KASPERSKY lab

Kaspersky ASAP: Automated Security Awareness Platform

Efficienza e semplicità di gestione per le aziende di ogni dimensione

www.kaspersky.it/awareness
asap.kaspersky.com/it
#truecybersecurity

Kaspersky ASAP: Automated Security Awareness Platform

La causa di oltre l'80% degli incidenti informatici è un errore umano. Le imprese perdono milioni di dollari per rispondere a questo tipo di incidenti, ma l'efficacia dei programmi di formazione tradizionali destinati a prevenire questi problemi è limitata e di solito non riesce a motivare il comportamento desiderato.

Errori umani come principale rischio informatico

$ 83.000 per PMI
Impatto finanziario medio degli attacchi causati da dipendenti disattenti/disinformati[1]

$ 101.000 per PMI
Impatto finanziario degli attacchi causati da phishing/social engineering[1]

$ 400 per dipendente all'anno
Costo medio degli attacchi di phishing (altri tipi di minacce informatiche sono esclusi da questo conteggio)[2]

Il 52% di tutte le organizzazioni
Ha individuato nelle negligenze dei dipendenti/utenti il principale problema nella loro strategia di sicurezza IT[1]

Fattori da considerare per un approccio efficiente a un programma formativo sulla cybersecurity

Nonostante le aziende siano pronte a implementare i programmi formativi sulla cybersecurity, non molte sono soddisfatte dei processi e risultati. Le piccole e medie imprese invece, che di solito non hanno esperienza e risorse dedicate, sono particolarmente interessate.

Poche idee su come impostare obiettivi e piano formativo

La formazione richiede troppo tempo di gestione

La creazione di report non è utile nel monitoraggio dell'obiettivo

I dipendenti non apprezzano il programma → non acquisiscono competenze

Anche le organizzazioni con team dedicati alla sicurezza si impegnano per ottenere un reale miglioramento nel comportamento dell'utente come risultato del programma formativo sulla cybersecurity.

Molte aziende scelgono tra una formazione una tantum (come ad esempio "tutto sulla cybersecurity in 1 ora") e programmi di formazione professionale ben strutturati di cui, però, utilizzano solo alcune funzioni e strumenti di base. In genere si tratta di una serie di attacchi di phishing simulati, oltre ad alcune lezioni più generiche, perché gli altri elementi del programma sono troppo difficili da implementare e gestire. Ad ogni modo, i dipendenti non acquisiscono le competenze necessarie a rafforzare efficientemente la strategia di sicurezza dell'organizzazione.

[1] "Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within", Kaspersky Lab e B2B International, giugno 2017

[2] Risultati basati sui dati del Ponemon Institute, "Cost of Phishing and Value of Employee Training", agosto 2015.

Efficienza e semplicità di gestione del programma formativo per aziende di ogni dimensione

Kaspersky Lab introduce la piattaforma Automated Security Awareness Platform che costituisce il focus principale del portfolio di formazione Kaspersky Security Awareness.

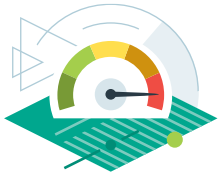
La Piattaforma è uno strumento online per la formazione dei dipendenti sulle tematiche relative alla sicurezza informatica nell'arco di un anno. L'implementazione e la gestione della Piattaforma non richiede risorse e configurazioni specifiche e offre all'organizzazione una guida integrata per tutti gli step del percorso verso una strategia aziendale di cybersecurity:

Step 1:

Definizione degli obiettivi di formazione e motivazione del programma

- Scelta del target rispetto al benchmarking globale.
- Selezione dell'equilibrio tra il livello auspicato di competenza per ciascun gruppo di dipendenti e il tempo di apprendimento totale necessario per portare i dipendenti a questo livello

Step 2:



Garanzia che la formazione sia ottimale per tutti i dipendenti

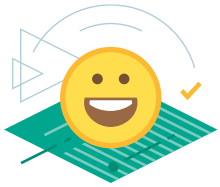
- Gestione dell'apprendimento automatizzata che permette a ogni dipendente di ottenere un livello di competenze appropriato ai rischi del proprio ruolo
- Rinforzo costante delle competenze acquisite per evitare che vengano dimenticate
- Formazione individuale delle persone, sulla base del proprio ritmo, in modo da evitare un eccessivo impegno o il rifiuto della stessa

Step 3:

Controllo dei progressi con analisi e report pratici

- Verifica in tempo reale dei dati, dei trend e delle previsioni
- Utilizzo dello strumento di real-time forecast per monitorare il raggiungimento dell'obiettivo formativo annuale
- Gestioni dei potenziali problemi prima che diventino reali (ad esempio, è possibile sapere quali unità organizzative hanno bisogno di più attenzione)
- Confronto dei benchmark sui risultati con i dati globali di Kaspersky Lab

Step 4:



Apprezzamento della formazione: garanzia ed efficienza

- Coinvolgimento dei dipendenti con esercizi interattivi pratici
- Scenari di apprendimento pertinenti alla vita lavorativa quotidiana dei partecipanti
- Possibilità di evitare una formazione eccessiva e inefficiente

Gestione del programma: la semplicità attraverso l'automazione

Avvio del programma in 10 minuti

- Obiettivi prefissati in base alle statistiche mondiali/del settore
- Avvio della formazione
- Fatturazione dei soli utenti attivi

La piattaforma consente di personalizzare l'apprendimento secondo le capacità individuali di ogni dipendente

- La piattaforma verifica automaticamente l'apprendimento e il superamento dei test sulle nozioni di base da parte dell'utente, prima di proseguire con la formazione.
- I responsabili non devono perdere tempo con l'analisi dei progressi individuali e le configurazioni manuali

Benefit derivanti da percorsi di apprendimento specifici per ogni profilo professionale

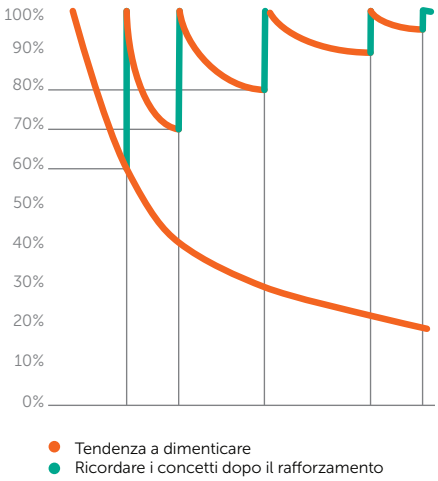
- Utilizzo di regole automatizzate per assegnare il livello di formazione finale desiderato ai singoli dipendenti Il livello finale è strettamente correlato al rischio rappresentato dallo specifico utente per l'azienda. Maggiore è il rischio, più elevato dovrebbe essere il livello di formazione finale. Ad esempio, utenti del reparto IT o contabilità tipicamente rappresentano un rischio più elevato rispetto a quello della maggior parte dei dipendenti di un ufficio.
- Ogni gruppo di utenti viene formato esclusivamente sul materiale pertinente al proprio ruolo, senza sprecare tempo di lavoro in altri training

Possibilità di ottenere report pratici in qualsiasi momento

- Dashboard contenenti tutte le informazioni necessarie alla valutazione dei progressi
- Suggerimenti su cosa fare per migliorare i risultati
- Confronto dei risultati con benchmark mondiali/di settore

La Curva dell'oblio di Ebbinghaus

Rafforzamento ripetuto per la creazione efficiente di competenze



Efficienza della formazione: micro apprendimento continuo

Le competenze aumentano livello dopo livello, dal più facile al più avanzato. La piattaforma riassegna automaticamente più moduli di formazione a coloro che non sono riusciti a completare il livello precedente. In questo modo si garantisce il mantenimento delle competenze e si evita che vengano dimenticate.

Micro apprendimento

- I contenuti sono strutturati appositamente per la micro formazione (da 2 a 10 minuti), per evitare lezioni lunghe e poco stimolanti.

Set completo di strumenti per tutti i moduli di formazione

- Ogni livello comprende: Modulo e video interattivi → Rafforzamento → Valutazione (test o attacco di phishing simulato)

Ciascun argomento comprende diversi livelli, in cui vengono spiegate nel dettaglio le competenze di sicurezza specifiche. I livelli vengono definiti secondo i gradi di rischio che contribuiscono a eliminare: il livello 1 è generalmente sufficiente a fornire protezione dagli attacchi più semplici e di massa, mentre per una protezione da attacchi più sofisticati e mirati è necessario studiare i livelli successivi.

Argomenti del corso di formazione*

- E-mail
- Navigazione in Internet
- Password
- Social network e servizi di messaggistica
- Sicurezza del PC
- Dispositivi mobili
- Dati riservati
- Dati personali/GDPR
- Social engineering
- Sicurezza a casa e in viaggio

Esempio: Competenze apprese nel modulo "Navigazione in Internet"

Base per prevenire attacchi semplici da individuare	Principiante per prevenire attacchi su un profilo specifico	Intermedio per prevenire attacchi di media complessità	Avanzato per prevenire attacchi mirati
13 competenze, tra cui: - Come configurare il PC (aggiornamenti, antivirus) - Come evitare siti web chiaramente dannosi (che chiedono di aggiornare il software, ottimizzare le prestazioni del PC, inviare SMS, installare lettori e così via) - Come riconoscere file eseguibili dai siti web	20 competenze, tra cui: - Come effettuare la registrazione/accesso solo su siti attendibili - Come evitare link numerici - Come inserire informazioni sensibili solo su siti attendibili - Come riconoscere gli indicatori di un sito web dannoso	14 competenze, tra cui: - Riconoscere link falsi - Riconoscere file e download dannosi - Riconoscere software pericolosi	13 competenze, tra cui: - Riconoscere link fittizi sofisticati (compresi i link che assomigliano ai siti web aziendali, link con reindirizzamento) - Evitare siti Black SEO - Effettuare il logout al termine delle sessioni di lavoro - Configurazione avanzata del PC (disattivare Java, adblock, noscript e così via)
	+ rafforzamento delle competenze di base	+ rafforzamento delle competenze precedenti	+ rafforzamento delle competenze precedenti

Argomenti chiave trattati: Link, Download, Installazioni software, Registrazione e accesso, Pagamenti, SSL

* L'elenco definitivo degli argomenti di formazione potrebbe subire modifiche.

Lingue

Nell'autunno 2018 la piattaforma è disponibile nelle seguenti lingue*:
- Inglese
- Tedesco
- Italiano
- Russo

Prossimamente:
- Arabo
- Francese
- Spagnolo

Nuove lingue vengono aggiunte regolarmente al fine di garantire una profonda ed efficace formazione in tutte le aree geografiche.

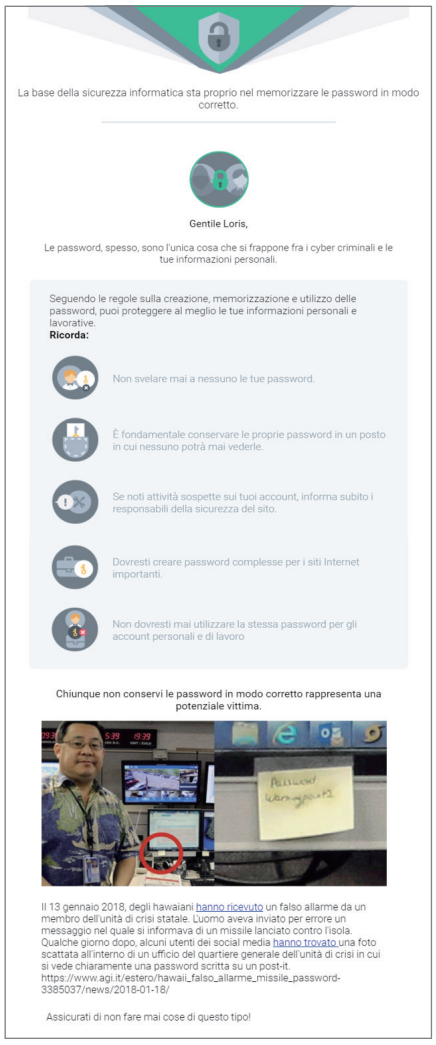
Approccio ludico ed esempi concreti per garantire l'efficienza della formazione

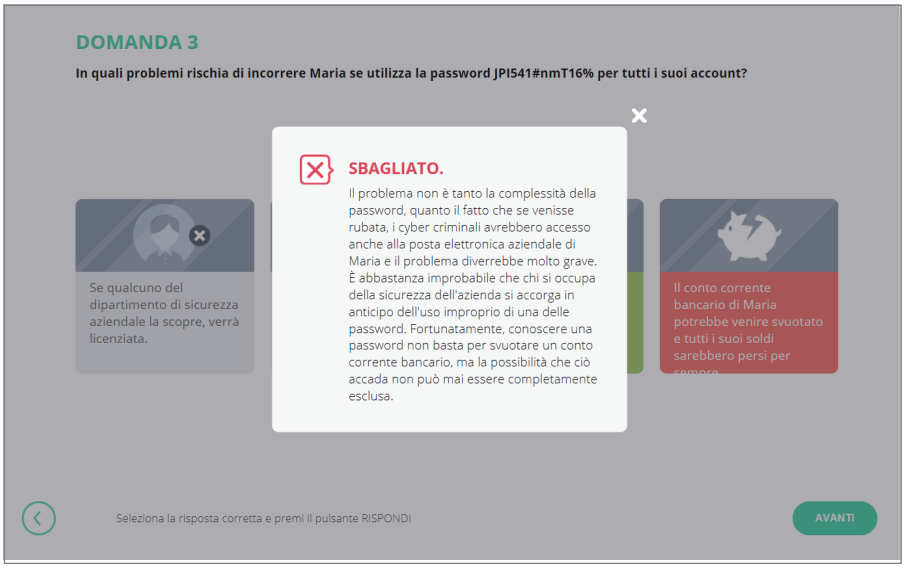
I contenuti della Piattaforma sono basati su principi di simulazione che mostrano eventi e situazioni reali ed evidenziano l'importanza della cybersecurity per i dipendenti. La Piattaforma è incentrata sulle competenze di formazione, non solo sulla parte teorica: gli esercizi pratici e le attività legate al dipendente sono al centro di ogni modulo.

I moduli combinano diversi tipi di esercizi, per mantenere alto l'interesse degli utenti, per allertarli e motivarli nell'apprendimento di un comportamento sicuro.

Lo stile e i testi non sono solo tradotti nelle diverse lingue, ma vengono adattati perché riflettano le culture locali.

Attività ed esercizi basati sulla simulazione per creare competenze pratiche e mantenere gli utenti attivi e motivati





* L'ordine e le date definitive delle localizzazioni possono variare.

Kaspersky® Security Awareness

Kaspersky Lab ha lanciato una famiglia di prodotti di formazione assistita tramite computer e basata su approccio ludico che utilizza tecniche di apprendimento moderne e si rivolge a tutti i livelli della struttura organizzativa. Questo approccio consente di creare una cultura collaborativa sulla cybersafety che genera un livello di sicurezza informatica autosufficiente in tutta l'organizzazione.

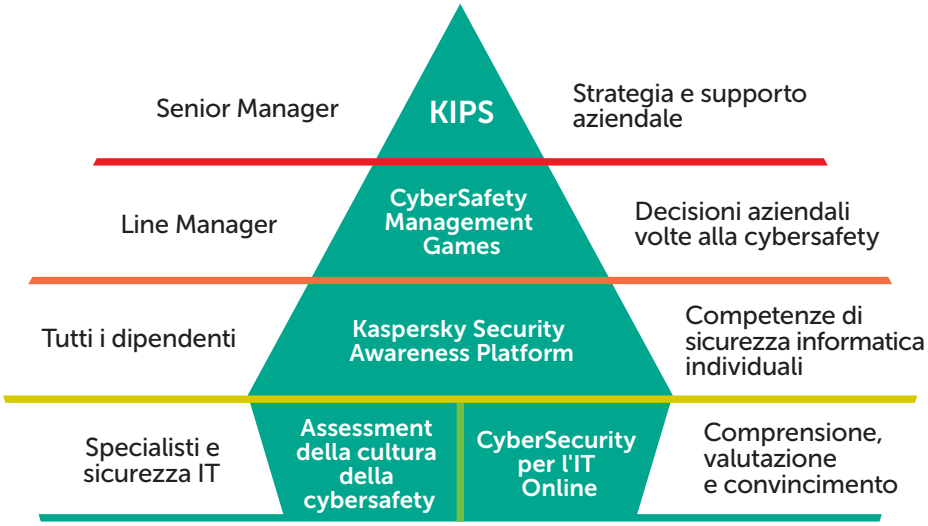
fino al
90%
di riduzione del numero totale di incidenti

non meno del
50%
di riduzione dell'impatto finanziario degli incidenti

fino al
93%
di probabilità che le conoscenze vengano applicate nel lavoro di tutti i giorni

oltre
30x
è l'incremento del ROI derivante dall'investimento nella consapevolezza in materia di sicurezza

sorprendente
86%
la percentuale dei partecipanti disposta a consigliare l'esperienza



Impostazione degli obiettivi e scelta del programma

- Impostazione degli obiettivi sulla base di dati globali
- Benchmarking su medie mondiali/del settore

Gestione dell'apprendimento

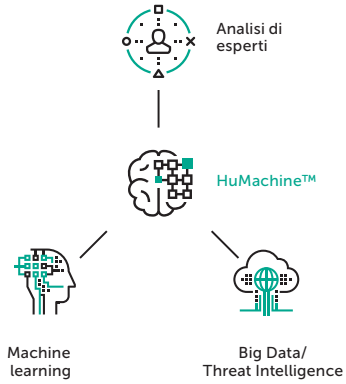
- Automazione dell'apprendimento
- Percorso di apprendimento adattivo
- Calcolo del tempo impiegato

Creazione di report e analisi

- Report pratici in qualsiasi momento
- Analisi "on-the-fly" del potenziale di miglioramento

Apprezzamento ed efficacia del programma

- Esercizi di coinvolgimento pratici
- Possibilità di evitare una formazione eccessiva e inefficiente
- Garanzia di un elevato livello di conoscenza e mantenimento delle competenze



Kaspersky Lab
Security Awareness **www.kaspersky.it/awareness**
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Novità sulle cyberminacce: **www.securelist.com**
Novità sulla sicurezza IT: **business.kaspersky.com/it**

#truecybersecurity
#HuMachine

www.kaspersky.it