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

IMPROVING CYBERSECURITY READINESS OF THE EUROPEAN VOCATIONAL EDUCATION AND TRAINING SECTOR

CYBER.EU.VET

INTELLECTUAL OUTPUT IO3

TRAINERS TRAINING TOOLKIT

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

Introduction

The partners of CYBER.EU.VET project elaborated this toolkit for trainers' training – consisting of 6 modules + materials – to be used by teachers and trainers in the VET sector. Each module covers a theoretical part, practical examples and tasks for working in groups. The training format is open to be used in different European countries and shall be adapted to local needs and conditions whenever appropriate. Adjustments might relate primarily to the practical examples and case studies provided by the training format.

TRAINING MODULES HAVE BEEN DEVELOPED BY PARTNERS AS FOLLOWS:

CYBER ATTACKS

Module 1

1. Module Overview

Target Group

- VET educators and trainers
- Students
- Representatives or relevant organisations or initiatives (NGO, national and regional authorities, educational institutions)

Module description

Considering the growing number and scale of cyber attacks every year, specifically in the light of the latest economic, political and social events (consequences of Covid-19 restrictions, military conflict in Ukraine, etc.), it is important to discuss actual cyber attacks more frequently.

Therefore, the aim of the lecture is to provide fundamental understanding of cyber attacks and to learn how to react to possible incidents.

The content of this module covers the following aspects (units):

- Definition and relevant issues
- Typology
- The most actual incidents (practical examples)
- How to protect from cyber attacks and how to react on incidents

At the end of each unit, a practical activity is foreseen.

Learning Objectives

- To provide a fundamental understanding of issues related to cyber attacks.
- To understand the consequences and impacts of the potential cyber attacks and threats.
- To recognize and classify the most common forms of cyber attacks.
- To know how to react to the attacks – where to report, if an incident occurs.
- To ensure sources of information and literature for further and more detailed learning, for following actual cyber attacks and for ways of protection.

Overall duration

Max 1,5 hours

CYBER ATTACKS

Module 1

This module will be delivered by the trainer as a PowerPoint presentation sharing theoretical knowledge accompanied by more visual elements, practical examples and exercises (max. 20 minutes + a practical activity per each unit).

It is recommended to prepare the presentations on the PPT templates customised to the CYBER.EU.VET project. Considering the fast-paced developments and progress in the field of cybersecurity, it is recommended to continuously review the units and, if required, adjust the content considering the most recent developments in the field.

In addition, it is recommended that trainers adapt this module to the needs of their local VET and include examples of topical incidents in the region. This module covers mainly practical examples of Latvia as well as some international examples. It is recommended to give a greater focus on Unit 3 to analyse and discuss practical examples of incidents, along with pictures and videos.

Unit 1 - Cyber Attacks

What Does it Mean? Introduction to the Topic

Learning Activity #1 - Theory

DEFINITION AND MEANING

Cyber Attack (pl. cyber attacks) = an attempt to gain illegal, unauthorised access to a computer or computer system for the purpose of causing damage or harm to it. Its aim is to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal data held within these systems.

With the appearance of Covid-19 restrictions and the need to switch to a digital working and learning format, the number of cyber threats and attacks have increased and digital protection has become more important.

The term "cyber attack" closely interrelates with such terms as “cyber threat” (possibility that a particular attack may occur) and “cyber risk”.

The most common cyber attacks: malware attack, phishing attack, man-in-the-middle-attack, password attack, denial of service attack and many more.

Types of attackers' communication: personal contacts, phone, electronic mail, malware.

SOURCE: https://cert.lv/lv/2022/02/kiberuzbrukuma-riskam-paklauts-ikviens-interneta-lietotajs; https://www.investopedia.com/terms/c/cybersecurity.asp

CYBER ATTACKS

Module 1

Who can perform cyberattacks?

A cyber attack can be launched from any place of the world by any individual or group using one or more various attack strategies, and can be targeted to individuals, public or private companies (businesses).

Why do cyber attacks happen and what can it cause?

Attacks in the virtual environment are usually related to identity theft, acquisition of computer resources, information theft and falsification, access to trade secrets, blackmail or defamation. Cyber attacks are designed mainly to achieve financial gain (e.g. stealing credit card numbers and codes), disruption and revenge (e.g. to damage the reputation of an organisation)

For example, crises such as Covid-19 or the military conflict in Ukraine are used to attract the attention of users in fraudulent emails and social media announcements.

STATISTICS

Pandemic-forced remote work has obviously increased cybersecurity risks and facilitated new types of incidents. Most of them are relevant also for education institutions and should be taken into account in further education and training activities for educators and youth.

According to analysed information by Deloitte, 350 cyberattacks took place in April 2020 in Switzerland, compared to a norm of 100 - 150 cyberattacks - (phishing, fraudulent web sites, direct attacks on companies etc.).

The increase in remote working calls for a greater focus on cybersecurity, because of the greater exposure to cyber risk. This is apparent, for example, from the fact that 47% of individuals fall for a phishing scam while working at home.

In Latvia, for example, the highest number of threatened unique IP addresses in Latvia were detected from February to April 2020 when the Covid-19 pandemics began (over 10.000 per month) according to the CERT.LV (the Information Technology Security Incident Response Institution of Latvia), which monthly and annually publishes data and overview of the most relevant incidents called “Kiberlaikapstākļi” (Cyber Weather).

SOURCE: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

INTERACTIVE TOOL: **The live cyber threat map (world)**

Learning Activity #1 - Practical Activity

Discussion with participants on their experience on cyber attacks (10-15 min):

1) What kind of cyber attacks do you know?

2) Have you or relatives/friends ever experienced a cyber attack/cyber incident? How did it end up?

Unit 2 - Types of Cyber Attacks

Learning Activity #2 - Theory

THE MOST COMMON METHODS (TYPES) OF CYBER ATTACKS:

Malware is a malicious software (worms, viruses) which is used to damage the user's devices (computers, phones, etc.) or network. Examples of malware: Spyware and Trojans, Worms, Viruses, Adware, Spam. Depending on the type of malicious code, malware can be used by hackers to steal or secretly copy sensitive data, delete data, block access to files, disrupt system operations or make systems inoperable [DigiCERT]

Malware is mainly spread for two purposes — to obtain information (spying malware forwarding data from the victim's device) or to make a profit (encrypting ransomware that is encrypting data on user's device and later a ransom is requested from user) [CERT Report 2020]

Phishing or Personal Data Scams – a method in which a hacker sends a seemingly legitimate email asking users to disclose confidential information. The recipients are tricked into downloading the malware contained within the email by either opening an attached file or embedded link. Usually these are websites that look like real companies and users have to enter their personal info (bank account, credit card numbers and passwords, including those from authentication services). Data scam can be performed also by phone call or through WhatsApp messages [Investopedia]

Denial of Service (DoS) – hackers bombard an organisation's servers with large volumes of simultaneous data requests until the target cannot respond or crashes, thereby making the servers unable to handle any legitimate requests. As a result, access to the service is not possible for system users. DoS attacks can last from a few hours to many months and can cost companies time and money while their resources and services are unavailable [Investopedia]

Man-in-the-Middle-Attack – attackers secretly insert themselves between two parties, e.g., an individual computer user and a financial institution. Depending on the details of the actual attack, this type of attack may be more specifically classified as a man-in-the-browser attack, monster-in-the-middle attack or machine-in-the-middle attack. In this case, the attacker intercepts, deletes, or modifies data as it is transmitted over a network by a computer, smartphone or any other connected device [Investopedia, TechTarget]

Learning Activity #2 - Practical Activity

Group Discussion - what kind of features indicate about attacking/fraudulent messages? (10 -15 min)

- Participants are provided with 10 min to write down the features
- Discussion of the results

Unit 3 - Example of threats and attacks

How to identify threats?

Learning Activity #3 - Theory

Examples of cyber attacks (in the light of the war in Ukraine)

- Fraudulent e-mails in English calling for support for one of the parties to the military conflict - Ukraine or Russia. Support can be shown by buying votes and voting in this way - it is a fraud aimed at stealing users' payment card data (see print screen)
- VIDEO – How scammers are hijacking Ukraine war charity donations - BBC News
- ARTICLE – 4 Types of Russia-Ukraine War Scams Targeting Consumers

Examples are based on main incidents in Latvia (2020-2021) and other international examples (followed by visual examples) **(PLEASE ADAPT TO LOCAL NEEDS)**

Malware

The Covid-19 situation was used to spread malware attempts: e.g. emails in the name of the World Health Organization (WHO), indicating that the attachment includes the latest information on Covid-19; links to charts showing the spread of Covid-19, the functionality of which was to steal user data; malicious emails to healthcare institutions regarding the delivery of Covid-19 protective equipment, etc.

The spread of the world's most dangerous malware Emotet, both on global and Latvian networks, is intended to steal sensitive information and usually originates from an email of an already infected contact. Emotet serves as a door opener for other computers, allowing unauthorised access to other malware families. More than 200 Latvian companies were infected.

Phishing or Personal Data Scams

The majority of cases were aimed at the scamming of email and Office 365 data, acquisition of bank, international payment system (including Smart-ID - electronic authentication tool in Latvia), access data, and defrauding of access data to accounts on popular social media (Facebook and Instagram). The Covid-19 topic was often used to attract the attention of users in fraudulent emails and social media announcements.

During the pandemic, intensified attempts at data fraud were observed using the brands of parcel delivery service providers (Latvijas Pasts, DHL, Omniva, DPD, AliExpress, etc.) Also, innovative attacks were observed, e.g. an attack on Office 365 access rights that was difficult to detect by technical means since no malicious actions were carried out on the victim's device but attacks were carried out within Office 365.

VIDEO Phishing (with English subtitles)

Fraud

Intensive fraud attempts, including social engineering attacks. Most of the frauds were aimed at obtaining access data for citizens' payment cards, financial resources, as well as email access data. The attackers sent fraudulent emails and text messages to the population, as well as made fraudulent phone calls, most often pretending to be representatives of banks or email service providers. Several companies suffered from business interference (BEC), suffering a total loss of almost € 200,000.

The issue of delivery of goods was also featured in attempted fraud against sellers who posted information about the sale of goods on advertising portals. Pretending to be interested buyers and using the WhatsApp communication platform, fraudsters expressed a desire to buy the product, as if using a courier company's services, and asked sellers to enter card details on the counterfeit Omniva, DPD and later Latvijas Pasts websites to reveal both the CVV code and the balance.

Attackers used customised website addresses (domains) that were similar to the original website addresses to mislead the public.

Attackers also tried to obtain payment card information by sending emails asking them to apply for a Bitcoin balance by signing up for a fraudulent cryptocurrency exchange service.

The most active attempts were extortion campaigns, where hackers claimed to have hacked a user's device and obtained compromising material for which a ransom was set; fraudulent lotteries on behalf of the known brands, offering to win the newest smartphones or other valuable prizes.

OTHER EXAMPLES

Misleading advertisements on social media – using the names of famous Latvian people without their knowledge, internet users were invited to invest in cryptocurrency. Scammers also made phone calls and tried to persuade people to invest. In certain cases, repeated fraudulent attempts were observed where the victims of financial fraud were offered help to get their lost resources back.

Phone scams – by falsifying the phone numbers of different credit institutions and pretending to be bank representatives, scammers, using the public's poor knowledge on additional authentication methods, defrauded financial resources from several thousands of users, causing total losses worth hundreds of thousands of euros to Latvian credit institutions.

Hackers are also adapting to the spread of remote work: considering the need of companies to rapidly switch to a remote work condition and the implementation of electronic documents' circulation, hackers make use of this situation to adapt their attacks - e.g. a number of company accountants received emails in the name of the director or another employee to make an urgent payment or change the payroll account.

Latvia and Lithuania detain 108 over multi-million euro call centre scam

Interference in business correspondence of companies – by compromising the emails of companies or their collaboration partners, attackers pick a suitable moment to send one of the parties a bill with a changed account.

Scam messages – attackers try to intercept WhatsApp's accounts by asking for a six-digit code to be sent to the recipient's phone number by mistake. As a message will be received from the people on your contact list, some people transfer their codes, losing access to their WhatsApp account. The use of two-factor authentication would be a means of protection against such an attack.

EXAMPLE When user shares digits code to hacker
EXAMPLE SMS from local bank with fraud link (Latvian example)

Scam emails – fraudsters pretend to be a national post office (Latvijas Pasts) and ask people to pay for delivery for an allegedly delayed shipment. The link provided in the email leads to a fake website for fraudulent payment card data (see Latvian example).

Fake online stores – specifically high activity have been observed during the holiday season by means of social media advertisements and due to the Covid-19 restrictions which forced companies to sell their products online.
EXAMPLES Scammers lure AliExpress users to fake online stores (picture and scam case); How to Recognize a Scam

Romance scam - scammers take advantage of people looking for romantic partners, often via dating websites, apps or social media by pretending to be prospective companions. They play on emotional triggers to get you to provide money, gifts or personal details.
EXAMPLE Investigation story on Romance Scammer [by North Lab]

Denial-of-Service Attacks (DoS and DDoS)
DDoS attacks against public and municipal institutions were registered (e.g., National Library, Cultural Information Systems Centre, etc.) Prolonged DDoS attacks disrupted a school. Similar reports were received from other educational institutions at the beginning of the school year. Educational institutions elsewhere in Europe are also facing such challenges.

Both in Europe and in Latvia, the following incidents became topical – money extortion attempts primarily aimed at financial institutions or private sector companies (attackers performed a series of trial attacks, threatening to suspend the operation of company websites or other resources by means of attacks of up to 2 Tb/s).

OTHER TRENDS

Compromised Devices and Data Leaks

Equipment compromises can affect individuals, companies, as well as state and municipal institutions. This can happen through already compromised email, or the infection of a device through opening attachments or links from seemingly familiar contacts, such as colleagues and business partners; it can also happen through compromised websites, e.g. via an outdated plugin or outdated content management system.

As was the case in 2020-2021, when several national institutions temporarily lost access to their social network accounts as attackers took control of one of the account administrators' profiles. Reports were filed of Zoom & MS Teams meeting break-ins, a result of poor knowledge on available safeguards (i.e., waiting room, limited access from abroad, etc.).

Intrusion Attempts (any attack that aims to compromise the security goals of an organization) - after the rise of remote work activity of bots searching for vulnerable, inadequately configured devices and/or weak passwords for devices connected to a network (hastily employer-issued devices, personal laptops that started to be used for work, as well as poorly protected RDP services with weak passwords) has increased significantly.

VIDEO Intrusion Examples

More at the Intrusion Detection

SOURCE CERT.LV and “Kiberlaikapstākļi” (Cyber Weather); Investopedia

Additional elements

NOTE Consider also discussions on other methods on fake and fraudulent information, such as deepfake and others.

Learning Activity #3 - Practical Activity

At the end of the unit a Kahoot test is organised where participants have to detect whether the provided information is fraudulent and need to identify the type (method) of cyber threat: https://create.kahoot.it/details/421c14d4-9c70-47cb-94d5-e6c0174ef3a3

Unit 4 - What to Do in Case of an Incident?

Prevention and How to Prepare.

Learning Activity #4 - Theory

SOME TIPS AND TRICKS FOR PROTECTION

- Always check your emails carefully and look out for: attachments or embedded links from unknown/suspicious sources or senders; messages with a sense of urgency asking you to download something or perform some other task; offers with a promise of reward that sounds too good to be true.

VIDEO Clicker (Spaidonis) with subtitle in English

- Pay attention into spelling of the URL address. Phishing sites often use web addresses that look similar to an official site, but contain a simple misspelling, like replacing a "1" for an "l". Incorrect or strange spelling is an indication signal of possible scam.
- Use strong and different password among your devices, email accounts and social media accounts. For more tips, see CYBER.EU.VET module on passwords (Module 4).

- Whereever possible, adjust your settings to use multifactor authentication on your devices. For instance, password and face ID or fingerprint on your phone; Gmail, meanwhile, has one such setting, whereby when a user signs in from a new device, after entering their username and password, they receive a request to confirm their identification from another device, usually a phone.

  two-step verification in WhatsApp (for Android users).
- Do not perform sensitive transactions within the unsecured public Wi-Fi at the coffee shops and other similar public places.
- Ensure that at least most important data on your device have a backup copy (in cloud storage or an external device). Make sure that you can restore the necessary data from backups, and find out how long it takes.
- Software updates – it is crucial to follow software updates and install them immediately. Even a single day's delay can be critical.
- Use a VPN. Virtual private networks add a further layer of protection to internet use from home. They cannot solely be relied upon to prevent cyberattacks, but they can be a useful barrier against cyberattack.
- Regularly follow the news in the world of attacks and try to think that global, national, and local events, both political and economic, but also those related to global suffering (pandemics, military conflicts) can be used as a topic/"cover" for potential cyber attacks.
- Additional (in Latvian): CERT.LV Recommendations in the light of the geopolitical situation worsening and an increase of cyber threats in Europe: https://cert.lv/lv/2022/02/cert-lv-ieteikumi-saasinoties-geopolitiskajai-situacijai-eiropa-un-pieaugot-kiberdraudiem

Where to report about a cyber threat or incidents

- Your workplace, educational institution – send screenshots, pictures or video to relevant person at your institution (e.g. IT department). Warn your colleagues and friends.
- Institutions supporting the national cyber space (case of Latvia):

1. CERT.LV (support in solving incidents, monitoring of cyberspace, warnings), Instruction how to forward fraudulent e-mails (in Latvian)
2. State police
3. Latvian Safer Internet Centre (violations and illegal content on the Internet, child safety on the Internet), and others

INFORMATION SOURCES AND ACTUALITIES

To follow the news on cyber security and cyber threats, regularly **read local or international resources:**

https://portswigger.net/daily-swig/cyber-attacks

https://www.euronews.com/tag/cyber-attack

OUCH! Newsletters - the world's leading, free security awareness newsletter designed for everyone.

Links for Latvia (some info is also available in English) **(PLEASE ADAPT TO LOCAL NEEDS)**

https://www.esidross.lv/

https://cert.lv/lv/ (including, "Cyber Weather "(Kiberlaikapstākļi), instruction how to forward fraudulent e-mails (in Latvian)

https://drossinternets.lv/

Learning Activity #4 - Practical Activity

Discussion with participants: evaluation of the usefulness of the module (5-10 min activity)

2. Learning Outcomes for the Module

Knowledge

- Learners will have a basic understanding on the main issues of cyber attacks.
- Learners will have an overview on the actual incidents (in light of global events).
- Learners will know which information sources to follow for warnings and topicalities of threats.

Skills

Learners will be able to identify and classify common types of cyber threats and to explain them.

Competences

- Learners will be able to recognize a potential cyber threat and know where to report the threat.
- Learners will be able to select basic tools and techniques to protect themselves from cyber attacks.

3. Bibliography

CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcija): https://cert.lv/lv

Covid-19 phishing examples: https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp

Digicert, What are Malware, Viruses, Spyware, and Cookies? https://www.websecurity.digicert.com/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them

Fichtner, E. (2022), Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks: https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks

Information Technologies Security Incident Response Institutions (2021), CERT.LV Annual Report 2020: https://cert.lv/uploads/parskati/CERTLV-annual-report-2020_ENG.pdf

Informative report, Cybersecurity Strategy of Latvia 2019-2022 (in Latvian only): https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf

Latvian Safer Internet Centre (Project-platform "Drossinternets.lv"): https://drossinternets.lv

LIKTA (Latvian Information and Communication Technologies Association): https://likta.lv/digitalas-parmainas-izglitiba/

Li, Y., Liu, Q (2021), A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Science Direct, Vol. 7, p. 8176-8186: https://www.sciencedirect.com/science/article/pii/S2352484721007289

Merriam-webster dictionary, cyberattack: https://www.merriam-webster.com/dictionary/cyberattack

Prat, M.K. (2021), Cyber-attack – definition: https://www.techtarget.com/searchsecurity/definition/cyber-attack

Simplilearn, Cyber Security Full Course 2022: https://youtu.be/yr1Psapupsc

CERT.LV (2022), IT drošības seminārs "Esi drošs" martā (in Latvian): https://cert.lv/lv/2022/02/it-drosibas-seminars-esi-dross-marta#Sanita_Vitola

Esi Drošs (2022), Kiberuzbrukuma riskam pakļauts ikviens interneta lietotājs (in Latvian): https://www.esidross.lv/2022/02/10/kiberuzbrukuma-riskam-paklauts-ikviens-interneta-lietotajs/

1. Module Overview

Target Group

- VET Educators
- Students
- Representatives of public institutions active in the educational sectors: municipalities, regional and national authorities

Module description

Nowaday, people spend a lot of their time in front of a screen. Young people are growing up in a world where new technologies are needed and the main means of communication they use is the Internet. Being on social media for example, offers many advantages, but also many risks.. There are a lot of people who have been bullied or they are being bullied. In most of the cases, they were not aware of this or the problems that it can cause in their lives. For this reason, we would like to use this module, to understand what cyberbullying is and how we can prevent it.

Learning Objectives

- Understanding of Cyberbullying
- Knowing how to detect it
- Effects of Cyberbullying
- Understand the main consequences
- Deliver techniques for preventing it and dealing with it

Overall duration

2 hours

Unit 1 - How to detect cyberbullying

What are the effects?

This Unit will be delivered by the trainer as a PowerPoint presentation whose aim is to share theoretical knowledge accompanied by more visual elements - short videos and real cases of cyberbullying summarising the information from the PowerPoint slides (max. 30 minutes).
It is recommended to prepare the presentations on the PPT templates customised for the CYBER.EU.VET project.

Learning Activity 1

Trainer presents learners a presentation with the following suggested content (max. 30 minutes):
Cyberbullying, while often associated with cyberstalking, is a very serious issue on its own and one that has been increasing in prevalence over the past few years.

How to detect cyberbullying?

Cyberbullying can be **difficult to recognize** because it takes place behind closed doors or in a private phone/computer.

Here are some of the most common signs, that someone may be a victim of cyberbullying:

- Gets unusually upset if she/he cannot use the computer or phone or after using the computer.
- Quickly switches screens or closes programs when someone walks by.
- Avoids discussions about what they are doing on the computer.
- Withdrawal from family or friends.
- Reluctance to participate in activities that they previously enjoyed.
- Unexplained decline in academic performance.
- Refuses to go to school.
- Increasingly reports symptoms of illness.
- Shows signs of depression or sadness.

The effects of cyberbullying can be devastating for the victims. They may experience various negative emotions, such as sadness, anger, frustration, and humiliation. They may also feel isolated and alone, as if they have no one to turn to.

The victims may also suffer academically, as they may be too embarrassed to go to school or participate in class. In some cases, the victims may even consider suicide.

Cyberbullying can also have adverse effects on those who witness it happening to someone else. They may feel scared, helpless, and sad. They may also have trouble sleeping and eating and may even develop anxiety and depression.

Effects and consequences of cyberbullying:

When bullying happens online it can feel as if you're being attacked everywhere, even inside your own home. It can seem like there's no escape. The effects can last a long time and affect a person in many ways:

- **Mentally:** feeling upset, embarrassed, stupid, even afraid or angry
- **Emotionally:** feeling ashamed or losing interest in the things you love
- **Physically:** feeling tired (from loss of sleep), or experiencing symptoms like stomachaches and headaches

The feeling of being laughed at or harassed by others, can prevent people from speaking up or trying to deal with the problem. In extreme cases, cyberbullying can even lead to people taking their own lives.

VIDEO Words Hurt | Cyberbully Short Film

Effects:

- Illness
- Depression
- Isolation
- Anger
- Humiliation

Learning Activity 2

Group Discussion – Q&A; Assessment and Feedback (max. 10 minutes)
Now that you know the most common signs of someone that is being cyberbullied,

- Do you know someone in this situation?
- Could you help them?

Unit 2 - How to Prevent/Stop Cyberbullying

Learning Activity 1

Trainer presents learners a presentation with the following suggested content (max. 30 minutes):

Cyberbullying is facilitated by easy access to digital media platforms and devices. Often, these are used without any oversight. This makes cyberbullying an incredibly difficult problem to tackle. Preventing the practice would require a great amount of time and resources to effectively monitor every online interaction. While it is often not feasible for people to completely rid themselves of digital tools, there are methods that parents, students, and educators can employ to combat the phenomenon and reduce its harmful effects.

For parents, an effective way to address the harm resulting from cyberbullying is simply by talking through the issue with their children.
It is also important to discuss online safety, privacy, and password management. Set guidelines on how students are to conduct themselves online and instruct youngster to be open with their parents about any harm they have experienced from bullying online or in the real world.
Young people can help prevent being a victim of cyberbullying by being cautious about what they post. They should avoid sharing their passwords and ensure their online privacy settings are keeping them safe.
Students play an important role in the prevention of cyberbullying. If young people who know the cyberbullying facts notice it happening to someone else, they can notify a trustworthy adult. They should also be kind, generous, and supportive to the child who is being bullied. Teachers, educators, and other trusted adults must join with parents and youngsters to combat cyberbullying. Often these individuals can spot changes in a child's behaviour and can help address the issue before parents can.

Technology and the internet are not the issue. It's the people who use it to harm others who are the real problem. For that, it's important to teach teenagers how to use social media safely and responsibly and to become aware of how to act, should they experience cyberbullying.

What to do if you are being cyberbullied?

- Do NOT ANSWER or comment on the cyberbully message.
- BLOCK the people involved.
- LOG OFF the site where the bullying is happening.
- Safeguard your PASSWORDS and check your PRIVACY CONTROLS.
- SAVE everything. Screenshot or print the incident as evidence.
- REPORT cyberbullying: almost every technology site has an option to report someone for cyberbullying.
- Tell a trusted ADULT what is going on or contact LAW enforcement.

What should you do if you see cyberbullying happening?

- Tell your parents or a trusted adult and ask for their advice.
- Report the situation to the technology, app, or social media provider.
- If the situation involves classmates, inform your teachers.
- Show your support for the person who is being bullied, for example by addressing a kind message to them.

Taking legal action: Both slander and libel are crimes that can result in a trial.

Ask for help:

- It is very difficult to deal with cyberbullying on your own.

VIDEO Emma's Story: Cyberbullied by a Best Friend

How can I educate myself?

- Organizations that can help: There are many organizations out there sharing information around cyberbullying. The websites below are creating and sharing useful content that is truly helpful to anyone anxious about or experiencing cyberbullying.
- Blogs and podcasts: keeping up with blogs and podcasts that focus on the topic is a great way to stay up-to-date and get the latest advice or perspective.
- Books.
- Apps and software: There are numerous products out there that allow parents to restrict and/or monitor their children's online activity. It is up to each parent to decide whether this kind of monitoring is appropriate based on their child's age and internet habits. Some even scan for language that might be bullying. There are also companies partnering with schools to allow for anonymous reporting of bullying incidents.

Learning Activity 2

Group Discussion – Q&A; Assessment and Feedback (max. 15 minutes)

Writing exercise:
Describe a situation where you know there is cyberbullying going on.
This may be real or fictional.
Can you help? How? Why or why not? Explain how this makes you feel.

2. Learning Outcomes for the Module

Knowledge

- The learner will know how to detect cyberbullying and how the victim feel and experience this.
- Understanding cyberbullying facts and being aware of methods to address it, youngsters, adults, and educators can help create a better, more empathetic digital world.

Skills

- The learner will understand how to recognize when someone is being cyberbullied.
- The learner will be able to understand what level of response and support is needed depending on the scenario at hand.

Competences

- The learner will be able to recognize an episode of cyberbullying and address it immediately using the proper tools.
- The learner will be able to identify what the best method of support is, and which is most suitable to the case at hand.

3. Bibliography

https://socialmediavictims.org/cyberbullying/effects/
https://americanspcc.org/impact-of-cyberbullying/
https://www.unicef.org/end-violence/how-to-stop-cyberbullying
https://www.security.org/resources/cyberbullying-resources-books-podcasts/

1. Module Overview

Target Group

- VET Educators
- Representatives of public institutions active in the educational sectors: municipalities, regional and national authorities

Module description

This is a follow-up module of "Cyberbullying. What is it? How can we detect it?" and provides the target groups with the competences for spreading awareness of cyberbullying and for providing prevention techniques so as not to become a victim of cyberbullying.

Learning Objectives

- Understand the importance of prevention
- Spread awareness on cyberbullying
- Raise awareness on cyberbullying prevention techniques

Overall duration

1,5 hours

Unit 1 - Why prevent Cyberbullying?

This Unit will be provided by the educator as a PowerPoint presentation that will include both theoretical material and more visual features such as short movies and real-life cyberbullying scenarios that will summarize the information from the PowerPoint slides (20 to 30 minutes respectively on each Unit).
We recommend preparing presentations on the PPT templates customised to the CYBER.EU.VET project. The presentation is followed by a group discussion, for everyone to reflect on the learning.

Learning Activity 1

Trainer presents students a presentation with the following suggested content (max. 20 minutes):

To prevent or to intervene?

According to research, persons who are cyberbullied have a variety of negative outcomes, including emotional, physical, mental, and academic difficulties. Furthermore, cyberbullying is a significant source of stress for young people. Victims are psychologically wounded, ashamed, and sometimes afraid as a result of cyberbullying. They not only blame themselves for the harassment and abuse they get, but they are also left feeling tremendously anxious. In fact, over 35% of individuals targeted by cyberbullies exhibited stress symptoms, according to one research. This kind of bullying can be particularly harmful as it is often very public. Usually, many people can see what is written or posted. It is difficult, if not impossible, to delete all traces of something once it has been published online. This means that the bullying can be ongoing.

When people are harassed by others on social media, via text messages, instant chatting, and blog postings on a frequent basis, they may begin to feel hopeless. They may feel that suicide is the only way to stop their suffering. Because the dangers of cyberbullying are so serious, it is critical for VET Educators to teach their students about this issue before it causes real harm. Getting preventive reduces the risks of being exposed to cyberbullying.

Learning Activity 2

Group Discussion (max. 10 minutes)

Ask your students:

- Why is prevention so important in cyberbullying?
- Have you ever been informed about cyberbullying?
- How do you usually get informed about cyberbullying offences?

Unit 2 - Spreading awareness

Learning Activity 1

Trainer delivers a presentation to students with the following suggested content (max. 30 minutes):

It is crucial to discuss with students how to use social media securely and responsibly, by detecting cyberbullying offenders and learning what to do if they are bullied online.

VIDEO Cyberbullying - How to Avoid Cyber Abuse

THINK BEFORE POSTING

Students should make it a habit to read through their work before posting it. They can type the post in the notes section of their computer or smartphone and then revisit it a few hours later to decide whether or not to publish it. Because cyberbullies could use what you post against you in some way, you'll be less inclined to say anything you'll later regret or that could be used against you. Sure, if someone wants to use something against you, they'll strive to get even the most insignificant information, but checking before sharing can reduce the severity of the cyber-attack. Thinking before you publish might help you maintain a healthy relationship with social media.

BE MINDFUL WITH PUBLIC DEVICES

Students should also be careful when using public devices such as university or library computes as there are many ways someone could take advantage of this.

There are many possibilities for public devices to be infected with malicious programs, such as keystroke loggers (keyloggers).

A keylogger, according to most sources, is a software application that discreetly monitors and logs all keystrokes. They can be used to intercept passwords and other personal information input via the keyboard, posing a major threat to users, such as handing over access to your social media accounts to cyber criminals. The most important thing to be aware of when it comes to keyloggers is that they often cannot be detected by anti-virus programs, since there are many legitimate keyloggers available on the market for purposes of parental control, company security, etc.

VIDEO Could a Keylogger Be Spying on You?

Apart from specialised monitoring programs, students should also be reminded to log out from their accounts as they might unintentionally leave them open and available to the ones who will use the computers next to him.

ONLINE PROTECTION

It is critical to use strong passwords everywhere when it comes to combating cyberbullying and other fraudulent activities. A strong password is the one that cannot be easily guessed or compromised. A strong password should be long, contain a combination of numbers, special character(s) and lower/uppercase letters and should under no circumstances include obvious information like name, date of birth, etc.

By safeguarding your accounts, you ensure no one has access to them.

CYBERBULLYING SHOULD BE REPORTED.

Make sure your students understand the importance of reporting cyberbullying. This involves not just detecting cyberbullies, but also informing the social media platform, internet service provider, and any other relevant parties. To put an end to the harassment, they might even need to inform local authorities.

After they have filed all the necessary paperwork, students must take the actions required for blocking the individual or account responsible for the cyberbullying. They should also be aware that even after blocking the offender, they might create alternatives accounts to approach the victim. The good news regarding online bullying that occurs online is that it can typically be recorded, preserved, and presented to someone who can assist. Victims should keep that proof in case things get out of hand.

VIDEO: IGNORE OR REPORT A CYBER BULLY

Learning Activity 2

Present to the students the case study below

YouProMe Erasmus+ project – www.youpromeproject.eu

Jessica is 18 years old. She lives with her two parents, both of whom are professionalsand always busy working. Jessica is the oldest of three children. There is nobody in the family with any known health problems. She studies at school and is a hard-working student. She is passionate about animals and likes to go out with her friends. She has a boyfriend. Jessica has a mobile phone and is a regular user of social networks.

Jessica reported: "I sent my boyfriend some pics a few weeks ago. I thought he was my boyfriend anyway, but then he showed them to his friend and his friend sent them to everyone. The school found out and now the police have spoken to him and his friend. I haven't gone back to school since, but everyone now calls me a slut on social media. I can't stand it when they stare at me, and I already know what they're thinking. Even the girls have a similar opinion about me. The stupid thing is, everyone does it, everyone sends pics, but I was just unlucky to have a boyfriend who betrayed me. I will never trust anyone again. I feel likeeverything is over and there's no going back now."

As a consequence, Jessica has been absent from school for a month and refuses to return. She dropped out of all her school sport activities. Her mother spoke with the sport youth worker and has said she is concerned about some of the "dark" things Jessica has been saying. Jessica is eager to change her online presence and regain initial confidence. Jessica and her family are not aware of what support is available and how to best support her mental health or any knowledge of how a youth worker can mediate in this situation. Jessica has realized the risk of misusing the internet and recognizes that she requires support to manage her mental health as this has influenced her decision making.

Now you can initiate a conversation based on these questions (max. 30 minutes):

- What risks are present here?
- What services should you involve?
- What course of action do you suggest to Jessica and her mother?

2. Learning Outcomes for the Module

Knowledge

- The learner will understand the importance of preventing cyberbullying
- The learner will know what kind of techniques are available to avoid being victimised by cyberbullies

Skills

- The learner will be able to spread awareness of cyberbullying prevention
- The learner will be able to teach important prevention techniques to their students

Competences

- The learner will be able to implement efficient spreading awareness events against cyberbullying
- Depending on the situation, the learner will be able to determine which type of assistance is required.

3. Bibliography

https://www.verywellfamily.com/how-to-prevent-cyberbullying-5113808
https://anti-bullyingalliance.org.uk/sites/default/files/uploads/attachments/cyberbullying-and-send-module-final%281%29_1.pdf
https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/
https://www.connectsafely.org/tips-to-help-stop-cyberbullying/

AUTHENTICATION AND PASSWORD

Module 4

1. Module Overview

Target Group

- VET Educators
- Students
- Representatives of public institutions active in the educational sectors: municipalities, regional and national authorities

Module description

VET Professionals and their students are facing different cybersecurity threats on a daily basis. Although there are various educational materials on Cybersecurity available online, they are not all update to date, or are perceived by the learners as either too basic or too complex.

The educational content of this module will equip learners with skills and knowledge to enhance their understanding of Authentication and Passwords, in order to strengthen their training capacity, but also to improve their skills so as to avoid cybersecurity attacks. Better equipped VET educators will be able to further support their students in recognizing the daily threats avoiding them.

Learning Objectives

- Enhance understanding of authentication in Cybersecurity
- Enhance understanding of different authentication methods
- Enhance understanding of the main characteristics of the most common authentication methods
- Understand the risks of not using complex passwords
- Deliver techniques to easily manage complex passwords

Overall duration

2 hours

AUTHENTICATION AND PASSWORD

Module 4

UNIT 1 - AUTHENTICATION

This Unit will be delivered by the trainer as a PowerPoint presentation sharing theoretical knowledge accompanied by more visual elements - short videos summarising the information from the PowerPoint slides (max. 20 minutes).

It is recommended to prepare the presentations on the PPT templates customised to the CYBER.EU.VET project. Considering the fast-paced developments and progress in the field of Cybersecurity, it is recommended that one continuously review the units, and if required, adjust the content considering the most recent developments in the field.

The presentation is followed by a 10-minute group discussion in order to reflect on the learning process and assess the learners' level of understanding of the topic, while creating space further questions and feedback.

Learning Activity 1

The trainer delivers a presentation with the following suggested content (max. 20 minutes):

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. When logging onto a network, a user must provide unique log-in information including a user name and password, a practice designed to protect a network from infiltration by hackers. Authentication has further expanded in recent years to require more personal information of the user, for example, biometrics, to ensure the security of the account and network from those with the technical skills to take advantage of vulnerabilities.

VIDEO: WHAT IS AUTHENTICATION?

Why is Authentication important?

Authentication is a crucial step to keep the users' data safe and to prevent and block any unauthorised access to online data. If the authentication is not secure, the system can be easily attacked and hacked and cybercriminals can gain access to data and information stored in the system from happening.

It is very important to prevent this to happen and make sure that users are aware of different free-to-use or payed methods of authentication to prevent any unauthorised access to their personal or professional data. For organisations and businesses, we recommend investing in high-quality authentication tools in order to secure their online data from any potential breaches.

VIDEO: WEEKLY CYBERSECURITY TIP - AUTHENTICATION

Common password authentication methods

Considering the constantly changing nature of different types of cyber threats and attacks, there has been a wide range of different authentication methods developed over the past few years.

Some of the most common authentication methods are:

1. Standard Password Authentication
2. Two-Factor Authentication
3. Token Authentication
4. Biometric Authentication
5. Computer Recognition Authentication
6. CAPTCHAS

1. STANDARD PASSWORD AUTHENTICATION

- Most basic and most frequently used form of authentication:
- Require entering username, accompanied by a secret code or password that allows access to a network, account, or application.

To reduce the risk of a password being compromised, users should choose a strong password. A secure password manager or software can help to prevent any unauthorised access to the data stored online.

2. TWO-FACTOR AUTHENTICATION (2FA)

- Two-factor authentication requires 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.).

3. TOKEN AUTHENTICATION

- Token systems use a purpose-built physical device to deliver two-factor authentication, and it is recommended if you prefer not to rely on mobile phones.
- This could be a dongle that is inserted into your device's USB port, or perhaps a smart card with radio frequency identification or near-field communication chip.
- To keep a token system secure, it is crucial to ensure that the physical authentication device (i.e., dongle or smart card) does not fall into the wrong hands.

4. BIOMETRIC AUTHENTICATION

- Biometric authentication relies on a user's physical characteristics to identify them. Biometric authentication might make use of fingerprints, retinal or iris scans, or facial and voice recognition. This is a highly secure form of authentication because no two individuals will have the same physical characteristics. Biometric authentication is an effective way of knowing precisely who is logging into the system.

5. COMPUTER RECOGNITION AUTHENTICATION

- Computer recognition is a password authentication method that verifies a user's legitimacy by checking that they are on a particular device. These systems install a small software plug-in on the user's device the first time they successfully login. This plug-in contains a cryptographic device marker. When the user next logs in, the marker is checked to make sure they are on the same, trusted device.
- This system is invisible to the user and doesn't require any additional authentication actions from them. They simply enter their username and password as usual, and verification happens automatically.
- To maintain a high level of security, computer recognition authentication systems must enable logins from new devices using other forms of verification (i.e., two-factor authentication with a code delivered via SMS).

6. CAPTCHAS

- CAPTCHAs do not focus on verifying a particular user, in contrast to the other methods listed in this article do. Instead, CAPTCHAs aim to determine whether a user is human, prevent computer-driven attempts to break into accounts (e.g. brute force attacks).

The CAPTCHA system displays a distorted image of letters and numbers, or pictures, and asks the user to type in what they see. Because computers and bots struggle to identify these distortions correctly, CAPTCHAs enhance security by creating an additional barrier to automated hacking systems.

Learning Activity 2

Group Discussion – Q&A, Assessment and Feedback (max. 10 minutes)

Recommended Questions for Assessment:

- What is authentication?
- Why is authentication important?
- What are the most common methods of authentication currently in use and what are their main characteristics?

UNIT 2 - PASSWORD

Learning Activity 1

1. THINGS YOU SHOULDN'T DO

Slides with pictures that exemplify things people shouldn't do, in order to get in the audience

CASE STUDIES

- "The Belgian Police have posted it with the WiFi password on. This was shown on national TV" - https://www.reddit.com/r/cybersecurity/comments/cnkhft/the_belgian_police_have_a_post_it_with_the_wifi/
- "A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note" - https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1
- "Four embarrassing password leaks on live TV" - https://www.itgovernance.co.uk/blog/four-embarrassing-password-leaks-on-live-tv

2. STATISTICS

Presentation of some statistics:

- 81% of Data Breaches happen due to poor password security
- Bad employee password habits
- Top 200 most common passwords

3. THE IMPORTANCE OF A SAFE PASSWORD

The anatomy of an unhackable password

4. BASIC RULES

Describe a set of basic rules like:

- Avoid using the browser's password managers; it is an easy way for a "malware" to gain access to them.
- Do not share your password.
- Memorize passwords, do not record them on paper or digitallyChange passwords regularly (every two months at least)
- If possible, enable two-factor authentication
- Each password must be used on only one platfor
- Change the original password when purchasing a device
- Do not use common words. One of the most frequent types of attack is via "dictionary"

Rules for a safer password:

- Create complex passwords: at least 12 characters, with both uppercase and lowercase characters, with numerals and special characters
- Do not use easily 'discoverable' terms, which typically include: name, city of birth, or known terms, pet's name, car registration number; mobile number, family member birthdays, etc..

Memorize instead of recording:

- Create a personal "key", which is part of all passwords
- Use a saying, common expressions, or something easy to memorize
- For example, use the first two letters of each word
- Switch between uppercase, lowercase and symbols
- Add something that associates with the site/tool

Learning Activity 2

Group Exercise

Test your password length! - https://www.passwordmonster.com

Have I already been cracked? - https://haveibeenpwned.com/Passwords

Discussion and Feedback (max. 10 minutes)

Recommended Questions for Assessment:

- How many years does your password resist a normal crack algorithm machine?
- Should I change my password?

Learning Activity 3

Trainer presents learners a presentation with the following suggested content (max. 20 minutes):

What are password managers?

- Digital safes
- Allows you to store credentials and notes of various services
- Bank details can also be safeguarded
- A single master key

Biometric authentication can be used

Local Password Managers

- Save the data on the current device
- The password file is encrypted
- Each password must be saved in a separate encrypted file
- May only be used on a single device

Example like KeePassXC

Online Password Managers

- Data is stored in the Cloud
- Allow access to credentials and notes of various services on any device
- No installation required
- A single master key
- Data is encrypted from the device to the server

Example of online password managers include Bitwarden, Latspass, Keeper, 1Password

Learning Activity 4

Group hands-on

- Create a complex password
- Install a Password Manager at laptop or smartphone
- Activate MFA

Discussion and Feedback (max. 10 minutes)
Recommended Questions for Assessment:

- How difficult was it?
- Will you use these best practices?

2. Learning Outcomes for the Module

Knowledge

- Understand the definition of authentication, its importance, and some of the most common authentication methods
- Understand the risks of not using complex passwords
- Use best practices in managing personal passwords

Skills

- Identify and apply the most adequate and appropriate authentication method
- Identify and apply the most adequate and appropriate password complexity

Competences

- Perceive the importance of authentication
- Decide on the most appropriate authorisation method for different online activities and apply them to enhance online security
- Perceive the importance of using complex passwords
- Structure best practice techniques to manage personal passwords

3. Bibliography

https://www.sangfor.com/blog/cybersecurity/the-basics-of-authentication-in-cyber-security
https://www.passportalmsp.com/blog/which-password-authentication-method-works-best-businesses

WI-FI SECURITY TRAINING MODULE

Module 5

1. Module Overview

Target Group

- VET Educators
- VET Learners
- Public and private stakeholders interested in improving knowledge and awareness of cybersecurity threats

Module outline

The present module will focus on shedding light on the actual threats connecting to public wifi systems, how do they work and eventually how to prevent them.

Learning Objectives

- Raising awareness about misconceptions regarding the use of public wifi networks
- Providing knowledge on the threats incurring the use of public wifi networks

Overall duration

1 hour

Unit 1

The module comprises both video learning parts and open discussions. Specifically, initially a first introductory video will be shown. This video demonstrates, through the help of an expert, how public networks are a risky place to connect to the internet. Nevertheless, this first video is very short and it does not allow to grab much of the process underneath. This first part then concludes with a discussion among learners.

Unit 2

Secondly, a more specific video will be taken into account. Despite its informal way to address the topic, it definitely conveys a better grasp of the matter. Once the video is done, the facilitator is asked to put forward a discussion among the participants about the risks of public networks and, if possible, sharing their personal experiences.

Learning Activity 1

One of the aspects on which this module wants to raise attention is the facility with which this public wifi threats are put forward. A continuous learning activity is to try to apply the suggestions learned through the video contents of this module, from the restaurant/bar where the participants will have lunch break to the train station and airport where the participants will stop coming back home after the mobility

2. Bibliography

https://www.youtube.com/watch?v=4YbXXW3DLQM&ab_channel=Techquickie
https://www.youtube.com/watch?v=1OVTmrXGHyU&ab_channel=CBSBoston
https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks
https://goodspeed.io/blog/7-dangers-of-public-wifi.html
https://www.youtube.com/watch?v=NkNgW3TwMy8&ab_channel=TheModernRogue

THE USE OF SOCIAL MEDIA NETWORKS

Module 6

1. Module Overview

Target Group

- VET Educators
- Students
- Representatives of public institutions active in the educational sectors: municipalities, regional and national authorities;

Module Overview

Online Social Networks (OSN) have assumed an unprecedented space in the professional, educational and private spheres of people's daily lives, including those of VET educators and their students. While the benefits of such an integration have been easier to recognize and adopt as an integral component of formal and informal education, the multiple risks associated with it have not received due attention and they are often ignored by the educator themselves.

A simplistic approach often used with regards to multifaceted issue of social network security, as well as the complexity of some of the available training materials, are not enough to build the required capacity to prevent and respond to the threats posed by the use of these platforms.

This module will try to provide learners with a basic set of knowledge and to strengthen their training capacity, but also to improve their own personal approach to social network security.

Learning Objectives

- Understanding cyber risks and threats associated with the use of social media networks
- Strengthening the impact of misinformation processes on the security of UGC platforms
- Identifying the different types of cybersecurity threats
- Strengthening capacity to prevent and respond cyber threats on social media
- Delivering techniques to manage easily complex passwords

Overall duration

2 hours

THE USE OF SOCIAL MEDIA NETWORKS

Module 6

Unit 1 - Social Media Threats

This Unit will be facilitated by the use of a Power Point presentation and introduced by the reading of news headlines offering widespread stories of victims of cyberthreat through social media (photos of VIP stolen, people who lost their lives because of fake news on immunization, etc...)
The stories and the content will be adjusted to be context-relevant and updated to the latest findings.
The presentation is followed by a 10-minute group discussion in order to reflect on learning and assess learners' ability to understand the topic, but also to create space for further questions and feedback.

Learning Activity 1

The trainer presents learners with a presentation of the following suggested content (max. 20 minutes):

What is an Online Social Network?
An Online Social Network (OSN) is a social structure made up of individuals or organizations called nodes, connected by one or more specific types of interdependence, such as friendship, common interest, and exchange of finance, relationships of beliefs, knowledge, or prestige. Social networking sites such as Facebook, Twitter, Instagram, etc.. are not only used to communicate or interact with other people globally, but also an effective way for business promotion. Contrary to traditional web and media platforms, Social Media's are exclusively dedicated to host and distribute user-generated contents (UGC) according criteria (algorithms) based on the actions and the preferences expressed by the users themselves and registered in data. In this sense, all users are active participants in the sustainability of social networks processes.

What Is a Social Media Threat?
A social media threat can be anything that compromises the safety of an account. A cyber threat can be both intentional and unintentional, targeted or non-targeted, and it can come from a variety of sources, including foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, disgruntled employees and contractors working within an organization.

THE USE OF SOCIAL MEDIA NETWORKS

Module 6

What a Social Media Threat looks like

Since social networks have enormous numbers of users and store enormous amounts of data, they are natural targets for spammers, phishing and malicious attacks. Moreover, online social attacks include identity theft, defamation, stalking, injury to personal dignity and cyberbullying. Hackers create false profiles and mimic personalities or brands, or slander a known individual within a network of friends.

Privacy concerns demand that user profiles never publish and distribute information over the web. Information on personal home pages may contain very sensitive data such as birth dates, home addresses, personal mobile numbers, and so on. This information can be used by hackers who use social engineering techniques to get the benefits of such sensitive information and steal money.

How Social Media Threats change across platforms

The way a social media threat is carried out by an attacker depends on their goals. Facebook allows users to keep their images and comments private, so an attacker will often friend a targeted user's friends or directly send a friend request to a targeted user to access their posts. LinkedIn is another common social media target known for business networking. If an attacker targets a business, LinkedIn is an excellent social media site to collect business emails for a phishing attack. Because many social media platforms publicly display user posts, attackers can silently collect data without a user's knowledge. Some attackers will take further steps into gaining access to user information by contacting targeted users or their friends.

Why is it important to talk about OSN threats?

As of Dec 30, 2020, there are nearly 4 billion users in the internet landscape. Out of the total population on the internet, there are 2.7 billion monthly dynamic clients on Facebook, 330 million active users on Twitter, and 320 million active users on Pinterest.

The use of social networking sites is growing exponentially. If we only look at Facebook, seven new profiles are created every second, 510,000 comments are posted in every 60s, 298,000 statuses are updated, and 136,000 photos are uploaded in the same time. Since a huge amount of data is uploaded, there is a high risk of a security breach. Anyone can post malicious content hidden inside multimedia data or with shortened uniform resource locators (URLs). There are around 83 million fake profiles corresponding to illegitimate users or professionals doing testing and research. Around 100.000 websites are hacked daily.

THE USE OF SOCIAL MEDIA NETWORKS

Module 6

Although some Social Networking Sites like Twitter do not allow disclosing private information to users, some experienced attackers can infer confidential information by analysing users' posts and the information they share online. The personal information we share online could give cybercriminals enough to get our email and passwords.

The value of personal data

Social media networks often offer their services for free. Personal information is not only the currency of social media networks, but also the main objective of cyberthreats on social media.

It can be easy to launch an attack because many people usually give out their personal information to social media platforms. Attackers can easily collect these data and use them for gain.

Collecting information to steal is only one type of social media for reconnaissance. The information posted on social media could be used to obtain passwords or impersonate business users.

With a list of targets, an attacker could then review social media accounts for personal information. Personal information can help the attacker gain the target's trust in a social engineering attack. It can also be used to guess answers to security questions for an account takeover or used to get closer to a user with higher privileges. The names of pets, favourite sports teams and education history are all potential password clues or answers to questions used to verify the user's identity to reset a password.

Why learn about OSN threats?

The user-friendly interfaces and processes these platforms offer might have alluded to people without the knowledge or skilled required to safely access their services and contents.

Education is key to stopping online social network threats.

The first step is to educate users on the dangers of disclosing too much information online to the public. Even social media accounts set to private could be used in an attack should the attacker gain access to private feeds. Users should never post private corporate information on their social media accounts or information that could be used in an account takeover.

The second step is to educate users on how digital contents are produced and distributed, and how they can drive user actions towards specific objectives for which the content has been created. All social media contents are created and vehiculated by users according to their different personal and/or collective objectives. For these reasons, some of these contents might not always be convenient, true, or ethical.

Finally, users must be educated to the safe use and maintenance of devices through which they access online social network services, as they are normally vectors of risks and intrusion. Some educational points in this regard are already illustrated in other training modules and would include:

- Avoid clicking ads, especially popups instructing users to download software to view content.
- Do not share passwords.
- Avoid messages or social media posts urging quick actions as a social engineering technique
- Do not accept friendly looking requests from unknown people even if the user has several friends in common
- Avoid the use of social media sites on public wi-fi hotspots (a common location for attackers to snoop on data using man-in-the-middle [mitm] attacks)
- Regularly change access codes and passwords.

Learning Activity 2

Ask learners to search their own names on a social media-operated search engine or on Google, and to list all the private information that can be detected by the multiple contents that are found (place and date of births, details and information on family members, addresses, phone numbers, pets, romantic partners, hobbies and preferences). Invite them to think of ways in which this information might be used against them.

Unit 2 - Type of OSN Threats

Learning Activity 1

Ask learners to list any security threat they think they could encounter on social media and ask them to explain whether they believe that threat could exist before OSN existed.

VARIOUS THREATS ON ONLINE SOCIAL NETWORK AND MEDIA

We can divide OSN threats into three categories:

1. Conventional threats include threats that users have been experiencing from the early days of social networks.
2. Modern threats are attacks that use advanced techniques to compromise user accounts.
3. Targeted attacks are attacks that are targeted on some particular user.

CONVENTIONAL THREATS

Spam

Spam is the term used for unsolicited bulk electronic messages. Although email is the conventional way to spread spam, social networking platform is more successful in spreading spam. The communication details of legitimate users can easily be obtained from company websites, blogs, and newsgroups. It is not difficult to convince the targeted client to read spam messages and trust it to be protected. Most spam is commercial advertising, can also be used to collect sensitive information from users or may contain viruses, malware or scams.

Malware attack

Malware is a programmed application that is explicitly evolved to contaminate or access a computer system, ordinarily without the knowledge of the user. Malware can use social networks structure to propagate itself through shared URLs or sub OSN applications such as e-games or plugins.

Phishing

A phishing attack is a kind of social engineering attack where the aggressor can acquire sensitive and confdential information like username, password and credit card details of a user through fake websites and emails that appears to be real.

In the case of OSN, an assailant needs to attract the client to a phony page where they can execute a phishing attack. To accomplish this, the assailant uses different social engineering methods. For example, he can send a message to a user which says, "your personal pictures are shared on this website, please check!". By clicking on that URL, the user is redirected to a fake website that looks like some legitimate social networking site

MODERN THREATS

Cross-site scripting attack

Cross-site scripting is a very prevalent attack vector among infiltrators. Fundamentally, the attack executes a malicious JavaScript on the victim's browser through different techniques. The browser can be hijacked with just a single click of a button that can send a malicious script to the server. This script is boomeranged back to the victim and gets executed on the browser. Attractive links and buttons in popular social media sites like Twitter and Facebook can trick the user into following URLs, as well as virus pop-up alerts and promising ads or multimedia contents that require visiting a link or clicking on a button to be unlocked. Some users may be invited to copy and paste JavaScript containing links onto their browser's address bar. These attacks can either steal information or act as spyware. Such attacks can also hijack computers to launch attacks on unsuspecting users while the real perpetrator of the attack is hidden behind the compromised machine.

Profile cloning attack

In this attack, the assaulter clones the users' profile thanks to prior knowledge or to information collected online. The attacker can use this cloned profile either in the same or in a different social networking platform to create a trusting relationship with the real user's friends. Once the connection is established, the attacker tricks the victim's friends into believing in the validity of the fake profile and into successfully accessing confidential information that is not shared in their public profiles. This attack can also be used to commit other types of cybercrimes like cyberbullying, cyber-stalking, and blackmailing

Hijacking

In hijacking, the adversary compromises or takes control of a user's account to carry out online fraud. The sites without multifactor authentication and accounts with weak passwords are more vulnerable to hijacking, as passwords can be obtained through phishing. Once an account is hijacked, the hijacker can send messages, share the malicious link, and change the account information, all of which compromises the user's control of their own account, as well as their reputation.

Inference attack

Inference attack infers a handler's confidential information which the user may not want to disclose, through other statistics that is put out by the user on some OSN. It uses data mining procedures on visibly available data like the user's friend list and network topology. Using this technique, an attacker can find an organization's secret information or a user's geographical and educational information

Sybil attack / Botnet

In the Sybil attack, a node claims multiple identities in a network. It can be harmful to social networking platforms as they contain a huge number of users who are coupled through a peer-to-peer network. Peers are the computer frameworks which are associated with one another by means of the internet and they can share records straightforwardly without the need of a central server. This network of machines can also be called BotNet. One online entity can make several fake identities and use those identities to distribute junk information, malware or even affect the reputation and popularity of an organization. For instance, a web survey can be manipulated utilizing various Internet Protocol (IP) deliveries to submit an enormous number of votes, and the aggressor can outvote a genuine client. A similar army can for instance share a single message multiple times and make its content viral.

Clickjacking

Clickjacking is a procedure in which the invader deceives a user to click on a page that is different from what he intended to click. The attacker exploits the vulnerability of the browsers to perform this attack. He loads another page over the page which the user wants to access, as a transparent layer. The two known variations of clickjacking are likejacking and cursorjacking. The front layer shows the substance with which the client can be baited. At the point when the client taps on that content he actually taps the like button. The more individuals like the post, the more it spreads. In cursor jacking, an attacker replaces the actual cursor with a custom cursor image. The actual cursor is shifted from its actual mouse position. In this manner, the intruder can trick a consumer to click on the malicious site with clever positioning of page elements

De-anonymization attack

In quite a lot of social networking sites like Twitter and Facebook, users can hide or protect their real identity before releasing any data by using an alias or fabricated name. But if a third party wants to find out the real identity of the user, it can be done by tracking cookies, network topologies, and user group enrollment to uncover the client's genuine identity. It is a sort of information mining method in which mysterious information is cross-referred to other information sources to re-recognize the unknown information. An attacker can collect information about the group membership of a user by stealing history from their browser and by combining this history with the data collected. Thus the attacker can deanonymize the user who visits that attacker's website

TARGETED THREATS

Cyberbullying

Cyberbullying is the use of electronic media such as emails, chats, phone conversations, and online social networks to bully or harass a person. Unlike traditional bullying, cyberbullying is a continuous process as it is continuously maintained through social media. The attacker repeatedly sends intimidating messages, sexual remarks, posts rumors, and sometimes publishes embarrassing pictures or videos to harass a person. He can also publish personal or private information about the victim causing embarrassment or humiliation. Cyberbullying can also happen accidentally, although repeated patterns of such emails, texts, and online posts are rarely accidental.

Cyber grooming

Cyber grooming is establishing an intimate and emotional relationship with the victim (usually children and adolescents) with the intention of compelling sexual or mental abuse, The principle point of cyber grooming is to acquire the trust of the youngster and through which intimate and individual information can be attained from the child. The data is often voluptuous in nature through sexual conversations, pictures, and videos which gives the attacker an advantage to threaten and blackmail the child. Assailants frequently approach teenagers or kids through counterfeit identity in child-friendly sites, leaving them vulnerable and uninformed of the fact that they have been drawn closer with the end goal of cyber grooming. However, the victim can also unknowingly initiate the grooming process when they get rewarding offers, for example, cash in return for contact details or personal photographs of themselves. The anonymity and accessibility of advanced media permit groomers to move toward various youngsters simultaneously, exponentially increasing the instances of cyber grooming.

Cyberstalking

Cyberstalking is the observation of an individual by means of the internet, email or some other type of electronic correspondence that results in fear of violence and interferes with the mental peace of that individual. It involves the invasion of a person's right to privacy. The attacker tracks the personal or confidential information of the victims and uses it to threaten them by continuous and persistent messages throughout the day. This conduct makes the victim exceptionally worried for his own safety and actuates a type of trouble, fear or disturbance in him. Most of the individuals these days share their personal information like telephone number, place of residence, area, and schedule in their social networking profile, as well as their live location. An assailant can gather this data and use it for cyberstalking.

Learning Activity 2

Ask learners to work in pairs and ask them to impersonate their respective partner while they are interviewing them for 10 minutes. Invite them to attempt their responses by trying to get the required information from the way they dress, the gadgets they carry with them, and any other contextual details they might find useful to impersonate them.

Learning Activity 3

Ask learners to scroll through their social media feeds for 1 minutes and count all the call-to-actions, links and buttons they are invited to click on. Invite them to a group reflection on how each of those links represent potential threats and how they should decide when and when not to interact with the content.

Unit 3 - Tips for Social Media Protection

Learning Activity 1

Distribute to each learner one or more cards proposing screenshots of (made-up) social media publications from different platforms and invite them to identify what sensitive information they can get from the single post and what possible threats can come from that post.

THE USE OF SOCIAL MEDIA NETWORKS

Module 6

WHAT IS SOCIAL MEDIA PROTECTION

Social media protection guidelines are meant to prevent unauthorized access to your social media accounts, protect your online identity from false impersonation or data theft, and shield your network from malicious identities or social media content.

Because modalities and objectives of OSN threats often depend on the type of platform, some specific practices to prevent threats should also be taken into account accordingly.

GENERAL PRACTICES

Use a strong password: for maintaining the security of accounts, users should choose a strong password. It should not be too short as short passwords can be easily guessed. It should be long enough and must contain alphanumeric values with some special characters. Users should not use the same password that they use for other accounts because if somehow an attacker gets to know that password, they can compromise all accounts of that user

Limit location sharing: Nowadays sharing location has become a trend. Many social networking sites have also introduced a geotagging feature, which automatically tags the geographical location of a user when the user uploads any multimedia content on social media The user has to switch it to manual, so that it does not tag location automatically. Users must upload their multimedia content online very carefully, as it may contain sensitive metadata, and it is recommended that geotagging be switched to manual mode in all their mobile devices and accounts.

Be selective with friend requests: it has been observed that many users accept friend requests without analysing the complete profile of the requester. People generally accept friend requests based on mutual friends. If the requester has some mutual friends, they then accept it. Sometimes attackers make their profile attractive deliberately or they may impersonate an account. So, if the person sending a friend request is unknown, one should ignore that friend request. It could be a fake account attempting to steal sensitive information.

Be careful about what you share: users should be careful about their posts, as they may reveal their personal information, and sometimes that of others also. Many organizations keep strict rules and regulations for sharing information and multimedia content. There are many reports of people getting fired from their job for sharing information illegally.

This situation can be avoided if employees are well informed about the protocols of the organization they are working in regarding pictures, videos, and messages that they post online. Sharing information illegitimately can harm an organization's reputation in the market, along with its data and its intellectual property.

Be aware of links and third-party applications: Illegitimate users can gain access to someone's account and get sensitive information by sharing a malicious link. Nowadays shortened URLs are becoming very popular on various social media platforms. These shortened URLs may be obfuscated with malicious code or script. These scripts try to gather the personal and confidential information of a user, which may serve to breach the privacy of that user. Moreover, hackers may take advantage of vulnerabilities present in a third-party application that is integrated with many popular social networks. An example of such a third-party application happens to be games that are playable on online social networks, and which ask for a user's public information to consume their services. This information may be provided to outsiders or third-party interventions. To avoid this risk, users should be careful while installing third-party applications in their profile.

Install internet security software: Some threats whose pattern is known may easily be detected through antiviruses. Threats like cyber grooming, cyberbullying can be detected to some extent by using anti-virus software.

PRACTICES FOR MULTIMEDIA SHARING PLATFORM

- One should not post sensitive information in their photos or captions. Exposing too much private information in a profile can be dangerous.
- Sharing current locations on social media should be avoided. Geotagging services provided by different multimedia platforms should be turned off manually.
- If an application is not in use for a long period, it is better to revoke access to that application. There are so many third-party applications that use social media accounts to log-in. For security and privacy concerns, one should allow access to trustworthy applications only.
- Enable two-step authentication for all your social media accounts wherever possible. This provides an extra layer of security to the account. In case an adversary finds out the password of a user, they will still need a second factor to authenticate themselves. The second factor consists of a unique, time-sensitive code that users receive via text on their mobile phone.

PRACTICES FOR DISCUSSION FORUMS

- One should pay attention while clicking on links provided by various sources. It may be some suspicious site trying to obtain the user's credentials.
- Users should always keep an eye on the site's URL. Harmful sites may look compellingly indistinguishable from real ones. The URL, however, may contain slight inconsistencies, like a slight variation in spelling (e.g. a '0' instead of an 'o', indiscernible if reading quickly) or an alternative domain name.
- Be careful with communications requesting the client to act promptly, offering something that sounds unrealistic or requesting personal information.

PRACTICES FOR SOCIAL CONNECTION PLATFORMS

- Users should learn about the privacy and security settings of different social media platforms, and use them. Every platform provides settings, configuration, and privacy sections meant to limit who and what groups can see various aspects of the user's profile. The privacy setting provided by the sites as default settings should not be left unaltered.
- The more details provided, the easier it is for an adversary to use that information to steal identity or to commit other cybercrimes. Thus, information sharing should be limited.
- Before accepting a friend request, one should completely check the profile of the requester. One can make different groups for sharing different kinds of information, like a different group for colleagues and family

PRACTICES FOR PROFESSIONAL NETWORKS

- Professional networks are primarily used to create contacts and increase visibility to potential recruitment companies. So, to safely use a professional network, one should look for the details provided by other users before adding them to one's contact list. Generally, an adversary does not provide many details about their career.
- A user should check if there are any spelling or grammar mistakes in someone's profile, because if someone is applying for a job, it should be very well written and should be free from any spelling or grammar mistakes. It should contain accurate and well-presented information about that person.
- Checking for consistency in a person's career can be a good practice if a user wants to stay safe on a professional network. A profile that continually and definitely changes over a short span of time is the most used part as a draw by the invader. At the point when the fraudster needs to target one sort of organization or vertical, they can simply add a new position that could be pertinent to their targets.

- One should also cross-check information. If a person claims to be from the employer's company, the user can check the company's directory and should not hesitate to verify with the company's human resource department.

Learning Activity 2

Ask learners to explain who they think has access to the latest post they have published on their favorite OSN. Finally, help them to check their privacy settings and see how much of what they said corresponded to the truth. Open a group discussion on their findings.

Learning Activity 3

Invite learners to look again at the cards they have received during **Learning Activity 1 of this Unit** and ask them if they can identify additional risks in the social media publications presented before. Ask them what they would do to mitigate those risks.

2. Learning Outcomes for the Module

Knowledge

- Cyber risks and threats associated with the use of social media networks
- Security of UGC platforms (UGC = User Generated Content)

Skills

- Identifying different types of cybersecurity threats

Competences

- Preventing and responding to cyber threats on social media
- Managing complex passwords

3. Bibliography

https://www.proofpoint.com/us/threat-reference/social-media-threats
https://www.digitalshadows.com/blog-and-research/how-cybercriminals-weaponize-social-media/
https://www.researchgate.net/publication/221663523_Cyber_Threats_In_Social_Networking_Websites
https://www.researchgate.net/publication/324860729_Social_Media_Security_Risks_Cyber_Threats_And_Risks_Prevention_And_Mitigation_Techniques

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

YBER.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
tandemplus network
Latvian European Community Studies Association
COFAC
EOS
inerciadigital
meath partnership

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

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

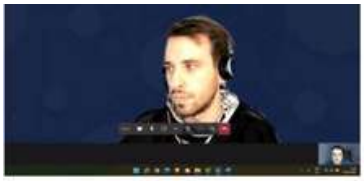
Cyberbullying is one of the main Internet risks for young people. It is common to find posts with offensive content towards some people and that these are used in order to harass and mock the victims.

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

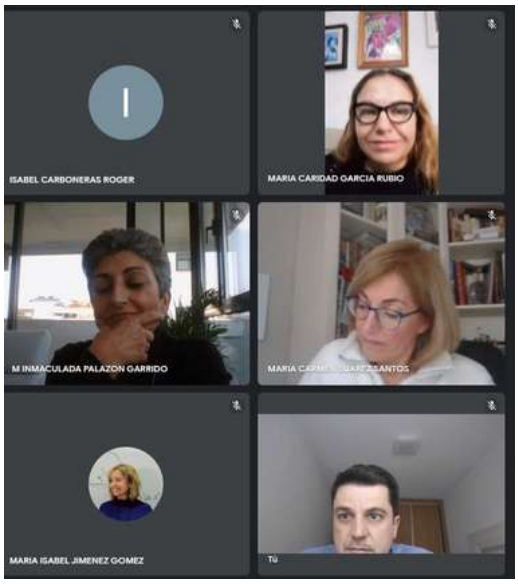
This challenge consists of studying and analyzing what young people know about safety, as well as making them aware of the risks they run in their educational centers and daily life. This challenge seeks, through gamification, the greater awareness of students and teachers in everyday life on issues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



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

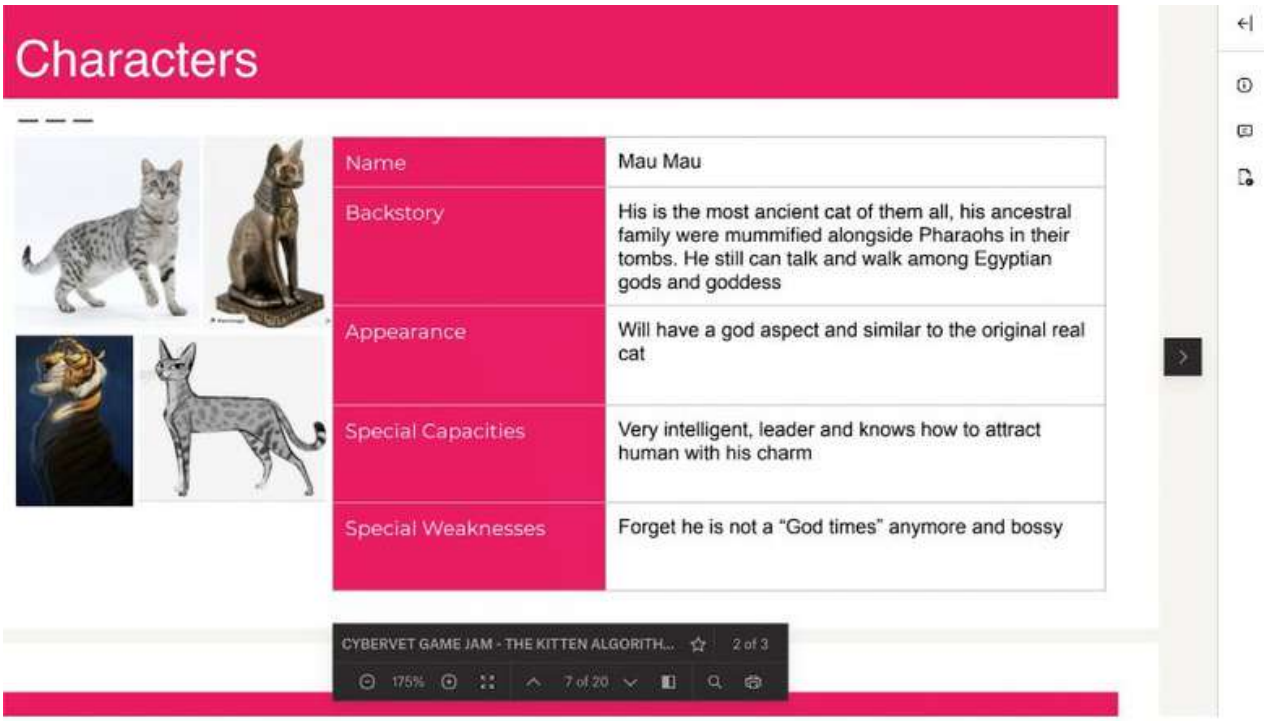
It is a 2 to 6 player turn base, strategic board game, that takes about 30 to 60 minutes to play. In this game you trick the humans to convince them that you are the best cat and get more prestige by getting as many human cat's servant you can. Keep your eye open, the other boss cats will actively try 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.

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

Mau Mau



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.

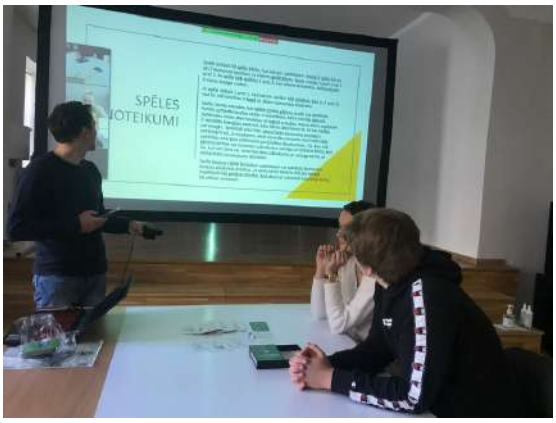
ACTIVITIES

- 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)

GAME JAM

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)

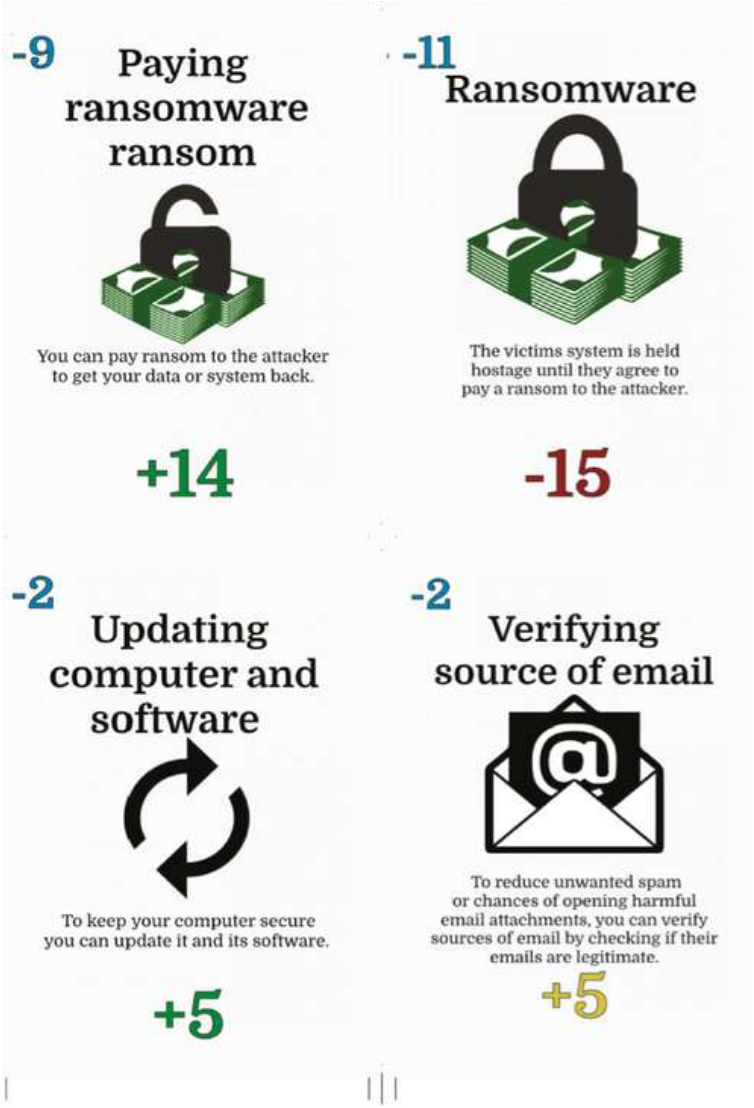
Examples of cards

In **blue** – Energy

In **red** - Attack Cards

In **yellow** - Shield Cards

In **green** - Healing Cards



Example for health calculation

LECSA (LV)

GAME JAM

EXAMPLE Cyberwar - Board Game

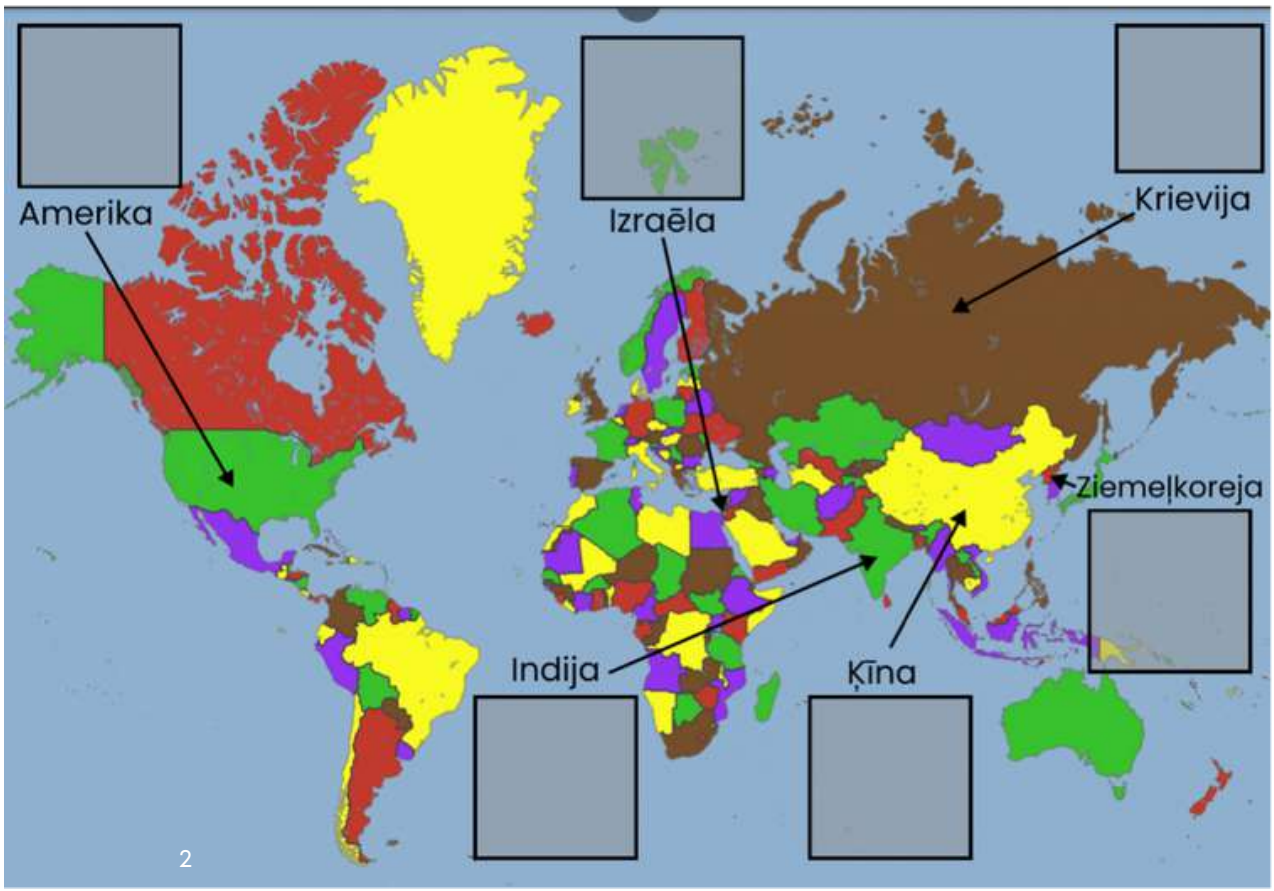
Developed by the team Exodus (students of the Saldus Technical School), leader of the team Valdemārs Šperbergs.

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

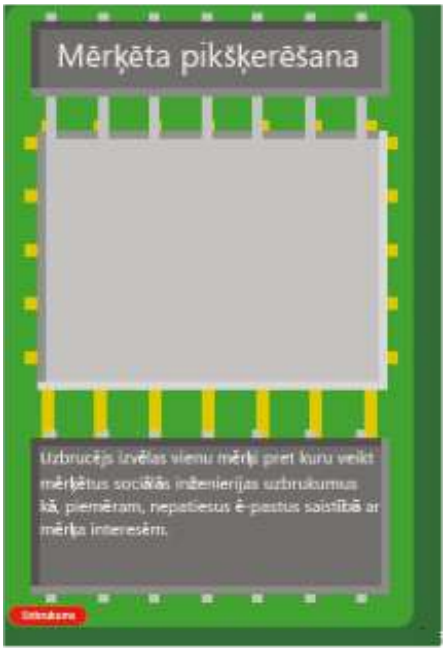
- The player names the target of the attack (e.g., "I attack a Russian 2 level vulnerability") and reveals attack card to all players, placing it next to the vulnerability.
- The player rolls the dice to see if the attack works by comparing the roll to the vulnerability difficulty + bonuses (if the rolled 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.

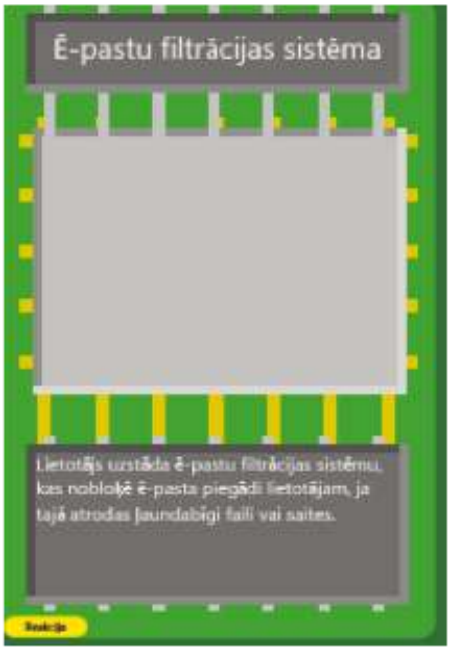
Difficulty levels

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).





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

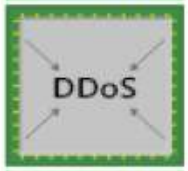
Rūtera panelis ar noklusējuma lietotājvārdu un paroli

XSS ievainojums ar filtru

SQL injekcija ar filtru

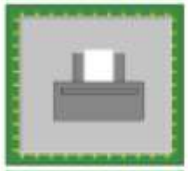
Nepilnīgi nokonfigurēts ugunsmūris

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

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

MEATH PARTNERSHIP (IE)

3) Multiplier Event – Cybersecurity Awareness Morning

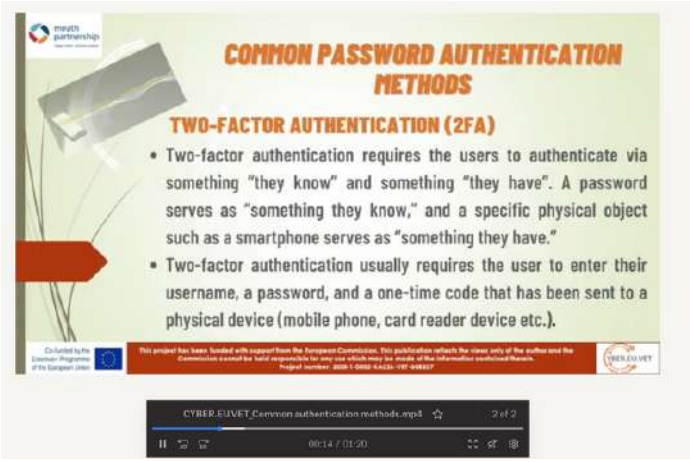
Date: November 2021

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.



COFAC / UNIVERSIDADE LUSÓFONA (PT)

GAME JAM

ACTIVITIES

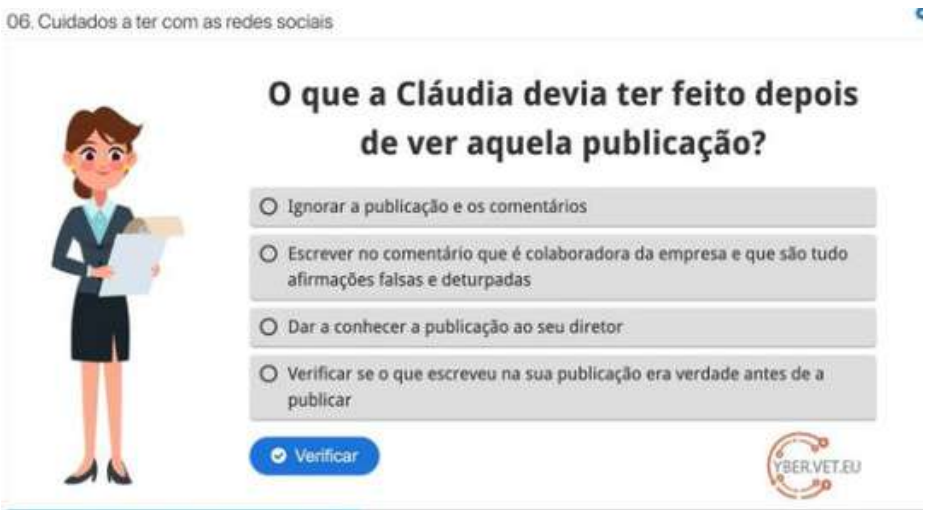
1) Cyber & Ethical Hacking post-graduation for future professionals and market teachers
Oct 2021 – Feb 2022 (in partnership with a local consultancy firm named Cybersec)

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.



TANDEM PLUS NETWORK – MEMBER IASIS [GR]

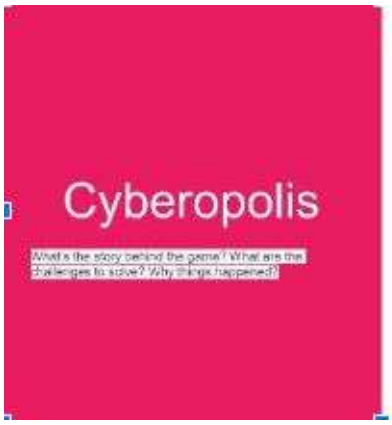
GAME JAM

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.



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.

YBER.EU.VET

Funded by
the European Union

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

CC BY NC SA