

# Drošība pret pikšķerēšanu (personas datu izmānīšanu) 4. Rūpnieciskās revolūcijas ērā (Kiberpikšķirēšana)



## A2: Īstenošanas vadlīnijas

**Projekta ilgums:** 2020. Gada novembris – 2022. gada novembris

**Projekta Nr.:** 2020-1-LT01-KA203-078070



Funded by the  
Erasmus+ Programme  
of the European Union

This project has been funded with support from the European Commission.

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



## Saturs

<b>1. IEVADS .....</b>	<b>3</b>
<b>2. KIBERDROŠĪBA, PIKŠĶERĒŠANA UN SOCIĀLĀ INŽENERIJA .....</b>	<b>4</b>
2.1. Kiberdrošība un pikšķerēšana studiju programmās.....	4
2.2. Pikšķerēšanas un sociālās inženierijas atpazīšana .....	4
<b>3. CYBERPHISH MĀCĪBU PROGRAMMA .....</b>	<b>5</b>
<b>4. CYBERPHISH IZMĒGINĀJUMA MĀCĪBU ORGANIZĀCIJA .....</b>	<b>6</b>
<b>5. Izmēginājuma apmācības rezultāti.....</b>	<b>7</b>
Anketa pirms apmācības.....	7
Tiešsaistes mācību vide.....	10
<b>6. IZMĒGINĀJUMA APMĀCĪBAS PARTNERU VALSTĪS .....</b>	<b>26</b>
Latvija .....	26
<b>Secinājumi .....</b>	<b>28</b>
<b>Informācijas avoti .....</b>	<b>29</b>
<b>Pielikums Nr. 1.....</b>	<b>30</b>
<b>CYBERPHISH MĀCĪBU VIDE .....</b>	<b>30</b>
Piesakieties e-mācību vidē.....	30
Lietotāja knts .....	31
Mācību materiāls .....	34
Pašnovērtējumu testi.....	35
Simulācijas .....	35
Lietotāju reitingi.....	38



## 1. IEVADS

Ceturtās industriālās revolūcijas laikmetā kiberdrošība klūst par vienu no lielākajiem izaicinājumiem. Plašā digitālo iekārtu un informācijas sistēmu izmantošana kibernoziņniekiem klūst arvien pievilcīgāka. Saskaņā ar Eurostat datiem, "... 2019. gadā pēdējo 12 mēnešu laikā aptuveni katrs trešais ES pilsonis vecumā no 16 līdz 74 gadiem ziņoja par ar drošību saistītiem incidentiem, izmantojot internetu privātām vajadzībām. Šajā periodā pikšķerēšana bija visbiežākais drošības incidents, par kuru ziņoja 2019. gadā. Praksē neviens informācijas sistēma vai drošības programmatūra nevar nodrošināt 100% aizsardzību pret pikšķerēšanas uzbrukumiem. Cīņa pret šiem apdraudējumiem ir saistīta ne tikai ar aparātūras un programmatūras drošības risinājumiem, bet arī ar lietotāja zināšanām par šādiem draudiem un spēju tos atpazīt.

Kiberuzbrukumi ir vērsti arī pret uzņēmumiem Eiropā. Saskaņā ar 2017. gada globālo informācijas drošības stāvokļa apsekojumu aptuveni 80% Eiropas uzņēmumu tajā gadā saskārās ar vismaz vienu kiberdrošības incidentu, un darbinieki bija atbildīgi par 27% no visiem kiberdrošības incidentiem.

Tātad tikai cilvēks – lietotājs, kurš saprot kibernoziņnieka darbību un spēj atpazīt jaunprātīgas darbības brīdinājuma pazīmes, var palīdzēt novērst kiberuzbrukumus, piemēram, pikšķerēšanu.

Saskaņā ar ENISA datiem, ar kiberoziegumiem saistītie priekšmeti ir nepietiekami pārstāvēti netehniskajās mācību programmās. Tāpēc ir svarīgi izstrādāt un piedāvāt sabiedrībai plaši pieejamu tiešsaistes apmācību kursu par pikšķerēšanas identificēšanu.

Šo iemeslu dēļ tika uzsākts un īstenots starptautisks projekts "Drošība pret pikšķerēšanu 4. industriālās revolūcijas laikmetā" (CyberPhish). Eiropas Savienība projektu finansēja Erasmus+ programmas ietvaros. Projektu koordinēja Viļņas Universitātes Kauņas fakultāte, un projekta partneri bija Tartu Ulikool (Igaunija), Dorea (Kipra), MECB (Malta), Altacom (Latvija) un Informācijas tehnoloģiju institūts (Lietuva). Projekta ilgums ir no 2020. gada novembra līdz 2022. gada novembrim.

Projekta "CyberPhish" galvenais mērķis ir izglītot augstākās izglītības studentus, pasniedzējus, augstskolu darbiniekus (kopienas pārstāvjus), izglītības centrus un biznesa sektoru (darba devējus un darbiniekus), kā arī veicināt kritisko domāšanu kiberdrošības jomā mērķa grupā.

Projekta "Cyberphish" mērķis ir izstrādāt mācību programmu, e-mācību materiālus, jauktu mācību vidi, simulācijas, pašnovērtējuma un zināšanu vērtēšanas testus. Izstrādātais CyberPhish kurss ļauj lietotājiem aizsargāties pret pikšķerēšanas uzbrukumiem. Lietotāji iegūst zināšanas, kas palīdzēs pievērst uzmanību apdraudējumiem un veikt nepieciešamos profilakses pasākumus.

Projekta ietvaros ir izstrādāts intelektuāls produkts lietotāju kritiskās domāšanas un pikšķerēšanas identificēšanas prasmju apmācībai. Lietotāji iemācīsies atpazīt pikšķerēšanas zīmes (sarkanos karogus), sociālās inženierijas metodes un kiberdrošības prasmes. Jauktās mācīšanās pieeja/koncepcija ļaus lietotājiem sagatavoties zināšanu pārbaudei un saņemt sertifikātu par kursu.

Projekta partneri izmēģinājuma apmācībās piecās partnervalstīs izmantoja tiešsaistes mācību platformu, kas aptver mācību materiālus, simulācijas, pašnovērtējuma testus un zināšanu novērtēšanas testus. Pamatojoties uz šo pieredzi, ir izstrādātas šīs vadlīnijas.

### Vadlīniju mērķis

Šīs vadlīnijas ir paredzētas, lai iepazīstinātu ar projekta rezultātiem, labāko izmēģinājuma praksi un metodiku CyberPhish apmācības kura izstrādei mērķauditorijai un ieinteresētajām personām. Vadlīnijas ir paredzētas organizācijām, kuras ir ieinteresētas izstrādātā materiāla pielāgošanā un izmantošanā interneta lietotāju izglītošanai pikšķerēšanas atpazīšanā: augstākās izglītības iestādes, pieaugušo izglītības/apmācību centri, uzņēmējdarbības sektori.

### Vadlīniju uzdevumi

"CyberPhish" ieviešanas vadlīniju galvenais uzdevums ir iepazīstināt ar apmācību organizēšanas rīkiem, saturu un procesu. Šī procesa laikā dalībnieki apgūst zināšanas un prasmes, kas nepieciešamas, lai identificētu pikšķerēšanas uzbrukumus darbā un personīgajā dzīvē un sagatavotos zināšanu pārbaudei. Pēc veiksmīgas pabeigšanas viņiem tiks piešķirts sertifikāts. Īstenošanas process ir balstīts uz iesaistīto partnervalstu pieredzi.



## 2. KIBERDROŠĪBA, PIKŠKERĒŠANA UN SOCIĀLĀ INŽENERIJA

### 2.1. Kiberdrošība un pikškerēšana studiju programmās

Kopš 2013. gada Eiropas Komisija ir akcentējusi kiberdrošības jautājuma nozīmi. Pirmā kiberdrošības stratēģija kā galveno stratēgisko mērķi izceļ izpratnes veidošanu un prasmju attīstību. 2017. gada ENISA ziņojumā arī uzsvērtā kiberdrošības nozīme. Tajā ES dalībvalstīm ieteikts stiprināt kiberdrošības izglītību un prasmes (ENISA, 2019, 23. lpp.). Rezultātā visas ES dalībvalstis ir izstrādājušas un publicējušas savas nacionālās kiberdrošības stratēģijas (NCSS).

Eiropadome 2021. gada martā izdarīja jaunus secinājumus par ES kiberdrošības stratēģiju<sup>1</sup>. Rezultāti atzīst digitālo un kiberdrošības prasmju trūkumu un uzsver nepieciešamību apmierināt tirgus pieprasījumu, turpinot attīstīt izglītības un apmācības programmas.

Projekta CyberPhish ietvaros tika pētītas esošās mācību programmas un apmācību programmas kiberdrošības un pikškerēšanas jomā partnervalstīs Kiprā, Igaunijā, Latvijā, Lietuvā un Maltā. DOREA Izglītības institūts vadīja pētījumu. Pētījuma galvenie secinājumi bija:

- HEI studiju programmu analīze visās projekta partnervalstīs, izņemot Igauniju, neietver pikškerēšanas un sociālās inženierijas tēmas kā atsevišķus moduļus. Tomēr informāciju par šim tēmām tā var iekļaut citos kursu moduļos. Divas HEI studiju programmas Igaunijā ietver studiju moduļus, kas vērsti uz sociālo inženieriju. Vidējais šādu moduļu ilgums ir 4,5 ECTS.
- Analizētās HEI studiju programmas Igaunijā, Latvijā un Maltā ietver kursu moduļus netehniskajās prasmēs, piemēram, komunikācijas prasmes, uzņēmējdarbība, psiholoģija u.c. Turpretim HEI studiju programmas Kiprā un Lietuvā galvenokārt ir vērstas uz tehniskajām prasmēm, mazāk akcentējot netehnisko prasmju nozīmi.
- Visās partnervalstīs dažas publiskas un privātas organizācijas piedāvā apmācību kursus kiberdrošības jomā, kas paredzēti kiberdrošības un IT speciālistiem, uzņēmumiem, darbiniekiem un plašai sabiedrībai. Lai gan ūtie apmācību kursi parasti koncentrējas tikai uz apdraudējumiem, tostarp pikškerēšanu, sociālo inženieriju un veidiem, kā sevi aizsargāt, ilgākie apmācību kursi sniedz plašāku informāciju par kiberdrošību. Ir arī dažas organizācijas, kas piedāvā iekļūšanas un sociālās inženierijas testus, kuru mērķauditorija ir uzņēmumi un to darbinieki.

Aptaujas laikā iegūtie dati palīdzēja noteikt prasmju trūkumus un izstrādāt ieteikumus jaunai apmācību programmai CyberPhish. Šīs programmas mērķis ir uzlabot interneta lietotāju prasmes un informētību un izglītot viņus par jaunākajām kiberdrošības problēmām un draudiem, īpaši pikškerēšanu.

### 2.2. Pikškerēšanas un sociālās inženierijas atpazīšana

Kiberdrošība ir arī Eiropas uzņēmumu problēma. Uzņēmumi arvien biežāk kļūst par kiberuzbrukumu mērķiem. Tā kā noziedznieki kļūst arvien izglītotāki, arvien grūtāk atklāt un novērst kiberuzbrukumus, un šādu uzbrukumu veikšanai tiek izmantotas jaunas metodes un platformas. Saskaņā ar 2017. gada globālo informācijas drošības stāvokļa apsekojumu aptuveni 80% Eiropas uzņēmumu tajā gadā saskārās ar vismaz vienu kiberdrošības incidentu. Aptauja liecina, ka darbinieki ir atbildīgi par 27% no visiem kiberdrošības incidentiem. Tikai 2019. gada pirmajā ceturksnī uzņēmumi visā pasaulei tika pakļauti kiberuzbrukumiem par 120% biežāk nekā 2018. gadā, un tie cieta milzīgus zaudējumus (22,2 miljardus eiro).

Kā teikts 2019. gada Cilvēkfaktora ziņojumā, vairāk nekā 99% e-pasta ziņojumu, kuros tiek izplatīta ļaunprātīga programmatūra, ir nepieciešama cilvēka iejaukšanās, t.i., sekošana saitēm, dokumentu atvēršana, drošības brīdinājumu pieņemšana un citas darbības [5].

Tāpēc ir būtiski izglītot un palielināt izpratni šajā jomā. Kiberneturība prasa izskaidrot/mācīt, kā atpazīt pikškerēšanu tādā veidā, kas ir saprotams un pieejams lielākajai daļai cilvēku. Brīdinājuma zīmu pārzināšana un noziedznieku metožu izpratne, pirmkārt, liks interneta lietotājiem justies pārliecinātākiem un drošākiem, otrkārt, palīdzēs novērst vai vismaz palēnināt šādu uzbrukumu izplatību.

<sup>1</sup> Eiropas Savienības Padome (2021): Padomes secinājumu projekts par ES kiberdrošības stratēģiju digitālajai desmitgadei, URL [https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm\\_source=dsms-auto&utm\\_medium=email&utm\\_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy](https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy) (publicēts 09/09/2022)



Pikšķerēšana ir nelikumīga lietotāja personas datu iegūšana (pieteikšanās akreditācijas dati, kreditkartes informācija utt.), izmantojot sociālās inženierijas metodes. Noziedznieki aktīvi darbojas sociālajos tīklos, sūta e-pastus un zvana. Šo ziņojumu mērķis ir pārliecināt lietotāju atvērt Jaunprātīgu pielikumu vai noklikšķināt uz viltotas tīmekļa saites, atklājot viņa paroli. [6]

Visizplatītākie pikšķerēšanas veidi ir Spray and Pray, Cat phishing, Advanced fee scam, Spear fishing, Whaling, Vishing, Smishing, Angler Phishing, Clone Phishing, un Malvertising.

Informācijas drošības kontekstā sociālā inženierija tiek definēta kā psiholoģiska manipulācija ar cilvēkiem, veicot darbības vai izpaužot konfidenciālu informāciju. ENISA norāda, ka sociālā inženierija joprojām ir galvenais drauds cita veida kiberoziegumiem, jo 84% kiberuzbrukumu ir balstīti uz sociālo inženieriju. Pikšķerēšanas upuru skaits turpina pieaugt, jo tiek izmantots cilvēciskais faktors, kas ir vājākais posms[6]

Sociālās inženierijas metodes balstās uz cilvēka vājībām, piemēram, alkatību, bailēm, zinātkāri, uzticību, empātiju un steigu. Tāpēc rūpīgi izstrādāts un personalizēts e-pasts, balss pasts, tālrūņa zvans vai īsziņa var ietekmēt cilvēkus un likt viņiem atklāt savu konfidenciālo informāciju, noklikšķināt uz Jaunprātīgas saites, lejupielādēt un atvērt failu, kurā ir Jaunprātīga programmatūra, vai pat pārskaitīt naudu noziedzniekiem.

Dr. Robert B. Cialdini savā grāmatā "Ietekme: pārliecināšanas psiholoģija" aprakstīja sešus pārliecināšanas principus, kas tika pieņemti un izmantoti sociālajā inženierijā un pikšķerēšanā. Vēlāk tie tika paplašināti līdz septiņiem: Atlīdzība, trūkums, autoritāte, konsekvence, vienprātība, patika un vienotība. Krāpnieki, kas izmanto šādus paņēmienus, var sagaidīt veiksmīgus rezultātus no viņu radītajiem uzbrukumiem. Tāpēc ir īpaši svarīgi izglītot cilvēkus, lai viņi zinātu, kā atpazīt šādus uzbrukumus un izvairīties no tiem. [7; 8; 9]

Projekta partneri veica aptauju, lai noskaidrotu, kā cilvēki atpazīst pikšķerēšanas uzbrukumus, noskaidrotu cilvēku informētību par pikšķerēšanu un dažadiem pikšķerēšanas veidiem, kā arī identificētu prasmju trūkumus partnervalstīs Kiprā, Igaunijā, Latvijā, Lietuvā un Malta. Pētījuma rezultāti ir pieejami Pētījuma ziņojumā "Pikšķerēšanas un prasmju nepilnību atpazīšana". [7]

Aptaujā piedalījās piecsimt četrpadsmiņ cilvēki, no kuriem 259 bija sievietes, 248 vīrieši, bet 7 cilvēki deva priekšroku neidentificēt savu dzimumu. Visvairāk aptaujāto ir studenti (304), kam seko darba īņēmēji (139), uzņēmumu īpašnieki (53), bezdarbnieki (10) un pašnodarbinātie (8). Lielākā daļa aptaujāto ir augsti izglītoti – lielākajai daļai respondentu (38%) ir bakalaura grāds, kam seko maģistra grāds (23%) un doktora grāds (6%).

Interesanti, ka gandrīz katrs piektais respondents ziņoja, ka pagātnē ir bijis pikšķerēšanas uzbrukuma upuris. Visbiežāk pikšķerēšanas uzbrukumi notikuši, noklikšķinot uz saitēm e-pastos vai ziņojumos, atverot pielikumus vai atbildot uz e-pastiem un sniedzot konfidenciālus datus. Visbiežākie šo uzbrukumu iemesli bija izklaidība, zinātkāre vai steiga. Lielākā daļa aptaujāto (74%) nav apmeklējuši nevienu kiberdrošības apmācību vai semināru. Vairāk nekā puse aptaujāto (54%) norādīja, ka viņi interesējas par šo jomu patstāvīgi. Tas viss liecina par pieaugošu nepieciešamību pēc zināšanām par pikšķerēšanu un kiberdrošību.

### 3. CYBERPHISH MĀCĪBU PROGRAMMA

Pamatoties uz vajadzību analīzi, partneru konsorcijā ir izstrādājis mācību programmu par kiberdrošību, kiberuzbrukumiem, sociālo inženieriju, īpašu uzmanību pievēršot pikšķerēšanas identificēšanai un novēršanai.

Mācību programmas mērķis ir sniegt ievadu kiberdrošībā, īpašu uzmanību pievēršot pikšķerēšanas uzbrukumiem. Kursu programma ir paredzēta privātpersonām, studentiem, uzņēmējiem, organizāciju darbiniekiem un sagatavos viņus ceturtās industriālās revolūcijas laikmeta drošības apdraudējumiem. Kurss sniegs studentiem prasmes identificēt un pārvaldīt kiberuzbrukumus un aizsargāt ierīces un datus.

Mācību programma ir izstrādāta jauktai apmācībai, taču tās struktūra padara to elastīgu, un to var izmantot gan tālmācības, gan klātienes apmācībai. Pilna apmācības programma sastāv no 30 stundām, kas atbilst 1 ECTS. Iesakām veltīt pašmācībai un vērtēšanai tādu pašu stundu skaitu vienam modulim.

Mācību programma ir sadalīta četrās daļās (moduļos):

1. Ievads kiberdrošībā;
2. Pārskats par kiberdrošību ES;
3. Kiberuzbrukumi — sociālā inženierija un pikšķerēšana;
4. Kiberuzbrukumu izpratne un rīcība ar tiem.



Pilnu mācību programmu var atrast CyberPhish vietnē: [https://cyberphish.eu/wp-content/uploads/2022/12/I02-A2\\_Extended-version-of-curricula\\_LV.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/I02-A2_Extended-version-of-curricula_LV.pdf)

## 4. CYBERPHISH IZMĒGINĀJUMA MĀCĪBU ORGANIZĀCIJA

Izmēginājuma apmācība ir paredzēta, lai apmācītu dalībniekus identificēt pikšķerēšanas uzbrukumus, izprast sociālo inženieriju un apgūt jaunas un uzlabot esošās prasmes. Pieteikumā norādīts, ka projekta laikā izstrādātie produkti ir jāizmēģina, lai izvērtētu rezultātus un nepieciešamības gadījumā tos pielāgotu, nemot vērā dalībnieku un skolotāju/mentoru komentārus un atsauksmes.

**Dalībnieki.** Izmēginājuma mācības notika visās projekta partnervalstīs – Kiprā, Igaunijā, Latvijā, Lietuvā un Malta. Dalībnieku vidū bija:

- Augstākās izglītības studenti,
- Augstskolu un augstākās izglītības organizāciju darbinieki,
- Pieaugušo izglītības centru pasniedzēji un darbinieki.

Katra partnerorganizācija savā valstī apmācīja vismaz 24 dalībniekus, tādējādi paplašinot projekta ietekmi ārpus savas organizācijas.

**Ilgums.** Partneriem vienojoties, izmēginājuma apmācība ilga vairākus mēnešus (maijs-septembris), nemot vērā katra partnera vasaras brīvdienas. Daži partneri izmēginājuma apmācības rīkoja mācību gada beigās, t.i., maijā, pavasara semestra beigās. Citi partneri rīkoja mācību gada sākumā septembrī un pulcēja dalībniekus izmēginājuma apmācībām līdz septembra beigām.

**Pieeja.** Izmēginājuma apmācības var organizēt kā jauktu mācību kursu vai, nesmot vērā Covid-19 pandēmijas ierobežojumus, var organizēt attālināti.

Vilņas Universitāte un Tartu Universitāte izmēgināja apmācību savās organizācijās, integrējot Cyberphish kursu savos mācību priekšmetos. Pārējie partneri Altacom, Dorea un MECB izmēginājuma apmācības veica sadarbībā ar citām augstākās izglītības iestādēm vai pieaicinot ārējus dalībniekus.

**Mācību platforma.** Mācību platforma CyberPhish tika izstrādāta un testēta piecās valodās – angļu, igauņu, grieķu, latviešu un lietuviešu. Dalībniekiem bija jāiepazīstas ar izstrādāto mācību materiālu, pēc katras kurga tēmas jākārto pašnovērtējuma testi, jāatrisina simulācijas un jākārto zināšanu gala tests.

### Izmēginājuma apmācības organizēšana

Pirms izmēginājuma apmācības pieci partneri vienojās organizēt apmācību savās valstīs, lai nodrošinātu, ka:

- vismaz 24 dalībnieki no katras partnervalsts pabeidz izmēginājuma apmācību (kopā vismaz 120 dalībnieki visās valstīs);
- dalībnieki aizpilda pirms izmēginājuma anketu, t.i., lai novērtētu savas esošās zināšanas pirms apmācībām (kopā vismaz 120 aizpildītas anketas);
- gala zināšanu pārbaude tiek uzskatīta par nokārtotu, ja dalībnieks ir ieguvis vismaz 75%;
- dalībnieki izmēginājuma apmācību beigās aizpildīs anketu, t.i., lai novērtētu savas esošās zināšanas pēc apmācībām (kopā vismaz 120 aizpildītas anketas);
- vismaz viens treneris no katras partnervalsts arī aizpildīs anketu par apmācībām (vismaz 5 anketas). Šī anketā palīdzēs novērtēt projekta izmēginājuma apmācības. Treneru sniegtās atbildes (atsauksmes) sniegs informāciju par izstrādātā kursa kvalitāti, t.i., tēmu atbilstību mērķauditorijai, kursa tēmu vispusīgumu, kursa materiāla struktūru un saturu, apmācības ilgumu. Svarīgākais būs jautājums, cik lielā mērā kurss ir sasniedzis savu mērķi – iepazīstināt auditoriju ar kiberdrošību un krāpšanu.
- Izmēginājuma apmācības beigās katrs partneris iesniegs koordinatoram izmēginājuma apmācības kopsavilkumu. Koordinators izmants šo informāciju, lai sagatavotu IO6 ziņojumu. Partneri atjauninās intelektuālos rezultātus (IO2, IO3, IO4 un IO5) pēc izmēginājuma apmācības rezultātu sintēzes.

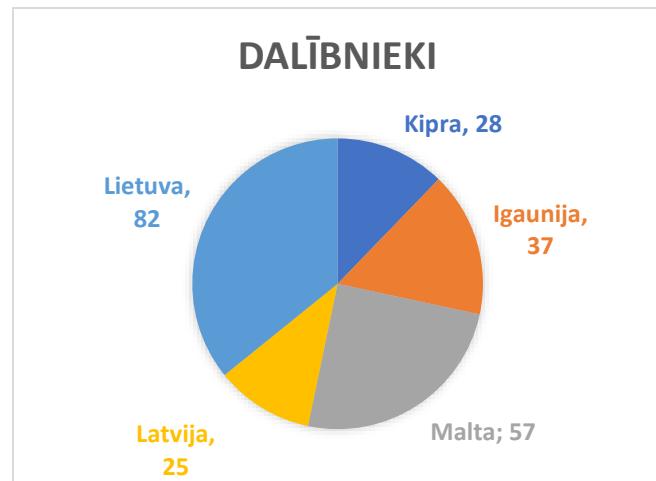


## 5. IZMĒGINĀJUMA APMĀCĪBAS REZULTĀTI

Izmēginājuma mācības notika piecās projekta partnervalstīs – Kiprā, Igaunijā, Latvijā un Maltā. Kopā apmācībās piedalījās 229 dalībnieki. Simt septiņdesmit pieci (175) dalībnieki pabeidza apmācību ar 75% vai augstāku punktu skaitu.

### Anketa pirms apmācības

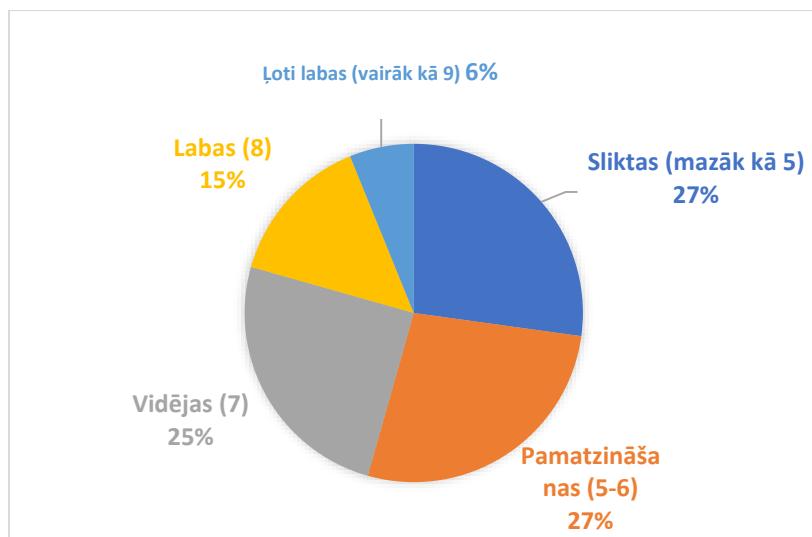
Pirms izmēginājuma apmācības sākuma visi dalībnieki aizpildīja pirms apmācības anketu, lai novērtētu savas sākotnējās zināšanas par krāpšanu un kiberdrošību. Kopā šādas anketas aizpildīja 229 dalībnieki. Dalībnieku sadalījums pa valstīm ir parādīts attēlā zemāk.



Attēls Nr. 1 Izmēginājuma apmācības dalībnieki pa valstīm

### Dalībnieku sākotnējais zināšanu līmenis pirms apmācības

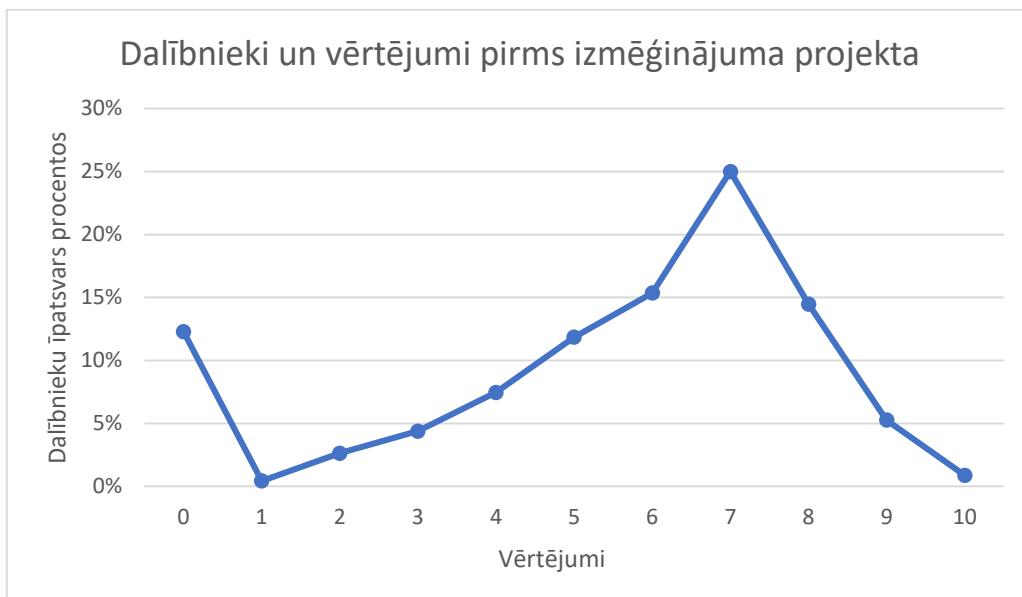
Anketas tika analizētas, lai novērtētu dalībnieku zināšanas pirms izmēginājuma apmācību sākuma. 2. attēlā parādīts dalībnieku sadalījums pēc iegūtajiem punktiem. 27% dalībnieku zināšanas par pikšķerēšanu bija vājas (rezultāts ir mazāks par 5 punktiem). Tai pašai daļai (27%) dalībnieku bija tikai pamatzināšanas (t.i., vērtējums 5-6 punkti). 25% dalībnieku bija "vidējais" rezultāts (7 punkti). 15% dalībnieku zināšanas bija novērtētas kā "labas" (t.i., 8 punkti), un tikai 6% dalībnieku bija ar vērtējumu "loti labi" (9 punkti vai vairāk). Dalībnieku zināšanas tika vērtētas desmit ballu skalā.



Attēls Nr. 2. Izmēginājuma apmācības dalībnieku zināšanas pirms apmācībām



3. attēlā parādīts dalībnieku zināšanu sadalījums (pēc novērtējuma) pirms izmēģinājuma apmācībām desmit ballu skalā.  
3. attēlā parādīts dalībnieku zināšanu sadalījums (10 ballu skalā) pirms izmēģinājuma apmācībām. Var redzēt, ka nedaudz vairāk kā piektā daļa aptaujāto ieguva augstus rezultātus (t.i., 8, 9 un 10).



**Attēls Nr. 3. Zināšanu punktu sadalījums pa izmēģinājuma apmācības dalībniekiem**

#### Jautājumu sarežģītība: 5 visvienkāršākie jautājumi

analizējot dalībnieku anketas, tika noskaidrots, kuri jautājumi bija smagi un kuri pietiekami viegli. Balstoties uz dalībnieku sniegtajām atbildēm, esam noteikuši piecus visvienkāršākos jautājumus. Apmēram 70-75% no visiem dalībniekiem atbildēja uz šiem jautājumiem pareizi. Šie jautājumi ir parādīti tabulā zemāk.

##### **Top 1. 15. Vai tā ir taisnība, ka pikšķerēšanas uzbrukums tiek veikts tikai pa e-pastu?**

Nē

Jā

##### **Top 2. 13. Kādas darbības var novērst sociālās inženierijas uzbrukumus?**

###### **Visas uzskaitītās**

Uzziniet, kāda jūsu personiskā informācija ir pieejama tiešsaistē

Izmantojiet daudzfaktoru autentifikāciju

Iespējojiet mēstuļu filtru

Atjauniniet programmatūru

##### **Top 3. 5. Kurš no šiem vislabāk nosaka termina "kiberuzbrukums" darbības jomu?**

**Jebkādas ļaunprātīgas darbības kibertelpā, pat ja tās ir neveiksmīgas**

Kaitīgas darbības, izmantojot internetu

Vīrusu un Trojas zirgu sūtīšana pa e-pastu vai SMS

Veiksmīgi pikšķerēšanas uzbrukumi

##### **Top 4. 12. Sociālā inženierija ir**

**Manipulācijas ar cilvēkiem, parasti ar psiholoģiskas pārliecināšanas palīdzību, lai pieklūtu informācijas sistēmām vai datiem.**



uzbrukums, kas izmanto jaunprātīgu programmu, kas ir paslēpta šķietami likumīgajā programmā  
jaunprātīga programmatūra, kas draud publicēt upura personas datus vai pastāvīgi bloķēt piekļuvi tiem, ja vien netiek  
samaksāta maksā  
kad uzbrucējs pārtver divu pušu darījumus, darbojoties kā starpnieks  
programmas veids, kas lejupielādēta, lai apkopotu informāciju par lietotājiem, viņu sistēmām vai pārlūkošanas  
paradumiem, nosūtot datus attālinātam lietotājam

#### Top 5. 14. Kādas taktikas tiek izmantotas pikšķerēšanas e-pastos?

**Pieprasī nosūtīt konfidenciālu informāciju pa e-pastu**

**Lūdz noklikšķināt uz saites e-pastā**

Informācijas sniegšana par veiksmīgi veikto pikšķerēšanas uzbrukumu skaitu un rezultātiem pagājušā gada laikā

Lūgums ziedot okeāna tīrišanai

Lūgums sazināties ar sūtītāju pa tālrundi

#### Tabula Nr. 1. Vienkāršākie jautājumi (5 populārākie)

Pirmais jautājums ir par krāpšanas rīkiem. Otrais ir par profilakses pasākumiem. Trešais ir par kiberuzbrukumu definīciju. Ceturtais ir par sociālo inženieriju, bet piektais ir par krāpšanas taktiku, ko izmanto e-pastos.

Tātad, mēs varam redzēt, par ko dalībniekiem bija pietiekami daudz zināšanu pirms apmācības.

#### Izmēģinājuma apmācība: jautājumu sarežģītība: 5 visizaicinošākie jautājumi

Dalībnieku sniegtot atbilžu analīze atklāja visgrūtākos jautājumus. 60-80% dalībnieku uz šiem jautājumiem neatbildēja vai atbildēja nepareizi. Šie jautājumi ir parādīti tabulā zemāk.

#### Top 1. 7. Kāds ir kiberdrošības sertifikācijas sistēmas mērķis?

**Sertificēt IKT produktus, procesus un pakalpojumus**

Izsniegt iegūto kiberdrošības kompetenču sertifikātu, kas ir atpazīstams visā ES

Izsniegt ārpus ES atpazīstamu IKT sertifikātu

Neviena no sniegtajām atbildēm

#### Top 2. 8. Kura direktīva bija pirmais ES mēroga kiberdrošības tiesību akts, kurā drošības prasības tika ieviestas kā juridiskas saistības digitālo pakalpojumu sniedzējiem (DSP) un būtisko pakalpojumu (OES) operatoriem?

E-privātuma direktīva

ES kiberdrošības likums

**NIS direktīva**

Eiropas Elektronisko sakaru kodeksa direktīva

#### Top 3. 3. Kuri apgalvojumi par tālruņu/centrāļu manipulācijām ir pareizi?

**Tālruņu/centrāļu manipulācijas iemācījās kontrolēt tālruņa līnijas, klausoties skaņas, kad operatori savienoja zvanus**

**Tālruņu/centrāļu manipulācijas lasa telefonkompāniju tehniskos žurnālus**

Tālruņu/centrāļu manipulācijas neielauzās birojos, lai izstrādātu savu aparatūru

Tālruņu/centrāļu manipulācijas nerakās pa telefonu kompāniju atkritumu tvertnēm, lai atrastu "slepenus" dokumentus

#### Top 4. 4. Kāda ir atšķirība starp kiberdrošību un datoru drošību?

**Kiberdrošība aptver dažadas IT jomas**

Nav atšķirību

kiberdrošība ir daļa no datoru drošības

kiberdrošība nodarbojas tikai ar interneta draudiem



kiberdrošība ir saistīta ar vīrusiem utt.

#### Top 5. 11. Kuri apgalvojumi par pikšķerēšanas uzbrukumu ir pareizi?

Pikšķerēšana jeb personas datu izmānišana ir sociālās inženierijas krāpniecība, kas var izraisīt datu zudumu, reputācijas bojājumus, identitātes zādzību, naudas zaudējumus un daudzus citus negatīvus efektus individuāliem un organizācijām.

Pikšķerēšanas krāpniecība parasti sākas ar e-pasta ziņojumu, kurā tiek mēģināts iegūt potenciālā upura uzticību un pārliecināt viņu veikt uzbrucējam vēlamās darbības.

Pikšķerēšana ir sistēmas līdzekļa īpašība, kas var radīt sistēmas drošības vājumu vai trūkumu.

Pikšķerēšana apraksta standarta pasākumu, ar kuru draudu aģents īsteno draudus

#### Tabula Nr. 2. Dalībnieku grūtākie jautājumi (Top 5)

Pirmais jautājums bija par kiberdrošības sertifikācijas shēmas mērķi; otrs jautājums bija par šifrēšanas priekšrocībām; trešais jautājums bija par bojātas ierīces īpašībām; ceturtais jautājums bija par NIS direktīvu; piektais jautājums tika uzdots par atšķirībām starp kiberdrošību un datoru drošību.

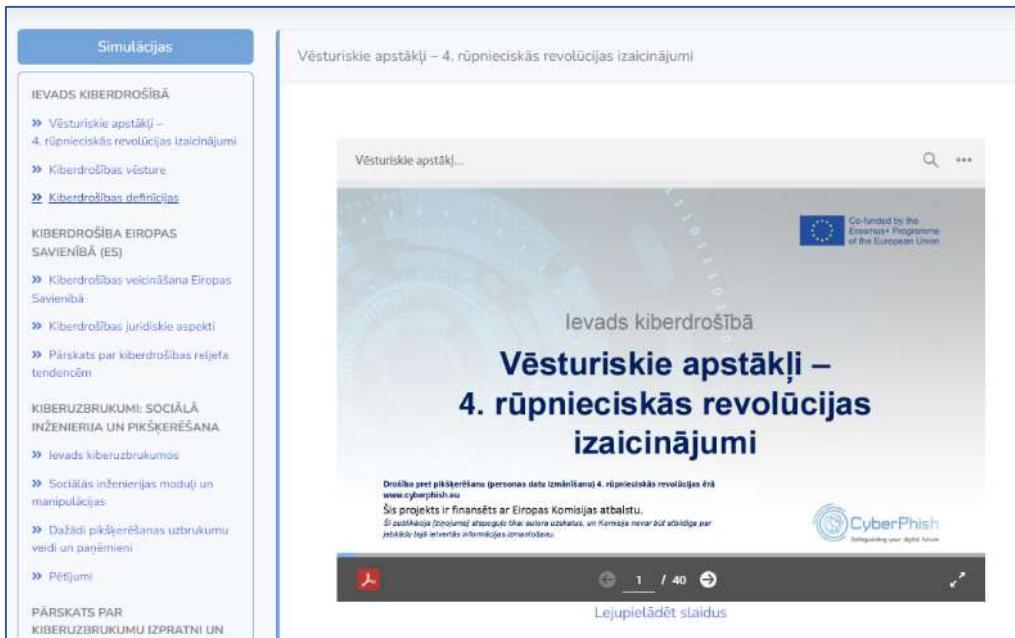
Kā redzams, jautājumi bija saistīti vai nu ar tehniskām tēmām, vai arī ar konkrētiem jautājumiem, piemēram, kiberdrošības sistēmu vai direktīvu.

## Tiešsaistes mācību vide

Izmēģinājuma apmācības notiek sistēmā, ko izstrādā un uztur projekta koordinatore Viļņas Universitāte. Sistēmai var piekļūt, izmantojot saiti <https://cyberphish.vuknf.lt/>. Mācību platformu var izmantot gan reģistrēti, gan nereģistrēti dalībnieki. Nereģistrētie dalībnieki var skatīt vispārīgu informāciju par apmācību kursu, skatīt reitingu tabulas un skatīt vai lejupielādēt apmācību materiālus visās partneru valodās: Angļu, igauņu, grieķu, latviešu un lietuviešu.



Attēls Nr. 4. Tiešsaistes mācību vide



The screenshot shows a presentation slide with the following content:

- Simulācijas**
- IEVADS KIBERDROŠĪBĀ**
  - » Vēsturiskie apstākļi – 4. rūpnieciskās revolūcijas izaicinājumi
  - » Kiberodrošības vēsture
  - » [Kiberodrošības definīcijas](#)
- KIBERDROŠĪBA EIROPAS SAVIENĪBĀ (ES)**
  - » Kiberodrošības velcinātāja Eiropas Savienībā
  - » Kiberodrošības juridiske aspekti
  - » Pārskats par kiberodrošības reljefa tendencēm
- KIBERUZBRUKUMI: SOCIĀLĀ INŽENIERIJA UN PIKŠĶERĒŠANA**
  - » Ievads kiberuzbrukumos
  - » Sociālās inženierijas moduli un manipulācijas
  - » Dažādi pikšķerēšanas uzbrukumu veidi un pamēri
  - » [Pētījumi](#)
- PĀRSKATS PAR KIBERUZBRUKUMU IZPRATNI UN**

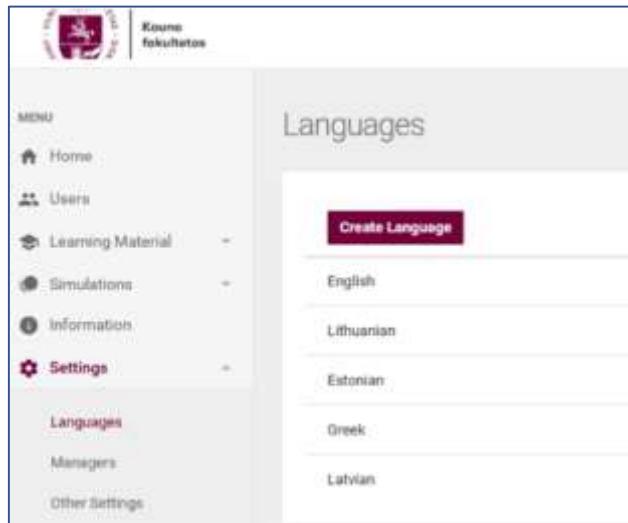
The main slide title is "Vēsturiskie apstākļi – 4. rūpnieciskās revolūcijas izaicinājumi". It includes a footer with the text "Drošība pret pikšķerēšanai (personas dati izmālināti) 4. rūpnieciskās revolūcijas ērā www.cyberphish.eu" and "Šis projekts ir finansēts ar Eiropas Komisijas atbalstu. Šī platforma (tiekoties) atspoguļo viņu autoru uzskatus, un Komisija nevar būt atbildīga par jebkādu tagħiġi tiegħi referenti informācijas izmantošon."

**Attēls Nr. 5. Mācību materiāli tiešsaistes mācību vidē**

#### Trīs tiešsaistes mācību vides lomas

Tiešsaistes mācību vidē ir trīs lietotāju lomas: administrators, vietējais administrators un kursa dalībnieks.

**Administrators** var apskatīt visu lietotāju statistisko informāciju, piemēram, pēdējo pieteikšanos, IP adresi, statusu un e-pasta adresi.



The screenshot shows the "Languages" section of the administrator interface. The left sidebar has a "Settings" menu item selected. The right panel lists languages: English, Lithuanian, Estonian, Greek, and Latvian. A "Create Language" button is visible at the top right of the list.

**Attēls Nr. 6. Sistēmas administratora logs**

**Administrators** var augšupielādēt mācību materiālus, importēt un redīgēt simulācijas, izveidot lokālo administratoru lietotājus un norādīt citas ar e-platformu saistītas darbības, kas citiem lietotājiem nav pieejamas.

**Vietējais administrators** var redzēt statistisko informāciju par lietotāju progresu, kā arī informāciju par veiktajiem pašnovērtējuma testiem un atrisinātajām simulācijām, pēdējās pieteikšanās un zināšanu novērtējuma pārbaudes rezultātiem. Lietotājs var arī apskatīt atrisinātos pašnovērtējuma jautājumus un scenārijus, redzēt, kā dalībnieks atrisināja konkrēto scenāriju un cik punktus ieguvīs par katru atbildi.

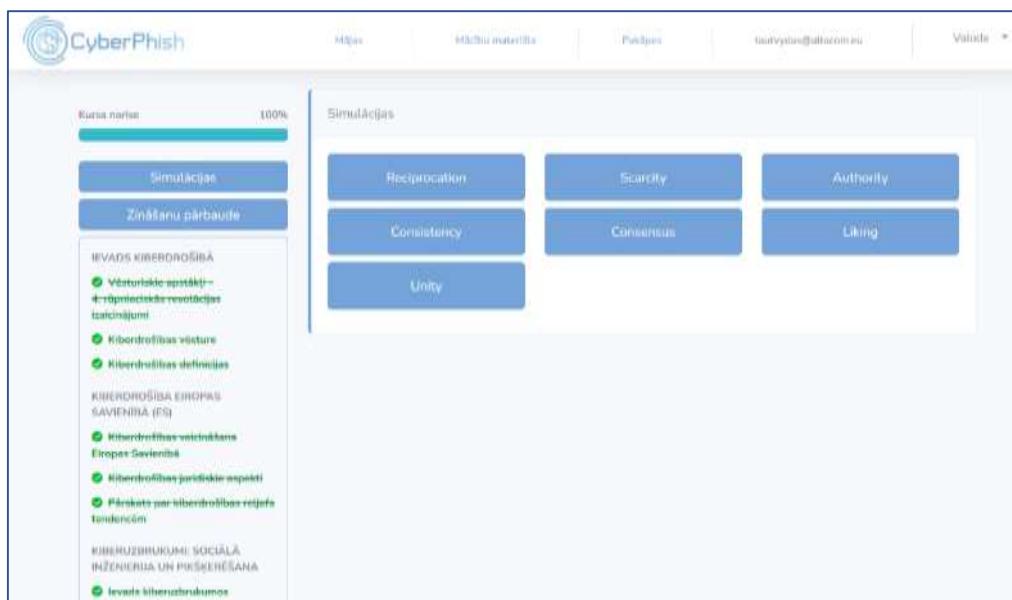


Funded by the  
Erasmus+ Programme  
of the European Union

Users							
Username	Email	Course Progress	Self Evaluation	Simulations	Knowledge results	Last Login	
User12345	user1@user.com	0%	Self Evaluation History	Simulation History (0/1/0)			
User12345	user1@user.com	100%	Self Evaluation History	Simulation History (0/1/13)	100%	2023-08-22 08:01:31	
User12345	user1@user.com	100%	Self Evaluation History	Simulation History (0/1/0)	100%	2023-08-22 08:01:31	
User12345	user1@user.com	100%	Self Evaluation History	Simulation History (0/1/1)	100%	2023-08-22 08:01:31	
User12345	user1@user.com	100%	Self Evaluation History	Simulation History (0/1/0)	100%	2023-08-22 08:01:31	

**Attēls Nr. 7. Vietēja administratora logs**

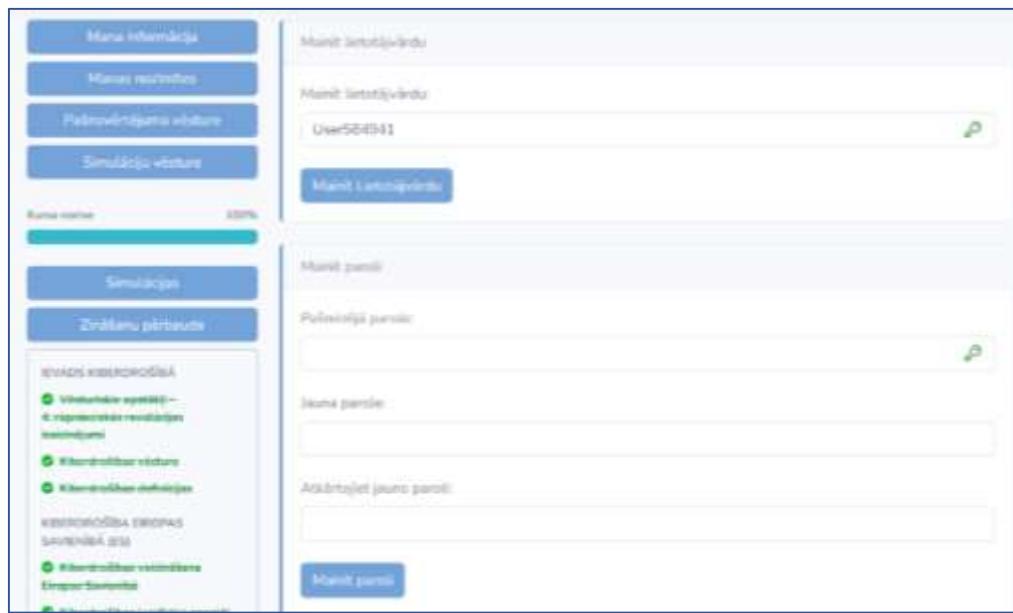
Reģistrētais kursu dalībnieks var izmantot mācību vidi mācību nolūkos. 8. attēlā parādīts kursa dalībnieka loga piemērs.



The screenshot shows a user interface for a CyberPhish course. On the left, there's a sidebar with course navigation and a progress bar at 100% completion. The main area has tabs for 'Mācību materiāls' (Learning materials), 'Pielikumi' (Attachments), and 'Izmaiņas' (Changes). The 'Mācību materiāls' tab is active. It displays several sections: 'IEVADS KIBERDROŠĪBĀ' with topics like 'Vētoriskie epakuļi - 4 rāpnoteciskie rezonējošie izziņojumi', 'Kiberdrošības vēsture', and 'Kiberdrošības definīcijas'; 'KIBERDROŠĪBA EIROPAS SAVIENĪBĀ (FS)' with 'Hizendrofības vērtināšana' and 'Eiropei Savienība'; 'KIBERUZĪBUJUMI: SOCĀLĀ INŽENIERIJA UN PIKEĒRĒŠANA' with 'Pārskats par kiberdrošības reģe' and 'Ievade kiberauzukumos'. On the right, there's a 'Simulācijas' section with categories: Reciprocation, Scarcity, Authority, Consistency, Consensus, and Unity.

**Attēls Nr. 8. Kursa dalībnieku mācību vides logs**

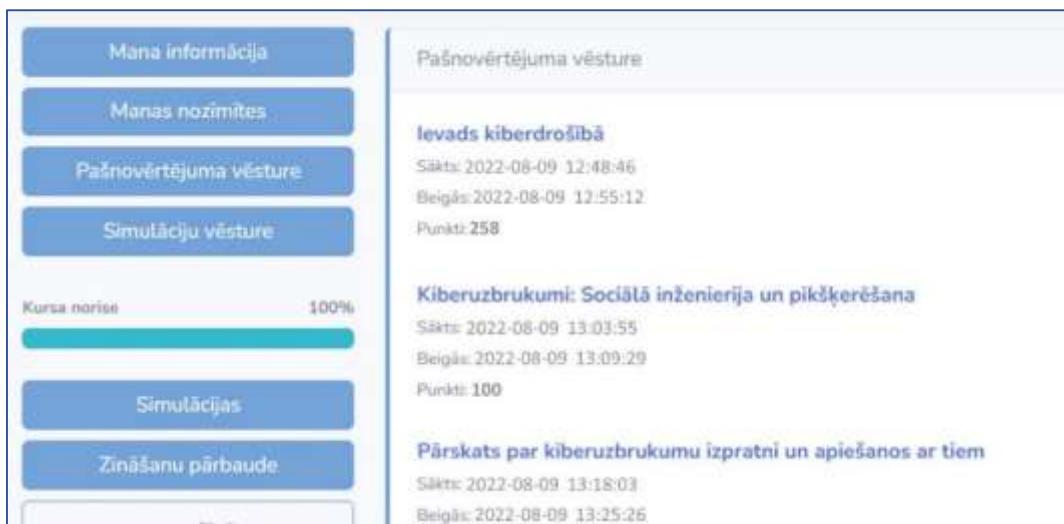
Reģistrējoties kursiem, dalībnieks var mainīt informāciju par sevi, t.i., lietotājvārdu un paroli (skat. 9. attēlu).



The screenshot shows a user profile page. On the left, there's a sidebar with buttons for 'Manā informācija', 'Manas nozīmītes', 'Pielikovērtējuma vēsture', 'Simulāciju vēsture', 'Kursa norise' (progress bar at 100%), 'Simulācijas', and 'Zināšanu pārbaude'. Below these are sections for 'IEVĀDĀS KIBERDROŠĪBĀI', 'KIBERDROŠĪBAS EKSPERTĀS SAŅĒMĒJĀS', and 'KIBERDROŠĪBAS VĒSTURE' (with a note about the scenario being used). On the right, there are fields for 'Manā ietvertīvā līnija' (with 'User564941'), 'Manā latvīgā līnija' (with a green checkmark), 'Manā pasīti' (with a green checkmark), and 'Pielikovērtējuma parole' (with a green checkmark). There are also fields for 'Jauna parole' and 'Arakērtīgā jauno parole'.

**Attēls Nr. 9. Kursa dalībnieka personīgās informācijas iestatīšanas logs**

Kā reģistrēts kursu dalībnieks varat sekot līdzī pašpārbaudes vēsturei un zināšanu pārbaudes vēsturei un redzēt, cik žetonu esat noplīnījis (skat. 10. attēlu).



The screenshot shows the 'Pašnovērtējuma vēsture' section. It lists a completed assessment titled 'Ievads kiberdrošībā' with the following details: Sākts: 2022-08-09 12:48:46; Beigās: 2022-08-09 12:55:12; Punkti: 258. Below it is another entry: 'Kiberuzbrukumi: Sociālā inženierija un pikēkerēšana' with the following details: Sākts: 2022-08-09 13:03:55; Beigās: 2022-08-09 13:09:29; Punkti: 100. At the bottom, there's a link to 'Pārskats par kiberuzbrukumu izpratni un apiešanos ar tiem'.

**Attēls Nr. 10. Kursa dalībnieka pašnovērtējuma pārbaudes vēstures logs**

Kā reģistrēts kursu dalībnieks varat sekot līdzī veikto/atrisināto simulāciju vēsturei:

- kad un kā jūs atbildējāt uz jautājumiem;
- Kādus scenārijus jūs atrisinājāt;
- Cik punktus esat ieguvis par katru no tiem.



The screenshot shows a user interface for a cybersecurity course. On the left, a sidebar lists course sections: 'Manā informācija', 'Manas nozīmības', 'Pašnovērtējuma vēsture', and 'Simulāciju vēsture'. Below this is a progress bar labeled 'Kursa mācīšie' at 100%. A large blue button at the bottom says 'Simulācijān'. The main area is titled 'Simulāciju vēsture' and contains three entries:

ID: 92	ID: 92	ID: 92
Aktieri: Uzņēmumu adreses, Uzņēmuma klienti Tips: Emails	Aktieri: Uzņēmumu adreses, Uzņēmuma klienti Tips: Emails	Aktieri: Uzņēmumu adreses, Uzņēmuma klienti Tips: Emails
Uzbrukuma veids: GDPR related attacks	Uzbrukuma veids: GDPR related attacks	Uzbrukuma veids: GDPR related attacks
Sākts: 2022-08-10 10:22:16 Beigās: 2022-08-10 10:25:53 Punkti: 200	Sākts: 2022-08-10 10:27:45 Beigās: 2022-08-10 10:31:50 Punkti: 500	Sākts: 2022-08-10 10:35:44 Beigās: 2022-08-10 10:38:18 Punkti: 400

**Attēls Nr. 11. Kursa dalībnieku simulācijas vēstures logs**

### Žetoni

Pirms izmēģinājuma apmācības partneri vienojās par sešiem žetoniem. Tomēr projekta laikā tika izveidoti astoņi žetoni:

- testa nokārtošana;
- kursa pabeigšana;
- visu simulāciju pabeigšana;
- pirmais pašnovērtējuma tests;
- kategorijas un tēmas pabeigšana;
- visu prezentāciju izskatīšana;
- pieteikšanas sistēmā desmit dienas pēc kārtas.

12. attēls žetonu piemēri.



**Attēls Nr. 12. Žetonu piemēri**

### Vērtēšana

Reģistrētie kursu dalībnieki var vākt punktus par pašpārbaudēm saskaņā ar partneru saskaņotiem noteikumiem. Šie punkti tiek parādīti tabulā Pašnovērtējuma reitingi. Kursu dalībnieka vārds un rezultāts tiek parādīts kopā.

Pašnovērtējuma rangi		
Posicija	Lietotājvārds	Punkti
1	Viktoria.V	1998
2	Oleg4.	1597
3	User774920	432
4	User446990	233
5	User731791	98

**Attēls Nr. 13. Reģistrēto kursu dalībnieku reitingi**



### Mācību materiāli tiešsaistes mācību vidē

Partneru konsorcijas izstrādāja tiešsaistes mācību materiālu, ievērojot Cyberphish mācību programmu<sup>2</sup> un atbilstoši 4. industriālās revolūcijas vajadzībām. Izstrādāto mācību materiālu labi novērtēja neatkarīgi eksperti (viens no katras partnervalsts).

4. tabulā ir sniegs izstrādātā mācību materiāla kopsavilkums.

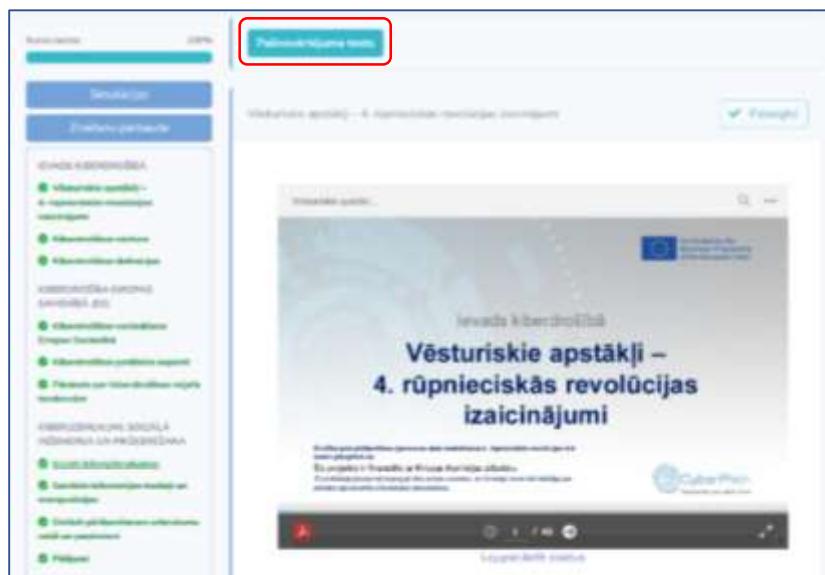
Moduļi un apakštēmas				Slaidu skaits
1	Ievads kiberdrošībā	1.1	Vēsturiskie apstākļi – 4. rūpnieciskās revolūcijas izaicinājumi	40
		1.2	Kiberdrošības vēsture	31
		1.3	Kiberdrošības definīcijas	15
2	Kiberdrošība Eiropas Savienībā (ES)	2.1	Kiberdrošības veicināšana Eiropas Savienībā	31
		2.2	Kiberdrošības juridiske aspekti	14
		2.3	Pārskats par kiberdrošības relijefa tendencēm	41
3	Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana	3.1	Ievads kiberuzbrukumos	20
		3.2	Sociālās inženierijas moduļi un manipulācijas	73
		3.3	Dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni	37
		3.4	Pētījumi	37
4	Kiberuzbrukumu izpratne un to risināšana	4.1	Pamatzināšanas par e-drošību	22
		4.2	Proaktīvas darbības;	59
		4.3	Pikšķerēšanas uzbrukumu atpazīšana	108
		4.4	Kiberuzbrukumu risināšana	87
		4.5	Bojājumu samazināšana līdz minimumam, reagējot uz incidentiem,	34
			<b>Kopā:</b>	<b>649</b>

**Tabula Nr. 3. Mācību materiālu kopsavilkums**

### Uzdevumi tiešsaistes mācību vidē

Kursa saturu var apskatīt uz ekrāna un/vai lejupielādēt .pdf formātā. Kad reģistrētais dalībnieks ir iepazinies ar visu mācību materiālu par konkrēto tēmu, viņš var pārbaudīt savas zināšanas, veicot pašpārbaudi. Par to tiks piešķirti punkti.

<sup>2</sup> CyberPhish paplašinātā mācību programma: [https://cyberphish.eu/wp-content/uploads/2022/12/I02-A2\\_Extended-version-of-curricula\\_LV.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/I02-A2_Extended-version-of-curricula_LV.pdf)



Attēls Nr. 14. Pašnovērtējuma testa poga kursa dalībnieka vidē

Ievads kiberdrošībā Pašnovērtējuma tests

Kādas cilvēka dzīves jomas ietekmē programmatūra un informācijas sistēmas?

- Lielo datu analīze
- Mākoņskaitļošana
- Neviens no sniegtajām atbildēm
- Lietu interneta (IoT)

Nākamais

40%

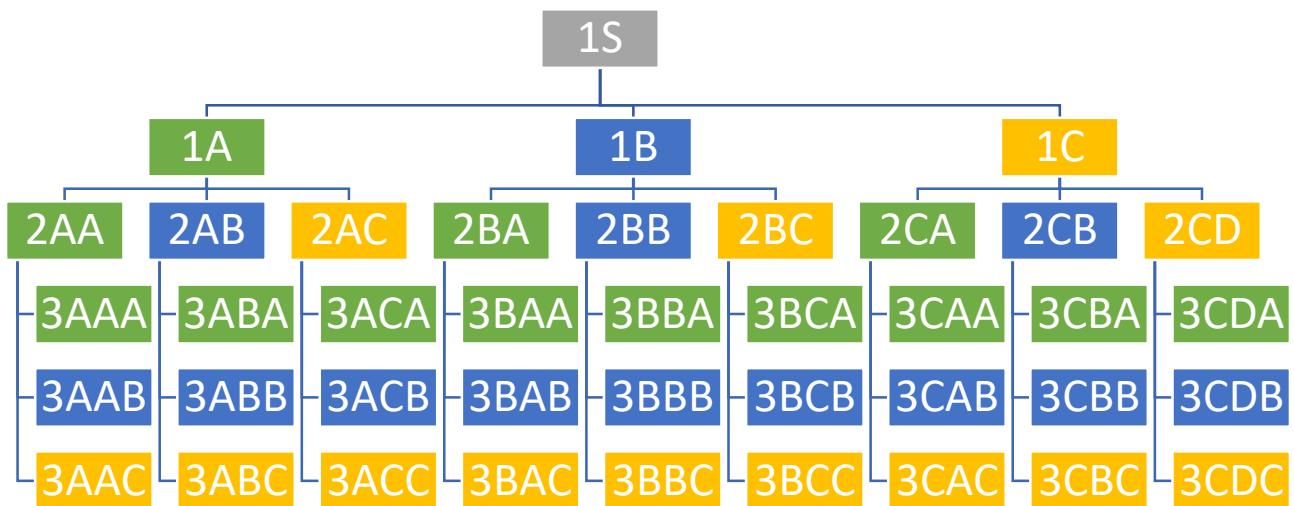
Attēls Nr. 15. Pašnovērtējuma testa fragments

### Simulācijas

Simulācija simulē faktiskus krāpšanas uzbrukumus, parādot procesu lietotājam rotaļīgā formā. Simulācijas mērķis ir palīdzēt cilvēkiem uzlabot kritisko domāšanu par kiberdrošību un krāpšanu, atpazīstot pikšķerēšanu, surogātpastu, kiberhuligānismu un citus incidentus. Projekta partneri izstrādāja 55 simulācijas.

Simulācija ietver situācijas aprakstu, mērķi, varoņus, uzbrukuma veidu un vairākas (3- 4) atbildes iespējas lietotāja rīcībai.

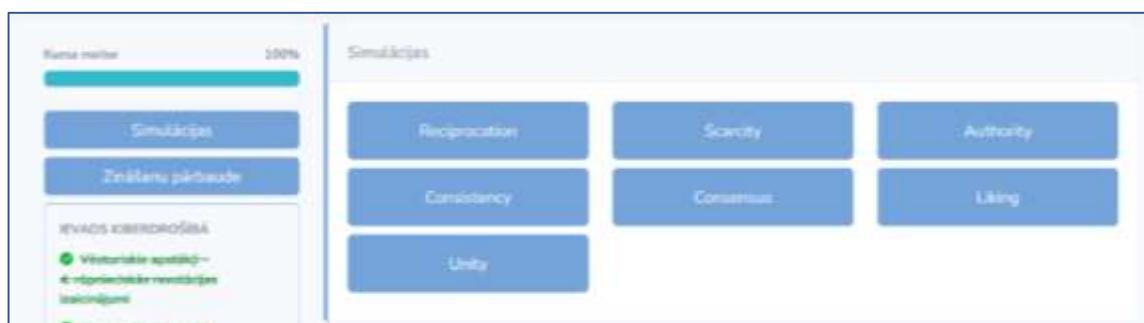
Visas simulācijas ir balstītas uz lēmumu koka pieeju. 15. attēlā parādīts simulācijas modelis. Katrai simulācijai ir trīs līmeņi. Kopējais opciju skaits (iespējamie varianti) ir vismaz 50, bet ne vairāk kā 84 opcijas.



Attēls Nr. 16. Simulācijas modelis ir balstīts uz lēmumu koka pieeju

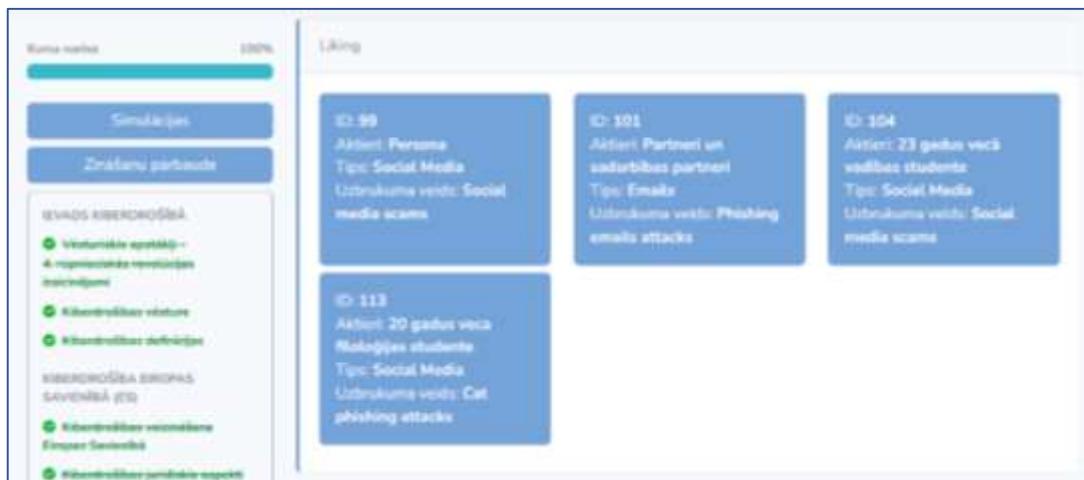
Simulācijā katra lietotāja izvēlētā atbilde ved uz nākamo iespējamo atbilžu variantu līmeni. Simulācijā ir trīs veidu risinājumi: pareizi, daļēji pareizi un nepareizi. Par katru atbildi sistēma kursa dalībniekiem piešķir noteiktu punktu skaitu. Sistēma parāda atgriezenisko saiti uz ekrāna, ja ir izvēlēta daļēji pareiza vai nepareiza atbilde. Sniegti arī priekšlikumi, kuru materiāla daļu studentam vajadzētu atkārtot un kuru tēmu sīkāk aplūkot.

Dalībnieks var izvēlēties simulācijas pēc tēmas/kategorijas.



Attēls Nr. 17. Simulācijas kategorijas/tēmas

Simulācijas var izmantot divos veidos: mācībām un zināšanu pārbaudei. Vienā veidā atgriezeniskā saite dalībniekiem tiek sniepta pēc katras situācijas, bet otrā - tikai pēc tam, kad ir pabeigts viss simulācijas scenārijs. Par simulāciju risināšanu tiek piešķirti punkti, bet par visu scenāriju risināšanu tiek piešķirts žetons.



Kursa nārķe: 100%

Simulācijas

Zināšanu pārbaude

LEIVĀDS KIBERĀDĀZĀ

- Vēlētošķeles spēkstāji - 4. hipnotizēšanas metodes
- Kibernetiskās vārstības
- Kibernetiskais definīcijas

KIBERĀDĀZĀ EIROPS  
SAVENĀBĀ (EIS)

- Kibernetiskais vārstībās  
Eiropas Savienībā
- Kibernetiskais jūtīgāsības

Likting

ID: 99  
Autors: Personas  
Tipi: Social Media  
Uzbrukuma veids: Social media scams

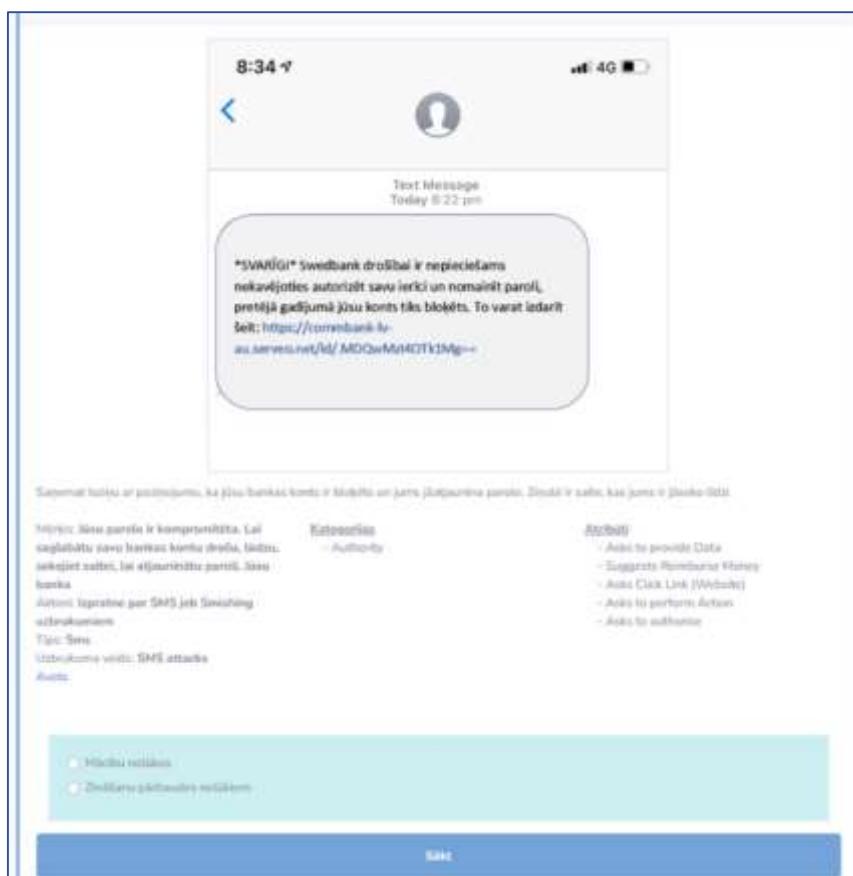
ID: 101  
Autors: Partneri un  
sadarbības partneri  
Tipi: Emails  
Uzbrukuma veids: Phishing emails attacks

ID: 113  
Autors: 20 gadus vecā  
Mācījējus studentes  
Tipi: Social Media  
Uzbrukuma veids: Cat phishing attacks

### Attēls Nr. 18. Simulāciju izvēle tēmā Patīk

Pēc simulācijas izvēles kursa dalībniekam tiek parādīts situācijas apraksts, simulācijas mērķis, varoņi, pikšķerēšanas uzbrukuma veids un citi atribūti. Bieži (bet ne vienmēr) attēls tiek rādīts, lai uzlabotu iespāidu (lai padarītu dalībnieku empātiskāku).

Pēc tam ir iespēja izvēlēties simulācijas mērķi: mācību nolūkiem vai zināšanu pārbaudei.



8:34 AM 4G

< Text Message Today 8:22 PM

\*SWĀRĪGI! Swedbank drošībal ir nepieciešams nekavējoties autorizēt savu ierīci un nomairīt paroli, pretējā gadījumā jūsu konts tiks blokēts. To varat izdarīt šeit: <https://commbank.lv- au.services.net/lb/MODQwMh407k1Mg-->

Sākumā būtu ar prioritētu, ka jūsu bankas konts ir blokēts un jums jāizjauno paroli. Zināt ir saņēt, kas jums ir jāzinaši.

MĒRĶS: Jāņa gārtne ir kompromitēta. Lai saglabātu savu bankas kontu droši, lūdz, saņemiet zīmi, lai atjauninātu paroli. Jāņa banka  
Automa izpratne par SkRS jeb Swedbank  
uzbrukumiem  
Tipi: Sms  
Uzbrukuma veids: SMS attack  
Autors:

Kategorijas: Automa

Ezīmējumi:

- Automa notikums
- Zināšanu pārbaude notikums

Sākt

### Attēls Nr. 19. Simulācijas risinājuma piemērs

Kad simulačija ir sākusies, dalībniekam tiek piedāvātas izvēles iespējas. Viņiem ir jāizvēlas, kā viņš/viņa rīkosies šādā situācijā. Zemāk redzamajā attēlā parādīts simulačijas risinājuma piemērs.



Simulācija

Novērtāt, vai ziņojums ir likumīgs  
 Neklākības uz saitām  
 Brīdiniet cilvēku par ziņojumu  
 Atzīst un izdzīst e-pastu un neko nedarīt.

**Nākamais**

**Attēls Nr. 20. Simulācijas risinājums**

Simulācijas laikā lietotājs saņem atgriezenisko saiti uz ekrāna, kad tiek izvēlēta nepareiza vai daļēji pareiza atbilde. 21. attēls ilustrē lietotājam uz ekrāna redzamo atgriezenisko saiti simulācijas risināšanas laikā.

Simulācija

Tas vielā mērā ir atkarīgs no jūsu brīdinājuma konteksta.

Ziņojiet par e-pastu māksla ortīclības un drošības komandai uz report.phishing@airbnb.com;  
 Brīdiniet savus draugus par šādu Airbnb e-pastu  
 Esiet piesārtīgi, ja e-pastus tiek pieprasīta izdzīzamais laiks.  
 Ja Airbnb ir jūsu biznesa partneris, informējiet par šo ziņojumu sava uzņēmuma kolēģus.

**Nākamais**

**Attēls Nr. 21. Uz ekrāna redzamā atgriezeniska saite simulācijas risināšanas laikā**

Kad simulācija ir pabeigta, lietotājam tiek parādīts ziņojums, kurā redzams iegūto punktu skaits un aicinājums atrisināt citas simulācijas. Ja simulācija tika atrisināta nepareizi, tiek sniegts ieteikums simulāciju atrisināt vēlreiz (skat. 21. attēlu).

Simulācija

Varamu ieviešt draugu datorus ar jaunprātīgu programmasdāru.

**Simulācija pabeigta!**  
Savākti punkti: 200

**Veiciet šo simulāciju vēlreiz!**

**Otrs simulačjons**

**Attēls Nr. 22. Pabeigtās simulācijas logs**

**Zināšanu vērtēšanas tests**

Pēc mācību materiāla apguves (pašpārbaudes un simulācijas) dalībniekiem mācību vidē būs pieejama poga, lai veiktu zināšanu pārbaudi. Izmēģinājuma apmācību laikā zināšanu testu var kārtot trīs reizes.



The screenshot shows a user interface for a knowledge test. On the left, there's a sidebar with a progress bar at 70% and buttons for 'Sākums' (Start) and 'Zināšanu pārbaude' (Knowledge check). Below these are sections for 'LEVADS KIBERDROŠĪBĀ' (including 'Vidējums' - Average, 'Kibernetiskās sistēmas' - Computer systems, 'Kibernetiskās vidiņi' - Network, 'Kibernetiskās definīcijas' - Definitions), 'KIBERDROŠĪBA, KIBOPĀL' (including 'SAVĒRĒJĀ ESIS' - Computer Emergency Response Team, 'Kibernetiskās viedotākās ESIS' - Computer Emergency Response Team, 'Kibernetiskās viedotākās apdzīvi' - Computer Emergency Response Team), and 'ZINĀŠANU TESTS' (Knowledge test).

In the main panel, the title 'Zināšanu pārbaude' is at the top. Below it is the question 'Ko nozīmē CERT?' with four options:

- Datora avāriju reagēšanas komanda (Computer Emergency Response Team)
- Datora efektivitātes reagēšanas komanda (Computer Efficiency Response Team)
- Visaptverīga ar klūdām saistīta testātana (Comprehensive Error-Related Testing)
- Demoralizē un efektīvs atliktošas iekārtas pārtraukums (Computerised and Efficient Removal)

A blue 'Nākamais' (Next) button is at the bottom right.

**Attēls Nr. 23. Zināšanu vērtēšanas testa jautājuma piemērs**

Zināšanu testa beigās kursa dalībnieks redz procentuālo daļu no savu zināšanu novērtējuma.



The screenshot shows a summary screen after a test. It has a header 'Zināšanu pārbaude' and a note 'Jūs atjaunāt izmēģināt šo testu tikai 3 reizes'. Below that is 'Testējums: 1/3' and a large blue 'Sākt' (Start) button. At the bottom, it says 'Rezultāts 70%'.

**Attēls Nr. 24. Zināšanu vērtēšanas testa novērtējumu loga piemērs**

**Piezīme:** Zināšanu tests ir paredzēts zināšanu novērtēšanai. Šis tests nav paredzēts mācību nolūkiem. Zināšanu testi netiek publiski izpausti dalībniekiem, mentoriem un/vai skolotājiem. Jautājumi teksta formātā ir pieejami visiem projekta partneriem/izstrādātājiem un sistēma nenodrošina pieeju detalizētiem testa rezultātiem. Citi mentori/skolotāji arī nevarēs skatīt pilnus testa rezultātus.

#### Zināšanu testi

Partneri ir vienojušies izstrādāt jautājumus pašpārbaudēm un jautājumus zināšanu testiem, pamatojoties uz pieteikumā sniegtog informāciju. Būs šāda veida jautājumi.

#### Pašnovērtējuma testos būs trīs veidu jautājumi:

- jautājumi ar atbilžu variantiem ar vienu pareizo atbildi (iespējamo atbilžu skaits: 3-6),
- jautājumi ar atbilžu variantiem (4-6 iespējamās atbildes),
- jā/nē jautājumi.

Partneri ir vienojušies/pieņēmuši lēmumu par jautājumu skaitu/jautājumu daudzumu katrai mācību materiāla tēmai. Piemēram, 8-14 jautājumi no tēmām "Ievads kiberdrošībā" un "Pārskats par kiberdrošību ES". Izveidojet 12-20 jautājumus katrai no tēmām "Kiberuzbrukumi – sociālā inženierija un pikšķerēšana" un "Kiberuzbrukumu izpratne un pārvaldība".

Specifikācija pašnovērtējuma jautājumiem:

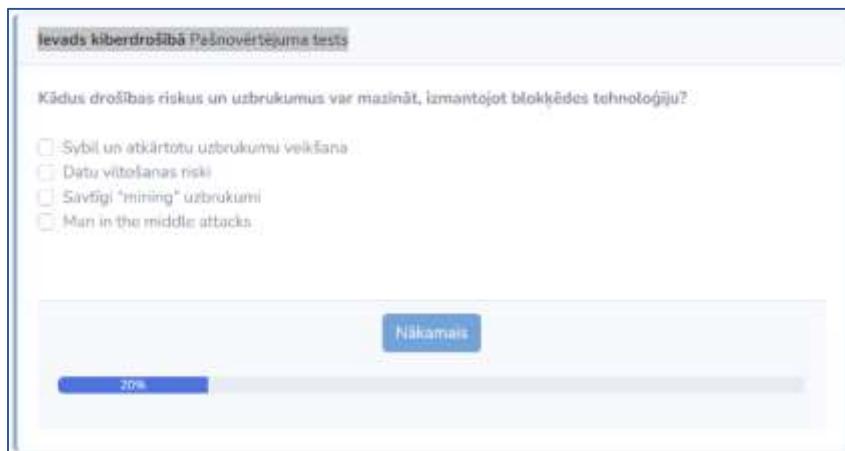


Moduļi	Izstrādāti pašnovērtējuma jautājumi
Ievads kiberdrošībā	13
Pārskats par kiberdrošību ES	12
Kiberuzbrukumi — sociālā inženierija un pikšķerēšana	16
Kiberuzbrukumu izpratne un to risināšana	19
<b>Kopā:</b>	<b>60</b>

**Tabula Nr. 4. Pašnovērtējuma testa jautājumu specifikācija**

Mācību vidē parādās poga "Pašnovērtējuma tests", kad ir pārskatītas visas konkrētā moduļa apakštēmas. Tests sastāv no pieciem jautājumiem. Jautājumi tiek nejauši atlasīti no pašreizējās kategorijas jautājumu bankas.

Pašnovērtējuma testa laikā ekrāna apakšā tiek parādīta progresu josla, kas parāda atbildēto jautājumu procentuālo daļu un atlikušo jautājumu skaitu.



The screenshot shows a poll interface with the title "Ievads kiberdrošībā Pašnovērtējuma tests". The question is: "Kādus drošības riskus un uzbrukumus var mazināt, izmantojot blokķēdes tehnoloģiju?". There are four options with checkboxes:

- Sybil un atkārtotu uzbrukumu veikšana
- Datu vītolanas niski
- Savīdi "mining" uzbrukumi
- Man in the middle attacks

A progress bar at the bottom indicates "20%" completion. A blue button labeled "Nākamais" is visible above the progress bar.

**Attēls Nr. 25. Piemērs pašnovērtējuma testa jautājumam kategorijā "Ievads kiberdrošībā"**

Pašnovērtējuma testa beigās dalībniekam tiek parādītas pareizās un nepareizās atbildes. Dalībnieka atzīmētās atbildes ir izezīmētas zaļā krāsā. Dalībnieks ekrāna augšējā labajā pusē redz sākuma datumu un laiku, beigu datumu un laiku, kā arī iegūto punktu skaitu.

Pašnovērtējuma testu skaits nav ierobežots. Kursu dalībnieki to var lietot tik bieži, cik vēlas. Nākamajā reizē, kad viņi veiks testu, viņiem tiks uzdoti citi nejauši izvēlēti jautājumi.

Dalībniekiem tiks piešķirts arī žetons saskaņā ar noteikumiem, par kuriem vienojušies partneri.



levads kiberdrošībā Pašnovērtējuma tests

Izmaiņa to vērtētā

Sākts: 2022-06-28 13:07:52  
Beigās: 2022-06-28 13:08:47  
Punkti: 66

Kādi ir drošības apdraudējumu veidi?

- Pareizā atbildē
- Nepareiza atbildē
- Atlaistā atbildē

Kādi ir drošības apdraudējumu veidi?

- Kriptoloģija un vienkāršums
- Atzīkums un informācijas izraudzīšana
- Atzīkums pilnīgumam un privātību pieteikšanai
- Nievienā no minētajām atbildēm

Kas ir SSL?

- Secure Socket Layer
- Solid Stateless Lightning
- Safety Socket Layer
- Stainless Steel Landing

Kāda ir attīstība starp kiberdrošību un datoru drošību?

- kiberdrošība aptver daļās IT jomas
- tie ir vienādi
- kiberdrošība ļauja novērst datora drošību
- kiberdrošība atbēcas tikai uz draudiem internetā
- kiberdrošība ir saistīta ar virušiem utt

Kuri no tiem nav kiberuzbrukuma veids?

- Cyber exploit
- SQL injection
- Zero day exploit
- DNS tunneling

Kuri no šiem jēdzieniem vislabāk raksturo jēdzienu "kiberuzbrukums" darbības jomu?

- Iebūvētais jaunais hīps darbības kibērēpā, pat ja tās ir neveiksmīgas
- Kaitīgas darbības internetā
- Virusu un Trojas zirgu sūtīšana, izmantojot e-pasta vai SMS ziņojumus
- Veiksmīgi pilēķenēšanas uzbrukumi

### Attēls Nr. 26. Pašpārbaudes rezultātu piemērs

**Zināšanu testi.** Partneri vienojušies arī par Zināšanu testos uzdodamo jautājumu skaitu.

- Uz visiem jautājumiem būs četras atbildes, no kurām tikai viena būs pareiza
- Izveidojiet 144 zināšanu pārbaudes jautājumus.

Zināšanu tests sastāvēs no 36 jautājumiem. Testa aizpildīšana aizņems līdz 45 minūtēm. Jāiegūst 75 %.

Partneri ir vienojušies par jautājumu skaitu katrai mācību materiāla tēmai. Piemēram, 20-25 jautājumi no tēmām "Ievads kiberdrošībā" un "Pārskats par kiberdrošību ES". Izveidojiet 45-65 jautājumus katrai no tēmām "Kiberuzbrukumi – sociālā inženierija un pikšķerēšana" un "Kiberuzbrukumu izpratne un pārvaldība".

Zināšanu novērtēšanas testu jautājumu specifikācija:

Moduļi	Izstrādāti zināšanu testa jautājumi
Ievads kiberdrošībā	24
Pārskats par kiberdrošību ES	20
Kiberuzbrukumi — sociālā inženierija un pikšķerēšana	62
Kiberuzbrukumu izpratne un to risināšana	46
<b>Kopā:</b>	<b>152</b>

**Tabula Nr. 5. Zināšanu novērtēšanas testu jautājumu specifikācija**

Izmēģinājuma apmācību laikā zināšanu testu skaits bija ierobežots. Maksimālais šo testu kārtošanas reižu skaits ir 3.



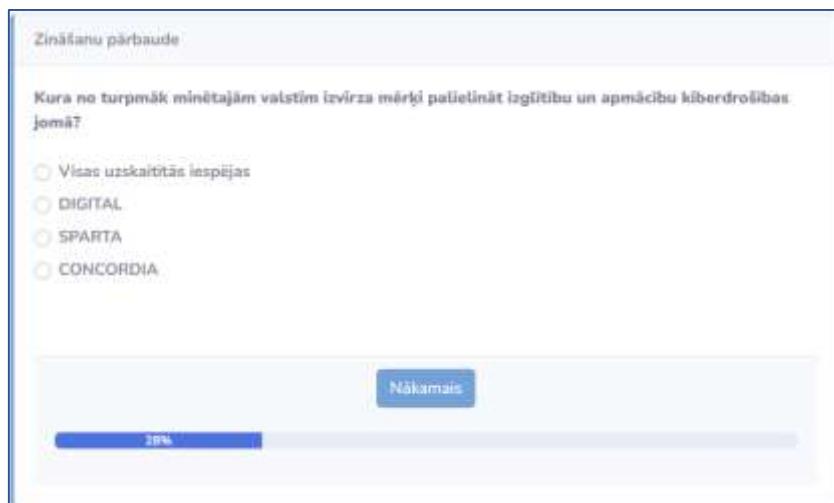
Mācību vidē zināšanu testu poga ir pieejama, kad ir pabeigts viss kurss. Noklikšķinot uz testa pogas, tiek parādīts, cik mēģinājumu dalībniekam ir jāveic, lai pabeigtu testu. Ja tests ir pildīts iepriekš, iepriekšējā testa rezultāts tiek parādīts procentos.



The screenshot shows a light blue header bar with the text "Zināšanu pārbaude". Below it is a white main area. At the top center, there is a message: "Jūs atjaunojat izmēģināt šo testu tikai 3 minūtes." Below that, it says "Testa līmeņs: 1/3". A large blue horizontal progress bar is centered, with the word "Sākt" (Start) written in white in its middle section. At the bottom right of the main area, the text "Rezultāts: 70%" is displayed.

**Attēls Nr. 27. Zināšanu testa sākuma logs**

Zināšanu tests sastāv no 36 nejauši izvēlētiem jautājumiem. Ir iestatīts noteikums par jautājumu skaitu, kas nejauši jāizvēlas no katras kategorijas. Testa laikā progresā josla parāda atbildēto jautājumu procentuālo daļu un atlikušo jautājumu skaitu. Testa beigās tiek parādīts testa rezultāts, bet dalībnieks nevar redzēt, kā viņš ir atbildējis uz jautājumiem, jo šis ir zināšanu pārbaudes tests.



The screenshot shows a light blue header bar with the text "Zināšanu pārbaude". Below it is a white main area. At the top center, there is a message: "Kura no turpmāk minētajām valstīm izvirza mārkī palielināt izgūtību un apmācību kiberdrošības jomā?" Below that, there is a list of four options, each preceded by a small circular icon:

- Vissas izaugsmei līspējas
- DIGITAL
- SPARTA
- CONCORDIA

A large blue horizontal progress bar is centered, with the word "Nākamais" (Next) written in white in its middle section. At the bottom right of the main area, the text "20%" is displayed.

**Attēls Nr. 28. Zināšanu vērtēšanas testa jautājuma piemērs**

Ja dalībnieki testu nenokārto, viņi var mēģināt atkārtot mācību materiālu, kārtot pašnovērtējuma testus un vēlreiz mēģināt nokārtot zināšanu testu.

Veiksmes gadījumā dalībniekam tiek dota iespēja ievadīt savu vārdu un lejupielādēt sertifikātu .pdf formātā.



Funded by the  
Erasmus+ Programme  
of the European Union

Zināšanu pārbaudie

Tests ir pabeigts!

Jūs izturējāt!

Rezultāts: 83%

Lejupielādēt sertifikātu

Pilnais vārds:

Vārds Uzvārds

Mainīt pilno vārdu

Lejupielādēt sertifikātu



**Attēls Nr. 29. Nokārtota zināšanu testa logs**

### Sertifikāts

Pēc testa nokārtošanas dalībnieks saņem saiti, lai aizpildītu pēctesta anketu, pēc kuras var aizpildīt savu vārdu un lejupielādēt sertifikātu PDF formātā. Šī sertifikāta izsniegšanas metode atvieglo sertifikāta izsniegšanas procesu.

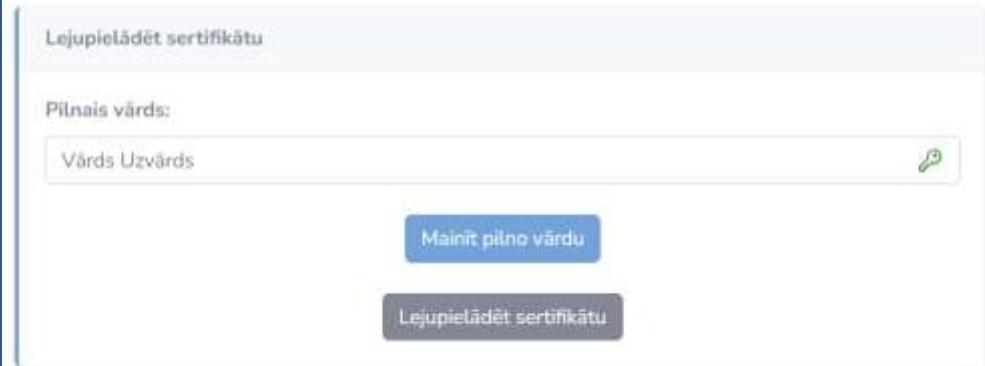
Lejupielādēt sertifikātu

Pilnais vārds:

Vārds Uzvārds

Mainīt pilno vārdu

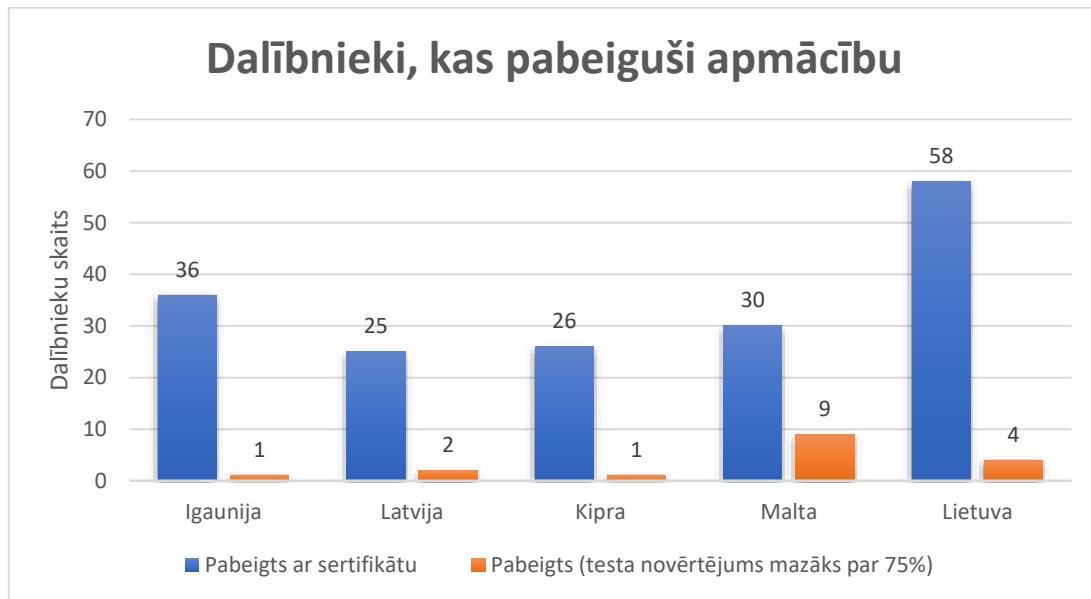
Lejupielādēt sertifikātu



**Attēls Nr. 30. Sertifikātu ģenerēšanas logs**

### Dalībnieki, kas pabeidza apmācību

Zemāk esošajā attēlā ir parādīti apmācības kursa rezultāti. Simt septindesmit pieci dalībnieki pabeidza (175) apmācību kursu un saņēma sertifikātu: 36 Igaunijā, 25 Latvijā, 26 Kiprā, 30 Maltā un 58 Lietuvā. Vēl 17 dalībnieki kursu pabeidza bez sertifikāta, t.i., viņu zināšanu pārbaudes rezultāts bija zem 75%.



**Attēls Nr. 31. Statistika par lietotājiem, kuri ir pabeiguši apmācību**

Pēcpāmācības anketas aizpildīja un iesniedza 139 dalībnieki: 31 Igaunijā, 24 Latvijā, 16 Kiprā, 27 Maltā un 40 Lietuvā.

Pēcapmācības anketas aizpildīja 8 skolotāji: 2 Maltā, 3 Lietuvā un 1 Igaunijā, Latvijā un Kiprā. Skolotāji bija vienisprātis, ka kurss sasniedza savu mērķi iepazīstināt studentus ar kiberdrošību un pilķķerēšanu (tāds pats procents respondentu norādīja, ka piekrīt un pilnībā piekrīt apgalvojumam). Respondenti piekrīt (62,5 %) un pilnībā piekrīt (37,5 %), ka programmā ietverto tēmu detalizācijas apjoms bija atbilstošs. Lielākā daļa skolotāju (62,5%) pilnībā piekrīt apgalvojumiem "Dalībniekiem izmēģinājuma kursa pabeigšanai atvēlētais laiks bija pietiekams" un "Kursa aptvertās tēmu jomas bija piemērotas mērķauditorijai".

Skolotāji komentēja, ka kurss ir labi izstrādāts un attīsta dalībnieku izpratni un kritisko domāšanu. Tā ieviešanai nevajadzētu aprobežoties tikai ar IKT saistītiem kursiem, bet gan daļēji vai pilnībā jāievieš dažados kursos. Vislabākās atsauksmes bija par scenāriju risinājumiem.

Dalībnieku zināšanu salīdzinājums pirms un pēc izmēģinājuma apmācības

Salīdzinot zināšanu novērtējumu pirms un pēc apmācības, atklājās, ka dalībnieki būtiski uzlaboja savas zināšanas par kiberdrošību un pikšķerēšanu. Zemāk esošajā grafikā parādīts, kā dalībnieku zināšanas par kiberdrošību un krāpšanu izskatījās pirms un pēc izmēģinājuma apmācības. Horizontālā ass parāda punktu diapazonus (atzīmes), un vertikālā ass parāda skolēnu procentuālo daļu ar atbilstošo punktu skaitu.

Tādējādi attēlā redzams, ka pēc CyberPhish apmācības dalībnieku rezultāti ievērojami uzlabojās, t.i., vairāk studentu ieguva 8 vai augstākus vērtējumus. Tīkmēr to dalībnieku skaits, kuri neizturēja zināšanu pārbaudi, t.i., ar punktu skaitu no 0 līdz 6, samazinājās.



**Attēls Nr. 32. Dalībnieku zināšanas par kiberdrošību un pikšķerēšanu pirms un pēc izmēģinājuma apmācības**

## 6. IZMĒGINĀJUMA APMĀCĪBAS PARTNERU VALSTĪS

Šajā nodaļā ir atspoguļota partnervalstu – Igaunijas, Kipras, Latvijas, Lietuvas un Maltas – pieredze apmācību programmu īstenošanā. Katra valsts sniedz informāciju, kas saistīta ar tādām jomām kā dalībnieku informēšana un atlases process, dalībnieku profils, studenta motivācija pievienoties izmēģinājuma apmācībai, apmācību procesa organizācija un dalībnieku viedoklis par saturu.

### Latvija

#### Dalībnieku informēšana un atlases process

Izmēģinājuma apmācības tika īstenotas ar sociālajiem partneriem Rīgas Tehnisko universitāti (RTU) un Latvijas Kultūras koledžu, tāpēc tika aicināti piedalīties šo HEI studenti. Altacom organizēja atsevišķas tikšanās ar RTU un LKK studentu pašvaldībām, lai iepazīstinātu ar CyberPhish projektu un paredzēto izmēģinājuma apmācību. Studenti pēc tikšanās tika novirzīti pie personas, kas bija atbildīga par neformālo izglītību viņu HEI. Sociālie partneri un kontakti no Latvijas kultūras koledžas, izsūtīja ielūgumus studentiem (pārsvarā no ne-IT fakultātēm).

#### Dalībnieku profils

Izmēģinājuma apmācībā piedalījās 27 dalībnieki. Izmēģinājuma apmācību dalībnieku vidējais vecums bija 23 gadi, vecākajam — 26 un jaunākajam — 19 gadi. Dalībnieku vīriešu bija pusotru reizi vairāk nekā sieviešu (60% vīriešu un 40% sieviešu). Kopumā dalībnieki bija tehniskas un kultūras jomas studenti. Lielākā daļa dalībnieku bija latvieši, kuri šobrīd dzīvo Rīgā, bet bija arī apmaiņas studenti, kuri bija no dažādām valstīm un studē Latvijā.

#### Studentu motivācija pievienoties izmēģinājuma apmācībai

Izmēģinājums tika ieviests kā jauns papildu neformālās izglītības līdzeklis, kas var palīdzēt skolēniem iegūt vērtīgas teorētiskās un praktiskās iemaņas kiberdrošībā. Mūsdienās šīs prasmes ir Joti noderīgas ne tikai personīgai lietošanai, bet arī gandrīz visās darba vietās, kur tiek lietoti datori. Tāpēc daži uzaicinātie studenti nolēma, ka dalība izmēģinājumā viņiem var būt patiešām noderīga, un piekrita pievienoties.

#### Apmācību procesa organizēšana

Galvenā informācija par izmēģinājumu tika sniegtā tikšanas laikā ar RTU un LKK studentu pašpārvaldēm un ielūgumā. Turklat dalībnieki varēja nosūtīt savus jautājumus un atsauksmes pa e-pastu vai citiem saziņas līdzekļiem (piem. ziņojums sociālajā tīklā).



Mācību platformā bija reģistrēti 45 dalībnieki. 25 dalībnieki zināšanu pārbaudi nokārtoja ar punktu skaitu virs 75%. 2 dalībnieki nokārtoja zināšanu pārbaudi (latviešu valodā) ar punktu skaitu zem 75%

#### Dalībnieku viedoklis par saturu

Dalībnieku aptauja pēc izmēģinājuma apmācības parādīja, ka viņi ieguva daudz zināšanu par pikšķerēšanu gandrīz visos CyberPhish kursa kiberdrošības priekšmetos. Dalībnieki papildināja savas zināšanas par pikšķerēšanu moduļos "Kiberdrošības juridiskie aspekti", "Kiberdrošības tendences", "Proaktīvas kiberdrošības darbības" un "Kiberuzbrukumu apstrāde". Lielākā daļa dalībnieku pēc CyberPhish kursa beigšanas bija apmierināti ar savām zināšanām par kiberdrošības priekšmetiem, īpaši ar moduļiem "Kiberuzbrukumi – sociālā inženierija un pikšķerēšana" un "Kiberuzbrukumu izpratne un to risināšana". Gandrīz visi studenti piekrita, ka simulācijas palīdzēja uzlabot viņu prasmes atpazīt pikšķerēšanu. Lielākā daļa respondentu piekrita vai pilnībā piekrita apgalvojumiem:

- viņi ieteiktu šo kursu citiem cilvēkiem;
- apmācība un atbalsts visa kursa laikā ir atbilstošs;
- tiešsaistes mācību platforma bija viegli lietojama;
- kursa pabeigšanai atvēlētais laiks ir pietiekams;
- kursa saturs aptvēra kursa mērķus;
- viņiem bija skaidra izpratne par kursa mērķiem;
- tiešsaistes pieeja mācībām atbilst kursam.



## SECINĀJUMI

Pamatojoties uz vajadzību analīzi, partneru konsorcijs ir izstrādājis mācību programmu par kiberdrošību, kiberuzbrukumiem, sociālo inženieriju, īpašu uzmanību pievēršot pikšķerēšanas identificēšanai un novēršanai. Mācību programma ir izstrādāta jauktai apmācībai, taču tās struktūra padara to elastīgu, un to var izmantot gan tālmācības, gan klātienes apmācībai. Pilna apmācības programma sastāv no 30 stundām, kas atbilst 1 ECTS.

Mācību programma ir sadalīta četrās daļās (moduļos): Ievads kiberdrošībā; Pārskats par kiberdrošību ES; Kiberuzbrukumi — sociālā inženierija un pikšķerēšana; Kiberuzbrukumu izpratne un risināšana.

Partneru konsorcijs izstrādāja tiešsaistes mācību materiālu, ievērojot Cyberphish mācību programmu un atbilstoši 4. industriālās revolūcijas vajadzībām. Projekta laikā partneri izveidoja mācību materiālus, kas sastāv no slaidiem, vērtējumiem un saitēm uz ārējiem avotiem un video. Izstrādāto mācību materiālu labi novērtēja neatkarīgi eksperti.

Izstrādātās mācību programmas, mācību materiālus un mācību vidi var izmantot dažādām mērķa grupām, piemēram, studentiem, pedagoģiem, augstskolu darbiniekiem (kopienas pārstāvjiem), pieaugušo centriem un uzņēmējdarbības sektoram (darba devējiem un darbiniekiem).

Izstrādātie e-mācību materiāli, jauktā mācību vide un simulācijas tika integrētas mācību priekšmetos iesaistītajās universitātēs izmēģinājuma apmācības laikā.

Izstrādātais mācību materiāls, simulācijas, pašnovērtējuma testi un zināšanu vērtēšanas testi palīdz pilnveidot dalībnieku kritisko domāšanu un prasmes kiberdrošības jomā pielietot profesionālajā praksē. Kursu CyberPhish var veiksmīgi izmantot apmācību organizēšanai citām mērķa grupām ne tikai izmēģinājuma apmācību laikā iesaistītajās valstīs, bet arī adaptējot citām Eiropas valstīm.

Salīdzinot zināšanu novērtējumu pirms un pēc apmācības, atklājās, ka dalībnieki būtiski uzlaboja savas zināšanas par kiberdrošību un pikšķerēšanu. Dati liecina, ka dalībnieku sniegums ievērojami uzlabojās, t.i., vairāk studentu ieguva 8 un augstākus vērtējumus.

Sint septiņdesmit pieci dalībnieki pabeidza (175) apmācību kursu un saņēma sertifikātu: 36 Igaunijā, 25 Latvijā, 26 Kiprā, 30 Malta un 58 Lietuvā. Vēl 17 dalībnieki kursu pabeidza bez sertifikāta, t.i., viņu zināšanu pārbaudes rezultāts bija zem 75%.



## INFORMĀCIJAS AVOTI

1. ENISA (2019): Kiberdrošības prasmju attīstība ES. Eiropas Savienības Drošības aģentūra. 2019. gada decembris. Vietne: [Cybersecurity Skills Development in the EU — ENISA \(europa.eu\)](https://cybersecurityskills.enisa.europa.eu/) (accessed 09/08/2022)
2. Eiropas Savienības Padome (2021): Padomes secinājumu projekts par ES kiberdrošības stratēģiju digitālajai desmitgadei, vietne: [https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm\\_source=dsms-auto&utm\\_medium=email&utm\\_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy](https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy) (accessed 09/08/2022)
3. Labā prakse inovāciju jomā kiberdrošībā saskaņā ar NCSS, 2019. gada 19. novembris
4. IO1 A2: Rezultāti "Esošo kiberdrošības apmācību programmu analīze", 2021, vietne: [https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A2-Report\\_Analysis-of-existing-Cybersecurity-training-programmes\\_LV.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A2-Report_Analysis-of-existing-Cybersecurity-training-programmes_LV.pdf)
5. Pierādījums (2019): Cilvēciskā faktora pārskats 2019, vietne <https://www.proofpoint.com/us/resources/threat-reports/human-factor>
6. Eiropas Savienības Kiberdrošības aģentūra (2020): Pikšķerēšana — ENISA apdraudējumu reljefs 2019.–2020. gads
7. IO1 A1 "PIŠĶERĒŠANAS UN PRASMES TRŪKUMU ATZĪŠANA", 2021. gads, vietne: [https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A1-Report\\_Recognising-Phishing-and-Skills-Gaps\\_LV.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A1-Report_Recognising-Phishing-and-Skills-Gaps_LV.pdf)
8. Robert B. Cialdini (2006) Pārliecināšanas psiholoģija. Harper Business, 336.lpp. ISBN: 978-0061241895
9. NCC grupa (2020): Pikšķerēšanas psiholoģija: Septiņu ietekmes principu izmantošana, vietne: [https://www.mynewsdesk.com/nccgroup/blog\\_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433](https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433)



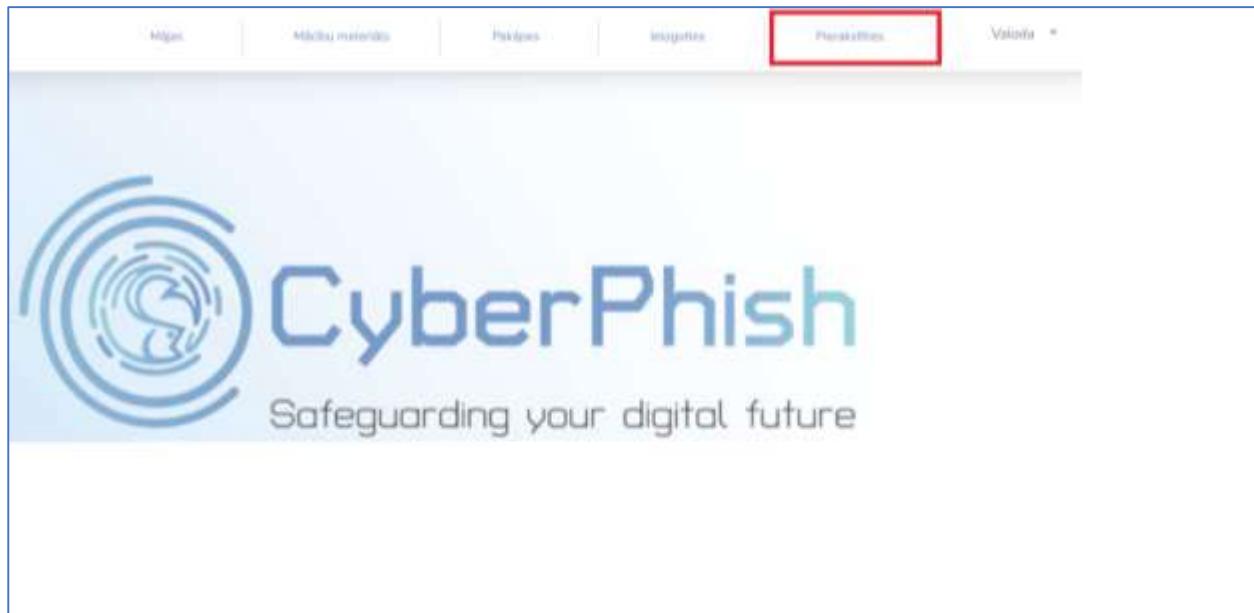
## PIELIKUMS NR. 1

### CYBERPHISH MĀCĪBU VIDE

Mācību materiāli, kas izvietoti e-mācību vidē <https://cyberphish.vuknf.lt> ir pieejami visiem apmeklētājiem un ir bez maksas. Mācību materiāls ir pieejams piecās valodās: Angļu, igauņu, grieķu, latviešu un lietuviešu. Nereģistrēti apmeklētāji var tikai apskatīt mācību materiālu, bet nevar pildīt pašnovērtējuma testus, zināšanu testus, nopelnīt un krāt nozīmītes, veikt simulācijas vai saņemt sertifikātus. Lai kļūtu par reģistrētu vietnes apmeklētāju ir jāreģistrējas.

#### Piesakties e-mācību vidē

Lai kļūtu par reģistrētu lietotāju, izveidojiet kontu, noklikšķinot uz pogas "Pierakstīties" [Reģistrēties].



Nospiežot **Pierakstīties** [Reģistrēties] lapas augšdaļā ierakstiet savu e-pastu, paroli, atkārtojiet savu paroli un atlasiet savu valsti. Jums arī jāapstiprina, ka neesat robots un ka piekrītat noteikumiem un nosacījumiem, un pēc tam noklikšķiniet uz **Pierakstīties** [Reģistrēties].



Izveidot kontu

Ievadīt e-pasta adresi...  
Parole  
Atkārtojiet paroli  
Valsts

Neesmu robots 

Es piekrītu Noteikumiem un nosacījumiem

**Pielikties**

Kurši esmu  
jaunais/kontakti / pārliecinās...



Kad būsiet reģistrējies, jums pa e-pastu tiks nosūtīta apstiprinājuma saite. Nospiediet uz saites.

Piezīme: Ja skolēns nav saņēmis apstiprinājuma e-pastu no sistēmas nepieciešams pārbaudīt surogātpasta mapi. Iespējams, ka apstiprinājuma e-pasts nonāks mēstuļu/surogātpasta mapē.

Izveidot kontu!

Lietotājs reģistrēts! Pārbaudiet verifikācijas saiti savā e-pastā.

Ievadiet e-pasta adresi...

Parole

Noklikšķiniet uz apstiprinājuma saites, lai pieteiktos sistēmā.

Laipni lūdzam atpakaļ!

Ievadiet e-pasta adresi...

Parole

Pieslēgties

Aizmirsi paroli?  
Izveidot kontu!

## Lietotāja kants

Kad esat pieteicies, noklikšķiniet uz savas e-pasta adreses lapas augšdaļā un noklikšķiniet uz vienuma **Mana informācija**.



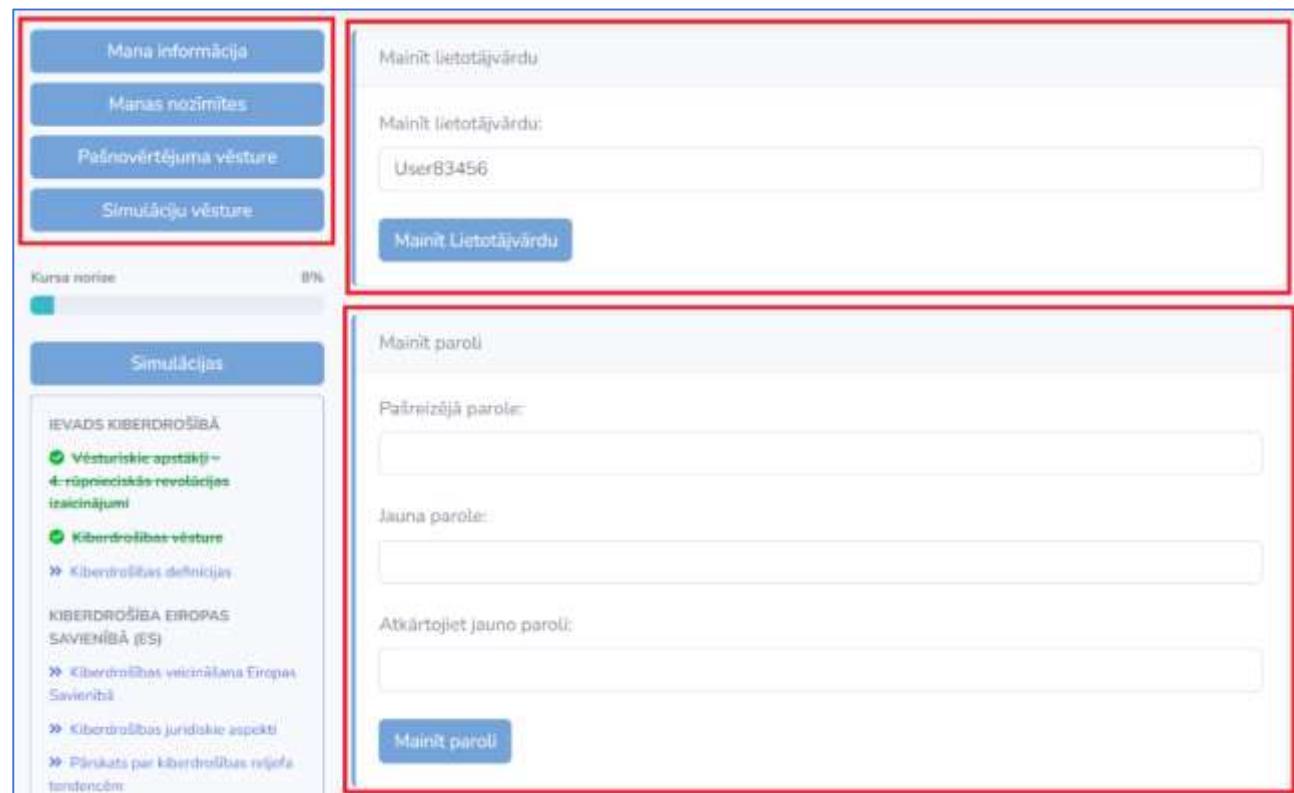
Funded by the  
Erasmus+ Programme  
of the European Union



The screenshot shows the CyberPhish platform's main dashboard. At the top, there are three navigation tabs: "Mājas", "Mācību materiāls", and "Pakalpes". A red box highlights the search bar containing the email address "mscorvald0933@mtu.edu.com". To the right of the search bar is a dropdown menu labeled "Valoda" with a "—" symbol. Below the search bar, the CyberPhish logo and tagline "Safeguarding your digital future" are displayed. On the left side, there is a sidebar with four blue buttons: "Mana informācija", "Manas nozīmītes", "Pašnovērtējuma vēsture", and "Simulāciju vēsture". A progress bar indicates "Kursa norise: 0%". The main content area features the CyberPhish logo and tagline again. A red box highlights a sidebar on the right with three items: "Mana informācija", "Manas nozīmītes", and "Ispogoties".

Lapas **Mana informācija** kreisajā pusē jūs redzēsiet galveno lietotāja izvēlni, kas novirza uz lapu **Mana informācija** (jūsu pašreizējā lapa), **Badges page [Mani žetonij]**, **Self-Evaluation History [Pašnovērtējuma vēstures]** un **Simulations History [Simulāciju vēstures]** lapām.

Jūs varat mainīt savu lietotājvārdu un paroli lapā **Mana informācija**.



The screenshot shows the "Mana informācija" page. On the left, there is a sidebar with a "Simulācijas" section containing a list of topics under "IEVADS KIBERDROŠĪBĀ" and "KIBERDROŠĪBA EIROPAS SAVIENĪBĀ (ES)". The main content area has two red-highlighted forms. The first form is titled "Mainīt lietotājvārdu" and contains a field "Mainīt lietotājvārdu:" with the value "User83456" and a "Mainīt Lietotājvārdu" button. The second form is titled "Mainīt paroli" and contains three fields: "Pārmeizējā parole:", "Jauna parole:", and "Atkārtojiet jauno paroli:". It also has a "Mainīt paroli" button.

Lapā **Manas nozīmītes** jūs redzēsīt visus žetonus, kurus esat savācis par dažādiem paveiktajiem uzdevumiem.



Mana informācija

Manas nozīmītes

Pašnovērtējuma vēsture

Simulāciju vēsture

Kursa norise 81%

Simulācijas

IEVADS KIBERDROŠĪBĀ:  
• Vesturiskie apstākļi –  
• Rūpnieciskās reakcijas

Manas nozīmītes

Topic

Topic

Category

Category

Topic

Topic

Topic

Topic



Lapā **Pašnovērtējuma vēsture** varēsiet skatīt visu uzsāktu vai pabeigto pašnovērtējuma testu vēsturi. Ja pašnovērtējuma tests nav pabeigs, to var pabeigt, noklikšķinot uz testa nosaukuma. Ja tests ir pabeigs, varat noklikšķināt uz tā, lai redzētu rezultātus.

Mana informācija

Manas nozīmītes

Pašnovērtējuma vēsture

Simulāciju vēsture

Kursa norise 100%

Simulācias

Pašnovērtējuma vēsture

Levads kiberdrošībā

Sākts: 2022-08-09 12:48:46

Beigās: 2022-08-09 12:55:12

Punkti: 258

Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana

Sākts: 2022-08-09 13:03:55

Beigās: 2022-08-09 13:09:29

Punkti: 100

**Simulāciju vēstures** lapā varat skatīt iesākto vai pabeigto simulāciju vēsturi. Ja simulācija nav pabeigta, to var pabeigt, noklikšķinot uz simulācijas nosaukuma. Ja simulācija ir pabeigta, jūs varat apskatīt rezultātus, noklikšķinot uz tās.

Mana informācija

Manas nozīmītes

Pašnovērtējuma vēsture

Simulāciju vēsture

Kursa norise 100%

Simulācijas

Simulāciju vēsture

ID: 92  
Aktieri: Uzņēmumu adreses, Uzņēmuma klienti  
Tips: Emails  
Uzbrukuma veids: GDPR related attacks

Sākts: 2022-08-10 10:22:14  
Beigās: 2022-08-10 10:25:53  
Punkti: 200

ID: 92  
Aktieri: Uzņēmumu adreses, Uzņēmuma klienti  
Tips: Emails  
Uzbrukuma veids: GDPR related attacks

Sākts: 2022-08-10 10:27:45  
Beigās: 2022-08-10 10:31:50  
Punkti: 200

ID: 92  
Aktieri: Uzņēmumu adreses, Uzņēmuma klienti  
Tips: Emails  
Uzbrukuma veids: GDPR related attacks

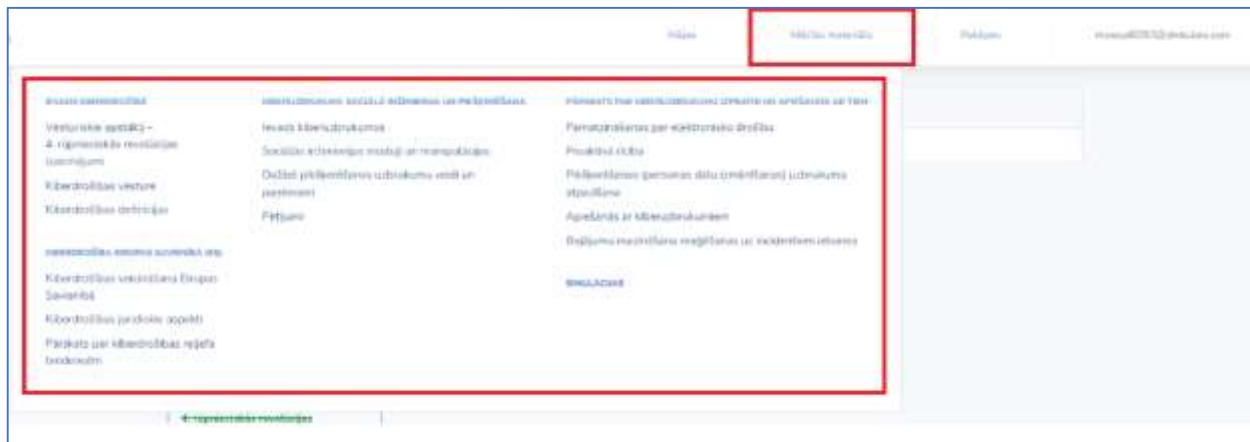
Sākts: 2022-08-10 10:35:44  
Beigās: 2022-08-10 10:38:18  
Punkti: 400



## Mācību materiāls

Mācību materiāliem varat piekļūt lapas augšpusē, izvēloties izvēlnes vienumu **Mācību materiāls** un izvēloties jūs interesējošo tēmu\*.

\*Visiem mācību materiāliem var piekļūt bez reģistrācijas, taču dažas funkcijas var būt ierobežotas. Apmācāmais var lasīt mācību materiālu, nepiesakoties sistēmā, taču nevarēs apstiprināt mācību materiāla skatīšanās statusu, kā arī nevarēs piekļūt testiem un simulācijām.



The screenshot shows a user interface for an e-learning platform. At the top, there are tabs for 'Mācību materiāls' (highlighted with a red box), 'Mācību rezultāti', 'Pielikumi', and 'Mācību materiāla izmaksas'. The main content area is divided into several sections:

- Kibēdrošības aspekti:**
  - Vertuņķie aplāni – 4 rūpniecības revolūcijas izmaiņu
  - Kibēdrošības vesture
  - Kibēdrošības definīcijas
- IEVĀDĀS KIBĒDROŠĪBĀ:**
  - Vertuņķie aplāni – 4 rūpniecības revolūcijas izmaiņu
  - Kibēdrošības vesture
- KIBĒDROŠĪBA EIROPAS SAVIENĪBĀ (ES):**
  - Kibēdrošības vesture
  - Kibēdrošības juridiskie aspekti
  - Pārskats par kibēdrošības reģīta tendenciju
- KIBĒDROŠĪBUZBRUKUMI: SOCIĀLĀ INŽENIERIJA UN PRIKSĒRĒŠANA:**
  - Ievads kibēdrošībā
  - Sociālās ietekmes moduli un manipulācijas
  - Datādi priekšķēdējās uzbrukuma veidi un papārtemi
  - Pētījumi
- PĀRSKATS PAR KIBĒDROŠĪBUZBRUKUMU IZPRATNI UN ATSPĀRTOŠĀBU TĒMĀM:**

Ja atlasīsit kādu tēmu, lapas galvenajā dalā redzēsīt šīs tēmas slaidus, bet lapas kreisajā pusē – saites uz visām tēmām. Ja esat pieteicies, varat atzīmēt tēmas kā pabeigtas, nospiežot pogu **Atzīmēt kā pabeigts!** lapas augšdaļas labajā pusē un lapas kreisajā pusē skatiet savu kursa gaitu.



The screenshot shows a detailed view of the 'Kibēdrošības definīcijas' topic. On the left, there's a sidebar with a progress bar at 8% and a 'Simulācijas' tab. The main content area has a title 'Ievads kibēdrošībā' and 'Kibēdrošības definīcijas'. In the bottom right corner of the content area, there's a teal button with a checkmark and the text 'Atzīmēt kā pabeigts!'. The content area also contains a large image of a globe and some descriptive text about the project's funding.



## Pašnovērtējumu testi

Lai piekļūtu pašnovērtējuma jautājumiem, katras tēma kategorijā ir jāatzīmē kā pabeigta. Pēc tam galvenās lapas augšdaļā redzēs pogu **Pašnovērtējuma tests**. Lai piekļūtu **Pašnovērtējuma tests**, jums ir jāpiesakās.



Kursa norise: 10%

**Simulācijas**

**IEVADS KIBERDROŠĪBĀ**

- Vēsturiskie aspekti – 4-rūpnieciskās revolūcijas izcīņu laikā
- Kiberdrošības vēsture
- Kiberdrošības definīcijas

**KIBERDROŠĪBA EIROPAS SAVIENĪBĀ (ES)**

- » Kiberdrošības vēcinātāja Eiropas Savienībā
- » Kiberdrošības juridiskie aspekti
- » Pārskats par kiberdrošības ietekmes tendencēm

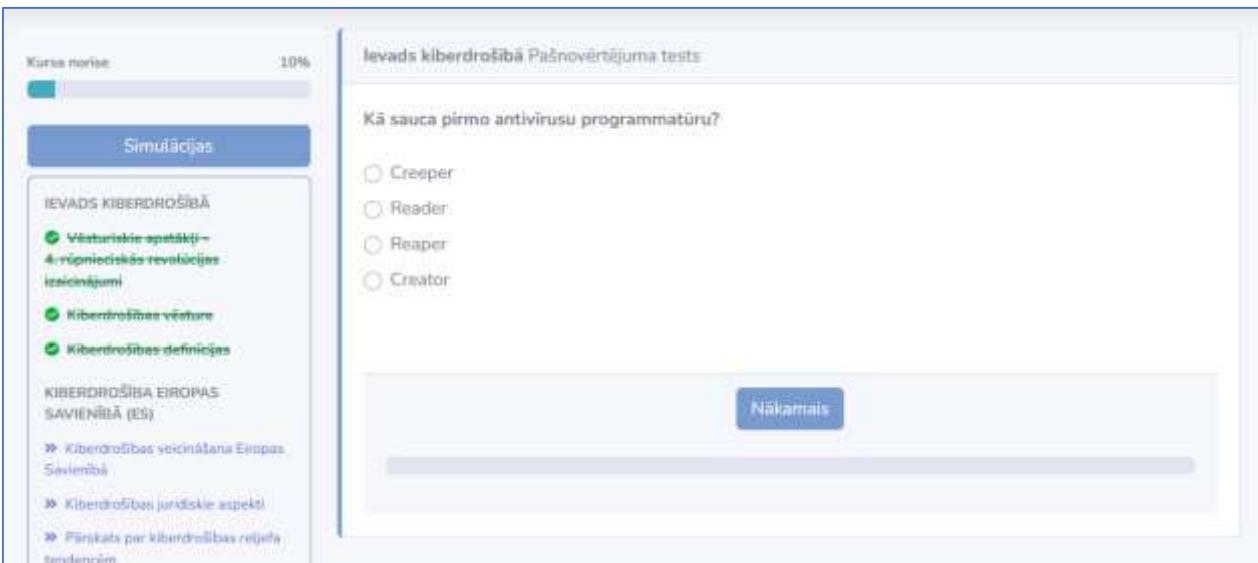
**KIBERUZBRUKUMI: SOCIĀLĀ INŽENIERIJA UN PIKŠERĒSĀNA**

**Pašnovērtējuma tests**

Kiberdrošības definīcijas

Pabeigta!

Noklikšķinot uz pogas **Pašnovērtējuma tests**, jūs saņemsiet šīs kategorijas 5 jautājumus, lai novērtētu savas zināšanas.



Kursa norise: 10%

**Simulācijas**

**IEVADS KIBERDROŠĪBĀ**

- Vēsturiskie aspekti – 4-rūpnieciskās revolūcijas izcīņu laikā
- Kiberdrošības vēsture
- Kiberdrošības definīcijas

**KIBERDROŠĪBA EIROPAS SAVIENĪBĀ (ES)**

- » Kiberdrošības vēcinātāja Eiropas Savienībā
- » Kiberdrošības juridiskie aspekti
- » Pārskats par kiberdrošības ietekmes tendencēm

levads kiberdrošībā Pašnovērtējuma tests

Kā saucē pirmo antivīrusu programmatūru?

Creeper

Reader

Reaper

Creator

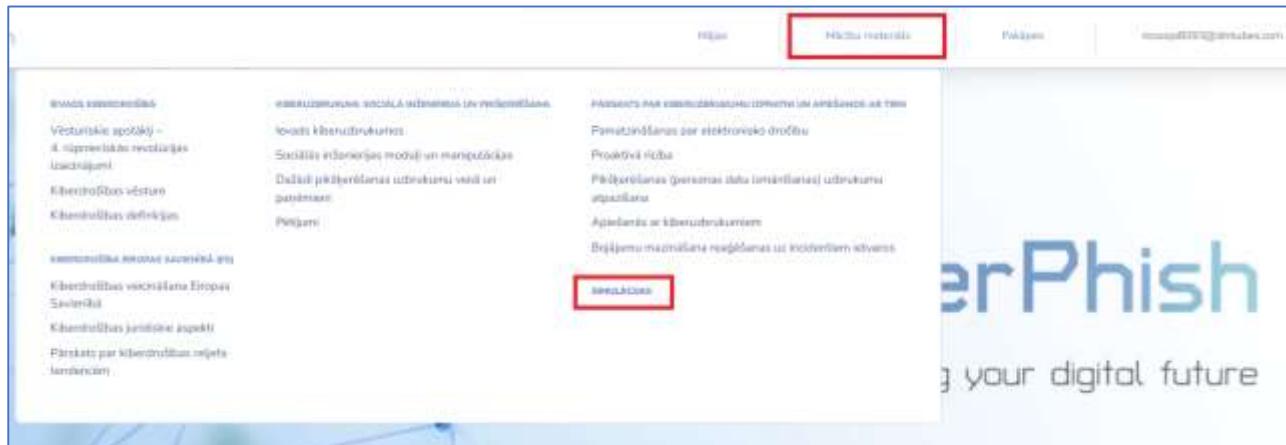
Nākamais

## Simulācijas

Lietotāji var piekļūt simulācijām, tikai piesakoties.

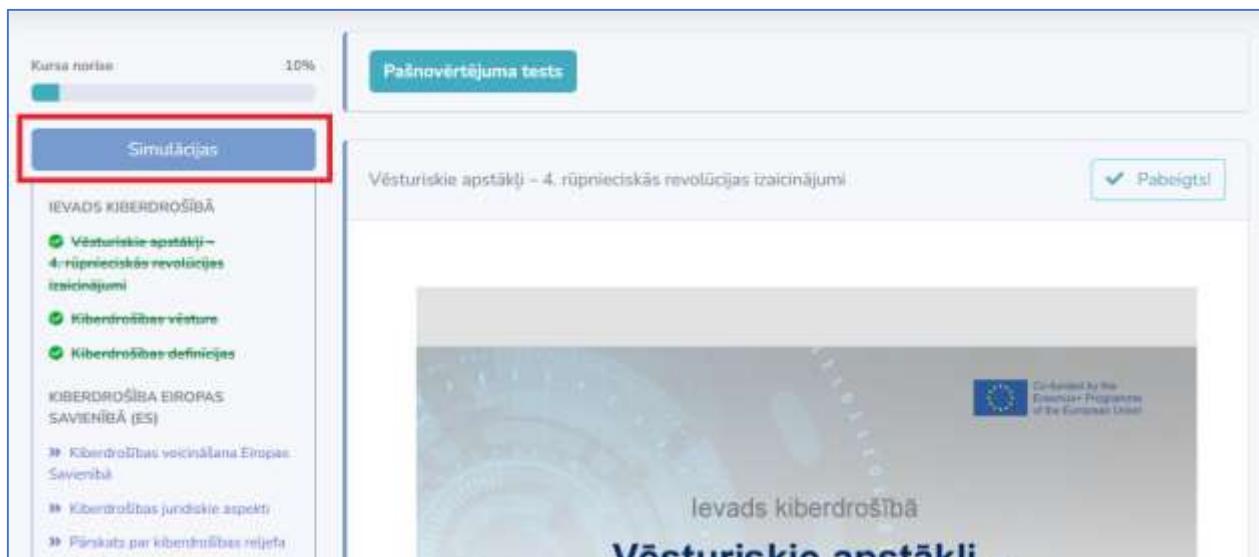


Simulācijām var piekļūt, noklikšķinot uz **Mācību materiāla** un atlasot **Simulācijas**.



The screenshot shows a web-based learning environment. At the top, there are tabs for 'Filtri', 'Mācību materiāls' (which is highlighted with a red box), 'Pielikumi', and 'E-mail: support@cyberphish.com'. Below the tabs, there are two columns of course topics. The left column includes 'Ievads kiberdrošībā', 'Vēsturiskie apstākļi – 4. rūpnieciskās revolūcijas izraisījumi', 'Kiberdrošības vēsture', and 'Kiberdrošības definīcijas'. The right column includes 'Vēsturiskais apstākļu analīza ietekmes līdzekļos', 'Ieavots kiberuzbrukums', 'Stabilas ieteknes moduli un manipulācijas', 'Daudzi pārķērķēšanas ietekumi vairāk ne par vienu', 'Pielikumi', and 'Pielikumi'. A large blue banner on the right side of the page features the 'CyberPhish' logo and the tagline 'Safeguarding your digital future'.

Simulācijām varat piekļūt arī no jebkuras atlasītās **Mācību materiāla** tēmas lapas.



This screenshot shows a course navigation interface. On the left, a sidebar lists course sections: 'IEVADS KIBERDROŠĪBĀ' (with items 'Vēsturiskie apstākļi – 4. rūpnieciskās revolūcijas izraisījumi', 'Kiberdrošības vēsture', and 'Kiberdrošības definīcijas'), 'KIBERDROŠĪBA EUROPAS SAVIENĪBĀ (ES)' (with items 'Kiberdrošības veicinātāja Eiropas Savienība', 'Kiberdrošības juridiskie aspekti', and 'Pārskats par kiberdrošības sejai'), and 'Simulācijas'. The 'Simulācijas' button is highlighted with a red box. The main content area shows a 'Pašnovērtējuma tests' section with a green 'Pabeigtis' button. Below it, there's a preview of a slide titled 'Vēsturiskie apstākļi – 4. rūpnieciskās revolūcijas izraisījumi' featuring a circular graphic and the text 'Ieavots kiberdrošība' and 'Vēsturiskie apstākļi'.

Noklikšķinot uz **Simulācijas**, jums ir jāizvēlas simulāciju kategorija. Vienu simulāciju var iedalīt vairākās kategorijās.



This screenshot shows the same course navigation interface as the previous one. The 'Simulācijas' category is now highlighted with a red box. The main content area displays a grid of six boxes under the heading 'Simulācijas', each representing a different type of simulation: 'Reciprocity', 'Scarcity', 'Authority', 'Consistency', 'Consensus', and 'Unity'. The 'Authority' box is also highlighted with a red box.

Atlasot kategoriju **Simulācijas**, varēsiet atlasīt simulācijas šajā kategorijā. Ja kādreiz esat pabeidzis noteiktu simulāciju, zem ūdens simulačijas redzēs laika zīmogu.



Kurš norise: 10%

Simulācijas

IEVADS KIBERDROŠĪBĀ

- Vēsturiskie apstākļi – 4. rūpnieciskās revolūcijas izraisījumi
- Kiberdrošības vēsture
- Kiberdrošības definīcija

KIBERDROŠĪBA EIROPĀS

Consistency

ID: 94 Aktier: e-pasta lietotāji Tips: Emails Uzbrukuma veids: Tech support attacks Pēdējo reizi bildzis: 2022-08-10 16:45:11	ID: 103 Aktier: Labi zināmi tiemekļa vietņu iepānieki Tips: Websites Uzbrukuma veids: Websites Scams Pēdējo reizi bildzis: 2022-08-10 16:55:19	ID: 106 Aktier: 40 gadus vecs ilggadējs "Internet Providers" klients Tips: Sms Uzbrukuma veids: Spear phishing attacks Pēdējo reizi bildzis: 2022-08-10 16:59:47
---	--	--

Izvēloties jebkuru simulačiju, jūs redzat situācijas aprakstu, pirms sākat to risināt. Pirms sākat, jums ir jāizvēlas, vai vēlaties to darīt **Mācību nolūkos** vai **Zināšanu pārbaudes nolūkiem**.

Ja izvēlaties **Mācību nolūkos**, pēc katra atbildētā jautājuma redzēsit atsauksmes.

Ja izvēlaties **Zināšanu pārbaudes nolūkiem**, atsauksmes redzēsit tikai pēc simulačijas pabeigšanas.

Noklikšķiniet uz **Sākt**.

ID: 10

8:34 4G

Text Message  
Today 8:22 pm

\*SVARĪGI\* Swedbank drošībai ir nepieciešams nekavējoties autorizēt savu ierīci un normāri paroli, pretējā gadījumā jūsu korts tiks bloķēts. To varat izdarīt šeit: <https://commbank-hr.au.serveo.net/id/MDDQwMzI4OTk1Mg==>

Sāņemot līzinu ar padocojumu, ka jūsu bankas korts ir bloķēts un jums jāatlāgnina parole. Zieviņš ir saite, kas jums ir jāsēko līdz.

Mērķis: Jūsu paroli ir komromēta. Lai saglabātu savu bankas kontu drošu, lūdzu, saņemiet saitei, lai iņjauninātu paroli. Jūsu banka

Aktier: Izpratne par SMS ja Smishing uzbrukumiem

Tips: Sms

Uzbrukuma veids: SMS attacks

Autots

Atributi

- Asks to provide Data
- Suggests Reimburse Money
- Asks Click Link (Website)
- Asks to perform Action
- Asks to authorize

Mācību nolūks  
 Zināšanu pārbaudes nolūks

Sākt



## Lietotāju reitingi

Izmantojot šo opciju, lietotāji tiek sarindoti pēc viņu labākajiem rezultātiem **pašnovērtēšanas testos** un **simulācijās**. Lietotāju reitingiem var piekļūt, lapas augšdaļā noklikšķinot uz **Pakāpes** un atlasot vai nu **Pašnovērtējums**, vai **Simulācijas**.



The screenshot shows a navigation bar with several tabs: 'Mējus', 'Vidēja materiāls', 'Pakāpes' (which is highlighted with a red box), 'Izglītības', 'Pielikumi', and 'Vai vada'. Below the navigation bar, there are two main options: 'Pašnovērtējums' and 'Simulācijas', each with a small icon. The background features the CyberPhish logo.