamenti.

Facilità di gestione

facile da gestire	La gestione dell'apprendimento completamente automatizzata permette a ogni dipendente di ottenere un livello di competenze appropriato ai rischi del proprio ruolo, senza alcun intervento da parte dell'amministratore della piattaforma.
Facile da controllare	Dashboard "all-in-one" e report pratici.
Facilità di coinvolgimento	La piattaforma invia in automatico inviti ed e-mail motivazionali, così come i report settimanali per utenti e amministratori.

Gestione ASAP: massima semplicità attraverso la completa automazione

Avvio del programma in 4 semplici step

Caricamento degli utenti

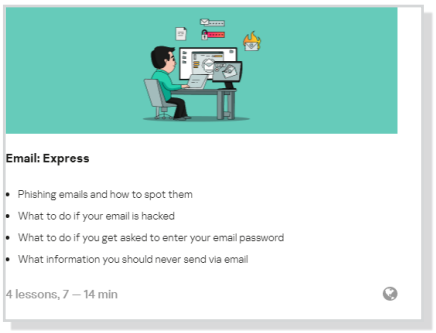
Suddivisione degli utenti in base al profilo di rischio e impostazione del livello di destinazione per ciascun gruppo

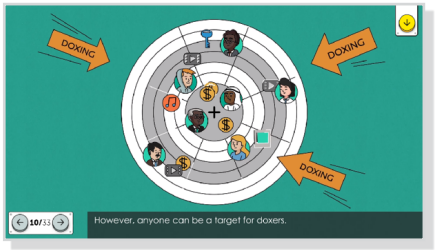
Questo è l'unico step in cui l'amministratore deve prendere decisioni

Avvio del programma di formazione

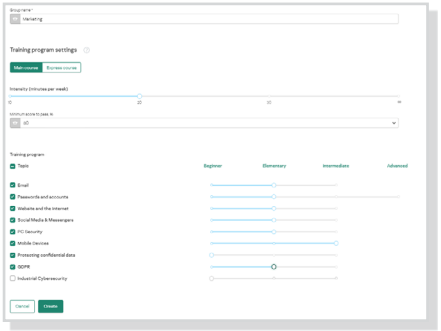
La piattaforma crea un programma formativo per ciascun gruppo, sulla base del ritmo di apprendimento e del livello target; fornisce inoltre report e suggerimenti pratici

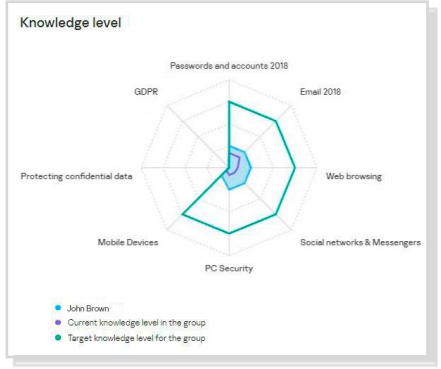
Gestione automatizzata dell'apprendimento tramite ASAP





Percorso di apprendimento flessibile





Principi di apprendimento ottimizzati

Kaspersky ASAP sta cambiando il modo di erogare contenuti didattici sulla sicurezza informatica. Adesso è possibile scegliere se assegnare ai dipendenti un corso rapido di livello base che aiuterà a soddisfare rapidamente i requisiti normativi per la formazione sulla sicurezza informatica, aggiornare le loro conoscenze oppure optare per un corso completo suddiviso in livelli di complessità

Corso rapido

Versione breve del corso di formazione audio/video. Ciascuno dei 6 principali argomenti di sicurezza informatica contiene diverse micro-lezioni per aiutare l'utente ad acquisire padronanza rispetto alle abilità di sicurezza informatica di base.
- Teoria interattiva
- Video
- Test

Gli attacchi di phishing simulati non sono inclusi nel percorso di apprendimento, ma possono essere assegnati in aggiunta dall'amministratore come campagna di phishing

Percorsi di apprendimento specifici per ogni profilo di rischio

Utilizzo di regole automatizzate per assegnare il livello di formazione finale desiderato ai singoli dipendenti. Il livello target è strettamente correlato al rischio rappresentato dallo specifico ruolo svolto dall'utente per l'azienda. Maggiore è il rischio, più elevato dovrebbe essere il livello di formazione finale. Ad esempio, utenti del reparto IT o contabilità tipicamente rappresentano un rischio più elevato rispetto a quello attribuibile agli altri dipendenti.

Massima flessibilità nell'apprendimento

- La formazione si svolge in maniera flessibile, pur conservando i tipici vantaggi di un prodotto che automatizza il processo di apprendimento
- Per ogni gruppo di utenti si possono selezionare:
  - Corso principale, corso rapido o una combinazione di entrambi
  - Argomenti di apprendimento per la formazione nel corso principale e/o nel corso rapido rivolta agli studenti del gruppo
  - Il livello target che gli studenti devono raggiungere per ciascun argomento selezionato nel corso principale.

Report finalizzati all'azione in qualsiasi momento

- Sono disponibili dashboard con tutte le informazioni necessarie per controllare e gestire i riepiloghi statistici sugli utenti aziendali, gli slot di formazione e la formazione di gruppo, con la possibilità di scendere fino al livello individuale
- Suggerimenti su come migliorare i risultati
- Download dei report dalla pagina principale con un semplice clic e configurazione della frequenza di ricezione dei report tramite e-mail

Massima libertà

I dipendenti possono studiare in qualsiasi momento e da qualsiasi dispositivo. Il design ottimizzato per i dispositivi mobili rende l'apprendimento ancora più comodo. Gli utenti possono accedere al portale di formazione utilizzando collegamenti personalizzati dall'invito alla formazione o utilizzare un unico collegamento per tutti gli utenti tramite la tecnologia Single Sign-On (SSO)

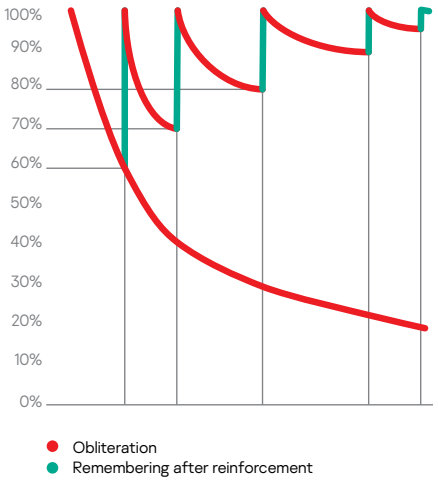
Metodologia del corso principale ASAP

Apprendimento incrementale continuo

- Dall'argomento più semplice a quello più complesso, modulo dopo modulo, livello per livello: aumento progressivo delle conoscenze
- Ampliamento delle conoscenze precedentemente acquisite e relativa applicazione a nuovi contesti

La Curva dell'oblio di Ebbinghaus

Rafforzamento ripetuto per la creazione efficiente di competenze.



Numerosi elementi formativi per lo sviluppo della consapevolezza

- Ogni livello comprende: modulo interattivo, rafforzamento, valutazione (test e attacco di phishing simulato, ove applicabile)
- Tutti gli elementi formativi supportano la specifica competenza oggetto di apprendimento in ogni singola unità; in tal modo gli utenti acquisiscono una perfetta padronanza delle varie competenze, le quali divengono parte effettiva del nuovo modello comportamentale desiderato

Apprendimento modulare

- "Curva dell'oblio" di Ebbinghaus: metodologia di apprendimento basata sulle caratteristiche specifiche della memoria umana
- La ripetizione dei concetti crea abitudini comportamentali sicure e impedisce di dimenticare quanto appreso in precedenza
- Rafforzamento incluso in ogni singolo modulo

Argomenti della formazione

- Password e account
- E-mail
- Siti Web e Internet
- Social media e strumenti di messaggistica
- Sicurezza del PC
- Dispositivi mobili
- Protezione dei dati confidenziali
- GDPR
- Industrial CyberSecurity

Ciascun modulo comprende diversi livelli, in cui vengono spiegate nel dettaglio le competenze specifiche in materia di sicurezza IT. I livelli sono definiti in base al grado di rischio che consentono di contrastare: il livello 1 in genere è sufficiente per proteggere dagli attacchi più semplici e dagli attacchi di massa. Per la protezione dagli attacchi più sofisticati e mirati, vanno esaminati i livelli superiori.

Esempio: competenze acquisite nell'argomento "Siti Web e Internet".

Base Per prevenire attacchi generici e semplici da individuare	**Principiante** Per prevenire attacchi di massa su un profilo specifico	**Intermedio** Per prevenire attacchi di media complessità	**Avanzato*** Per prevenire attacchi mirati
23 competenze, tra cui: – Riconoscere i finti pop-up – Fare attenzione ai reindirizzamenti – Distinguere i collegamenti di download autentici da quelli falsi – Riconoscere i file eseguibili trovati nel Web – Essere in grado di determinare l'autenticità di un'estensione del browser	**34 competenze, tra cui:** – Immettere i dati solo nei siti con un certificato SSL valido – Usare password diverse per registrazioni diverse – Riconoscere i siti falsi in base a diversi indicatori – Evitare link numerici – Riconoscere gli indirizzi dei collegamenti di rete non validi dai sottodomini fasulli	**12 competenze, tra cui:** – Verificare i collegamenti di condivisione prima dell'invio – Utilizzare solo software di produttori affidabili per i torrent – Scaricare i contenuti legali solo dai torrent – Cancellare regolarmente i cookie del browser	**13 competenze, tra cui:** – Come riconoscere link malevoli complessi (compresi quelli creati ad hoc, molto simili a domini relativi a siti web leciti, link con reindirizzamenti) – Controllare i siti che utilizzano utilità speciali – Riconoscere se il browser è pensato per il mining – Evitare siti Black SEO
	+ rafforzamento delle competenze di base	+ rafforzamento delle competenze precedenti	+ rafforzamento delle competenze precedenti

Argomenti chiave trattati nel modulo: Collegamenti, download, installazioni software, registrazioni e accessi, pagamenti, SSL

* Sarà aggiunto nel 2022

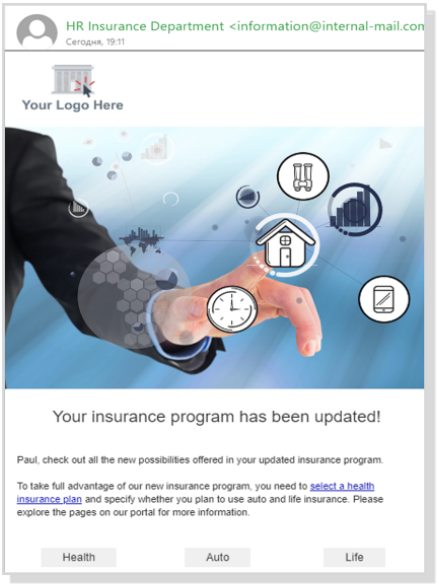
Lingue

La piattaforma (sia interfaccia utente, sia interfaccia amministratore) risulta disponibile nelle seguenti lingue:

- Arabo
- Olandese
- Inglese
- Francese
- Tedesco
- Italiano
- Portoghese
- Russo
- Spagnolo
- Ceco
- Kazako
- Polacco
- Sloveno
- Rumeno
- Turco
- Ungherese
- Danese
- Svedese
- Greco*
- Serbo
- Brasile (Portoghese)*
- Portoghese
- Rumeno
- Serbo
- Sloveno
- Svedese
- Turco
- Greco
- Giapponese
- Cinese (Mandarino)*

* in arrivo nel 2022

Esempio del modello di phishing simulato modificabile e feedback



Efficienza della formazione: contenuti ben strutturati e bilanciati, basati su eventi e situazioni reali

I principi di apprendimento implementati attraverso la piattaforma ASAP si basano sulla particolare metodologia che tiene conto delle specificità della natura umana, della nostra capacità di percepire e assorbire le informazioni. Il contenuto è ricco di esempi e casi reali che sottolineano l'importanza personale della sicurezza informatica per i dipendenti. La Piattaforma è incentrata sulle competenze di formazione, non solo sulla parte teorica: gli esercizi pratici e le attività legate al dipendente sono al centro di ogni modulo.

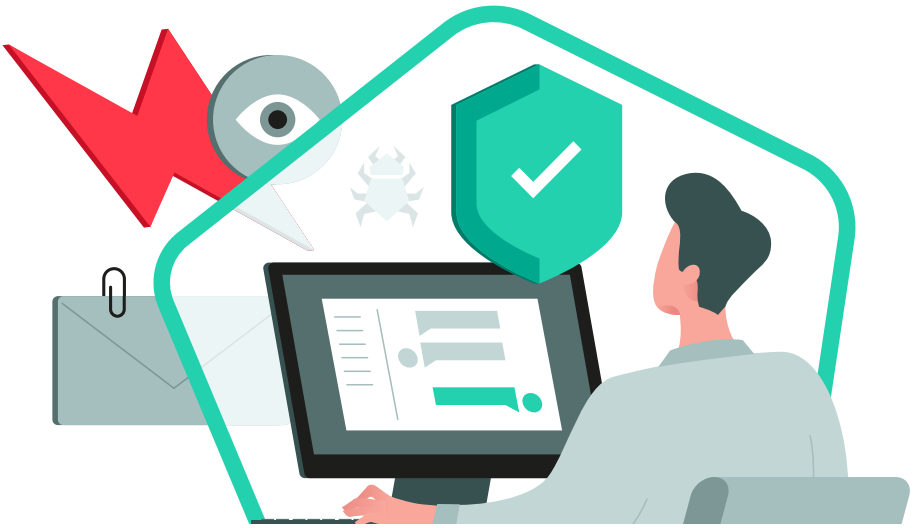
Lo stile e i testi non sono solo tradotti nelle diverse lingue, ma vengono adattati perché riflettano le culture locali.

Campagne di phishing simulate

Le campagne di phishing sono un'aggiunta al processo di formazione principale che mette alla prova le capacità pratiche dei dipendenti nell'evitare gli attacchi di phishing. Ciò aiuterà il responsabile della formazione a identificare le lacune nelle conoscenze degli utenti e li incoraggerà a studiare gli argomenti difficoltosi.

La piattaforma viene fornita con modelli di e-mail già pronti contenenti esempi di phishing che possono essere inviati agli utenti della piattaforma in tutte le lingue disponibili. Il set di modelli disponibili viene aggiornato regolarmente con quelli nuovi. È inoltre possibile creare e-mail personalizzate in base a modelli predefiniti.

Provando un attacco di phishing simulato prima di iniziare la formazione sarà possibile mettere alla prova la resilienza dei dipendenti! Dipendenti e addetti alla gestione potranno così constatare i vantaggi della formazione.



Kaspersky Security Awareness – un nuovo approccio all'apprendimento di abilità di sicurezza IT

Principali elementi distintivi del programma

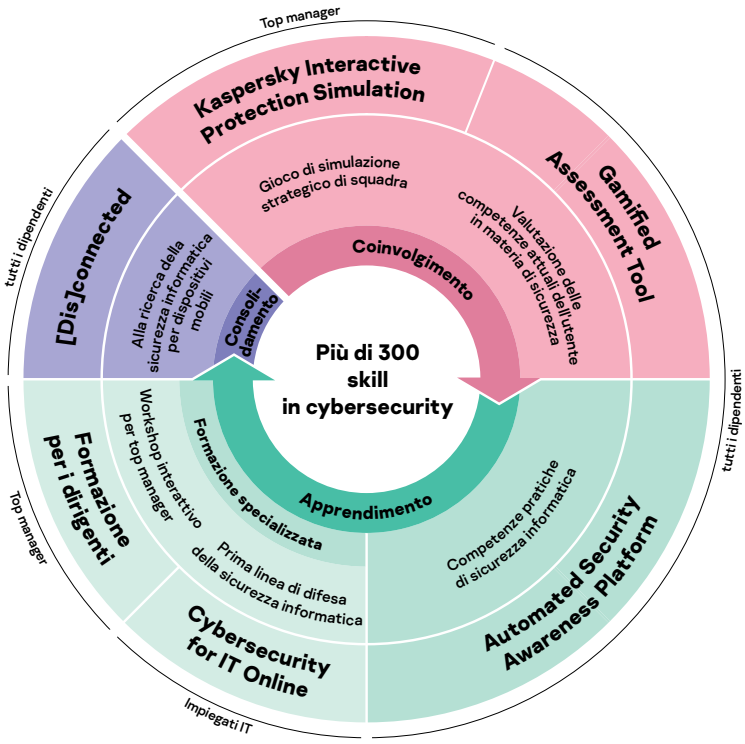
Solida competenza nel campo della cybersecurity
Oltre vent'anni di esperienza nel campo della sicurezza informatica tradotti nella competenza su cui si basano i nostri prodotti

Formazione che modifica il comportamento dei dipendenti a ogni livello dell'organizzazione
Il nostro corso di formazione basato sulla gamification garantisce coinvolgimento e motivazione grazie all'istruzione unita al divertimento, mentre le piattaforme di apprendimento aiutano a interiorizzare le competenze di cybersicurezza, per assicurare che le nozioni apprese non vadano perse nel tempo.

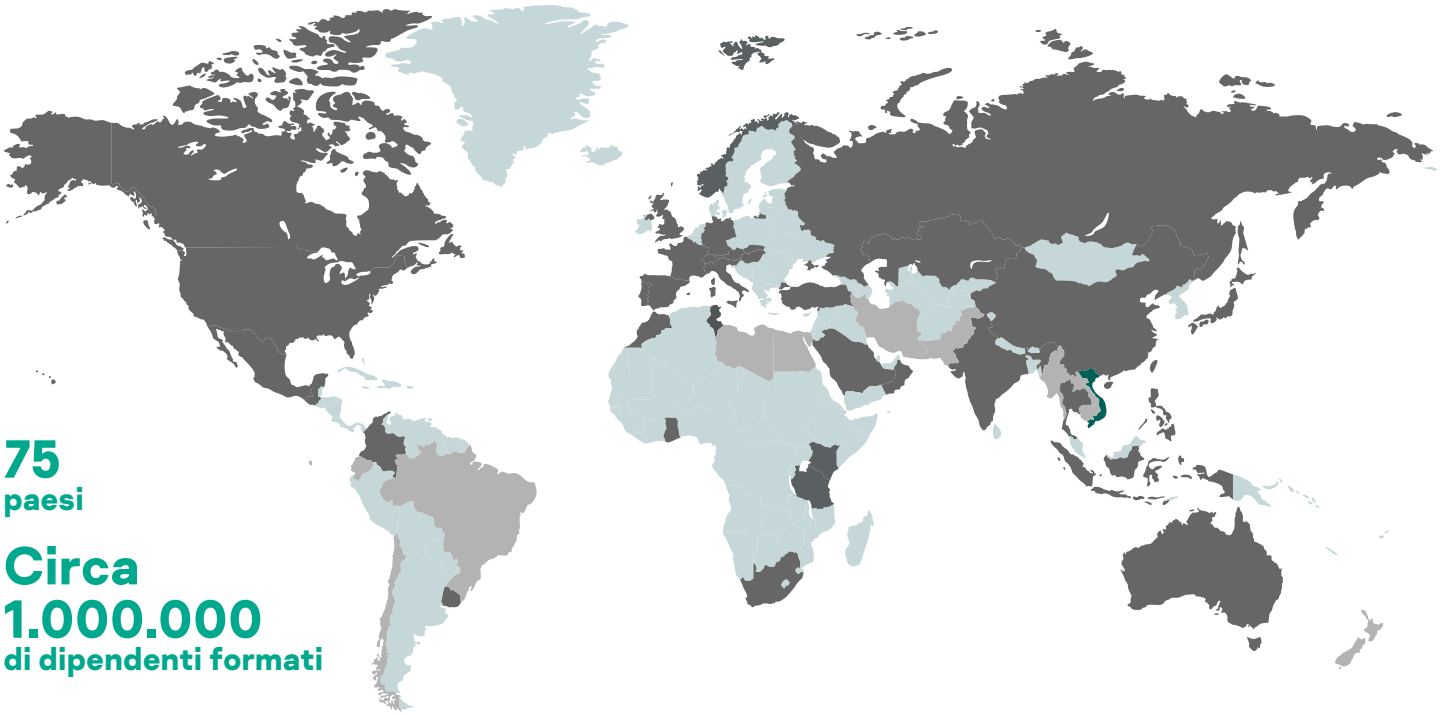
Kaspersky Security Awareness offre una gamma diversificata di soluzioni per rispondere a tutte le esigenze di sicurezza informatica delle aziende e consente a chiunque di acquisire le competenze necessarie, utilizzando le tecniche e le tecnologie di apprendimento più recenti.

Una soluzione di formazione flessibile per tutti

Scegliete un'unica soluzione in grado di soddisfare una specifica esigenza di sicurezza o affidatevi ai nostri pacchetti che garantiscono una formazione mirata in base a tutte le esigenze e priorità. Ulteriori informazioni sui pacchetti sono disponibili qui: kaspersky.com/awareness



Kaspersky Security Awareness worldwide



75
paesi

Circa
1.000.000
di dipendenti formati

Prova gratuita della soluzione Kaspersky ASAP: k-asap.com
Enterprise Cybersecurity: www.kaspersky.it/enterprise
Kaspersky Security Awareness: www.kaspersky.it/awareness
Novità sulla sicurezza IT: business.kaspersky.com

www.kaspersky.it

kaspersky **BRING ON THE FUTURE**