Competenze di sicurezza informatica per i dipendenti di ogni livello

Kaspersky Security Awareness

kaspersky bring on the future

Ulteriori informazioni sono disponibili sul sito kaspersky.it/awareness

Kaspersky Security Awareness

Costruite una cultura della cybersecurity in tutta la vostra organizzazione

Oltre l'80% di tutti gli incidenti informatici è riconducibile a errori umani. Creando una cultura di comportamenti informatici sicuri, basata su abilità e consapevolezza di cybersecurity diffuse in tutta l'azienda, è possibile ridurre la superficie d'attacco e il numero di incidenti da gestire. Il modo migliore per raggiungere i cambiamenti nel comportamento che risolvono il problema del "fattore umano" nella sicurezza informatica è attraverso una formazione che utilizzi le tecniche e le tecnologie più recenti nell'educazione degli adulti e fornisca i contenuti più pertinenti e aggiornati.

Il fattore umano è l'elemento più vulnerabile della cybersecurity

Le soluzioni di cybersecurity si stanno rapidamente sviluppando e adattando alle minacce complesse, rendendo più difficile la vita dei cybercriminali, che prendono dunque di mira l'elemento più vulnerabile della catena: il fattore umano.

Il **55% delle aziende** segnala violazioni dei criteri di sicurezza IT da parte dei propri dipendenti*

Il **43% delle piccole aziende** segnala che le violazioni dei criteri di sicurezza IT da parte dei dipendenti causano incidenti di sicurezza**

Le fughe di dati sono il problema di sicurezza più comune, spesso **causato dai dipendenti** (22%) e dagli autori degli attacchi (23%).*

Il **30% dei dipendenti** ammette di condividere con i colleghi i dati di accesso e le password del proprio PC di lavoro***

Il **23% delle organizzazioni** non applica alcuna regola o criterio di cybersecurity relativamente all'archiviazione dei dati aziendali***

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

Kaspersky Security Awareness è una soluzione collaudata ed efficiente, con una lunga storia di successi a livello internazionale. Utilizzata da aziende di ogni dimensione per la formazione di oltre un milione di dipendenti in più di 75 paesi, la soluzione combina gli oltre 25 anni di esperienza di Kaspersky nel campo della cybersecurity con le approfondite competenze nella formazione per gli adulti.

Le soluzioni di formazione altamente coinvolgenti ed efficaci aumentano la consapevolezza della cybersecurity nel vostro staff, affinché tutti contribuiscano alla sicurezza informatica dell'azienda. Poiché le modifiche comportamentali sostenibili richiedono tempo, il nostro approccio si basa sulla creazione di un ciclo di apprendimento continuo con più componenti.

Ciclo di apprendimento continuo

1 **Coinvolgimento / motivazione**
- Perché ne ho bisogno?
- Cognizione

2 **Punto di partenza**
- Sono consapevole?
- Cosa so e dove sono le falle?

3 **Apprendimento**
- Micro apprendimento
- Apprendimento continuo
- Adattabilità

4 **Consolidamento**
- Ho capito bene?
- Me lo ricordo ancora?
- Ho agito conformemente?

Principali elementi distintivi del programma

Solida competenza nel campo della cybersecurity

Oltre venticinque anni di esperienza nel campo della cybersecurity tradotti nella competenza che dà fondamento ai nostri prodotti

Formazione che modifica il comportamento dei dipendenti in ogni livello dell'organizzazione

Il nostro corso di formazione basato sulla gamification garantisce il coinvolgimento e la motivazione dell'edutainment, mentre le piattaforme di apprendimento aiutano a interiorizzare le competenze di cybersecurity, per assicurare che le nozioni apprese non vadano perse nel tempo.

* "IT Security Economics 2022", Kaspersky

** Report "IT Security Economics 2021", Kaspersky.

*** "Sorting out a Digital Clutter". Kaspersky Lab, 2019.

I dipendenti commettono errori. Le aziende perdono denaro...

52.887 dollari
per azienda Enterprise
Il costo medio di un cyberattacco causato dall'uso inappropriato delle risorse IT da parte dei dipendenti*

Il 30%
delle violazioni malware
si verifica tramite e-mail con allegati e collegamenti falsi**

Il 79%
dei dipendenti
ha ammesso di aver svolto almeno un'attività rischiosa durante l'anno pur essendo consapevole dei rischi***

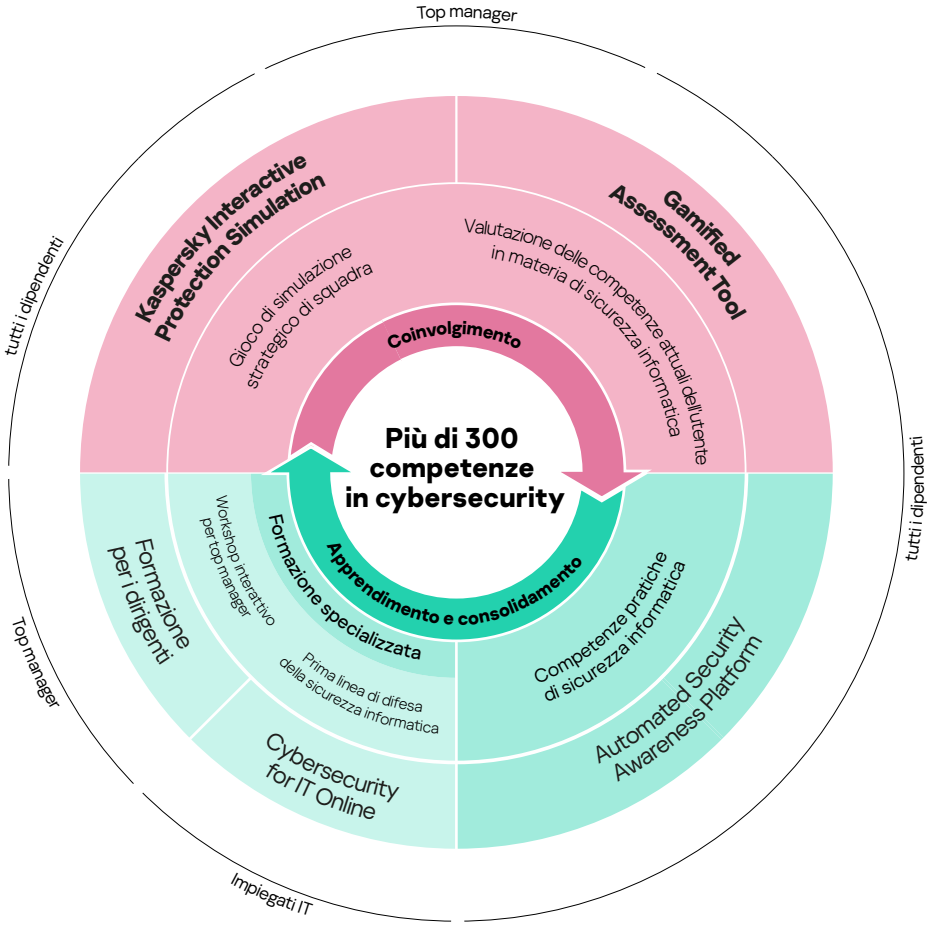
164 dollari
per record
Il costo globale medio per le violazioni che coinvolgono tra 2.200 e 102.000 record****

Il 42% dei partecipanti
impiegato in aziende con più di 1.000 dipendenti
ha dichiarato che la maggior parte dei corsi di formazione frequentati era inutile e non interessante*****

Alimentare la motivazione per una security awareness efficace

Modificare il comportamento dei dipendenti rappresenta la vostra principale sfida a livello di cybersecurity. Le persone sono generalmente poco motivate nell'acquisire nuove abilità e modificare le proprie abitudini, ecco perché molti tentativi di formazione finiscono per trasformarsi un una mera formalità. Un training efficiente si compone di più parti, tiene in considerazione le particolarità della natura umana e la capacità di assimilare le competenze acquisite. In quanto esperti di cybersecurity, noi di Kaspersky conosciamo bene i comportamenti informatici più adeguati da mettere in atto. Affidandoci alla nostra esperienza e alle nostre competenze, abbiamo sfruttato tecniche e metodi di apprendimento che immunizzino i dipendenti dei nostri clienti dagli attacchi, pur dando loro la libertà di lavorare senza restrizioni.

Formati di apprendimento diversi, per i vari livelli della struttura organizzativa



* "IT Security Economics 2022", Kaspersky

** Data Breach Investigation Report (Report sull'indagine sulle violazioni dei dati) 2022

*** «Balancing Risk, Productivity, and Security», Delinea 2021

**** Report "Cost of a Data Breach" (Report sul costo di una violazione dei dati), 2022. IBM

*****Capgemini "The digital talent gap"

Soluzioni Kaspersky Security Awareness

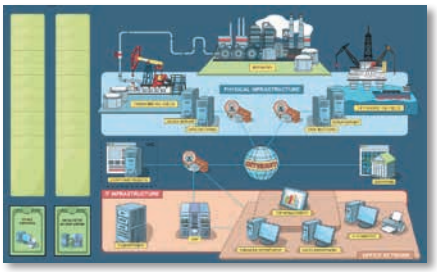
Coinvolgimento e motivazione

I dipendenti non sempre hanno voglia di seguire corsi di formazione obbligatori e molti ritengono l'argomento della cybersecurity troppo complicato o noioso, oppure pensano che non li riguardi affatto. Se manca la motivazione, è improbabile che il processo di apprendimento dia esiti positivi. Un'altra sfida per i formatori è coinvolgere i dirigenti aziendali nella formazione, sebbene i loro errori potrebbero costare all'azienda tanto quanto gli errori dei sottoposti. Qui entra in gioco la gamification: è così coinvolgente da essere il modo più efficace per incoraggiare il personale a superare la sua resistenza iniziale all'apprendimento.

Il **76%** dei CEO ammette di ignorare i protocolli di sicurezza per ottenere più rapidamente i risultati desiderati, sacrificando la sicurezza a favore della velocità*.

Il **62%** dei manager ammette che i problemi relativi alla comunicazione sulla sicurezza IT all'interno della propria organizzazione hanno portato ad almeno un incidente di cybersecurity**

Il corso di formazione KIPS si rivolge ai senior manager, agli esperti di sistemi aziendali e ai professionisti del settore IT, per aumentare la loro consapevolezza sui rischi e sulle sfide associate all'uso di sistemi e processi IT di ogni tipo.



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

KIPS è un gioco di squadra interattivo di 2 ore, in grado di stabilire comunicazioni efficaci tra i decision-maker (responsabili Senior, IT e della Cybersecurity) e cambiare la loro percezione della cybersecurity. Tramite un software simula l'impatto reale che il malware e altri attacchi potrebbero avere sui profitti e le performance aziendali. Obbliga i giocatori a pensare in modo strategico, ad anticipare le conseguenze di un attacco e a rispondere adeguatamente, entro i limiti di tempo e di budget forniti. Ogni decisione ricade su tutti i processi aziendali. L'obiettivo principale è evitare le interruzioni. Vince la squadra che completa il gioco con il maggior profitto, avendo individuato e analizzato tutte le insidie nel sistema della cybersecurity e avendovi adeguatamente risposto.

13 scenari dei settori industriali (ne vengono costantemente aggiunti)

Ogni scenario dimostra il ruolo della cybersecurity in termini di continuità operativa e redditività aziendale, evidenziando le sfide e le minacce emergenti, oltre agli errori tipici che le organizzazioni commettono durante il processo di costruzione della loro cybersecurity. Gli scenari promuovono inoltre la cooperazione fra il team commerciale e quello della sicurezza, che insieme mantengono stabili le operazioni e la sostenibilità, contro le cyberminacce.

KIPS è disponibile in due modalità

L'opzione molto popolare KIPS Live crea un'atmosfera indescrivibile di entusiasmo grazie alla competitività faccia a faccia in sede. È un ottimo strumento per coinvolgere e sviluppare una cultura della cybersecurity all'interno di un'organizzazione.

Nella versione KIPS Online gli utenti possono interagire con un numero elevato di partecipanti ovunque si trovino. Perfetto per organizzazioni globali o attività pubbliche, KIPS Online può essere unito a KIPS Live per aggiungere team remoti all'evento in sede.

- Fino a 300 team (= 1.000 partecipanti) contemporaneamente, da qualsiasi parte del mondo.
- I vari team possono scegliere una lingua diversa per l'interfaccia di gioco.
- Dalla libreria i clienti possono personalizzare gli scenari preinstallati determinando il numero e il tipo degli attacchi sferrati durante il gioco.
- Un altro vantaggio della versione online è che consente di visualizzare le statistiche delle scelte dei partecipanti, ottenere dati sulle azioni dei team in determinate situazioni e confrontare le azioni dei partecipanti in relazione alla sessione di gioco precedente.

KIPS per le aziende

I clienti con una licenza che consente loro di utilizzare KIPS senza limitazioni durante il periodo di licenza possono adattare le impostazioni predefinite o personalizzare lo scenario a ogni sessione di gioco, scegliendo e combinando diversi attacchi dalla libreria. Grazie a questa funzionalità è possibile rendere il gioco ancora più interessante perché sempre diverso.

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritysgreatest-insider-threat-is-in-thec-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speakfluent-infosec-2023/

Punto di partenza

Le persone sono spesso ignare del proprio livello di incompetenza, il che le rende particolarmente vulnerabili. Vanno messe alla prova e devono ricevere un feedback chiaro e dettagliato sul proprio livello di competenza in cybersecurity, affinché la formazione continua sia efficace. Inoltre, questo assicura che non si perda tempo su argomenti che sono già familiari.

Gamified Assessment Tool: un modo rapido e divertente di verificare le abilità dei dipendenti a livello di cybersecurity

Kaspersky Gamified Assessment Tool (GAT) vi permette di valutare rapidamente il livello di conoscenza di ciascun dipendente in materia di cybersecurity. I suo approccio coinvolgente e interattivo è diametralmente opposto ai noiosi strumenti di valutazione classici. Il dipendente impiegherà solo 15 minuti per considerare le 12 situazioni quotidiane collegate alla cybersecurity, valutando se le azioni del personaggio siano rischiose oppure no, ed esprimendo il livello di fiducia nelle proprie risposte.

Una volta completato, l'utente riceve un certificato con un punteggio che riflette il proprio livello di consapevolezza della cybersecurity. Inoltre, riceverà un feedback su ogni argomento, con spiegazioni e consigli utili.

L'approccio videoludico di GAT motiva i dipendenti, senza mancare di evidenziare eventuali falle nelle loro competenze mentre risolvono le situazioni legate alla cybersecurity. Questo strumento si rivela utile anche per i reparti IT/HR, per ottenere un quadro più chiaro dei livelli di consapevolezza informatica all'interno dell'azienda e per compiere un primo passo verso una più ampia campagna di formazione.

Apprendimento

La nostra piattaforma di apprendimento online è il fulcro del programma orientato alla consapevolezza. Contiene **più di 300 competenze di cybersecurity** e tratta tutti i principali argomenti di cybersecurity. Ogni lezione presenta casi ed esempi reali, così che i dipendenti percepiscano un legame con ciò che devono affrontare nel loro lavoro quotidiano. Le abilità apprese potranno essere messe immediatamente in pratica, anche dopo la prima lezione.

Kaspersky Automated Security Awareness Platform: efficienza e facilità di gestione della formazione per organizzazioni di qualsiasi dimensione

Kaspersky ASAP è uno strumento online efficiente e semplice da utilizzare, che forma le abilità di cybersecurity dei dipendenti, motivandoli a comportarsi nel modo corretto.

Sebbene la formazione risponda alle esigenze di consapevolezza sulla sicurezza di tutte le aziende, la gestione automatizzata si rivolge soprattutto a chi non dispone di risorse di gestione della formazione dedicate.

Vantaggi chiave:

- **Semplicità grazie all'automazione totale:** il programma di formazione è semplicissimo da avviare, configurare e monitorare. Inoltre, la gestione è completamente automatizzata, senza alcun intervento da parte degli amministratori. La piattaforma stessa crea un programma di formazione per ciascun gruppo di dipendenti, fornendo automaticamente un apprendimento a intervalli attraverso una combinazione di tipologie di formazione.
- **Facilità di utilizzo per amministratori...:** gestione automatizzata della piattaforma, sincronizzazione con AD (Active Directory), SSO (Single Sign-On), Open API (la capacità di interagire con soluzioni di terze parti), una dashboard intuitiva, onboarding online durante la prima visita, una sezione di domande frequenti e suggerimenti: tutto questo rende la gestione pratica ed efficiente.
- **...e studenti:** struttura chiara delle lezioni, lezioni di breve durata, esempi reali, un'interfaccia intuitiva, promemoria tramite e-mail, possibilità di tornare e ripetere le lezioni se necessario, interfaccia ottimizzata per PC o dispositivi mobili: tutto rende piacevole, interessante ed efficace il processo di apprendimento.

Kaspersky ASAP: uno strumento online semplice da gestire, che incrementa gradualmente le competenze di cybersecurity dei dipendenti

Argomenti affrontati in ASAP:

- 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
- Dati personali
- Sicurezza delle carte bancarie e PCI DSS
- Doxing
- Sicurezza delle criptovalute
- Sicurezza delle informazioni durante il lavoro in remoto
- Legge federale russa 152-FZ

Corso rapido ASAP

Versione breve del corso di formazione in formato audio/video.

- Teoria interattiva
- Video
- Test

Kaspersky ASAP è una soluzione multilingue

ASAP è ideale per MSP e xSP – i servizi di formazione per più aziende possono essere gestiti tramite un unico account e sono disponibili abbonamenti con licenze mensili.

La versione completa di Kaspersky ASAP è disponibile all'indirizzo https://asap.kaspersky.com/it. Scoprirete quanto è facile configurare e gestire il proprio programma di formazione orientato alla consapevolezza sulla sicurezza aziendale!

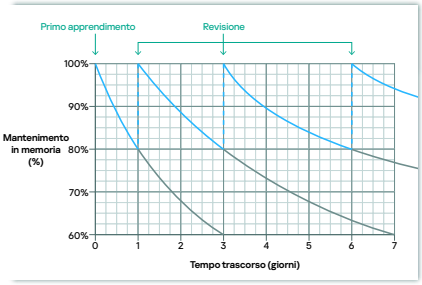
Consolidamento

Il consolidamento è una parte fondamentale del programma di formazione ed è necessario per rafforzare le competenze e le abilità acquisite durante l'apprendimento.

Il miglior modo per trasformare in abitudini le abilità apprese è metterle in pratica. Certo, si può anche imparare per esperienza, dai propri errori... Ma nel campo della cybersecurity, imparare dai propri errori può costare molto caro.

Usando un percorso di formazione basato sulla gamificatiopn è possibile creare una situazione in tempo reale e verificare le conseguenze senza danneggiare sé stessi o l'azienda.

Il 70%
di ciò che si apprende
viene dimenticato dopo un solo giorno, con i programmi formativi tradizionali



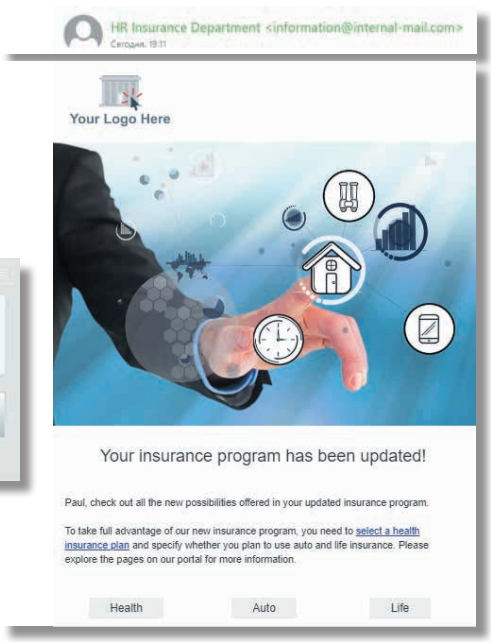
- **Efficienza dell'apprendimento:** i contenuti del programma sono strutturati in modo tale da supportare l'apprendimento incrementale, basato sul rafforzamento continuo dei concetti appresi. La metodologia adottata riflette le caratteristiche peculiari della memoria umana, al fine di garantire il perfetto mantenimento delle conoscenze acquisite e la successiva applicazione pratica delle competenze.
- **Personalizzazione:** è facile modificare l'aspetto del programma di formazione, sostituendo il logo Kaspersky con il logo della vostra azienda nel portale di amministrazione e per gli studenti e nelle e-mail della piattaforma, personalizzando i certificati e aggiungendo contenuti personali a qualsiasi lezione.
- **Apprendimento flessibile:** scegliete l'opzione di formazione dei dipendenti più adatta a voi tra un corso rapido di livello base, che consente di soddisfare tempestivamente i requisiti normativi per la formazione sulla cybersecurity e aggiornare le conoscenze, oppure un corso principale suddiviso in livelli di complessità per lo sviluppo di competenze di cybersecurity più approfondite e dettagliate.
- **Licenza flessibile** (per MSP): il modello di licenza per utente può partire da un minimo di 5 licenze e più aziende possono essere gestite da un singolo account.

Campagne di phishing simulate

Gli attacchi di phishing simulati possono essere utilizzati prima, durante e dopo la formazione, per testare la capacità dei dipendenti di resistere agli attacchi informatici e consentire a dipendenti e manager di constatare i vantaggi della formazione.

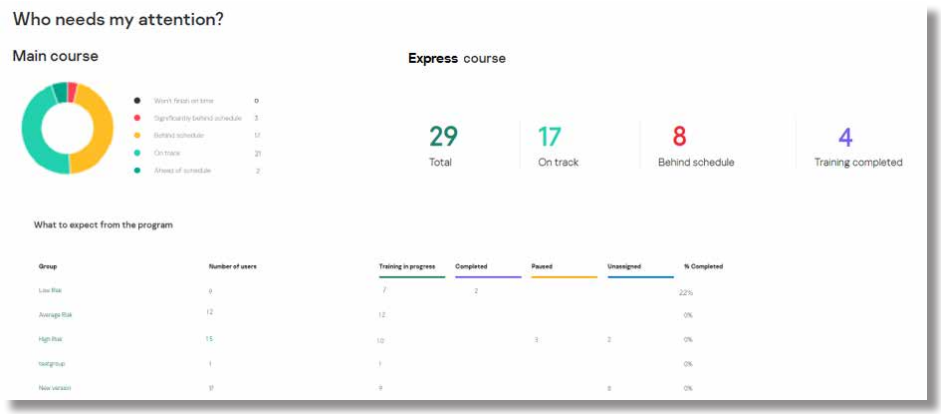
Lezioni interattive

Attacchi di phishing simulati



Tracciamento dei risultati

Potete seguire il progresso dei dipendenti dalla dashboard e valutare così l'avanzamento dell'intera azienda e di tutti i gruppi con una sola occhiata. Potete anche ottenere dettagli sul livello dei singoli dipendenti.



Formazione specializzata

Specialisti IT generici: gli addetti all'helpdesk e gli altri dipendenti con competenze tecniche sono spesso esclusi dalla formazione perché i programmi di consapevolezza standard non sono sufficienti per loro. Al contempo, le aziende non vogliono che queste figure si specializzino nella cybersecurity perché ciò richiederebbe un inutile e corposo investimento di tempo e risorse.

Siamo lieti di annunciare una formazione che risponde perfettamente all'esigenza di essere non eccessivamente approfondita come quella riservata agli esperti, ma comunque più avanzata della formazione riservata ai normali dipendenti.

Moduli di formazione CITO:

- Software malevolo
- Programmi e file potenzialmente indesiderati
- Concetti di base sulle investigation
- Phishing incident response
- Sicurezza dei server
- Sicurezza con Active Directory

Metodo di erogazione dei corsi CITO:

Formato SCORM o cloud

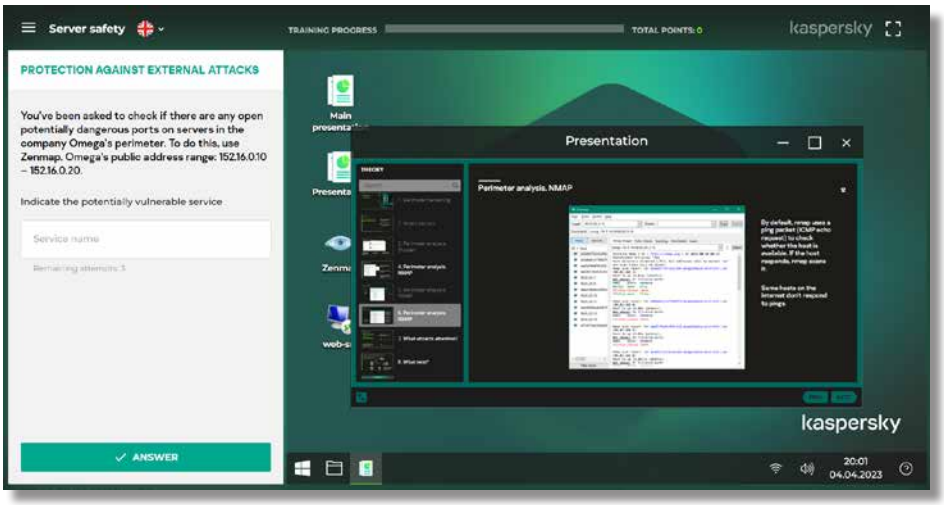
Cybersecurity for IT Online: la prima linea di difesa dagli incidenti

Cybersecurity for IT Online è una formazione interattiva per tutti gli attori coinvolti nell'IT. Costruisce solide abilità di cybersecurity e incident response di primo livello.

Il programma offre ai professionisti IT competenze pratiche per riconoscere un possibile scenario di attacco in un incidente PC apparentemente benigno. Sviluppa inoltre la capacità di in dividuare gli indicatori dannosi, consolidando il ruolo di tutti i membri del team IT come prima linea di difesa per la sicurezza.

CITO insegna anche i concetti di base sulle indagini e come utilizzare gli strumenti e il software di sicurezza IT, e consente ai professionisti IT di acquisire le competenze teoriche, pratiche e basate sull'esercizio necessarie per raccogliere i dati degli incidenti che verranno gestiti dal team della sicurezza IT.

Questa formazione è consigliata a tutti gli esperti IT all'interno della vostra organizzazione, ma in particolare agli addetti ai service desk e agli amministratori di sistema. Il corso è utile anche alla maggior parte dei membri dei team non specializzati in sicurezza IT.



Coinvolgere i dirigenti

I top manager sono tra gli obiettivi più ambiti per i criminali informatici, eppure spesso rappresentano una vera sfida per chi eroga formazione. Tuttavia, senza il loro coinvolgimento e supporto per varie iniziative di cybersecurity è impossibile creare una cultura della cybersecurity all'interno dell'organizzazione.

La cybersecurity ha un ruolo fondamentale nella generazione del fatturato insieme alla gestione dei progetti, agli strumenti finanziari e all'efficienza operativa aziendale. È proprio questo il focus del nostro corso per dirigenti.

Formazione per i dirigenti:

Nel programma di formazione rivolto al personale dirigente, i leader aziendali e i top manager apprendono le basi della cybersecurity attraverso un workshop interattivo o un corso guidato da tutor grazie al quale impareranno a conoscere meglio le minacce informatiche e a proteggersi da esse.

Viene data particolare attenzione agli aspetti finanziari della cybersecurity e alla sostenibilità dell'investimento, offrendo ai top manager una migliore comprensione della relazione tra cybersecurity ed efficienza aziendale. Scopriranno cosa significa l'attuale panorama delle minacce per l'azienda, quali azioni intraprendere in caso di attacco informatico, oltre a una serie di altre informazioni interessanti, pertinenti e utili.

Per ottenere ancora di più da questo corso, è ideale combinarlo con il corso di formazione KIPS. Questo corso di formazione per la dirigenza può essere seguito prima o dopo aver svolto gli scenari KIPS, in base all'approccio alla Security Awareness.

* L'elenco corrente dei moduli è disponibile all'indirizzo cito-training.com

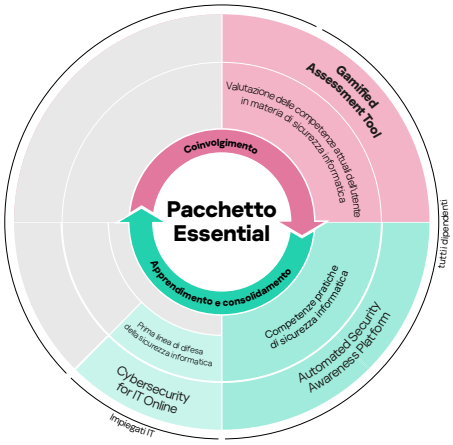
Kaspersky Security Awareness: opzioni di formazione flessibili

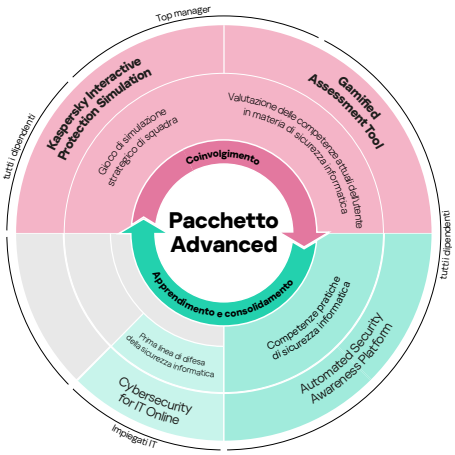
Le soluzioni di formazione Kaspersky sono adatte a tutti i livelli aziendali e possono essere usate singolarmente o insieme. Offriamo inoltre semplici pacchetti su misura per le vostre esigenze.

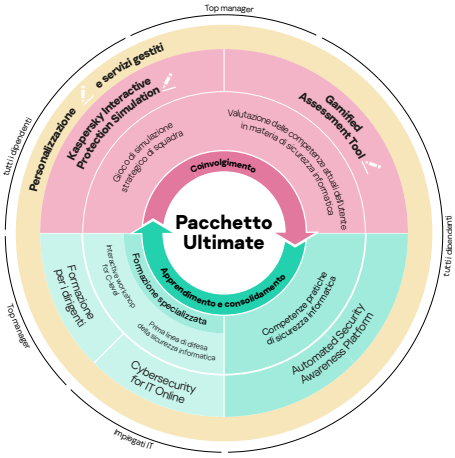
L'opzione essenziale per aumentare la consapevolezza dei dipendenti nei confronti della cybersecurity: semplice da configurare, facile da gestire
Offre un livello base di formazione sulla security per garantire uno svolgimento ottimale delle attività e la compliance ai requisiti normativi o di terze parti per la formazione generale sulla cybersecurity.

Aiuta le aziende più grandi a mantenere la business continuity con una semplice soluzione di formazione 'chiavi in mano'. Supporta tutti i livelli dell'organizzazione e introduce cambiamenti di comportamento includendo ogni singola fase del ciclo di apprendimento.

Offre il massimo livello di consapevolezza sulla cybersecurity, con servizi gestiti e di personalizzazione, in modo che i dirigenti siano ben consapevoli dei potenziali scenari di minaccia, i dipendenti possano contare su competenze di cybersecurity automatiche e il personale IT generico sia in grado di supportare tutti come prima linea di difesa.







La formazione Kaspersky Security Awareness utilizza i metodi di formazione più recenti e le tecniche più avanzate per garantire risultati ottimali. Le nuove soluzioni flessibili possono essere adattate alle vostre esigenze specifiche, senza esclusioni. Maggiori informazioni sono disponibili all'indirizzo kaspersky.it/awareness

Kaspersky Security Awareness: kaspersky.it/awareness
IT Security News: www.kaspersky.it/blog/category/business/

kaspersky.it

kaspersky