KASPERSKY lab

Kaspersky Security Awareness

Programmi di formazione con approccio ludico per tutti i livelli della struttura organizzativa

www.kaspersky.it

#truecybersecurity

Un modo efficace per promuovere una cultura sulla cyber safety in tutta l'organizzazione

Oltre l'80% di tutti gli incidenti informatici è riconducibile a errori umani. Le aziende perdono ingenti somme di denaro per porre rimedio a questo tipo di incidenti, ma i programmi di formazione tradizionali destinati a prevenire tali problemi sono spesso poco efficaci e raramente consentono di ottenere i risultati desiderati in termini di motivazione e comportamenti adeguati.

Nella maggior parte dei casi, gli incidenti di cybersecurity che si verificano nelle moderne organizzazioni sono dovuti a errori involontari dei dipendenti:

- Come emerge da uno studio realizzato da IBM nel 2015, la percentuale di **violazioni interne causate da errori umani supera il 95%**[1].
- **Nel 2015, il 75% delle aziende di grandi dimensioni** e il 31% delle piccole aziende del Regno Unito **hanno subito violazioni di sicurezza legate al personale**[2].
- **L'impatto finanziario medio** di un incidente dovuto a comportamenti imprudenti da parte dei dipendenti ammonta a **865.000 dollari per violazione**[3].
- **Il costo medio degli attacchi di phishing arriva a 400 dollari per dipendente all'anno** (nel conteggio non sono inclusi altri tipi di cyberminacce)[4].
- **Solo il 25% dei piani assicurativi contro il cyber risk** coprono gli incidenti dovuti a errori umani e negligenze (mentre i rischi causati da cybercriminali esterni sono coperti dall'84% dei piani assicurativi che includono, nel 75% dei casi, anche gli attacchi perpetrati da "criminal insider" o colleghi malintenzionati)[5].

L'analisi effettuata ha dimostrato la scarsa efficacia della maggior parte degli attuali programmi di formazione sulla consapevolezza della cybersecurity:

- La lettura di documenti e istruzioni è noiosa, eccessivamente tecnica e alimenta troppi dubbi, poiché le tante minacce descritte e i divieti elencati non sono supportati da esempi di comportamenti sicuri.
- Le persone non sono motivate ad apprendere (solo il 22% ritiene di poter diventare vittima di cybercriminali).
- I dipendenti non attribuiscono alla sicurezza IT la dovuta importanza e cercano spesso di aggirarla.
- Non vi sono adeguati strumenti per misurare la consapevolezza, eccetto il numero di persone a cui è stata impartita una formazione".

1 IBM 2015 Cyber Security Intelligence Index.

2 2015 Information Security Breaches Survey. Governo del Regno Unito in associazione con InfoSecurity Europe e PwC.

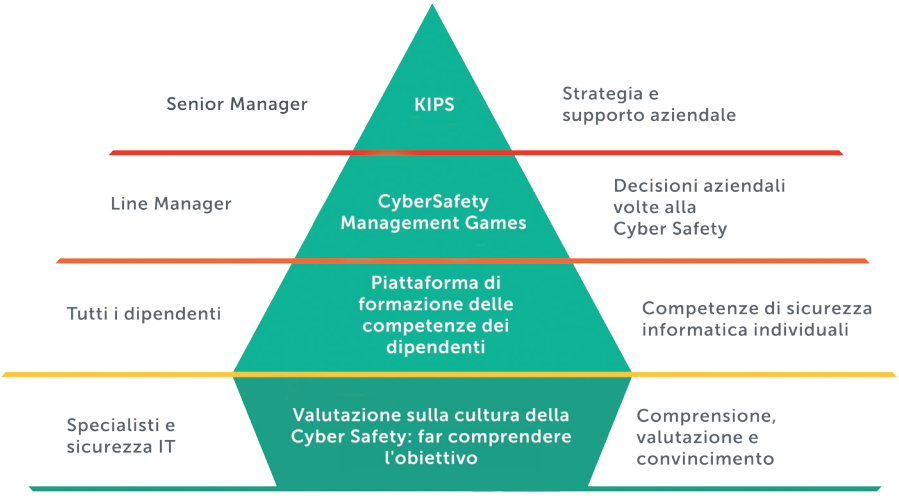
3 "La percezione della sicurezza IT da parte delle aziende: un inevitabile compromesso", Kaspersky Lab, 2016.

4 Calcoli basati sui dati del Ponemon Institute, "Costo del phishing e valore della formazione dei dipendenti", agosto 2015.

5 2015 Global Cyber Impact Report. Ponemon Institute LLC.

Benefici e vantaggi del programma

Kaspersky Lab ha lanciato una famiglia di prodotti di formazione assistita tramite computer che utilizza tecniche di apprendimento moderne e si rivolge a tutti i livelli della struttura organizzativa. Il nostro programma di formazione ha già dimostrato tutta la sua efficacia.



Il portafoglio di prodotti Kaspersky Security Awareness è specificamente progettato per rispondere in modo adeguato alle esigenze e preferenze delle aziende:

- **Non si limita a fornire conoscenze, ma aiuta a costruire una cultura del comportamento:** l'approccio formativo, che prevede l'applicazione di dinamiche ludiche, l'apprendimento attraverso la pratica, attacchi simulati e altre attività, consente di sviluppare solidi modelli comportamentali e produrre effetti duraturi.
- Permette di creare **comportamenti specifici per i diversi livelli organizzativi**, Senior manager, Line/Middle manager e dipendenti, tenendo conto delle loro particolari esigenze e limitazioni in termini di tempo e formazione.
- Essendo basato sull'uso di strumenti informatici, **è semplice da gestire e produce risultati facilmente misurabili**. Può essere gestito dai team dalla sicurezza IT o delle Risorse Umane. Kaspersky Lab offre una metodologia di implementazione comprovata, best practice e supporto tecnico e metodologico.
- Si basa sulle vaste competenze di **Kaspersky Lab in tema di cybersecurity e su importanti investimenti nel settore della ricerca e dello sviluppo**.

Formazione KIPS come strumento di supporto strategico

La formazione KIPS, destinata a esperti di sistemi aziendali, personale responsabile dell'IT e line manager, mira a promuovere la consapevolezza dei rischi e dei problemi di sicurezza derivanti dalla complessità dei moderni sistemi informatici.

Kaspersky Interactive Protection Simulation (KIPS) è un esercizio di simulazione in cui i team si trovano immersi in un contesto aziendale dove devono affrontare una serie di cyberminacce cercando, al tempo stesso, di massimizzare i profitti e preservare la fiducia. L'idea è quella di costruire una strategia di difesa informatica scegliendo i più efficaci controlli proattivi e reattivi disponibili.

Ogni reazione dei team al susseguirsi degli eventi modifica il modo in cui si evolve lo scenario e, in ultima analisi, l'entità dei profitti che l'azienda riesce o meno a realizzare. Trovando un equilibrio tra priorità tecniche, aziendali e di sicurezza e i costi di un attacco informatico reale, i team analizzano i dati e assumono decisioni strategiche sulla base di informazioni incerte e risorse limitate. L'approccio è assolutamente realistico perché ogni scenario si basa su eventi reali.

KIPS è un programma dinamico volto a promuovere la consapevolezza, che si basa su un metodo di "apprendimento attraverso la pratica":

- Divertente, coinvolgente e rapido (2 ore)
- Il lavoro in team favorisce la collaborazione
- La competizione stimola la capacità di analisi e di iniziativa
- L'approccio ludico sviluppa una maggiore comprensione delle misure di cybersecurity

"Dall'esercizio emerge, tuttavia, che alcune delle prime e più basilari decisioni strategiche, come gli audit e la formazione sulla sicurezza, la modifica delle password e la gestione delle patch, contribuiscono in larga misura a fornire una risposta efficace agli incidenti che possono presentarsi in futuro".

Mark Jenkins · 16 dicembre 2015 · ICT Qatar

Scenari disponibili (come KIPS Live e KIPS Online, tradotti in 10 lingue)

Azienda	Protezione dell'azienda da ransomware, APT, bug di sicurezza.
Banca	Protezione degli istituti finanziari da APT di alto profilo, che colpiscono terminali ATM, server gestionali e sistemi aziendali.
Pubblica amministrazione	Protezione dei server Web pubblici da attacchi ed exploit.
Industria	Protezione dei sistemi di controllo industriali e delle infrastrutture critiche.

Ogni scenario è incentrato su vettori di minaccia specifici e permette di individuare e analizzare i tipici errori che caratterizzano i processi di sviluppo della cybersecurity e le procedure di risposta agli incidenti dei vari settori.

Cybersafety Management Games per decisioni aziendali più efficaci in tema di cyber safety

Questo workshop altamente interattivo, che coniuga attività formative tramite computer e con istruttori, sensibilizza l'attenzione dei line manager sull'importanza della cybersecurity per il loro lavoro e permette di acquisire competenze, conoscenze e attitudini essenziali per garantire la sicurezza dell'ambiente di lavoro nelle proprie divisioni.

Le organizzazioni stanno adottando una serie di provvedimenti per affrontare le cyberminacce attraverso la creazione di strutture per la sicurezza IT e la realizzazione di iniziative di formazione adeguate. Ma è sufficiente?

- Le conoscenze acquisite durante la formazione riescono realmente a orientare i comportamenti dei dipendenti? O c'è bisogno di altro?
- L'efficienza aziendale deve essere sacrificata in funzione della sicurezza?
- I responsabili della sicurezza pensano di non essere sempre in grado di far comprendere a tutti l'importanza della cyber safety?

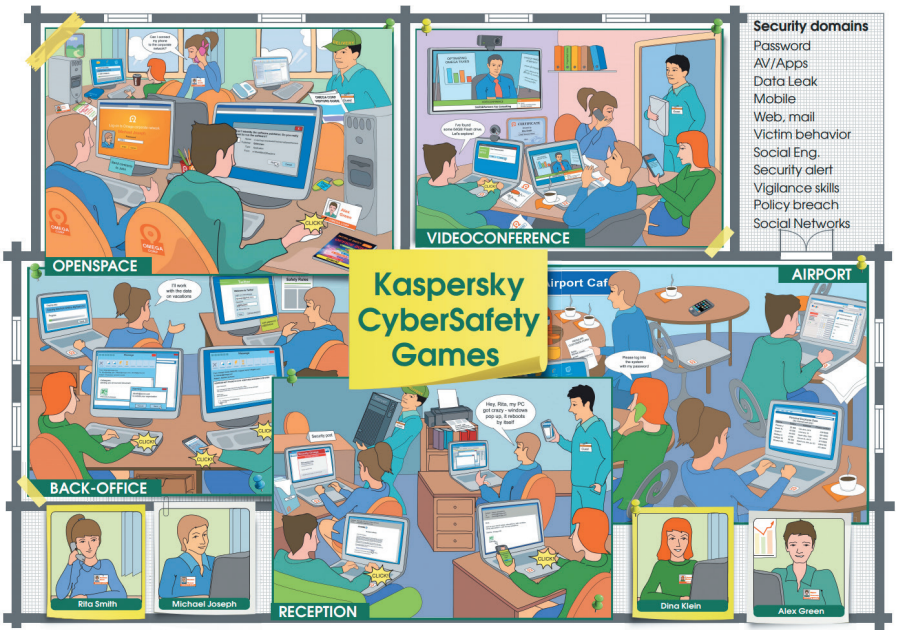
Queste sfide possono essere affrontate soltanto coinvolgendo i **line manager nella creazione di organizzazioni sicure dal punto di vista informatico, senza sacrificare l'efficienza. Solo loro** interagiscono quotidianamente con i dipendenti e assumono decisioni che producono effetti per l'azienda. La risposta consiste nel rendere la cyber safety un elemento indispensabile dei processi decisionali quotidiani.

Kaspersky CyberSafety Management Games fornisce ai manager le **competenze, conoscenze e attitudini** essenziali per garantire la sicurezza dell'ambiente di lavoro nella loro divisioni.

- **Comprensione:** adozione delle misure interne di cybersecurity come un insieme di azioni importanti e, al tempo stesso, non complicate
- **Monitoraggio:** valutazione dei processi di lavoro quotidiani sotto il profilo della cyber safety
- **Processo decisionale orientato alla cyber safety:** considerazioni sulla cybersecurity come parte integrante dei processi aziendali
- **Rafforzamento e ispirazione:** leadership influente e consigli utili per i dipendenti

Il prodotto può essere concesso in licenza per i centri di formazione aziendale e offre importanti vantaggi a livello di implementazione:

- Facilità di distribuzione: i formatori dei corsi non devono essere esperti in materia di sicurezza.
- Facilità di pianificazione: le brevi sessioni di formazione modulari possono essere svolte in funzione degli impegni del dipendente.



Da febbraio 2017 la piattaforma è disponibile in 27 lingue.

Utilizzando questa piattaforma con il supporto della Best Practice Guide di Kaspersky Lab, i clienti saranno in grado di definire e implementare un piano di formazione sulla cybersecurity efficace, continuo e misurabile, in cui i dipendenti affronteranno lezioni di complessità crescente e tematiche di sicurezza diverse per acquisire una formazione in linea con il panorama delle minacce attuali e con le loro specifiche competenze.

Visitate il sito www.kaspersky.com/demo-sa per provare la nostra demo interattiva.

Piattaforma di formazione dei dipendenti per lo sviluppo di competenze in tema di sicurezza informatica

Sviluppare le competenze e le conoscenze già acquisite grazie alla possibilità di accedere a una piattaforma online dove lavorare su situazioni e scenari tipici è fondamentale per approfondire la conoscenza, migliorare la comprensione delle potenziali minacce e apprendere il modo per poterle affrontare e gestire in maniera efficace. L'apprendimento online permette ai dipendenti di fare pratica e imparare attraverso un portale per l'apprendimento interattivo.

Moduli di formazione interattivi

- Divertenti e brevi
- Basati su esercizi collegati tra di loro
- Iscrizione automatica per rafforzare le competenze
- Oltre 20 moduli che trattano tutti gli aspetti della sicurezza

Valutazione delle conoscenze

- Include questionari di valutazione con domande e durata predefinite o personalizzabili
- Copre vari moduli di sicurezza
- Ampia libreria di domande e randomizzazione per evitare imbrogli

Attacchi di phishing simulati

- 3 tipi di attacchi di phishing di diversa difficoltà, tutti basati su casi di vita reale
- Vengono proposti momenti di apprendimento ogni volta che i dipendenti aprono e-mail di phishing
- Modelli personalizzabili
- Assegnazione automatica dei moduli di formazione per chi non ha superato la prova dell'attacco simulato

Creazione di report e analisi

- Fornisce statistiche per l'intera organizzazione o per ogni reparto, posizione e singolo dipendente
- Consente di monitorare il livello di competenza dei dipendenti e le relative dinamiche
- Permette di esportare dati in diversi formati o direttamente nella piattaforma LMS del cliente

Punti di attenzione

La valutazione prende in esame la cultura della sicurezza da prospettive diverse:
- Livello organizzativo (gestionale)
- Livello personale (dipendente)
- Esperienze disponibili
- Garanzia di sicurezza a livello di processo

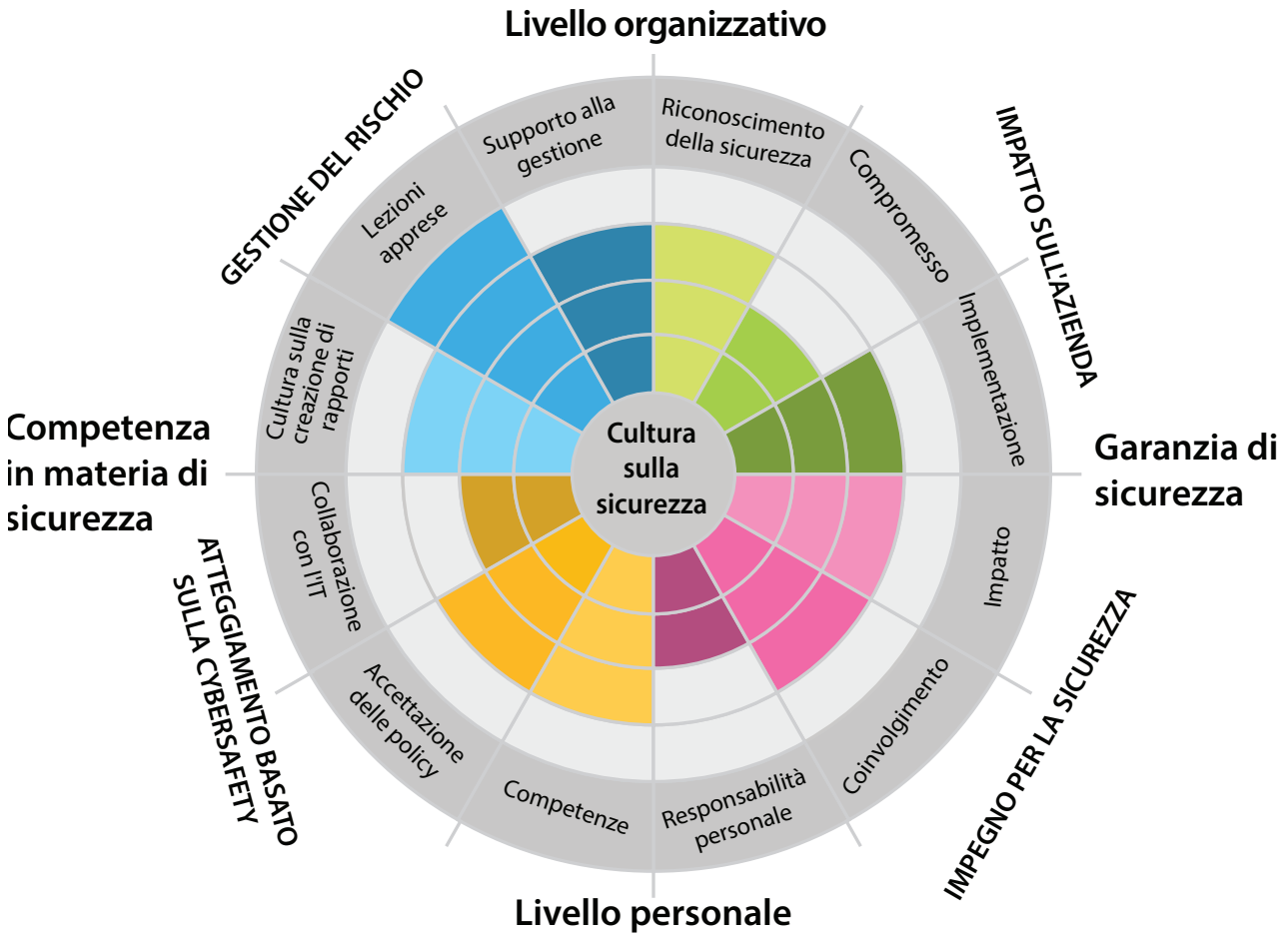
Valutazione della cultura sulla cyber safety

La valutazione della cultura sulla cyber safety permette di analizzare gli effettivi comportamenti e atteggiamenti quotidiani nei confronti della cybersecurity a tutti i livelli dell'azienda, evidenziando il modo in cui i dipendenti dell'organizzazione ne percepiscono i diversi aspetti.

I risultati della valutazione possono essere utilizzati per comprendere eventuali punti deboli e le aree a cui prestare maggiore attenzione al fine di motivare e allineare le priorità del reparto responsabile della sicurezza in termini di attività interne ed esterne, come le iniziative di formazione e sviluppo della consapevolezza, le relazioni pubbliche interne, la condivisione delle informazioni e i principi di collaborazione sul lavoro.

La cultura sulla cyber safety riguarda aspetti che verranno valutati e misurati globalmente in tutta l'azienda. I risultati della valutazione costituiscono la base di discussione per analizzare il ruolo e la posizione che la cybersecurity occupa nel supportare l'efficienza aziendale:

- Approccio mentale alla cyber safety (percezione della sicurezza e delle policy)
- Gestione dei rischi (orientamento, feedback, miglioramenti).
- Impegno (atteggiamento e comportamento delle persone nei confronti della sicurezza)
- Impatto sull'azienda (equilibrio tra sicurezza ed efficienza aziendale).



Il report relativo alla cultura sulla cyber safety non intende valutare il livello di maturità della sicurezza tecnica dell'azienda né misurare l'efficacia dell'operato del reparto responsabile della sicurezza.

Il suo obiettivo è quello di mostrare in che modo i dipendenti, nella media, considerano o concepiscono la cybersecurity, cosa pensano della cultura, delle abitudini e delle pratiche quotidiane in materia di cybersecurity e qual è la loro percezione personale dei vari aspetti della cultura che rende possibile proteggere l'azienda dalle cyberminacce. Tale percezione è il risultato di diverse pratiche aziendali, non solo dell'attività svolta dal reparto responsabile della sicurezza o della gestione dei rischi.

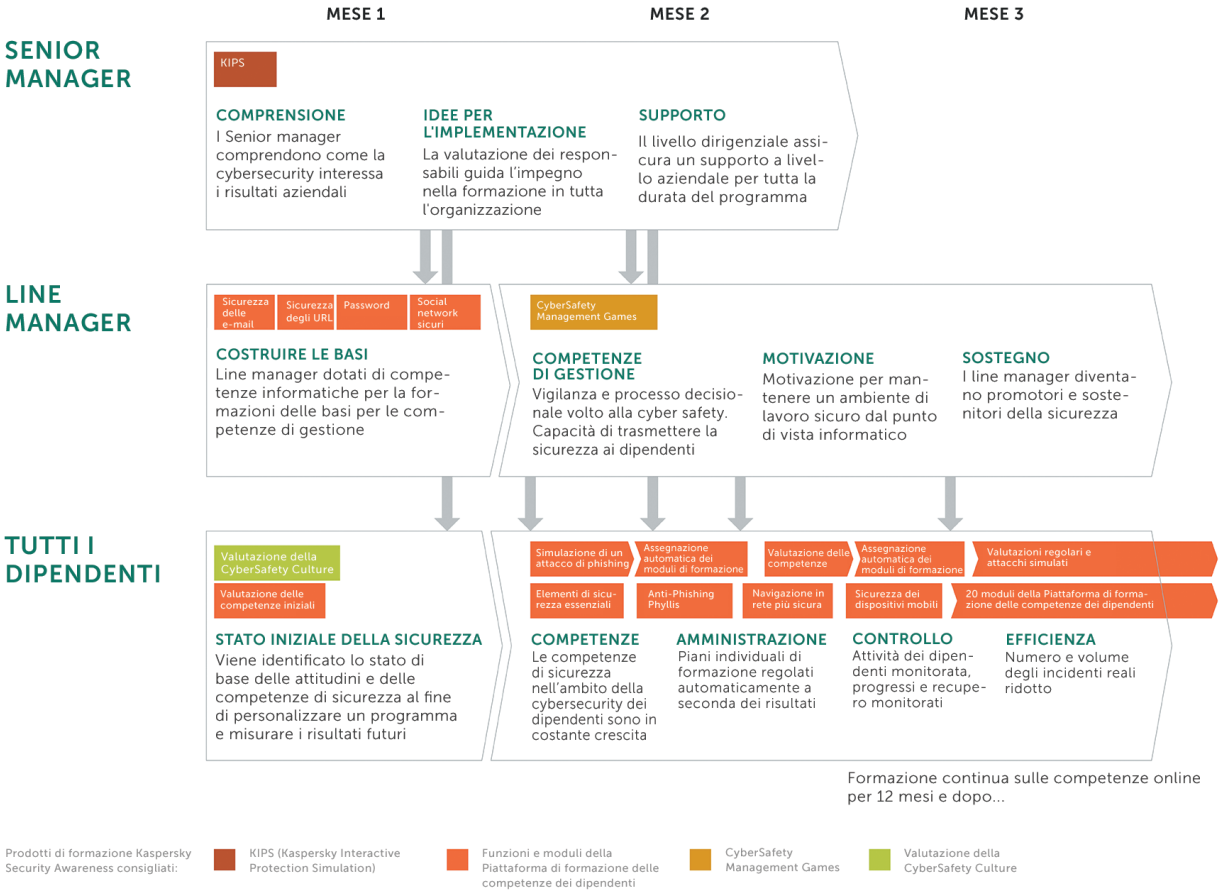
La valutazione viene eseguita mediante un sondaggio erogato via internet. Il completamento richiede circa 15 minuti per dipendente e occorrono mediamente 2 settimane per somministrare il sondaggio a tutti i dipendenti.

Al termine del sondaggio, il cliente riceve un report consolidato.

Metodologia di implementazione: Avvio rapido ed effetto cumulativo

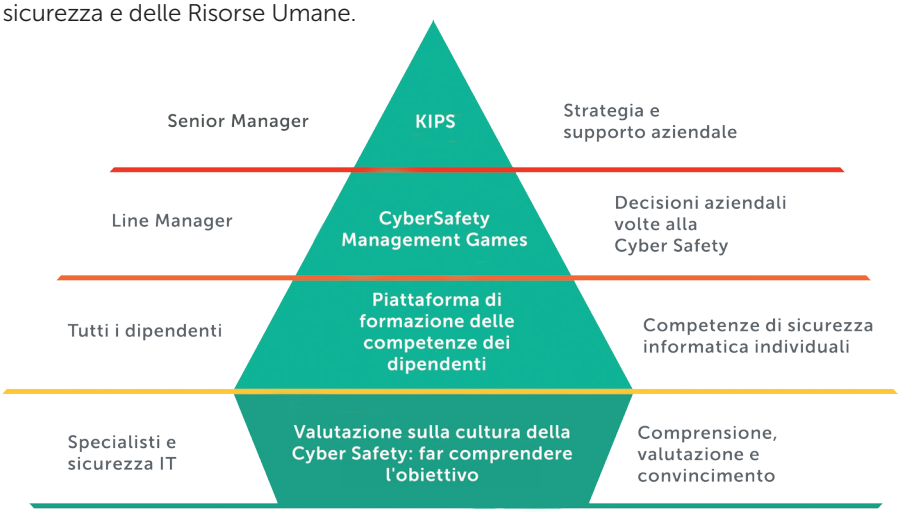
Di seguito è indicata la sequenza consigliata per la formazione dei dipendenti con i prodotti Kaspersky Security Awareness (per i nostri clienti è anche disponibile la "Best Practice Guide"). Forniamo istruzioni dettagliate e sostegno metodologico ai clienti per agevolare l'implementazione e la gestione dei nostri prodotti e massimizzarne il valore.

Effetto cumulativo - Il percorso formativo è interconnesso e sequenziale



Prodotti di formazione Kaspersky Security Awareness

La formazione Interactive Protection Simulation (KIPS) è parte integrante del pacchetto di prodotti Security Awareness di Kaspersky, basato sulla metodologia della "cultura sulla cyber safety". Lo sviluppo della cultura sulla cyber safety si fonda su una serie di attività di formazione, che utilizzano dinamiche ludiche destinate a tutti i livelli della struttura organizzativa e gestite dai team responsabili della sicurezza e delle Risorse Umane.



Formazione completa e al tempo stesso semplice e chiara

- Ampia gamma di tematiche relative alla sicurezza
- Processo di formazione coinvolgente
- Esercizi pratici
- Linguaggio comprensibile a chi non possiede specifiche competenze IT

Vantaggi per l'azienda

93%
di probabilità di applicare le conoscenze acquisite nel lavoro quotidiano

90%
di incidenti in meno

50-60%
di riduzione dei costi legati al cyber risk

30x
ritorno degli investimenti nella sensibilizzazione alla sicurezza

www.kaspersky.it

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Kaspersky Security Awareness:
www.kaspersky.com/awareness
Demo del prodotto: **www.kaspersky.com/demo-sa**