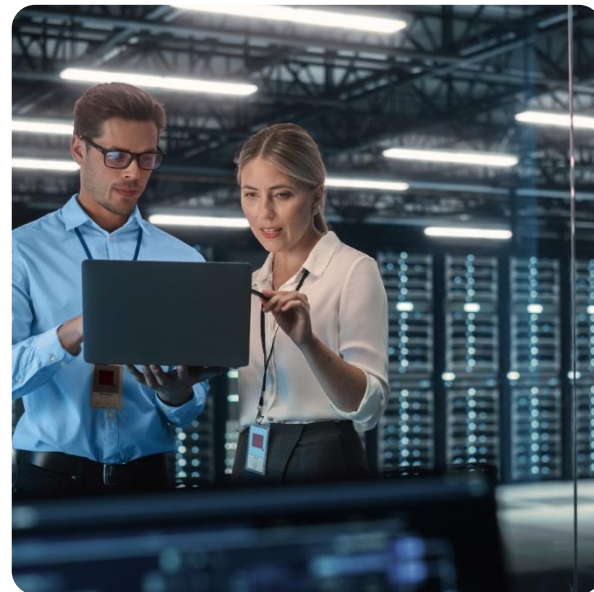


E-volve: la
formazione
cyber nell'era
del
cambiamento
permanente

RICOH
imagine. change.





Agenda

1

Introduzione e
scenario, a cura di
Ricoh

2

Perché la
formazione cyber
oggi deve evolvere

3

E-volve: la
metodologia e i
suoi principi

4

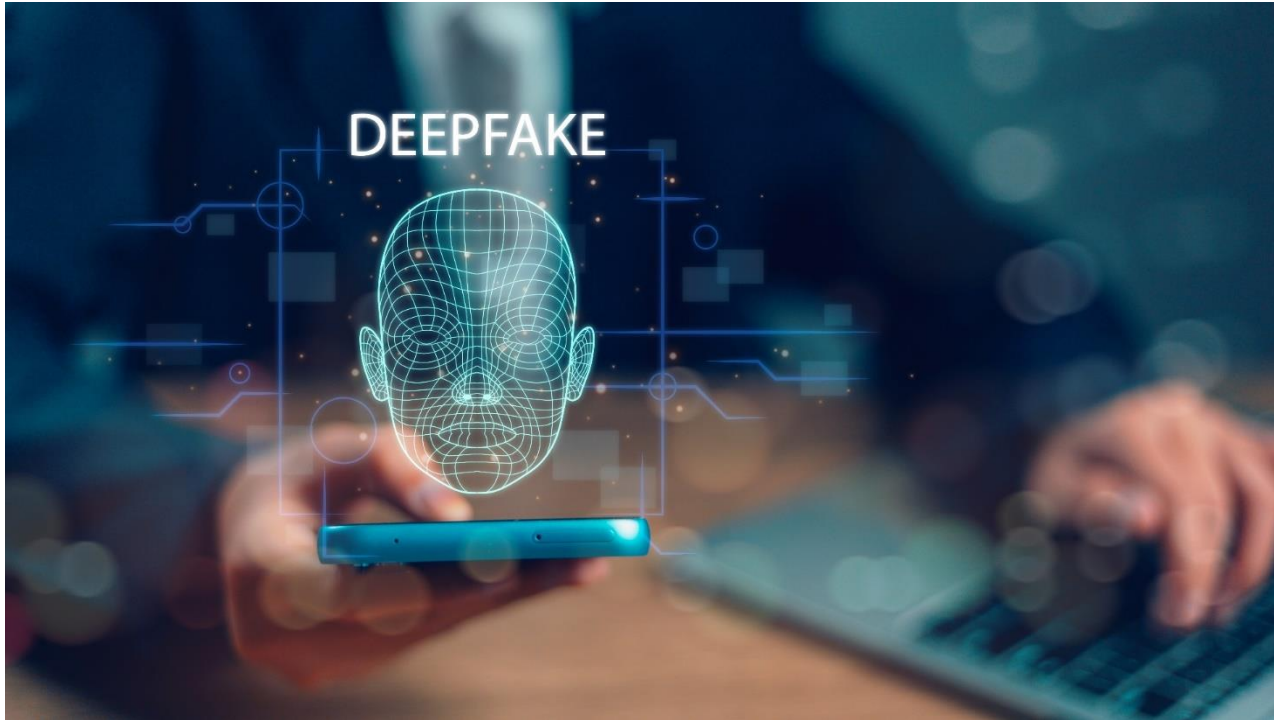
Demo Live:
progettare e
produrre contenuti
formativi con
E-volve

5

Conclusione e
Q&A

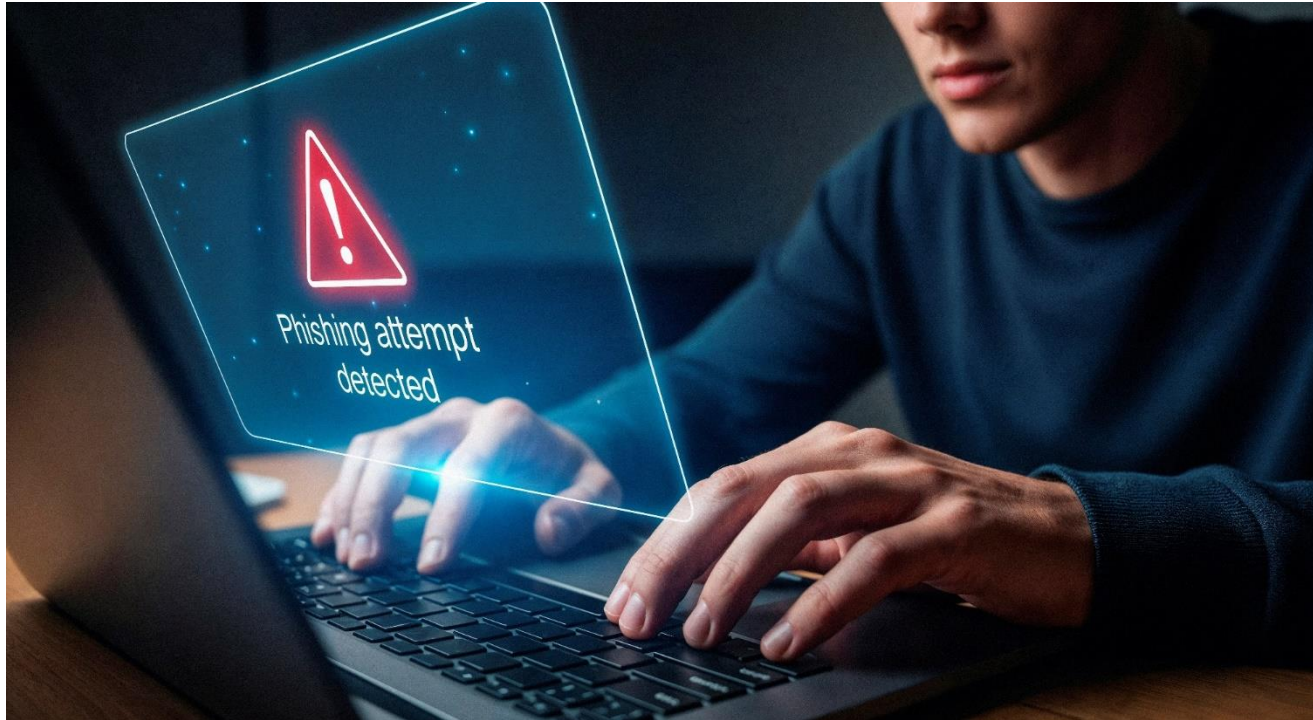


Deepfake





AI Agentic Phishing









Come aumentare la consapevolezza degli utenti aziendali rispetto a minacce così sofisticate e in continua evoluzione?



FORMAZIONE
CONTINUA



CONTENUTI
DINAMICI



APPROCCIO
INTERATTIVO



Luca Rossi

Presales

LibraCyber



formerly  **Cyber Guru**

Evolve

La formazione nell'era del cambiamento permanente



STRANGER THINGS

THE SPHERE

Evolve Learning Paths

COSA

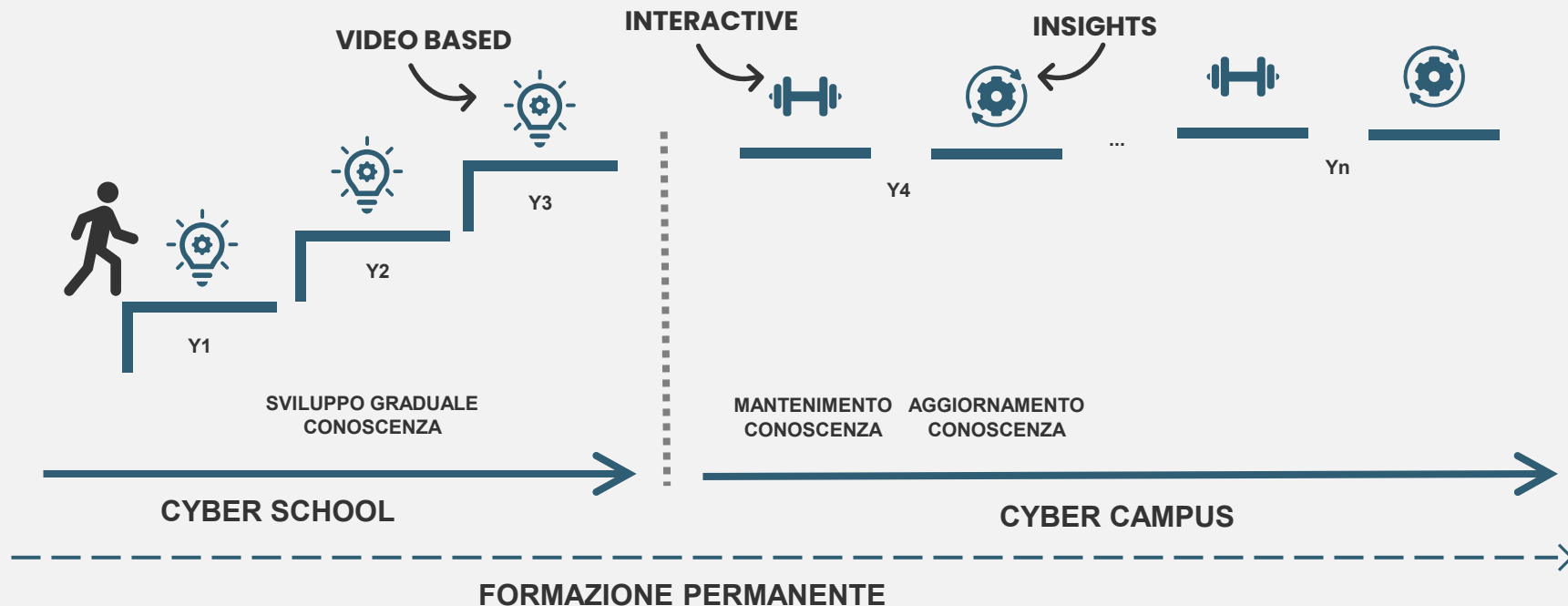
- Nuovi percorsi che bilanciano didattica ed esercitazioni.
- Viene rimossa la barriera tra School e Campus rivedendo l'ordine di fruizione
- Disponibilità di percorsi tematici che si affiancano ai percorsi pianificati

PERCHÈ

- Rendere la nostra formazione ancora più efficace e ingaggiante
 - Sfruttare l'innovazione di contenuto e di formato
 - Essere rapidi nel cogliere l'esigenza di approfondire argomenti di attualità
- Aumentare la flessibilità della fruizione mantenendo il rispetto dell'approccio metodologico

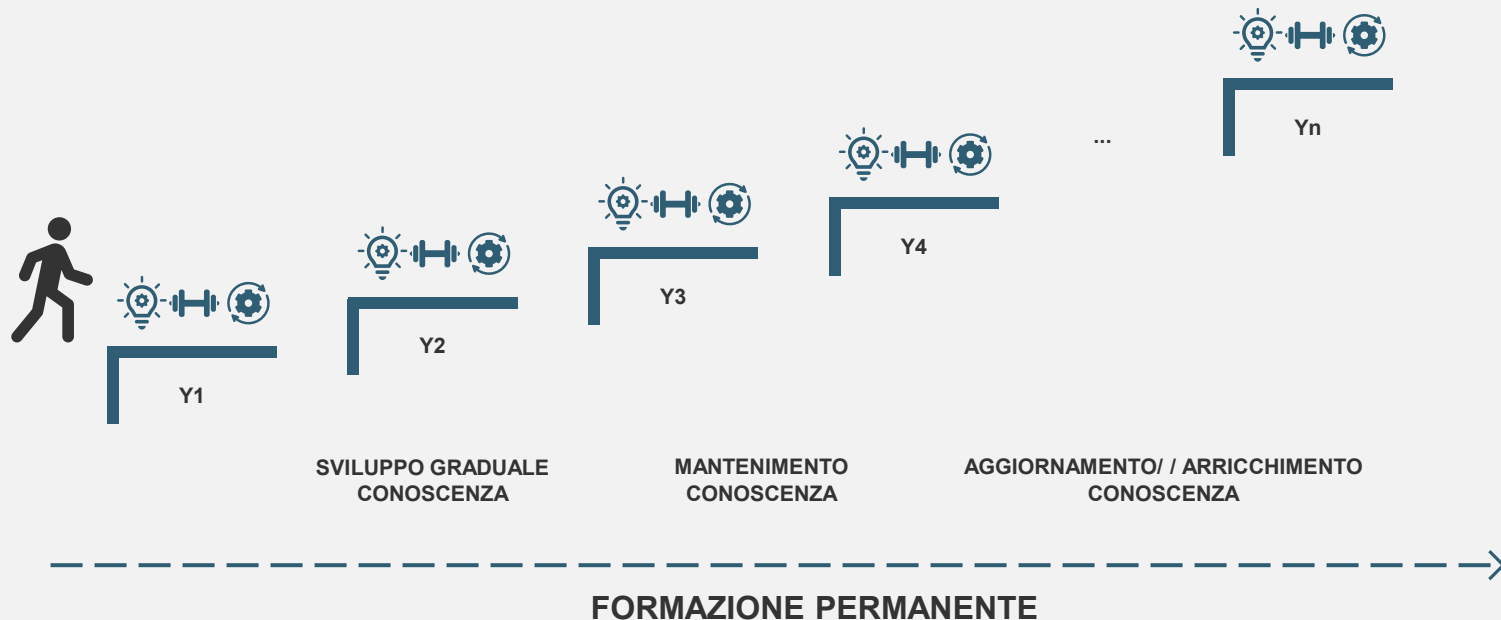
Progress Maintenance & Update

Un percorso graduale di apprendimento per sviluppare il giusto grado di conoscenza, per poi lavorare al mantenimento e all'aggiornamento delle competenze acquisite

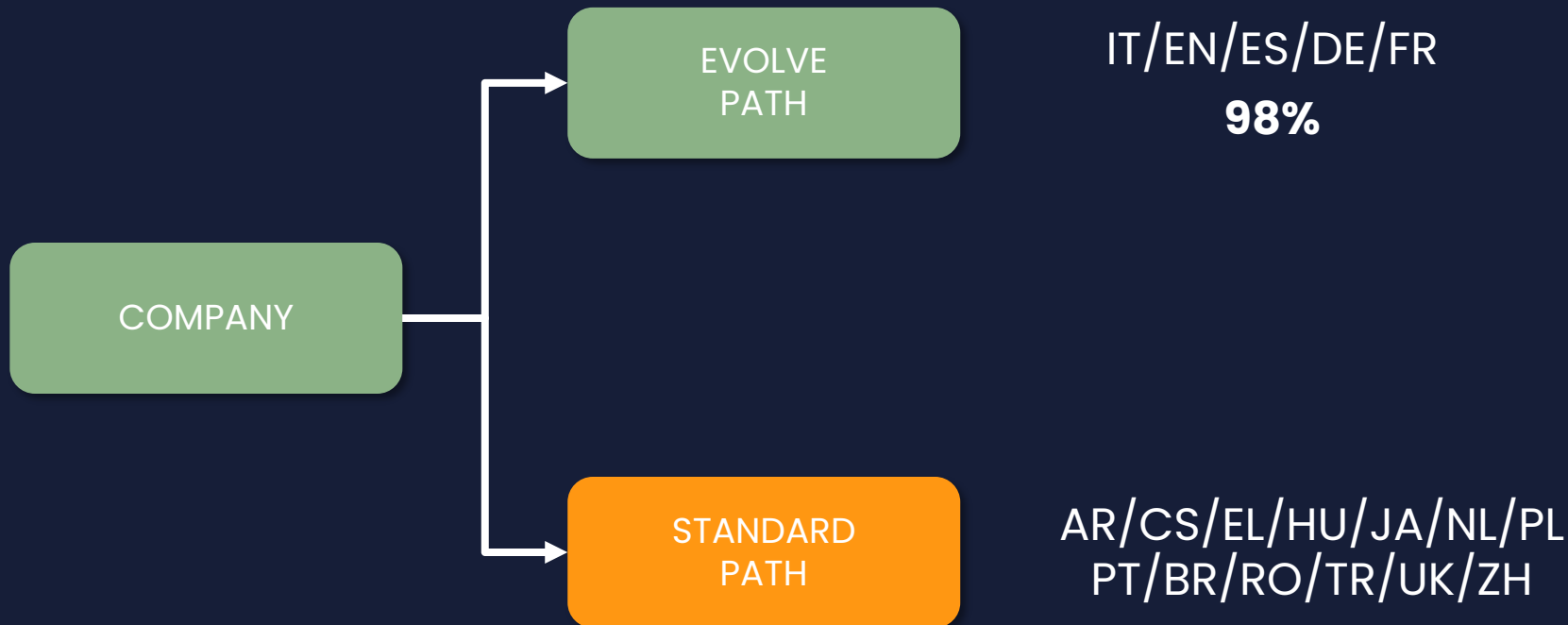


Progress Maintenance & Update

Un percorso graduale di apprendimento per sviluppare il giusto grado di conoscenza, per poi lavorare al mantenimento e all'aggiornamento delle competenze acquisite

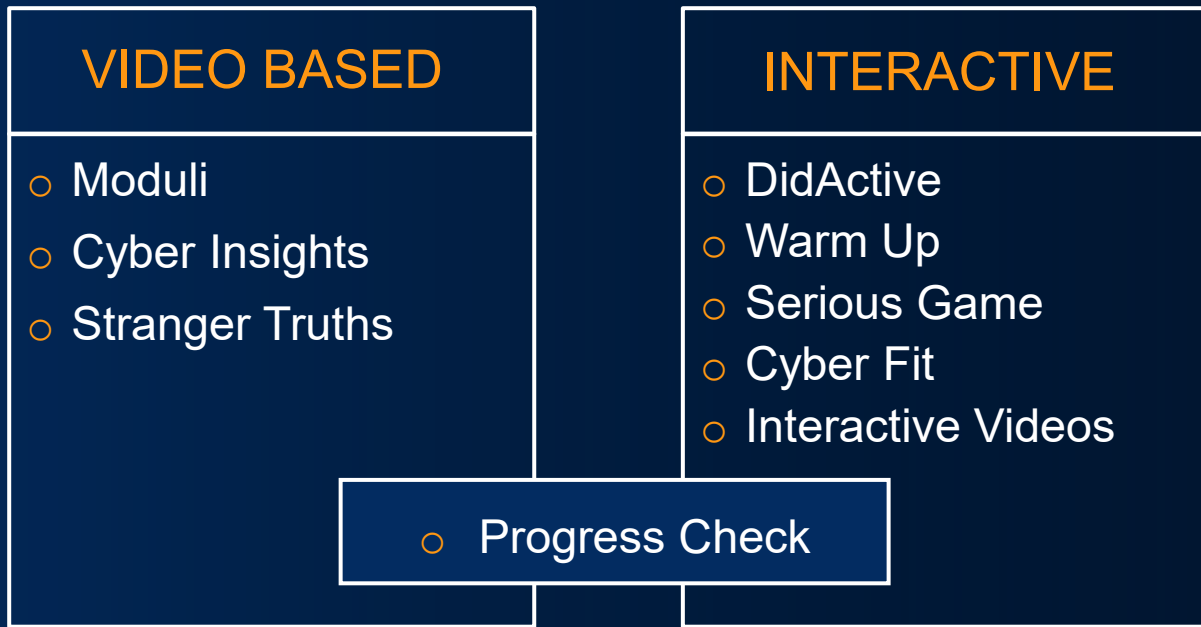


Staged Rollout



EVOLVE 2.5

TIPOLOGIE DI LEARNING OBJECT



OGGETTI FORMATIVI VIDEO BASED

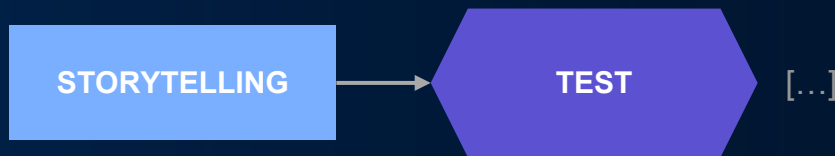
MODULI

- ▶ **39 MODULI** (in continuo aggiornamento)
- ▶ **CARATTERISTICHE**
 - 3 video lezioni (“micro-learning”, max 5 min)
 - 1 quiz a fine lezione (4 domande a scelta singola con 3 alternative)
 - PDF (con trascrizione delle lezioni)
 - Propedeuticità (è necessario fruire di una lezione per passare alla successiva)
- ▶ **OBIETTIVI FORMATIVI:**
 - rafforzare comprensione e memorizzazione dei concetti chiave
 - rendere l’esperienza formativa accessibile e coinvolgente
 - favorire un apprendimento strutturato e graduale
 - offrire contenuti sempre aggiornati e pertinenti rispetto all’evoluzione dei temi

▶ METODOLOGIA DI APPRENDIMENTO

- Obiettivi formativi:
 - approfondire una determinata minaccia cyber
 - aggiornare le conoscenze su attacchi cyber che hanno subito rapide evoluzioni
 - sensibilizzare su determinati rischi cyber attraverso esempi concreti
- Struttura didattica: video «storytelling» – test (4 domande a risposta singola)

Durata: 10 min



ESEMPIO

Intenti

 APPROFONDIRE



La truffa del codice WhatsApp

Obiettivi formativi

Anna riceve un messaggio dal suo amico Marco su WhatsApp, in cui le chiede di mandargli un codice di 6 cifre che le ha inviato per abbaglio. Anna, fidandosi, fa subito quanto richiesto. Poco dopo, scopre di non poter più accedere al proprio account WhatsApp. Anna è stata vittima di una strategia di Social Engineering, nota come "Truffa del codice su WhatsApp" che l'ha portata a diventare inconsapevolmente complice dei criminali cyber. La truffa ha sfruttato la fiducia tra amici ed è stata attuata tramite la compromissione del doppio fattore di autenticazione per prendere il controllo degli account.

 Versione PDF

 Vai al test

SE SIETE TRA LE VITTIME DELLA TRUFFA

- 1 Denunciate l'accaduto alla Polizia Postale
- 2 Comunicate con l'assistenza WhatsApp
- 3 Avvisate i propri contatti tramite altro mezzo di comunicazione



DOMANDA 1 DI 4

Cosa fare se si è stati vittima della truffa del codice WhatsApp?

- ☒ Denunciare l'accaduto alla Polizia Postale
- ☐ Interrompere la connessione Internet
- ☐ Cercare con ogni mezzo di entrare in contatto con i truffatori

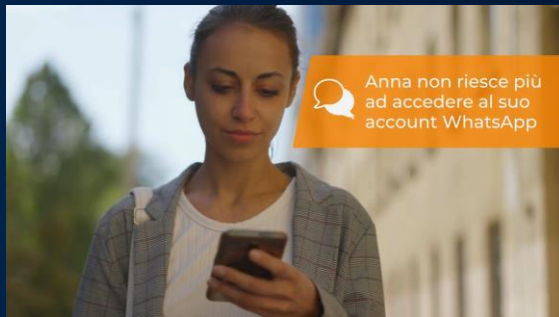
Conferma

STRATEGIA DI SOCIAL ENGINEERING

Rapporto di fiducia
Senso di urgenza
Forte pressione



Anna non riesce più ad accedere al suo account WhatsApp



COME FUNZIONA

- 1 Compromissione di un account WhatsApp
- 2 Tentativo di controllo degli altri contatti
- 3 Procedura di sicurezza WhatsApp: invio di codice a 6 cifre



STRANGER TRUTHS

4 episodi generati con l'AI, ambientati in futuri distopici in cui l'intelligenza artificiale assume un ruolo totalizzante e minaccioso

► METODOLOGIA DI APPRENDIMENTO

- Obiettivi formativi:
 - stimolare una riflessione critica sul ruolo dell'essere umano nell'ambito della cybersecurity
 - promuovere un'alfabetizzazione emotiva e cognitiva sulle tematiche complesse legate all'AI
 - accrescere la consapevolezza rispetto alle forme evolute di truffa, manipolazione e inganno digitale
 - rafforzare il senso di responsabilità e la capacità di pensiero critico nell'utilizzo delle tecnologie digitali
- Struttura didattica:
 - video ST di 4' + video After ST 2' + test (4 domande)

Durata: 10 min



ESEMPIO

Internet

 RIFLETTERE



OGGETTI FORMATIVI INTERACTIVE

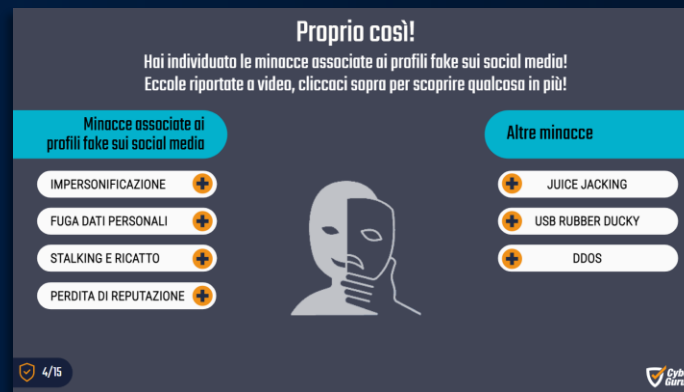
► METODOLOGIA DI APPRENDIMENTO

- Obiettivi formativi:
 - allenare la memoria sulle conoscenze già acquisite durante la School, mantenendo la conoscenza attiva
 - riorientare la conoscenza
 - colmare le eventuali lacune maturate
- Struttura didattica basata su 3 componenti: video – interazione – feedback

- Tipologie interazione (5):
 - scelta singola/multipla
 - abbinamenti/associazioni (drag and drop)
 - fill the form



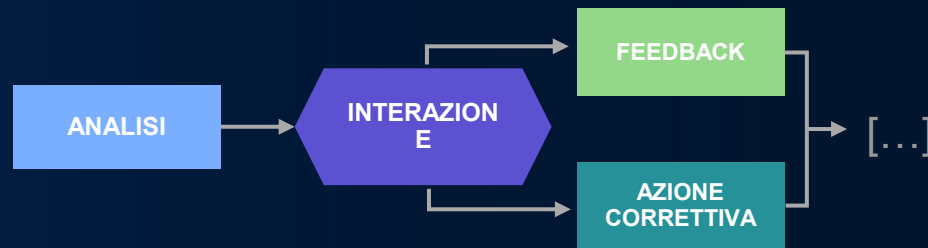
Durata: 15-20 min



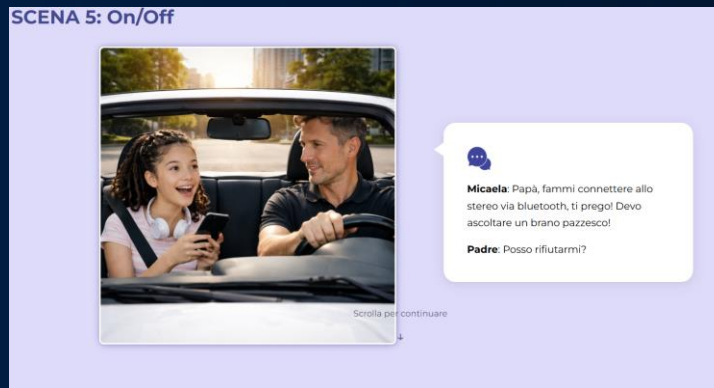
► METODOLOGIA DI APPRENDIMENTO

- Obiettivi formativi:
 - ripassare le conoscenze acquisite
 - allenare le competenze in tema di CSA
 - riconoscere le minacce cyber in situazioni specifiche
- Struttura didattica: analisi – interazione – feedback/azione correttiva

- Tipologie interazione (5):
 - scelta multipla
 - caccia all'errore (individuare nelle scene le pratiche scorrette)



Durata: 10-12 min



Cosa potrebbe essere accaduto alla nostra protagonista? E con quali rischi?

Seleziona le 2 opzioni che ritieni corrette e conferma.

- ☐ Sistema operativo non aggiornato
- ☐ Cryptojacking
- ☒ Attacco via bluetooth
- ☐ Sfruttamento delle risorse del dispositivo per estrarre criptovalute
- ☒ Connessione fraudolenta al dispositivo con intercettazione di comunicazioni, furto dati, ecc.

Conferma



RISPOSTA CORRETTA
Hai ottenuto 2 scudi

Cosa è accaduto?

Aver lasciato il **bluetooth attivo** ha consentito al cybercriminale di individuare i dispositivi con strumenti di scansione fatti apposta, e procedere alla successiva connessione.

A quel punto, l'attaccante ha potuto facilmente **inviare richieste di connessione bluetooth mascherate** per sembrare connessioni innocue, ad esempio un auricolare Bluetooth o un altro dispositivo comune.

Da quel momento diventa possibile attivare **attacchi per rubare dati sensibili**, come dati di accesso, messaggi, o qualsiasi informazione scambiata tra i dispositivi, nonché **distribuire malware** ai dispositivi connessi.



Avanti

SERIOUS GAME



Giochi digitali progettati per scopi educativi, informativi e formativi

► METODOLOGIA DI APPRENDIMENTO

- Obiettivi formativi:
 - insegnare e valutare competenze specifiche nell'ambito della CSA
 - sviluppare spirito critico nei confronti di diverse situazioni rischiose
 - generare un'esperienza di apprendimento attiva e coinvolgente
 - favorire il recupero di elementi di conoscenza già presenti
- Alcune meccaniche di gioco presenti:
 - storytelling ingaggiante
 - risoluzione di enigmi di vario tipo contestualizzati rispetto all'oggetto formativo
 - uso della variabile «tempo massimo» per il completamento della prova
 - uso dei meccanismi di aiuto che possono concorrere al superamento della prova
 - uso dei feedback ai fini degli obiettivi di apprendimento
 - utilizzo di scudi/badge/premi per stimolare e coinvolgere

SERIOUS GAME



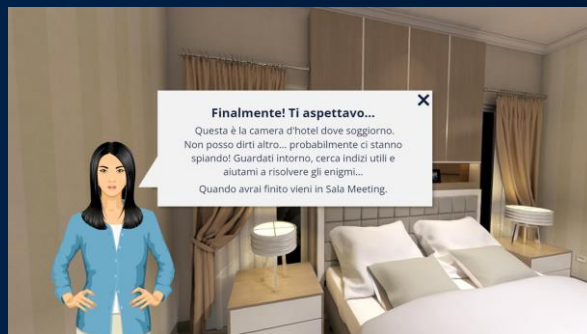
▶ LE PRINCIPALI TIPOLOGIE

- Escape Room
- Fantasy Game (Role Play)
- Quiz show format

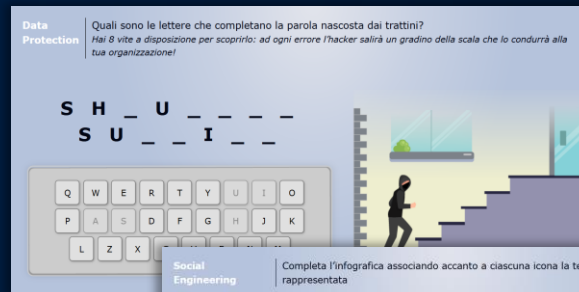


ALCUNI ESEMPI

Escape Room – Una trasferta difficile



ALCUNI ESEMPI



CYBER FIT

Circuito di allenamento formato da 4 "postazioni":

► METODOLOGIA DI APPRENDIMENTO

Attraverso un circuito digitale di quattro postazioni, ciascuna mirata a sviluppare competenze di cybersecurity e comportamenti digitali sicuri, l'utente potrà:

- sviluppare abilità pratiche attraverso esercizi interattivi e dinamiche di gioco,
- promuovere comportamenti digitali sicuri e consapevoli nell'uso quotidiano delle tecnologie,
- rafforzare la prontezza decisionale e la reattività di fronte a possibili minacce informatiche,
- favorire un apprendimento progressivo, esperienziale e modulare, adattabile all'evoluzione delle minacce e degli obiettivi formativi.

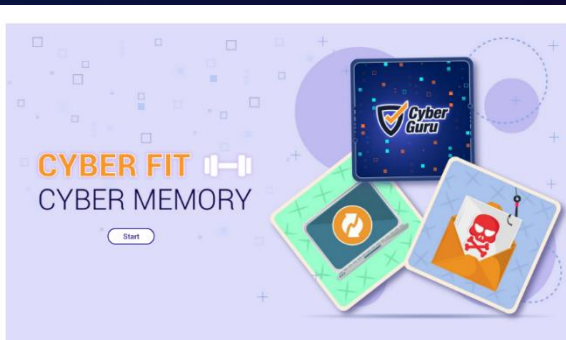
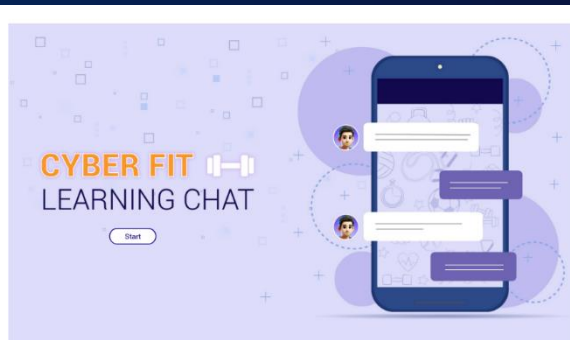
CYBER FIT

Integrità

 ESERCITARSI

Learning Chat

sessione di chat con Alex, un tutor che faciliterà l'apprendimento di temi sulla cyber security awareness

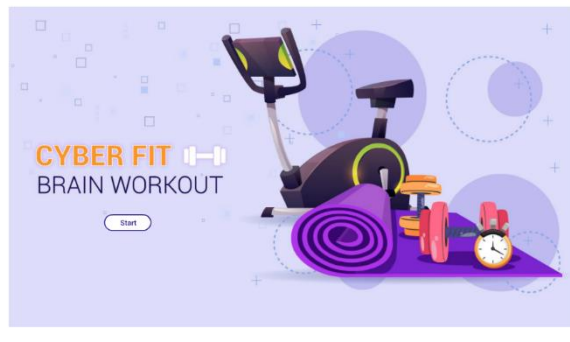


Cyber Memory

un serious game coinvolgente ispirato al classico gioco memory con le carte, con l'aggiunta di quiz e tips

Brain Workout

un percorso allenante fatto di drag&drop, domande, scenari e altri quiz di vario genere

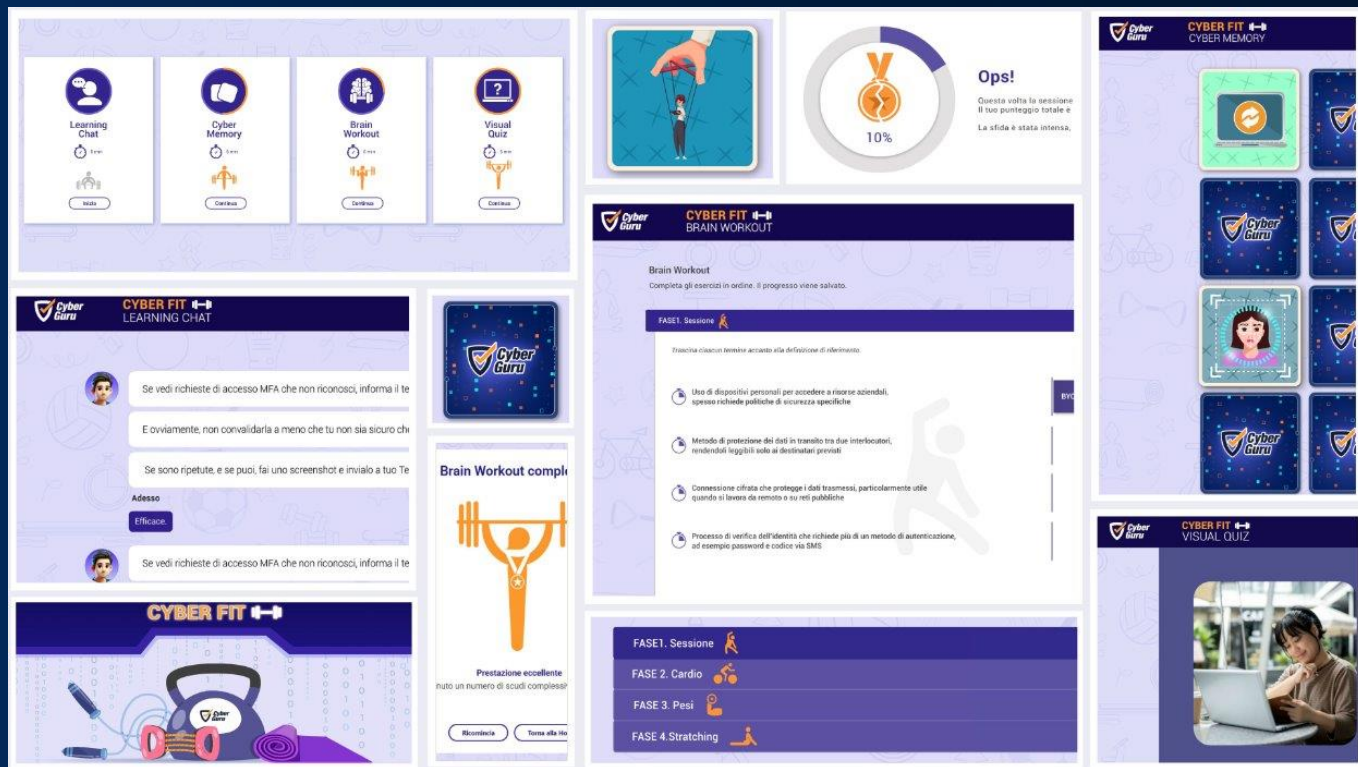


Visual Quiz

contenuto visual come un breve video, una scenetta o un'infografica, seguito da 4 domande a scelta singola

ESEMPIO

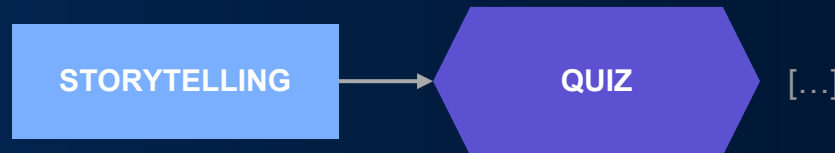
Interno



CYBER GAME

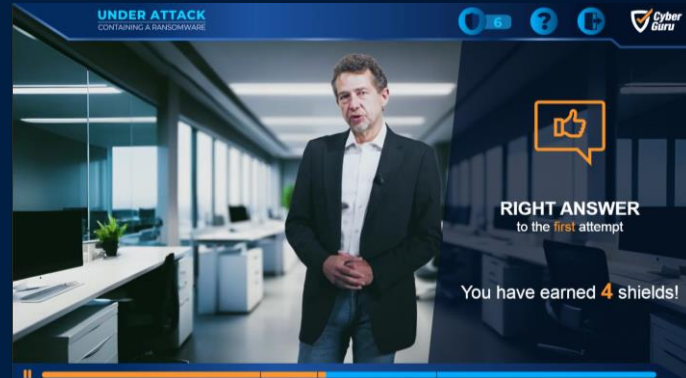
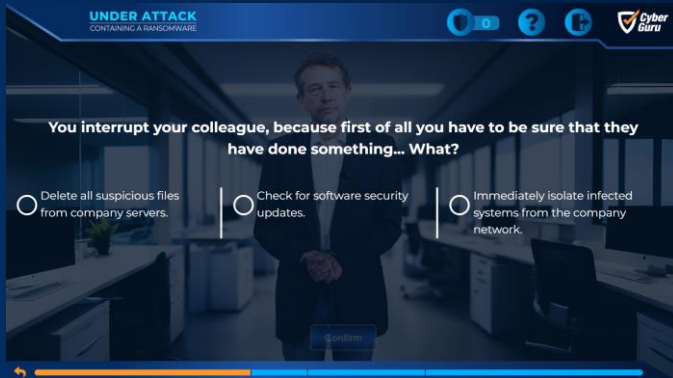
▶ METODOLOGIA DI APPRENDIMENTO

- Obiettivi formativi:
 - impersonare il responsabile della cyber security di un'azienda
 - alzare il livello di attenzione rispetto alle minacce Cyber
 - mostrare la catena di eventi che si sussegue a seguito di un attacco informatico
 - sensibilizzare sull'importanza della formazione del personale in tema CSA
- Struttura didattica: video «storytelling situazionale» – quiz (il video si interrompe e si chiede all'utente di prendere una decisione)



ESEMPIO

Internal



SOCIAL ENGINEERING STORIES

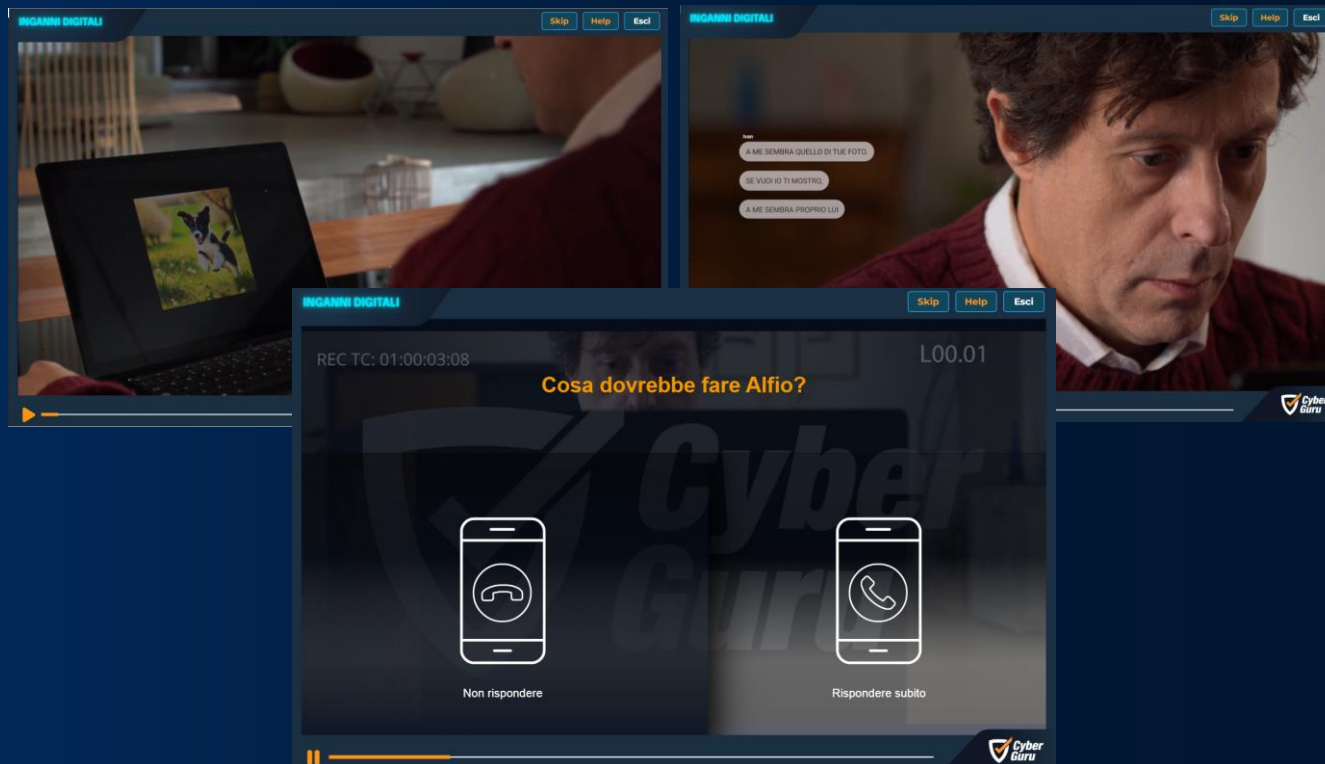
► METODOLOGIA DI APPRENDIMENTO

- Obiettivi formativi:
 - riconoscere e attuare le migliori scelte all'interno di una narrazione dinamica, caratterizzata da una forte componente emotiva
- Struttura didattica:
 - video «storytelling emozionale» con struttura ad albero decisionale
 - l'utente di fronte a specifici momenti decisionali opera delle scelte con cui influenza il successivo sviluppo della storia



ESEMPIO

Internal



INGANNI DIGITALI

Skip Help Esc

INGANNI DIGITALI

Skip Help Esc

REC TC: 01:00:03:08

L00.01

Cosa dovrebbe fare Alfio?

Non rispondere

Rispondere subito

Cyber Guru

PROGRESS CHECK

Oggetti di valutazione formativa pensati per verificare le competenze acquisite al termine di una sezione del percorso, attraverso un test a tentativo unico

► METODOLOGIA DI APPRENDIMENTO

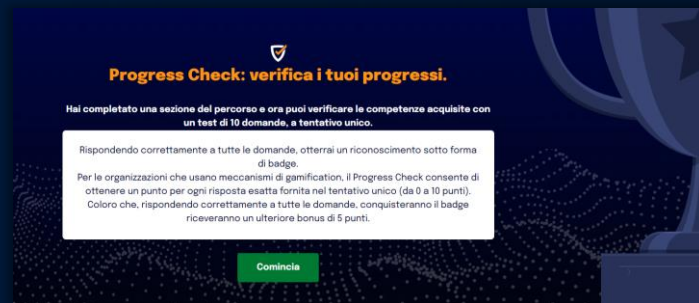
○ Obiettivi formativi:

- verificare livello di apprendimento e consolidamento delle competenze acquisite
- stimolare autovalutazione e consapevolezza dei propri progressi
- rafforzare la motivazione attraverso meccaniche di riconoscimento e gamification

○ Struttura didattica:

10 domande a risposta singola, in un unico tentativo:

- 1 punto per ogni risposta corretta (da 0 a 10 pt)
- in caso di risposte corrette a tutte le domande, assegnazione di un badge + bonus di 5 punti





formerly  **Cyber Guru**

Grazie