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

CYBER.VET.EU

IMPROVING CYBERSECURITY READINESS OF THE EUROPEAN VOCATIONAL EDUCATION AND TRAINING SECTOR

TRAINING MATERIALS

CYBERSECURITY AWARENESS TRAINING MATERIAL FOR THE VET SECTOR

NGO NEST Berlin
AEII Asociación Educativa por la Integración y la Igualdad
tandemplus network
Latvian European Community Studies Association
COFAC Cooperativa de Formação e Animação Cultural C.R.L.
EOS
inerciadigital
meath partnership

INTRODUCTION TO TRAINING MATERIALS

GAME JAMS

INTRO

From fall 2021, related to the European Month of Cybersecurity, to spring 2022, partners of CYBER.VET.EU project organized several GameJams in partners' countries. Young people were involved giving them the opportunity to be close to cybersecurity topics and providing new tools.

The main objective here was to solve the need for increased awareness on cybersecurity. We turned to the process of "gamification" in order to obtain a solution which is easy to adopt, fast to implement, scalable with time and inclusive. The process of gamification, defined as "the application of gaming mechanics to non-gaming contexts with the aim of inducing engagement and raising levels of motivation", is a demonstrated way to keep users engaged in learning activities, with great results even over short period of time thanks to the exploitation of entertainment which motivates participants to engage more with the material and to practice. As such, this output will act as a combination of guidelines, training and practicing, with the feature of being easily upgradable when new material should be added.

OUTCOMES FROM ACTIVITIES / GAME JAMS

- Increased digital security awareness
- Increased digital security awareness among participants' communities (family, friends, colleagues)
- Reduction in malware success rate within the institutions
- Reduction in data leaks events
- Increased interests for the cybersecurity sector as a job opportunity.

AEII / INERCIA DIGITAL [ES]

ACTIVITIES

The most relevant activities carried out by Spanish partners AEII and Inercia Digital were:

- Hackathon
- GameJams
- Info days
- International conference
- Dissemination event

RESULTS

The GameJam sessions in Spain provided some useful results that can be viewed here: https://www.youtube.com/watch?v=3QFI9iB0iJU&t=124s

ON SCRATCH

https://scratch.mit.edu/projects/611211889/
Cybersecurity - Under Attack

https://scratch.mit.edu/projects/610354561/
in Spanish

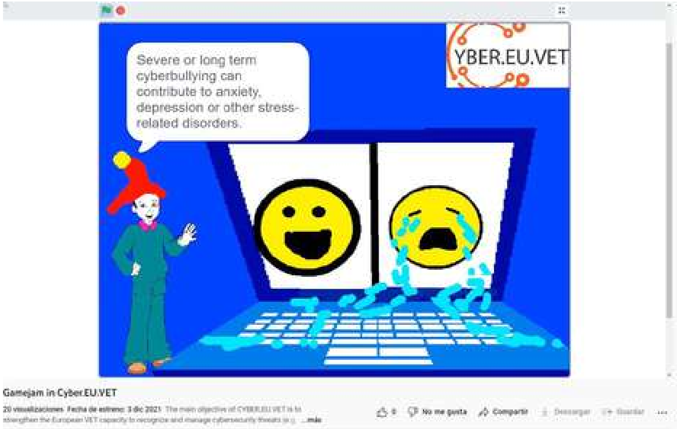
https://scratch.mit.edu/projects/611201682/
https://scratch.mit.edu/projects/714361293/
in Spanish

https://scratch.mit.edu/projects/714362963/
in Spanish

https://scratch.mit.edu/projects/714362911/
on phishing - a remix
https://scratch.mit.edu/projects/606933322
on phishing - in English

AEII / INERCIA DIGITAL [ES]

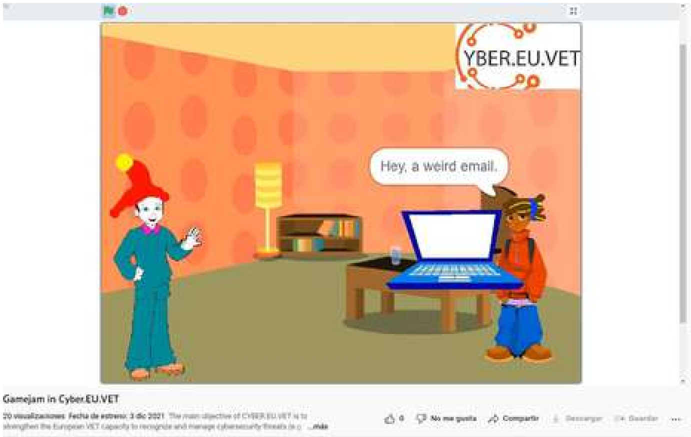
GAME JAM


Severe or long term cyberbullying can contribute to anxiety, depression or other stress-related disorders.
YBER.EU.VET

Gamejam in Cyber.EU.VET

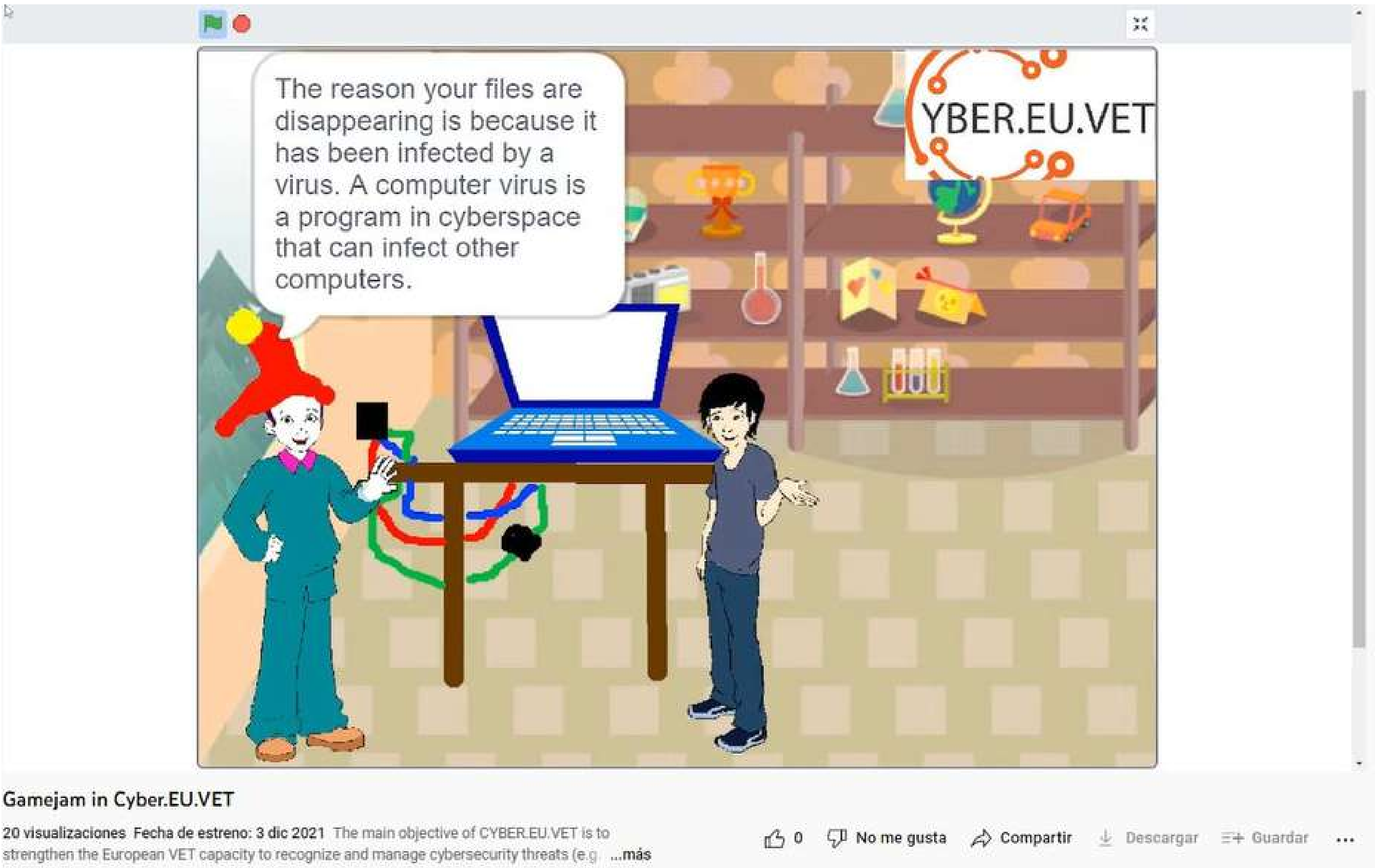
20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

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


The reason your files are disappearing is because it has been infected by a virus. A computer virus is a program in cyberspace that can infect other computers.
YBER.EU.VET

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
...

AEII / INERCIA DIGITAL [ES]

Hackathon

Cybersecurity in Education

Spanish partners AEII and Inercia Digital participated online in a Hackathon from 20 – 22 October 2021, with 47 participants, many of them IT Experts. https://www.comprometidosporelfuturo.com/proyectos# supported by Boehringer Ingelheim in Spain.

PROBLEM TO SOLVE

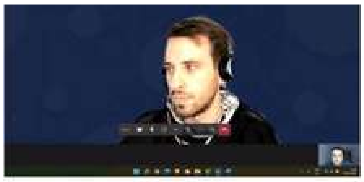
Cyberbullying is one of the main Internet risks for young people. It is common to find posts with offensive content towards some people and that these are used in order to harass and mock the victims.

Cyberbullying often causes serious disturbances in victims such as post-traumatic stress disorder, depression, suicidal thoughts and behaviors, or anxiety.

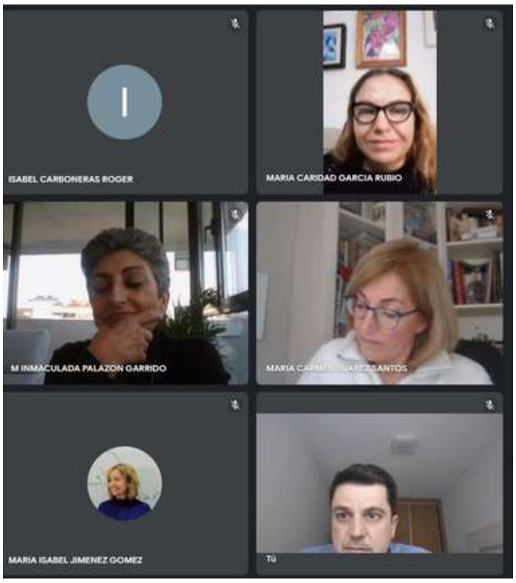
This challenge consists of studying and analyzing what young people know about safety, as well as making them aware of the risks they run in their educational centers and daily life. This challenge seeks, through gamification, the greater awareness of students and teachers in everyday life on issues related to safety in the use of new technologies.

RESULTS

- Game and animation linked to cybersecurity in education
- Involvement of public administration, VET schools, IT experts, teachers, students and project partner
- Creation of short interactive videos



AEII / INERCIA DIGITAL [ES]


ISABEL CARBONERAS ROGER
MARIA CARIDAD GARCIA RUBIO
M INMACULADA PALAZON GARRIDO
MARIA CARMEN SUAREZ SANTOS
MARIA ISABEL JIMENEZ GOMEZ
Tú

Desarrollo – Opción libre

HACKATHON

? WEB vs APP

? Lenguajes

Hosting & arquitectura ?

Entorno de desarrollo (IDE) ?

In general, after conducting numerous surveys, the cybersecurity knowledge of teachers and students in VET centers is still low in Spain. For this reason, this project and other similar ones are very relevant in Spain.

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

GAME JAM

NGO Nest Berlin, Extrafondente Open Source - EOS and IASIS together carried out a GameJam session in February 2022. The GameJam started on Saturday 12th and lasted 6 days overall. It saw the national teams developing and working together on a game draft (of an online or a board game).

An independent jury was gathered and was asked to evaluate the game draft following common guidelines and an evaluation template.

The winning team was awarded a mentorship of 6 months as well as technical resources in order to further develop the game idea.

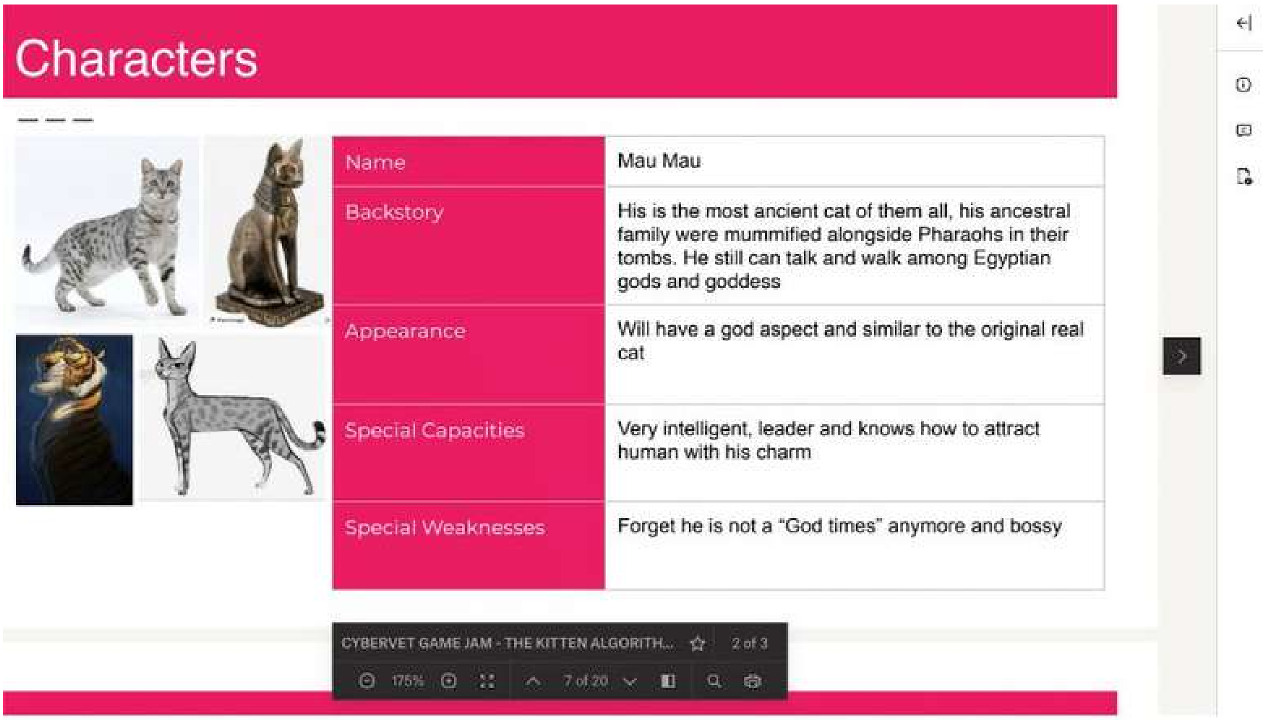
ABOUT THE GAME

It is a 2 to 6 player turn base, strategic board game, that takes about 30 to 60 minutes to play. In this game you trick the humans to convince them that you are the best cat and get more prestige by getting as many human cat's servant you can. Keep your eye open, the other boss cats will actively try to sabotage your way to get to the humans and take the glory for themselves. Don't trust their cute faces!

You lose the game if you don't have a high number of humans as your servants or the 10th round is over and none of the players have at least 4 humans in their command.

The difficulty is that there are 6 Bosses trying to trick humans to be their servant and so the bosses can control them, but everybody has the same objective and some could even be helping the humans to be free from the cat's control.

Mau Mau



Characters

Name	Mau Mau
Backstory	His is the most ancient cat of them all, his ancestral family were mummified alongside Pharaohs in their tombs. He still can talk and walk among Egyptian gods and goddess
Appearance	Will have a god aspect and similar to the original real cat
Special Capacities	Very intelligent, leader and knows how to attract human with his charm
Special Weaknesses	Forget he is not a "God times" anymore and bossy

LECSA (LV)

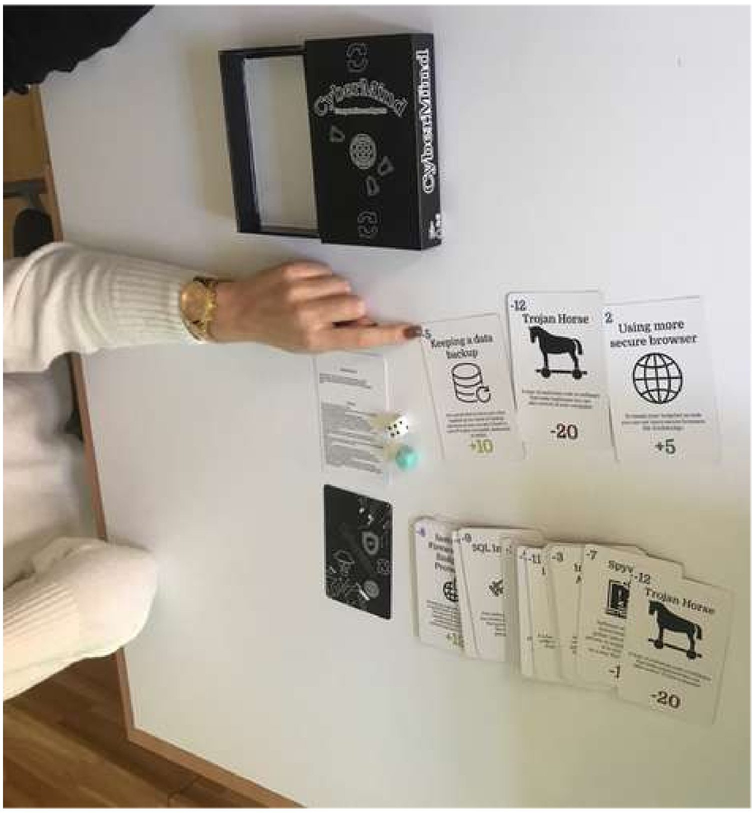
GAME JAM

LECSA partner from Latvia organized a GameJam event from 27 September – 1 October 2021. Due to the epidemiological restrictions and different locations of participants, it was organized as a hybrid type event (on site in Saldus Technical School and via platform Zoom). During the event 6 teams (4-5 persons per team) were formed to work on the development of game's prototypes. To achieve some tangible results, the Game Jam concept foresaw development of two types of games - computer and board games.

ACTIVITIES

- August – September 2021 was devoted to planning and organisation of the event (searching experts in cybersecurity and game development, information distribution to potential participants, planning of the agenda and defining criteria for the game, etc.)
- Multiplier event – Actualities in the Cyberattacks (27.09.2021): Introduction of the CYBER.EU.VET project and lecture on the trends in the cyberattacks with Mr. Armins Palms, cybersecurity expert from CERT.LV (IT Security Incident Response Institution of the Republic of Latvia)
    - Number of participants: 26 persons
    - Place: Saldus Technical School (Saldus city) and ZOOM platform
- Announcement of the Game Jame (27.09.2021): definition and discussion on the actual challenges in cybersecurity (needs assessment); formation of teams, meeting with mentors and discussion about further work (workshop on the game engine Unity), brainstorming on the game's idea and concept.
- Game Jam activities in progress (28.09-30.09.2021): teams worked on the development of prototypes, consultation with mentors' were ensured, if needed.
- Pitching on the progress (30.09.2021): pitching about the game's concepts and work progress to receive mentors' suggestions.
- Grand finale (01.10.2021): four teams have presented their results and mentors provided evaluation. One team, developing a computer game, has dropped out. Conclusion of the event and informal discussion.
    - Number of participants: 30
    - Place: Saldus Technical School and ZOOM platform

LECSA (LV)



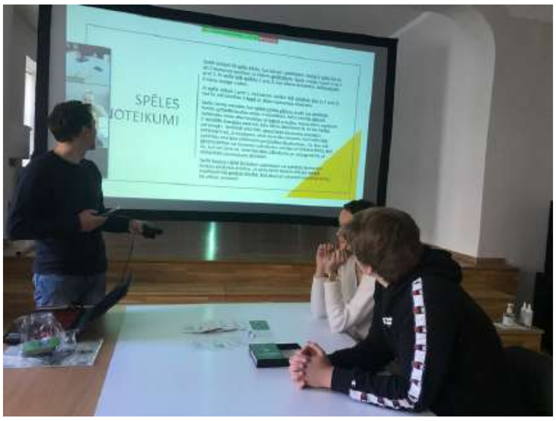
RESULTS

1.Prototype of online game - The Virus

2. Board game - Cards About Security

3. Board game - Cyberwar

4. Competitive Card game - Cyber Mind



EXAMPLE Cyber Mind - A competitive card game

This is an educational card game with quiz elements. The main task of the game is to teach the basics of everyday safety on the Internet and what people expose themselves to by doing foolish things on it. It covers such topics as Internet security and data protection in the context of social network use. In the result of the game people (players) should be able to recognise scam attempts in real life.

Developed by the team Veiksminieki (from Latvian: Successful People), students of the Saldus Technical school during the Game Jam in Latvia (October 2021):
Renars Ricards Hartmanis, Estere Ozoliņa, Sindija Diāna Valtere & others.

Level: basic (for beginners). Target group – pupils, students, teachers and parents

Game contains: 50 cards, 2 health pads (for counting health of players), 2 dices and rule card.

LECSA (LV)

ABOUT

Attempts of the cyberattacks in the world are rising every day, so world's government came up with idea to organise a tournament to identify people around that are bringing cyber risks, and counterattack against them.

Educational game helping to learn about key types of cyberattacks, prevention and elimination methods by protecting yourself or your team and counterattack the opponent. Aim of the game is to take away all the lives of the opponent/s.

HOW TO PLAY GAME/RULES

Number of players: 2 or 4 persons (1 vs 1 or 2 vs 2).

Each player or team (when 2 vs 2) has "100 lives" (Health=HP) at the beginning of the game.

Health counting is done by using black note pads or other available notes.

Assign a separate person which would follow and calculate the consumption of players' energy and health, if possible. Otherwise players do it by themselves.

Each player is dealt 5 cards. If the game is played 2 vs 2 then both players have "one common hand" in the team or 10 cards together.

There are three types of cards: Attack Cards (red), Shield Cards (yellow) and Life or Healing Cards (green).

The game is played in rounds. The player/team that rolls the highest number with dice starts the game.

Each card costs energy. At the beginning of each round, the player rolls 2 dice to define an Energy which is indicated at the top of the card (in blue). Cards need to be played so you don't exceed your rolled energy amount.

The player/team who starts the round can attack (with Attack Cards), protect themselves (Shield Cards) or add life (Healing Cards), while second movers can only use Attack and Shield cards to minimize their life vulnerability.

Keep in mind that the max number of lives per player/team during the game can be 100 HP (e.g., if sum of lives and energy after the round makes 110 HP in total, your number of lives anyway remains – 100 HP).

The game ends as soon as a player/team runs out of all lives (0 lives).

If the game runs out of cards, you need to shuffle cards from the pile again.

LECSA (LV)

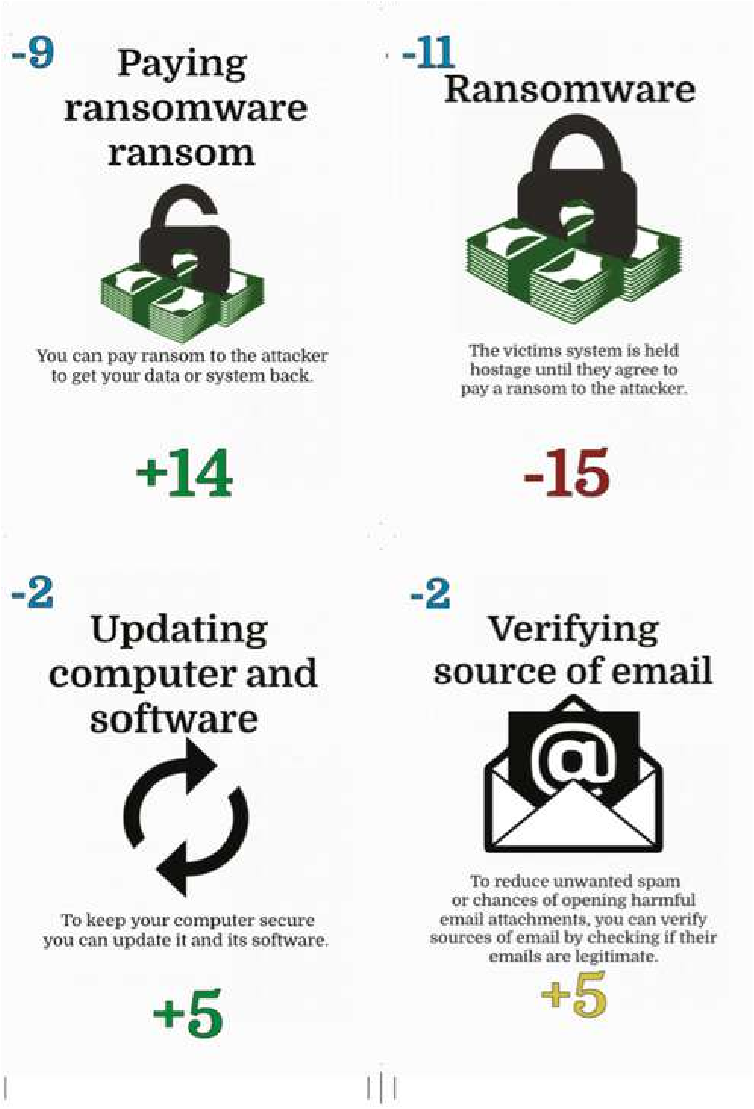
Examples of cards

In **blue** – Energy

In **red** - Attack Cards

In **yellow** - Shield Cards

In **green** - Healing Cards



-9
Paying ransomware ransom

You can pay ransom to the attacker to get your data or system back.

+14

-11
Ransomware

The victims system is held hostage until they agree to pay a ransom to the attacker.

-15

-2
Updating computer and software

To keep your computer secure you can update it and its software.

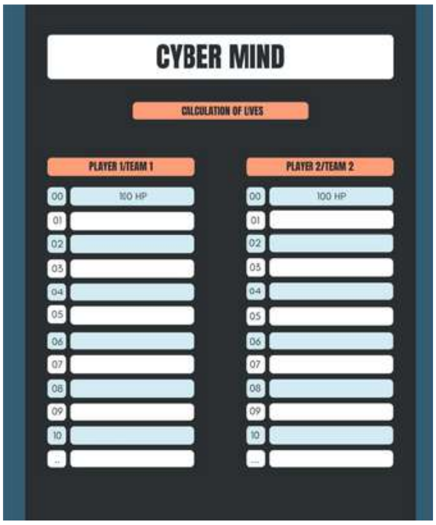
+5

-2
Verifying source of email

To reduce unwanted spam or chances of opening harmful email attachments, you can verify sources of email by checking if their emails are legitimate.

+5

Example for health calculation



CYBER MIND

CALCULATION OF LIVES

PLAYER 1/TEAM 1		PLAYER 2/TEAM 2	
00	100 HP	00	100 HP
01		01	
02		02	
03		03	
04		04	
05		05	
06		06	
07		07	
08		08	
09		09	
10		10	
..		...	

EXAMPLE Cyberwar - Board Game

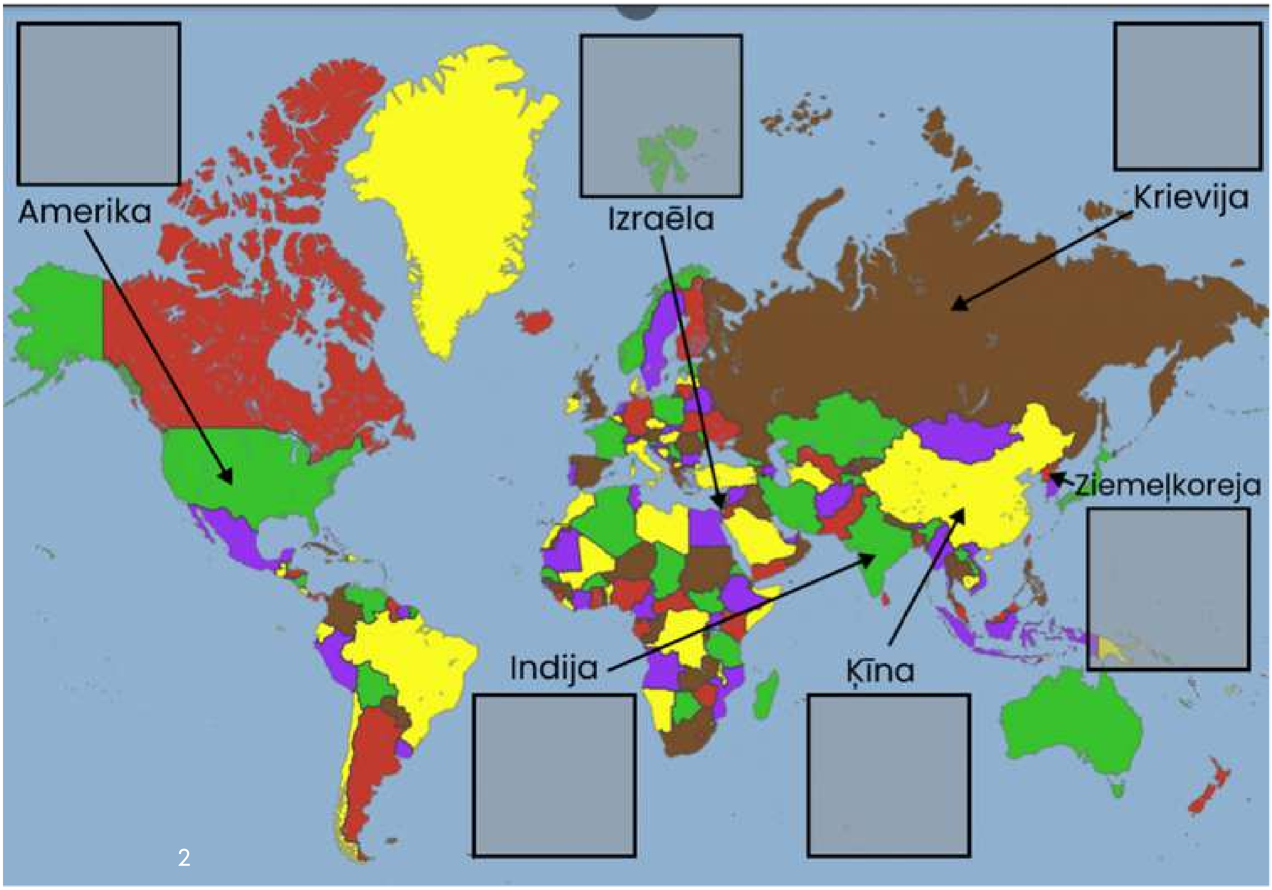
Developed by the team Exodus (students of the Saldus Technical School), leader of the team Valdemārs Šperbergs.

2-6 players < – > Suitable for people age 15+
A board game with a strong emphasis on tactics and randomness (chance).

Level: educational game for those having some understanding on cybersecurity.
Game contains: World map, 2 dices, servers, cards with function "attack", "defence" or "reaction", legend of vulnerabilities, a table with possible moves for each type of vulnerability.

ABOUT

The aim of the game is to protect player's represented country and attack other countries to win the cyberwar. In Cyberwar, each player must choose a country to represent. Each player has one server with 3 vulnerabilities. The goal of the player is to hack other countries' servers by exploiting two out of three vulnerabilities or to fix two out of three vulnerabilities on his own server.



LECSA (LV)

HOW TO PLAY

Players choose the country to be represented and places a server object in designated place in the map. Every country has its own bonuses.

Each player randomly draws (takes) 3 vulnerabilities – one from each difficulty level –, and places them face down in their respective locations on their server fields. The vulnerabilities are not known for the players.

Vulnerabilities have 3 levels of difficulty. Difficulty level also determines how big number is required to exploit a vulnerability (see "Attacks"), as well as determines how many moves it will take to fix the vulnerability (see "Défense").

Game takes place in the rounds, the following actions (moves) can be performed – **Scanning**, **Attack** and **Défense**. Players determine the sequence of players by rolling two dice.

START

- Each player receives 4 cards at the beginning of each round. At the end of the round, it is possible – to keep 2 cards or exchange them for existing ones.
- The 1st round is a Scanning Round where no Attack or Défense cards are allowed. In subsequent rounds, players can choose to Scan or Attack or try to repair their vulnerabilities (see Défense). The game continues round by round until a winning condition is reached.

Scanning

- The attacker chooses a country to scan for its vulnerability (e.g., "I'm scanning a Russian 2nd level of vulnerability").
- Player performs scanning – rolls two dices, applying bonuses of its represented country, compares with difficulty level of vulnerability + bonuses of victim's country.
- If the attacker rolled a number equal to or greater than the victim's level of vulnerability difficulty, the attacker may look at the scanned vulnerability.
- Country bonuses are not added when scanning yourself.

Difficulty levels

1st – player must roll at least number 4 (excluding bonuses of the country)

2nd – player must roll at least 8 (excluding bonuses of the country)

3rd – player must roll at least 11 (excluding bonuses of the country).

ATTACK

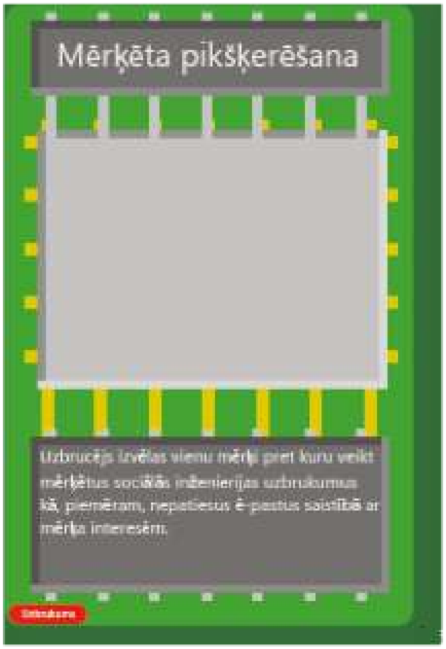
- The player names the target of the attack (e.g., "I attack a Russian 2 level vulnerability") and reveals attack card to all players, placing it next to the vulnerability.
- The player rolls the dice to see if the attack works by comparing the roll to the vulnerability difficulty + bonuses (if the rolled number + bonuses match or exceed the difficulty, the attack succeeds).
- Attacks can be forced back by using the Reaction Card that is designed for that attack.
- Each attack has its own type of reaction that can be played and own type of vulnerability that it works for.
- If the attack fails or is blocked by a Reaction Card – the played Attack and Reaction cards remain on the table until the end of the next round and prevent from attacking by other players with the same attack for the same vulnerability. After the move both cards return to the pile.

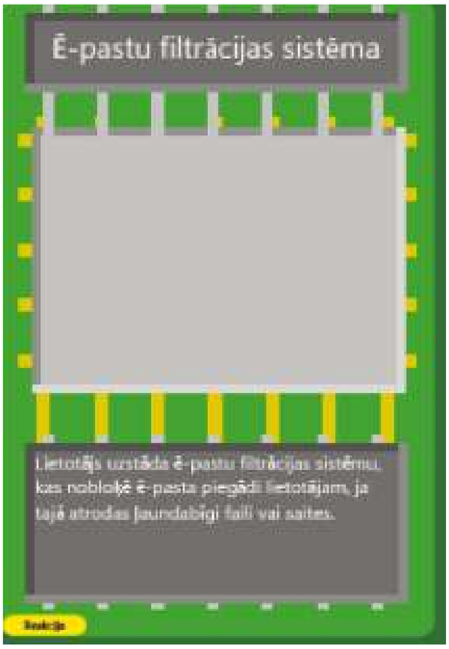
Difficulty levels

1st – player must roll at least number 4 (excluding bonuses of the country)

2nd – player must roll at least 8 (excluding bonuses of the country)

3rd – player must roll at least 11 (excluding bonuses of the country).


Mērķēta pikšķerēšana
Uzbrucējs izvēlas vienu mērķi pret kuru veikt mērķētus sociālās inženierijas uzbrukumus kā, piemēram, nepatiesus ē-pastus saistībā ar mērķa interesēm.
Uzbrukums


Ē-pastu filtrācijas sistēma
Lietotājs uzstāda ē-pastu filtrācijas sistēmu, kas nobloķē ē-pasta piegādi lietotājam, ja tajā atrodas ļaundabīgi faili vai saites.
Reakcija

LECSA (LV)

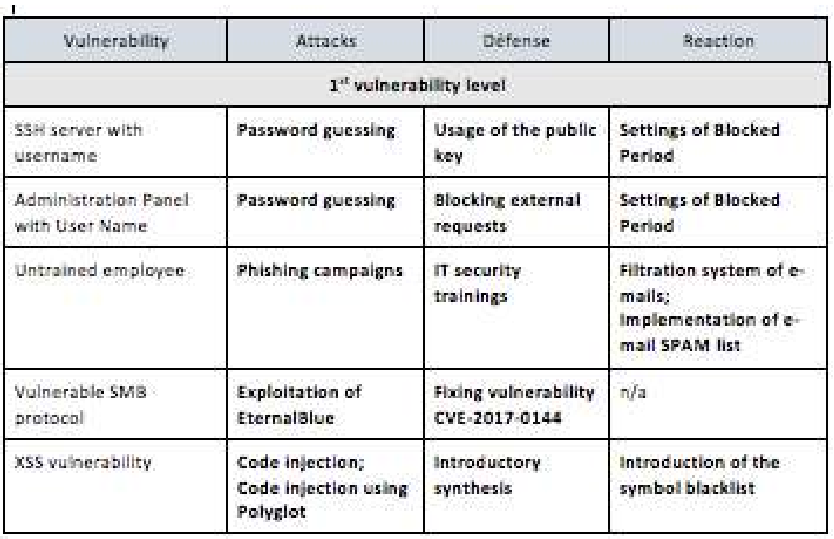
Defense

- Defense – choosing the right method against a particular vulnerability. Reaction Cards stops (cancel) the incoming attack (and all other attacks targeting the same vulnerability) for 1 turn.
- To cancel an incoming attack, the player places a Reaction Card matching the attack type (See table with vulnerabilities) on the attack card as soon as the attack is played.
- To begin repairing of injury, a player places a Défense Card next to the injury to be repaired.
- Other players can attack this injury while it is on Défense (before Défense turn is over).
- When the player tries to repair an injury on his server with a Défense Card, it cannot attack, but may try to prevent attacks with Reaction Cards. For complete repair, it is required |difficulty level + 1| turn. Scanning action is allowed during the repair period.
- If the Défense method is not correct, the player skips 3 turns and cannot use Défense Cards during this period (reactions and scanning actions are allowed).

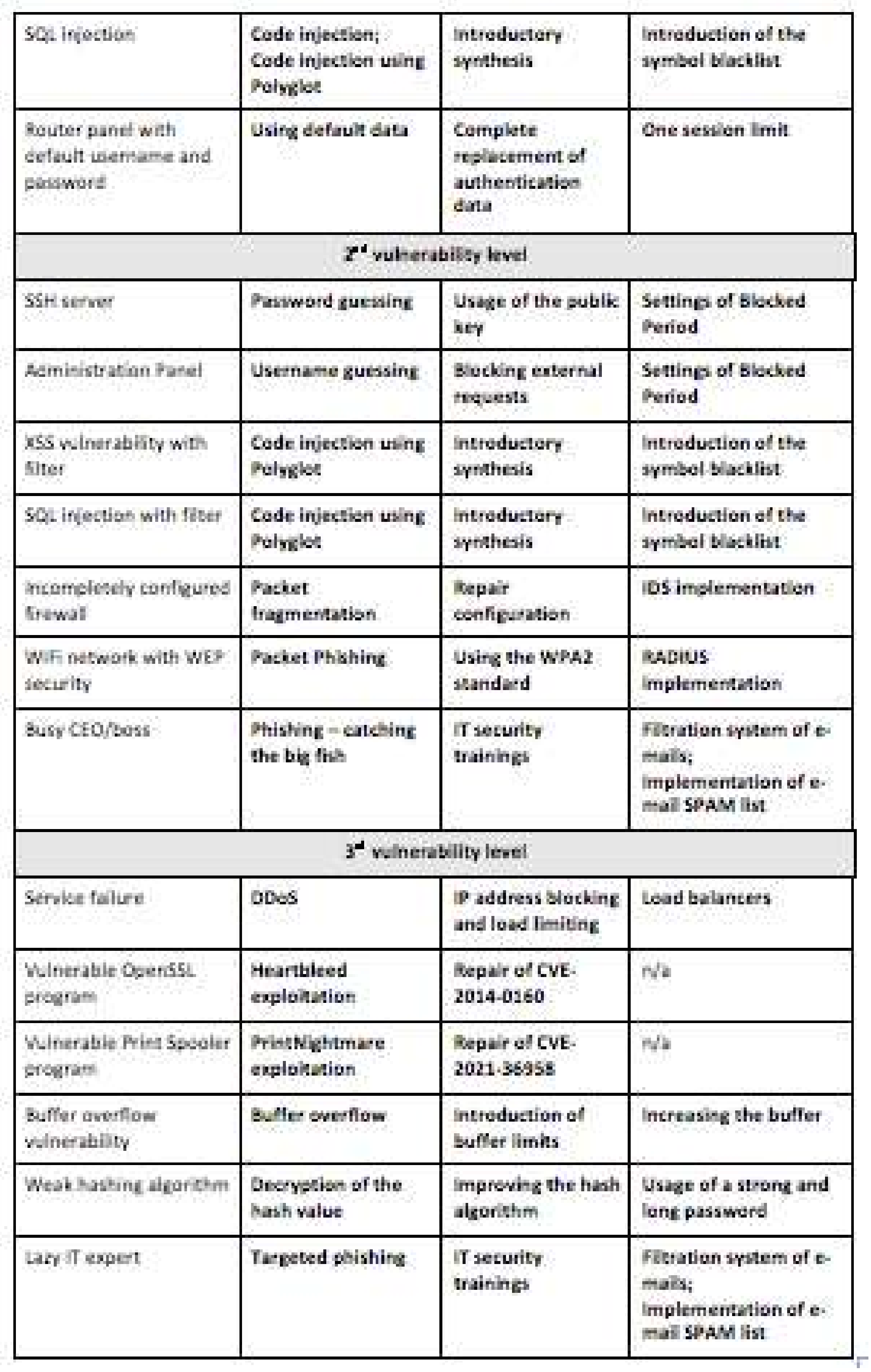
Bonuses of the countries

- USA: +2 in scanning
- Russia: +2 for attacks
- China: +2 for defence against attacks
- North Korea: +2 for defence against scanning
- India: +1 in all attacks, -1 against attacks
- Israel: +3 in all attacks, -3 against attacks

Vulnerabilities by levels

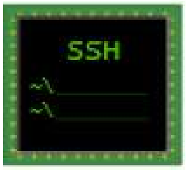


Vulnerability	Attacks	Défense	Reaction
1st vulnerability level			
SSH server with username	Password guessing	Usage of the public key	Settings of Blocked Period
Administration Panel with User Name	Password guessing	Blocking external requests	Settings of Blocked Period
Untrained employee	Phishing campaigns	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



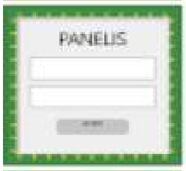
SQL injection	Code injection; Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
Router panel with default username and password	Using default data	Complete replacement of authentication data	One session limit
2nd vulnerability level			
SSH server	Password guessing	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

LECSA (LV)



SSH serveris

SSH serveris ar lietotājvārdu

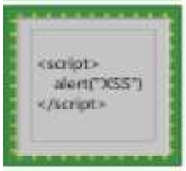


Administrācijas panelis

Administrācijas panelis ar lietotājvārdu

Neapmācīts darbinieks

Ievainojams SMB protokols



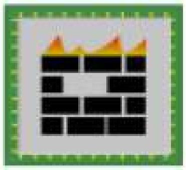
XSS ievainojums

SQL injekcija

Rūtera panelis ar noklusējuma lietotājvārdu un paroli

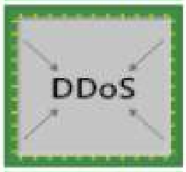
XSS ievainojums ar filtru

SQL injekcija ar filtru



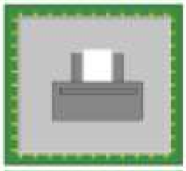
Nepilnīgi nokonfigurēts ugunsmūris

WiFi tīkls ar WEP drošību

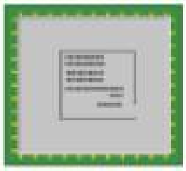


Pakalpojuma atteices kļūda

Ievainojama OpenSSL programma



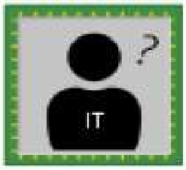
Ievainojama Print Spooler programma



Bufera pārpildes ievainojums

Vājš jaucējvērtības algoritms

Aizņemts priekšnieks

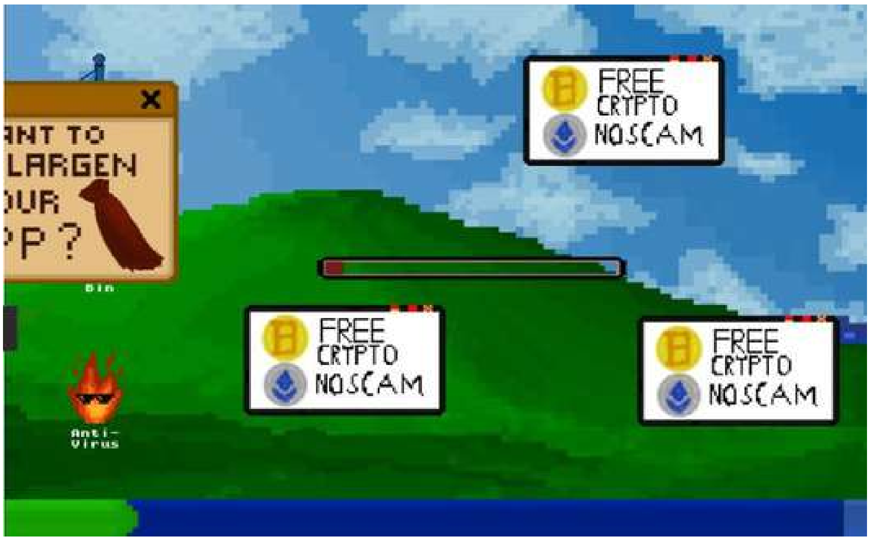


Slinks IT speciālists

LECSA (LV)

GAME JAM

LECSA (LV)



TIPS & EXPERIENCES FROM THE GAMEJAM IN LATVIA

- During the 2-days-event it is not possible to develop a real computer game, but rather the first prototype, which might or not further be developed depending on participants' motivation.
- Prize or other types of benefits can help to involve more participants and ensure better (more tangible) results at the end (in our case – pizza and drinks were provided at the end of the event, further support from mentors, (e.g. placing games in the platform)).
- Mentors on the game development and cybersecurity issues play an important role in the Game Jam by consulting and helping participants.
- Planning in advance – as this is quite a complex event and requires careful planning.
- Organisers have to consider that some teams may fall out of the competition (due to the limited timing).

Please see the FB posts with the results of event:
https://www.facebook.com/cybereuvetproject.eu/posts/138127645211214
https://www.facebook.com/saldustehnikums/posts/1780232175520378

The event was organised by LECSA in cooperation with the Latvijas Universitāte | Ekonomikas un kultūras augstskola / EKA University of Applied Sciences | McĀbols | cert.lv | Coldwild Games | Saldus tehnikums!

MEATH PARTNERSHIP (IE)

ACTIVITIES

- Needs assessment information meeting with students (coding training in a local Adult Education Institution)
- 2-day GameJam (online information session on the 1st day; 2nd day dedicated to Game Jam)
- Multiplier Event – Cybersecurity Awareness Morning

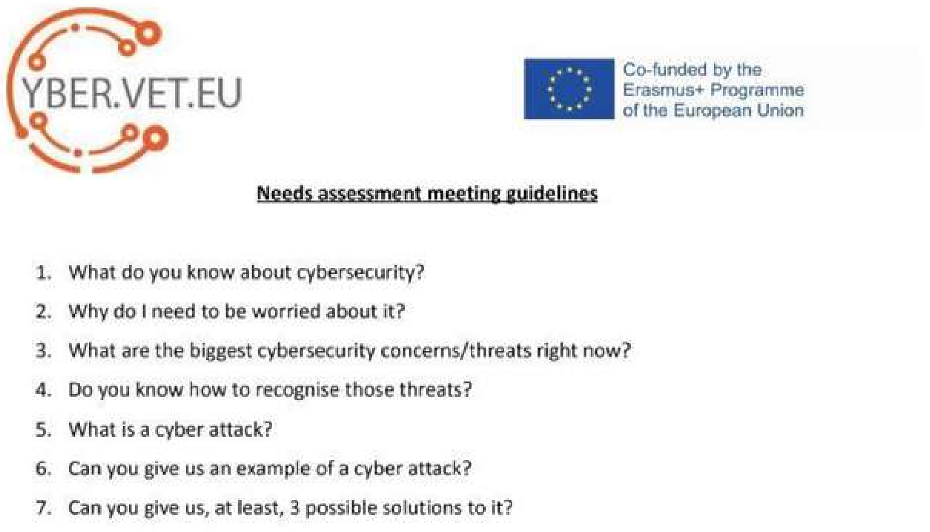
DESCRIPTION & RESULTS

1) Needs assessment information meeting with students
(coding training in a local Adult Education Institution) Date: October 2021

DESCRIPTION

In order to disseminate the project and identify the main topics for the Game Jam, the team of Meath Partnership arranged an information session with the students of a local Coding training class. Sharing information about Cybersecurity and discussion about the most recent threats was followed by a group brainstorming session where students were divided into two groups in order to discuss questions leading to identifying the most interesting topics to be further explored during the Gamejam. Further information about the Gamejam and the CYBER.EU.VET project were also shared with the participants on the day.

EXAMPLE FOR ASSESSMENT



YBER.VET.EU

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

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)

RESULTS

As a result of this activity, the team of Meath Partnership gained a better understanding of the overall knowledge of the students in relation to cybersecurity and cyber threats as well as collected information that was further included in the planning and implementation process of the GameJam.

ASSESSMENT IN ACTION

2) 2-days Gamejam

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

DESCRIPTION

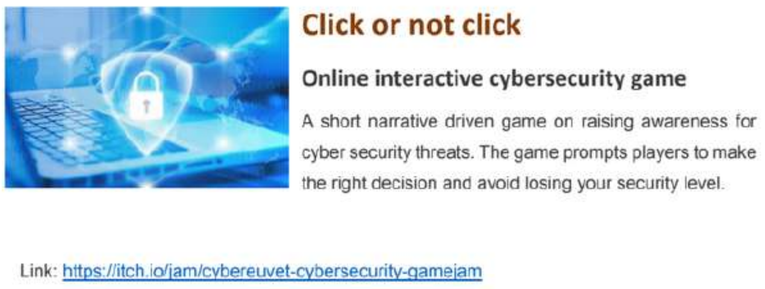
DAY 1 was dedicated to welcoming the participants and presentation of the CYBER.EU.VET project and opening of the Game Jam as well as sharing information about the 2 topics identified during the needs assessment meeting. The participants were offered options to work individually or as part of a team. They also had the opportunity to ask any questions or receive further clarification about proceedings related to the development of the games on day 2.

DAY 2 was dedicated to development of the games and members of our team and an IT support expert were available via Zoom to support the participants throughout the duration of the Game Jam from
9am till 9pm.

The participants were invited to upload their games to the Itchio platform under a profile created for the purpose of this event: CYBER.EU.VET : Cybersecurity Game Jam - itch.io

RESULTS

After participants shared their draft games with the team, one participant decided to go ahead and upload the game for further evaluation. The rest of the participants decided not to submit their drafts as they were in very early stages.



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

CYBERSECURITY GAMEJAM 2021
8TH AND 9TH OCTOBER 2021
JOIN US IN KELLS CO MEATH OR ONLINE
LIMITED PLACES
SIGN UP TODAY
TO FIND OUT MORE OR TO REGISTER YOUR INTEREST
CONTACT IRENA:
IRENA@VOLUNTEERMEATH.IE OR 086 026 5665
YBER.EU.VET
Co-funded by the Erasmus+ Programme of the European Union
meath partnership

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

MEATH PARTNERSHIP (IE)

3) Multiplier Event – Cybersecurity Awareness Morning

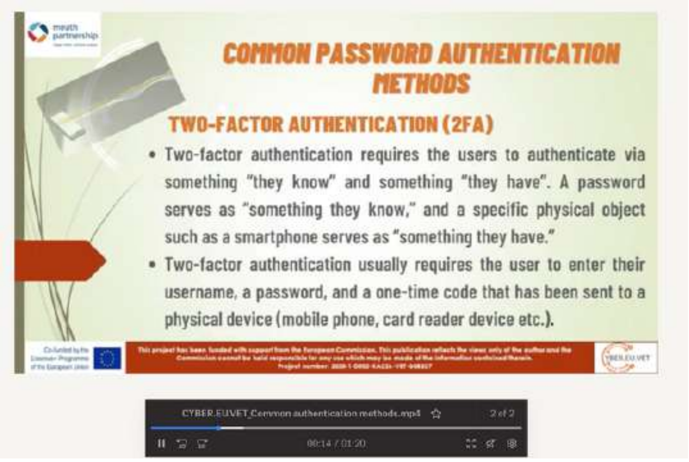
Date: November 2021

DESCRIPTION

The Multiplier Event was held online Via Zoom in order to raise awareness about the project and its activities. The event was widely disseminated among a wide variety of stakeholders interested or involved in Cybersecurity. The event started with a presentation and overview of the project and the Game Jam, followed by a presentation and discussion about Cybersecurity and sharing practical information about how to stay online (the current cyber threats and how to eliminate possible attacks were possible).

RESULTS

The Multiplier Event contributed to raising awareness about the project and also created the opportunity to present the milestones achieved since the beginning of the project to a wider audience. It was also a great opportunity to share practical information and advice related to cybersecurity with the participants attending the event.



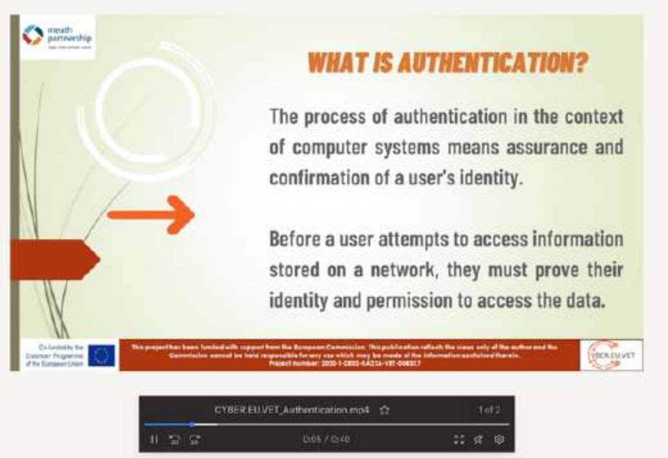
COMMON PASSWORD AUTHENTICATION METHODS

TWO-FACTOR AUTHENTICATION (2FA)

- Two-factor authentication requires the users to authenticate via something "they know" and something "they have". A password serves as "something they know," and a specific physical object such as a smartphone serves as "something they have."
- Two-factor authentication usually requires the user to enter their username, a password, and a one-time code that has been sent to a physical device (mobile phone, card reader device etc.).

This project has been funded with support from the European Commission. This publication reflects the views only of the author and the Commission cannot be held responsible for any use which may be made of the information contained therein. Project number: 2020-1-DE02-KA226-VET-008317

meath partnership
Co-funded by the Erasmus+ Programme of the European Union
YBER.EU.VET
CYBER.EU.VET_Common authentication methods.mp4
2 of 2
00:14 / 01:20



WHAT IS AUTHENTICATION?

The process of authentication in the context of computer systems means assurance and confirmation of a user's identity.

Before a user attempts to access information stored on a network, they must prove their identity and permission to access the data.

This project has been funded with support from the European Commission. This publication reflects the views only of the author and the Commission cannot be held responsible for any use which may be made of the information contained therein. Project number: 2020-1-DE02-KA226-VET-008317

meath partnership
Co-funded by the Erasmus+ Programme of the European Union
YBER.EU.VET
CYBER.EU.VET_Authentication.mp4
1 of 2
0:05 / 0:40

COFAC / UNIVERSIDADE LUSÓFONA (PT)

GAME JAM

ACTIVITIES

1) Cyber & Ethical Hacking post-graduation for future professionals and market teachers
Oct 2021 – Feb 2022 (in partnership with a local consultancy firm named Cybersec)

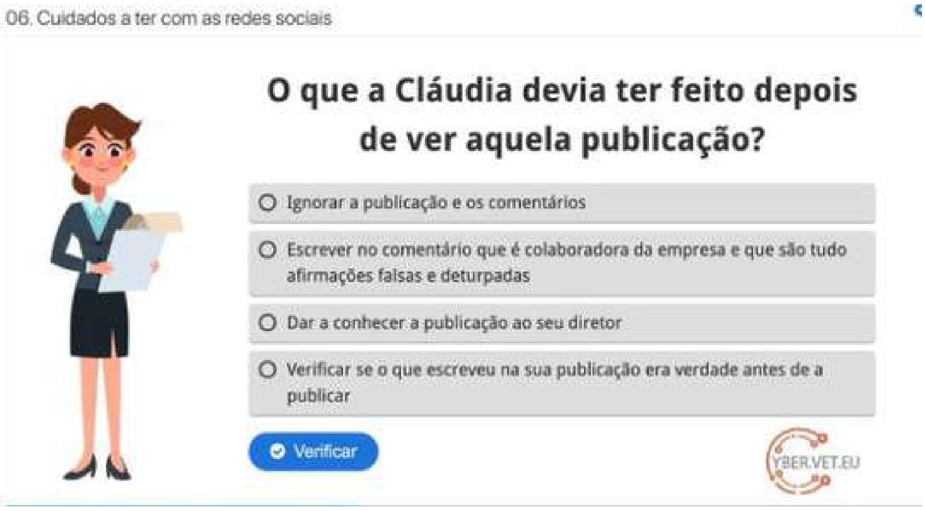
2) 2 GameJam sessions delivered in January 2022 at VET schools:
Escola de Comércio de Lisboa - https://escolacomerciolisboa.pt
Escola Profissional Almirante Reis - https://www.epar.pt

3**)** A three-half-days cybertraining for high school students in march 2022 at
University Lusofona as part of the Tecweb event - https://tecweb.ulusofona.pt

RESULTS

Dissemination report evidence where you can see the different tests that have been carried out during a calendar year (April 2021 to April 2022). In this report we can see screenshots of publications on social networks, posters of different events, questionnaires on cybersecurity awareness (available in portuguese language at https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oeplRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform).

During the Cyberjams, it was also created, based on the cybersecurity awareness surveys a set of mini-user friendly/interactive games about simple situations done.



06. Cuidados a ter com as redes sociais

O que a Cláudia devia ter feito depois de ver aquela publicação?

○ Ignorar a publicação e os comentários

○ Escrever no comentário que é colaboradora da empresa e que são tudo afirmações falsas e deturpadas

○ Dar a conhecer a publicação ao seu diretor

○ Verificar se o que escreveu na sua publicação era verdade antes de a publicar

TANDEM PLUS NETWORK – MEMBER IASIS [GR]

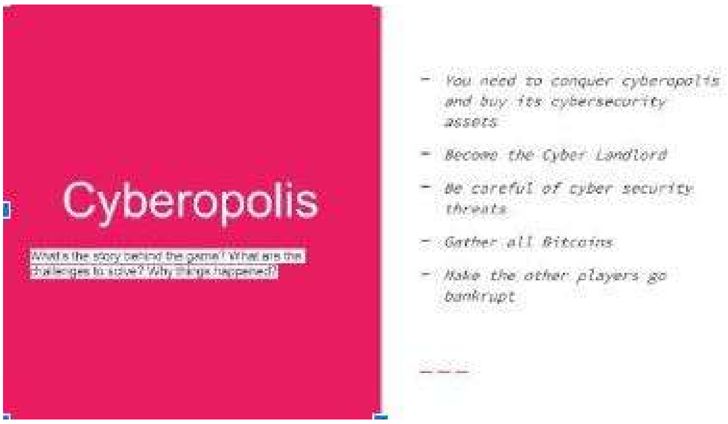
GAME JAM

Game Design Tool (IASIS) - Cyberopolis

This game is a board game aimed at people interested in cybersecurity, with a maximum of 2-4 players, and its main aspects are data confidentiality and data integrity… while the topics it deals with are malware, phishing, web -based attacks, web-application attacks, spam, identity theft, DDoS and Man in the middle…

See the image of ''Cyberopolis'' to better understand the steps to follow during the game and what challenges are to be solved…

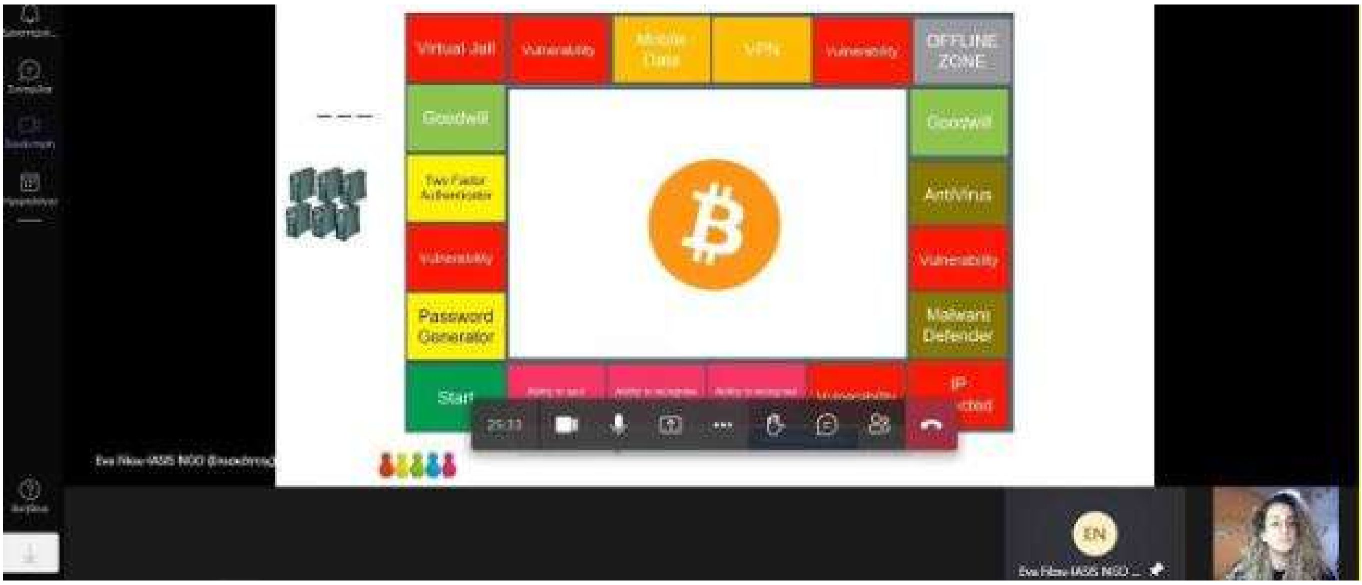
Screenshots of the game during the GameJam session where we can see the success of the game and the great interest shown by the participants.



Cyberopolis

What's the story behind the game? What are the challenges to solve? Why things happened?

- You need to conquer cyberopolis and buy its cybersecurity assets
- Become the Cyber Landlord
- Be careful of cyber security threats
- Gather all Bitcoins
- Make the other players go bankrupt



TANDEM PLUS NETWORK – MEMBER IASIS [GR]

VIDEO - Preventing Cyberbullying

This video developed by the Greek partner brings visitors closer to different ways to prevent and fight cyberbullying.

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.
Berlin, 2022

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