



CORSO DI FORMAZIONE

Security Awareness 2025

LA TUA AZIENDA È UNICA:
PERSONALIZZA IL TUO PERCORSO FORMATIVO



***“La sicurezza non è un prodotto,
ma un processo. E tutto inizia dalla
consapevolezza.”***

Bruce Schneier, esperto di sicurezza informatica

Difendi il tuo mondo digitale!

Architettura modulare: libertà di costruire

Il corso **Security Awareness 2025** introduce un'innovativa **struttura a blocchi autonomi**. Ogni modulo vive di vita propria e può essere erogato indipendentemente dagli altri.

Questa architettura offre ai responsabili della formazione la libertà di comporre percorsi su misura, calibrando i contenuti in base ai profili di rischio specifici dei vari reparti.

L'indipendenza dei moduli consente inoltre una distribuzione temporale strategica, trasformando la sicurezza informatica da formazione una tantum a processo continuo che mantiene viva l'attenzione nel tempo.

Un approccio flessibile che risponde alle diverse esigenze aziendali e si adatta all'evoluzione costante delle minacce digitali.

Percorso formativo intelligente

Formazione adattiva su piattaforma Moodle

Il nostro corso introduce un sistema di apprendimento personalizzato: ogni modulo è preceduto da un test di assessment che valuta il livello di preparazione dell'utente sui 15 argomenti fondamentali della cybersecurity moderna. In base ai risultati ottenuti, il percorso si adatta automaticamente, mostrando solo i contenuti necessari per colmare i gap di conoscenza reali.

Modalità di erogazione flessibile: questa modalità adattiva rappresenta una delle opzioni disponibili. L'architettura modulare del corso consente anche l'erogazione tradizionale completa o percorsi personalizzati in base alle specifiche esigenze organizzative.

Benefici strategici per l'azienda:



Assessment intelligente: a differenza delle soluzioni che utilizzano fake phishing generico, i nostri test erogati su piattaforma Moodle ed elaborati con AI determinano con maggiore attendibilità la preparazione reale dell'utente



Gestione automatizzata: nessuna necessità di definire manualmente chi deve vedere quali contenuti - il sistema determina automaticamente il percorso ottimale per ogni utente



Efficienza formativa: riduzione drastica dei tempi morti e focus sui gap di competenza effettivi



Tracciabilità completa: monitoraggio dettagliato dei progressi individuali e delle competenze acquisite



Compliance automatica: documentazione puntuale del percorso formativo per audit e certificazioni



Protezione aziendale rafforzata: dipendenti formati specificamente sui rischi del loro ruolo e settore



Riduzione degli incidenti: prevenzione mirata delle vulnerabilità umane più critiche per l'organizzazione

Dalla cybersecurity di base alle truffe con intelligenza artificiale, ogni dipendente riceve la formazione esatta di cui ha bisogno. un approccio smart che trasforma l'obbligo formativo in crescita professionale strategica, garantendo protezione aziendale ottimale e riducendo significativamente l'esposizione ai rischi informatici.

La sicurezza è essenziale nel lavoro e nella vita quotidiana

Nel panorama digitale attuale, ogni click può rappresentare un rischio, sia in ufficio che a casa. Le minacce informatiche si evolvono con una rapidità impressionante: i criminali perfezionano continuamente le loro strategie, rendendo gli attacchi sempre più difficili da rilevare.

Il corso **Security Awareness 2025** è stato completamente rinnovato per affrontare le sfide più recenti.

Basato su casi reali, fornisce strumenti concreti per:



Riconoscere immediatamente tentativi di phishing e social engineering



Proteggere efficacemente dati sensibili personali e aziendali



Implementare misure di sicurezza per dispositivi mobile e smart home



Difendersi dalle truffe avanzate con intelligenza artificiale



Salvaguardare la privacy personale e l'identità digitale

La consapevolezza è la prima e più potente linea di difesa contro le minacce informatiche. Questo corso va oltre la sicurezza aziendale, offrendo competenze essenziali per proteggere anche la vita digitale privata, la famiglia e le informazioni personali in un mondo sempre più connesso.

Scopri le chiavi della sicurezza: un percorso completo

Il corso **Security Awareness 2025** offre un percorso formativo strutturato che copre tutte le dimensioni della sicurezza digitale moderna. Ogni modulo è stato progettato per affrontare minacce specifiche con un approccio pratico e immediatamente applicabile.

Dal social engineering alle truffe basate sull'intelligenza artificiale, dalla protezione delle password alla sicurezza dello smart working, questo corso fornisce strumenti concreti per navigare con sicurezza nel complesso panorama digitale attuale.

I moduli che compongono il percorso formativo sono stati sviluppati analizzando centinaia di casi reali di attacchi informatici, con particolare attenzione al contesto internazionale. Le tecniche di difesa presentate sono state selezionate per la loro efficacia e semplicità di implementazione, garantendo risultati 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 tecniche di manipolazione psicologica utilizzate dai criminali informatici per indurre le persone a divulgare informazioni riservate o compiere azioni rischiose. Vengono analizzati i meccanismi psicologici sfruttati, come l'arte dell'inganno e i punti deboli umani, insieme alle tecniche più utilizzate dai truffatori. Il corso insegna a riconoscere i tentativi di manipolazione e presenta strategie pratiche di difesa sia personale che aziendale, con l'obiettivo di sviluppare una vera cultura della sicurezza.

3.

Phishing: l'inganno perfetto

Il modulo approfondisce il phishing in tutte le sue forme, dalla versione tradizionale alle tecniche più sofisticate. Vengono esaminati il phishing via email e siti falsi insieme ai loro meccanismi psicologici, per poi passare agli attacchi mirati come spear phishing e whaling contro i dirigenti. Si analizzano le varianti moderne come smishing (SMS), vishing (telefono) e QRishing (codici QR), oltre alle tecniche avanzate quali typosquatting, calendar phishing e IM phishing. Il corso affronta anche i pericoli dell'integrazione dell'intelligenza artificiale nel phishing e fornisce tecniche efficaci di difesa e riconoscimento.

4.

E-mail: regole base per proteggersi

Questo modulo analizza le email come principale vettore di attacco informatico, esplorando le vulnerabilità, le tipologie di minacce e le migliori pratiche per comunicare in sicurezza. Si esaminano le email come porta d'accesso al mondo digitale, le truffe BEC (Business Email Compromise) in ambito aziendale e gli attacchi di massa con tecniche "spray-and-pray". Viene spiegato il pericolo degli allegati malevoli e vengono fornite regole base e strategie di difesa efficaci nell'era dell'intelligenza artificiale.

5.

Password: la prima linea di difesa

Il modulo esplora i sistemi di autenticazione, dall'uso corretto delle password tradizionali fino alle moderne tecnologie di autenticazione. Vengono insegnate tecniche per la creazione di password sicure e la corretta gestione degli accessi, i vantaggi e l'utilizzo dei password manager, e le passphrase come alternativa efficace. Il corso sfata i falsi miti sulla sicurezza delle password, spiega l'autenticazione a più fattori (MFA) con le sue diverse tipologie e introduce le passkey come futuro dell'autenticazione senza password.

6.

Navigazione protetta

Questo modulo illustra i rischi della navigazione online e le precauzioni necessarie per proteggere i propri dati. Si analizzano le differenze tra HTTP e HTTPS e le loro implicazioni per la sicurezza, come verificare l'autenticità dei siti web e i limiti del lucchetto HTTPS che può creare falsi sensi di sicurezza. Vengono evidenziati i rischi del phishing avanzato anche su siti HTTPS e fornite tecniche pratiche per una navigazione sicura quotidiana.

7.

Mobile: opportunità e rischi

Il modulo si concentra sulla sicurezza dei dispositivi mobili, analizzando rischi specifici e strategie di protezione per smartphone e tablet. Vengono esaminati opportunità e pericoli dei dispositivi mobili, come riconoscere malware e spyware, la sicurezza delle app 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 app di messaggistica, con particolare attenzione alle truffe più comuni 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 creano tracce permanenti. Si spiega cosa sia l'impronta digitale e come si formi, il suo impatto sulla vita personale e professionale, con attenzione particolare ai rischi per i minori. Vengono illustrate le minacce legate all'esposizione dei propri dati, le tecniche 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 in dettaglio la minaccia del ransomware, spiegando i meccanismi di attacco, le conseguenze e le strategie di prevenzione e risposta. Viene definito cosa sia il ransomware e come funzioni, i suoi meccanismi d'azione e vettori di infezione, l'impatto a breve e lungo termine 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 fuori dall'ambiente aziendale. Si analizzano i rischi dell'ufficio domestico e le vulnerabilità nascoste, come proteggere la privacy durante il lavoro da remoto, e gestire le emergenze informatiche da casa. Si parla della sicurezza dello spazio di lavoro fisico, delle comunicazioni sicure 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 truffe potenziate dall'intelligenza artificiale, analizzando tecniche emergenti e strategie di difesa. Vengono esaminate le videochiamate deepfake e come riconoscerle, la clonazione vocale e le truffe telefoniche avanzate, e i metodi per identificare contenuti generati dall'IA. Si forniscono buone pratiche quotidiane contro queste truffe, 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 ambito 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 sempre 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 ai dati. 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.

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. Si analizzano 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

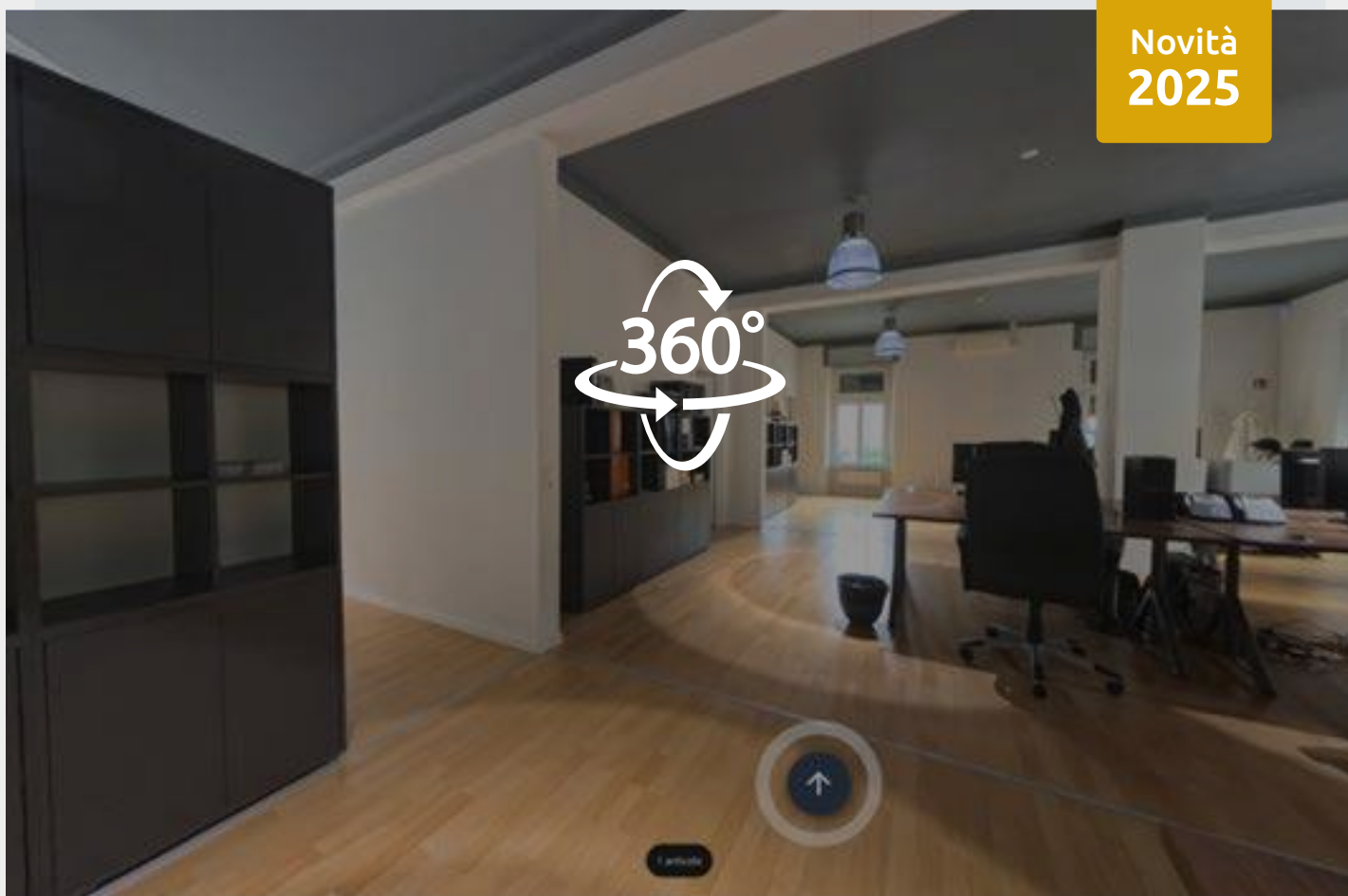
Questo modulo interattivo offre un'esperienza pratica di apprendimento dove l'utente può mettere alla prova le proprie capacità di riconoscimento delle email di phishing. Passando il mouse sui link sospetti e sugli indirizzi dei mittenti, è possibile analizzare in tempo reale l'autenticità degli URL 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

Novità
2025



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. Per ogni 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 è rivolto il corso?

Il corso **Security Awareness 2025** è stato progettato per rispondere alle esigenze di sicurezza di un pubblico diversificato.



In ambito professionale

Il corso si rivolge a manager e dirigenti che devono proteggere informazioni sensibili aziendali, dipendenti di ogni livello che utilizzano strumenti digitali quotidianamente e team amministrativi che gestiscono dati critici e comunicazioni importanti.



In ambito personale

Il corso è rivolto a tutti coloro che desiderano migliorare la propria sicurezza nel mondo digitale. Il corso offre strumenti pratici e conoscenze essenziali per navigare in sicurezza nel cyberspazio, indipendentemente dal livello di competenza tecnologica.



Non sono necessarie competenze tecniche avanzate

Il corso è stato sviluppato con un linguaggio chiaro e esempi concreti, rendendo la sicurezza informatica accessibile a tutti.

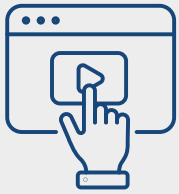
Esperienza di Apprendimento Innovativa

Il corso **Security Awareness 2025** 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, i tempi 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.



Proteggi la tua Azienda

Richiedi una demo gratuita del corso **Security Awareness 2025**

info@elearningatelier.ch ↗



www.elearningatelier.ch