Co-funded by the
Erasmus+ Programme
of the European Union

CYBER.VET.EU

IMPROVING CYBERSECURITY READINESS OF THE EUROPEAN VOCATIONAL EDUCATION AND TRAINING SECTOR

# MATERIALE DIDATTICO

## IMATERIALE FORMATIVO PER LA CONSAPEVOLEZZA SULLA SICUREZZA INFORMATICA NEL SETTORE IFP

NGO NEST Berlin
AEII
tandemplus network
Latvian European Community Studies Association
COFAC
EOS
inerciadigital
meath partnership

Co-funded by the Erasmus+ Programme of the European Union

# INTRODUZIONE AL MATERIAL FORMATIVO

# GAME JAMS

## INTRODUZIONE

Dall'autunno 2021, in occasione del Mese europeo della sicurezza informatica, alla primavera del 2022, i partner del progetto CYBER.VET.EU hanno organizzato diversi GameJam nei paesi dei partner. I giovani sono stati coinvolti dando loro la possibilità di essere vicini ai temi della cybersecurity e fornendo loro nuovi strumenti.

L'obiettivo principale di questo Intellectual Output era risolvere la necessità di una maggiore consapevolezza sulla sicurezza informatica. Ci siamo rivolti al processo di "gamification" per ottenere una soluzione facile da adottare, veloce da implementare, scalabile nel tempo e inclusiva. Il processo di gamification, definito come "l'applicazione delle meccaniche di gioco a contesti non di gioco con l'obiettivo di indurre coinvolgimento e aumentare i livelli di motivazione", è un modo dimostrato per mantenere gli utenti coinvolti in attività di apprendimento, con grandi risultati anche nel breve periodo di tempo grazie allo sfruttamento dell'intrattenimento che motiva i partecipanti a impegnarsi di più con il materiale e ad esercitarsi. In quanto tale, questo output fungerà da combinazione di linee guida, formazione e pratica, con la caratteristica di essere facilmente aggiornabile quando dovrebbe essere aggiunto nuovo materiale.

## RISULTATI DELLE GAME JAMS

- Maggiore consapevolezza della sicurezza digitale
- Maggiore consapevolezza della sicurezza digitale tra le comunità dei partecipanti (famiglia, amici, colleghi)
- Riduzione del tasso di successo del malware all'interno delle istituzioni
- Riduzione degli eventi di fuga di dati
- Cresce l'interesse per il settore della cybersecurity come opportunità di lavoro.

# AEII / INERCIA DIGITAL [ES]

## ATTIVITÀ

Le attività più rilevanti svolte dai partner spagnoli AEII e Inercia Digital sono state:

- Hackaton
- GameJams
- Giornate informative
- Conferenza internazionale
- Evento divulgativo

## RISULTATI

Le sessioni di GameJam in Spagna hanno fornito alcuni risultati utili che possono essere visualizzati qui:

https://scratch.mit.edu/projects/611211889/

https://scratch.mit.edu/projects/611201682/ https://www.youtube.com/watch?v=3QFI9iB0iJU&t=124s

# AEII / INERCIA DIGITAL [ES]

## GAME JAM


Gamejam in Cyber.EU.VET

20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

0 No me gusta Compartir Descargar Guardar ...


Gamejam in Cyber.EU.VET

20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

0 No me gusta Compartir Descargar Guardar ...

Co-funded by the Erasmus+ Programme of the European Union

# AEII / INERCIA DIGITAL [ES]

## Hackathon

*La cybersicurezza nell'educazione*

I partner spagnoli AEII e Inercia Digital hanno partecipato online a un Hackathon dal 20 al 22 ottobre 2021, con 47 partecipanti, molti dei quali esperti IT.
https://www.comprometidosporelfuturo.com/proyectos# supportato da Boehringer Ingelheim in Spagna.

**PROBLEMA DA RISOLVERE**

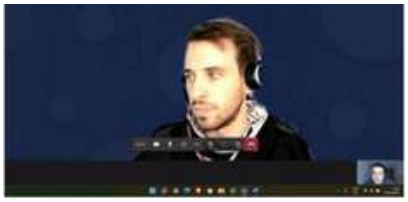
Il cyberbullismo è uno dei principali rischi di Internet per i giovani. È comune trovare post con contenuti offensivi nei confronti di alcune persone e che questi vengano utilizzati per molestare e deridere le vittime.

Il cyberbullismo spesso causa gravi disturbi nelle vittime come disturbo da stress post-traumatico, depressione, pensieri e comportamenti suicidari o ansia.

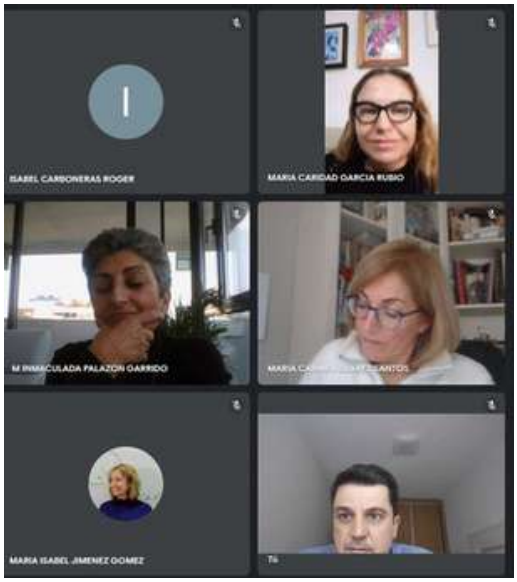
Questa sfida consiste nello studiare e analizzare ciò che i giovani sanno sulla sicurezza, oltre a renderli consapevoli dei rischi che corrono nei loro centri educativi e nella vita quotidiana. Questa sfida cerca, attraverso la gamification, la maggiore consapevolezza di studenti e insegnanti nella vita di tutti i giorni sui temi legati alla sicurezza nell'uso delle nuove tecnologie.

**RISULTATI**

- Gioco e animazione legati alla sicurezza informatica nell'istruzione
- Coinvolgimento della pubblica amministrazione, scuole di formazione professionale, esperti IT, insegnanti, studenti e partner di progetto
- Realizzazione di brevi video interattivi



# AEII / INERCIA DIGITAL [ES]





In generale, dopo aver condotto numerosi sondaggi, la conoscenza della sicurezza informatica di insegnanti e studenti nei centri di formazione professionale è ancora bassa in Spagna. Per questo motivo, questo progetto e altri simili sono molto rilevanti in Spagna.

# NGO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

## GAME JAM

NGO Nest Berlin, Extrafondente Open Source - EOS e IASIS hanno realizzato insieme una sessione di GameJam nel febbraio 2022. Il GameJam è iniziato sabato 12 ed è durato complessivamente 6 giorni. Ha visto le squadre nazionali sviluppare e lavorare insieme su una bozza di gioco (di un gioco online o da tavolo).

È stata riunita una giuria indipendente a cui è stato chiesto di valutare la bozza del gioco seguendo linee guida comuni e un modello di valutazione.

La squadra vincitrice ha ricevuto un tutoraggio di 6 mesi e risorse tecniche per sviluppare ulteriormente l'idea del gioco.

**RIGUARDO AL GIOCO**

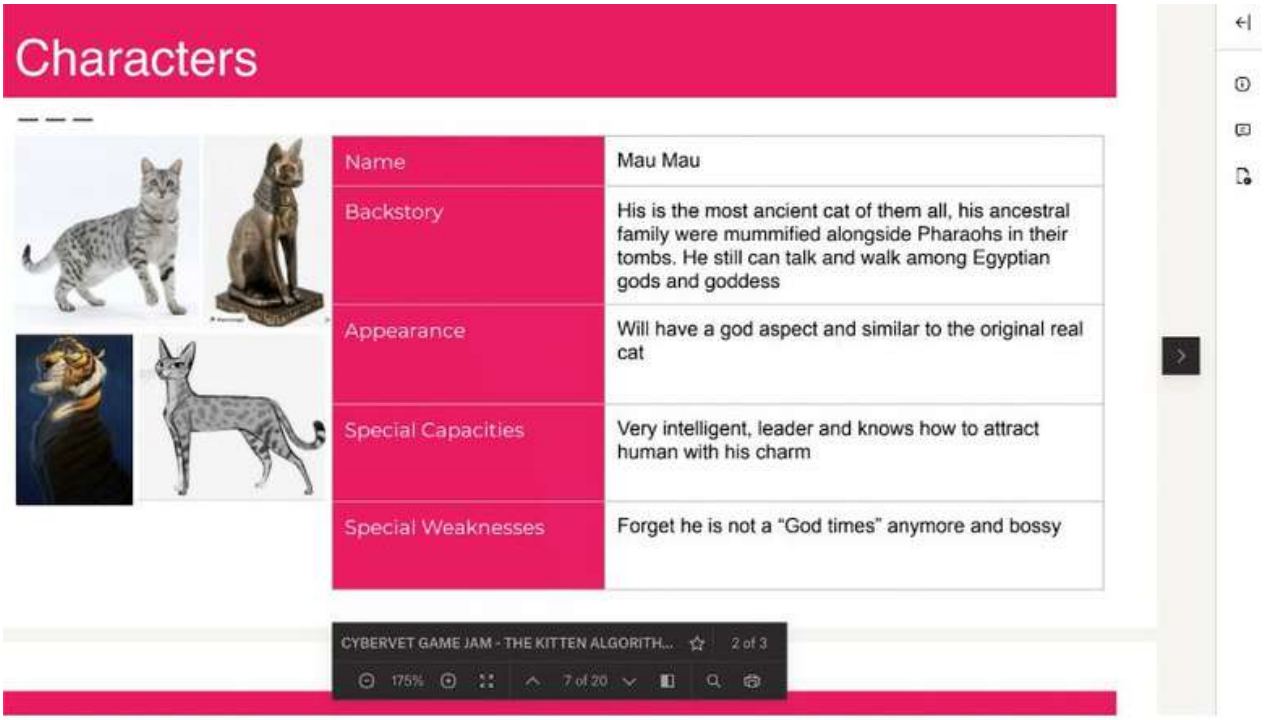
È un gioco da tavolo strategico a turni da 2 a 6 giocatori, che richiede dai 30 ai 60 minuti per essere giocato. In questo gioco inganni gli umani per convincerli che sei il miglior gatto e ottieni più prestigio ottenendo il maggior numero possibile di servitori di gatti umani. Tieni gli occhi aperti, gli altri gatti boss cercheranno attivamente di sabotare la tua strada per raggiungere gli umani e prendersi la gloria per se stessi. Non fidarti delle loro facce carine!

Perdi la partita se non hai un numero elevato di umani come servitori o il decimo round è finito e nessuno dei giocatori ha almeno 4 umani al proprio comando.

La difficoltà è che ci sono 6 Boss che cercano di ingannare gli umani per farli diventare i loro servitori e quindi i capi possono controllarli, ma tutti hanno lo stesso obiettivo e alcuni potrebbero persino aiutare gli umani a liberarsi dal controllo del gatto.

# NGO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

## Mau Mau



# LECSA (LV)

# GAME JAM

Il partner LECSA dalla Lettonia ha organizzato un evento GameJam dal 27 settembre al 1 ottobre 2021. A causa delle restrizioni epidemiologiche e delle diverse località dei partecipanti, è stato organizzato come un evento di tipo ibrido (in loco presso la Saldus Technical School e tramite la piattaforma Zoom). Durante l'evento sono state formate 6 squadre (4-5 persone per squadra) per lavorare allo sviluppo dei prototipi del gioco. Per ottenere alcuni risultati tangibili, il concetto di Game Jam prevedeva lo sviluppo di due tipi di giochi: giochi per computer e giochi da tavolo.

## ATTIVITÀ

Agosto - settembre 2021 è stato dedicato alla pianificazione e all'organizzazione dell'evento (ricerca di esperti in sicurezza informatica e sviluppo del gioco, distribuzione delle informazioni ai potenziali partecipanti, pianificazione dell'agenda e definizione dei criteri per il gioco, ecc.)

Evento moltiplicatore – Attualità nei cyberattacchi (27.09.2021): Introduzione del progetto CYBER.EU.VET e conferenza sulle tendenze nei cyberattacchi con Mr. Armins Palms, esperto di sicurezza informatica del CERT.LV (IT Security Incident Response Institution of the Repubblica di Lettonia)

Numero di partecipanti: 26 persone

Luogo: Saldus Technical School (città di Saldus) e piattaforma ZOOM

Annuncio del Game Jame (27.09.2021): definizione e discussione sulle attuali sfide nella sicurezza informatica (valutazione dei bisogni); formazione di team, incontro con i mentori e discussione su ulteriori lavori (workshop sul motore di gioco Unity), brainstorming sull'idea e sul concept del gioco.

Attività di Game Jam in corso (28.09-30.09.2021): i team hanno lavorato allo sviluppo dei prototipi, se necessario è stata assicurata la consultazione con i mentor.

Presentazione dei progressi (30.09.2021): presentazione dei concetti del gioco e dei progressi del lavoro per ricevere suggerimenti dai mentori.

Gran finale (01.10.2021): quattro squadre hanno presentato i loro risultati e i mentori hanno fornito la valutazione. Una squadra, che stava sviluppando un gioco per computer, si è ritirata. Conclusione dell'evento e discussione informale.

Numero di partecipanti: 30

Luogo: Saldus Technical School e piattaforma ZOOM

# LECSA (LV)

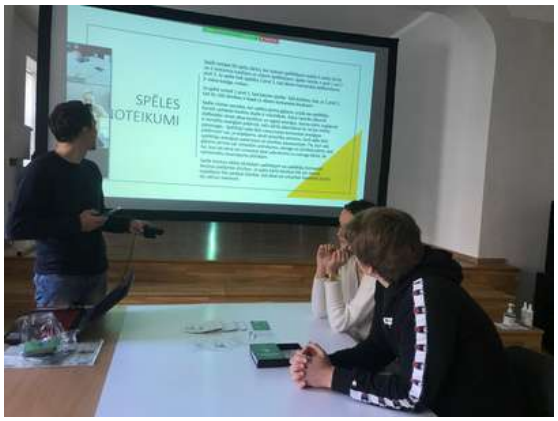

**RISULTATI**

1.Prototipo di gioco online - Il virus

2. Gioco da tavolo - Carte sulla sicurezza

3. Gioco da tavolo - Cyberwar

4. Gioco di carte competitivo - Cyber Mind




**ESEMPIO** Cyber Mind - A competitive card game

Questo è un gioco di carte educativo con elementi quiz. Il compito principale del gioco è insegnare le basi della sicurezza quotidiana su Internet e ciò a cui le persone si espongono facendo cose sciocche su di esso. Copre argomenti come la sicurezza in Internet e la protezione dei dati nel contesto dell'utilizzo dei social network. Nel risultato del gioco le persone (giocatori) dovrebbero essere in grado di riconoscere i tentativi di truffa nella vita reale.

Sviluppato dal team Veiksminieki (dal lettone: persone di successo), studenti della scuola tecnica Saldus durante il Game Jam in Lettonia (ottobre 2021):
Renars Ricards Hartmanis, Estere Ozoliņa, Sindija Diāna Valtere e altri.

Livello: base (per principianti). Gruppo target – alunni, studenti, insegnanti e genitori

Il gioco contiene: 50 carte, 2 cuscinetti sanitari (per contare la salute dei giocatori), 2 dadi e una carta delle regole.

# LECSA (LV)

# GAME JAM

## IL GIOCO

I tentativi di attacchi informatici nel mondo aumentano ogni giorno, quindi il governo mondiale ha avuto l'idea di organizzare un torneo per identificare le persone che portano rischi informatici e contrattaccare contro di loro.
Gioco educativo che aiuta a conoscere i principali tipi di attacchi informatici, i metodi di prevenzione ed eliminazione proteggendo te stesso o la tua squadra e contrattaccando l'avversario. Lo scopo del gioco è togliere tutte le vite dell'avversario/i.

## COME GIOCARE GIOCO/REGOLE

Numero di giocatori: 2 o 4 persone (1 contro 1 o 2 contro 2).
Ogni giocatore o squadra (quando 2 contro 2) ha "100 vite" (Salute=HP) all'inizio del gioco. Il conteggio della salute viene eseguito utilizzando blocchi note neri o altre note disponibili.
Assegna una persona separata che segua e calcoli il consumo di energia e salute dei giocatori, se possibile. Altrimenti i giocatori lo fanno da soli.
Ogni giocatore riceve 5 carte. Se il gioco si gioca 2 contro 2, entrambi i giocatori hanno "una mano comune" nella squadra o 10 carte insieme.

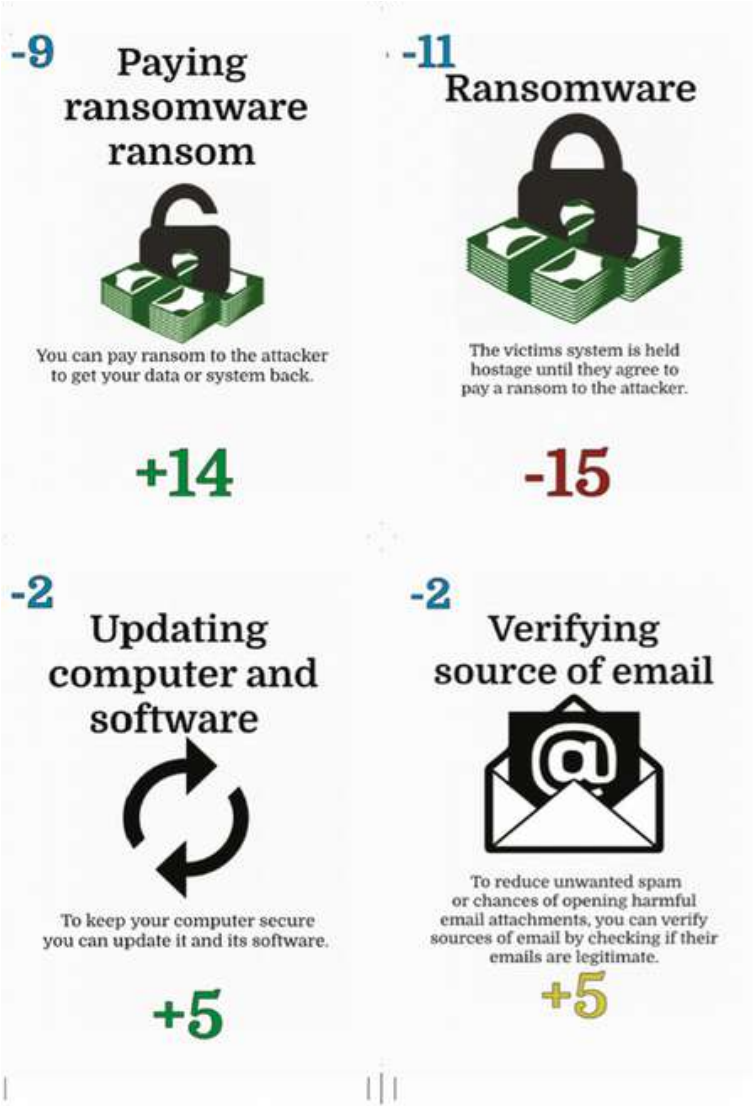
Ci sono tre tipi di carte: Carte Attacco (rosse), Carte Scudo (gialle) e Carte Vita o Cura (verdi).

Il gioco si gioca a turni. Il giocatore/la squadra che ottiene il numero più alto con i dadi inizia il gioco.
Ogni carta costa energia. All'inizio di ogni round, il giocatore tira 2 dadi per definire un'Energia che è indicata nella parte superiore della carta (in blu). Le carte devono essere giocate in modo da non superare la quantità di energia ottenuta.
Il giocatore/squadra che inizia il round può attaccare (con Attack Cards), proteggersi (Shield Cards) o aggiungere vita (Healing Cards), mentre i second mover possono usare solo Attack e Shield card per ridurre al minimo la loro vulnerabilità alla vita.
Tieni presente che il numero massimo di vite per giocatore/squadra durante il gioco può essere di 100 HP (ad esempio, se la somma di vite ed energia dopo il round fa 110 HP in totale, il tuo numero di vite rimane comunque – 100 HP).
Il gioco termina non appena un giocatore/squadra esaurisce tutte le vite (0 vite).
Se il gioco esaurisce le carte, devi rimescolare le carte dalla pila.

# LECSA (LV)

**Esempi di carte:**

In **blu** – Energia
In **rosso** - Carte attacco
In **giallo** - Carte scudo
In **verde** - Carte guarigione



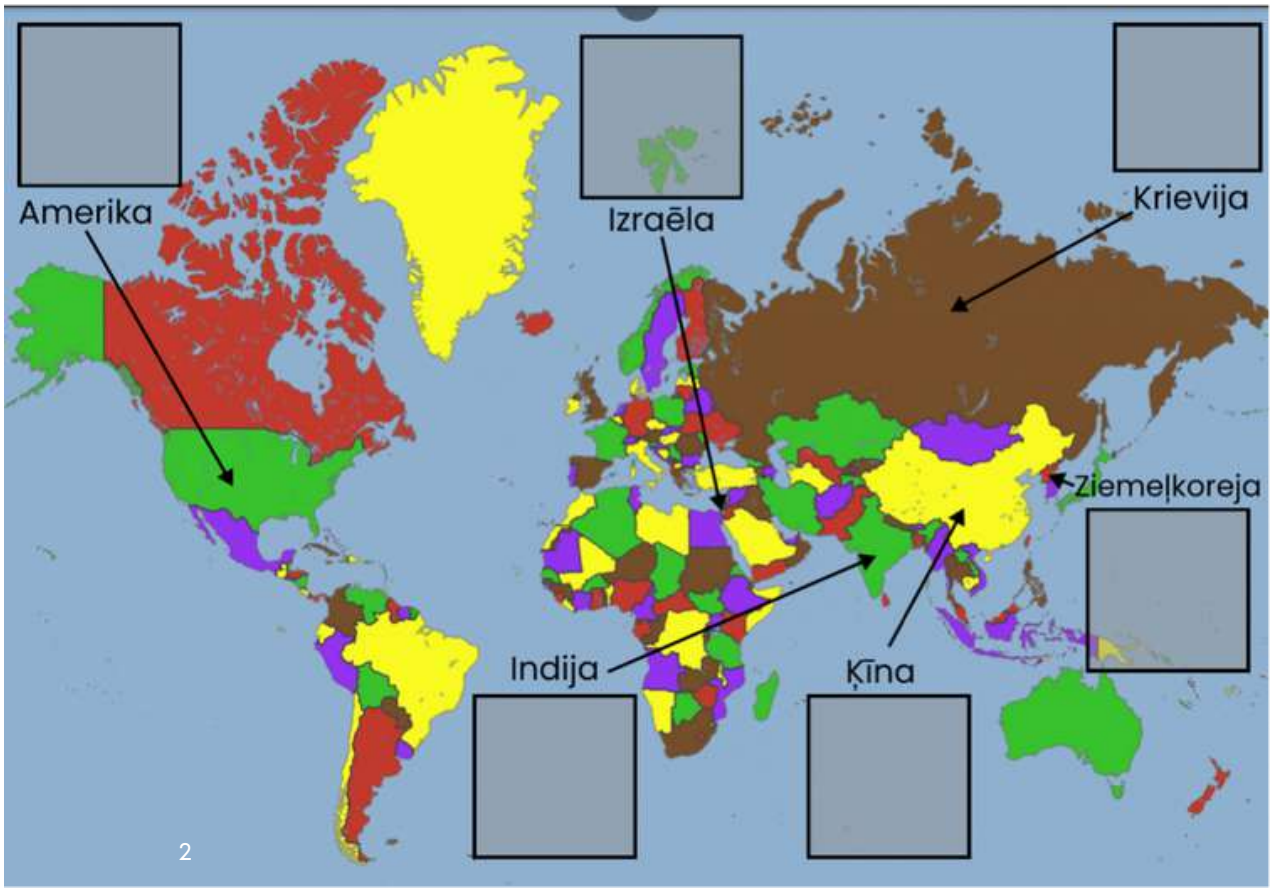

**Esempio di calcolo della guarigione:**

**ESEMPIO** Cyberwar - Gioco da tavolo

Sviluppato dal team Exodus (studenti della Saldus Technical School), leader del team Valdemārs Šperbergs.
2-6 giocatori < – > Adatto a persone dai 15 anni in su
Un gioco da tavolo con una forte enfasi sulla tattica e sulla casualità (caso).
Livello: gioco educativo per coloro che hanno una certa conoscenza della sicurezza informatica.
Il gioco contiene: mappa del mondo, 2 dadi, server, carte con funzione "attacco", "difesa" o "reazione", legenda delle vulnerabilità, una tabella con le possibili mosse per ogni tipo di vulnerabilità.

**IL GIOCO**

Lo scopo del gioco è proteggere il paese rappresentato dal giocatore e attaccare altri paesi per vincere la guerra informatica. In Cyberwar, ogni giocatore deve scegliere un paese da rappresentare. Ogni giocatore ha un server con 3 vulnerabilità. L'obiettivo del giocatore è hackerare i server di altri paesi sfruttando due vulnerabilità su tre o correggere due vulnerabilità su tre sul proprio server.



# LECSA (LV)

## COME GIOCARE

I giocatori scelgono il paese da rappresentare e posizionano un oggetto server in un punto designato della mappa. Ogni paese ha i suoi bonus. Ogni giocatore pesca (prende) casualmente 3 vulnerabilità, una per ogni livello di difficoltà, e le posiziona a faccia in giù nelle rispettive posizioni sui propri campi del server. Le vulnerabilità non sono note per i giocatori. Le vulnerabilità hanno 3 livelli di difficoltà. Il livello di difficoltà determina anche quanto grande numero è necessario per sfruttare una vulnerabilità (vedi "Attacchi"), così come determina quante mosse saranno necessarie per correggere la vulnerabilità (vedi "Défense").

Il gioco si svolge nei round, è possibile eseguire le seguenti azioni (mosse): scansione, attacco e difesa. I giocatori determinano la sequenza dei giocatori lanciando due dadi. Inizio Ogni giocatore riceve 4 carte all'inizio di ogni round. Alla fine del round, è possibile – tenere 2 carte o scambiarle con quelle esistenti. Il primo round è un round di scansione in cui non sono consentite carte di attacco o difesa. Nei round successivi, i giocatori possono scegliere di scansionare o attaccare o provare a riparare le proprie vulnerabilità (vedi Défense). Il gioco continua round dopo round fino al raggiungimento di una condizione vincente. Scansione L'attaccante sceglie un paese per scansionare la sua vulnerabilità (ad esempio, "Sto scansionando un russo di 2° livello di vulnerabilità"). Il giocatore esegue la scansione: lancia due dadi, applicando i bonus del paese rappresentato, confronta con il livello di difficoltà di vulnerabilità + bonus del paese della vittima. Se l'attaccante ha ottenuto un numero uguale o superiore al livello di difficoltà di vulnerabilità della vittima, l'attaccante può esaminare la vulnerabilità scansionata. I bonus del paese non vengono aggiunti durante la scansione di te stesso.

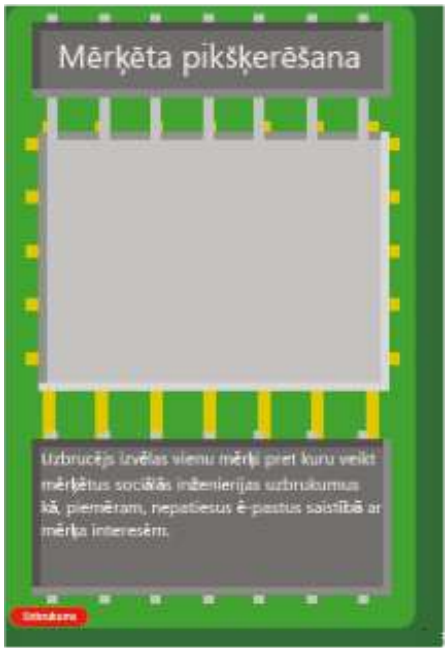
Livelli di difficoltà 1° – il giocatore deve ottenere almeno il numero 4 (esclusi i bonus del paese) 2° – il giocatore deve tirare almeno 8 (esclusi i bonus del paese) 3° – il giocatore deve tirare almeno 11 (esclusi i bonus del paese).

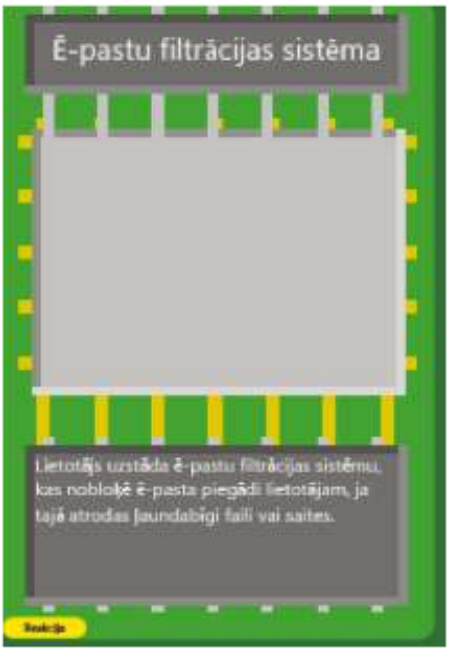
## ATTACCHI

- Il giocatore nomina l'obiettivo dell'attacco (ad esempio, "Attacco una vulnerabilità russa di livello 2") e rivela la carta di attacco a tutti i giocatori, posizionandola accanto alla vulnerabilità.
- Il giocatore tira i dadi per vedere se l'attacco funziona confrontando il tiro con la difficoltà di vulnerabilità + bonus (se il numero ottenuto + i bonus corrispondono o superano la difficoltà, l'attacco ha successo).
- Gli attacchi possono essere respinti utilizzando la Carta Reazione progettata per quell'attacco.
- Ogni attacco ha il proprio tipo di reazione che può essere giocato e il proprio tipo di vulnerabilità per cui funziona.
- Se l'attacco fallisce o viene bloccato da una Carta Reazione, le carte Attacco e Reazione giocate rimangono sul tavolo fino alla fine del round successivo e impediscono agli altri giocatori di attaccare con lo stesso attacco per la stessa vulnerabilità. Dopo la mossa entrambe le carte tornano nel mazzo.

**Livelli di difficoltà**

1° – il giocatore deve ottenere almeno il numero 4 (esclusi i bonus del paese)
2° – il giocatore deve tirare almeno 8 (esclusi i bonus del paese)
3° – il giocatore deve tirare almeno 11 (esclusi i bonus del paese).



# LECSA (LV)

## DIFESA

- Difesa: scegliere il metodo giusto contro una particolare vulnerabilità. Reaction Cards blocca (annulla) l'attacco in arrivo (e tutti gli altri attacchi che mirano alla stessa vulnerabilità) per 1 turno.
- Per annullare un attacco in arrivo, il giocatore posiziona una carta di reazione corrispondente al tipo di attacco (vedi tabella con le vulnerabilità) sulla carta di attacco non appena l'attacco viene giocato.
- Per iniziare a riparare un infortunio, un giocatore posiziona una carta Défense accanto all'infortunio da riparare.
- Gli altri giocatori possono attaccare questo infortunio mentre è in Difesa (prima che il turno di Difesa sia terminato).
- Quando il giocatore cerca di riparare un infortunio sul suo server con una carta Défense, non può attaccare, ma può tentare di prevenire gli attacchi con le carte di reazione. Per una riparazione completa è necessario |livello di difficoltà + 1| giro. L'azione di scansione è consentita durante il periodo di riparazione.
- Se il metodo Défense non è corretto, il giocatore salta 3 turni e non può usare Carte Défense durante questo periodo (le reazioni e le azioni di scansione sono consentite).

| Vulnerability | Attacks | Défense | Reaction |
|---|---|---|---|
| 1st vulnerability level | | | |
| SSH server with username | Password guessing | Usage of the public key | Settings of Blocked Period |
| Administration Panel with User Name | Password guessing | Blocking external requests | Settings of Blocked Period |
| Untrained employee | Phishing campaigns | IT security trainings | Filtration system of e-mails; Implementation of e-mail SPAM list |
| Vulnerable SMB protocol | Exploitation of EternalBlue | Fixing vulnerability CVE-2017-0144 | n/a |
| XSS vulnerability | Code injection; Code injection using Polyglot | Introductory synthesis | Introduction of the symbol blacklist |

**Bonus per i Paesi**

- USA: +2 in scansione
- Russia: +2 per gli attacchi
- Cina: +2 per la difesa dagli attacchi
- Corea del Nord: +2 per la difesa contro la scansione
- India: +1 in tutti gli attacchi, -1 contro gli attacchi
- Israele: +3 in tutti gli attacchi, -3 contro gli attacchi

| | | | |
|---|---|---|---|
| SQL injection | Code injection; Code injection using Polyglot | Introductory synthesis | Introduction of the symbol blacklist |
| Router panel with default username and password | Using default data | Complete replacement of authentication data | One session limit |
| 2nd vulnerability level | | | |
| SSH server | Password guessing | Usage of the public key | Settings of Blocked Period |
| Administration Panel | Username guessing | Blocking external requests | Settings of Blocked Period |
| XSS vulnerability with filter | Code injection using Polyglot | Introductory synthesis | Introduction of the symbol blacklist |
| SQL injection with filter | Code injection using Polyglot | Introductory synthesis | Introduction of the symbol blacklist |
| Incompletely configured firewall | Packet fragmentation | Repair configuration | IDS implementation |
| WiFi network with WEP security | Packet Phishing | Using the WPA2 standard | RADIUS implementation |
| Busy CEO/boss | Phishing – catching the big fish | IT security trainings | Filtration system of e-mails; Implementation of e-mail SPAM list |
| 3rd vulnerability level | | | |
| Service failure | DDoS | IP address blocking and load limiting | Load balancers |
| Vulnerable OpenSSL program | Heartbleed exploitation | Repair of CVE-2014-0160 | n/a |
| Vulnerable Print Spooler program | PrintNightmare exploitation | Repair of CVE-2021-36958 | n/a |
| Buffer overflow vulnerability | Buffer overflow | Introduction of buffer limits | Increasing the buffer |
| Weak hashing algorithm | Decryption of the hash value | Improving the hash algorithm | Usage of a strong and long password |
| Lazy IT expert | Targeted phishing | IT security trainings | Filtration system of e-mails; Implementation of e-mail SPAM list |

Co-funded by the
Erasmus+ Programme
of the European Union



# LECSA (LV)


SSH serveris


SSH serveris ar lietotājvārdu


Administrācijas panelis


Administrācijas panelis ar lietotājvārdu


Neapmācīts darbinieks


Ievainojams SMB protokols

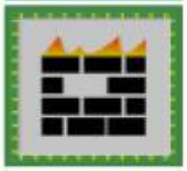

XSS ievainojums


SQL injekcija


Rūtera panelis ar noklusējuma lietotājvārdu un paroli


XSS ievainojums ar filtru


SQL injekcija ar filtru

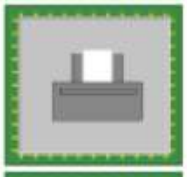


Nepilnīgi nokonfigurēts ugunsmūris


WiFi tīkls ar WEP drošību


Pakalpojuma atteices kļūda

Ievainojama OpenSSL programma



Ievainojama Print Spooler programma

Bufera pārpildes ievainojums

Vājš jaucējvērtības algoritms

Aizņemts priekšnieks


Slinks IT speciālists

Co-funded by the
Erasmus+ Programme
of the European Union

YBER.VET.EU

# LECSA (LV)

## GAME JAM


# LECSA (LV)



## TIPS & EXPERIENCES FROM THE GAMEJAM IN LATVIA

- Durante l'evento di 2 giorni non è possibile sviluppare un vero gioco per computer, ma piuttosto il primo prototipo, che potrebbe essere ulteriormente sviluppato o meno a seconda della motivazione dei partecipanti.
- Premi o altri tipi di benefici possono aiutare a coinvolgere più partecipanti e garantire risultati migliori (più tangibili) alla fine (nel nostro caso - pizza e bevande sono state fornite alla fine dell'evento, ulteriore supporto da parte dei mentori (ad es. la piattaforma)).
- I tutor sullo sviluppo del gioco e sui problemi di sicurezza informatica svolgono un ruolo importante nel Game Jam consultando e aiutando i partecipanti.
- Pianificare in anticipo – poiché si tratta di un evento piuttosto complesso e richiede un'attenta pianificazione.
- Gli organizzatori devono considerare che alcune squadre potrebbero non partecipare alla competizione (a causa dei tempi limitati).

Si prega di consultare i post FB con i risultati dell'evento:
https://www.facebook.com/cybereuvetproject.eu/posts/138127645211214
https://www.facebook.com/saldustehnikums/posts/1780232175520378

L'evento è stato organizzato da LECSA in collaborazione con Latvijas Universitāte | Ekonomikas un kultūras augstskola / EKA University of Applied Sciences | McĀbols | cert.lv | Coldwild Games | Saldus tehnikums!

# MEATH PARTNERSHIP (IE)

## ATTIVITÀ

- Incontro informativo sulla valutazione dei bisogni con gli studenti (formazione di codifica in un istituto locale per l'educazione degli adulti)
- 2 giorni GameJam (sessione informativa online il 1° giorno; 2° giorno dedicato a Game Jam)
- Evento - Mattinata di sensibilizzazione sulla sicurezza informatica

## 1) Incontro informativo sulla valutazione dei bisogni con gli studenti

(formazione sulla codifica in un istituto locale per l'educazione degli adulti)
Data: ottobre 2021

## DESCRIZIONE

Al fine di diffondere il progetto e identificare i temi principali per la Game Jam, il team di Meath Partnership ha organizzato una sessione informativa con gli studenti di un corso di formazione locale di Coding. La condivisione delle informazioni sulla Cybersecurity e la discussione sulle minacce più recenti è stata seguita da una sessione di brainstorming di gruppo in cui gli studenti sono stati divisi in due gruppi al fine di discutere le domande che hanno portato all'identificazione degli argomenti più interessanti da approfondire durante il Gamejam. Durante la giornata sono state condivise con i partecipanti anche ulteriori informazioni sul Gamejam e sul progetto CYBER.EU.VET.

## ESEMPIO DI DOMANDE PER LA VALUTAZIONE

**Needs assessment meeting guidelines**

1. What do you know about cybersecurity?
2. Why do I need to be worried about it?
3. What are the biggest cybersecurity concerns/threats right now?
4. Do you know how to recognise those threats?
5. What is a cyber attack?
6. Can you give us an example of a cyber attack?
7. Can you give us, at least, 3 possible solutions to it?

# MEATH PARTNERSHIP (IE)

## RISULTATI

Come risultato di questa attività, il team di Meath Partnership ha acquisito una migliore comprensione della conoscenza complessiva degli studenti in relazione alla sicurezza informatica e alle minacce informatiche, nonché informazioni raccolte che sono state ulteriormente incluse nel processo di pianificazione e implementazione del GameJam.

# MEATH PARTNERSHIP (IE)

# GAME JAM

**2) 2-days Gamejam**

(online information session on the 1st day; 2nd Day dedicated to Game Jam)

## DESCRIZIONE

Il GIORNO 1 è stato dedicato all'accoglienza dei partecipanti e alla presentazione del progetto CYBER.EU.VET e all'apertura del Game Jam, nonché alla condivisione delle informazioni sui 2 temi individuati durante l'incontro di valutazione dei bisogni. Ai partecipanti è stata offerta la possibilità di lavorare individualmente o come parte di un team. Hanno anche avuto l'opportunità di porre qualsiasi domanda o ricevere ulteriori chiarimenti sui procedimenti relative allo sviluppo dei giochi nel giorno 2.

Il GIORNO 2 è stato dedicato allo sviluppo dei giochi e i membri del nostro team e un esperto di supporto IT erano disponibili via Zoom per supportare i partecipanti per tutta la durata del Game Jam da
Dalle 9:00 alle 21:00.
I partecipanti sono stati invitati a caricare i loro giochi sulla piattaforma Itchio sotto un profilo creato appositamente per questo evento: CYBER.EU.VET : Cybersecurity Game Jam - itch.io

## RISULTATI

Dopo che i partecipanti hanno condiviso le loro bozze di gioco con la squadra, un partecipante ha deciso di andare avanti e caricare il gioco per un'ulteriore valutazione. Il resto dei partecipanti ha deciso di non inviare le proprie bozze poiché erano nelle primissime fasi.

**Click or not click**

**Online interactive cybersecurity game**

A short narrative driven game on raising awareness for cyber security threats. The game prompts players to make the right decision and avoid losing your security level.

Link: https://itch.io/jam/cybereuvet-cybersecurity-gamejam

Online interactive cybersecurity game:
https://itch.io/jam/cybereuvet-cybersecurity-gamejam

# MEATH PARTNERSHIP (IE)

**3) Evento - Mattinata di sensibilizzazione sulla sicurezza informatica**

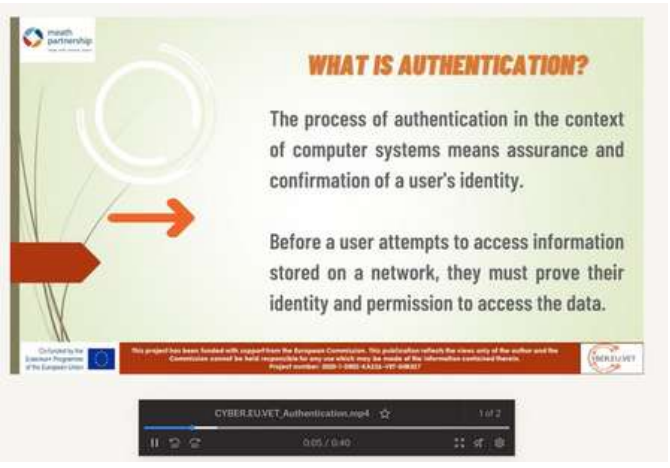
Date: November 2021

## DESCRIZIONE

L'Evento si è tenuto online Via Zoom per far conoscere il progetto e le sue attività. L'evento è stato ampiamente diffuso tra un'ampia varietà di parti interessate interessate o coinvolte nella sicurezza informatica. L'evento è iniziato con una presentazione e panoramica del progetto e della Game Jam, seguita da una presentazione e discussione sulla Cybersecurity e dalla condivisione di informazioni pratiche su come rimanere online (le attuali minacce informatiche e come eliminare possibili attacchi erano possibili).

## RISULTATI

L'evento ha contribuito a sensibilizzare sul progetto e ha anche creato l'opportunità di presentare a un pubblico più ampio i traguardi raggiunti dall'inizio del progetto. È stata anche una grande opportunità per condividere informazioni pratiche e consigli relativi alla sicurezza informatica con i partecipanti all'evento.

# COFAC / UNIVERSIDADE LUSÓFONA (PT)

## GAME JAM

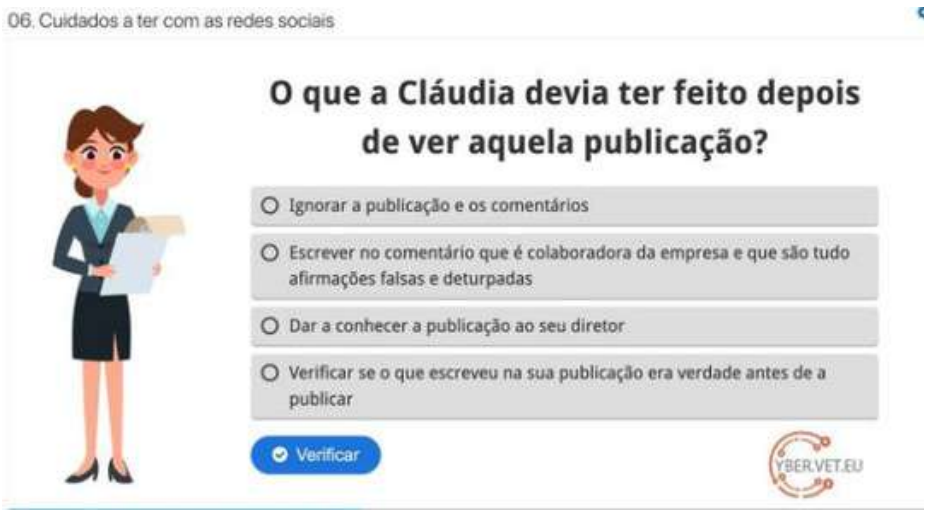
### ATTIVITÀ

1) Cyber &Ethical Hacking post-laurea per futuri professionisti e docenti di mercato
Ott 2021 - Feb 2022 (in collaborazione con una società di consulenza locale denominata Cybersec)
2) 2 sessioni GameJam erogate a gennaio 2022 presso le scuole VET:
Escola de Comércio de Lisboa - https://escolacomerciolisboa.pt
Escola Profissional Almirante Reis - https://www.epar.pt
3) Un cybertraining di tre mezze giornate per gli studenti delle scuole superiori nel marzo 2022: Università Lusofona nell'ambito dell'evento Tecweb - https://tecweb.ulusofona.pt

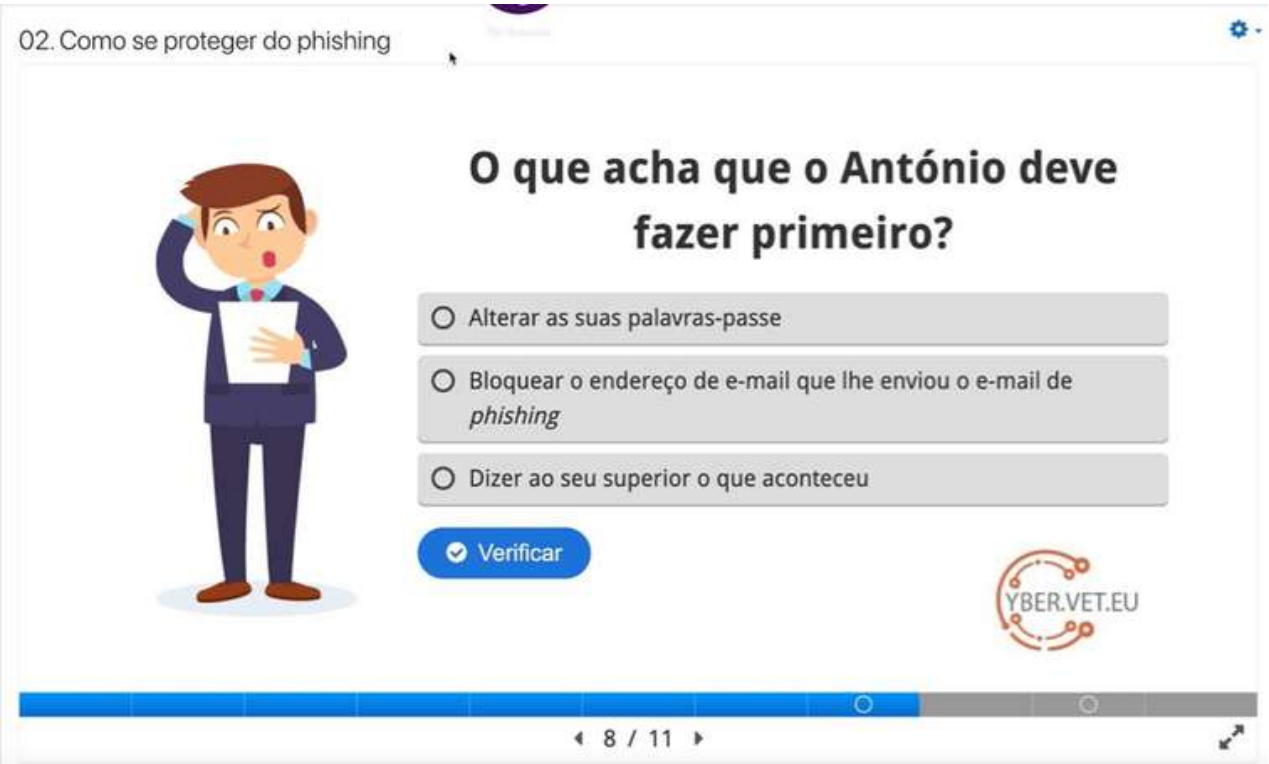
### RISULTATI

Rapporto di diffusione delle prove in cui è possibile vedere i diversi test che sono stati effettuati durante un anno solare (da aprile 2021 ad aprile 2022). In questo rapporto possiamo vedere screenshot di pubblicazioni sui social network, poster di diversi eventi, questionari sulla consapevolezza della sicurezza informatica (disponibili in lingua portoghese su https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oeplRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform).

Durante i Cyberjams, è stato anche creato, sulla base dei sondaggi sulla consapevolezza della sicurezza informatica, una serie di mini-giochi intuitivi/interattivi su semplici situazioni fatte.



# COFAC / UDL (PT)




Inoltre, i partner hanno organizzato alcune sessioni per sensibilizzare i partecipanti sull'argomento scelto e hanno anche organizzato un evento moltiplicatore in cui hanno presentato tutti i materiali ei contenuti creati.


# TANDEM PLUS NETWORK – MEMBER IASIS [GR]

## GAME JAM

**Strumento di progettazione del gioco (IASIS) - Cyberopolis**

Questo gioco è un gioco da tavolo rivolto a persone interessate alla sicurezza informatica, con un massimo di 2-4 giocatori, e i suoi aspetti principali sono la riservatezza dei dati e l'integrità dei dati... mentre i temi che tratta sono malware, phishing, attacchi web-based , attacchi alle applicazioni Web, spam, furto di identità, DDoS e Man in the middle...

Guarda l'immagine di ''Cyberopolis'' per capire meglio i passi da seguire durante il gioco e quali sono le sfide da risolvere...

Screenshot del gioco durante la sessione di GameJam dove possiamo vedere il successo del gioco e il grande interesse mostrato dai partecipanti.


# TANDEM PLUS NETWORK – MEMBER IASIS [GR]

## VIDEO - Prevenire il cyberbullismo

Questo video sviluppato dal partner greco avvicina i visitatori ai diversi modi per prevenire e combattere il cyberbullismo.

Co-funded by the Erasmus+ Programme of the European Union

YBER.VET.EU

# DISCLAIMER

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

**Design**
NGO Nest Berlin e.V.
Berlino, 2022


Co-funded by the Erasmus+ Programme of the European Union