Programmi di formazione assistita tramite computer per tutti i livelli della struttura organizzativa

Kaspersky Security Awareness

kaspersky BRING ON THE FUTURE

Maggiori informazioni su kaspersky.it/awareness

Kaspersky Security Awareness

Il modo più efficace per promuovere una cultura sulla cybersafety in tutta l'organizzazione

Oltre l'80% di tutti gli incidenti informatici è riconducibile a errori umani. Una cultura di comportamenti informatici sicuri, basata su abilità e consapevolezza di cybersecurity diffuse in tutta l'azienda, è la chiave per ridurre la superficie d'attacco e il numero di incidenti da gestire. Le aziende spesso faticano a trovare gli strumenti e i metodi adatti per formare adeguatamente i propri dipendenti, migliorando il loro comportamento. Il segreto per ottenere questo risultato è affidarsi a un corso che utilizzi le più recenti tecniche e tecnologie per la formazione rivolta agli adulti, e che 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 52% dei top manager afferma che i dipendenti rappresentano la più grande minaccia per la sicurezza operativa*

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

Il 60% dei dipendenti custodisce dati di natura riservata sul proprio dispositivo aziendale (dati finanziari, database di posta elettronica e così via)***

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 offre una gamma di soluzioni di formazione altamente coinvolgenti ed efficaci, che aumentano la consapevolezza della cybersecurity nel vostro staff, affinché tutti contribuiscano alla sicurezza informatica della vostra 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

Coinvolgimento / motivazione	Punto di partenza	Apprendimento	Consolidamento
– Perché ne ho bisogno? – Cognizione	– Sono consapevole? – Cosa so e dove sono le falle?	– Micro apprendimento – Apprendimento continuo – Adattabilità	– Ho capito bene? – Me lo ricordo ancora? – Ho agito conformemente?

Principali elementi distintivi del programma

Solida competenza nel campo della cybersecurity

Oltre vent'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.

* Report "Weathering the Perfect Storm: Securing the Cyber-Physical Systems of Critical Infrastructure", 2020

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

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

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

1.315.000 dollari
per azienda Enterprise
L'impatto finanziario medio di una violazione dei dati causata dall'uso inappropriato delle risorse IT da parte dei dipendenti*

Il 50%
delle imprese
ha riferito di aver subito minacce direttamente causate dal comportamento inappropriato dello staff, fattore che costituisce la minaccia più comune per la sicurezza IT*

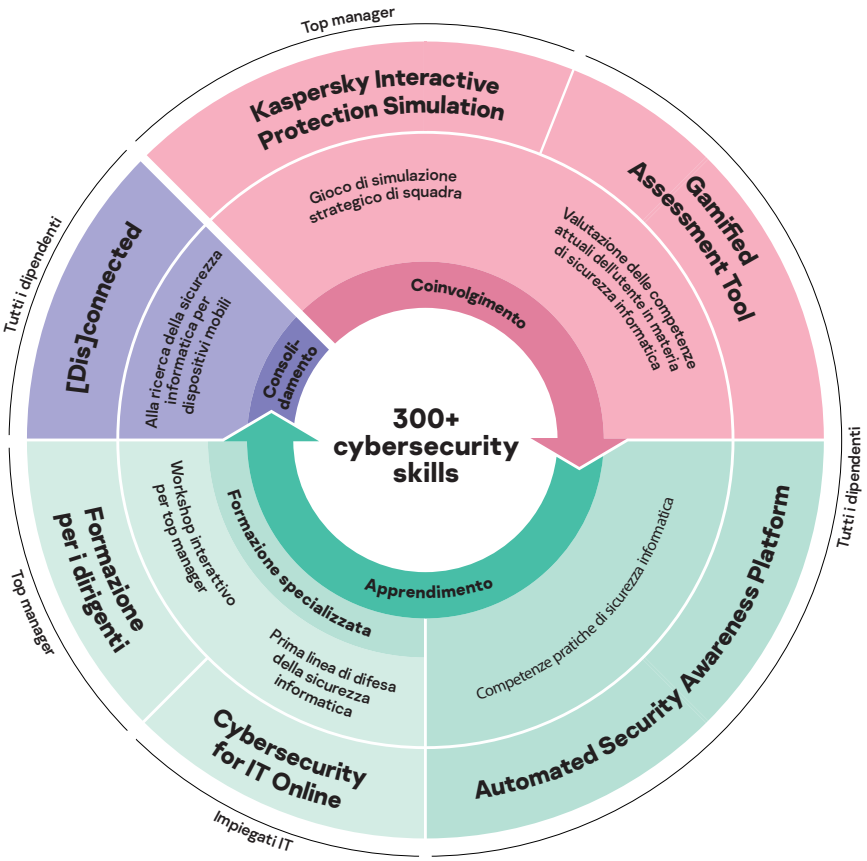
L'86%
delle aziende
ha affermato che almeno una persona ha fatto clic su un collegamento di phishing**

5,01 milioni di dollari
il costo medio per violazione
in seguito ad attacchi BEC (BEC - Business Email Compromise - è un tipo di phishing in cui gli autori degli attacchi dirottano o falsificano account di posta elettronica aziendali legittimi)

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 in 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



* Report "IT Security Economics 2021", Kaspersky
** Report "Cybersecurity Threats Trends" 2021, CISCO
*** Report "Cost of a Data Breach", 2021. IBM

Soluzioni Kaspersky Security Awareness

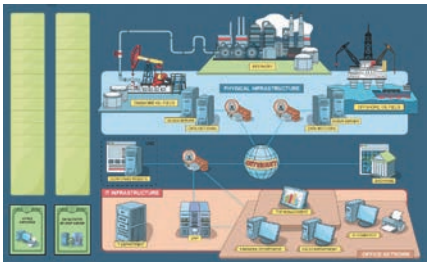
Motivazione

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.

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

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**

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-makers (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.

Personalizzazione degli scenari

Dal terzo trimestre del 2022, per determinati scenari industriali le aziende potranno creare i propri scenari di gioco con diversi attacchi. Utilizzando diverse combinazioni di attacco, le aziende con una licenza aziendale KIPS potranno riprodurre più volte lo stesso scenario industriale.

KIPS Virtual Reality

KIPS Power Station VR è una nuova esperienza immersiva in un ambiente realistico che riproduce nel modo più autentico possibile il funzionamento di una centrale elettrica. La tecnologia consente ai manager di vestire i panni di specialisti della sicurezza delle informazioni. Con una dimostrazione visiva del ruolo della cybersecurity e del relativo impatto sul business, i manager potranno vedere le conseguenze delle loro decisioni IT in una grafica 3D estremamente realistica anziché limitarsi ad avere un'idea astratta.

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.

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 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

Corso rapido ASAP

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

- Teoria interattiva
- Video
- Test

Kaspersky ASAP è una soluzione multilingua

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.

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 plasma 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 crea uno specifico programma di formazione per ciascun gruppo di dipendenti, fornendo un'efficace tipologia di apprendimento in vari formati, che includono moduli di formazione, il rafforzamento delle conoscenze tramite e-mail motivazionali, test e attacchi di phishing simulati.
- **Efficienza:** 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.
- **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.
- **Licenze flessibili** (per Managed Service Provider): il modello di licensing in base al numero di utenti prevede un numero minimo di 5 licenze.

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 asap.kaspersky.com. Scoprirete quanto è facile configurare e gestire il proprio programma di formazione orientato alla consapevolezza sulla sicurezza aziendale!

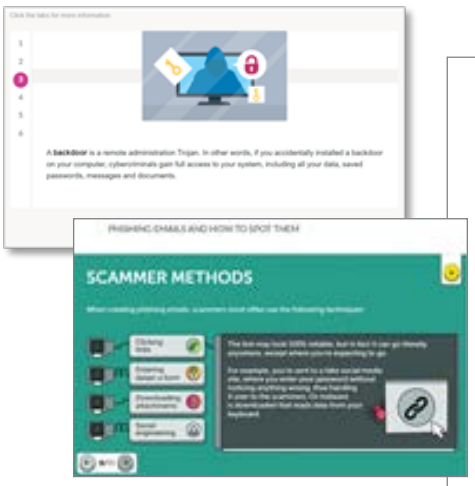
Campagne di phishing simulate

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.

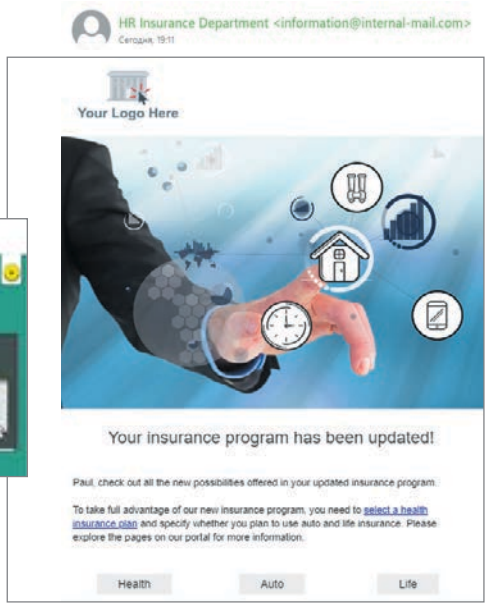
Lezioni interattive

Corso principale

Corso rapido



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.

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 gamification è possibile creare una situazione in tempo reale e verificare le conseguenze senza danneggiare sé stessi o l'azienda.

[Dis]connected: alla ricerca della cybersecurity per dispositivi mobili

[Dis]connected è un gioco narrativo estremamente coinvolgente e dalla grafica accattivante sul tema della cybersecurity per dispositivi mobili che sfida gli utenti a mantenere un equilibrio vita-lavoro, raggiungendo il successo sia in ambito personale che professionale.

Gli elementi della cybersecurity si intrecciano alla trama di gioco, rivelando come le decisioni al riguardo possano portare al conseguimento o al fallimento di tali obiettivi. Ci sono 24 casi da risolvere, che includono argomenti come password e account, e-mail, navigazione Web, social network e servizi di messaggistica, sicurezza del computer e dei dispositivi mobili. Le simulazioni di applicazioni integrate, come servizi di messaggistica o app bancarie, permettono un'esperienza totalmente immersiva.

Al termine del gioco, i giocatori ricevono un riassunto delle loro prestazioni all'interno del progetto, per scoprire se le loro abilità in materia di sicurezza siano sufficienti ad

affrontare le sfide di oggi e di domani.
Il gioco viene eseguito sui cellulari. Una **demo gratuita** è disponibile in Google Play e AppStore: https://kas.pr/mobilestores

Apprendimento avanzato

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

Provate gratuitamente uno dei moduli CITO: cito-training.com

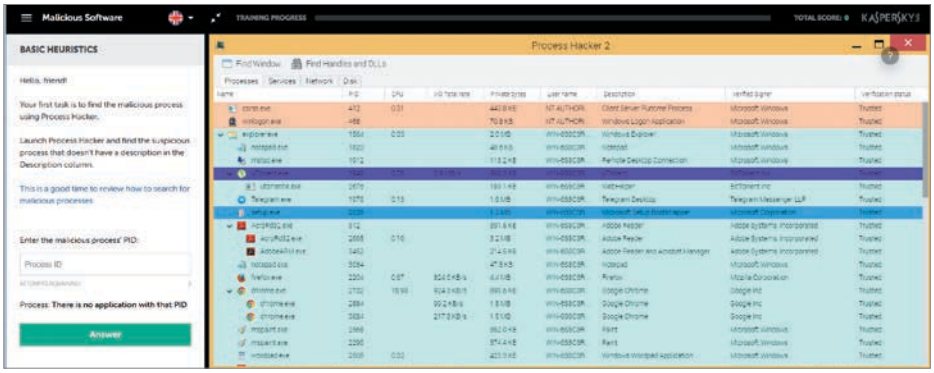
Cybersecurity for IT Online: la prima linea di difesa dagli incidenti

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 individuare 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.



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 di entrate 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 dirigenti: aumentare la resilienza aziendale per la trasformazione digitale

I leader aziendali e i top manager apprendono le basi della cybersecurity attraverso un corso guidato da tutor grazie al quale impareranno a conoscere meglio le minacce informatiche e a proteggersi da esse.

Gli studi dimostrano che esiste un legame diretto tra la velocità e l'efficienza della risposta agli incidenti e il livello di danno che può essere causato da un incidente. Il corso presta 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.

Kaspersky Interactive Protection Simulation (KIPS) può essere utilizzato in aggiunta a questa formazione per consolidare ulteriormente le competenze attraverso esercitazioni pratiche.

Obiettivi del corso

- Condividere le più recenti informazioni sulle moderne minacce informatiche e sui relativi rischi per le aziende
- Consentire a chi usufruisce della formazione di rimanere al passo con l'attuale panorama delle minacce informatiche
- Offrire l'opportunità di mettere in pratica le regole di base della cultura della cybersecurity aziendale e personale
- Illustrare chiaramente l'impatto aziendale delle principali questioni normative nel campo della sicurezza delle informazioni
- Chiarire i concetti base della cybersecurity e le modalità di protezione contro gli attacchi mirati
- Offrire suggerimenti pratici per i criteri aziendali
- Dare indicazioni sulle comunicazioni per la risposta e le indagini sugli incidenti

Kaspersky Security Awareness: opzioni di formazione flessibili

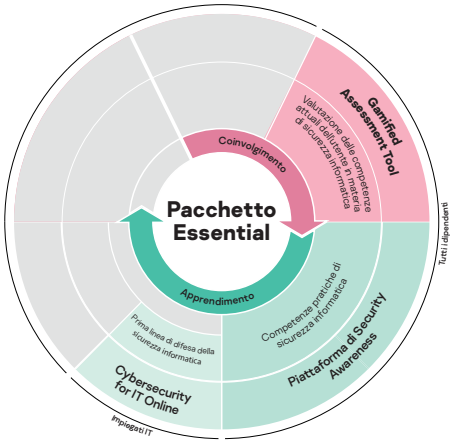
Le soluzioni di formazione Kaspersky sono adatte a tutti i livelli aziendali e possono essere usate singolarmente o insieme. Offriamo inoltre semplici pacchetti su misura per le vostre esigenze.

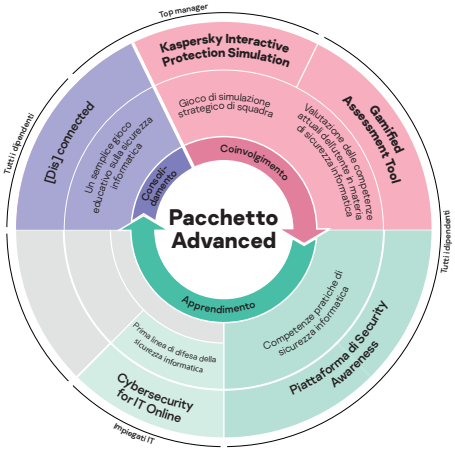
L'opzione essenziale per aumentare la consapevolezza dei dipendenti nei confronti della cybersecurity: semplice da configurare, facile da gestire

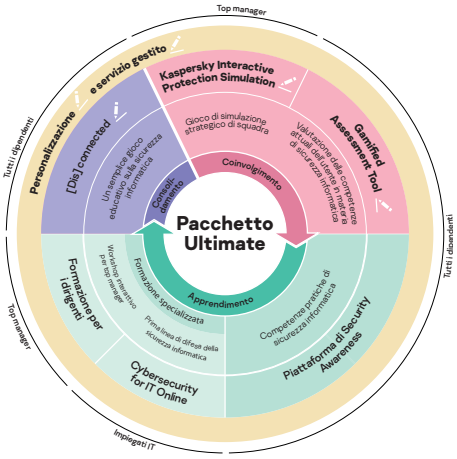
Offre un livello base di formazione sulla sicurezza per garantire uno svolgimento ottimale delle attività e la conformità ai requisiti normativi o di terze parti per la formazione generale sulla cybersecurity

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.com/awareness

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

kaspersky.it

kaspersky BRING ON THE FUTURE