YBER.EU.VET

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

CYBER.EU.VET

KA226 – Partnerships for Digital Education Readiness

Projekts Nr. 2020-1-DE02-KA226-C31C2976

Konsorcija ziņojums

par galvenajiem kiberdrošības izaicinājumiem un labajām praksēm

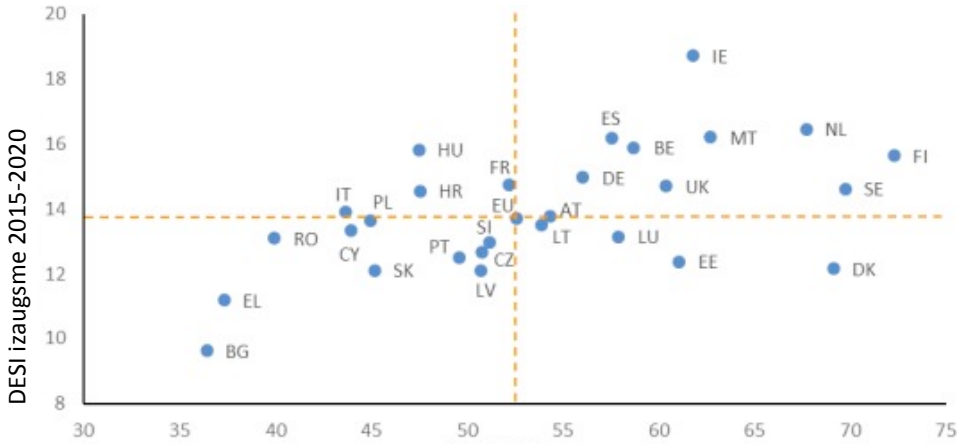
"Eiropas Komisijas atbalsts nenozīmē piekrišanu šī dokumenta saturam, kurš atspoguļo vienīgi tā autoru viedokli. Komisija nevar būt atbildīga par jebkādu šeit ietvertās informācijas izmantošanu."

Satura rādītājs

Ievads

Tā kā pasaule kļūst arvien digitālāka, ir kļuvis acīmredzams, ka šāda prakse ir jāapvieno ar pašreizējo politiku. Eiropas kontekstā liela uzmanība tiek pievērsta digitālās pratības politikai un kiberdrošības politikai, tomēr praksē ir maz tādu iniciatīvu, kas atbilstu šo izstrādāto politiku mērķiem. Lai novērotu, cik lielā mērā digitālās un kiberdrošības kompetences ir centrālā un sazarotā tēma, ir lietderīgi aplūkot 2020. gada Digitālās ekonomikas un sabiedrības indeksu (DESI).

DESI uzrauga Eiropas vispārējo digitālo veiktspēju un mēra digitālās konkurētspējas līmeni visās ES valstīs. Sniedzot informāciju par digitalizācijas līmeni visās dalībvalstīs, tas palīdz noteikt investīciju jomas un turpmākās darbības. Ceļā uz digitālu nākotni, kas pielāgota cilvēku vajadzībām un ievēro ES pamatvērtības, Eiropas Komisija 2020. gada februārī prezentēja digitālās transformācijas vīziju "Eiropas digitālās nākotnes veidošana". 2020.g. DESI ziņojumā tiek novērtēta digitālā ekonomika un sabiedrība pandēmijas sākumā, pamatojoties uz 2019. gada datiem.

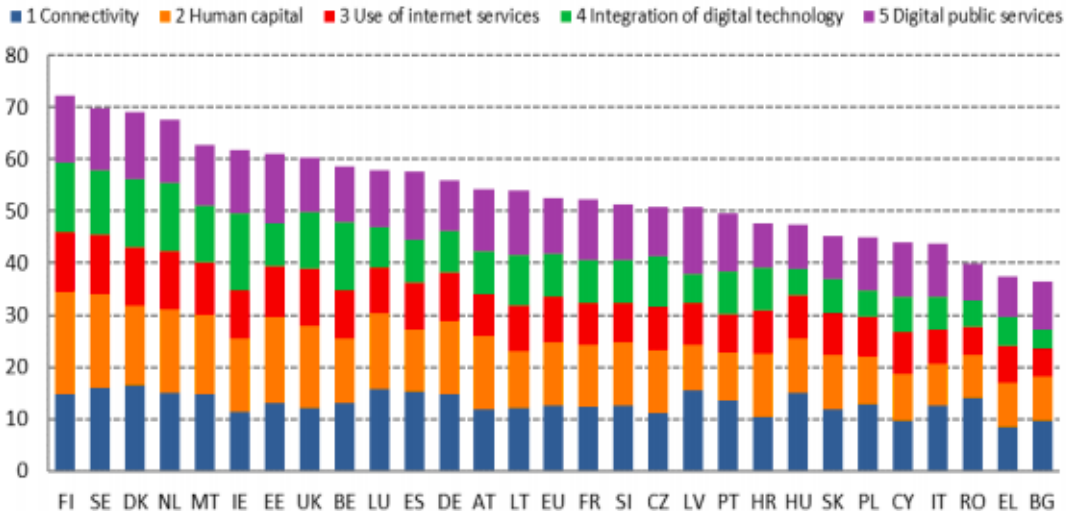


Avots: Eiropas Komisija, DESI 2020.

Šis indekss īpaši pēta un apkopo datus par:

- Savienojamību: ātras un uzticamas interneta piekļuves pieejamība (tostarp fiksēta un mobila savienojuma) ir ļoti svarīga pašreizējā tiešsaistes laikmetā, kur tiek sniegti galvenie sabiedriskie un ekonomiskie pakalpojumi;
- Cilvēkkapitālu: digitālās sabiedrības mugurkauls ir tās cilvēku digitālās prasmes. Digitālo pakalpojumu lietotāji un cilvēki ar ierobežotām pārvietošanās spējām var veikt pamata darbības tiešsaistē, izmantojot šīs ierīces;
- Interneta lietošanu: pandēmijai progresējot, arvien vairāk cilvēku sāka izmantot internetu. Vispārējās izolācijas rezultātā palielinājās regulāra piekļuve sociālajiem medijiem un izklaides platformām, kā arī attālinātā darba un e-komercijas pakalpojumiem;
- Digitālo tehnoloģiju integrāciju: uzņēmumi ātri pieņēma jaunu darba kārtību un formu, lai pielāgotos valdības pasākumiem vērstiem uz sociālās mijiedarbības samazināšanu;
- Sociālās distancēšanās pasākumu ietvaros ir jāturpina valdības aktivitātes, lai nodrošinātu to, ka digitālie sabiedriskie pakalpojumi sniedz ieguvumus. Lai īstenotu veiksmīgu pašreizējās pandēmijas pārvarēšanas stratēģiju, visās dalībvalstīs būs nepieciešami spēcīgi digitālie sabiedriskie pakalpojumi.

Šāda analīze ir noderīga, lai noskaidrotu starp kurām projekta partneru valstīm ir vērojamas atšķirības digitālās un kiberdrošības jomās. Saskaņā ar DESI datiem, trīs projekta partneru valstis – Īrija, Spānija un Vācija – parāda rezultātu virs ES vidējā, bet pārējo četru partnervalstu (Francijas, Latvijas, Portugāles un Itālijas) rezultāti ir zemāki.



Avots: Eiropas Komisija, DESI 2020.

Ir svarīgi uzsvērt, ka DESI 2020 rezultāti neapstiprina lineāru atbilstību starp valsts IKP un digitālo prasmju izplatību. Piemēram, Spānija ieņēma 5. vietu ES ekonomikā un tikai 10. vietu Digitālās ekonomikas un sabiedrības indeksā. Dažās valstīs, kas veido projekts konsorciju, nesen ir ieviesušas vairākas iniciatīvas, lai uzlabotu ekonomikas un sabiedrības digitalizāciju. Vācija kā ES vadošā valsts 5G gatavības jomā ir ieviesusi vairākus pasākumus, lai veicinātu digitalizāciju, tostarp iniciatīvas IT drošības, superskaitļošanas, AI un blokķēdes jomās. Francijā ir bijuši vairāki centieni, lai veicinātu uzņēmumu un sabiedrisko pakalpojumu digitalizāciju, tostarp centieni izveidot ekosistēmu, lai atbalstītu tehnoloģiju jaunuzņēmumus. Itālijas valdība 2020. gada decembrī pieņēma "Italia 2025" — 5 gadu plānu, kurā inovācija un digitalizācija ir "valsts radikālas un strukturālas pārveides procesa" centrā. Nākamajos gados šīs iniciatīvas, kurām nepieciešama ilgstoša īstenošana un kuras prasa arī ieguldījumus, var veicināt šo dalībvalstu progresu DESI jomā.

Vēl viens svarīgs aspekts, apsverot digitālo un kiberdrošības prasmju līmeni, ir saistīts ar Covid-19 pandēmijas ietekmi uz šīm tēmām. Lai gan saikne starp ārkārtas situāciju veselības jomā un kiberuzbrukumu rādītājiem plašākai sabiedrībai nav uzreiz skaidra, patiesībā tā ir izraisījusi kiberuzbrukumu gadījumu skaita pieaugumu. Kibernoziedznieki ir ļoti elastīgi, kad iet runa par jaunu notikumu izmantošanu, kā mēs to redzējām nesenajā ārkārtas situācijā veselības jomā.

2020. gadā daudzi uzņēmumi ir pārgājuši uz jaunām digitālajām stratēģijām (t.i., attālināto darbu), un šādi ir pavērušies sevi vairākiem jauniem uzbrukuma vektoriem, kurus noziedznieki ir ātri izmantojuši. Cita starpā Covid-19 negaidītā parādīšanās ir izmantota, lai mēģinātu izplatīt ļaunprātīgu programmatūru – piemēram, Pasaules Veselības organizācijas (WHO) vārdā tika sūtītas e-pasta vēstules, kurās norādīts, ka pielikumā ir ietverta jaunākā informācija par pandēmiju; saites uz grafikiem, kas parāda vīrusa izplatību, kuru mērķis bija lietotāju datu zagšana; ļaunprātīgi e-pasta ziņojumi veselības aprūpes iestādēm par Covid-19 aizsardzības līdzekļu piegādi un daudz ko citu.

Lai izstrādātu šo konsorcija pētījuma ziņojumu, tika veikta dokumentu izpēte, kas ietvēra datu, publikāciju, ES ziņojumu, valstu un Eiropas tiesību aktu meklēšanu un apkopošanu. Pētījumā tika aplūkoti digitālās pratības un kiberdrošības jautājumi dažādos valstu kontekstos, īpašu uzmanību pievēršot profesionālo izglītības iestāžu (VET) pedagogu apmācībai. Turklāt šajā ziņojumā ir uzsvērti daži no galvenajiem kiberdrošības sektorā iesaistītajām pusēm, tostarp valsts iestādes un Eiropas Savienības Kiberdrošības aģentūra (ENISA), kas sadarbojas ar ES dalībvalstīm un iestādēm un palīdz Eiropai gatavoties kiberdrošības nākotnes izaicinājumiem.

1. Dokumentu izpēte par profesionālo izglītības iestāžu pedagogu digitālajām prasmēm

Vācija:

- Profesionālās izglītības un apmācību (VET) datu pārskatā (2019), ko izstrādājis Vācijas Federālais profesionālās izglītības un apmācības institūts (BIBB), "digitalizācija" tika iekļauta starp 3 galvenajām profesionālās izglītības profesiju un profesionālās izglītības un apmācību tendencēm.
- Proti, ziņojumā teikts, ka „Digitalizācija pastiprinās darba tirgus strukturālās izmaiņas", kas norāda uz nepieciešamību mainīt apmācību kapacitāti attiecīgajās jomās. Rezultātā Vācijas, kā arī Eiropas darba tirgū nākotnē būs īpaši nepieciešami augsti kvalificēti speciālisti.
- Kā norādīts Izglītības un kultūras ministru pastāvīgās konferences (2016-2017) rezolūcijā – "Bildung in der digitalen Welt" (Izglītība digitālajā pasaulē) – profesionālās izglītības jomā, ar nodarbinātību saistīto kompetenču veicināšana digitālā darba un biznesa procesu kontekstā ir pedagogu kompetences neatņemama sastāvdaļa kā viņu didaktiskās darbības sākumpunkts.
- Kopš 2015.g. Federālā Izglītības un pētniecības ministrija (BMBF) un Federālais profesionālās izglītības un apmācības institūts (BIBB) risina pētniecības, attīstības un prakses jautājumus, kas saistīti ar darba vides un profesionālās izglītības un apmācību (VET) digitālo transformāciju.

Īrija:

- Viena no Īrijas galvenajām stratēģijām attiecībā uz profesionālās izglītības un apmācību pedagogu digitālajām prasmēm ir Nacionālā digitālā stratēģija, kas tika uzsākta 2013. gada jūlijā.

- Stratēģija ir vērsta uz iesaistīšanos digitālajā jomā un uzsver, kā Īrija var gūt labumu no digitāli iesaistītas sabiedrības.
- Stratēģijā ir izklāstīts skaidrs redzējums par Īrijas digitālo attīstību, īstenojot vairākas praktiskas darbības, lai palīdzētu palielināt to iedzīvotāju un uzņēmumu skaitu, kuri iesaistās tiešsaistē caur rūpniecību un uzņēmumiem, pilsoņu apmācību, skolām un izglītību.
- Attiecībā uz profesionālās izglītības un apmācību pedagogu digitālajām prasmēm joprojām ir pierādījumi, ka pastāv lielāka atšķirība starp pedagogiem, kuri savā klasē izmanto digitālās ierīces kā mācību līdzekli, un tiem, kuri tos neizmanto.
- Daudzi pedagogi uzskata, ka digitālās ierīces var "novērst" skolēnu uzmanību. Tajā pašā laikā, daudzi pedagogi uzskata, ka digitālās ierīces un lietojumprogrammas (aplikācijas) mācību aktivitātēs var dot iespēju izglītojamiem un atbalstīt viņus 21. gadsimta dzīves prasmju apguvē, piemēram, rēķinu apmaksa tiešsaistē/pieteikšanos darbam.

Portugāle:

- Nacionālā kvalifikāciju sistēma ir reorganizējusi profesionālo izglītību un apmācību vienotā sistēmā, kurā programmas nodrošina dubulto sertifikāciju. Profesionālā izglītība un apmācības pieaugušajiem ir valsts kvalifikāciju sistēmas neatņemama sastāvdaļa, kuras galvenie elementi ir izglītības un apmācību programmas pieaugušajiem, kā arī iepriekšējās izglītības atzīšana un apstiprināšana.
- Portugāle ir panākusi ievērojamu progresu attiecībā uz izglītības līmeni, taču tas joprojām ir zemāks par ES vidējo līmeni. 2019. gadā cilvēku ar zemu kvalifikāciju vai bez tās īpatsvars bija 50,2% un salīdzinot ar 2015.g. rādītājs ir krietni uzlabojies (73,7%).

Itālija:

- Izglītības jomā darbības galvenokārt tika veiktas, īstenojot Nacionālo digitālo skolu plānu (Piano Nazionale Scuola Digitale – PNSD).
- Šis ir Izglītības, universitāšu un pētniecības ministrijas pamatnostādņu dokuments, lai uzsāktu Itālijas skolas vispārējo inovāciju stratēģiju un pārveidotu tās izglītības sistēmu digitālajā laikmetā.
- Lielākā daļa pasākumu saistībā ar skolu personāla apmācībām ir vērstas uz sākumskolām un vidusskolām, kas pārstāv lielāko daļu skolu Itālijā, savukārt profesionālās izglītības un apmācību (VET) nozarei ir pievērsta zema uzmanība.
- Šajā sakarā tiek īstenoti projekti pēc-vidusskolas tehniskajā izglītībā un profesionālajās izglītības iestādēs (Instituti Tecnici Superiori — ITS), īpašu uzmanību pievēršot studentu prasmju stiprināšanai.
- Piemēram, 2019. gadā projektā "ITS 4.0" bija iesaistīti vairāk nekā 1170 ITS studenti un aptuveni 130 partneruzņēmumi 106 tehnoloģisko inovāciju projektos, kas koncentrējās uz tādām tehnoloģijām kā 3D drukāšana, virtuālā realitāte un lielie dati.

Spānija:

- Spānijas Digitālā stratēģija (ADpE, Agenda Digital para España), kas publicēta 2013. gadā, ir ceļvedis Eiropas Digitālajā stratēģijā uzstādīto mērķu sasniegšanai 2015. un 2020. gadā, kā arī konkrētu mērķu sasniegšanai, lai veicinātu ekonomikas un digitālās sabiedrības attīstību Spānijā. Tā ir strukturēta ap sešiem galvenajiem mērķiem un vairākiem konkrētiem plāniem. Sestais mērķis paredz digitālo iekļaušanu un lasītprasmes veicināšanu, kā arī jaunu IKT speciālistu apmācības. Šī pētījuma ietvaros vajadzētu izcelt vairākus specifiskus pasākumus:

- atjaunināt Nacionālo profesionālo kvalifikāciju katalogu IKT prasmju un apmācību ziņā un iekļaut šo atjauninājumu apmācību piedāvājumos, kas atbalsta profesionālo kvalifikāciju;
- palielināt apmācību līdzekļu pārvaldības un piešķiršanas efektivitāti nepārtrauktām apmācībām IKT jomā, gan privātajā, gan valsts sektorā strādājošajiem, īpašu uzmanību pievēršot virtuālo apmācību platformu izmantošanai;
- daļu no profesionālās izglītības un apmācību (VET) pieejamajiem resursiem novirzīt IKT profesionāļu digitālo prasmju apguvei un pilnveidošanai;
- pielāgot ar IKT saistīto profesionālo apmācību, tostarp specializācijas kursus izglītības jomā;
- veicināt augstskolu piedāvājumu pilnveidošanu, kas vērsta uz IKT profesionāļu sagatavošanu, pielāgojot tos tirgus vajadzībām, apsverot jaunus profesionālos profilus IKT jomā un palielinot sistēmas efektivitāti.

Francija:

- Aplūkojot apmācību tempu IKT izmantošanā Francijas universitātēs, mēs redzam, ka nav skaidras un noturīgas politikas pasniedzēju apmācībai par IKT/E-apmācību izmantošanu. Apmēram 58% ziņo tikai par vienu apmācības sesiju gadā, salīdzinot ar 7,4% mēnesī un 0,5% nedēļā.
- Francijas Nacionālā informācijas sistēmu drošības aģentūra (ANSSI) ir konstatējusi ļoti strauju kiberdraudu līmeņa pieaugumu Francijā. Turpinot 2019. gadā aizsākto trajektoriju, kiberuzbrukumu skaits ir pieaudzis sprādzien veidā: upuru skaits gada laikā ir reizinājies par 4.
- Statistika liecina, ka IT apmācību blīvums dažādos franču valodā runājošajos reģionos ir atšķirīgs. Tam ir vairāki iemesli, no kuriem nozīmīgākie neapšaubāmi ir saistīti ar akadēmiskajām iestādēm un to valdībām.

- Lai noskaidrotu atšķirības, reģionālie biroji vai CNF varētu veikt turpmākos pētījumus saskaņā ar vietējo vai reģionālo digitālo izglītības politiku.

Latvija:

- Lai gan šobrīd Latvijā trūkst pētījumu un datu par kiberdrošību un citām PIA un citu izglītības iestāžu pedagogu digitālajām prasmēm, ir acīmredzams, ka pāreja uz attālinātām mācībām Covid-19 krīzes dēļ daudziem pedagogiem izrādījās nopietns izaicinājums.
- Attiecībā uz nacionālajām stratēģijām un plānošanas dokumentiem jaunajā budžeta periodā (2021-2027) jāizceļ šādus aspektus:
    - Digitālo prasmju attīstība izglītības nozarē (Digitālās transformācijas pamatnostādnes 2021-2027.gadam) – kas paredz pedagogu un izglītības iestāžu vadītāju digitālo prasmju attīstību, digitālo prasmju attīstību un izmantošanu izglītības procesā, kā arī atbalstu nodarbināto digitālo prasmju attīstību;
    - Digitālo prasmju attīstība ir iekļauta pedagogu profesionālo kompetenču pilnveides programmā (Izglītības attīstības pamatnostādnes 2021-2027.g.). 2020. gadā LR Izglītības un zinātnes ministrija par prioritāru mērķi saistībā ar profesionālo kompetenci izvirzījusi pedagogu digitālās kompetences pilnveidi, piešķirot šim mērķim papildu finansējumu (0,5 milj. EUR);
    - Nepieciešamība palielināt izglītojamo un pedagogu izpratni par informācijas drošību, privātuma aizsardzību un uzticamu e-pakalpojumu lietošanu (Kiberdrošības stratēģija 2019-2022. gadam, rīcības virziens "Sabiedrības izpratne, izglītība un pētniecība");
    - Sabiedrības digitālo kompetenču attīstība (Izglītības attīstības pamatnostādnes 2021-2027. gadam, Digitālās transformācijas pamatnostādnes 2021-2027. gadam), jo digitālās prasmes tagad pēc to

> nozīmes tiek pielīdzinātas lasītprasmei un rēķinātspējai, vismaz pamatlīmenī tās ir nepieciešamas ikvienam neatkarīgi no darbības jomas (digitālās prasmes = starpnozaru prasmes). Ir nepieciešams veikt pasākumus, lai izglītotu iedzīvotājus par digitālajām pamatprasmēm, medijpratību un informācijas pratību, kas ietver visu pamatprasmju kopumu, tostarp kiberprasmes;

Uzmanība, kas ziņojuma ievadā tiek pievērsta DESI indeksam, ir pamatota ar precizitāti, ar kādu tas raksturo Eiropas valstu situāciju un atšķirības. Šādu precizitāti apstiprina arī atsevišķie valstu ziņojumi par profesionālā izglītības līmeņa pedagogu digitālajām prasmēm.

Mēs uzskatām, ka ir noderīgi salīdzināt divas konsorcija valstis ar zemākajiem un augstākajiem rādītājiem, lai saprastu kā dažādi digitālo prasmju līmeņi ietekmē valsts iedzīvotājus un jo īpaši profesionālā līmeņa pedagogus. Tāpēc vispirms tiks apskatīta Īrija, kas DESI klasifikācijā ieņem 6.vietu.

Saskaņā ar 2018. gada Īrijas Centrālās statistikas biroja (CSO) datiem 89% mājsaimniecību ir piekļuve internetam. Turklāt vairāk nekā 30% no visiem ES datiem tiek glabāti Īrijā, kur atrodas daudzu pasaules lielāko tehnoloģiju uzņēmumu galvenā mītne. Abu radītāju kopā skatīšana liek saprast, ka kiberdrošības gatavībai ir izšķiroša nozīme. Šīs ziņojums balstās uz galvenajiem tiesību aktiem, kas pastāv Īrijā, gan attiecībā uz digitālo pratību, gan kiberdrošību. Tā kā pasaule turpina pielāgoties "dzīvei ar COVID-19", ir svarīgi nodrošināt to, lai kibernoziedzības apkarošanas ainava un labākās prakses modeļi turpinātu ietekmēt politiku un praksi.

Viena no Īrijas galvenajām stratēģijām attiecībā uz digitālajām prasmēm ir Nacionālā digitālā stratēģija, kas tika uzsākta 2013. gada jūlijā. Stratēģija ir vērsta uz iesaistīšanos digitālajā jomā un uzsver, kā Īrija var gūt labumu no digitāli iesaistītas sabiedrības.

Stratēģijā ir izklāstīts skaidrs redzējums (vīzija) par Īrijas digitālo attīstību, īstenojot vairākas praktiskas darbības, lai palīdzētu palielināt to iedzīvotāju un uzņēmumu skaitu, kuri iesaistās tiešsaistē, izmantojot rūpniecību un uzņēmumus, pilsoņu apmācību, skolas un izglītību. 2021. gadā izglītības ministre Norma Folija (Norma Foley) paziņoja par jaunas Digitālās stratēģijas izstrādi sākumskolām. Stratēģijā ir paredz galvenokārt koncentrēšanos uz digitālo tehnoloģiju izmantošanu izglītībā un mācīšanas procesa uzlabošanu, integrējot tehnoloģijas nākotnē. Īrijas augstākās izglītības jomā viens no ievērojamākajiem sasniegumiem ir 2015–2017.g. Ceļvedis digitālajām mācībām augstākajā izglītībā, kas tika izstrādāts, lai atbalstītu "koordinētu, daudzlīmeņu pieeju digitālās pratības, prasmju un pārliecības veicināšanai studentu vidū visos izglītības līmeņos".

Attiecībā uz tālākizglītību un apmācībām tika izveidots salīdzinoši jauns Īrijas valdības (Government of Ireland) Tālākizglītības un augstākās izglītības, pētniecības, inovāciju un zinātnes departaments. Departamenta trīs gadu stratēģijā galvenā uzmanība tiek pievērsta digitālajām prasmēm un tās mērķis ir īstenot jaunu 10 gadu stratēģiju, lai uzlabotu lasītprasmi, rēķināšanu un digitālās prasmes. Papildus departaments koncentrējas uz prasmju apmācību reformu un ieguldījumiem digitālo prasmju veicināšanā. Attiecībā uz profesionālā izglītības līmeņa pedagogu digitālajām prasmēm, fakti joprojām liecina, ka pastāv palielināta atšķirība starp pedagogiem, kuri savā klasē izmanto digitālās ierīces kā mācību līdzekli, un tiem, kuri tās neizmanto.

Vairākuma pedagogiem varētu šķist, ka digitālās ierīces var "provocēt skolēnu uzmanības novēršanu". Tomēr realitātē ir pretēji – daudzi pedagogi tic, ka digitālās ierīces un aplikācijas mācību procesā var dot iespējas un atbalstīt audzēkņus 21.gs. dzīves prasmju apgūšanā, piem., rēķinu apmaksa tiešsaistē, pieteikšanās darbam. No Īrijas viedokļa ir vērts pieminēt pēdējo starpvaldību stratēģiju - Īrijas 2018. gada Nākotnes darba iniciatīva (Future Jobs Initiative), kas uzsver mūžizglītības filozofiju. Divas no piecām stratēģijas galvenajām tēmām fokusējās uz "inovācijām un

tehnoloģijām, tostarp gatavošanos pārejai uz digitālo ekonomiku". Stratēģijai ir centrālā nozīme diskusijās par nepieciešamību veikt turpmākus pētījumus un ieguldījumus digitālo prasmju jomā.

Šāda kopīga atzinība un izpratne par digitālajiem rīkiem liecina, ka Īrija ir viena no vadošajām valstīm digitālo tehnoloģiju integrācijas ziņā. Savukārt Itālijas kontekstā šādas digitālās integrācijas rezultāts ir viens no galvenajiem problēmjautājumiem. Itālijā mazāk nekā pusei iedzīvotāju ir pamata digitālās prasmes, bet IKT speciālistu īpatsvars, kas veido tikai 1% no Itālijas absolventiem, joprojām ir zem ES vidējā rādītāja, lai gan pēdējos gados tas ir palielinājies.

Saskaņā ar 2013.g. Ekonomiskās sadarbības un attīstības organizācijas (OECD) starptautisko pētījumu par mācību vidi TALIS (Teaching and Learning International Survey), Itālija ieņem pirmo vietu attiecībā uz pedagogu IKT apmācību vajadzībām. Vismaz 36% Itālijas pedagogu paziņoja, ka nav pietiekami sagatavoti pasniegšanai digitālajā vidē, salīdzinot ar OECD vidējo rādītāju – 17%, kas liecina par specializēto apmācību nepieciešamību.

Saistībā ar politiskas plānošanu dažos pēdējos gados Itālija ir iekļāvusi digitālo prasmju veicināšanas pasākumus vairākās nozaru stratēģijās. Izglītības jomā aktivitātes galvenokārt tiek īstenotas izmantojot Nacionālo digitālo skolu plānu (Piano Nazionale Scuola Digitale – PNSD), kas ir Izglītības, universitāšu un pētniecības ministrijas vadlīniju dokuments par vispārējas inovācijas stratēģijas uzsākšanu Itālijas skolās un tās izglītības sistēmas jaunai pozicionēšanai digitālajā laikmetā.

Tas ir La Buona Scuola (likums Nr. 107/2015) pamatpīlārs – darbības redzējums, kas atspoguļo valdības nostāju attiecībā uz svarīgākajiem valsts sistēmas inovācijas izaicinājumiem, un šīs vīzijas centrā ir skolu sistēmas inovācija un digitālās izglītības iespējas.

PNSD noteiktās intervences jomas ir: piekļuve, telpas un mācību vide, digitālā administrācija, digitālā identitāte, studentu prasmes, uzņēmējdarbība un darba tirgus, digitālais saturs, personāla apmācība. Attiecībā uz pēdējo punktu PNSD norāda, ka pedagogu apmācībām jābūt vērstam uz izglītības inovāciju, ņemot vērā digitālās tehnoloģijas kā atbalstu jaunas izglītības paradigmas ieviešanai un operatīvai pasākumu plānošanai. Šīs pasākuma mērķi:

- Stiprināt personāla sagatavotību digitālo prasmju jomā, sasniedzot visu "skolas kopienu";
- Veicināt sasaisti starp izglītības inovāciju un digitālajām tehnoloģijām;
- Laika gaitā izstrādāt efektīvus, ilgtspējīgus un ilgstošus standartus apmācībām izglītības inovācijas jomā;
- Stiprināt apmācības izglītības inovācijas jomā visos līmeņos (sākotnējā, ienākošajā, aktīvajā).

Lai veicinātu skolotāju apmācību IT priekšmetos, ar mācību iestādēm tika parakstīts sapratnes memorands (Memoranda of Understanding) un piešķirti finanšu līdzekļi, lai veicinātu dalību kursos, piemēram:

- Sapratnes memorands Nr. 785, 2021. g. 22. janvāris, starp Izglītības ministriju un korporāciju Cisco "Inovācijas un digitālo prasmju uzlabošana skolās" un apmācību programmu "Savienoti un droši skolotāji" ("Connected and safe teachers").
- Sapratnes memorands Nr. 4, 2020. g. 28. oktobris, starp Izglītības ministriju un S.O.S. Telefono Azzurro ONLUS (NVO) par kopīgu izglītības un apmācības pasākumu īstenošanu, lai veicinātu izglītību digitālajai sabiedrībai un apzinātu digitālo tehnoloģiju, sociālo mediju un apmācību kursus izmantošanu skolotājiem.

Līdz šim lielākā daļa ar skolu personāla apmācību saistīto pasākumu bija vērsti uz pamatskolām un vidusskolām, kas veido lielāko Itālijas skolu daļu, savukārt profesionālās izglītības un apmācības (VET) nozarei ir pievērsta nepietiekama uzmanība.

Šajā sakarā projekti tiek īstenoti pēc-vidusskolas tehniskas izglītības un profesionālo izglītības institūtu (Istituti Tecnici Superiori – ITS) ietvaros, īpašu uzmanību pievēršot studentu prasmju stiprināšanai. Piemēram, 2019. gadā projektā "ITS 4.0" bija iesaistīti vairāk nekā 1170 ITS studenti un aptuveni 130 partneruzņēmumi 106 tehnoloģisko inovāciju projektos, kas fokusējās uz tādām tehnoloģijām kā 3D drukāšana, virtuālā realitāte un lielie dati.

Vēl viens rīks, kas veicinās digitālo prasmju apguvi, ir iekļauts Nacionālajā atveseļošanas un noturības plānā (Piano Nazionale di Ripresa e Resilienza – PNRR) ar 750 miljardu EUR finansējumu. Gandrīz puse no tā veido dotācijas, par kurām vienojusies Eiropas Savienība, reaģējot uz pandēmijas krīzi. PNRR veicinās skolu personāla digitālo prasmju attīstību, lai nodrošinātu pieejamu, iekļaujošu un inteliģentu pieeju digitālajai izglītībai.

Galvenais mērķis ir izveidot digitālo prasmju ekosistēmu, kas spēs paātrināt skolu organizācijas un mācīšanas procesu digitālo transformāciju saskaņā ar Eiropas Iedzīvotāju digitālās kompetences ietvaru DigComp 2.1 un DigCompEdu (pedagogiem). Šī darbības virziena īstenošanu nodrošina Izglītības ministrija, un tajā būs iesaistīti aptuveni 650 000 cilvēku, tostarp skolotāji un skolas darbinieki, un vairāk nekā 8 000 izglītības iestāžu. Valdība plāno stiprināt profesionālo izglītību, jo īpaši augstākās profesionālās izglītības sistēmu (ITS) un STEM izglītību, īpašu prioritāti izvirzot dzimumu līdztiesībai.

Iepriekš minētie piemēri atspoguļo divus dažādus valstu kontekstus. Lai iegūtu tuvāku norādi uz vispārējo Eiropas sistēmu, ir lietderīgi analizēt digitālo prasmju ainavu Francijā, kuras DESI indekss ir ļoti tuvs Eiropas vidējam rādītājam.

Francijas Nacionālā informācijas sistēmu drošības aģentūra (ANSSI) norādījusi ļoti strauju kiberdraudu līmeņa pieaugumu Francijā. Turpinot 2019. gadā iesākto

trajektoriju, strauji pieaudzis kiberuzbrukumu skaits, kur gada laikā upuru skaits ir četrkāršojies. Tas ir īpaši satraucoši, jo īpaši situācijā, kad jebkuram kiberuzbrukumam var būt pastiprinošas sekas veselības krīzes dēļ. Kiberrisku izpratnes trūkums, informācijas sistēmu kontroles trūkums, datoru higiēnas pasākumu neievērošana, kiberdrošības ekspertu trūkums un zināmā mērā uzbrukuma virsmas palielināšanās sakarā ar plašo attālinātā darba iespēju izmantošanu – ir vājās vietas, ko izmanto kibernoziedznieki. Uzbrukuma kampaņas, kas 2020. gadā skāra Franciju, veiksmīgi izjauca daudzu uzņēmumu darbību un radīja ievērojamus finansiālus zaudējumus. Digitālo ārpakalpojumu masveida izmantošana, kas bieži vien ir mazāk droša, ir plaši izplatīta prakse, ko uzbrucēji nebaidās izmantot. Statistika liecina, ka IT apmācību blīvums dažādos franciski runājošajos reģionos ir atšķirīgs un tam ir vairāki iemesli. No tiem nozīmīgākais neapšaubāmi ir saistīts ar akadēmiskajām iestādēm un to vadītājiem. Turpmākus pētījumus, lai noskaidrotu atšķirību, reģionālie biroji vai CNF varētu veikt vēlākā posmā saskaņā ar savu vietējo vai reģionālo digitālās izglītības politiku. Apmācību statistika liecina, ka arī rīkoto apmācību tematiskās vajadzības dažādos reģionos atšķiras. Tematiskais biežums šajā ziņā ir atkarīgs arī no endogeniem faktoriem, kas saistīti ar pieprasījumu un piedāvājumu atbilstoši vietējo partneru vajadzībām un attīstības līmenim IKT/E un ODL (Open Distance Learning) jomās.

2. Dokumentu izpēte par galvenajiem digitālās drošības jautājumiem partneru valstīs

Vācija:

- Lai analizētu Vācijas kontekstu un veiktu vajadzību analīzi, īpaši nozīmīgs ir 2020. gada digitālā barometra apskats, kas ir reprezentatīva privātpersonu tiešsaistes aptauja par kiberdrošību, ko kopīgi īstenoja BSI un Vācijas Federatīvā Republika un Vācijas Federālās policijas Noziedzības novēršanas komisija.
- Pēdējos gados Vācijas un Eiropas vidē kibernoziedzība ir bijis galvenais neseno kiberuzbrukumu cēlonis. 2020. gada Federāla informācijas drošības biroja (BSI) ziņojums apstiprināja datu noplūdes un kritiskas ievainojamības, kas konstatētas programmatūras un aparatūras produktos. Šis pētījums ir arī konstatējis masveida kibernoziegumu pieaugumu, kas vērsts pret privātpersonām, komercuzņēmumiem un citām iestādēm, kas izmanto ļaunprātīgu programmatūru.
- Visizplatītākā ļaunprogrammatūras izmantotā ievainojamība ir resursdatora sistēmas (host system) ievainojamība. Programmatūras vai aparatūras produktu gadījumā ievainojamības var atrast vārtejās, piemēram, tajās, kas darbojas starp birojiem vai ražošanas tīkliem, vai arī tās var izraisīt cilvēku kļūdīšanās sociālajā inženierijā.
- Šāda digitalizācijas pakāpe nav bez riskiem un briesmām. Katrs ceturtais respondents ziņoja, ka pēdējā gada laikā ir bijis kibernoziegumu upuris. Kopējais kibernoziedzības līmenis 2020. gadā paliek nemainīgs. Iepirkšanās tiešsaistē un trešo pušu piekļuve tiešsaistes kontiem ir visizplatītākie krāpšanas veidi, kas skar upurus - attiecīgi (44%) un (30%).

Neskatoties uz secinājumiem, divas trešdaļas aptaujāto izteica vēlmi pēc plašākas informācijas par datu zādzību novēršanu (66%). Visbiežāk meklētie padomi ir saistīti ar praktiskiem padomiem, piemēram, veidiem, kā nodrošināt drošas paroles vairākiem tiešsaistes kontiem (59%). Tam seko padomi par to, kura programmatūra ir vispiemērotākā tiešsaistes kontu aizsardzībai (52%) un padomi par paroļu pārvaldīšanas plusiem un mīnusiem (49%).

Īrija:

- Kiberdrošības apdraudējumi Īrijā turpina pieaugs – vienam no nesenajiem kiberdrošības uzbrukumiem Īrijas veselības aprūpes dienestam (HSE), kas notika 2021. gadā, joprojām ir postoša ietekme uz Īrijas veselības aprūpes sistēmu.
- Īrijā glabājās vairāk nekā 30% no ES datiem, jo valstī atrodas daudzu kiberdrošības centru galvenās mītnes. No vienas puses tas sniedz virkni iespēju, no otras – palielina kibernoziedzības draudu līmeni. Tā kā Īrija pārstāv atvērto liberālo demokrātiju, tā tiek uzskatīta par īpaši neaizsargātu pret tā sauktajiem "hack and leak" veida uzbrukumiem.
- Īrijas otrā nacionālā kiberdrošības stratēģija (2019.–2024. gadam) tika uzsākta, lai palielinātu valsts gatavību kiberdrošībai. Stratēģijas galvenie mērķi ir:
    - nodrošināt Īrijas kiberdrošības gatavību, un spēju reaģēt un pārvaldīt kiberdrošības incidentus, tostarp saistītus ar valsts drošību,
    - aizsargāt no kiberuzbrukumiem un pārvaldīt jebkādus pakalpojumu traucējumus, kas saistīti ar kritisko valsts infrastruktūru,
    - turpināt attīstīt un celt kiberdrošības nozari Īrijā un būt gatavam kiberdrošībai,

- Īrijas uzņēmumos ieviest labākās starptautiski pieejamās tehnoloģijas un pasākumus,
- Palielināt organizāciju un privātpersonu izpratni par kiberdrošību un attīstīt ar to saistītas prasmes.

- 2018. gadā tika uzsākts Rīcības plāns drošībai tiešsaistē un tajā ir ietvertas 25 darbības zem pieciem galvenajiem mērķiem, kas vērstas uz noziedzīgu nodarījumu likumdošanas veicināšanu saistībā ar kibernoziegumiem, nelegāla un kaitīga materiāla novēršanas un tiešsaistes drošības veicināšanu.

Portugāle:

- Galvenās digitālās drošības tēmas, kuram jāpievērš uzmanība:
  - Pamatlīmenī
    - Noteikt savas skolas infrastruktūras un lietojumprogrammu ievainojamību tiešsaistes vidē un veikt riska mazināšanas pasākumus (gan strukturālos, gan uzvedības veidus);
    - ievainojamību identificēšana un novēršana;
    - Identificēt personisko informāciju internetā, kas var būt izmantot uzbrukumam;
    - Apgūt atbilstošu uzvedības veidu kopumu kibertelpas izmantošanā
  - Vidējais un augstākais līmenis:
    - Drošības programmēšanas tehniskās vides
    - Sociālā inženierija
    - Atvērto datu avotu izpēte
    - Bezvadu tīkli
    - Šifrēšana un paroles

Itālija:

- Visplašāk izplatītā drošības jomas problēma pēdējo trīs gadu laikā ir paroļu pikšķerēšana, kā norāda 48% Itālijas uzņēmumu vadītāju, salīdzinot Eiropas uzņēmumu vadītājiem (36%). Turklāt 28% Itālijas vadītāju saskaras ar problēmām saistītām ar piekļuvi un identitāti (atbilstoši Eiropas procentuālajam rādītājam), kam seko problēma saistīta ar sociālās inženierijas ļaunprātīgo programmatūru (24%).
- Turklāt tikai 42% iedzīvotājiem vecumā no 16 līdz 74 gadiem ir digitālās pamatprasmes, un IT/IKT jomas absolventu īpatsvars salīdzinājumā ar Eiropas datiem ir ļoti zems.
- Jautājumu par digitālajām prasmēm valdība risina piecu gadu ilgajā inovāciju un digitalizācijas stratēģijā "Italia 2025", kas uzsākta 2019. gadā. Jo īpaši iniciatīvas "Digitālā Republika" ietvaros, ko īsteno un koordinē Tehnoloģiju inovāciju un digitalizācijas ministrija.
- Iniciatīvas mērķis ir izveidot aliansi starp publiskām un privātām organizācijām, kā arī iedzīvotājiem, un aicināt viņus veikt konkrētus pasākumus digitālo prasmju veicināšanai. Tā koncentrējas uz trim darbības virzieniem:
    - digitālo pamatprasmju uzlabošanu;
    - darbaspēka kvalifikācijas paaugstināšanas un pārkvalificēšanas veicināšanu;
    - IKT un jauno tehnoloģiju prasmju attīstību.
- Nākamais solis uz priekšu tiks sperts, izmantojot stratēģiju "Italia digitale 2026", kas nosaka piecus ambiciozus mērķus sasniegšanai nākamajos gados:
    - popularizēt digitālo identitāti – nodrošinot, ka to izmanto 70% iedzīvotāju;
    - digitālo prasmju atšķirību mazināšana – vismaz 70% iedzīvotāju spējīgi izmantot digitālos pakalpojumus;
    - ~ 75% no Itālijas publiskās administrācijas izmantot mākoņpakalpojumus;

- Sasniegt vismaz 80% būtisku sabiedrisko pakalpojumu, kas tiek sniegti tiešsaistē;
- Sadarbībā ar Mise sasniegt (nodrošināt) 100% Itālijas ģimeņu un uzņēmumu ar ultraplatjoslas tīkliem.

Spānija:

- Spānijas nodarbinātības aktivizēšanas stratēģijas 2017.–2020. gadam (Spain's Activation Strategy for Employment 2017-2020) mērķis ir konsolidēt ekonomikas atveseļošanos, veicinot kiberdrošības programmas un nodrošinot resursus profesionālās izglītības iestādēm, lai risinātu pašreizējā un nākotnes darba tirgus izaicinājumus, kas izriet no globalizācijas un digitalizācijas. Tajā noteikti pasākumi, kas valsts un reģionālā līmenī jāveic Valsts nodarbinātības dienestiem (Public Employment Services - PES);
- Kvantitatīvā izteiksmē viens no mērķiem ir digitālo prasmju apmācība vismaz 225 000 jauniešiem: 75% pamatprasmēs un 25% progresīvās digitālajās prasmēs (ar priekšzināšanām), kas veido attiecīgi 40% un 38% no visiem jauniešu vecumā līdz 30 gadiem.
  - atbalsts jaunām sievietēm tehnoloģijām balstītu jaunuzņēmumu (start-up) uzsākšanai, nodrošinot konsultācijas ar padomiem par viņu biznesa plānu un piedāvājot uzraudzības pakalpojumus;
  - specifiskās apmācības jaunām sievietēm no lauku apvidiem IKT tehnoloģijās un jaunās nākotnes nozarēs, izmantojot jauno tehnoloģiju iespējas, pedagogus un trenerus, tostarp tiešsaistes mācības;
  - uzņēmējdarbības, pašnodarbinātības un jaunu darba iespēju veicināšana, ko piedāvā digitālā ekonomika un dažādas sociālās ekonomikas formulas un digitālo platformu ekonomika nodarbinātības aktivizēšanas politikas ietvaros;

- labo prakšu redzamības uzlabošana, kas izstrādātas, lai izprastu, kādas ir galvenās kiberdrošības tēmas.

- Jaunatnes nodarbinātības valsts darbības programma (budžets 39 milj. EUR). Piemēram, programmā ir iekļaut apmācību veidi par digitālo transformāciju nodarbinātībai.
- Projekts, ko īsteno EOI partnerībā ar Google, ir vērsts uz to jauniešu nodarbinātības uzlabošanu, kuri jau no agras bērnības ir pametuši skolu, zaudējuši darbu vai kuriem ir grūtības atrast pirmo darbu.

Francija:

- 2015. gada 5. jūnijā Franciski runājošās kopienas augstākās izglītības ministri tikās Parīzē kopīgas OIF (Organisation internationale de la francophonie) un AUF (Agence universitaire de la francophonie) iniciatīvas ietvaros, lai pārbaudītu franču valodā runājošo universitāšu un profesionālo izglītības un apmācību iestāžu digitālās attīstības situāciju un perspektīvas.
- Šī darba galvenais mērķis bija sniegt ieguldījumu frankofonijas stratēģijas izstrādē pasniedzēju apmācībai digitālās izglītības jomā un novērtēt attiecīgo mērķa grupu apmācību vajadzības un gaidas, lai noteiktu, kas ir nepieciešams šo vajadzību apmierināšanai - pakalpojumu, satura un kompetenču ziņā.
- Saskaņā ar pētījumu "Étude sur l'identification des besoins en formation tic/e dans les pays francophones du sud, 2016", pasniedzēju-pētnieku vajadzības raksturo izteikta tendence pēc IKT/E-apmācībām un kapacitātes palielināšanas saistībā ar digitālo izglītību (80,4%).
- Digitālie riski ir ļoti aktuāli jauno pasniedzēju starpā, kuri viegli pārraida mediju diskursu. Trīs riski, ar kuriem pasniedzēji visvairāk saskaras personīgi, ir tehniskie (66,20%), ētiskie un juridiskie (55,80%) un informatīvie riski (54,70%).

Latvija:

- Saskaņā ar nacionālo kiberdrošības stratēģiju 2019-2022, Latvijas kibertelpa turpina saskarties ar liela mēroga draudiem – pikšķerēšanas, izspiedējvīrusu un ļaunatūru izplatības kampaņām; mēģinājumiem uzlauzt sistēmas, tīklus un tīmekļa vietnes; piekļuves lieguma uzbrukumiem (DoS) kritiski svarīgām informācijas sistēmām, kā arī krāpnieciskas e-pasta un sociālās inženierijas kampaņas, kuru mērķis ir izgūt personu vai autentifikācijas datus konkrētas personas, uzņēmuma vai iestādes diskreditēšanai vai noziegumu veikšanai.
- gan Latvijā, gan Eiropā ir aktuāli naudas izspiešanas mēģinājumi, kas primāri vērsti pret finanšu institūcijām kā arī citiem privātā sektora uzņēmumiem. Uzbrucēji draudot apturēt uzņēmuma tīmekļa vietnes vai citu resursu darbību ar uzbrukumu līdz pat 2 Tb/s, ja netiks veikta izpirkuma samaksa, īstenoja testa uzbrukumu sērijas (Do Sand DDoS).
- 2021. gadā krāpšanas centieni, ļaunprogrammatūra un ievainojamības joprojām bija aktīvas – WhatsApp kontu nozagšana, izmantojot aktivizācijas kodus, ko pieprasīja uzlauztie konti no personas kontaktu saraksta; jauns šantāžas e-pastu vilnis (seksuālā rakstura izspiešana (sextortion)) – draudi izplatīt kompromitējošus materiālus, ja e-pasta lietotājs neveiks izpirkuma maksu.
- 2020. gads ar globālajām pārmaiņām ir pierādījis, ka profesionālo izglītības un apmācību (VET) un citu izglītības iestāžu pedagogiem ir svarīgas zināšanas/prasmes par drošu attālināto darbu, organizējot tiešsaistes nodarbības un izmantojot digitālos rīkus (e-pastu, WhatsApp, mācību platforma, utt.), kā arī būt informētiem par aktuālajiem krāpniecību veidiem un draudiem, īpaši sociālajos medijos, lai palielinātu savu skolēnu un studentu izpratni.

Lai gan saikne starp COVID-19 pandēmiju un kiberuzbrukumu skaitu plašākai sabiedrībai nav uzreiz skaidra, patiesībā pirmais ir izraisījis otrā gadījumu skaita pieaugumu. Kibernoziedznieki ir ļoti elastīgi, kad runa iet par jaunu notikumu izmantošanu, kā to parādīja nesena ārkārtas situācija veselības jomā. Daudzi uzņēmumi šogad pārgājuši uz savām pirmajām digitālajām stratēģijām (tostarp – attālinātā darba veidu), neapzināti pavērot sevi virknei jaunu uzbrukuma vektoru, ko noziedznieki ir ātri izmantojuši.

Valstu biroji piedāvā daudzpusīgu skatījumu uz galvenajiem digitālās un kiberdrošības jautājumiem. Tā kā attālinātās mācības kļūst par jaunu normu, kibernoziedznieki atrod jaunus veidus, kā izmantot tādus paņēmienus kā pikšķerēšana, izpirkuma programmatūra (ransomware), sociālā inženierija utt., lai uzsāktu savus uzbrukumus. Zemāk tiek apskatīti daži no vissvarīgākajiem riskiem.

1. Droša attālā piekļuve

Tā kā attālinātais mācību veids pārņem klātienes mācības, skolēniem un pedagogiem ir nepieciešama piekļuve tiešsaistes mācību rīkiem, kas galvenokārt atrodas mākonī, t.i., failu apmaiņas lietojumprogrammām, e-pastiem, lietojumprogrammām, un dažreiz viņiem ir nepieciešams attālināti piekļūt resursiem mācību iestāžu tīklā. Ja attālinātā piekļuve nav droša, hakeri var iekļūt sistēmā un pārņemt kontroli pār visu tīklu.

2. Piekļuve sensitīviem datiem

Izglītības iestādes ir sensitīvu datu dārgumu krātuve, ko var pārdot tumšajā tīmeklī. Studentu, pedagogu, absolventu un administratīvā personāla personas dati, kā arī sensitīvi dati saistīti ar skolas pētniecību un intelektuālo īpašumu, hakeriem var būt īsta dārgumu krātuve, ko pārdot vai izpirkt. Tāpēc ir būtiski ieviest uz identitāti balstītu piekļuvi, ļaujot autorizētiem lietotājiem piekļūt tikai tiem resursiem, kas tiem nepieciešami sava darba veikšanai.

3. Ļaunprātīga programmatūra

Pāreja uz attālinātajām mācībām nozīmē, ka daudzas skolas tīklam pievienotās ierīces ir BYOD (Bring Your Own Device) jeb "paņemiet savas ierīces līdzi". Ir grūti pārliecināties, vai izmantotās ierīces, lietojumprogrammas un antivīrusi ir regulāri atjaunināti. Tiklīdz šīs attālinātās ierīces ir pieslēgtas caur VPN, ir nepieciešams pārliecināties, vai tās ir drošas, pirms tās var piekļūt resursiem mācību tīklā. Ir svarīgi izmantot uzlabotas tīmekļa aizsardzības iespējas, kas var identificēt un bloķēt iespējamos tīmekļa draudus.

4. Pikšķerēšana

Sociālā inženierija un pikšķerēšanas uzbrukumi ir galvenais kiberdrošības risks Francijas mācību centriem. Pedagogi, treneri vai darbinieki, kuri tiek vilināti noklikšķināt uz ļaunprātīgām saitēm, var nodrošināt kibernoziedzniekiem piekļuvi mācību iestāžu tīklam un vērtīgiem resursiem. Labākais veids, kā cīnīties pret sociālās inženierijas un pikšķerēšanas uzbrukumiem, ir lietotāju informētība un apmācība. Lietotāju apmācība un testēšana ar simulētiem uzbrukumiem palīdzēs veidot pozitīvu drošības izpratnes kultūru un padarīs viņus mazāk neaizsargātus pret dažādām tiešsaistes krāpniecībām.

5. Krāpšana

2020. gads tiek ziņots kā ļoti intensīvs krāpšanu periods, tostarp sociālās inženierijas uzbrukumiem. Aktīvākie krāpšanas mēģinājumi bija izspiešanas kampaņas, kur hakeri apgalvoja, ka ir uzlauzuši lietotāja ierīci un ieguvuši kompromitējošus materiālus, nosakot izpirkuma maksu; krāpnieciskas loterijas atpazīstamo zīmolu vārdā, piedāvājot laimēt jaunākos viedtālruņus vai citas vērtīgas balvas.

Tika novērota jauna tendence – e-pastu izspiešana ar datu nopludināšanas draudiem. Daudzos gadījumos uzbrukumi tika vērsti uz uzņēmumiem. Maldinošas reklāmas sociālajos tīklos – slavenu cilvēku vārdu izmantošana bez viņu zināšanas, aicinot interneta lietotājus investēt kriptovalūtā. Krāpnieki arī zvanīja un mēģināja pārliecināt

cilvēkus investēt. Atsevišķos gadījumos tika novēroti atkārtoti krāpšanas mēģinājumi, kur finanšu krāpniecībā cietušajiem tika piedāvāta palīdzība, lai atgūtu zaudētos līdzekļus.

Telefona krāpniecība – viltojot dažādu kredītiestāžu tālruņu numurus un uzdodoties par banku pārstāvjiem, krāpnieki, izmantojot iedzīvotāju sliktās zināšanas par papildu autentifikācijas metodēm, ieguvuši finanšu līdzekļus no vairākiem tūkstošiem lietotāju, nodarot Latvijas kredītiestādēm kopējos zaudējumus simtiem tūkstošu vērtībā.

Hakeru pielāgošanās nepieciešamībai uzsākt attālināto darbu – ņemot vērā uzņēmumu nepieciešamību strauji pāriet uz attālinātā darba režīmu un elektronisko dokumentu aprites ieviešanu, hakeri izmantoja situāciju, lai pielāgotu savus uzbrukuma veidus - piem., vairāki uzņēmumu grāmatveži saņēma e-pastus direktora vai cita darbinieka vārdā par nepieciešamību veikt steidzamu maksājumu vai mainītu algas kontu.

Iejaukšanās uzņēmumu lietišķajā sarakstē – kompromitējot uzņēmumu vai to sadarbības partneru e-pastus, uzbrucēji varēja izvēlēties piemērotu brīdi, lai kādai no pusēm nosūtītu rēķinu ar mainītu kontu.

Krāpšana – valsts institūciju vārdā par ārkārtas stāvokli un epidemioloģisko situāciju valstī tika saņemti krāpnieciski ziņojumi ar īsinājumtaustiņiem (ej.uz), kas tika izmantoti, lai slēptu faktisko saites galamērķi.

Viltus interneta veikali – īpaši liela aktivitāte novērota svētku laikā ar sociālo mediju reklāmu starpniecību un Covid-19 ierobežojumu dēļ, kas piespiedu kārtā lika uzņēmumiem pārdot savus produktus tiešsaistē.

Ir noderīgi apskatīt dažus datus, kas sniegti nacionālajos ziņojumos. Piemēram, Francijā digitālie riski ir ļoti aktuāli jauno pedagogu vidū, kuri viegli pārraida mediju diskursu. Trīs risku veidi, kurus pedagogi izjūt visvairāk, ir tehniskie (66,20%), ētiskie un juridiskie (55,80%) un informatīvie riski (54,70%). Savukārt psihosociālie, kognitīvie un

sociālekonomiskie riski ir tie, kas uztrauc viņus mazāk. Pastāv sistemātiska neatbilstība starp pedagogu priekšstatiem par viņu riskiem un skolēnu riskiem. Skolotāju prāt, trīs riski, ar kuriem saskaras viņu skolēni – psihosociālie (69,95%), informatīvie (70,75%) un tehniskie (62,80%). Līdz ar to pedagogi jūtas tikpat neaizsargāti kā viņu skolēni attiecībā uz tehniskajiem riskiem, un uzskata, ka viņu skolēni ir vairāk ir pakļauti problēmām, kas īpaši saistītas ar uzmākšanos vai nepatiesu informāciju. Skolēnu risku palielināšanās ir izskaidrojama ar to, ka pedagogi viņus uztver kā ļoti neaizsargātus. Kāda skolotāja savus ceturtās klases skolēnus raksturoja kā ļoti neaizsargātus, diezgan naivus, kas ne vienmēr apzinās sociālo tīklu iespējamos apdraudējumus.

Vācijas Federālā informācijas drošības biroja (BSI) ziņojumā norādīts, ka vairākas kampaņas izmantoja COVID-19 radīto apjukumu un bailes, tostarp ļaunprātīgas programmatūras un pikšķerēšanas kampaņas, krāpniecības un uzbrukumi uzņēmuma vadītājiem. Turklāt BSI norādīja, ka šie notikumi iespējams palielinājuši uzbrukumu veiksmes iespējas, jo ar tiem ir saistītas bailes, uztraukums un nedrošība. Pēdējos gados Vācijas un Eiropas vidē kibernoziedzība ir bijis galvenais pēdējo kiberuzbrukumu cēlonis. Lai analizētu konkrēto Vācijas kontekstu un veiktu vajadzību analīzi, īpaši nozīmīgs ir 2020. gada digitālā barometra apskats, kas ir reprezentatīva privātpersonu tiešsaistes aptauja par kiberdrošību, ko kopīgi īstenoja BSI un Vācijas Federatīvā Republika un Vācijas Federālās policijas Noziedzības novēršanas komisija. Digitālā pāreja aktīvi veido mūsu ikdienas dzīvi – no iepirkšanās tiešsaistē līdz valkājamām ierīcēm (piemēram, fitnesa izsekošanas aproces, viedpulksteņi vai viedas brilles), jaunajiem maksājuma veidiem un ID shēmām.

Tomēr šāda digitalizācijas pakāpe nav bez riskiem un briesmām. Katrs ceturtais respondents ziņoja, ka pēdējā gada laikā ir bijis kibernoziegumu upuris. Kopējais kibernoziedzības līmenis 2020. gadā palika nemainīgs. Iepirkšanās tiešsaistē un trešo pušu piekļuve tiešsaistes kontiem ir visizplatītākie krāpšanas veidi, kas skar upurus –

attiecīgi (44%) un (30%). Lielākā daļa aptaujāto respondentu ir pārzinājusi jaunākos kiberdrošības ieteikumus kibernoziedzības novēršanai. Šie ieteikumi parasti tiek ievēroti tikai tad, ja personai ir jēga to darīt (41%) vai arī viņa tikko ir uzzinājusi par kādu konkrētu padomu (39%). Pētījumi liecina, ka cilvēki, kuri jau ir bijuši upuri vairākas reizes, visbiežāk padomu ņem vērā tikai tad, jo rodas jauna problēma (33%), pat ja viņi to jau apzinājās. Neskatoties uz konstatējumiem divas trešdaļas aptaujāto izteica vēlmi pēc plašākas informācijas par datu zādzību novēršanu (66%). Visbiežāk meklētie padomi sastāv no praktiskiem padomiem, piemēram, veidiem, kā nodrošināt drošas paroles vairākiem tiešsaistes kontiem (59%), kam seko padomi par to, kura programmatūra ir vispiemērotākā tiešsaistes kontu aizsardzībai (52%), un padomi par paroļu pārvaldnieku plusiem un mīnusiem (49%).

Vēl vienu nozīmīgu perspektīvu piedāvā Īrija – 2021.gada kiberdrošības draudi. Masveida un koordinēts uzbrukums sākās 2021. gada maijā, kad tika pārtraukta veselības aprūpes pakalpojumu un datorsistēmu darbība visā valstī – lielai daļai pacientu nozaga personas datus un turpināja pieprasīt izpirkuma maksu par datu atdošanu. Reaģējot uz to, Veselības aprūpes dienestam (HSE) bija jāslēdz slimnīcu un veselības dienestu IT sistēmas, lai aizsargātu pret jebkādu turpmāku datu zagšanu. Daudzi pakalpojumi tika traucēti, un personāla un medicīniskā informācija bija noplūdusi Īrijā glabājās vairāk nekā 30% no ES datiem, jo valstī atrodas daudzu kiberdrošības centru galvenās mītnes. No vienas puses tas sniedz virkni iespēju, no otras – palielina kibernoziedzības draudu līmeni. Tā kā Īrija pārstāv atvērto liberālo demokrātiju, tā tiek uzskatīta par īpaši neaizsargātu pret tā sauktajiem "hack and leak" veida uzbrukumiem. Parasti šie uzbrukumi tiek uzskatīti par politiski motivētiem un vērstiem uz dezinformāciju un "viltus ziņām", ko izmanto kā mēģinājumu destabilizēt valsti.

Daudzi Īrijas kiberdrošības nozares pārstāvji aicina palielināt finansējumu tādās valdības struktūrās kā Nacionālais kiberdrošības centrs (NCSC). Citi draudi/riski, kas joprojām

dominē, ir saistīti ar kritisko valsts infrastruktūru (CNI), publiskā sektora sistēmām un datiem. Sāk parādīties arī jauni izaicinājumi, kas saistīti ar 5G tehnoloģiju ieviešanu. Lai gan tās veicinās jaunu tehnoloģijas un pakalpojumu radīšanu, kiberdrošībai ir jābūt domāšanas priekšplānā.

Ārpus valsts un uzņēmējdarbības perspektīvas kiberdrošības noziegumi ikdienā joprojām notiek vidusmēra personu vidū. Tiesībaizsardzības iestādēm par tiem bieži netiek ziņots, tā piemēram, 2019.gadā Īrijas policijai it kā ziņots vien par 5% no visiem kibernoziegumiem. Turklāt 2019. gada ziņojumā, ko Īrijā pasūtīja Microsoft, ir konstatēts, ka darbinieki joprojām tiek uzskatīti par drošības "vājo posmu" sakarā ar sistēmas drošības apmācību trūkuma, sliktas paroļu pārvaldības, ar darbu saistītiem datu izmantošana kopā ar personiskajām ierīcēm un iespējamiem ES Vispārīgās datu aizsardzības regulas pārkāpumiem dēļ.

3. Labās prakses – Kiberdrošības programmas un resursi profesionālās izglītības iestādēm (VET) ES un partnervalstīs

Kā jau norādīts ievadā, projektam CYBER.EU.VET ir daudzveidīgs konsorcijs. Attiecībā uz digitālajām un kiberdrošības prasmēm konsorcija partnervalstis demonstrē dažādu efektivitātes līmeni un veiktspēju, kas augstāk tiek skaidri raksturots ar DESI indeksu. Informācijas analīze un labo prakšu izvērtēšana bija katra projekta partnera nacionālā līmenī veiktā pētniecības darba neatņemama sastāvdaļa. Šā pētījuma kopējais mērķis bija profesionālās izglītības un apmācību (VET) vajadzību analīze vietējā un valsts līmenī. Veicot šo darbu, septiņu valstu partneri saskarās ar zināmām grūtībām saistībā ar apmācību iniciatīvu un kiberdrošību meklēšanu, kas būtu paredzēta tieši VET pedagogiem. No vienas puses, tas ir padarījis uzdevumu sarežģītāku, no otras – vēl skaidrāk parādīja projekta izstrādes nozīmīgumu un vajadzību šajā jomā. Pētījums apstiprināja arī projekta CYBER.EU.VET novatorisko garu. Zemāk ir apkopotas partneru atrastas visatbilstošākās labo prakšu piemēri.

3.1 Vācija - VET 4.0 Iniciatīva

VET 4.0 ir jumtiniciatīva, ko kopš 2016.g. kopīgi īsteno Federālā Izglītības un pētniecības ministrija (BMBF) un Federālais profesionālās izglītības un apmācības institūts (BIBB), apvienojot sevī plašu projektu klāstu, balstoties uz trīs galvenajiem pīlāriem. Šīs visaptverošās iniciatīvas 2.pīlārs ir pilnībā veltīts „digitālajai pratībai/mediju kompetencei" (kas joprojām turpinās), un tā mērķis ir definēt mediju prasmes, kas būtu jāuzskata par iestāšanās prasību un par pamatprasmi visās VET profesijās (mācekļiem, pedagogiem un instruktoriem). Finansēšanas programmas, lai labāk aprīkotu mācību centrus un atbalstītu mazos un vidējos uzņēmumus (MVU), ņemot vērā digitalizāciju, papildina šo pieeju mediju kompetences veicināšanai profesionālajā izglītībā. Izmantojot īpašo ÜBS digitalizācijas programmu (71), BMBF un BIBB palīdz paātrināt mācekļu

apmācības procesu digitalizāciju "VET 4.0" kontekstā. Šī īpašā programma sastāv no diviem finansējuma virzieniem:

1) Tiek nodrošināts finansējums izvēlētu digitālo iekārtu iegādei (digitālās ierīces, mašīnas, sistēmas un programmatūras, piemēram, viedās mājas tehnoloģijas, industriālie roboti, 3D printeri un digitālie mācību līdzekļi, piemēram, planšetdatori un skārienekrāni), lai veiktu mācekļu apmācību modernizāciju, jo īpaši tiem, kurus apmāca MVU;

2) Programmas ietvaros tiek finansēti arī 8 pilotprojekti kompetences centros, kas identificē digitalizācijas ietekmi uz profesionālo darbību profiliem, kā arī nosaka prasības un no tā izrietošās sekas kvalificēta personāla kvalifikācijai un personāla apmācībām. Otrajā posmā tiek izstrādāta novatoriska mācīšanās koncepcijas VET 4.0 un tiek izplatīta caur kompetences centriem. Mērķis ir nodrošināt pārnēsājamos rezultātus un būtu plašs to lietojumu klāsts.

Daži iepriekšminēto pilotprojektu piemēri:

- "Digitālie mediji profesionālajā izglītībā", kas noslēgsies 2022. gadā, veido vairākas apakšprogrammas ar atšķirīgām finansējuma prioritātēm. Programma finansē nacionālos digitālos apmācību projektus, kas izstrādā jaunus mācību scenārijus un mūsdienīgus sākotnējās un tālākizglītības kursus, kas veicina digitālo mediju kompetences apguvi;

- "Kvalifikācijas iniciatīva digitālās pārmaiņas — Q 4.0" – kopš 2018. gada finansē tālākizglītības kursu koncepciju izstrādi un testēšanu VET pedagogiem. Projekts sastāv no diviem apakšprojektiem: 1) MIKA semināri (Mediju un IT kompetenču apmācības personālam), lai veicinātu mediju pedagoģisko pamatkompetenci, tālākizglītības moduļu izstrādi un testēšanu, lai stiprinātu apmācāmā personāla mediju un IT pamatprasmes; 2) Q 4.0 NETWORK – mērķis ir pielāgot apmācības

procesu digitālajām pārmaiņām, ņemot vērā arī reģionālās un sektorspecifiskās atšķirības. Abos projektos galarezultāts varētu būt notestēta semināra prototips, kas būtu pieejams VET darbiniekiem visā valstī;

- "Digitalizācija II" (kopš 2018. gada), kura mērķis ir noteiktu mācību procesu izstrādes stratēģijas, kas izmanto digitālo mediju potenciālu, lai atbalstītu veiksmīgu mācīšanos gan indivīdiem, gan grupām.

3.2 Francija – "Internet Sans Crainte" (Internets bez bailēm)

(Ņemot vērā to, ka Francijā trūkst labās prakses VET jomā, šīs piemērs tika izvēlēts kā prakse, kas atbilst nepieciešamajiem ierobežojumiem, bet neattiecas specifiski uz VET sektoru).

Ņemot vērā sistemātisko kibermobingu (uzbrukumus tiešsaistē), interneta atkarības, bīstamu tiešsaistes tikšanās gadījumus skaitu un to traģiskās sekas ļoti jauniem skolēniem, ir kļuvis nepieciešams pievērst ikviena uzmanību tiesībām un ierobežojumiem attiecībā uz tiešsaistes uzvedību, un, pat galvenais, prezentēt Internetu kā bagātināšanas un izklaides līdzekli brīvu no briesmām. "Tralalere", kas izveidota 2000. gadā, digitālās izglītības pionieris un jauniešu sabiedriskās komunikācijas eksperts, kā arī vadošais starpmediju izglītības programmu producents: multimediju veidošana ar multfilmu palīdzību, lietišķās spēles, mobilās lietotnes, e-grāmatas utt. Proti, Tralalere izstrādāja un vadīja nacionālo programmu, lai palielinātu izpratni par riskiem internetā: www.internetsanscrainte.fr.

Iniciatīva "Internet Sans Crainte", ko kopš 2008. gada pārvalda Tralalere, ir valsts programma, kas palīdz jauniešiem labāk kontrolēt savu digitālo dzīvi. Konkrētāk, tā piedāvā ap simts bezmaksas resursiem, lai palīdzētu pedagogiem, instruktoriem un vecākiem atbalstīt jauniešus vecumā no 6 līdz 18 gadiem, lai viņi saprātīgi un atbildīgi izmantotu ekrānus un digitālās tehnoloģijas. "Internet Sans Crainte" piedāvā arī

padomus un zināšanas par to, kā atbalstīt jauniešus digitālajā izglītībā, izmantojot tematiskos failus. "Tralalere" un "Internet Sans Crainte" koordinē arī "Safer Internet France", valsts un Eiropas programmu nepilngadīgo aizsardzībai internetā, kā arī Net Ecoute (e15 Enfance) līniju un kontaktpunktu (Point de contact). Ņemot vērā šo kapacitāti, "Internet Sans Crairnte" organizē Drošāka interneta dienu Francijā, kas ir vispasaules diena, lai veicinātu jauniešu izpratni par labāku interneta lietošanu. Šo programmu atbalsta Eiropas Komisija kā daļu no Inhope/Insafe tīkla, kurā ietilpst 38 valstis.

LABUMA GUVĒJI

"Internet Sans Crainte" piedāvā visa gada garumā digitālos resursus, kas pielāgoti dažādām auditorijām:

- Izglītības mediatoriem (skolotājiem, animatoriem, bibliotekāriem, utt.);
- Vecākiem un ģimenēm;
- Iestādēm un asociācijām.

3.3 Īrija – "Cybersafe Kids" (Kiberdroši bērni)

(Ņemot vērā to, ka Īrijā trūkst labās prakses VET jomā, šīs piemērs tika izvēlēts kā prakse, kas atbilst nepieciešamajiem ierobežojumiem, bet neattiecas specifiski uz VET sektoru).

Projekts "Cybersafe Kids" sākās 2015. gadā, un tagad ir kļuvis par atzītu labdarības organizāciju, ko finansē vairāki Īrijas filantropiskie fondi, piemēram, The Ireland Funds. "Cybersafe Kids" piedāvā vairākas apmācības programmas, kas vērstas uz kiberdrošību skolās visā Īrijas valstī. "Cybersafe Kids" vīzija ir par pasauli, kurā bērni izmanto tehnoloģijas drošā, pozitīvā un veiksmīgā veidā. Galvenās "Cybersafe Kids" ieinteresētās puses ir iesaistītās skolas visā Īrijā (skolēni, skolotāji, direktori un aizbildņi), pētniecības partneru universitātes, labdarības finansētāji un programmas īstenošanā iesaistītā komanda. Labdarības galvenais mērķis ir veicināt un nodrošināt izglītību un apmācību

bērniem, vecākiem un skolotājiem sabiedrībā, lai nodrošinātu drošu un atbildīgu navigāciju tiešsaistes pasaulē. Runājot par ietekmi, līdz šim programma "Cybersafe Kids" ir sasniegusi 24 000 bērnu vecumā no 8 līdz 13 gadiem, izmantojot savas skolas programmas. 2020. gadā vien programma sadarbojās ar 5 986 bērniem un 1 554 vecākiem 56 Īrijas skolās. Turklāt tika izplatīta anonīma tiešsaistes aptauja, kurā tika apkopoti dati no 3 764 bērniem vecumā no 8 līdz 12 gadiem par viņu tiešsaistes lietošanu.

Saskaņā ar direktoru ziņojumu (2019) galvenās ietekmes jomas bija šādas:

- Izglītības programmas īstenošana un uzvedības izmaiņu mērīšanas projekta uzsākšana sadarbībā ar Dublinas Universitāti un Bērnu un jauniešu komiteju (CYPSC);
- Spēcīgas kampaņas "Droša interneta diena" organizēšana;
- Tiešsaistes satura un resursu palaišana, kas paredzēta jaunāku bērnu vecākiem (vecumā no 2 līdz 10 g.). Iepriekšējos gados tika publicēts materiāls vecākiem bērniem;
- Politikas "jautājumu" sērijas izstrāde, kuru mērķis ir ietekmēt visaptverošu valsts politiku attiecībā uz kiberdrošību.

3.4 Spānija – SPACE: Skills for school professionals against cyberbullying events (SPACE: prasmes skolu profesionāļiem pret kibermobingu)

PAMATINFORMĀCIJA

Jauno tehnoloģiju plašā izplatība un izmantošana ir saistīta ar kibermobingu jeb emocionālo pazemošanu virtuālajā vidē. 2009. gadā aptuveni 18% Eiropas jauniešu vecumā no 13 līdz 19 gadiem tika iebiedēti /izsekoti/ vai tiem tika uzmākts internetā un mobilajos tālruņos, pašreizējais rādītājs svārstās no 10% līdz 52%. Eiropas Parlaments

uzsver, ka kibermobings starp bērniem vecumā no 11 līdz 16 gadiem pieauga no 7% 2010. gadā līdz 12% 2014. gadā.

MĒRĶAUDITORIJAS VAJADZĪBAS

Projekts SPACE atbild uz skolu pedagogu apmācību vajadzībām, lai viņi apgūtu kompetences kibermobinga novēršanai/kontrastēšanai. Faktiski, neskatoties uz to, ka ES dalībvalstis uzsāk daudzas iniciatīvas un projektus kibermobinga novēršanai un apkarošanai, šķiet, ka tās pieaug: tā kā tā ir jauna parādība, tai trūkst organiskas zināšanu, prasmju un strukturētu izglītības pasākumu sistēmas, kas nodrošinātu to, lai skolotāji apgūst zināšanas par tā dinamiku, digitālo tehnoloģiju apguvi drošai interneta lietošanai, kā arī spēju plānot profilakses, informēšanas un izglītošanas pasākumus.

MĒRĶI

Daudzus resursus un saturu par kibermobingu ir izstrādājušas dažādas skolas un iestādes; tomēr tās bija atsevišķas iniciatīvas, kas nebija apkopotas vienā tīmekļa telpā un tādējādi netika novērtētas. SPACE ir pieņēmis šo izaicinājumu un ir izstrādājis MOOC — bezmaksas tiešsaistes atvērto kursu — skolu pedagogiem par kibermobingu, kā arī daudzvalodu publisko digitālo bibliotēku ar atvērtiem izglītības resursiem par kibermobingu. Projekta galvenie mērķi:

- kartēt un aprakstīt kompetences, kas nepieciešamas kibermobinga novēršanai un pretstatīšanai;
- izstrādāt digitālu atvērto izglītības resursu (OER) bibliotēku par kibermobingu ar uzlabotām meklēšanas funkcijām;
- izstrādāt MOOC skolu skolotājiem par kibermobingu, izmantojot iepriekš iegūtos un marķētos OER;
- pilnveidot iesaistīto pedagogu digitālās prasmes, proti, par kiberdrošību, tīmekļa riskiem un tīkla etiķeti;

- atbalsts skolotājiem, kuri apgūst prasmes iejaukties kibermobinga gadījumos skolā, kā arī plānot un īstenot informācijas un apmācību pasākumus ar saviem skolēniem.

DALĪBNIEKI

Galveno mērķa grupu pārstāv skolu pedagogi (ISCED2 un ISCED3 līmeņi). Netiešās mērķa grupas bija skolas vadītāji un administratīvais personāls; studenti; vecāki; vietējās varas iestādes jeb lēmumu pieņēmējiem. 139 skolotāji bija iesaistīti MOOC izmēģinājumā un 300 piedalījās partnervalstīs organizētajos Multiplier (informatīvajos) pasākumos. Publisko digitālo bibliotēku projekta dzīves cikla apmeklēja vairāk nekā 8 000 lietotāju.

AKTIVITĀTES

Projekts ilga 24 mēnešus un tā laikā tika īstenotas šādas aktivitātes:

- kompetenču kartes un MOOC modeļa realizācija;
- tiešsaistes digitālās bibliotēkas izstrāde par kibermobingu;
- OER identificēšana, ieguve un kataloģizēšana par kibermobingu, kā arī šo resursu ievietošana digitālajā bibliotēkā;
- CMS platformas uzstādīšana un konfigurēšana MOOC mitināšanai;
- daudzvalodu MOOC par kibermobingu izstrāde un testēšana;
- rīku kopuma (Toolkit) izveide ar norādēm, vadlīnijām un ieteikumiem par SPACE sistēmu un instrumentiem;
- 10 multiplikatoru (multipliers) pasākumu īstenošana partnervalstīs un noslēguma konference;
- 4 konsorcija sanāksmju organizēšana;
- informācijas izplatīšana, izveidojot tīmekļa vietni, brošūras, prezentācijas, piedaloties kā reportierim uz DIDACTA gadatirgū Florencē, publicitāte žurnālos un laikrakstos.

IETEKME

Projektam ir bijusi pozitīva ietekme, veicinot izpratni par kibermobingu, plašākas zināšanas par tā dinamiku, novēršanas un pretstatīšanas metodēm, kā arī attīstot daudzdimensionālu zināšanu un prasmju kopumu iesaistīto Eiropas skolotāju grupā. Testēšanā iesaistītie skolotāji un organizācijas ir apguvušas kompetences kibermobinga novēršanai un pretstatīšanai, speciālistu digitālās kompetences par kiberdrošību, tīmekļa riskiem un tīkla etiķeti, attīstījušas stratēģiskās prasmes un metodiski didaktiskās kompetences, pilnveidojot savu pedagoģisko profesiju. Ir kļuvuši pieejami efektīvāki instrumenti realizēt informācijas un apmācību pasākumus saviem skolēniem, lai novērstu kibermobingu.

3.5 Latvija – programma "Pedagogu digitālās pratības pilnveide e-vides veidā izglītības tehnoloģiju izmantošanai"

MĒRĶIS

Programmas mērķis ir pilnveidot pedagogu digitālas kompetences – apmācīt par tehnoloģijām un rīkiem, lai palīdzētu pedagogiem efektīvāk organizēt savu darba procesu. Programmu īsteno LR Izglītības un zinātnes ministrija kopš 2014. gada.

LABUMA GUVĒJI (AUDITORIJA)

2020.g. kursu saturs ir veidots tā, lai maksimāli sasniegtu mērķa auditoriju:

- izglītības iestāžu vadības komandas,
- profesionālo un vispārizglītojošo skolu pedagogus (VET),
- pirmsskolas pedagogus,
- sākumizglītības skolotājus,
- dažādu mācību priekšmetu (matemātika, latviešu valoda, datorika, inženierzinības, dizains un tehnoloģijas, fizika, ķīmija un bioloģija) skolotājus.

APRAKSTS

2020. gadā Izglītības un zinātnes ministrijas izvirzījusi pedagogu digitālās kompetences pilnveidošanu par profesionālās kompetences prioritāro mērķi, piešķirot tam papildu finansējumu. Programma nodrošina bezmaksas kursu pedagogiem ar dažādām priekšzināšanām neatkarīgi no viņu priekšmeta/ specializācijas jomas. Kursu īstenotāji ir izstrādājuši detalizētus mācību uzdevumus un piesaistījuši grupu līderus – lai nodrošinātu pedagogiem labvēlīgu mācību režīmu. Kursu saturs veidots atbilstoši mūsdienu mācību vides prasībām.

SASNIEGTIE REZULTĀTI

4 339 pedagogi apmeklējuši garos (ar piešķirtām tiesībām strādāt par informātikas skolotāju) un īsos profesionālās kompetences pilnveides kursus (2014-2020).

INOVĀCIJAS

Kursu inovatīva pieeja slēpjas to organizācijas procesā - jo paredz iespēju katram kursu dalībniekam apgūt saturu sev ērtā tempā un laikā. Kursa laikā tiek apgūti tehnoloģijas un rīki, kurus var izmantot studiju procesā, lai veicinātu sadarbību un atvieglotu mācību procesa / pedagogu darba procesa organizēšanu (piem., rīki efektīvākai ikdienas darba rezultātu apkopošanai, darbam komandās).

3.6 Portugāle

Neskatoties uz dažām ad hoc iniciatīvām, apmācības pasākumi kiberdrošības jomā VET sektoram netika identificēts. Tirgū tika identificēti tikai vairāki augstākās izglītības kursi, pēcdiploma vai uzņēmējdarbības rakstura kursi, tāpēc profesionālās izglītības kiberdrošības apmācībām ir jābūt par fundamentālu prioritāti, lai veicinātu valsts kiberdrošu nākotni, proti, tādu kas spēj garantēt personīgo un biznesa drošību.

Nacionālais kiberdrošības centrs ar misiju veicināt zināšanu apmaiņu un nacionālo kiberdrošības kultūru izstrādāja Kiberdrošības izpratnes un apmācību programmu, ar

kuras palīdzību paredzēts masveidā palielināt iedzīvotāju un organizāciju darbinieku apmācību un informētību par draudiem lietojot kibertelpu neinformēti; veicot darbības, lai palielinātu izpratni un apmācītu par kiberdrošību dažādās valsts daļās no ziemeļiem uz dienvidiem, ejot cauri salām, ar partneru atbalstu, bet nekas no tā nav tieši vērsts uz profesionālām izglītības iestādēm.

3.7 Itālija - Docenti connessi e sicuri (Savienoti un droši skolotāji)

PAMATINFORMĀCIJA

Programmas vispārējais mērķis ir īstenot aktivitātes, kas vērstas uz inovāciju un digitālo prasmju stiprināšanu skolās. Konkrēti, programmas mērķis ir uzlabot skolotāju prasmes un zināšanas par jauno integrēto digitālo mācību pieredzi, lietiskā interneta (Internet of Things) darbību un priekšrocībām, kā arī kiberdrošības nozīmi. Programma tiek popularizēta saskaņā ar jauno sapratnes memorandu starp Itālijas Izglītības ministriju un korporāciju Cisco.

DALĪBNIEKI

Programmas ieguvēji ir jebkuras pakāpes un klases Itālijas skolu skolotāji.

AKTIVITĀTES

Apmācību programma, ko Cisco piedāvātā skolotājiem, sastāv no 3 vebināriem, ar kuriem ir saistīti 3 padziļināti kursi. Dalība visā programmā ir pilnīgi bez maksas.

1. Digitālās pasaules vebinārs "DAD un jaunā integrētās digitālās pasniegšanas pieredze", ko organizē Cisco darbinieki vai Cisco partneri, un saistīts tiešsaistes kurss "Get Connected". Paredzamais izpildes laiks: 30h. Kursa pārskats: kurss māca attīstīt digitālās pamatzināšanas. Īpaši interaktīvā kursa struktūra rada viegli pieejamu vidi auditorijai, kas IT pasaulei tuvojas pirmo reizi.
2. Apzinātie digitālie pilsoņi: vebinārs "Viedā pilsēta un lietu internets: jauni digitālie pakalpojumi pilsoņiem", ko organizē Cisco darbinieki vai Cisco partneri, un saistīts

tiešsaistes kurss "Ievads lietiskajā internetā (IoT)". Paredzamais izpildes laiks: 20 h. Kursa pārskats: kurss iepazīstina pasniedzējus ar tehnoloģijām, kas atbalsta IoT, un iespējām, ko rada pieaugošais tīkla savienojumu skaits starp cilvēkiem, procesiem, datiem un lietām.

3. IT drošība: vebinārs "Kā pasargāt sevi no tīkla apdraudējumiem?", ko organizē Cisco darbinieki vai Cisco partneri, un saistīts tiešsaistes kurss "Ievads kiberdrošībā". Paredzamais izpildes laiks: 20h. Kursa pārskats: kursā tiek analizētas tendences IT pasaulē, draudi un fakts par atrašanos pilnīgā drošībā kibertelpā, aizsargājot personas datus.

IETEKME

Tā kā projekts noslēdzās 3. jūnijā, skaitļi par apmācītajiem skolotājiem joprojām tiek precizēti. Tomēr projekts ir novatorisks, jo tas apvieno ar tehnoloģijām saistītas apmācības ar digitālo uzņēmējdarbību, kā arī ar programmēšanu.

Secinājumi

Projekta CYBER.EU.VET veiktais pētījums atklāja, ka trūkst datu un informācijas par izglītības iestāžu pedagogu kiberdrošības kompetencēm un izaicinājumiem Eiropas līmenī, kā arī ir ierobežots iniciatīvu skaits, kas vērstas uz kiberdrošības jautājumiem profesionālās izglītības un apmācību (VET) ietvaros, uzsverot to, ka projekts CYBER.EU.VET ir pievērsies svaigai un svarīgai tēmai visās dalībvalstīs.

Savukārt, eksistējošās iniciatīvas ir visaptverošas un izrādījušās efektīvas (skatīt sadaļu par labajām praksēm). Šobrīd lielākā daļa aktivitāšu un projektu ir vērsti uz iedzīvotāju kiberdrošības izpratnes celšanu un pedagogu vispārējo digitālo kompetenču uzlabošanu, ko ietekmējusi straujā pielāgošanās attālinātā darba/mācību procesam.

Partneru konsorcijs ir daudzšķautņains, un tas skaidri parāda dažāda līmeņa digitālās prasmes visā Eiropā. Tomēr neatkarīgi no atsevišķu valstu DESI izvietojuma, šo konsorcija ziņojumu var izmantot, lai iegūtu jēgpilnas un derīgas norādes visā Eiropas kontekstā.

Apmācības nepieciešamības būtība ir skaidra, pat tiem VET pedagogiem, kuri jau tika apmācīti IKT jomā. Netiek noliegta apmācību nepieciešamība, kā arī netiek apšaubīta tās lietderība. Mēs vēlamies atzīmēt, ka jo vairāk skolotāji jūtas pakļauti psihosociāliem, ētiskiem, juridiskiem, tehniskiem vai veselības riskiem, jo vairāk viņi runā par to, ka jūt apmācību nepieciešamu.

Saskaņā ar nacionālo aptauju, vairāk nekā puse skolotāju, kuri jūtas neaizsargāti pret kibermobingu (emocionālo pazemošanu virtuālajā vidē), uzskata, ka šādas apmācības ir nepieciešamas. Priekš viņiem sākotnējā un tālākizglītība ir iespēja dalīties pieredzē un analizēt profesionālās prakses metodes šajā jomā. Joprojām pastāv uzskats, ka digitālo

rīku izmantošana izglītībā ir veids, kā apmācīt vai arī ir objekts, par kuru mācīt skolēniem, nevis viņu vispārējās kultūras sastāvdaļa.

Ir nepieciešams izstrādāt informācijas avotu un prakses kultūru par digitālajiem riskiem (pētniecība un uzraudzība). Tāpat nepieciešams pastiprināt apmācības par digitālo tehnoloģiju izaicinājumiem un jo īpaši par psihosociālām, ētiskām, juridiskām un tehniskām problēmām, kas var rasties, izmantojot digitālos rīkus un kas satrauc skolotājus tiktāl, ka viņi var atteikties no to izmantošanas.

Tādējādi zināšanas par digitālajiem riskiem var pozitīvi ietekmēt pedagoģisko praksi izglītojot skolēnus digitālajā pratībā. Skolotājs ar spēcīgu digitālo kultūru būs vairāk tendēts izmantot digitālās tehnoloģijas kopā ar saviem skolēniem klasē un padarīt digitālās tehnoloģijas par mācību priekšmetu.

Risku acīmredzamo ietekmi nav iespējams pozitīvi mainīt bez vienotas un daudzveidīgas digitālās kultūras, kas papildina informācijas kultūru visplašākajā nozīmē, un kas ļauj izvairīties no tehniskā objekta demonizācijas un izmantot izglītības potenciālu. Šeit nav runa par izglītošanu bailēs, bet gan par emancipāciju (arī kā skolotājam), kritiski un gaiši uztverot digitālo pasauli.

Atsauces

ADEI (2017), El trabajo del futuro. Technical Note

Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Andries B. et Beigbeder I. (coordonné par) (1993), La culture scientifique et technique pour les professeurs des écoles, Paris: Hachette éducation, CNDP

Baron G.-L. et Baudé J. (1992), L'intégration de l'informatique dans l'enseignement et la formation des enseignants, Tours: EPI - INRP

Baron G.-L. et Bruillard É. (2000), Technologies de l'information et de la communication dans l'éducation : Quelles compétences pour les enseignants?, Éducation et Formation, No 56

Baron G.-L. et Bruillard É. (sous la direction) (2002), Les technologies en éducation: perspectives de recherche et questions vives, Actes du Symposium international francophone, Paris : INRP, IUFM de Basse-Normandie, MSH

BIBB (2016), "Economy 4.0 needs Education 4.0", Strengthening the media competence of training staff and trainees

Blanco, R., Fontrodona, J., Poveda, C. (2017), La industria 4.0: el estado de la cuestión, Revista Economía Industrial, No 406

Buisán García, M.; Valdés, F. (2017), La industria Conectada 4.0., Revista de economía, No 898

Bihouix P, Mauvilly, K (2016), Le Désastre de l'école numérique, Le Seuil

Capelle, C., Cordier, A., Lehmans, A., (2018), Usages numériques en éducation: l'influence de la perception des risques par les enseignants, Open Edition Journals

Carrizosa Prieto, E (2018), Lifelong learning e industria 4.0. Elementos y requisitos para optimizar el aprendizaje en red., Revista internacional y comparada de relaciones laborales y derecho del empleo. Vol. 6, No 1

Central Statistics Office (CSO) (2018), Information Society Statistics – Households: https://www.cso.ie/en/releasesandpublicatons/er/isshh/informationsocietystatisticshouseholds2018/ (piekļūts 06.07.2021.).

CEFEDOP, (2021), Vocational education and training in Portugal, EU Agenda.

Cyber Ireland, (2021), Cyber Security Skills Report 2021: National Survey: https://www.cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report2021.pdf(piekļūts 03.07.2021).

Latvijas nacionālo izglītības iestāžu datubāze – Niid.lv, studiju programmas kiberdrošībā

Department of Education and Skills, Government of Ireland (2015), Digital Strategy for Schools (2015-2020)-Enhancing Teaching, Learning and Assessment

Department of Education and Skills, Government of Ireland (2017), Higher Education System Performance Framework 2018-2020

Department of Enterprise, Trade and Employment (2018), Future Jobs Ireland – Preparing Now for Tomorrow's Economy

Department of Further and Higher Education, Research, Innovation and Science, Government of Ireland (2021), Statement of Strategy 2021-2023

Department of Justice (2021). Cybercrime: www.justice.ie/en/jelr/pages/cybercrime (piekļūts 02.07.2021.)

Department of Tourism, Culture, Arts, Gaeltach, Sport and Media (2019), Action Plan for Online Safety 2018 – 2019

Dig8tal (2020), Is German Cybersecurity ready for 2021?, https://dig8ital.com/resources/library/is-german-cyber-security-ready-for-2021

Erasmus+ project DIG4VET (Digital Tools for Learning and Validation in VET and WBL: Training Program for VET Teachers, Trainers and Potential I-Coaches)

Escuela de organizacion industrial, Activa industria 4.0.

EFVET (2021), Digital Balance: Balancing Digital Competences and Wellbeing

European Commission (2020), Italy in the Digital Economy and Society Index

European Commission (2020), Latvia in the Digital Economy and Society Index

Federal Office for Information Security, (2019),The State of IT Security in Germany in 2019

Federal Office for Information Security, (2020), The State of IT Security in Germany in 2020

Federal Office for Information Security, (2020). Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit

Government of Ireland (2018), National Cyber Security Strategy 2019-2024

Government of Italy (2020), Piano Nazionale di Ripresa e Resilienza -PNRR

Government of Latvia, (2019), Informative report, Cybersecurity Strategy of Latvia

Government of Latvia, (2020), Education Development Guidelines 2021-2027 "Future Skills for the Future Society"

Government of Latvia, (2020), Digital Transformation Guidelines 2021-2027.

Guir, R. (2002), Pratiquer les TICE : Former les enseignants et les formateurs à de nouveaux usages, Bruxelles: De Boeck et Larcier

Huismann, A. (2020), Vocational education and training for the future of work: Germany, Cedefop ReferNet thematic perspectives series

Information Technology Security Incident Response Institution, (2021), CERT.LV Annual Report 2020

Izglītības un zinātnes ministrija (2017), Informatīvais ziņojums "Priekšlikumi konceptuāli jaunas kompetencēs balstītas izglītības prasībām atbilstošas skolotāju izglītības nodrošināšanai Latvijā

Izglītības un zinātnes ministrija (2020), Pedagogiem nodrošināta iespēja bez maksas pilnveidot digitālās prasmes

Joseph, V. (2020). Vocational education and training for the future of work: France, Cedefop ReferNet thematic perspectives series

Kultusministerkonferenz (2016), "Bildung in der digitalen Welt: Strategie der Kultusministerkonferenz"

Lardellier P., Moatti, D. (2014), Les ados pris dans la Toile. Des cyberaddictions aux techno-dépendances, Paris: Éditions Le Manuscrit, Coll. «Addictions: Plaisir, Passion, Possession»

Latvijas Drošāka interneta centrs, platform "Drossinternets.lv": https://drossinternets.lv/

LIKTA - Latvijas Informācijas un komunikācijas tehnoloģijas asociācija: https://likta.lv/digitalasparmainas-izglitiba/

Likumi.lv, Noteikumi par pedagogiem nepieciešamo izglītību un profesionālo kvalifikāciju un pedagogu profesionālās kompetences pilnveides kārtību. https://likumi.lv/ta/id/301572-noteikumi-par-pedagogiem-nepieciesamo-izglitibu-un-profesionalo-kvalifikaciju-un-pedagogu-profesionalas-kompetences-pilnveides

Microsoft Digital Defense Report: https://www.microsoft.com/de-de/security/business/security-intelligence-report

Ministry of Education, University and Research, Government of Italy, Piano Nazionale Scuola Digitale – PNSD

Ministry of Education, University and Research, Government of Italy, (2018), La Buona Scuola (Law No. 107/2015)

Ministry of Education, University and Research, Government of Italy (2020), Accordo di collaborazione per lo svolgimento di attività didattiche e formative congiunte per promuovere l'educazione alla cittadinanza digitale e l'utilizzo consapevole delle tecnologie digitali e dei social media, Memorandum of Understanding n. 4 of 28 October 2020

Ministry of Education, University and Research, Government of Italy (2021), Innovare e potenziare le competenze digitali nella scuola, Memorandum of Understanding n. 785 of 22 January 2021

Ministry of Industry, Trade and Tourism, Government of Spain, Industria Conectada 4.0, Agenda Digital para Espana

Ministry of Technological Innovation and Digital Transition (2020), 2025 – Strategia per l'innovazione tecnologica e la digitalizzazione del Paese

Mokhtar Ben Henda (2016), Identification des besoins en formation tic/e dans les pays francophones du sud. Étude réalisée par: Initiatives pour le Développement numérique de

l'espace universitaire francophone francophone, [Rapport de recherche] Agence universitaire de la Francophonie.

National Centre for Vocational Education Research, (2020), Teaching digital skills: Implications for VET educators - good practice guide

OECD (2021), Going Digital in Latvia

OECD, (2018), TALIS - The OECD Teaching and Learning International Survey TALIS - OECD Teaching and Learning International Survey

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

Principes et organisation de la deuxième année de la formation des enseignants stagiaires en IUFM, (2002). La circulaire du 4 avril 2002 parue au Bulletin officiel n° 15 du 11 avril 2002

Saldus Tehnikums, studiju programma "Civilā aizsardzība un drošība": https://www.saldustehnikums.lv/izglitibas-iespejas/profesijas/profesionala-videja

Stolterman, E (2004), Information Technology and the Good Life, International Federation for Information Processing Digital Library; Information Systems Research. Volume 143

Télé-enseignement : les 5 risques majeurs en matière de cybersécurité – Sophos News

Thélot C. (sous la direction) (2004), Pour la réussite de tous les élèves, rapport officiel de la Commission du débat national sur l'avenir de l'École, Paris : La documentation Française

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.