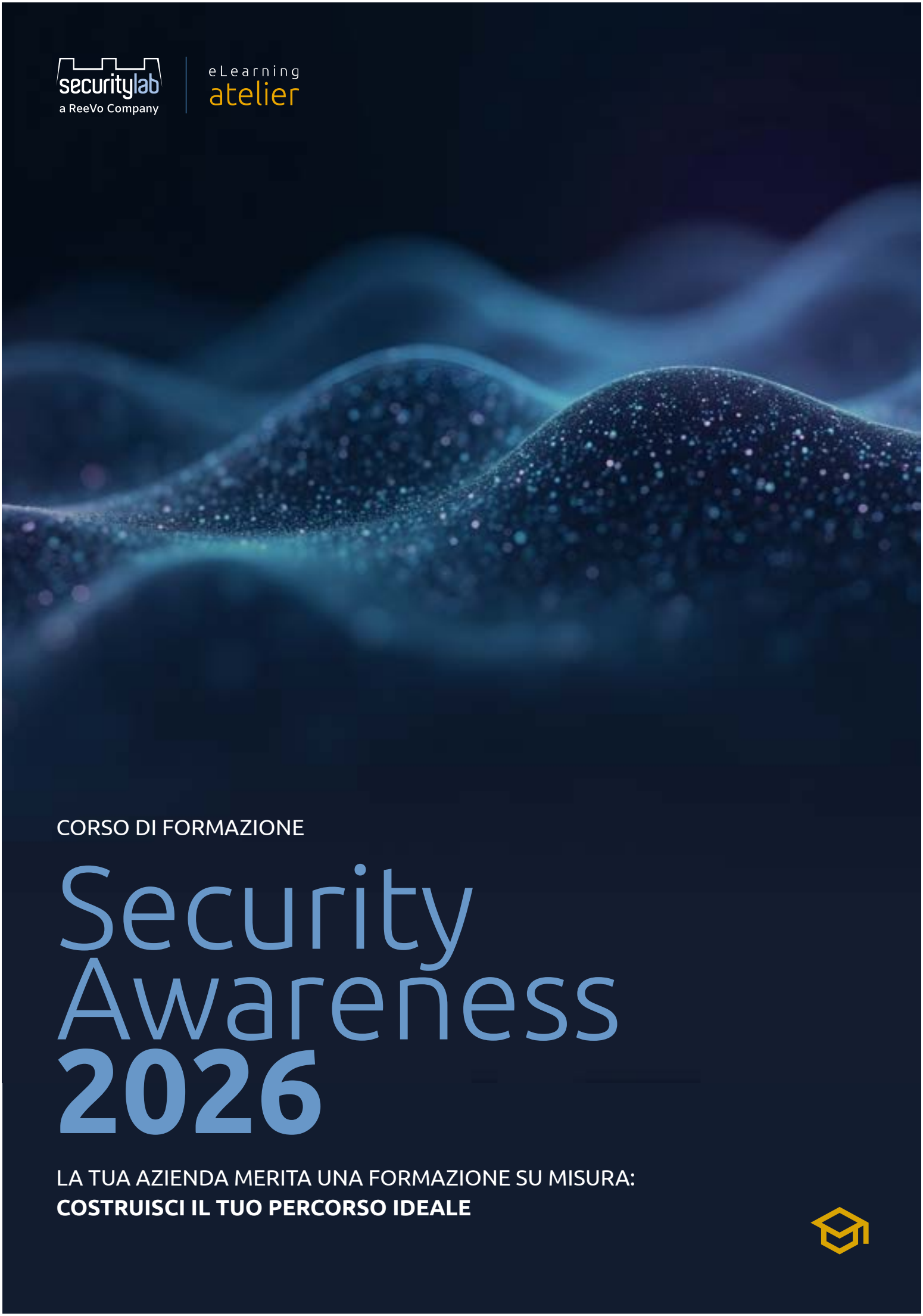
securitylab
a ReeVo Company

eLearning
atelier



CORSO DI FORMAZIONE

Security Awareness 2026

LA TUA AZIENDA MERITA UNA FORMAZIONE SU MISURA:
COSTRUISCI IL TUO PERCORSO IDEALE

“Gli esseri umani non sono l’anello debole, semplicemente non li abbiamo formati adeguatamente.”

Jessica Barker

Proteggi il tuo ecosistema digitale!

Formazione intelligente e personalizzata

Il nostro corso introduce un **approccio formativo su misura**: prima di ogni modulo, un test diagnostico valuta la competenza reale dell'utente sui 15 pilastri della cybersecurity contemporanea. Grazie ai risultati, il sistema configura automaticamente il percorso, proponendo esclusivamente i contenuti che colmano le lacune effettive di conoscenza.

Flessibilità di erogazione: questa modalità intelligente è una delle configurazioni possibili. La struttura modulare consente sia l'implementazione completa tradizionale che percorsi calibrati sulle necessità specifiche della vostra organizzazione.

Vantaggi concreti per l'organizzazione:

- **Valutazione affidabile**: diversamente dalle soluzioni basate su simulazioni phishing generiche, i nostritest su piattaforma Moodle, potenziati da intelligenza artificiale, misurano con precisione superiore le competenze reali
- **Automazione completa**: il sistema identifica autonomamente il percorso ottimale per ciascun utente, eliminando la necessità di configurazioni manuali
- **Ottimizzazione del tempo**: drastica riduzione delle ore improduttive concentrando l'apprendimento sulle effettive necessità formative
- **Monitoraggio puntuale**: tracciamento completo dei progressi e delle competenze sviluppate per ogni partecipante
- **Conformità normativa**: documentazione automatica dell'intero percorso formativo per audit e verifiche
- **Sicurezza potenziata**: dipendenti preparati specificamente sui rischi del proprio ruolo e settore
- **Prevenzione efficace**: riduzione mirata delle vulnerabilità umane più critiche per l'azienda

Architettura modulare: massima libertà progettuale

Il corso **Security Awareness 2026** presenta una struttura innovativa a componenti indipendenti. Ciascun modulo è autosufficiente e implementabile separatamente dagli altri.

Quest'architettura garantisce ai responsabili della formazione completa autonomia nella composizione di percorsi personalizzati, adattando i contenuti ai profili di rischio dei diversi reparti aziendali.

L'autonomia dei moduli permette inoltre una pianificazione temporale strategica, trasformando la sicurezza informatica da evento formativo isolato a processo continuativo che mantiene costante l'attenzione nel tempo.

Un metodo flessibile che risponde alle diverse necessità organizzative e si evolve insieme al panorama delle minacce digitali.

La sicurezza è fondamentale sul lavoro e nella quotidianità

Nell'attuale scenario digitale, ogni interazione online può nascondere un pericolo, sia in ambito lavorativo che personale. Le minacce informatiche evolvono con velocità sorprendente: i criminali affinano costantemente leloro tecniche, rendendo gli attacchi sempre più sofisticati e difficili da individuare.

Il corso **Security Awareness 2026** è stato interamente rinnovato per fronteggiare le sfide più attuali.

Fondato su situazioni reali, fornisce competenze concrete per:

- **Identificare istantaneamente attacchi di phishing e social engineering**
- **Salvaguardare efficacemente informazioni sensibili personali e aziendali**
- **Applicare misure di sicurezza per dispositivi mobile e domotica**
- **Proteggersi dalle frodi avanzate basate su intelligenza artificiale**
- **Tutelare la privacy personale e l'identità digitale**

Dalla cybersecurity fondamentale alle frodi potenziate da AI, ogni collaboratore acquisisce esattamente le competenze necessarie. Un metodo intelligente che trasforma l'adempimento formativo in investimento strategico, assicurando protezione aziendale ottimale e minimizzando drasticamente l'esposizione ai rischi informatici.

La consapevolezza rappresenta la prima e più efficace barriera contro le minacce informatiche. Questo corso supera la sicurezza aziendale, fornendo competenze fondamentali per proteggere anche la sfera digitale personale, la famiglia e i dati privati in un mondo costantemente connesso.

Esplora i fondamenti della sicurezza: un percorso strutturato

Il corso **Security Awareness 2026** propone un itinerario formativo completo che abbraccia tutte le dimensioni della sicurezza digitale contemporanea. Ciascun modulo è stato costruito per affrontare rischi specifici con un metodo pratico e immediatamente utilizzabile.

Dal social engineering alle frodi potenziate dall'intelligenza artificiale, dalla protezione delle credenziali alla sicurezza del lavoro remoto, questo corso fornisce strumenti concreti per muoversi con sicurezza nell'articolato panorama digitale odierno.

I moduli che costituiscono il percorso formativo sono stati realizzati analizzando centinaia di casi concreti di attacchi informatici, con particolare focus sul contesto internazionale. Le strategie di difesa proposte sono state selezionate per la loro comprovata efficacia e facilità di applicazione, assicurando benefici immediati sia in ambito professionale che personale.

I quindici moduli del corso

1

Introduzione alla Cybersecurity

Questo modulo fondamentale esplora i principi base della sicurezza informatica e la sua crescente importanza nella vita quotidiana. Vengono analizzate le principali minacce del panorama digitale attuale, dal furto di dati allo spionaggio, evidenziando come il fattore umano rappresenti spesso l'anello più debole nella catena della sicurezza. Il corso approfondisce gli obiettivi degli attacchi informatici e l'utilizzo malevolo dei dati personali rubati, sfatando il mito che solo le grandi aziende siano bersaglio dei criminali. Attraverso casi reali e scenari concreti, si acquisisce una solida consapevolezza sulla necessità di proteggere la propria presenza digitale, sviluppando un approccio proattivo alla cybersecurity.

2

Social engineering: l'arte dell'inganno

Questo modulo esplora le strategie di manipolazione psicologica impiegate dai criminali informatici per spingere le persone a rivelare informazioni confidenziali o eseguire azioni pericolose. Vengono analizzati imeccanismi psicologici sfruttati, come le tecniche di inganno e le fragilità umane, insieme alle metodologie più diffuse tra i truffatori. Il corso insegna a identificare i tentativi di manipolazione e presenta tattiche pratiche di difesa sia individuale che organizzativa, con l'obiettivo di sviluppare un'autentica cultura della sicurezza.

3

Phishing: l'inganno perfetto

Il modulo approfondisce il phishing in tutte le sue varianti, dalla modalità tradizionale alle tecniche più sofisticate. Vengono esaminati il phishing via email e siti contraffatti insieme ai loro meccanismi psicologici, per poi analizzare gli attacchi mirati come spear phishing e whaling verso i vertici aziendali. Si analizzano levarianti contemporanee come smishing (SMS), vishing (telefonate) e QRishing (codici QR), oltre alle tecniche evolute quali typosquatting, calendar phishing e IM phishing. Il corso affronta anche i rischi dell'integrazione dell'intelligenza artificiale nel phishing e fornisce metodologie efficaci di difesa e riconoscimento.

4

E-mail: regole essenziali per la protezione

Questo modulo analizza le email come principale canale di attacco informatico, esplorando le vulnerabilità, le categorie di minacce e le best practice per comunicare in sicurezza. Si esaminano le email come accesso privilegiato al mondo digitale, le frodi BEC (Business Email Compromise) in contesto aziendale e gli attacchi massivi con tecniche "spray-and-pray". Viene illustrato il rischio degli allegati dannosi e vengono fornite regole essenziali e tattiche di difesa efficaci nell'era dell'intelligenza artificiale.

5

Password: la prima linea di difesa

Il modulo esplora i sistemi di autenticazione, dall'utilizzo appropriato delle password convenzionali fino alle moderne soluzioni di autenticazione. Vengono insegnate metodologie per la generazione di password robuste e la gestione corretta degli accessi, i benefici e l'impiego dei password manager, e le passphrase come alternativa valida. Il corso sfata le false credenze sulla sicurezza delle password, spiega l'autenticazione multi-fattore(MFA) con le sue diverse tipologie e introduce le passkey come evoluzione dell'autenticazione passwordless.

6

Navigazione protetta

Questo modulo illustra i pericoli della navigazione online e le precauzioni indispensabili per proteggere i propridati. Si analizzano le differenze tra HTTP e HTTPS e le loro conseguenze per la sicurezza, come verificare l'autenticità dei siti web e i limiti del lucchetto HTTPS che può generare false sicurezze. Vengono evidenziati i rischi del phishing evoluto anche su siti HTTPS e fornite tecniche pratiche per una navigazione sicura quotidiana.

7

Mobile: opportunità e rischi

Il modulo si focalizza sulla sicurezza dei dispositivi mobili, analizzando rischi specifici e tattiche di protezione per smartphone e tablet. Vengono esaminati opportunità e pericoli dei dispositivi mobili, come identificare malware e spyware, la sicurezza delle applicazioni e la gestione delle autorizzazioni. Si affrontano i pagamenti digitali con i loro rischi, la protezione dei dati nel cloud, e la sicurezza sui social media e nelle applicazioni di messaggistica, con particolare attenzione alle frodi più diffuse su WhatsApp e altre piattaforme.

8

Digital Footprint: le tracce digitali

Questo modulo esplora il concetto di impronta digitale, analizzando come le nostre attività online generino tracce permanenti. Si spiega cosa costituisca l'impronta digitale e come si generi, il suo impatto sulla vita privata e professionale, con attenzione specifica ai rischi per i minori. Vengono illustrate le minacce connesse all'esposizione dei propri dati, le metodologie di pulizia e gestione della propria presenza online, e come costruire un'impronta digitale positiva e professionale.

9

Ransomware: l'arte del ricatto digitale

Il modulo analizza dettagliatamente la minaccia del ransomware, spiegando i meccanismi di attacco, le conseguenze e le strategie di prevenzione e risposta. Viene definito cosa costituisca il ransomware e come operi,i suoi meccanismi d'azione e canali di infezione, l'impatto immediato e duraturo degli attacchi. Si presentano strategie di prevenzione efficaci, l'importanza del backup e dei piani di recupero, e le azioni da intraprendere in caso di attacco.

10

Smart Working: lavorare in sicurezza

Questo modulo affronta le sfide di sicurezza specifiche del lavoro remoto, offrendo strategie pratiche per proteggere dati e comunicazioni al di fuori dell'ambiente aziendale. Si analizzano i rischi dell'ufficio domestico e le vulnerabilità nascoste, come tutelare la privacy durante il lavoro remoto, e gestire le emergenze informatiche da casa. Si parla della sicurezza dello spazio di lavoro fisico, delle comunicazioni protette durante videoconferenze e messaggistica, dell'equilibrio tra produttività e sicurezza, e della protezione dei dispositivi mobili in contesti lavorativi.

11

Truffe con l'Intelligenza Artificiale

Il modulo esplora le nuove frontiere delle frodi potenziate dall'intelligenza artificiale, analizzando tecniche emergenti e strategie di difesa. Vengono esaminate le videochiamate deepfake e come identificarle, la clonazione vocale e le frodi telefoniche evolute, e i metodi per identificare contenuti generati dall'IA. Si forniscono best practice quotidiane contro queste frodi, strumenti di verifica e protezione, e tecniche di salvaguardia dei propri dati biometrici.

12

Smart Home: proteggere i dispositivi

Questo modulo si concentra sulla sicurezza dei dispositivi connessi in ambiente domestico e personale, affrontando vulnerabilità e misure di protezione. Si esaminano rischi e vulnerabilità dei dispositivi smart home, la protezione di telecamere, assistenti vocali e altri dispositivi connessi, e l'importanza della configurazione sicura e degli aggiornamenti. Si illustra l'uso consapevole dei dispositivi IoT, la protezione della rete domestica, e la gestione della privacy con dispositivi costantemente connessi.

13

Fake news: riconoscerle e difendersi

Il modulo insegna come verificare l'autenticità delle informazioni online, fornendo strumenti pratici per riconoscere notizie false e contenuti manipolati. Si spiega cos'è il fact checking e perché è essenziale nella sicurezza digitale, la psicologia dietro la disinformazione e il metodo ESCAPE per la verifica rapida. Vengono presentati strumenti digitali accessibili per verificare immagini e notizie, come riconoscere contenuti falsi o manipolati, l'importanza del fact checking durante emergenze e crisi, e come proteggere familiari e amici dalla disinformazione.

14

Storage esterno: sicurezza dei dati in movimento

Questo modulo analizza i rischi legati ai dispositivi di archiviazione portatili e le strategie per proteggere i dati sensibili durante il trasporto. Vengono esaminati i pericoli della varietà e diffusione dei dispositivi, le vulnerabilità intrinseche dei supporti fisici e i rischi del trasferimento dati incontrollato. Si affrontano le minacce concrete come perdita, furto, degrado e danneggiamento dei supporti, e l'accesso non autorizzato aidati. Il corso fornisce strategie pratiche per la protezione efficace attraverso crittografia, controllo accessi, gestione fisica dei dispositivi e politiche di utilizzo sicuro, oltre a presentare strategie avanzate e alternative sicure per il backup strutturato.

15

Dispositivi indossabili: protezione pratica

Il modulo si concentra sulla sicurezza dei dispositivi indossabili e sulle strategie per proteggere i dati personali raccolti da questi strumenti sempre più diffusi. Vengono esaminati metodi efficaci per limitare la raccolta dati, gestire correttamente le autorizzazioni delle app companion e creare confini digitali per la propria privacy. Sianalizzano le tecniche per proteggere i dati sensibili attraverso la sicurezza degli account, la protezione delle trasmissioni Bluetooth e la sicurezza fisica dei dispositivi. Il corso illustra le configurazioni sicure, l'importanza degli aggiornamenti regolari e la separazione dei contesti d'uso, insieme a strategie di verifica periodica delle autorizzazioni e tecniche di minimizzazione dei dati.

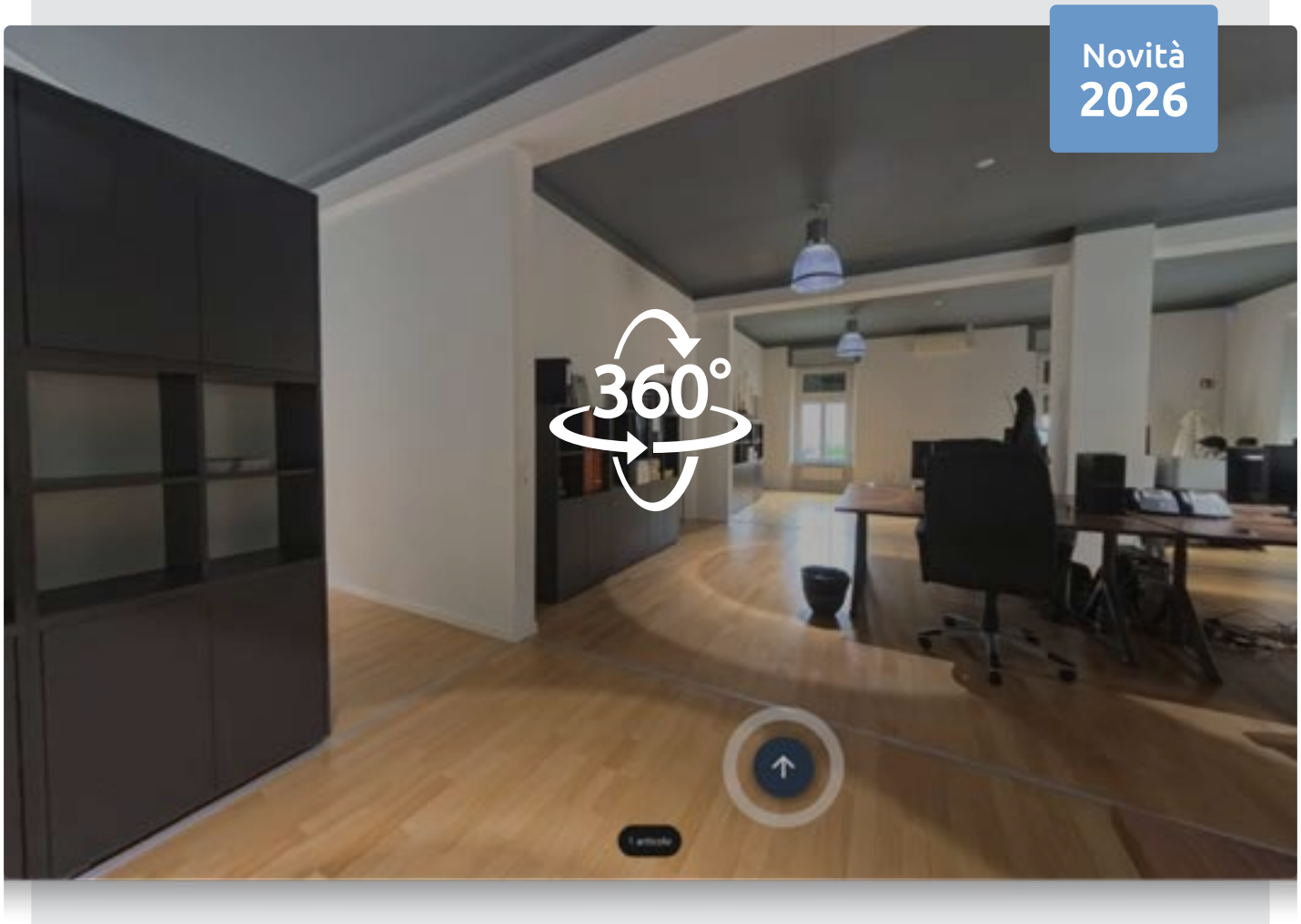
Phishing Detective: Esercitazione interattiva

Questo modulo interattivo offre un'esperienza pratica di apprendimento dove l'utente può testare le proprie capacità di riconoscimento delle email di phishing. Passando il mouse sui link sospetti e sugli indirizzi deimittenti, è possibile analizzare in tempo reale l'autenticità degli URL e dei dettagli del mittente per determinare se si tratta di comunicazioni legittime o tentativi di frode.

Attraverso esempi realistici e feedback immediato, questa simulazione sviluppa competenze concrete per identificare anche le più sofisticate tecniche di inganno, trasformando la teoria in abilità pratiche di difesa digitale quotidiana.

Ufficio a 360°: simulazione immersiva dei rischi

MODULO INTERATTIVO



Questo modulo offre un'**esperienza interattiva 3D** dove l'utente esplora un ambiente d'ufficio realistico per identificare rischi di sicurezza. Navigando nello spazio virtuale, il partecipante deve individuare vulnerabilità come dispositivi incustoditi, informazioni sensibili non protette, password visibili e altre minacce fisiche. Perogni elemento scoperto, il sistema fornisce spiegazioni sul rischio e suggerisce soluzioni pratiche.

Questa simulazione immersiva trasforma i concetti teorici in competenze pratiche, sviluppando la capacità di riconoscere rapidamente potenziali minacce nel proprio ambiente di lavoro quotidiano.

A chi si rivolge il corso?

Il corso **Security Awareness 2026** è stato progettato per rispondere alle esigenze di sicurezza di un pubblico eterogeneo.

In ambito professionale
Il corso si rivolge a manager e dirigenti che devono tutelare informazioni strategiche aziendali, collaboratori di ogni livello che utilizzano tecnologie digitali quotidianamente e team amministrativi che gestiscono dati critici e comunicazioni rilevanti.

In ambito personale
Il corso è rivolto a tutti coloro che desiderano migliorare la propria sicurezza nell'ambiente digitale. Il corso offre strumenti pratici e conoscenze essenziali per navigare con sicurezza nel cyberspazio, indipendentemente dal livello di competenza tecnologica.

Competenze tecniche avanzate non richieste
Il corso è stato sviluppato con un linguaggio accessibile ed esempi concreti, rendendo la sicurezza informatica comprensibile a tutti.

Esperienza di Apprendimento Innovativa

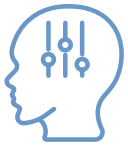
Il corso Security Awareness 2026 è stato sviluppato utilizzando tecnologie didattiche all'avanguardia per garantire un'esperienza di apprendimento coinvolgente ed efficace:

Navigazione intelligente e personalizzata

Il corso è strutturato con un'interfaccia interattiva che permette di navigare liberamente tra i contenuti. Ogni modulo è organizzato in sezioni tematiche interconnesse: un semplice click consente di accedere direttamente all'argomento di interesse, permettendo un percorso di apprendimento personalizzato in base alle proprie esigenze e priorità.

Contenuti multimediali accessibili

Ogni slide è arricchita da commenti audio professionali che guidano l'utente attraverso i concetti fondamentali. I sottotitoli sincronizzati garantiscono la piena accessibilità dei contenuti e facilitano la comprensione e la memorizzazione delle informazioni chiave, rendendo l'esperienza formativa completa ed inclusiva.



Apprendimento su misura

La struttura modulare e la ricca dotazione multimediale permettono di adattare il ritmo di apprendimento alle proprie necessità. Che si tratti di una formazione intensiva o di un percorso dilazionato nel tempo, la piattaforma supporta diverse strategie di apprendimento, mantenendo sempre alta l'attenzione grazie all'alternanza di elementi teorici e pratici.

Verifica formativa integrata

Ogni modulo si conclude con un test calibrato che consente di verificare la comprensione dei concetti fondamentali. La peculiarità di questo sistema risiede nel feedback articolato che accompagna ciascuna risposta: un commento mirato che approfondisce la tematica, chiarisce eventuali dubbi e consolida l'apprendimento. Questo approccio metodologico trasforma il momento valutativo in un'ulteriore occasione di crescita, favorendo una comprensione profonda e duratura dei contenuti essenziali del corso.

Monitoraggio e analisi dell'apprendimento

Il corso è supportato da un sofisticato sistema di monitoraggio che consente una visione completa del percorso formativo. Per i responsabili della formazione e i team HR, la piattaforma offre dashboard intuitive con report dettagliati sul progresso individuale e collettivo. È possibile visualizzare il tasso di completamento dei moduli, itempi di fruizione, le performance nei test e il livello di interazione con i contenuti. Questi dati, esportabili in diversi formati, permettono di valutare l'efficacia della formazione, identificare eventuali aree di miglioramento e personalizzare gli interventi formativi futuri. L'analisi integrata fornisce metriche oggettive sul ritorno dell'investimento formativo, trasformando la formazione da costo a investimento strategico misurabile.

Investi nella Sicurezza della tua Azienda

Richiedi una demo gratuita del corso Security Awareness 2026

info@elearningatelier.ch ↗

securitylab
a ReeVo Company

eLearning
atelier

www.elearningatelier.ch

eLearning Atelier - Corso Enrico Pestalozzi 21A, 6900 Lugano, Svizzera