

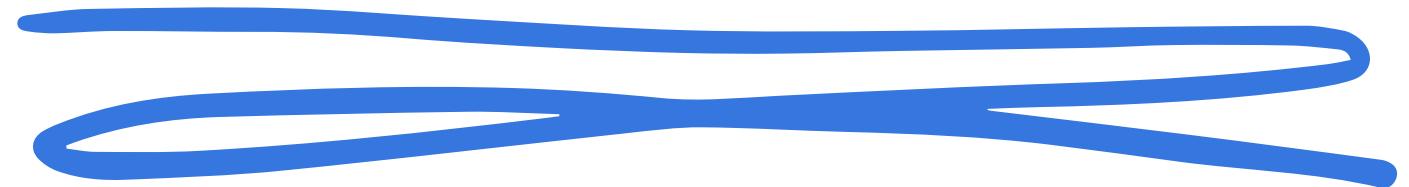


SERIOUS GAME:
Ambito Formativo



**UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO**

CyberShield



A cura di:



Leonardo Colucci
Gianfranco De Vincenzo

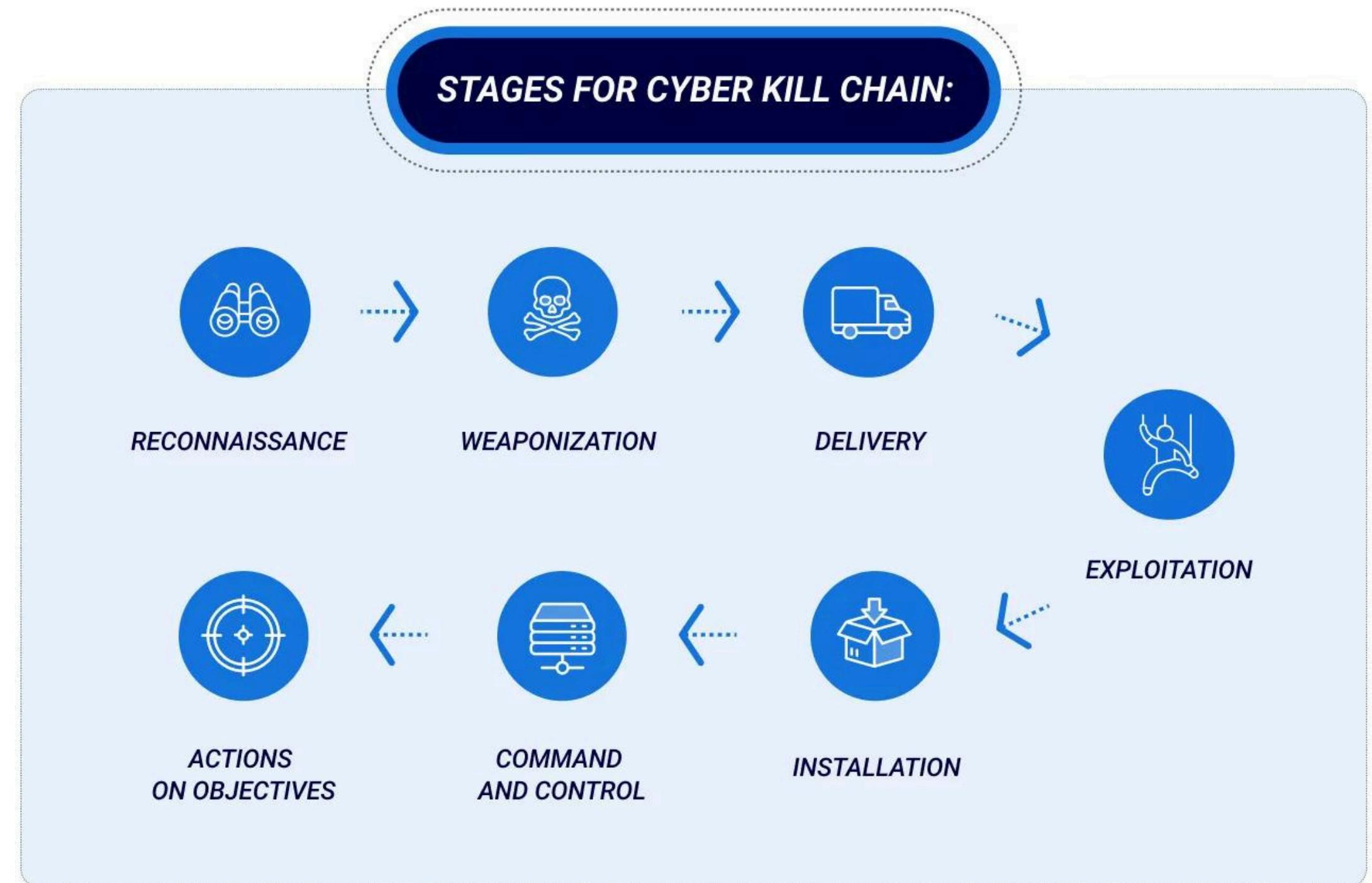
SICUREZZA INFORMATICA - A.A. 2023/24

Cyber Kill chain

il Serious Game segue la logica della **Cyber kill Chain** per cui ogni fase deve essere rappresentata da sfide interattive che consentano ai giocatori di comprendere e sperimentare le tecniche utilizzate dagli attaccanti e le contromisure difensive appropriate. Ad esempio, :

- la fase di ricognizione, include quiz e attività di raccolta di informazioni su bersagli simulati;
- la fase di delivery, coinvolge la gestione di phishing o malware prima e durante l'attacco stesso.

L'idea è quella di poter comprendere tecniche e strategie d'attacco ma soprattutto di difesa, in modo da sensibilizzare gli utenti e non, fornendo concetti e nozioni in base al caso specifico

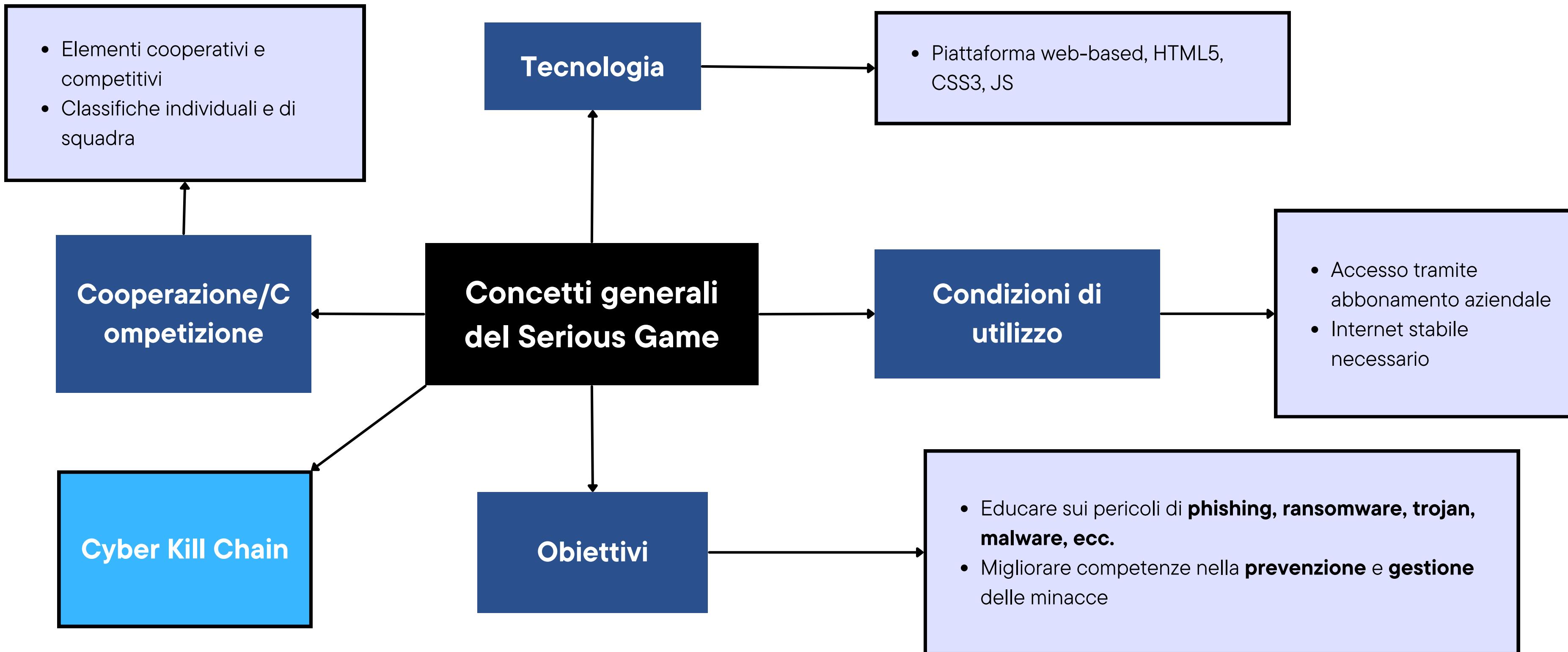


Indice

<u>SERIOUS GAME CONCEPT</u>	Concetti principali del gioco che permettono di avere un contesto di esso
<u>ASPETTI TECNOLOGICI</u>	Aspetti inerenti alle tecnologie presenti nel gioco
<u>CORE MECHANICS</u>	Regole e meccaniche di gioco
<u>ELEMENTI FUNZIONALI</u>	Elementi utili per il coinvolgimento dell'utente (storytelling, personaggi e scenario)
<u>USER INTERFACE</u>	Elementi di presentazione che permettono l'interazione utente-gioco



CyberShield Concept



Aspetti Tecnologici

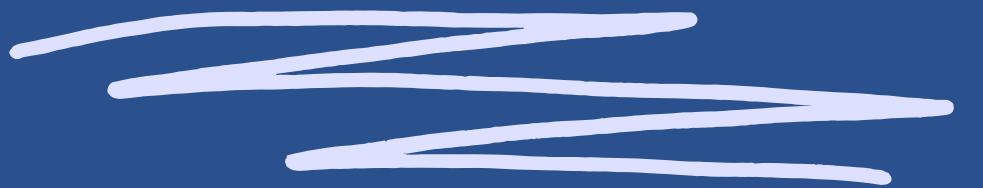
Tecnologie

- **Computer/Desktop/Laptop:** strumento principale per i dipendenti in ambiente di lavoro
- **Smartphone/Tablet:** per l'accesso mobile e flessibile, utile per microlearning e apprendimento in movimento

Input & Output

- **Tastiera e mouse:** per la navigazione alle domande
- **Touchscreen:** per selezionare risposte e interagire con il quiz tramite touch
- **Monitor:** display principale per visualizzare quiz e feedback
- **Schermo di smartphone/tablet:** display per l'accesso mobile al quiz e visualizzazione dei contenuti

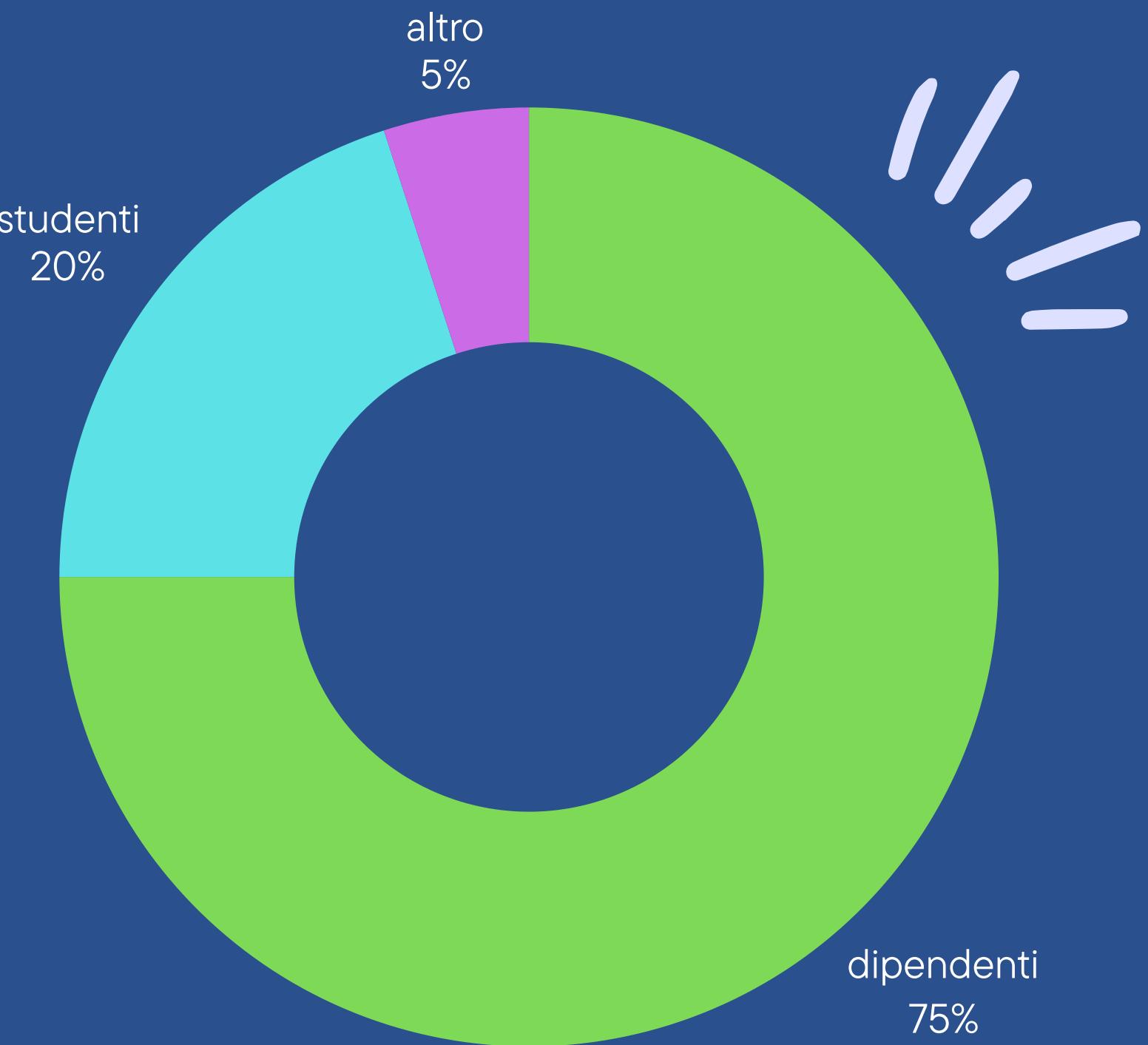
Utenti



Il gioco tiene conto di diverse caratteristiche in modo da abbracciare diverse aree di competenza e prospettive. Per questo è dedicato in percentuale diversa:

- 75%: dipendenti/personale (18 anni minimo)
- 20%: studenti (16 anni minimo)
- 5%: altro(diversa età)

(Ognuna di queste diverse aree comprende capacità e finalità diverse)



Meccaniche Fondamentali

Regole di gioco

- Completare quiz e sfide per avanzare nei livelli
- Ogni livello simula un attacco informatico diverso
- Guadagnare punti per risposte corrette e completamento delle sfide
- Penalità per risposte errate o comportamenti rischiosi

Meccaniche di gioco

- Quiz a scelta multipla con scenari realistici
- Sfide interattive: identificare minacce in email, siti web, software
- Mini-giochi: risposta a incidenti di sicurezza
- Sistema di punteggio e classifiche
- Feedback immediato e spiegazioni dettagliate

Elementi Funzionali

non sono elementi essenziali, ma la loro presenza garantisce un maggiore coinvolgimento, immersione e armonia, qualità che garantiscono il successo di un serious game a 360 gradi:



StoryTelling

Storia

- Giocatori parte di un team di sicurezza informatica che si affacciano a nuove sfide
- Ogni livello rappresenta una nuova minaccia e tramite dei quiz l'utente aumenta la propria consapevolezza a riguardo

Narrativa

- Briefing di missione all'inizio di ogni livello agevolando un elemento fondamentale: La Collaborazione
- Messaggi di aggiornamento durante le sfide per la comprensione di errori o di nuove nozioni in seguito alla buona riuscita del test

Personaggi



Giocatore

Membro del team di sicurezza, identifica e neutralizza le minacce, incrementando le proprie capacità nella sicurezza informatica nel rispetto delle regole del gioco



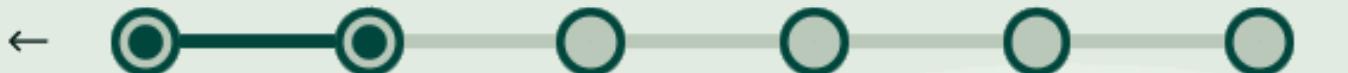
Team Leader

Mentore che fornisce briefing e feedback permettendo al team di procedere di pari passo nella identificazione e neutralizzazione della minaccia



Colleghi Virtuali

Altri membri del team che collaborano nelle sfide cooperative fornendo supporto logistico nelle diverse task o quiz



Quali sono le minacce informatiche più comuni?

Sono possibili più risposte.

Phishing

Malware

Scarsa gestione delle password

Ransomware

Controllo

Scenario



Proprietà fisiche

Gioco 2D, Rappresentazione visiva semplice, scenario simile ad un desktop computer



Dimensione temporale

Sessioni per sfide e quiz, senza limiti di tempo



Dimensione ambientale

Ambiente ufficio virtuale, grafica chiara e non distrattiva



Dimensione emozionale

Senso di urgenza e attenzione, fiducia e competenza



Dimensione etica

Promuove comportamenti etici e sicuri, educa sui rischi etici legati alla sicurezza informatica

CyberShield
Principiante

You're on fire!
Completa una sfida settimanale ogni settimana per creare una striscia e mantenere vivo il tuo modificatore di striscia!

578 entrate
Il tuo punteggio 7% La tua immagine

La tua storia

Sfida 1 Iniziamo
Quanto è importante cybersecurity? Gioca a questa sfida e realizza il tuo primo guadagno 🎉🎉🎉

Sfida bonus 1 Iniziamo
È il momento della sfida dei bonus! Ottieni un guadagno extra per la tua organizzazione. Dimostra di aver superato questa sfida.

Inizia a giocare →

Homepage

- La Homepage è composta da diversi elementi visivi come: icone, menù, button; che permettono la semplice comprensione della schermata, rendendola più efficiente e usabile da qualsiasi utente.
- E' progettato per essere in 2D con un modello di interazione desktop

- # Feedback
- Il Serious Game mostra messaggi di spiegazione in caso di errore che permettono l'utente ad apprendere qualcosa durante il quiz ma di comprendere anche il proprio livello

Quali sono le minacce informatiche più comuni?

Sono possibili più risposte.

✓ Ops, non è la risposta corretta... Spiegazione ⓘ

Spiegazione

Questi sono tutti esempi di minacce informatiche comuni. Durante le sfide affronteremo questi argomenti e altri ancora. Ogni sfida si concentrerà su un argomento specifico per aumentare il tuo livello di consapevolezza informatica. Continuiamo a giocare!

✓ Phishing

✓ Malware

✓ Scarsa gestione delle password

✓ Ransomware

Continua →

Ricompense

Qui puoi vedere tutte le ricompense che hai ottenuto e quelli che puoi ancora ottenere.



Raggiungi il livello 2

1/1 già completato



Raggiungi il livello 3

1/1 già completato



Raggiungi il livello 4

0/1 già completato

Raggiungi il livello 2 e diventa Medior. Raggiungi questo livello ottenendo almeno 5000 punti nelle sfide.

Raggiungi il livello 3 e diventa Senior. Raggiungi questo livello totalizzando almeno 15000 punti nelle sfide.

Raggiungi il livello 4 e diventa un professionista. Raggiungi questo livello ottenendo almeno 100.000 punti nelle sfide.



Raggiungi il livello 6

0/1 già completato



Raggiungi il livello 7

0/1 già completato

Raggiungi il livello 6 e diventa Maestro. Raggiungi questo livello ottenendo almeno 1.000.000 di punti nelle sfide.

Raggiungi il livello 7 e diventa una Leggenda. Raggiungi questo livello ottenendo almeno 3.000.000 di punti nelle sfide.



Punteggio 10.000 punti

0/1 già completato

Ottieni 10.000 punti completando le sfide. Vuoi fare più punti velocemente? Allora gioca anche alle sfide bonus.

Ricompense

- Vengono utilizzate anche delle ricompense sottoforma di livelli da raggiungere tramite la riscossione di punti esperienza in base alla "missione" superata. In questo modo aumenterà anche la reputazione del giocatore, rendendola pubblica o privata agli altri in base al proprio interesse

Nozioni

- Il serious game comprende anche dei messaggi informativi utili per risolvere delle sfide future tramite delle nozioni, a volte esplicate da immagini intuitive



Anche tu puoi essere un bersaglio

Forse non te lo aspetti, ma i criminali informatici prendono di mira tutti i tipi di organizzazioni grandi e piccole e anche i privati. Quindi anche tu sei a rischio, sia a livello privato che professionale.

Infatti, a volte i criminali informatici ti avvicinano mentre in realtà vogliono attaccare qualcun altro. Per questo motivo potrebbero anche cercare di contattarti attraverso un collega. Tutti possono essere un bersaglio, quindi anche tu. Anche se pensi di non avere nulla da nascondere.



Continua →

Attenzione! Ti stanno attaccando

Attenzione, un hacker ti sta attaccando con una SQL Injection! Quale delle seguenti azioni intraprenderai per difenderti?

Utilizzerò query parametrizzate per evitare l'iniezione di codice SQL.

Aggiornero il mio antivirus per rilevare e bloccare l'attacco.

Sanificherò e convaliderò attentamente tutti gli input forniti dagli utenti.

Cambierò la mia password del database per prevenire l'accesso non autorizzato.



Attacco

- A volte nei quiz compariranno delle domande "speciali" che simulano un'attacco (come quelli trattati nel caso di studio)
- La grafica di queste domande sara' diversa per rendere il quiz più immersivo
- Se si rispondera' a queste domande in maniera corretta, si ricevera' una ricompensa maggiore (in termini xp)

classifica

- Sarà presente una classifica tra i vari dipendenti che partecipano al gioco
- Ci saranno dei livelli specifici che si sbloccheranno in base ai punti esperienza
- Ad ogni livello sbloccato l'utente otterra' una ricompensa per "invogliarlo" a fare sempre meglio

Leaderboard

La dashboard è il modo più semplice per ottenere informazioni sul tuo comportamento online su tutti i dispositivi.



Principiante

20/05/2024



Medior



Senior



Professionale



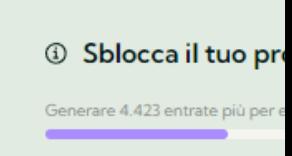
Specialista



Maestro



Leggenda



Classifiche

Progressi

Entrate

#1



Eurobet

578



SERIOUS GAME:
Ambito Formativo



**UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO**

***Graxie per
l'attenzione!***

contatti:

g.devincenzo14@studenti.uniba.it

l.colucci23@studenti.uniba.it

SICUREZZA INFORMATICA - A.A. 2023/24

[Torna all'indice](#)