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

CYBER.EU.VET

KA226 – Partnerships for Digital Education Readiness
Project N. 2020-1-DE02-KA226-C31C2976

Research on Cybersecurity for VET

National Report
(Latvia)

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

Table of Contents

Introduction

When discussing the national cybersecurity issues and needs of education system, incl. vocational education level – various aspects in Latvian scenery and other European countries should be considered:

- The rapid development of ICT is increasing cybersecurity threats. Thereof, the importance of public awareness and its education as well as the demand for IT specialists is growing.
- Due to the divide in digital skills between educators and youth learners (gap of generations), that having impact on education quality and cybersecurity risks during the study process, the improvement of teachers' digital competence is becoming more relevant.
- Impact of the covid-19 restrictions – education institutions, including VET, were forced to switch to virtual classes and to integrated digital tools in the study process rapidly, where many educators faced a challenge – insufficient digital skills.

The topicality of cybersecurity awareness of educators, learners and public in general is addressed only in few national midterm or short-term planning documents. Most of the attention is given to the improvement of society's basis digital skills or improvement general digital competence of educators (see Chapter 1).

In general, the Latvian education system is oriented towards the development of the information society – equipping society with digital skills, where digital security takes an important place as well as preparing the new qualified ICT specialists, incl. in cybersecurity specialisation.

Digital skills are included in both the primary and secondary education curricula in Latvia. Coding and computational thinking have also now been introduced in the compulsory curricula and will gradually be implemented starting from the 2020/2021 school year. Digital literacy in the curricula is defined as a cross-cutting competence and will be developed in each learning area for each student.[1] [2]

In Latvia, there is possible to acquire a higher-level education related to Cybersecurity – 3 master programmes (Cybersecurity Engineering or Cybersecurity Management), 1 bachelor

[1] European Commission, Digital Economy and Society Index – DESI 2020
[2] Digital Transformation Guidelines 2021-2027 (only in Latvian)
https://www.varam.gov.lv/sites/varam/files/content/files/digitalas-transformacijas-pamatnostadnes-_2021-27.pdf

programme (IT with specialisation on Cybersecurity and Programming) and 1 first level professional higher education study programme (Cybersecurity and Personal Data Protection), where qualification of security specialist is obtained. In addition, one study programme is available at the level of vocational secondary education – Civil Security and Defence, where profession of Cybersecurity Technician is obtained.[3]

In order to develop the Latvian National Report of the CYBER.VET.EU project, analysis of the national political documents, EU documents, scientific publications and various internet resources (website of VET and relevant national and public organisations) were performed. List of the used resources is available in the section References.

[3] Database of National Education Opportunities – Niid.lv, study programmes in cybersecurity (only in Latvian): http://www.niid.lv/niid_search?ct=&qy=Kiberdro%C5%A1%C4%ABba&tg=

1. Need analysis about the digital skills of VET educators

The research conducted for the project CYBER.VET. EU revealed that there is a lack of updated data and information (publications, reports) on the level of digital competences, and specifically for cybersecurity topics, of educators from vocational education institutions in Latvia or challenges related to it. Currently, information on the level of digital skills of general population is available mostly.

According to DESI 2020, Latvia remains behind EU average indicator on the share of population having basic digital skills and above basic digital skills - only 43% of people aged 16 to 74 have at least basic digital skills (EU average: 58%) and only 24% have advanced skills (EU average: 33%). Moreover, its rank has dropped, comparing with previous two years.[4]

The OECD Report (carried out 2019-2020) on Latvian digital assessment "Going Digital in Latvia"[5] it is stated that the lack of basic digital skills, incl. cyber security skills, hinder the wider use of ICT among the population, as half of adults in Latvia lack such skills.[6]

In Latvia, the topicality of educators' competence development was analysed within the working group of the Ministry of Education and Science of the Republic of Latvia, as a result, experts of the industry and Latvian higher education institutions developed an informative report "Proposals for Ensuring Conceptually New Competence-Based Teacher Education in Latvia" (2017)[7], indicating that the transition to updated competence education sets conceptually different requirements for the preparation of "new educators" (teachers) and for the professional development of existing educators to work with the new content of education, and this requirements should be considered further, when planning curriculum and training activities.

Pridzans, Dzerviniks (2019) within the study "Topicality of Educators' Digital Competence Development", conducted prior the covid-19 crises and need to rapidly adapt to remote work, conclude that the acquisition of digital competence is already integrated in the study programme of higher education institutions, which prepares future educators, as well as highlights the need to constantly update educators' digital competence. In the context of the development of digital education, existing educator training programmes should focus on

[4] European Commission, Digital Economy and Society Index – DESI 2020
[5] OECD (2021), Going Digital in Latvia: https://www.oecd.org/education/going-digital-in-latvia-8eec1828-en.htm
[6] Digital Transformation Guidelines 2021-2027 (only in Latvian): https://www.varam.gov.lv/sites/varam/files/content/files/digitalas-transformacijas-pamatnostadnes-_2021-27.pdf
[7] Izglītības un zinātnes ministrija (2017), Informatīvais ziņojums "Priekšlikumi konceptuāli jaunas kompetencēs balstītas izglītības prasībām atbilstošas skolotāju izglītības nodrošināšanai Latvijā": https://www.izm.gov.lv/lv/media/1831/download

improvement of digital competence, paying particular attention to the practical aspects of developing and using interactive teaching aid.

Within the framework of OECD TALIS 2018, 41% of Latvian schools' directors report that the implementation of a quality studying process in their school is hindered by the lack of digital technologies or insufficient skills (compared to OECD average: 25%). Opportunities to improve educators' professional competences in the field of ICT have expanded in recent years. However, this is still one of the most demanded areas. Digital skills of university educators also often lag behind the level of learners' skills.[8]

It is also important to mention a problem of ageing educators' population - an average age of educators in Latvia is 48 years (average indicator of OECD – 44 years) and the share of educators in the age above 50 makes 43% of the total number of educators that creates a **digital divide between educators and pupils/students** and points to the problem of educators' shortage.[9]

Although there is currently a lack of research studies and data in Latvia on cybersecurity and other digital skills of educators in VET and other educational institutions, it is obvious that the transition to distance learning, due to the covid-19 crises, proved to be a major challenge for many teachers. The Ministry of Education and Science of the Republic of Latvia has taken this problem into account by adding courses on digital skills within the annual competence development programme (more information see below).

Regarding to national strategies, planning documents of the new budgeting period (2021-2027) highlight the following aspects:

- the **development of digital skills in the education sector** (Digital Transformation Guidelines 2021-2027) – it foresees the development of digital skills of educators and heads of educational institutions, development and use of digital skills in the educational process, as well as support for the development of digital skills of employed adults.[10]
- The development of digital skills is included in the professional competence development programme for educators (Education Development Guidelines 2021-

[8] Digital Transformation Guidelines 2021-2027 (only in Latvian): https://www.varam.gov.lv/sites/varam/files/content/files/digitalas-transformacijas-pamatnostadnes-_2021-27.pdf
[9] Education Development Guidelines 2021-2027 "Future Skills for the Future Society" (only in Latvian): https://www.izm.gov.lv/sites/izm/files/iap2027_projekta_versija_apspriesana_160720201_2.pdf
[10] Digital Transformation Guidelines 2021-2027 (only in Latvian): https://www.varam.gov.lv/sites/varam/files/content/files/digitalas-transformacijas-pamatnostadnes-_2021-27.pdf

2027). In 2020, the Ministry of Education and Science of the Republic of Latvia has set the improvement of **educators' digital competence** as a priority goal of professional competence, allocating for this purpose additional funding (0,5 million EUR). Within the programme "Improvement of Teachers' Digital Competence in the Form of E-Environment for the Use of Educational Technologies*" ("Pedagogu digitālās pratības pilnveide e-vides veidā izglītības tehnoloģiju izmantošanai*") educators of different type of education institutions can take free of charge professional development courses. [11]

- the need for **raising the awareness of learners and educators** about information security, privacy protection and the use of reliable e-services (Cybersecurity Strategy 2019-2022, actions area "Public awareness, education and research").[12] In the previous strategy, of the period 2018-2020, one of the tasks were also an improvement of the competences of teachers on cyber security issues and to support the preparation of methodological materials.
- the **digital competences' development of general society** (Education Development Guidelines 2021-2027, Digital Transformation Guidelines 2021-2027) as digital skills are now equated with literacy and numeracy in terms of their importance and at least at the basic level they are needed to everyone regardless the area of activity (digital skills = cross-cutting skills). The measures should be taken to educate the population on the basic digital skills, media literacy and information literacy, which includes the whole set of basic skills, including cyber skills.
- the need **to strengthen public awareness on safe use of the Internet** (to develop educational and informative materials for various age groups with recommendations on safety measures when using the Internet, to organize social campaigns) and to organize in-depth education for certain society groups on cybersecurity issues (Cybersecurity Strategy 2019-2022, actions area "Public awareness, education and research").[13]

In the planning documents given above, it is also discussed the **challenge** related **to the lack of IT specialists**, which is not only phenomena for Latvia, but also a pronounced situation elsewhere in the world. The share of ICT specialists in Latvia is lower than the EU average (1.7% vs. to 3.9%). However, the number of graduates with a degree in the field of ICT in Latvia is

[11] https://www.izm.gov.lv/lv/jaunums/pedagogiem-nodrosinata-iespeja-bez-maksas-pilnveidot-digitalas-prasmes
[12] Informative report, Cybersecurity Strategy of Latvia (in Latvian only) – draft version: https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf
[13] Informative report, Cybersecurity Strategy of Latvia (in Latvian only) – draft version: https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf

significantly higher than the EU average (5% in Latvia, 3.6% in the EU)[14]. In order to provide the workforce with the opportunity to easily acquire advanced digital skills, it is necessary to digitalise vocational and higher education and implement a modular approach, incl. expanding the offer for adults.

2. Need analysis about the main digital security topics

According to the national Cybersecurity Strategy 2019-2022[15], Latvia's cyberspace continues to face large-scale threats – phishing, extortion and malware, attempts to hack the systems, networks and websites, denial-of-service attacks (DoS) on critical information systems as well as fraudulent e-mail and social engineering campaigns to retrieve personal or authentication data to discredit a specific person, company or institution or to commit crimes.

Pandemic-forced remote work has obviously increased cybersecurity risks and facilitated new types of incidents which 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. Based on the CERT.LV (the Information Technology Security Incident Response Institution of the Republic of Latvia[16]), which monthly and annually publishes data and overview of the most relevant incidents called “Kiberlaikapstākļi” (Cyber Weather), 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 thousand per month). The most often registered threats were vulnerabilities, malicious code and intrusion attempts.[17]

The main Incidents of 2020 by CERT.LV are:[18]

Denial-of-service Attacks (Do Sand DDoS)

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).

[14] European Commission, Digital Economy and Society Index – DESI 2020
[15] Informative report, Cybersecurity Strategy of Latvia (in Latvian only): https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf
[16] main institution in Latvia maintaining information on IT security threats, providing support in case of IT security incidents, advising governmental institution and educating society. CERT.LV provides support to Latvian and foreign, state and municipal institutions, merchants and natural persons.
[17] see more: https://cert.lv/en
[18] Information Technologies Security Incident Response Institutions (2021), CERT.LV Annual Report 2020: https://cert.lv/uploads/parskati/CERTLV-annual-report-2020_ENG.pdf

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), 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 - Office 365 access rights, which was difficult to detect by technical means, since no malicious actions were carried out on the victim's device, but the attacks were carried out within Office 365.

Fraud

Regarding fraud, year 2020 was very intensive, including social engineering attacks. Among the most active fraud 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 prices.

A new trend was observed - extortion e-mails with the threat of leaking data were also targeted at companies

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 representative, 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 to Latvian credit institutions.

Hackers' adaptation to the necessity to start remote work – considering the need of companies to rapidly switch to a remote work condition and implementation of electronic documents'' circulation, hackers used the 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.

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

Scam messages with shortcut links (ej.uz), used to mask the actual link destination, on behalf of the state institutions regarding the state of emergency and the epidemiological situation in the country.

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 sale their products online.

Vulnerabilities and Configuration Insufficiencies

The reporting period was marked by an alarming number of detected vulnerabilities. The vulnerabilities either allowed attackers to remotely execute arbitrary code on the target device, or to retrieve sensitive information from the target system. Also, the websites of several companies and institutions were subject to personal data retrieval attacks as a result of improper configuration.

At the beginning of 2020, an average of 20,000 unique IP addresses with OpenSSDP (Open Simple Service Discovery Protocol) vulnerabilities were registered every month, which are exposed to the risk of use in DoS attacks. A fraction of the inadequately configured devices were smart TVs.

Intrusion Attempts

Intrusion attempts have taken place throughout the year, but at a sufficiently low intensity, mainly against the servers of state and municipal institutions from other countries, as well as some attacks coming from Latvian IP addresses were aimed at state institution servers of other countries.

However, after the rise of remote work increased 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).

Malware

Malware was 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). Emails containing infected attachments were mainly used to distribute malware.

The covid-19 situation was used to spread malware attempts: e.g., e-mails in the name of the World Health Organization, 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.

In the second half of 2020, the malware Emotet saw the rapid spread both on the global and the Latvian networks, which is intended to steal sensitive information and it came usually from an e-mail of already infected contact. The Emotet serves a door opener for other computers, allowing unauthorised access to other malware families. More than 200 Latvian companies were infected

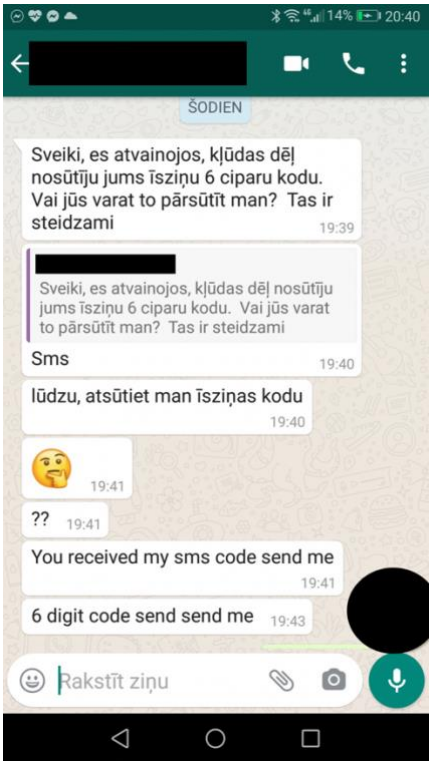
Compromised Devices and Data Leaks

Equipment compromises affected individuals, companies, as well as state and municipal institutions (already compromised email - infection of device through opening attachments or links from seemingly known contacts – colleagues and business partners; compromised websites - via an outdated plugin or outdated content management system).

Also, several national institutions temporarily lost access to their social network accounts as attackers took control of one of the account administrators' profiles. Reports of Zoom, MS Teams and other platform meeting break-ins were received which were caused due to the lack of knowledge on available safeguards (*waiting room, limited access from abroad, etc.).

At the of 2021, fraud, malware and vulnerabilities continue to be active - stolen WhatsApp accounts through activation codes which requested by hacked accounts of person's contact list; a new wave of blackmail emails (sextortion) – threaten to distribute compromising material, if e-mail user will not make a ransom; phishing scam "Who visited you Facebook profile"; fraudsters persistently continue to pretend to be well-known logistics companies – fraudsters pretended to buy the product from persons who published offer on the trading platforms using available delivery services in Latvia; scam messages from banks, etc.

The year 2020 with its global changes have demonstrated that for educators of the VET and other education institutions it is important to have increased knowledge/skills on the safe remote work when organising online classes and using digital tools (e-mails, WhatsApp, learning platform, etc.) as well as to be aware about the topical scams and frauds, especially on social media, to raise the awareness of their pupils and students.



Subject: [redacted]
Date: Thu, 23 Apr 2020 05:48:42 0300
From: Cicily Romine
To: [redacted]

It seems that, [redacted] your password.

I need your full attention for the the next 24 hrs, or I will certainly make sure you that you live out of guilt for the rest of your life.

Hello, you do not know me. Yet I know every thing concerning you. Your entire fb contact list, phone contacts as well as all the digital activity on your computer from past 156 days.

Consisting of, your masturbation video, which brings me to the primary motive why I 'm crafting this specific e mail to you.

Well the previous time you went to see the porno websites, my spyware was triggered in your computer system which ended up logging a lovely video of your masturbation play simply by triggering your webcam.
(you got a seriously odd preference by the way lmfao)

I have the complete recording. If perhaps you think I am playing around, just reply proof and I will be forwarding the particular recording randomly to 9 people you recognize.

It may be your friend, co workers, boss, parents (I don't know! My software will randomly select the contacts).

Will you be able to look into anyone's eyes again after it? I doubt it...

However, it does not need to be that route.

I would like to make you a 1 time, non negotiable offer.

Purchase USD 2000 in bitcoin and send it to the listed below address:

1KMD*uRkgyr82q5Fxy2WvRHiQ9bxbemM1kt
[CASE-sensitive so copy and paste it, and remove * from it]

(If you do not know how, lookup how to acquire bitcoin. Do not waste my precious time)

If you send this particular 'donation' (we will call this that?). Immediately after that, I will disappear for good . and under no circumstances make contact with you again. I will eliminate everything I have got in relation to you. You may very well carry on living your regular day to day life with zero concern.

You've 24 hours to do so. Your time will start as quickly you check out this e mail. I have got an one of a kind program code that will inform me as soon as you read this e mail so don't attempt to act smart.

3. Good practices about Cybersecurity Programmes and Resources for VET Institutions

In Latvia, there is a number of cybersecurity initiatives and recourses aimed at raising public awareness. However, when searching for examples of good practice in cybersecurity and vocational education institutions (their educators and learners), we have discovered the shortage of specific initiatives. Therefore, the best practices described below focus on educators in general (including those from VET) – development of professional digital competences, educational and informative initiative for youth (including those from VET) that provides also materials about cybersecurity for use in educational institutions, as well as preparation of cybersecurity specialists at the VET level (see below).

Examples of existing initiatives in Latvia – resources for VET institutions:

- The Latvian government annually organises initiatives "safer internet day", "e-skills week" and "cyber security month", which aim to raise awareness and share good practices.
- CERT.LV (Information Technology Security Incident Response Institution) provides training and information on digital security risks to IT professionals and the public, including employees, managers, students and pupils.
- The Ministry of Defence of the Republic of Latvia in cooperation with LIKTA (the Latvian Information and Communication Technologies Association) the annual award for "the best cybersecurity initiative".
- Erasmus+ project DIG4VET (Digital Tools for Learning and Validation in VET and WBL: Training Program for VET Teachers, Trainers and Potential I-Coaches) aimed at improvement of skills and competences of VET teachers, trainers, mentors for use of digital tools in education process, for both: classroom and distance learning.
- number of digital skills programmes available for unemployed people.
- regular seminars/webinars on cybersecurity organised by Latvian Safer Internet Centre, LIKTA and other relevant organisations, etc.

3.1 Best Practices n.1 – Project-platform "Drossinternets.lv" (from Latvian: Safe Internet)

https://drossinternets.lv/
https://www.facebook.com/drossinternets

OBJECTIVE

Latvian Safer Internet Centre is a leading organisation on Internet safety for children and young people in Latvia. In 2017, it has launched a platform "Drossinternets.lv" to organise educational and awareness raising activities on the safe use of internet as well as to provide possibility of reporting about violations on the Internet.

BENEFICIARIES

Platform "Drossinternets.lv" offers digital educational and informative resources for several groups:

- Educators (teachers; trainers; representatives of schools, VET; social workers; librarians; etc.)
- Parents
- Children (up to 11 years)
- Young people (from 12 to 18 years).

DESCRIPTION

Latvian Safer Internet Centre via its platform performs three main directions of activities:
(1) EDUCATIONAL WORK: informing and educating children, young people, teachers and parents about the safe Internet content - on the potential risks and dangers on the Internet (incitement to hatred, racism, child pornography and pedophilia, cyberbullying, identity theft and data misuse, rules of conduct on the Internet).

The Centre offers free of charge trainings for children /young people that should be booked by representatives of Latvian schools or VET (~40 min, considering certain conditions). During the covid-19 pandemics lectures are organised online.

In addition, there are seminars for adults by applying through Latvian Municipal Training Centre.

(2) REPORTING LINE: possibility for the public to electronically report detected violations and illegal content on the Internet. Reports are processed in accordance with the laws and regulations of the Republic of Latvia with the support of the State Police

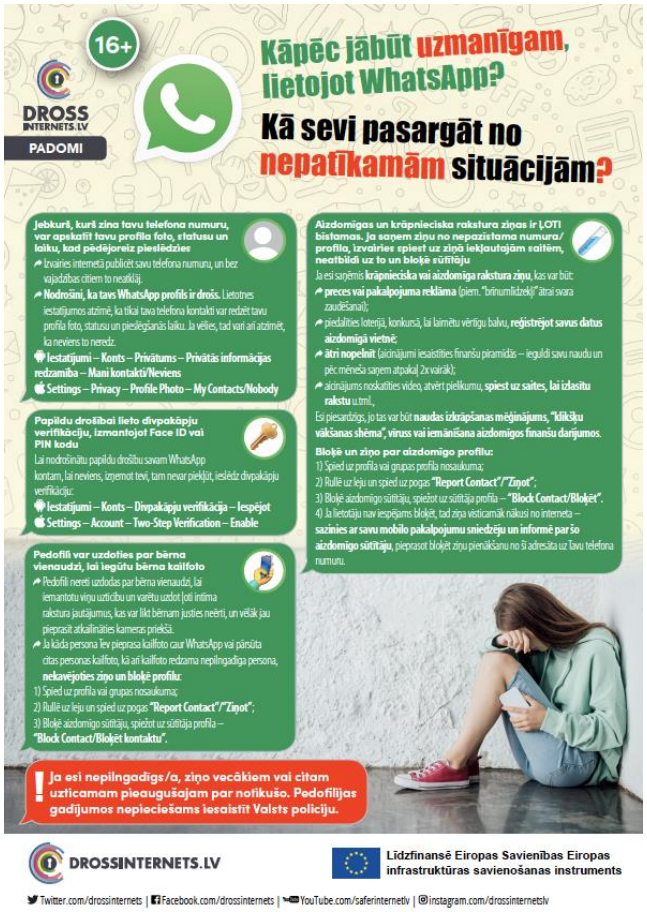
(3) HELPLINE 116111: opportunity for children/ young people to report violations on the Internet and receive psychologist's support and advice for solving various situations. The helpline is operated by the State Inspectorate for Protection of Children's Rights.

RESULTS ACHIEVED (AS OF 2018):

- Developed over 250 digital educational and printed materials.
- Created 98 educational videos that are available on YouTube channel: YouTube.com/saferinternetlv).
- Trained 26 volunteers as Ambassadors of "Drossinternets.lv" which later have trained over 10 000 pupils across all Latvia.
- Every year, a Safer Internet Day as well as related activities and social campaigns in Latvia are organised.
- The Reporting Line has received and processed 5,579 reports about illegal, harmful Internet content and problem situations in the Internet environment.
- Every year, over 500 classes for children and young people are organized on various topics related to Internet safety in schools throughout Latvia.
- Every year, ~ 30 trainings on Internet safety and media literacy are organized for adults (teachers, educators, librarians, social pedagogues, police officers, etc.).
- Annually the platform is visited by an average of ~ 130,000 unique users.
- Over 250 publications are published in the media each year, covering the Centre's activities and interviews with TV, radio and news portals on various topics related to Internet security.
- in cooperation with the National Centre for Education in spring 2018, organised a comprehensive online diagnostic test for 3rd and 6th grade students about internet safety and media literacy. 420 schools all over Latvia (60% of all schools), participated in the test involving 17,806 pupils.

INNOVATION

One-stop shop place for awareness raising events, free educational activities and materials covering diverse topics of cybersecurity as well as possibility to report about illegal content and breaches related to children and young people on the Internet.



Picture 1. Example of informative materials - Why to be careful when using WhatsApp? How to protect yourself from unpleasant situation?

3.2 Best Practices n.2 - Programme "Improvement of Teachers' Digital Competence in the Form of E-Environment for the Use of Educational Technologies"

https://www.izm.gov.lv/lv/jaunums/pedagogiem-nodrosinata-iespeja-bez-maksas-pilnveidot-digitalas-prasmes (in Latvian only)

OBJECTIVE

The aim of the programme is to improve educators' digital competence – to teach about technologies and tools that will help educators to organise their work process more efficiently. Programme is implemented by since 2014 by the Ministry of Education and Science of the Republic of Latvia

BENEFICIARIES

The content of the courses in 2020 is designed for:

- management teams of educational institutions,
- educators of vocational (VET) and general education schools,
- primary school teachers,
- pre-school teachers,
- various subjects' teachers (maths, Latvian language, computers science, engineering, design and technology, physics, chemistry and biology).

DESCRIPTION

In 2020, the Ministry of Education and Science has set the improvement of educators' digital competence as a priority goal of professional competence, allocating an additional funding. The programme offers free-of-charge course for educators with different knowledge level representing various subjects (their field of specialisation, see section Beneficiaries)

The implementers of the courses have developed detailed learning tasks, attracted group leaders - consultants to ensure a favourable learning regime for educators. The content of the courses is designed in accordance with the requirements of the modern learning environment.

RESULTS ACHIEVED

4339 educators have attended long (with the granted right to work as computer science teacher) and short professional competence development courses (2014-2020).

INNOVATION

Innovative approach hinders in the process organisation – each course participant can learn the content at a pace and time convenient for them. During the course, technologies and tools are

analysed that can be used in the study process in order to promote collaboration and simplify the organization of the study process/educators' work process.

3.3 Best Practices n.3 - Qualification of Cybersecurity Technician at the Saldus Technical School (VET) (study programme Civil Security and Defence)

https://www.saldustehnikums.lv/izglitibas-iespejas/profesijas/profesionala-videja-izglitiba/kiberdrosibas-tehnikis (in Latvian only)

OBJECTIVE

The aim of the Civil Security and Defence pro-gramme (established in 2018) is to educate cybersecurity specialists for national defence – to teach the basics of the profession and critical thinking. Thus, to ensure employees for institutions of national importance, NGOs and others (Ministry of Defence of the Republic of Latvia, military sector, telecommunications service provider, etc.).

BENEFICIARIES

The main beneficiaries are pupils in smaller living area – Saldus city and its surroundings, institutions of national importance and society in general (e.g. Ministry of Defence of the Republic of Latvia, etc.).

DESCRIPTION

The Saldus Technical School is the first and only one vocational education institution in Latvia that offers possibility to acquire qualification of Cybersecurity Technician. Length of the programme is 4 years.

The education programme prepares specialists who should be able to perform information system security manager duties and various operations - information system security checks, responding to information system security incidents, requesting assistance from responsible authorities and cooperation in the consequences elimination of information system security incidents.

During the study process, great emphasis is placed on the ability to notice and respond to false news spreaders on social networks.

In addition to the study programme, Technical School is offering a possibility for youth of Saldus city to participate in the cybersecurity group of interests, where they can learn about hackers,

Windows and Linux operating systems, FTP and web-server installation, social engineering, computer viruses, current cyber threats, digital forensics, SDR radio communications, etc.

RESULTS ACHIEVED

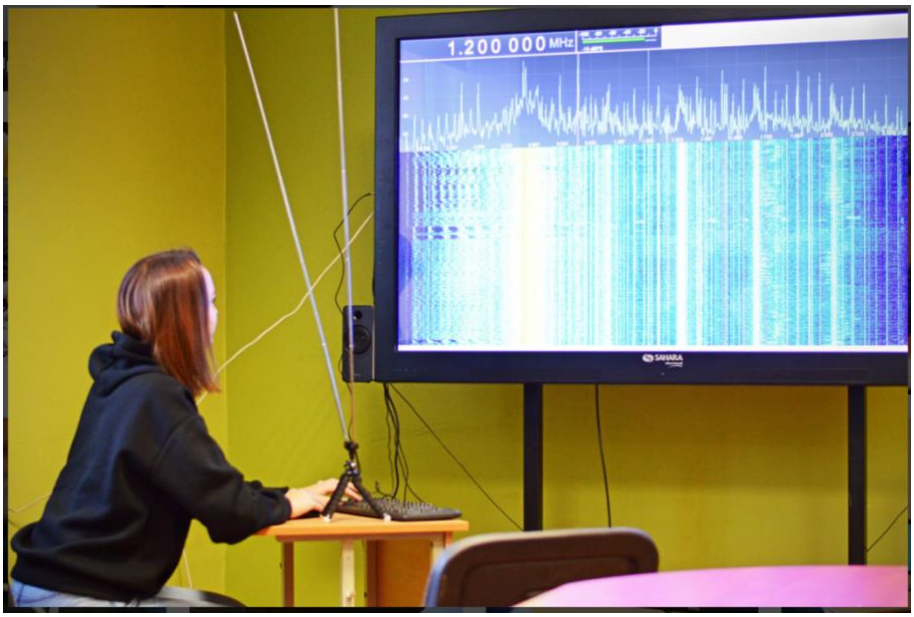
Interest on the programme is higher than expected, e.g., 22 students instead of planned 15 have applied to the study programme in 2018Developed over 250 digital educational and printed materials.

INNOVATION

The study programme prepares specialist of the world-demanding profession.

The study programme serves as a cyber polygon – a safe environment where pupils can apply their technical knowledge by trying to hack the information systems and have training without any criminal responsibility or other consequences. Pupils are taught to break things down (to hack) in order to gain a better understanding on how to protect the state and its institutions (national security).

The program also includes professional orientation courses and some of the study courses are organised in cooperation with the National Armed Force (communication training courses).



Picture 2. Study process at the study programme Civil Security and Defence, Saldus Technical School, source: Saldus Technical School

Concluding remarks

The research conducted for the project CYBER.VET.EU revealed that there is a lack of data and information on the cybersecurity competences and challenges of educators of education institutions in Latvia, as well as that there is a limited number of initiatives focusing on the cybersecurity issues within the VET, indicating that project CYBER.VET.EU have addressed the emerging topic in Latvia. Nevertheless, those existing initiatives are comprehensive and proved to be efficient (see section Good Practices). Currently, most of the activities and projects are focusing on the cybersecurity awareness raising of general population and improvement of overall digital competencies of educators, which was influenced by the rapid adaptation to remote work/learning process.

The various policy documents (planning documents) are addressing the following challenges, which are directly or not directly related to cybersecurity skills of educators and learners – low level of basic digital skills of Latvian population, insufficient digital skills of many educators to realise virtual learning process, ageing population of educators (that creates gap in digital skills of educators and learners) as well as the lack of the IT specialists, incl. those with cybersecurity specialisation (and the VET education is potential niche to tackle the problem).

The year 2020 with its global changes have demonstrated that for educators of the VET and other education institutions it is important to have increased knowledge/skills on the safe remote work when organising online classes and using digital tools (e-mails, WhatsApp, learning platform, etc.) as well as to be aware about the topical scams and frauds, especially on social media, to raise the awareness of their learners.

Latvia's cyberspace continues to face regular attempts to hack information systems and websites, fraudulent e-mail campaigns aimed at deceiving personal and authentication data or infecting the information system with malware, insufficient knowledge of secure ICT solutions and the use of digital technologies. These issues concern also educational institutions and educators in Latvia.

Considering the increasing number of operations conducted online, such as remote work, meetings, studies, shopping, and communication, as well as the data leaks that have already taken place and the potential ones, more adjusted and targeted cyberattacks can be expected, thereof improvement of educators' and learners' digital competence in a regular basis and awareness raising of public on cybersecurity issues is becoming more and more relevant, as well as the new activities should be designed.

References

CERT.LV (Information Technology Security Incident Response Institution): https://cert.lv/lv

Database of National Education Opportunities – Niid.lv, study programmes in cybersecurity (only in Latvian): http://www.niid.lv/niid_search?ct=&qy=Kiberdro%C5%A1%C4%ABba&tg=

Digital Transformation Guidelines 2021-2027 (only in Latvian) https://www.varam.gov.lv/sites/varam/files/content/files/digitalas-transformacijas-pamatnostadnes-_2021-27.pdf

Education Development Guidelines 2021-2027 "Future Skills for the Future Society" (only in Latvian): https://www.izm.gov.lv/sites/izm/files/iap2027_projekta_versija_apspriesana_160720201_2.pdf

Erasmus+ project DIG4VET (Digital Tools for Learning and Validation in VET and WBL: Training Program for VET Teachers, Trainers and Potential I-Coaches): https://www.visc.gov.lv/lv/projekts/projekts-dig4vet, https://qualityplacements.eu/wbl-projects/about-dig4vet/

European Commission, Digital Economy and Society Index – DESI 2020

https://likumi.lv/ta/id/301572-noteikumi-par-pedagogiem-nepieciesamo-izglitibu-un-profesionalo-kvalifikaciju-un-pedagogu-profesionalas-kompetences-pilnveides

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 (in Latvian only): https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf

Izglītības un zinātnes ministrija (2017), Informatīvais ziņojums "Priekšlikumi konceptuāli jaunas kompetencēs balstītas izglītības prasībām atbilstošas skolotāju izglītības nodrošināšanai Latvijā": https://www.izm.gov.lv/lv/media/1831/download

Izglītības un zinātnes ministrija (2020), Pedagogiem nodrošināta iespēja bez maksas pilnveidot digitālās prasmes: https://www.izm.gov.lv/lv/jaunums/pedagogiem-nodrosinata-iespeja-bez-maksas-pilnveidot-digitalas-prasmes (in Latvian only)

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

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

List of secondary vocational institutions in Latvia: https://www.izm.gov.lv/lv/pedagogu-profesionalas-kompetences-pilnveide

OECD (2021), Going Digital in Latvia: https://www.oecd.org/education/going-digital-in-latvia-8eec1828-en.htm

Pridzans, Dzerviniks (2019), The Topicality of Educators' Digital Competence Development, *SOCIETY. INTEGRATION. EDUCATION Proceedings of the International Scientific Conference. Volume V, May 24th -25th, 2019. 513-524*

Saldus Technical School, Study Programme Civil Security and Defence: https://www.saldustehnikums.lv/izglitibas-iespejas/profesijas/profesionala-videja-izglitiba/kiberdrosibas-tehnikis (in Latvian only)