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

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'organizzazione, è la chiave per ridurre la superficie d'attacco e il numero di incidenti da gestire. Le organizzazioni 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 sfrutti le più recenti tecniche e tecnologie per la formazione rivolta ad 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% delle aziende pensa che la principale minaccia alla Cybersecurity aziendale sia costituita dai 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 potenziano la consapevolezza in materia di Cybersecurity del vostro staff affinché tutti i dipendenti contribuiscano alla sicurezza informatica della vostra organizzazione. Poiché le modifiche comportamentali sostenibili richiedono tempo, il nostro approccio si basa sulla creazione di un ciclo di apprendimento continuo, che include 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 in un set di abilità che fanno da fondamento ai nostri prodotti

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

Il nostro corso di formazione in formato videogioco garantisce il coinvolgimento e la motivazione dell'edutainment, mentre le piattaforme di apprendimento aiutano a interiorizzare il set di abilità di Cybersecurity, per assicurare che le skill apprese non vadano perse nel tempo.

* Ricerca: "The cost of a data breach", Kaspersky Lab, primavera 2018.

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

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

$ 1.195.000
per azienda Enterprise
Impatto finanziario medio di un data breach causato dall'uso inappropriato delle risorse IT da parte dei dipendenti*

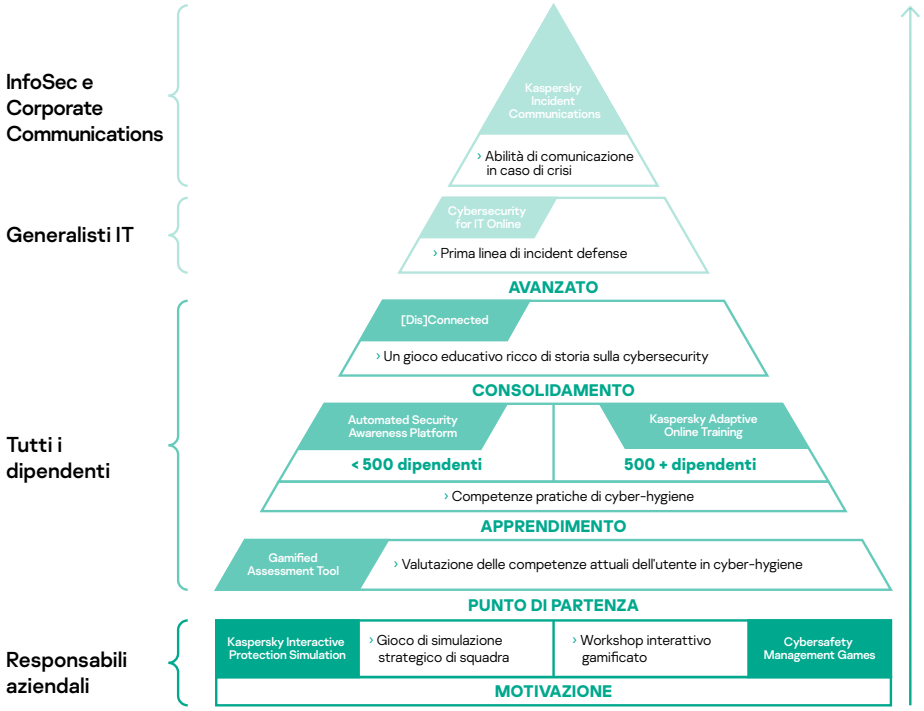
52%
delle aziende Enterprise
ha subito incidenti di sicurezza a causa dell'utilizzo inappropriato di risorse IT da parte dei dipendenti**

Oltre $ 1,7 miliardi
di perdite finanziarie globali
causate da attacchi business email compromise***

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, prende in considerazione le particolarità della natura umana e la capacità di assimilare le skill acquisite. In quanto esperti di Cybersecurity, noi di Kaspersky conosciamo bene i più adeguati comportamenti informatici 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: "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives". Kaspersky Lab, 2019

** Report: "IT security economics in 2019", Kaspersky

*** FBI "2019 Internet Crime Report"

Prodotti Kaspersky Security Awareness

Coinvolgimento / motivazione

Punto di partenza

Apprendimento

Consolidamento

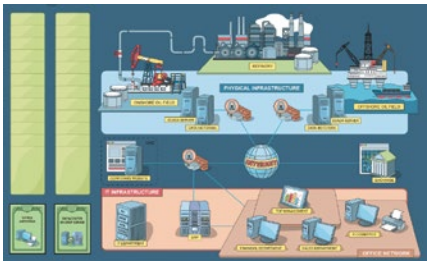
Motivazione

I dipendenti non sempre hanno voglia di ricevere ulteriori 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 nel corso i business executive, sebbene i loro errori potrebbero costare all'azienda tanto quanto gli errori dei sottoposti. Proprio per questo i nostri corsi si sviluppano sotto forma di videogioco: sono più coinvolgenti e sono il modo migliore per incoraggiare il vostro staff a superare le remore iniziali e partecipare attivamente al training.

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.



Gioco strategico 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 responsabili delle decisioni (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 dati. Ogni decisione ricade su tutti i processi aziendali. L'obiettivo principale è mantenere un funzionamento regolare e senza interruzioni. 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, vince.

10 scenari dei settori industriali (in continuo aggiornamento)

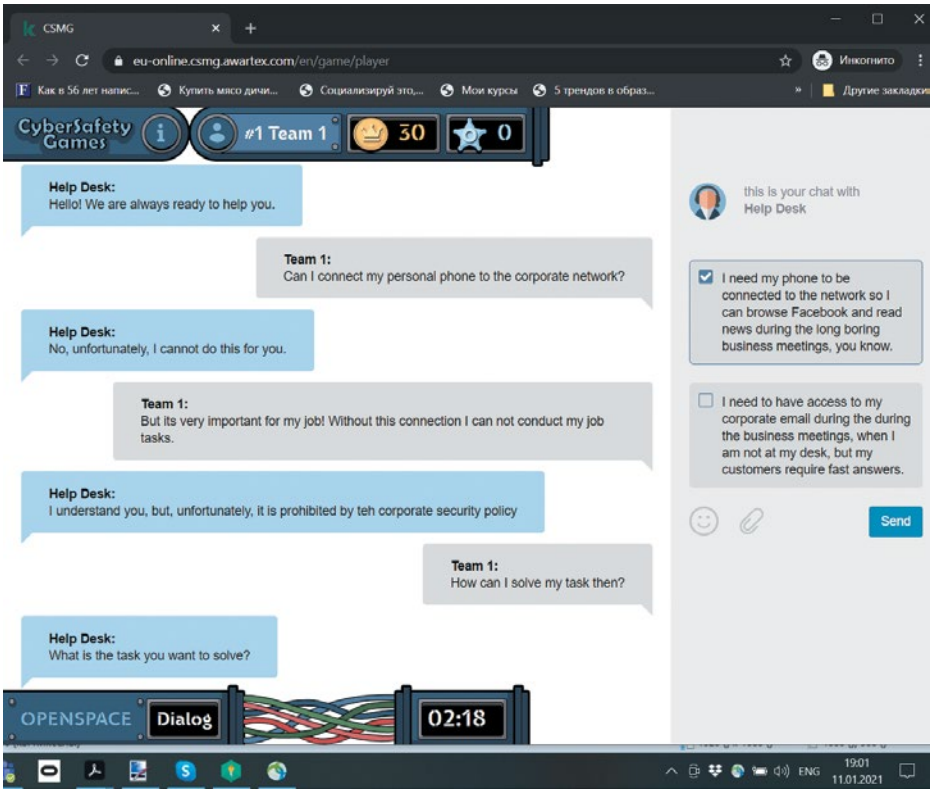
Ogni scenario dimostra il vero ruolo della Cybersecurity in termini di continuità e redditività aziendale, evidenziando le sfide e le minacce emergenti, oltre agli errori tipici che le organizzazioni commettono durante il processo di costruzione della loro sicurezza informatica. Gli scenari promuovono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

Cybersafety Management Games: trasformare i leader aziendali e i line manager in sostenitori proattivi della Cybersecurity

Cybersafety Management Games è un workshop interattivo (parzialmente basato su computer e parzialmente impartito da un istruttore, oppure interamente online), che dà ai line manager la competenza, la conoscenza e la forma mentis per mantenere un ambiente di lavoro sicuro, ciascuno nel proprio reparto, senza fare concessioni all'efficienza. Il corso di formazione trasforma i line o middle manager in sostenitori e fautori della Cybersecurity, rendendo la sicurezza informatica un ingrediente fondamentale del decision-making quotidiano.

* "Curva dell'oblio" di Ebbinghaus
** Capgemini "The digital talent gap"

Durante il training, identifichiamo gli equivoci più diffusi e aiutiamo i manager a capire perché i dipendenti tendano a ignorare le regole e i principi della Cybersecurity. Attraverso esercizi specificamente ideati, dimostriamo poi come sia possibile trasformare tali equivoci in comportamenti informatici positivi e sicuri.



Coinvolgimento / motivazione

Punto di partenza

Apprendimento

Consolidamento

Gamified Assessment Tool: un modo rapido e divertente di verificare le abilità in materia di Cybersecurity dei dipendenti

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 necessiterà di soli 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'organizzazione e per fungere da passo introduttivo a una più ampia campagna di formazione.

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 successiva sia efficace. Inoltre, questo assicura che non si perda tempo su materiali che sono già familiari.

Kaspersky Adaptive Online Training: competenze in materia di Cybersecurity fornite dal leader della sicurezza IT, grazie alla metodologia di apprendimento adattiva

Kaspersky Adaptive Online Training (KAOT) è una soluzione inedita, che unisce contenuti basati sugli oltre 20 anni di esperienza Kaspersky in materia di Cybersecurity a un'avanzata metodologia di apprendimento e sviluppo. KAOT è il risultato della collaborazione tra Kaspersky e Area9 Lyceum, società leader nel settore dei sistemi di apprendimento flessibile.

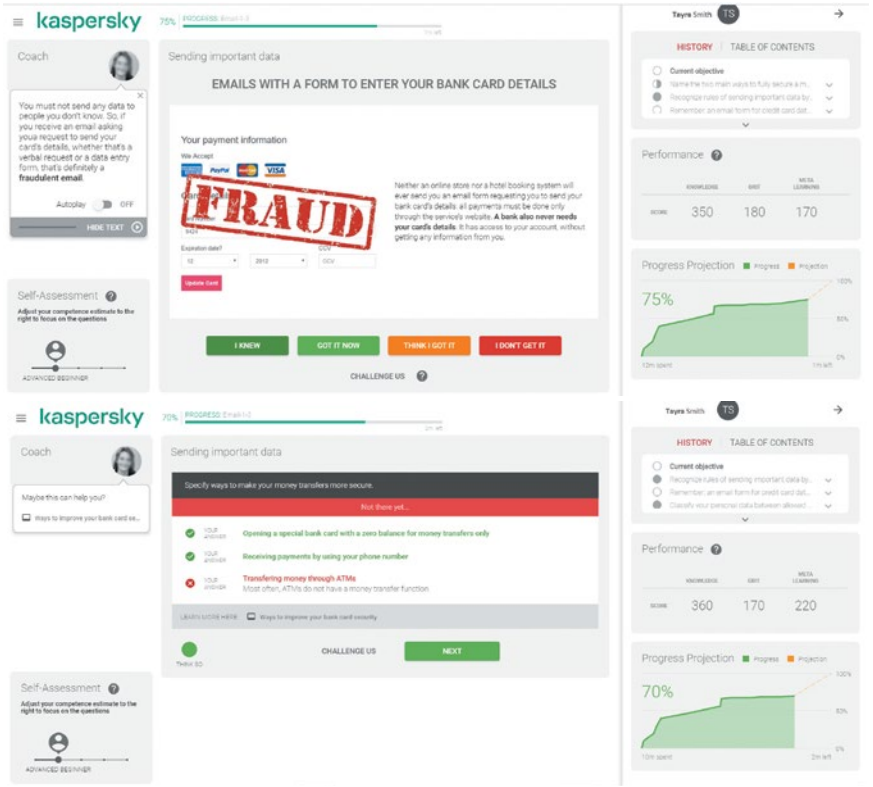
Basato su un'innovativa metodologia di apprendimento flessibile, questo approccio cognitivo offre un'esperienza di formazione personalizzata che tiene conto delle capacità e delle esigenze di ogni singolo studente.

Vantaggi chiave

- **L'approccio uno a uno come con un tutor individuale** ottenuto grazie all'impiego di una metodologia di apprendimento adattiva
- **Rivela e corregge le situazioni di incompetenza inconsapevole**, fornendo la necessaria motivazione ad apprendere e assicurando un perfetto comportamento cybersafe. Acquisendo consapevolezza su cosa si ignora e su cosa si debba migliorare, ogni utente può sviluppare le sue competenze in modo più rapido ed efficiente.
- **Niente noia né frustrazioni,** grazie all'approccio personalizzato per ogni studente. Ogni lezione inizia con una domanda, seguita da una lezione teorica solo se necessario. L'istruzione basata su problemi aumenta l'impegno e il coinvolgimento nella Cybersecurity.
- **Assicura un impiego automatico e abituale delle abilità,** grazie agli algoritmi adattivi che permettono agli studenti di avanzare a seconda delle loro competenze, usando diversi approcci per lo stesso argomento se necessario, e valutando costantemente se l'utente stia progredendo. Il training tappa le falle e costruisce una maggiore competenza in modo rapido ed efficace. Ad un alto livello di competenza, alcune conoscenze diventano una seconda natura, le azioni diventano automatiche e abituali, costantemente rafforzate da attività che "rinfrescano la memoria", nel caso in cui uno studente sia a rischio di dimenticare i contenuti.

Tracciamento dei risultati

Dati statistici completi ed esaustivi consentono di seguire perfettamente i progressi compiuti dal dipendente: KAOT prevede dei riepiloghi delle performance, oltre a report e grafici per gruppi e studenti singoli. L'amministratore è in grado di identificare agevolmente sia gli studenti che forniscono performance elevate, sia coloro che necessitano di ulteriore apprendimento. Inoltre, può vedere i report sui progressi degli utenti e delle classi, e i dettagli degli incarichi con analisi approfondite delle competenze e della metacognizione dei dipendenti.



Apprendimento

Le nostre piattaforme di apprendimento online sono il fulcro del programma di awareness. Contengono **più di 300 skill di Cybersecurity** che coprono tutti i principali argomenti della sicurezza IT, inclusi Password e account, Sicurezza delle e-mail, Social network e servizi di messaggistica, Sicurezza del PC, GDPR, ecc.

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 imparate potranno essere messe immediatamente in pratica, anche dopo la prima lezione.

Per massimizzare l'efficienza, sfruttiamo una tecnologia adattiva e dei percorsi di apprendimento automatizzati per ogni studente, prendendo in considerazione il loro livello iniziale di conoscenze e il livello target (il target dipende dal ruolo rivestito dallo studente all'interno dell'azienda). È un corso impegnativo, con molti esempi pratici, numerose spiegazioni sul PERCHÉ qualcosa è importante e svariati momenti di valutazione che danno un feedback immediato sulle azioni dell'utente.

"L'ignoranza genera fiducia più spesso della conoscenza."
Charles Darwin, L'origine dell'uomo

Argomenti affrontati in KAOT:
Password
- Sicurezza delle e-mail
- Navigazione su Internet
- Social network e servizi di messaggistica
- Sicurezza del PC
- Dispositivi mobili
- GDPR

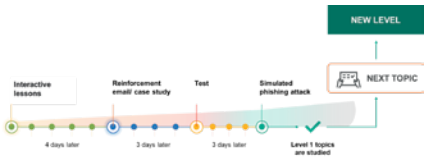
KAOT è attualmente disponibile in: inglese, tedesco, italiano, francese, spagnolo, arabo, russo.

Ulteriori informazioni: kaspersky.it/kaot

per PMI

Kaspersky Automated Security Awareness Platform: uno strumento online semplice da gestire, che aumenta livello dopo livello le abilità di Cybersecurity dei dipendenti

Percorso di apprendimento automatizzato per combattere l'annullamento e assicurare il mantenimento delle abilità



Argomenti affrontati in ASAP:
Password e account
- Sicurezza delle e-mail
- Navigazione su Internet
- Social network e servizi di messaggistica
- Sicurezza del PC
- Dispositivi mobili
- Protezione delle informazioni confidenziali
- GDPR

Kaspersky ASAP è una soluzione plurilingue, attualmente disponibile in inglese, tedesco, italiano, francese, spagnolo, russo, arabo, portoghese, olandese, ceco, polacco, kazako, sloveno, rumeno, turco, ungherese*.

ASAP si rivela ideale per MSP e xSP: i servizi di formazione per più aziende si possono facilmente gestire attraverso un unico account, mentre le licenze si possono acquistare tramite subscription mensile.

Scaricate una versione trial di Kaspersky ASAP con funzionalità complete all'indirizzo asap.kaspersky.com/it/: scoprirete subito quanto sia facile impostare e gestire il programma di formazione aziendale sulla Security Awareness!

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.

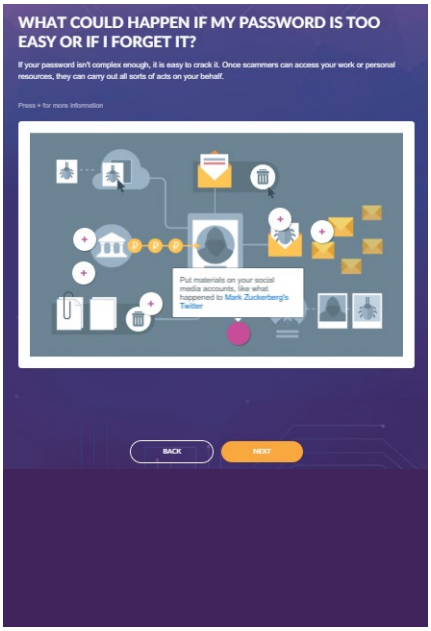
Questo training è ideale per piccole e medie imprese, soprattutto quelle prive di risorse dedicate alla gestione dei programmi di formazione.

Vantaggi chiave:

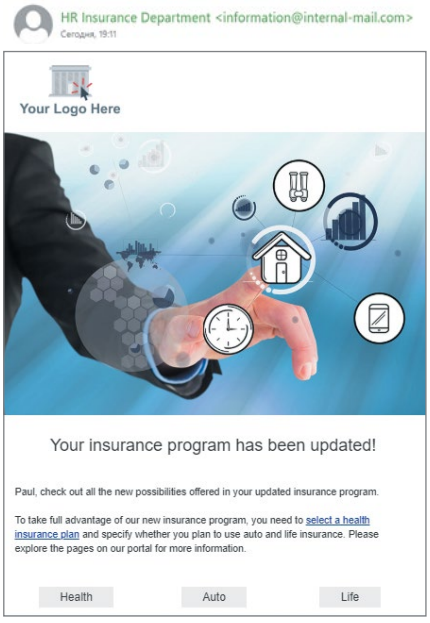
- **Il programma di formazione è semplicissimo da avviare, configurare e monitorare:** inoltre la gestione è completamente automatizzata, senza alcun intervento da parte di amministratori. La piattaforma stessa crea uno specifico programma di formazione per ciascun gruppo di dipendenti, fornendo un'efficace 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.
- **Licenze flessibili** (per Managed Service Provider): il modello di licensing in base al numero di utenti prevede un numero minimo di 5 licenze.

Ciascun modulo comprende vari livelli, in cui vengono sviluppate competenze di sicurezza specifiche. I livelli vengono definiti in base al grado di difficoltà che deve essere gestito in materia di sicurezza. Il Livello 1 riguarda il modello comportamentale da adottare di fronte agli attacchi più semplici e generali. I livelli superiori riguardano la specifica formazione per attacchi sofisticati e mirati.

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. È inoltre possibile accedere a ulteriori dettagli, fino al livello individuale.

Coinvolgimento / motivazione

Punto di partenza

Apprendimento

Apprendimento avanzato

Consolidamento

Avanzato

La maggior parte delle aziende offre una formazione sulla Cybersecurity a due livelli, ovvero corsi avanzati per i team di sicurezza IT e programmi di Security Awareness per i dipendenti degli altri reparti (Kaspersky propone una serie di prodotti completa per entrambi). Ma cosa manca? Team IT, service desk e altro personale tecnicamente specializzato. I programmi standard di Security Awareness non sono sufficienti per queste figure, ma non è neanche necessario trasformare questi dipendenti in esperti di Cybersecurity: è troppo costoso, troppo lungo e troppo rischioso.

Il corso di formazione CITO è completamente online: i partecipanti hanno solo bisogno di una connessione a Internet o di un accesso a un LMS aziendale e di un browser Chrome.

Ciascuno dei 4 moduli comprende una breve panoramica teorica, suggerimenti pratici e tra 4 e 10 esercizi, ognuno dei quali intende esercitare un'abilità specifica e dimostra come utilizzare gli strumenti e il software di sicurezza IT nel lavoro quotidiano.

Il corso di formazione KIC si assicura che il vostro team di gestione delle crisi:

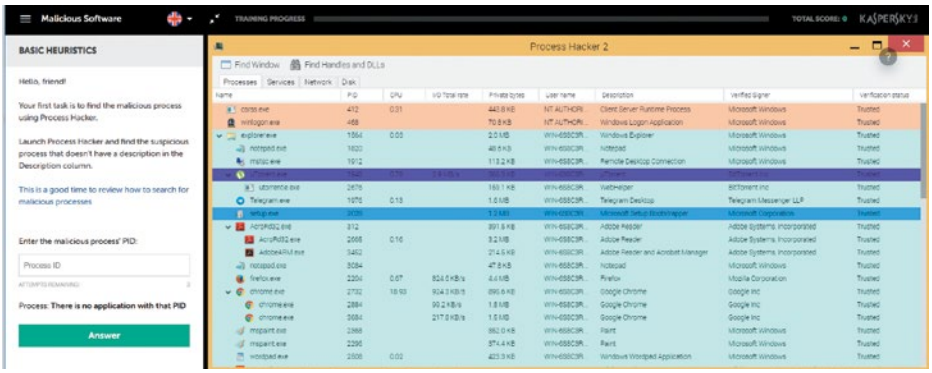
- Capisca le cyberminacce rivolte contro di voi
- Riconosca i potenziali esiti
- Possa coordinare efficacemente la risposta con il team di sicurezza IT
- Acquisisca esperienza attraverso la simulazione dei cyber-incidenti
- Sappia cosa sia essenziale e sicuro dire nelle comunicazioni sia interne che esterne, all'indomani di un cyberattacco
- Aggiorni e implementi il vostro piano di comunicazioni in caso di cybercrisi

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

Cybersecurity for IT Online è un training interattivo per tutti gli attori coinvolti nell'IT. Costruisce solide abilità di Cybersecurity e risposta agli incidenti di primo livello.

Il programma di formazione fornisce ai professionisti IT competenze pratiche su come riconoscere un possibile scenario di attacco su un PC apparentemente non infetto e su come raccogliere i dati relativi a un incidente affinché vengano gestiti dal personale di sicurezza IT. Sviluppa inoltre la capacità della ricerca dei sintomi dannosi, consolidando il ruolo di tutti i membri del team IT come prima linea di difesa per la sicurezza. Consiste di quattro moduli: software dannosi, programmi e file potenzialmente indesiderati, le basi dell'indagine e la risposta agli incidenti di phishing.

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



Kaspersky Incident Communications: rendere il vostro team di comunicazione aziendale in grado di rispondere a un cyberattacco

Dal momento in cui un incidente informatico viene scoperto, ogni azione conta. Il modo in cui vengono gestite le comunicazioni, sia interne che esterne, è fondamentale, soprattutto se si ha a che fare con vettori d'attacco sconosciuti e minacce avanzate persistenti (APT).

Kaspersky Incident Communications forma il top management, gli specialisti informatici e i professionisti delle comunicazioni aziendali nella gestione della comunicazione durante la crisi, incluso lo sviluppo e l'implementazione di risorse adeguate. Aiuta a costruire solidi legami fra i membri del team di gestione della crisi e insegna come preparare un piano di comunicazione della crisi, fornendo consigli pratici, procedure di operation security e strumenti per la cifratura delle comunicazioni durante l'incidente, a sostegno della continuità aziendale.

Coinvolgimento / motivazione

Punto di partenza

Apprendimento

Consolidamento

Consolidamento

Il consolidamento è una parte fondamentale del programma di formazione, ed è necessario per cementare le competenze e le abilità acquisite durante la fase di 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 sotto forma di videogioco, è possibile creare una situazione in tempo reale e verificare le conseguenze senza danneggiare sé stessi o l'azienda.

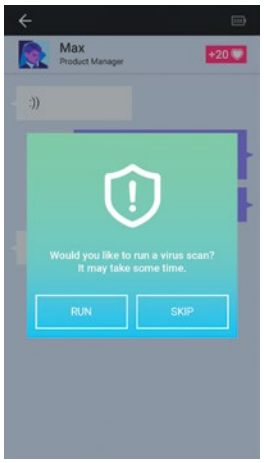
[Dis]connected: un casual game educativo

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

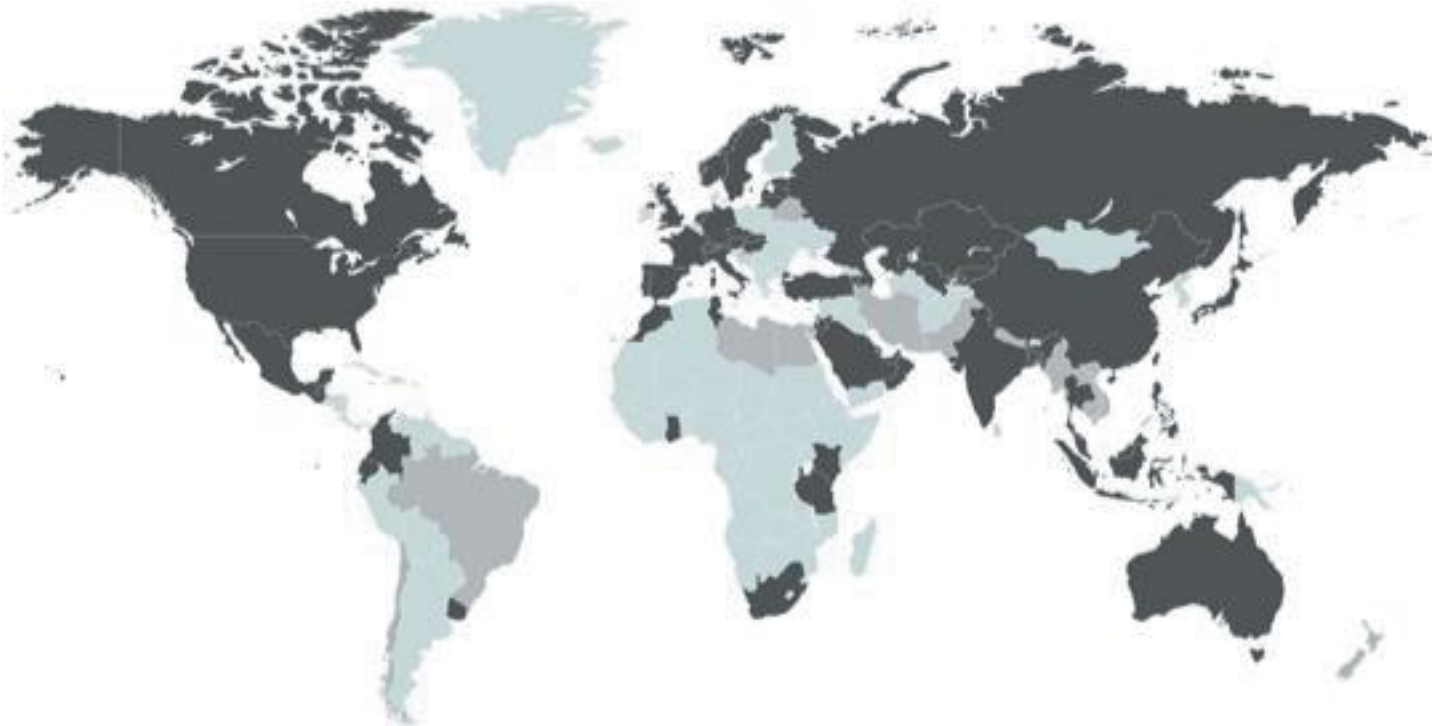
Gli elementi della Cybersecurity si intrecciano alla trama di gioco, rivelando come le decisioni in merito possano portare al conseguimento o al fallimento dei propri obiettivi. Ci sono 18 casi da risolvere, che includono argomenti come password e account, e-mail, navigazione Web, social network e servizi di messaggistica, sicurezza del computer e dei dispositivi mobili.

Le simulazioni di applicazioni integrate, come servizi di messaggistica o app bancarie, permettono un'esperienza immersiva ancor più completa.

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.



Kaspersky Security Awareness nel mondo



75
paesi

>500.000
dipendenti formati

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

www.kaspersky.it

Distributore per l'Italia
Avangate Security Srl
Via F. Sforza, 40 - 20122 Milano
T. +39 059 8341380
Web: wwwavangate.it

kaspersky BRING ON THE FUTURE