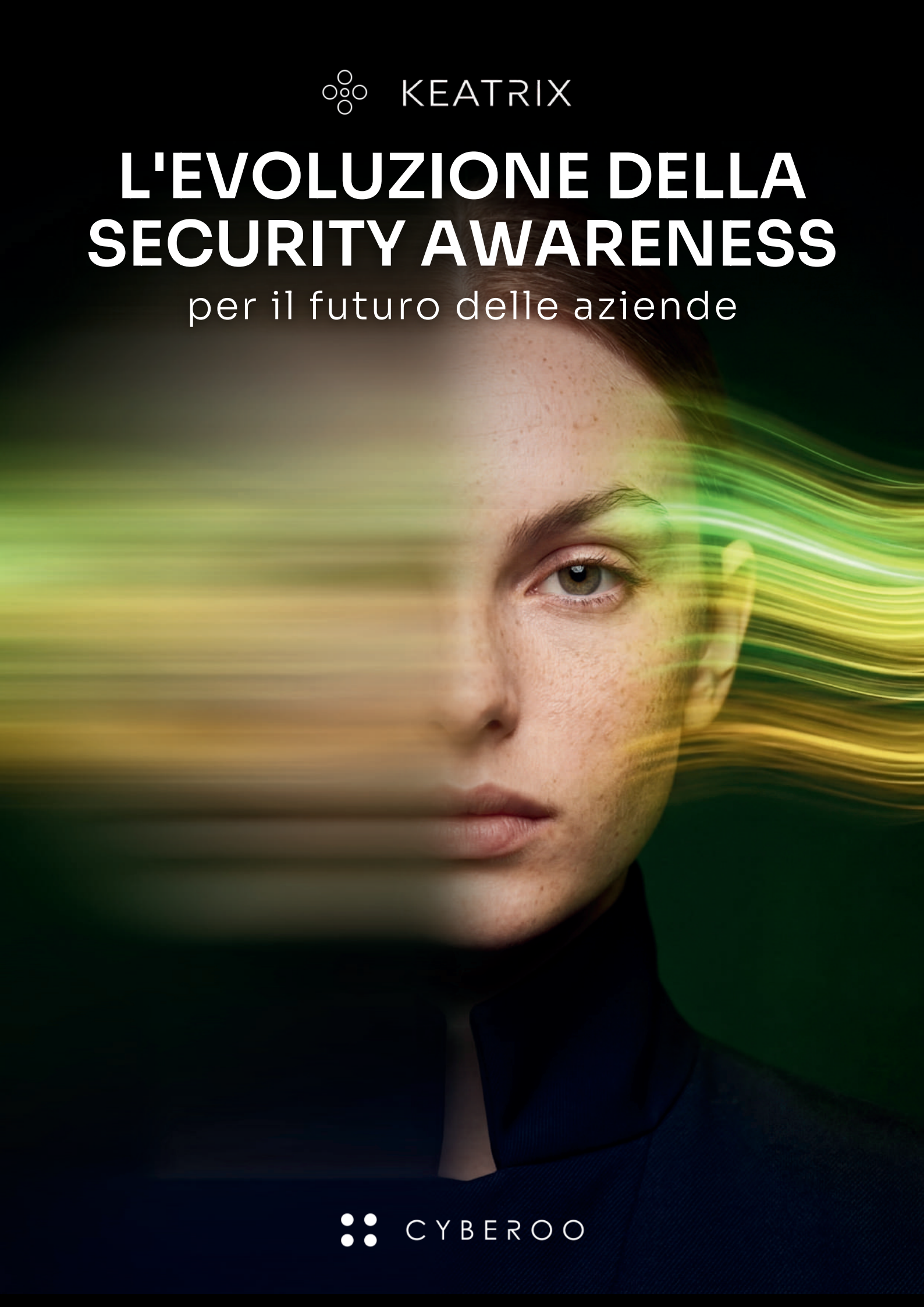
KEATRIX

L'EVOLUZIONE DELLA SECURITY AWARENESS

per il futuro delle aziende



CYBEROO

INDICE

Prefazione - Dentro il cervello umano	4
Verso la cyber resilience: una prospettiva strategica	11
Il ruolo del fattore umano negli incidenti di sicurezza	15
Security awareness: tutti i limiti dei modelli esistenti	20
Neuroscienze e comportamento umano: un approccio innovativo	24
KEATRIX: l'evoluzione del Security Awareness Training	27
Validazione scientifica e metriche di efficacia	41
Potenziali implicazioni per la cyber resilienza aziendale	45
Come finanziare la formazione in cybersecurity: quadro generale	47
Ricerca futura dell'apprendimento	49

Copyright © Cyberoo S.p.A. 2026
via Brigata Reggio 37, 42124, Reggio Emilia
email info@cyberoo.com
www.cyberoo.com

Tutti i diritti sono riservati a norma di legge e
a norma delle convenzioni internazionali.



Dentro il cervello umano: oltre i limiti neurocognitivi

La principale vulnerabilità alla base della maggior parte degli incidenti informatici non risiede in software non aggiornati, credenziali deboli o configurazioni di rete inadeguate, bensì in un organo di circa un chilogrammo e mezzo che consuma il 20% del nostro metabolismo energetico basale.

Tale organo è il cervello. Può trattarsi del proprio o di quello dei colleghi: di qualunque individuo che, in un determinato momento, stia elaborando un sovraccarico di stimoli, consultando comunicazioni tra impegni consecutivi, molteplici finestre operative aperte e continue notifiche in ingresso. Non si tratta di negligenza, ma di fisiologia.

Se il Novecento è stato definito il secolo del cuore, il Duemila è senza dubbio il secolo del cervello, perché sempre più discipline riconoscono che i processi cognitivi ed emozionali rappresentano la variabile determinante dei comportamenti complessi.

Il fattore umano è infatti coinvolto in circa il 60% delle violazioni di dati (Verizon, 2025). Non perché le persone siano incapaci, ma perché il cervello umano non è stato progettato per la cybersecurity. È stato progettato per garantire la sopravvivenza.

Per capire perché clicchiamo su un link malevolo prima di pensarci, bisogna capire come il cervello prende decisioni. Daniel Kahneman, premio Nobel per l'economia, ha descritto due modalità fondamentali: il Sistema 1, veloce, intuitivo e automatico, e il Sistema 2, lento, analitico e deliberativo.

Proprio il Sistema 1 è quello che ci fa frenare di colpo quando un bambino attraversa la strada. È anche quello che ci fa cliccare su "Verifica subito il tuo account" quando l'email sembra arrivare dalla nostra banca. I circuiti emotivi si attivano in millisecondi, prima che le aree prefrontali deputate al ragionamento e al controllo abbiano il tempo di intervenire.

È una scorciatoia evolutiva perfetta per sfuggire a un predatore. Molto meno perfetta per gestire un tentativo di phishing alle 17:30 di un venerdì.

Qui arriva la parte scomoda. La stragrande maggioranza dei dipendenti che cadono in un attacco, sanno che il phishing, ad esempio, esiste. Hanno fatto il corso. Hanno superato il quiz. Eppure, cliccano lo stesso.

Il motivo è che l'informazione, da sola, raramente basta a cambiare un comportamento in modo stabile. Se bastasse sapere, nessuno fumerebbe, tutti farebbero esercizio fisico e nessuno guiderebbe guardando il telefono.

Sul piano neuroscientifico, il processo che trasforma una conoscenza in un'azione abituale può essere descritto attraverso fasi distinte: prima l'informazione viene acquisita (letta, vista, ascoltata) e poi viene collegata a qualcosa che già conosciamo (attraverso esempi, analogie, storie), così che il cervello possa codificarla; dopo averla codificata, il cervello deve lavorarci sopra (la deve applicare, testare, deve sbagliare e correggersi), in altre parole, la deve rielaborare attivamente per consolidarla in una conoscenza stabile che sarà in grado di richiamare, in modo autonomo, nel momento in cui è richiesta. Soltanto a questo punto una conoscenza è in grado di tradursi in comportamento. Molti programmi di security awareness si fermano alle prime due fasi: trasferiscono informazioni e verificano la comprensione. Il risultato è che le persone “sanno” cosa dovrebbero fare, ma nel momento reale non lo fanno. Quel sapere non è ancora pronto per diventare un comportamento.

Ma c’è un passaggio ancora più a monte, che molti programmi formativi ignorano del tutto. Prima ancora di memorizzare, il cervello deve decidere che uno stimolo merita attenzione. Se questa soglia non viene superata, il processo di apprendimento non si attiva nemmeno.

Questo compito spetta a un sistema distribuito che le neuroscienze chiamano salience network: la rete della salienza. Questa rete funziona come un filtro continuo: tra le migliaia di stimoli che ci raggiungono ogni secondo, seleziona quelli che sono rilevanti (per novità, significato emotivo, urgenza, pericolo, ricompensa) e attiva le risorse cognitive necessarie a elaborarli.

Tutto ciò che non supera questo filtro, semplicemente, non entra nel circuito dell'apprendimento. Il motivo per cui, passeggiando in un bosco, noteremo un serpente a terra prima ancora di rendercene conto, è perché la nostra rete della salienza (con la nostra amigdala in prima linea) ha riconosciuto la minaccia e ha dirottato la nostra attenzione in una frazione di secondo.

Il problema è che un'email sospetta non è un serpente. Non è uno stimolo per cui il cervello ha una risposta biologica preparata. Nessuno nasce con un istinto per salvarsi dal phishing. Questo significa che la formazione in cybersecurity ha un compito particolarmente arduo: deve costruire artificialmente una salienza che la biologia non ci fornisce, facendo sì che il cervello impari a trattare un'email anomala con un livello di attenzione simile a quello che riserverebbe a un segnale di pericolo fisico.

Ed è esattamente il motivo per cui i contenuti emotivamente neutri, come slide, quiz, elenchi di regole, falliscono: non superano il filtro della salienza, sono rumore che il cervello scarta per risparmiare energia e risparmiare tempo. Per essere efficace, la formazione deve prima di tutto farsi notare. Per il cervello questo significa essere saliente, emotivamente rilevante.

Tutto questo succede proprio perché «il cervello è uno spilorcio cognitivo, se non può ricavarne del valore, smette di prestare attenzione» dice Oren Klaff e, infatti, conserva solo ciò che ritiene utile, ignora ciò che percepisce come ridondante e scarta ciò che non si aggancia a un'emozione o a un significato personale.

Hermann Ebbinghaus lo dimostrò già nel 1885 con la sua celebre curva dell'oblio: senza rinforzo, dimentichiamo la maggior parte delle informazioni nel giro di ore o giorni. Ma c'è un'eccezione potente: le esperienze emotivamente cariche. Un evento che ci spaventa, ci sorprende o ci coinvolge può restare impresso per anni.

Non è magia, è neurobiologia. Quando l'amigdala si attiva, potenzia i processi di consolidamento della memoria nell'ippocampo, rafforzando le connessioni sinaptiche che rendono quel ricordo duraturo.

C'è poi un ultimo problema strutturale: il modello one-to-many, in cui lo stesso corso viene proposto a centinaia di persone, ignora una realtà neuroscientifica fondamentale. Ogni cervello è unico, plasmato dalle proprie esperienze e dalla propria storia di apprendimento. Le differenze individuali nella capacità attentiva, nella memoria di lavoro e nella velocità di elaborazione sono documentate e misurabili, e incidono direttamente sull'efficacia di qualsiasi percorso formativo.

Il CFO che gestisce dati finanziari sensibili ha un profilo di rischio diverso dall'operaio in produzione che accede a un terminale condiviso. Formarli allo stesso modo, con gli stessi contenuti e gli stessi tempi, è come prescrivere lo stesso paio di occhiali a tutti i pazienti di un oculista.

È qui che entra in gioco l'adattività, attraverso la tecnologia. Parliamo di sistemi capaci di riconoscere come una persona apprende meglio, quali contenuti catturano la sua attenzione, quali si rivelano più efficaci e quali richiedono di cambiare approccio, trasformando la formazione in un processo one-to-one, modellato sul cervello della singola persona. In altre parole, la tecnologia diventa abilitante perché permette di adattare l'esperienza formativa a come ciascun individuo impara meglio.

Tutto questo porta a una conclusione chiara: la cybersecurity, per generare un cambiamento reale, deve allinearsi alle neuroscienze. Non basta aggiungere più informazioni, né aumentare la frequenza dei corsi. Serve costruire automatismi comportamentali.

E gli automatismi si costruiscono attraverso un mix preciso: ripetizione distribuita nel tempo, variazione dei contesti per generalizzare il comportamento, coinvolgimento emotivo per superare il filtro della salienza e attivare il consolidamento, e adattività per rispettare le differenze individuali. Quando un comportamento viene esercitato abbastanza a lungo secondo questi principi, il cervello lo automatizza progressivamente: l'attività delle aree prefrontali, inizialmente necessaria per guidare ogni decisione, diminuisce, mentre i circuiti sottocorticali legati alle risposte apprese assumono un ruolo crescente.

È un processo analogo a quello che ci permette di guidare senza pensare a ogni singolo gesto: dopo migliaia di ripetizioni in contesti diversi, il comportamento diventa fluido e naturale. La sicurezza informatica deve aspirare a questa stessa naturalezza.

Il giorno in cui un dipendente rifiuta una richiesta sospetta senza esitazione, segnala un'anomalia con la stessa naturalezza con cui chiude la porta di casa a chiave, controlla un link prima di cliccare senza che questo gli costi il minimo sforzo, quel giorno possiamo dire che la formazione ha funzionato. Non perché ha insegnato qualcosa, ma perché ha modificato il cervello.

È questo il contributo che le neuroscienze possono portare alla security awareness: trasformare un comportamento corretto da scelta consapevole a risposta automatica. Solo allora il fattore umano smette di essere una vulnerabilità e diventa, finalmente, parte della soluzione.

Di Andrea De Giorgio,
Head of Keatrix Research & Development



Verso la cyber resilience: una prospettiva strategica

La cybersecurity non è più quella di una volta. Quello che prima sembrava una questione di stampo tecnico confinata al reparto IT, oggi è diventata uno dei temi più importanti tra le priorità strategiche e di governance, in grado di condizionare l'esistenza e il futuro di un'azienda.

È un ecosistema invisibile ma ben presente, tutti ne facciamo parte, e una nostra piccola azione errata potrebbe aprire una voragine ben più grande, la cui bonifica e riempimento potrebbe costare milioni di euro. Basta un clic su un link di phishing o una password debole per compromettere interi sistemi. Come nel principio del Butterfly Effect, piccole variazioni nelle condizioni iniziali possono produrre grandi effetti sul comportamento a lungo termine dell'intero sistema.

"Che sarà mai!" viene facile pensare. Eppure, gli attacchi informatici causati da errori umani sono ancora oggi tra le cause principali degli incidenti cyber (ENISA, 2025). Un dato di fatto decisamente preoccupante se consideriamo che le piattaforme di security awareness esistono da molti anni. Allora perché ci sono ancora così tanti cyber attacchi causati da errori umani nonostante gli investimenti in formazione e tecnologie? Qualcosa non funziona.



Le tre cause principali degli incidenti informatici

- **Errori umani:** comportamenti involontari o distrazioni del personale che portano a esposizione o perdita di dati.
- **Attacchi malevoli:** violazioni perpetrate da attaccanti esterni o da insider con intenti criminali, mirano a sottrarre dati o compromettere sistemi.
- **Malfunzionamenti dei sistemi informatici:** problemi legati a malfunzionamenti tecnologici, configurazioni errate o vulnerabilità dei sistemi informatici.

Solo per citarne alcuni. 2023, ospedale ASL 1 Abruzzo: un dipendente apre un'email di phishing che porta al blocco dei sistemi e al furto di dati sanitari. 2024, Change Healthcare colpita da un ransomware dopo la violazione di un account remoto non protetto da autenticazione a più fattori (Cybersecurity Dive, 2024). 2025, azienda del Nord Italia: subisce un'intrusione dopo che un dipendente ha fornito inconsapevolmente agli attaccanti le credenziali VPN. Situazioni diverse, ma con lo stesso denominatore: un errore umano che trasforma una vulnerabilità potenziale in un incidente reale.

Gli esperti di etologia, nella coesistenza tra lupo e pastorizia, affermano: “Il lupo non è il problema. Il lupo scoperchia problemi già esistenti”. Non c’è dubbio che i criminali informatici rappresentino un problema serio, responsabili di gravi illeciti a danno di aziende e persone.

Tuttavia, questa affermazione ci offre uno spunto di riflessione. Quando un’azienda subisce un attacco informatico, c’è sempre qualcosa che è mancato, che non è stato fatto o è stato fatto male.

Tra gli errori più comuni rientrano:

- **La mancanza di processi avanzati** di monitoraggio e risposta attivi 24/7
- **Una gestione inadeguata del rischio** tramite la Cyber Threat Intelligence
- **La scarsa attenzione alla fase di remediation**, che include la gestione delle patch e degli aggiornamenti, oltre al semplice monitoraggio (detection)
- **L’assenza di una strategia preventiva** di risposta agli incidenti
- **Il controllo insufficiente della filiera** e dei fornitori
- **La carenza di formazione continua** rivolta a tutte le risorse umane (Osservatorio Cyberoo, 2025)

In questo documento ci focalizzeremo proprio sull'ultimo aspetto, la formazione, oggi più che mai di fondamentale importanza considerando la continua evoluzione delle tecniche, tattiche e procedure di attacco dei cyber criminali.

Solo per citarne alcune tra le più recenti: attacchi basati sull'intelligenza artificiale, come i deepfake o la clonazione della voce, nuove tecniche come il quishing, che sfruttano la fiducia nei QR Code per ingannare le vittime, i quantum attacks, che minacciano la sicurezza dei sistemi crittografici tradizionali (Global Risk Institute, 2024). Queste minacce rendono sempre più difficile distinguere il reale dal falso e accrescono in modo significativo il rischio di manipolazione e ingegneria sociale.

Solo trasformando il personale da anello debole a primo firewall dell'azienda, con metodologie di apprendimento realmente efficaci, è possibile costruire una cultura della resilienza e garantire la continuità del business. La vera sfida è cambiare i comportamenti delle persone, affinché ognuno diventi parte attiva della difesa aziendale (Gartner, 2024).

La Security Awareness deve, quindi, smettere di essere quel corso noioso che fai una volta l'anno e trasformarsi in un'abitudine quotidiana: così la consapevolezza non resta solo un'idea nella testa, ma diventa azione concreta, una difesa collettiva pronta a reagire anche quando le minacce cambiano strategia.



Il ruolo del fattore umano negli incidenti di sicurezza

Quando si parla di cybersecurity, il dibattito tende ancora a gravitare attorno ad aspetti tecnologici. La verità è ben diversa: la cybersecurity è più umana di quanto sembri. Non a caso, gran parte degli incidenti informatici non nasce da falle tecnologiche, ma da “falle cognitive”. In altre parole: non è stato il firewall a cliccare sul link del phishing, ma un essere umano in carne ed ossa e poca attenzione.

Un fatto è certo, oggi esiste una forte dissonanza cognitiva tra i comportamenti che adottiamo nella vita reale e quelli che mettiamo in atto nel mondo digitale. Nella quotidianità compiamo gesti di protezione in maniera quasi automatica: chiudiamo la porta a chiave quando usciamo di casa, non lasciamo incustoditi oggetti di valore, facciamo attenzione a chi ci avvicina in strada. Sono schemi di comportamento ormai radicati, che non richiedono nemmeno uno sforzo consapevole.

Eppure, quando ci spostiamo online, questa stessa logica di prudenza spesso viene meno. Si aprono link sospetti,
si condividono informazioni sensibili con leggerezza, si utilizzano password deboli o riutilizzate. In altre parole,
si dimentica di applicare al mondo digitale le stesse regole di buon senso e sicurezza che ci guidano nella vita fisica.

Il punto è che non si tratta di inventare nuovi comportamenti, ma semplicemente di trasferire quelli che già possediamo. Così come proteggiamo la nostra casa o i nostri beni, dobbiamo imparare a proteggere anche la nostra vita online, la nostra identità, i nostri dati e le nostre informazioni. Solo quando questo passaggio diventerà spontaneo, la security awareness smetterà di essere percepita come un obbligo e diventerà parte integrante della nostra quotidianità.

Questo concetto non vale solo a livello individuale: nelle aziende, la sicurezza informatica deve essere vista come una branca della gestione del rischio. Ogni decisione aziendale diventa un compromesso calcolato tra costi, benefici e rischio residuo accettabile. Non si tratta più solo di "evitare l'attacco", ma di ridurne l'impatto e garantire tre condizioni vitali: continuità operativa, reputazione integra e fiducia degli stakeholder.

Eppure, nonostante questa consapevolezza sia ormai scolpita in ogni policy aziendale, la pratica racconta un'altra storia. Le aziende investono milioni in soluzioni tecnologiche sempre più sofisticate, ma spesso ignorano processi e persone. Il risultato è sorprendente: una delle cause più impattanti degli incidenti di sicurezza è l'errore umano (ENISA, 2025). La conclusione è tanto semplice quanto importante: senza un coinvolgimento consapevole delle persone, nessuna tecnologia può garantire una protezione completa.

Le persone vengono frequentemente etichettate come “l’anello debole” della catena di sicurezza. Il dato statistico sembra confermarlo, ma la metafora è fuorviante: non si tratta di un anello fragile, quanto piuttosto di un elemento mai temprato. Un dipendente che non ha ricevuto la formazione adeguata non è un punto debole inevitabile, ma un firewall potenziale mai attivato. Con il giusto approccio, il fattore umano può trasformarsi dal problema più diffuso alla risorsa più potente.

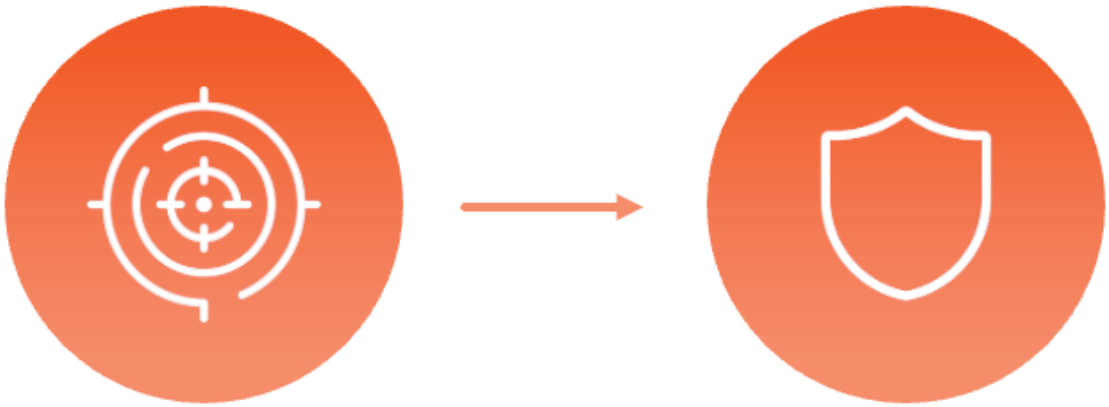
Gli attacchi moderni, dal phishing iper-personalizzato al ransomware-as-a-service, fino alle sofisticate compromissioni delle supply chain, hanno come bersaglio principale non tanto la tecnologia, ma la psicologia. L’anello debole non è il server, è la casella di posta dell’utente.

Ecco perché la cyber resilience non si costruisce soltanto accumulando tecnologie, ma sviluppando capacità adattive su tre fronti:

- **Riduzione del rischio residuo:** mappare vulnerabilità e processi per minimizzare l’impatto di un eventuale errore
- **Rapidità di risposta:** non basta evitare il disastro, bisogna saperlo contenere e ripartire in fretta
- **Preparazione del personale:** ogni dipendente deve saper riconoscere i segnali di un attacco e reagire in modo corretto e istintivo.

Sun Tzu, generale e filosofo cinese, ammoniva: “Se conosci il nemico e conosci te stesso, la tua vittoria è sicura”. Trasportato nel contesto della cybersecurity, questo concetto assume un doppio significato: conoscere a fondo i propri asset, i processi e le vulnerabilità interne, ma anche comprendere come evolvono le tattiche degli attaccanti. In questa prospettiva, l’errore umano non è un fastidio marginale, ma un punto critico da affrontare con metodo e rigore scientifico, esattamente come si farebbe aggiornando un IDS o calibrando una patch di sistema.

Il vero cambio di paradigma consiste nello spostare la percezione del personale: da vittime inconsapevoli a difensori proattivi. Non è l’errore umano il vero problema, ma la mancanza di una cultura della resilienza. Finché la sicurezza resterà percepita come un obbligo di compliance o un fastidio imposto dall’IT, gli incidenti continueranno a nascere da un clic sbagliato. Il giorno in cui ogni dipendente si sentirà parte attiva della difesa aziendale, l’anello debole diventerà finalmente l’anello forte.





I principali errori umani di cyber insicurezza

Cadere in trappole di phishing o social engineering: rispondere a email o messaggi ingannevoli, cliccare su link malevoli o fornire credenziali sensibili

Errori di configurazione dei sistemi: impostare in modo errato firewall, server o permessi di accesso, esponendo dati a malintenzionati

Perdita o furto di dispositivi non protetti: smarrire laptop, smartphone o chiavette USB senza adeguata sicurezza, consentendo l'accesso ai dati

Uso di password deboli o riutilizzate: facilitare accessi non autorizzati a sistemi e account aziendali o personali

Installazione di software non autorizzato: scaricare programmi non verificati che possono introdurre malware o vulnerabilità

Cancellazione o perdita accidentale di dati: eliminare file critici senza backup, causando interruzioni operative o esposizione di informazioni sensibili

Condivisione involontaria di informazioni sensibili: inviare dati riservati alla persona sbagliata o pubblicarli accidentalmente online.



Security Awareness: stato dell'arte e limiti dei modelli esistenti

Se la definizione di follia è "fare sempre la stessa cosa aspettandosi risultati diversi", allora buona parte dei programmi di security awareness rientra pienamente nella categoria. Come abbiamo visto, da anni le aziende investono in piattaforme di formazione senza ottenere i risultati sperati. È evidente che qualcosa non sta funzionando come dovrebbe.

Il primo problema è strutturale: la formazione tradizionale è episodica, statica e prevalentemente teorica. Corsi online, moduli e-learning, slide da scorrere e quiz finali: strumenti che generano un apprendimento superficiale, destinato a svanire nel giro di settimane. Non c'è nulla di "automatico" o "riflesso" in questo approccio. Non basta sapere che il phishing esiste: serve riconoscerlo in tempo reale, magari un lunedì mattina con tre riunioni in agenda e il caffè ancora a metà. I dati sono implacabili: **solo il 2% degli attacchi di phishing viene evitato** grazie ai modelli tradizionali (University of Chicago, 2025).

Chiunque sia stato a scuola lo sa: se l'approccio didattico è statico, molti studenti, anche se dotati di buon livello di intelligenza, finiscono per fallire. Allo stesso modo, un modello di formazione tradizionale non garantisce che le persone sappiano davvero reagire agli attacchi nella vita reale.

Un secondo vincolo concerne la portata dei programmi di formazione. Circa il 74% delle aziende non fornisce nessuna formazione o sensibilizzazione in cybersecurity tra i dipendenti (European Commission, 2024). Queste risorse rimangono prive di preparazione strutturata, con il conseguente effetto di generare potenziali vulnerabilità organizzative, assimilabili a "backdoor umane". Una backdoor, nel linguaggio informatico, è un accesso nascosto o non autorizzato a un sistema che permette a un attaccante di bypassare le normali protezioni di sicurezza. Allo stesso modo, un singolo errore di un dipendente può aprire un varco simile, compromettendo anche sistemi IT altamente protetti.



Inoltre, i programmi di formazione attualmente implementati adottano un approccio uniforme, trattando i dipendenti come un gruppo omogeneo e trascurando variabili quali ruolo, livello di esposizione al rischio e modalità di apprendimento individuali. Ad esempio, un CEO soggetto a spear phishing e un neoassunto alle prime interazioni con le comunicazioni aziendali ricevono lo stesso corso standardizzato, determinando un effetto formativo inefficace e generalizzato.

Numerosi interventi confondono inoltre la trasmissione di conoscenze con lo sviluppo di competenze operative. L'obiettivo dei sistemi formativi è spesso limitato a trasferire nozioni teoriche ("cos'è il malware", "quali sono le buone pratiche"), mentre l'obiettivo strategico dovrebbe essere la modifica dei comportamenti quotidiani, comprendenti azioni minime ma critiche: verificare la provenienza delle comunicazioni, non condividere credenziali e riconoscere tentativi di ingegneria sociale.

Se il fine resta la mera erogazione di conoscenze, il ritorno sull'investimento in sicurezza (ROSI) risulta trascurabile: le risorse vengono impiegate, la conformità normativa rispettata, ma il rischio permane invariato. Pertanto, la compliance normativa non è sinonimo di sicurezza effettiva.

È chiaro che il vero problema non risiede nell'assenza di programmi di formazione, bensì nella loro inefficacia metodologica. Evidenze neuroscientifiche indicano che per trasformare l'apprendimento in abitudine è necessario combinare ripetizione distribuita nel tempo, variabilità contestuale e coinvolgimento emotivo.

Trasformare l'apprendimento in abitudine



Contrariamente a tali indicazioni, la security awareness continua a proporre sessioni isolate, statiche e poco immersive, limitando l'efficacia dei percorsi formativi. La sfida non è "fare un corso in più", ma radicare la sicurezza nella cultura aziendale, trasformando la conoscenza in comportamento e il comportamento in abitudine. Quando ogni dipendente comprende di essere il primo livello di protezione, la sicurezza smette di essere una burocrazia IT e diventa un valore condiviso.



NEUROSCIENZE E COMPORTAMENTO: un approccio innovativo

Se la cybersecurity fosse solo questione di sapere, oggi saremmo tutti invincibili. Nessuno userebbe mai un Wi-Fi pubblico e le password sarebbero tutte composte da 32 caratteri alfanumerici con simboli e maiuscole alternate. Eppure, non è così.

Perché? Perché tra il “sapere” e il “fare” esiste un abisso: il cervello umano.

Ogni informazione che riceviamo segue un percorso preciso nel cervello . Prima viene filtrata dai sensi e inviata al talamo, che smista i segnali. Da qui, la rotta può prendere due direzioni:

- **La via veloce**, che passa per **l’amigdala**, il nostro centro di reazioni istintive
- **La via lenta,** che coinvolge la **corteccia prefrontale**, sede del ragionamento logico e della valutazione consapevole

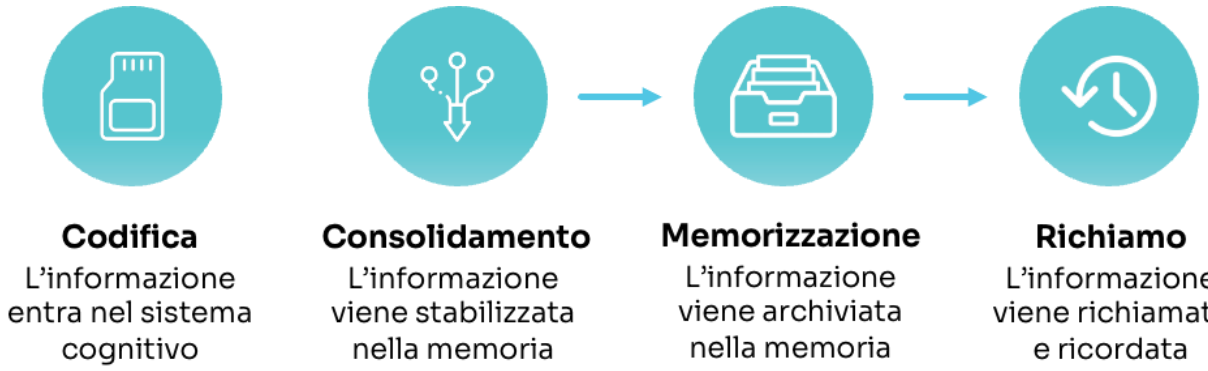
L’amigdala è molto più rapida della corteccia: il nostro cervello reagisce prima di ragionare. È il motivo per cui, sotto stress, possiamo cliccare sul link malevolo ancor prima di ricordarci che “il phishing esiste”.

Affinché la conoscenza diventi comportamento servono almeno tre passaggi fondamentali:

1. **Codifica:** l'informazione viene registrata nella memoria a breve termine

2. **Consolidamento:** attraverso la ripetizione e il coinvolgimento emotivo, il dato viene spostato nella memoria a lungo termine (ippocampo e corteccia).

3. **Automatizzazione:** con l'esercizio costante, il comportamento diventa riflesso, bypassando lo sforzo cognitivo cosciente.



La vera difesa nasce quando il cervello non deve più "pensare" alla sicurezza, ma la applica in modo naturale e immediato. Pertanto, è necessario superare la fase 1 (codifica), tipica delle piattaforme tradizionali, e procedere alle fasi 2 e 3 (consolidamento e automatizzazione), che implicano un effettivo cambio di comportamento e l'instaurazione di abitudini durature a livello individuale e organizzativo.

Le neuroscienze ci ricordano sempre che:

- **La ripetizione dilatata nel tempo** rafforza la memoria a lungo termine
- **La variazione dei contesti aumenta** la capacità di riconoscere la minaccia in situazioni reali
- **Il coinvolgimento emotivo** attiva l'amigdala, creando ancore mnemoniche molto più durature di un elenco di "best practice" su slide

Un dipendente formato non è quello che sa definire cos'è un malware durante un quiz, ma quello che, quando un collega gli chiede al volo la password di accesso a un gestionale "perché ha urgenza e non riesce a loggarsi", rifiuta la richiesta, la segnala e continua a lavorare senza farsi prendere dal senso di colpa. La differenza la fa il comportamento, non la nozione.

Ecco perché il cambiamento comportamentale è il vero fattore critico della sicurezza: senza trasformare la teoria in automatismi cognitivi, la formazione rimane sterile.

L'obiettivo è proprio allenare il cervello a reagire in modo corretto senza pensarci troppo. Un po' come guidare: all'inizio controlli lo specchietto con consapevolezza, poi diventa un gesto naturale. La cybersecurity deve diventare la stessa cosa: un riflesso condizionato, non un esercizio di memoria. Solo allora la consapevolezza smette di essere un concetto teorico e diventa vera resilienza quotidiana.

KEATRIX: l'evoluzione del Security Awareness Training

Per superare queste criticità nasce KEATRIX, la Human Risk and Security Training Platform innovativa sviluppata da Cyberoo per trasformare radicalmente il concetto di security awareness e inaugurare una nuova era nella cybersecurity.

Si tratta di una piattaforma che parte da un presupposto diverso rispetto al passato: la cybersicurezza non si insegna, si allena. L'obiettivo non è far ricordare nozioni astratte, ma modificare comportamenti. Attraverso il metodo scientifico innovativo NeLP, mette al centro l'essere umano come protagonista attivo dell'apprendimento, valorizzando le sue modalità uniche di percepire, decidere e agire.

Il nome KEATRIX non è casuale. Unisce due figure simboliche molto distanti, ma accomunate da un'idea fondamentale: la consapevolezza richiede la capacità di osservare il mondo con occhi nuovi.

- **John Keating:** l'insegnante anticonformista de "L'attimo fuggente", rappresenta un approccio educativo che libera dalla rigidità dei modelli tradizionali. Non si limita a trasmettere nozioni, ma insegna a guardare le cose da punti di vista diversi, sviluppando il pensiero critico.

- **Neo:** protagonista di Matrix, incarna l'atto volontario di scegliere la verità anche quando è scomoda. La famosa pillola rossa non è solo una metafora filosofica, ma un invito a vedere ciò che di solito ignoriamo.

KEATRIX eredita da entrambi un principio fondamentale: per affrontare il rischio cyber, non basta imparare delle regole. Occorre mettere l'utente in condizione di ragionare, scegliere, riconoscere i segnali, anticipare il pericolo.

Le tre discipline che rendono KEATRIX davvero efficace

La piattaforma si fonda sull'integrazione di tre ambiti che raramente dialogano tra loro nel mondo della formazione sulla sicurezza:

1. **Neuroscienze:** il Metodo NeLP sfrutta i processi cognitivi umani per strutturare l'apprendimento in modo naturale e progressivo

2. **Tecnologia:** un motore di AI adattiva che costruisce percorsi personalizzati, capaci di seguire il ritmo, le necessità e il livello di ciascun utente

3. **Arte e narrativa:** contenuti cinematografici, animazioni, personaggi e storytelling per rendere memorabile ciò che viene appreso.

Il risultato è un mix che non somiglia ai classici corsi di awareness: più vicino a un'esperienza immersiva che a un modulo didattico.

Il cuore neuroscientifico: il Metodo NeLP

Il nucleo metodologico di KEATRIX si fonda sul metodo scientifico **Neuroscientific Learning Pattern (NeLP)** che unisce le più recenti evidenze delle neuroscienze cognitive alla sicurezza informatica.
A differenza della formazione tradizionale, basata sul bombardamento di informazioni, il Metodo NeLP segue il modo in cui il cervello realmente impara. Il percorso è suddiviso in quattro fasi, ciascuna studiata per attivare specifici meccanismi cognitivi, dall'acquisizione al richiamo:

Acquisizione

I concetti vengono introdotti in modo chiaro, calibrati sul ruolo e sul contesto dell'utente. Nessuna terminologia complicata, nessuna barriera cognitiva. L'obiettivo è creare un primo aggancio mentale solido e comprensibile.

Codifica

Qui entra in gioco la multimodalità. Testo, immagini, suoni, interazione, elementi narrativi: tutto ciò che serve per stimolare simultaneamente più canali percettivi. Questa fase rafforza l'immagazzinamento delle informazioni nella memoria a lungo termine.

Rielaborazione attiva

Il cuore della formazione comportamentale. L'utente viene esposto a scenari realistici, simulazioni e micro-situazioni ispirate a casi concreti. Questo permette di costruire una memoria procedurale, la stessa che utilizziamo quando guidiamo o rispondiamo automaticamente a un imprevisto.

Richiamo

Le conoscenze vengono riproposte nel tempo, con variazioni che impediscono il semplice ricordo meccanico. Il fine è consolidare la capacità di recuperare l'informazione quando serve davvero, non solo durante un test.



Spacing, interleaving e plasticità neurale: come KEATRIX consolida l'apprendimento

Il metodo si basa su evidenze scientifiche consolidate:

Spacing effect

Distribuire l'apprendimento nel tempo permette al cervello di sedimentare meglio le informazioni. È il contrario della formazione concentrata "tutta in un giorno", che dà un'illusione di apprendimento rapido ma si dissolve nel giro di poche settimane.

Interleaving

Alternare gli argomenti rende l'apprendimento più flessibile. L'utente impara a riconoscere pattern e a trasferire ciò che ha imparato in contesti diversi, qualità essenziale per affrontare minacce in continua evoluzione.

Plasticità sinaptica e LTP

Il cervello si modifica fisicamente quando apprende. KEATRIX progetta i contenuti affinché le nuove reti neurali vengano rafforzate nel tempo, trasformando concetti astratti in competenze operative.

L’AI adattiva che costruisce percorsi davvero unici

Una delle convinzioni più diffuse nel mondo della formazione è che basti creare un corso chiaro e completo perché tutti possano apprendere allo stesso modo. La realtà è molto diversa. Le persone non sono identiche. Non hanno le stesse esperienze, non partono dallo stesso livello, non apprendono con lo stesso ritmo, non reagiscono agli stessi stimoli.

Se la formazione ignora queste differenze, diventa inevitabilmente inefficace: c’è chi si annoia, chi si perde, chi non capisce, chi dimentica.

KEATRIX parte da un presupposto molto semplice ma raramente applicato: **l’apprendimento è personale**.

Per questo la piattaforma utilizza un motore di AI adattiva progettato per modellare il percorso sulla singola persona. Non esiste un “programma standard” che tutti devono seguire.

Esistono migliaia di percorsi possibili, costruiti istante per istante analizzando:

- **Il livello** di conoscenza iniziale
- **Lo stile** di apprendimento individuale
- **Il tempo reale** che l'utente può dedicare
- **Il ruolo e l'ambiente** operativo in cui lavora
- **La difficoltà dei contenuti** man mano che vengono affrontati
- **La velocità** con cui l'utente risponde, sbaglia, recupera
- **I pattern personali** che emergono durante il percorso

L'obiettivo non è solo rendere la formazione "più comoda", ma più naturale. Quando il cervello si trova davanti a contenuti calibrati esattamente sul proprio livello, entra in quello che gli psicologi chiamano "stato di flusso": tutto sembra scorrere meglio, lo sforzo cognitivo si riduce e le informazioni vengono immagazzinate più velocemente.



Perché la personalizzazione è così importante, soprattutto nella cybersecurity

La sicurezza informatica non è una competenza teorica. È un insieme di riflessi, micro-decisioni, abitudini. Sono comportamenti che si mettono in atto automaticamente nei momenti critici: quando arriva una mail sospetta, quando un collega chiede con troppa leggerezza una password, quando una procedura frena sul flusso di lavoro e si è tentati di aggirarla.

Questi automatismi si formano solo se l'apprendimento è sedimentato. E si sedimenta solo se è modellato sulla persona.

Un utente esperto di tecnologia non ha bisogno di essere trattato come un principiante. Un utente che ha già subito un attacco di phishing reagisce in modo diverso rispetto a chi non ha mai avuto esperienze negative. Una persona impulsiva apprende in modo diverso da una riflessiva.

KEATRIX riconosce queste differenze e si adatta. Cambia tono, ritmo, livello di profondità, complessità degli scenari. Suggerisce contenuti diversi a seconda dei punti deboli che emergono nel tempo. È una formazione che cresce insieme alla persona.

C'è poi un effetto collaterale molto positivo: la personalizzazione spinge l'utente a capire meglio come apprende. È ciò che in psicologia viene chiamata metacognizione.

In altre parole, il sistema non si limita a “dare risposte”, ma aiuta la persona a prendere coscienza dei propri schemi mentali: cosa capisce subito, cosa le è difficile, quale modalità funziona meglio per lei.

Questa consapevolezza è fondamentale perché la sicurezza non è statica. Le minacce cambiano, le tecniche evolvono, e la capacità di aggiornarsi nel tempo diventa un valore professionale a lungo termine.

La personalizzazione non è un vezzo tecnologico, ma un mezzo per ottenere un obiettivo molto concreto: **trasformare le buone pratiche in abitudini stabili.**

Abitudini che non si dimenticano dopo due settimane. Abitudini che scattano automaticamente. Abitudini che, nel momento critico, fanno davvero la differenza tra un incidente evitato e un incidente subito.



EDUTAINMENT: quando l’emozione incontra la sicurezza

Il cervello ricorda ciò che lo coinvolge emotivamente. Non è una frase ad effetto, ma un dato neuroscientifico molto concreto: quando proviamo sorpresa, curiosità, tensione o empatia, entra in gioco l’amigdala, la struttura cerebrale che regola le risposte emotive e decide quali informazioni meritano di essere conservate nella memoria a lungo termine.

Se l’amigdala si attiva, le probabilità che un contenuto venga ricordato anche dopo settimane aumentano in maniera significativa. È lo stesso meccanismo che ci permette di ricordare un film visto anni fa, ma di dimenticare una presentazione aziendale dopo pochi giorni.

KEATRIX sfrutta questo principio biologico per trasformare la formazione in un’esperienza che il cervello riconosce come rilevante.

Per questo integra:

- **Avatar** e personaggi ricorrenti
- **Brevi cortometraggi** che simulano situazioni reali
- **Scenari narrativi** in cui l'utente deve compiere scelte
- **Un'estetica cinematografica** progettata per creare coinvolgimento emotivo

Non si tratta di intrattenimento fine a sé stesso. Lo scopo è stimolare l'amigdala e agganciare la memoria episodica dell'utente, così che gli errori da evitare, i segnali di allarme e le buone pratiche di sicurezza rimangano impressi molto più a lungo rispetto ai modelli tradizionali di formazione.

In altre parole: KEATRIX non vuole far "ricordare il corso", ma far ricordare le reazioni corrette quando servono davvero, nel momento in cui un attacco inizia a farsi strada nella casella di posta o nella vita digitale quotidiana.

CERTIFICAZIONI PERSONALI: un valore che segue la persona

Ogni utente riceve certificazioni individuali, tracciate tramite un codice univoco. Non sono badge generici, ma indicatori reali del livello di competenza raggiunto. Il valore di queste certificazioni rimane alla persona anche se cambia azienda, trasformando la formazione in un elemento concreto di crescita professionale.

KEATRIX non nasce per aggiungere l'ennesimo corso obbligatorio all'agenda dei dipendenti. Nasce per cambiare il modo in cui apprendiamo la sicurezza. Per trasformare l'utente da punto debole a risorsa attiva. E per creare, finalmente, una cultura cyber che non sia uno slogan, ma una pratica quotidiana.

Il contributo distintivo di KEATRIX ai processi di apprendimento

Chiarezza e misurabilità degli obiettivi

Ogni percorso formativo è definito da metriche verificabili, con l'obiettivo di generare cambiamenti comportamentali concreti. Non semplici nozioni, ma abitudini operative che riducono il rischio umano e rafforzano la compliance.

Didattica interattiva e coinvolgente

Attraverso l'edutainment – video-avatar, scenari narrativi e contenuti emotivamente coinvolgenti – la piattaforma stimola la memoria episodica, trasformando l'apprendimento da obbligo passivo a esperienza partecipativa.

Personalizzazione dinamica dei contenuti

I contenuti sono adattati al ruolo, al settore e al livello di consapevolezza dell'utente, garantendo percorsi pertinenti e mirati, con massima efficacia formativa.

Metodologie su misura e processi metacognitivi

Grazie all'Adaptive Learning, i percorsi si rimodellano in tempo reale sulle performance, stimolando elaborazione e metacognizione per consolidare comportamenti stabili e replicabili.

Il contributo distintivo di KEATRIX ai processi di apprendimento

Fruibilità e accessibilità ottimale

Interfacce intuitive e accesso multi-dispositivo rendono la fruizione continua e senza barriere, mantenendo il focus sull'apprendimento.

Profondità e autenticità delle valutazioni

Le valutazioni misurano il reale cambiamento comportamentale, con report dettagliati sull'impatto in termini di riduzione del rischio e ritorno sull'investimento formativo.

Rafforzamento continuo delle competenze

Tecniche di spacing e interleaving consolidano le conoscenze nel tempo, trasformandole in comportamenti operativi stabili e in abitudini durature.



Validazione scientifica e metriche di efficacia

La piattaforma KEATRIX si basa su metriche comportamentali oggettive e su un sistema di valutazione continuo. Questo metodo consente di monitorare l'efficacia del programma in tempo reale, fornendo dati concreti sulla riduzione del rischio comportamentale e sull'aumento della resilienza organizzativa.

L’efficacia di un programma di security awareness non può essere misurata unicamente attraverso la conoscenza teorica, ma deve essere valutata osservando la trasformazione dei comportamenti concreti degli utenti. Alcuni indicatori rilevanti includono:

- **Tasso di segnalazioni di incidenti:** incremento nella capacità dei dipendenti di riconoscere e comunicare tempestivamente situazioni anomale
- **Tempo di reazione agli stimoli critici:** riduzione dei tempi di risposta in presenza di minacce simulate o reali
- **Diminuzione degli errori ripetuti:** monitoraggio dell’evoluzione dei comportamenti per verificare la capacità di apprendere dai propri errori.

- **Performance in scenari realistici:** valutazione della prontezza operativa in contesti simulati (es. phishing, social engineering, allegati sospetti), in cui si misura la capacità di applicare le nozioni in maniera situazionale.

Questi parametri permettono di spostare il focus dalla conoscenza astratta alla **performance cognitiva e comportamentale**, fornendo una rappresentazione più aderente della resilienza organizzativa. Per superare i limiti delle metodologie tradizionali, la piattaforma **KEATRIX** introduce un sistema di assessment continuo, basato su metriche dinamiche e orientate al comportamento. In particolare, vengono monitorati i seguenti domini:

- **Coinvolgimento:** valutazione del livello di attenzione e partecipazione attiva, distinguendo l'interazione passiva dall'impegno immersivo in simulazioni e scenari interattivi.

- **Livello di competenza:** misurazione oggettiva di conoscenze e abilità attraverso test adattivi, esercizi contestuali e simulazioni pratiche, con monitoraggio dei progressi individuali e collettivi nel tempo

- **Capacità di richiamo:** valutazione della ritenzione a lungo termine delle informazioni, attraverso le tecniche di spacing e interleaving, al fine di verificare se le conoscenze si consolidino in competenze operative stabili

- **Riduzione del rischio comportamentale**: indicatore chiave che misura la frequenza e la gravità degli errori commessi in simulazioni e attività quotidiane, evidenziando l'impatto diretto della formazione sulla postura di sicurezza aziendale.

Risulta evidente che il ritorno sull'investimento in security awareness non può essere calcolato in termini di ore di formazione erogata o percentuali di completamento, bensì nella riduzione misurabile del rischio residuo e nell'aumento della resilienza complessiva. Il nostro approccio consente di collegare le attività formative a indicatori concreti di sicurezza, trasformando l'apprendimento da adempimento burocratico a leva strategica di riduzione del rischio.

La disponibilità di metriche oggettive offre al management la possibilità di agire con maggiore consapevolezza e precisione. Significa, innanzitutto, poter prendere decisioni basate su dati concreti e non su percezioni, indirizzando le risorse in modo mirato proprio verso le aree che presentano le maggiori vulnerabilità. Allo stesso tempo, queste metriche rendono possibile dimostrare in maniera chiara e tangibile il ROSI (Return on Security Investment), ossia il ritorno sull'investimento in sicurezza ottenuto dalle misure adottate.

L'aspetto più importante della formazione alla sicurezza è che aiuta a costruire una vera cultura diffusa della sicurezza: un contesto in cui le buone pratiche smettono di essere semplici linee guida teoriche e diventano comportamenti concreti, applicati ogni giorno all'interno dell'organizzazione.

La validazione scientifica dei programmi non si limita a registrare la partecipazione ai corsi, ma valuta se le persone sono davvero in grado di prevenire, riconoscere e reagire alle minacce informatiche. In questo modo, la security awareness diventa un elemento operativo e strategico fondamentale per rafforzare la resilienza cibernetica dell'azienda.



Potenziali implicazioni per la cyber resilienza aziendale

Immaginiamo il caso di una squadra di piloti automobilistici di Formula 1. All'inizio della stagione, nonostante il talento individuale, la squadra commetteva errori ripetuti in curva o nella gestione dei pit stop, con conseguente perdita di tempo e punti preziosi.

Dopo un programma strutturato di addestramento basato su simulazioni ad alta fedeltà e feedback continuo, i piloti hanno interiorizzato schemi decisionali corretti: la loro percezione dei segnali di pericolo, la gestione della pressione e la coordinazione con il team sono diventate automatiche.

A distanza di poche gare, l'impatto era evidente: riduzione degli errori, tempi di reazione più rapidi, strategie ottimizzate in tempo reale e incremento consistente dei punti in classifica.

L'addestramento non solo ha trasformato la performance individuale, ma ha anche creato una cultura condivisa di eccellenza all'interno del team, in cui ogni pilota funge da livello aggiuntivo di controllo e sicurezza, riducendo significativamente il rischio complessivo di incidenti.

Allo stesso modo, nel contesto della security awareness aziendale, quando i dipendenti interiorizzano comportamenti corretti, diventano attori proattivi della sicurezza informatica. Essi acquisiscono la capacità di identificare autonomamente minacce quali email di phishing, tentativi di spearphishing o attacchi di social engineering, riconoscendo segnali distintivi come mittenti sospetti, richieste urgenti inconsistenti, link con domini irregolari o allegati potenzialmente dannosi.

Grazie a scenari simulati ripetuti, i dipendenti sviluppano schemi decisionali automatici che riducono il rischio di errori, migliorando rapidità e precisione nella risposta agli stimoli di rischio. Parallelamente, i comportamenti preventivi quotidiani, come la verifica delle credenziali, l'autenticazione multifattoriale, l'aggiornamento regolare delle password, backup sicuri e la gestione consapevole delle informazioni sensibili, vengono consolidati, garantendo la loro applicazione anche in contesti imprevisti o sotto stress elevato.

A livello organizzativo, l'effetto è profondo: la superficie di attacco viene drasticamente ridotta, poiché ogni dipendente funge da primo livello di difesa. Le competenze acquisite si diffondono informalmente tra i team, rafforzando la cultura della sicurezza e generando una rete cognitiva collettiva capace di adattarsi dinamicamente a nuove minacce. L'adozione diffusa di comportamenti corretti traduce così la formazione in un incremento tangibile della cyber resilienza aziendale, con riduzione degli incidenti, maggiore continuità operativa e protezione concreta dagli attacchi informatici causati da errori umani.



Come finanziare la formazione in cybersecurity: quadro generale

Il rafforzamento delle competenze in materia di cybersecurity rappresenta un elemento essenziale per sostenere la resilienza digitale delle organizzazioni. In tale contesto, a livello nazionale e regionale, sono previsti diversi strumenti di sostegno che possono includere, tra le attività potenzialmente finanziabili, anche iniziative di formazione.

Tali strumenti sono generalmente finalizzati a supportare lo sviluppo e l'aggiornamento delle competenze all'interno delle imprese e presentano caratteristiche eterogenee in funzione delle singole misure attive. In particolare, requisiti di accesso, modalità di partecipazione e tipologie di interventi ammissibili sono stabiliti dalle rispettive discipline di riferimento e possono variare nel tempo.

Tra le principali opzioni, le imprese possono ricorrere ai Fondi Interprofessionali per la formazione continua o ad altri programmi pubblici dedicati allo sviluppo delle competenze, inclusi quelli in ambito digitale. L'accesso a tali strumenti è in ogni caso subordinato al rispetto delle condizioni previste dai singoli bandi o regolamenti applicabili.

Considerata la specificità delle singole misure, la verifica dell'ammissibilità delle attività formative deve essere effettuata caso per caso, alla luce della normativa e delle disposizioni attuative di riferimento. A tal fine, può risultare opportuno avvalersi del supporto di soggetti qualificati nella progettazione e gestione della formazione finanziata.

La definizione di un piano formativo richiede, ove previsto, il coinvolgimento di enti di formazione accreditati, incaricati di analizzare i fabbisogni dell'impresa e di verificare la coerenza delle attività proposte rispetto ai requisiti stabiliti dalla misura di finanziamento applicabile.



Ricerca futura dell'apprendimento

La direzione del futuro è già tracciata: l'integrazione sempre più profonda tra neuroscienze cognitive e tecnologie educative trasformeranno i paradigmi dell'apprendimento, con evidenze che supportano l'uso di misurazioni neurali e biomarcatori per ottimizzare esperienze formative su misura (Orovas et al., 2024).

La formazione non può più limitarsi a fornire contenuti standardizzati; deve trasformarsi in sistemi intelligenti che si adattano al modo in cui ciascuno apprende. Grazie a tecnologie neuro adattative e strumenti di learning analytics in "closed-loop", il ritmo, la complessità e la distribuzione dei contenuti verranno regolati in tempo reale in base allo stato cognitivo dell'utente (Jin et al., 2024).

L'orizzonte tecnologico prevede l'uso combinato di sensori biometrici non invasivi (es. EEG portatili, indicatori fisiologici del carico attentivo e dello stress), algoritmi predittivi basati su modelli neuromodulatori e interfacce intelligenti che chiudono il ciclo adattivo: la piattaforma osserva, modella e adatta continuamente il training sulla base di segnali neurali e comportamentali, massimizzando l'efficacia formativa e riducendo l'errore umano (Beauchemin et al., 2024).

Questa integrazione tra neuroscienze e tecnologie educative non è un'idea futuristica, ma un'evoluzione già supportata da studi e sperimentazioni concrete. I sistemi neuro adattativi e le piattaforme di apprendimento basate su dati in tempo reale permettono di trasformare la formazione aziendale in un processo dinamico e autoregolato, capace di anticipare i bisogni cognitivi delle persone, stimolare la capacità di adattamento e consolidare comportamenti sicuri in modo misurabile e facilmente scalabile.

In questa direzione, in collaborazione con istituzioni accademiche di rilevanza internazionale, come l'University College of London, Cyberoo sta sviluppando modelli di apprendimento personalizzati basati sulle neuroscienze. Questi modelli sono in grado di analizzare in modo dettagliato come ciascun individuo acquisisce, consolida e applica la conoscenza, permettendo di ottimizzare percorsi formativi altamente efficaci e adattati alle caratteristiche cognitive di ogni utente.

Con questa visione, la formazione diventa un ecosistema dinamico, che non si esaurisce in un corso o in un percorso di breve durata, ma accompagna il dipendente lungo tutto il ciclo di vita professionale. La sicurezza, infatti, è un campo in costante evoluzione: nuove minacce emergono ogni giorno, e solo un modello formativo capace di adattarsi e crescere nel tempo può garantire un reale vantaggio difensivo.

La cybersecurity va affrontata con un approccio realmente olistico: non bastano tecnologie e procedure, se non cambia profondamente la cultura e i comportamenti delle persone. Trasmettere semplicemente nozioni non è sufficiente; occorre una formazione che stimoli memoria, riflessi cognitivi e prontezza decisionale, trasformando la sicurezza in una competenza concreta e quotidiana.

In questa prospettiva, KEATRIX ridefinisce la formazione, trasformandola da obbligo amministrativo in investimento strategico, capace di rafforzare la continuità operativa, proteggere la reputazione e consolidare la fiducia degli stakeholder. Solo così è possibile ridurre efficacemente il rischio derivante dagli errori umani e costruire un mondo in cui la cybersecurity supporti il benessere delle persone, permettendo a tutti di vivere con fiducia e tranquillità.

BIBLIOGRAFIA DI RIFERIMENTO

ENISA (2025), “Trust Services Security Incidents 2024”

Cybersecurity Dive (2024, aprile), “Compromised credentials and lack of MFA in a major healthcare company”

Cyberoo (2025), “Osservatorio Cyberoo: nuove sfide e rilevazioni”

Lithuanian State Data Protection Inspectorate (2025), “Report on human error in data breaches. The Hacker Wire”

Global Risk Institute (2024) “Quantum Threat Timeline Report 2024”

Gartner (2024), “Top Cybersecurity Trends of 2024”

O'Donnell R. (2025), “Guida alla consapevolezza e formazione sulla sicurezza”, MetaCompliance

Verizon (2024), “Data Breach Investigations Report (DBIR)”, Compliance Week / Verizon

BIBLIOGRAFIA DI RIFERIMENTO

Smolen, P., Zhang, Y., & Byrne, J. H. (2016), “The right time to learn: mechanisms and optimization of spaced learning”

Chen X., Sacré, M., Lenzini, G., Greiff, S., Distler, V., & Sergeeva, A. (2024), “The effects of group discussion and role-playing training on self-efficacy, support-seeking, and reporting phishing emails”

Lain D., Kostiainen, K., & Capkun, S. (2021), “Phishing in Organizations: Findings from a Large-Scale and Long-Term Study”

Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., & Longhurst, C. A. (2025), “Understanding the efficacy of phishing training in practice”, University of Chicago

European Commission (2024), “EU must reinforce cybersecurity skills”

Yuan X. (2022), “Evidence of the Spacing Effect and Influences on Perceptions of Learning and Science Curricula”, Cureus

Schorn JM, Knowlton BJ (2021), “Interleaved practice benefits implicit sequence learning and transfer”, Mem Cognit

BIBLIOGRAFIA DI RIFERIMENTO

Hobson N. (2024, aprile 27), “Neuroscience says you can improve your memory with emotion”, Inc.com

Orovas C, Sapounidis T, Volioti C, Keramopoulos E. (2024), “EEG in Education: A Scoping Review of Hardware, Software, and Methodological Aspects. Sensors (Basel)”, PubMed Central

Jin W, Zhu X, Qian L, Wu C, Yang F, Zhan D, Kang Z, Luo K, Meng D, Xu G. (2024), “Electroencephalogram-based adaptive closed-loop brain-computer interface in neurorehabilitation: a review”, PubMed Central

Beauchemin N., Charland, P., Karran, A., Boasen, J., Tadson, B., Sénécal, S., & Léger, P-M. (2024), “Enhancing learning experiences: EEG-based passive BCI system adapts learning speed to cognitive load in real-time, with motivation as catalyst”. Frontiers in Human Neuroscience, 18, Article 1416683.

CONTACT US

Cyberoo S.p.A.
Via Brigata Reggio, 37, 42124 (RE)

tel. 0522 388111

www.cyberoo.com

CONTATTACI

CYBEROO