Kaspersky Security Awareness

Creazione di una cultura della cybersecurity a protezione della vostra azienda

kaspersky cybersecurity true to business

Errore umano

è una delle principali minacce: in media, il 64-86% delle violazioni deriva da azioni umane non malevole[1]

Oltre 4,4 milioni di dollari

è il costo medio di un data breach per organizzazione[2]

Requisiti normativi per la security awareness

come parte della conformità: PCI DSS, ISO /IEC 27001, GDPR, NIS 2 e altri richiedono o raccomandano l'adozione di programmi di formazione per la protezione dei dati sensibili

Creare una cultura attenta alla sicurezza porta i suoi frutti

Una recente ricerca di Kaspersky mostra che oltre l'85% dei dipendenti che completano la formazione sulla security awareness riferiscono una maggiore vigilanza e cautela: un cambiamento comportamentale che contribuisce a prevenire gli incidenti.

Il 92%

degli utenti consiglierebbe Kaspersky Security Awareness ad altri

3 milioni

di dipendenti hanno completato con successo i nostri programmi di formazione

Oltre 160

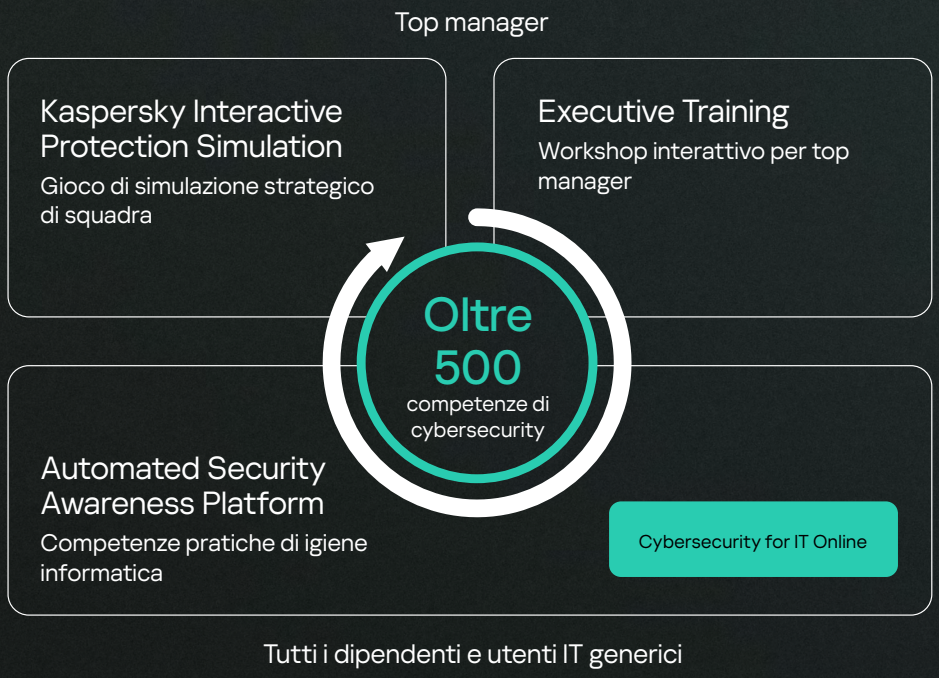
Paesi in cui le organizzazioni proteggono i dipendenti con le nostre soluzioni di formazione

Un approccio efficace per ridurre i rischi informatici legati al fattore umano

Promuovete la cultura di sicurezza informatica in tutta l'organizzazione, grazie ad una strategia basata su una solida cybersecurity awareness e su competenze pratiche per ridurre il numero di incidenti causati da errore umano. Il modo migliore per limitare questi incidenti è attraverso un programma di formazione strutturato che combini contenuti pertinenti e aggiornati con i metodi e le tecnologie di apprendimento più recenti.

Soluzioni Kaspersky Security Awareness

Kaspersky Security Awareness consente alle aziende di ogni dimensione in tutto il mondo di migliorare le competenze informatiche dei propri dipendenti e promuovere una cultura in cui la sicurezza è una responsabilità di tutti. Poiché una modifica sostenibile del comportamento richiede tempo, il nostro approccio prevede la creazione di un ciclo di apprendimento continuo che si avvale di vari strumenti e materiali di supporto: Kaspersky Interactive Protection Simulation, Executive Training, Automated Security Awareness Platform e Cybersecurity for IT Online.



Perché i clienti scelgono Kaspersky Security Awareness

Competenze e consapevolezza per individuare e rispondere alle minacce reali

Attingendo a quasi 30 anni di esperienza di Kaspersky nel campo della cybersecurity e della threat intelligence in tempo reale, creiamo contenuti formativi altamente pertinenti in materia di cybersecurity. Con l'emergere di nuove minacce, i nostri contenuti formativi si evolvono, contribuendo a garantire che i dipendenti siano sempre preparati.

Apprendimento interattivo accessibile

La nostra formazione si basa su un approccio didattico interattivo, caratterizzato da una struttura chiara e logica che aiuta i dipendenti a collegare le nozioni apprese alle attività quotidiane, migliorando la comprensione, la memorizzazione e l'applicazione pratica.

Cambiamento comportamentale duraturo

La nostra metodologia rafforza le nuove competenze, offre una motivazione costante e contribuisce a integrare l'apprendimento nelle routine aziendali. Il risultato è un cambiamento duraturo nel comportamento.

Coinvolgimento a tutti i livelli

Dai dirigenti che richiedono approfondimenti concreti di alto livello al personale in prima linea che necessita di indicazioni pratiche, forniamo il materiale giusto, nel formato giusto, per ogni tipo di audience.

1 Kaspersky Human Factor 360 Report, Cybersecurity Ventures, Verizon Data Breach Reports
2 Cost of a Data Breach Report 2025, IBM

Kaspersky Automated Security Awareness Platform: i dipendenti come prima linea di difesa

Kaspersky Automated Security Awareness Platform (ASAP) è uno strumento online che fornisce formazione continua, dotando i dipendenti di competenze e conoscenze per individuare e bloccare i vettori di attacco reali.

Realizzato da esperti di altissimo livello, Kaspersky ASAP valorizza le persone e migliora le prestazioni aziendali:

- **Riduzione del numero di incidenti dovuti al fattore umano** e dei conseguenti danni finanziari e di reputazione
- **Riduzione al minimo del rischio di sanzioni per non conformità** tramite supporto ai requisiti normativi
- **Riduzione del tempo e dell'impegno** necessari per gestire i corsi sulla security awareness e alleggerimento del carico di lavoro dei team IT

Kaspersky ASAP è più di un semplice strumento anti-phishing. La formazione fa riferimento alle tecniche del modello MITRE ATT&CK, indicando i vettori di attacco che i dipendenti possono contribuire a prevenire. Alcuni esempi sono:

Tecnica MITRE	Minaccia	Competenze e risultati comportamentali
T1566 - Phishing	E-mail dannose	Riconoscimento e segnalazione di tentativi di phishing
T1585 - Creazione di account	Account/profili falsi	Verifica dell'autenticità prima della condivisione di informazioni
T1199 - Rapporto di fiducia	Abuso della fiducia dei partner	Sviluppo della capacità di verificare richieste sospette
T1091 - Replica tramite supporti multimediali rimovibili	Supporti rimovibili	Comprensione del rischio di malware su dispositivi USB
T1078 - Account validi	Furto di credenziali	Prevenzione di accessi non autorizzati tramite social engineering

Il 95%

dei dipendenti qualificati ora può individuare gli attacchi di phishing

20x

in meno violazioni dei dati grazie alla formazione continua dei dipendenti

Gli argomenti chiave affrontati in ASAP includono, tra gli altri:

- E-mail
- Password e account
- Siti Web e Internet
- Sicurezza del PC
- Dati riservati
- Dati personali
- Protezione fisica dei dati
- GDPR
- Intelligenza artificiale e reti neurali
- Attacchi ai top manager
- Dispositivi mobili
- Social media e strumenti di messaggistica
- Attacchi alla supply chain
- Cybersecurity industriale
- Sicurezza delle carte bancarie e PCI DSS
- Come rispondere agli incidenti
- Vishing

Offrite ai dipendenti i mezzi per diventare essi stessi un livello di protezione aggiuntivo, a fianco degli strumenti tecnici.

Provate ora

1 2025 Kaspersky Automated Security Awareness Platform Research

Contenuti e metodologia efficaci per consolidare e applicare le competenze

Contenuti realizzati da esperti

Contenuti basati su quasi 30 anni di esperienza nel campo della cybersecurity e su un modello di competenze che copre le abilità pratiche ed essenziali in materia di cybersecurity in diversi ambiti.

Varie tipologie di contenuto

Supporto per il consolidamento delle conoscenze attraverso moduli ed esercizi interattivi, casi reali, test, video e simulazioni di phishing in più scenari.

Ampia gamma di opzioni di personalizzazione

Possibilità di aggiungere logo e certificazioni aziendali, arricchire le lezioni con slide, documenti o policy interne, integrare moduli personalizzati SCORM/PDF e adattare la struttura dei test.

Centralità della persona

Progettazione basata sul modo in cui le persone assimilano, memorizzano e applicano le informazioni.

Come funziona

Tutti i membri della vostra organizzazione devono essere consapevoli delle minacce per la sicurezza informatica, ma il livello di conoscenza richiesto varia a seconda del ruolo e del profilo di rischio. È proprio su questo punto che la formazione standardizzata si rivela inadeguata. La nostra piattaforma aiuta i team a sviluppare oltre 500 competenze pratiche, a raggruppare il personale in modo semplice e ad assegnare la formazione più adatta a ciascun partecipante con pochi clic, utilizzando i seguenti componenti.

Corso principale

Acquisizione di conoscenze approfondite attraverso microlezioni organizzate per livello di complessità.

Corso rapido

Adempimento dei requisiti di conformità per la formazione sulla cybersecurity o aggiornamento delle conoscenze attraverso corsi audio-video brevi e molto coinvolgenti.

Simulatore di phishing

Simulazioni di attacchi di phishing, durante e dopo la formazione, per testare la capacità dei dipendenti di resistere ai cyberattacchi.

Piano delle lezioni

Blocchi con diversi tipi di attività per favorire al massimo la memorizzazione

Soluzione facile da gestire per le organizzazioni di qualsiasi dimensione

Procedura di onboarding semplice

Registrazione online con accesso demo per un massimo di cinque utenti per due mesi. Sono inclusi supporto online e guida su "come iniziare".

Automazione totale

I moduli di formazione, i test e le simulazioni di phishing vengono assegnati automaticamente, in base alle impostazioni del gruppo di formazione.

Gestione proattiva dei rischi legati al fattore umano

La perfetta integrazione con Kaspersky SIEM e XDR, unita alle API per l'integrazione con applicazioni di terze parti, consente di ottenere un quadro completo del comportamento dei dipendenti e assegnare i corsi di formazione sulla base di eventi di sicurezza reali direttamente dalla console.

Supporto multi-tenant e ruoli amministrativi flessibili

È ideale per le organizzazioni con filiali e team distribuiti, poiché consente una supervisione centralizzata delegando al contempo la gestione agli amministratori locali.

Raggruppamento automatico degli utenti in base a regole personalizzate predefinite

Organizzazione per ruolo, dipartimento o profilo di rischio.

Reportistica dettagliata

Le dashboard forniscono dati essenziali con visualizzazioni dettagliate su progressi, ritardi o prestazioni insufficienti per ciascun dipendente, oltre a un report in formato PDF pronto per l'invio alla direzione con un solo clic.

Implementazione flessibile

Disponibile come piattaforma SaaS o installazione locale

Iscrizione semplice e immediata

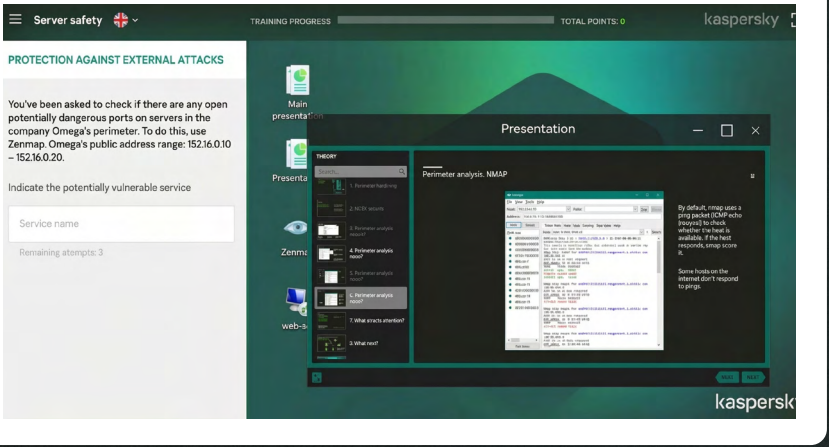
È integrabile con Active Directory e SSO.

Cybersecurity for IT Online

Cybersecurity for IT Online (CITO) è un programma di formazione interattivo che consente a specialisti del service desk, amministratori di sistema e membri non specializzati dei team di sicurezza IT di acquisire competenze pratiche per individuare cyberattacchi nascosti in normali incidenti sui PC, raccogliere dati pertinenti e agire come prima linea di difesa della cybersecurity.

Competenze pratiche per incident response di primo livello:

- Informazioni per individuare, analizzare e reagire a malware, programmi potenzialmente indesiderati, exploit e attacchi di phishing
- Applicazione di strumenti e tecniche concreti per rafforzare la sicurezza dell'infrastruttura IT e condurre indagini sugli incidenti in modo efficace
- Sviluppo di competenze nell'analisi dei log, nella raccolta di prove digitali e nelle indagini sulle minacce
- Formazione per la protezione di server e Active Directory attraverso l'ottimizzazione della sicurezza, la configurazione di criteri e il monitoraggio



Il programma è articolato in sei moduli, ciascuno con teoria concisa, consigli pratici e da 4 a 13 esercizi incentrati su strumenti reali di sicurezza IT e attività quotidiane.

Software malevolo	Programmi potenzialmente indesiderati ed exploit	Sicurezza dei server
Concetti di base sulle investigation	Phishing e open source intelligence (OSINT)	Sicurezza Active Directory

Kaspersky Executive Training

Promuovete una cultura della sicurezza guidata dai manager mostrando come le decisioni dirigenziali influiscono direttamente sul rischio, sulla conformità normativa e sulla resilienza organizzativa a lungo termine.

Kaspersky Executive Training è un workshop in tempo reale per leader aziendali e top manager che illustra il significato dell'attuale panorama delle minacce per le aziende, le azioni da intraprendere in caso di cyberattacco e molto altro. Oltre ai principi fondamentali della cybersecurity, i partecipanti acquisiranno conoscenze critiche sulla redditività degli investimenti in sicurezza, permettendo ai top manager di collegare protezione e prestazioni aziendali. È consigliabile integrare questo corso di formazione con KIPS.

Aspetti critici della cybersecurity in ambito aziendale, in un linguaggio chiaro, accessibile e non tecnico:

- Acquisizione di conoscenze sulla cybersecurity come parte integrante di un sistema globale
- Valutazione dell'impatto dei rischi informatici sulle operazioni aziendali e delle relative modalità di gestione
- Comprensione del ruolo dei senior manager nella governance della cybersecurity

Kaspersky Interactive Protection Simulation (KIPS): la cybersecurity dalla prospettiva aziendale

KIPS aumenta la consapevolezza dei rischi e delle sfide legati all'utilizzo di ogni tipo di sistema IT e processo aziendale. Si tratta di un gioco di squadra interattivo della durata di due ore rivolto a senior manager, esperti di sistemi aziendali e professionisti IT. Gli scenari specifici per settore consentono ai partecipanti di confrontarsi con le moderne tecniche di attacco individuate dagli esperti di Kaspersky nel corso di campagne attive, tra cui attacchi alla supply chain, sfruttamento degli accessi di terze parti, social engineering o malware. Lavorando con vincoli di tempo e di budget, i team devono elaborare strategie, prevedere l'impatto degli incidenti di sicurezza e reagire in modo efficace per salvaguardare le prestazioni e il fatturato dell'azienda.

- Definizione di un'intesa comune tra i decision maker
- Visualizzazione dei rischi per la cybersecurity e correlazione diretta con ricavi e operazioni
- Coinvolgimento dei team nelle tematiche di cybersecurity e promozione di una cultura della sicurezza

KIPS Live

Un'attività divertente che può essere organizzata come evento a sé stante o come sessione nell'ambito di una conferenza, un seminario o un evento aziendale già in programma.

- Fino a 100 partecipanti, 4-5 persone per team
- Facilitatore e assistente alla formazione in loco

KIPS online

La versione online è ideale per le organizzazioni globali o le attività pubbliche. Può anche essere utilizzata insieme a KIPS Live per includere team remoti all'evento in loco.

- Fino a 300 team (1.000 partecipanti) da qualsiasi parte del mondo

Opzioni di personalizzazione di KIPS

- Tabelloni, schede e numeri da tavolo co-branded o personalizzati con il logo del cliente
- Uno scenario esclusivo, realizzato in collaborazione con Kaspersky, in grado di riprodurre la rete aziendale, gli incidenti passati o le minacce specifiche del settore

14 scenari dei settori industriali (ne vengono costantemente aggiunti)

- Aeroporto
- Azienda
- Banca
- Settore Oil & Gas
- Trasporti
- Centrali elettriche
- Impianti idrici
- Pubblica amministrazione locale
- Settore petrolchimico
- Riserve petrolifere
- Piccole e medie imprese
- Telecomunicazioni
- Attribuzione tecnica
- IT

Creazione di una cultura della cybersecurity

La vera cyber resilienza non dipende solo dai criteri e dalle tecnologie, ma dalla cultura. E la cultura è plasmata dai comportamenti delle persone, dalla leadership dei dirigenti, dalla progettazione dei processi e da come la tecnologia rende possibile tutto ciò:

- Persone e comportamento
- Leadership e cooperazione
- Integrazione operativa
- Security Enablement & Readiness

Una cultura sostenibile della cybersecurity si costruisce grazie a un impegno costante. Abbiamo quindi sviluppato un approccio sistematico basato su cinque fasi fondamentali in cui è possibile utilizzare le soluzioni Kaspersky Security Awareness.

A che livello è la cultura della cybersecurity nella vostra azienda?

0 Frammentata
Rischio: l'assenza di strutture e di procedure di base crea un alto livello di vulnerabilità. Anche un incidente di lieve entità può portare a serie conseguenze.

1 Consapevole e reattiva
Rischio: vengono seguite solo regole espressamente prescritte. In situazioni non standard, i dipendenti agiscono secondo il proprio giudizio.

2 Gestita
Rischio: il numero di incidenti è in diminuzione, ma il sistema rimane vulnerabile a scenari più complessi.

3 Integrata
Rischio: i processi sembrano validi, ma se la cultura della cybersecurity non funziona come sistema auto-regolante, resta un "rischio di ritardo".

4 Resiliente
Risultato: il numero e il livello di criticità degli incidenti continuano a diminuire. L'organizzazione può adattarsi rapidamente al panorama delle minacce in continua evoluzione.

Quando la sicurezza non è più una semplice campagna e diventa una cultura, i rischi diminuiscono: e i risultati non tardano ad arrivare.

CISO

Servizi di Customer Engagement

Iniziate a costruire una cultura della cyber resilienza, allineando persone, processi e tecnologie con Kaspersky ASAP.

Provate ora

Kaspersky Security Awareness

Consapevoli dei rischi.
Al sicuro dalle minacce.

www.kaspersky.it

#kaspersky
#cybersecuritytruetobusiness