Andmepüügi vastu kaitsemine 4. tööstusrevolutsiooni ajastul (CyberPhish)

A2: Rakendusjuhised

Projekti periood: November 2020 – November 2022

Projekti number.: 2020-1-LT01-KA203-078070

Funded by the Erasmus+ Programme of the European Union

Sisukord

1. Sissejuhatus

Neljanda tööstusrevolutsiooni ajastul on küberturvalisusest saamas üks suurimaid väljakutseid. Digiseadmete ja infosüsteemide laialdane kasutamine on küberkurjategijate jaoks üha atraktiivsem. Eurostati andmetel "...2019. aastal teatas ligikaudu iga kolmas 16–74-aastane ELi kodanik viimase 12 kuu jooksul turvalisusega seotud intsidentidest, kui kasutas internetti isiklikuks otstarbeks. 2019. aastal oli andmepüük kõige sagedasem teatatud turvaintsident". Praktikas ei suuda ükski infosüsteem ega turvatarkvara anda andmepüügirünnakute eest 100% kaitset. Võitlus nende ohtude vastu ei seisne ainult riist- ja tarkvara turvalahendustes, vaid ka kasutaja vastupanuvõimes küberohtude suhtes ja nende äratundmise võimes.

Küberrünnakud on suunatud ka Euroopa ettevõtetele. 2017. aasta ülemaailmse teabeturbe seisukorra uuringu kohaselt koges umbes 80% Euroopa ettevõtetest aastas vähemalt ühte küberturvaintsidenti ja töötajad olid otseselt vastutavad 27% kõigist küberturbe intsidentidest. Seega saab küberrünnakuid, nagu andmepüüki, ära hoida vaid inimene – kasutaja, kes mõistab küberkurjategija tegutsemist ja suudab ära tunda pahatahtliku tegevuse hoiatusmärke.

ENISA andmetel on küberteemalised ained mittetehniliste programmide üliõpilaste seas alaesindatud. Seetõttu on asjakohane töötada välja ja pakkuda avalikkusele laialdaselt juurdepääsetavat veebipõhist koolitust andmepüügi tuvastamise kohta.

Nendel põhjustel algatati ja viidi ellu rahvusvaheline projekt "Safeguarding against Phishing in the age of 4th Industrial Revolution" (CyberPhish). Euroopa Liit rahastas projekti Erasmus+ programmi raames. Projekti koordineeris Vilniuse Ülikooli Kaunase teaduskond, projekti partneriteks olid Tartu Ülikool (Eesti), Dorea (Küpros), MECB (Malta), Altacom (Läti) ja Infotehnoloogia Instituut (Leedu). Projekti kestus on novembrist 2020 kuni novembrini 2022.

Projekti “CyberPhish” põhieesmärk on harida kõrgkoolide üliõpilasi, õppejõude, ülikoolide töötajaid (kogukonna liikmeid), hariduskeskusi ja ärisektorit (tööandjaid ja töötajaid) ning edendada küberturvalisuse alast kriitilist mõtlemist sihtrühmas.

Cyberphishi projekti eesmärk on välja töötada õppekava, e-õppematerjalid, segaõppe keskkond, simulatsioonid, enesehindamise ja teadmiste hindamise testid. Arendatud CyberPhishi kursus võimaldab kasutajatel ennast harida ja seeläbi kaitsta andmepüügirünnakute eest. Kasutajad omandavad kompetentsid, mis aitavad neil ohtudele tähelepanu pöörata ja vajalikke ennetusmeetmeid rakendada.

Projekti raames on välja töötatud intellektuaalne toode kasutajate kriitilise mõtlemise ja andmepüügi tuvastamise oskuste koolitamiseks. Kasutajad õpivad ära tundma andmepüügi märke (ohu märgid), sotsiaalse ründe tehnikaid ja üldisi küberturvalisuse oskusi. Segaõppe lähenemisviis/kontseptsioon võimaldab kasutajatel valmistuda teadmiste testiks ja saada lõputunnistuse.

Projektipartnerid kasutasid viie partnerriigi pilootkoolituste käigus veebipõhist õppeplatvormi, mis hõlmas koolitusmaterjale, simulatsioone, enesehinnangu teste ja teadmiste hindamise teste. Selle kogemuse põhjal on käesolevad rakendamise juhised välja töötatud.

Rakendusjuhendi eesmärk

Käesolevate juhiste eesmärk on tutvustada projekti tulemusi, parimaid piloteerimistavasid ja metoodikat CyberPhishi koolituskursuse väljatöötamiseks sihtrühmale ja sidusrühmadele. Juhend on adresseeritud organisatsioonidele, kes on huvitatud väljatöötatud materjali kohandamisest ja kasutamisest internetikasutajate harimiseks andmepüügi tuvastamisel: kõrgkoolid, täiskasvanute koolitus/koolituskeskused, ärisektor.

“CyberPhishi” juurutamise juhendi põhieesmärk on tutvustada koolituse korraldamise tööriistu, sisu ja protsessi. Kursuse käigus omandavad osalejad teadmisi ja oskusi, mis on vajalikud andmepüügirünnakute tuvastamiseks tööl ja isiklikus elus ning valmistuvad teadmiste testiks. Kursuse eduka läbimise korral antakse neile tunnistus. Rakendusprotsess põhineb osalevate partnerriikide kogemustel.

2. KÜBERTURVALISUS, ANDMEPÜÜK JA SOTSIAALSED RÜNDED

2.1 Küberturvalisus ja andmepüügi õppeprogrammid

Alates 2013. aastast on Euroopa Komisjon rõhutanud küberjulgeoleku teema olulisust. Esimeses küberturvalisuse strateegias tõstetakse peamiste strateegiliste eesmärkidena esile teadlikkuse tõstmist ja oskuste arendamist. 2017. aasta ENISA aruanne rõhutab ka küberturvalisuse tähtsust. Aruandes soovitatakse ELi liikmesriikidel tugevdada küberjulgeolekualast haridust ja oskusi (ENISA, 2019, lk 23). Selle tulemusena on kõik ELi liikmesriigid välja töötanud ja avaldanud riiklikud küberjulgeolekustrateegiad (NCSS).

2021. aasta märtsis võttis Euroopa Ülemkogu vastu uued järeldused ELi küberjulgeolekustrateegia kohta. Tulemused tunnistavad digitaalsete ja küberjulgeolekualaste oskuste nappust ning rõhutavad vajadust rahuldada turu nõudlust, arendades edasi haridus- ja koolitusprogramme.

Projekt CyberPhish uuris olemasolevaid küberjulgeoleku ja andmepüügi õppekavasid ja koolitusprogramme partnerriikides Küprosel, Eestis, Lätis, Leedus ja Maltal. Uuringut juhtis DOREA haridusinstituut. Uuringu peamised järeldused olid:

- Kõigi projekti partnerriikide, välja arvatud Eesti, kõrgkoolide õppekavade analüüs ei sisalda andmepüügi ja sotsiaalse inseneri teemasid eraldi moodulitena. Teavet nende teemade kohta saab aga lisada teistesse kursuse moodulitesse. Eestis on kaks kõrgkooli õppekava, mis sisaldavad sotsiaalsele ründamisele suunatud õppemooduleid. Selliste moodulite keskmine kestus on 4,5 EAP.
- Analüüsitud Eesti, Läti ja Malta kõrgkoolide õppeprogrammid sisaldavad pehmete oskuste kursuste mooduleid, nagu suhtlemisoskused, ettevõtlikkus, psühholoogia jne. Seevastu Küprose ja Leedu kõrgkoolide õppeprogrammid keskenduvad peamiselt kõvadele oskustele, pannes vähem rõhku pehmete oskuste tähtsusele.
- Kõigis partnerriikides pakuvad mõned avalikud ja eraorganisatsioonid küberturvalisuse koolitusi, mis on suunatud küberturvalisuse ja IT-spetsialistidele, ettevõtetele, töötajatele ja üldsusele. Kui lühema kestusega koolituskursused keskenduvad tavaliselt ainult ohtudele, sealhulgas andmepüügile, sotsiaalsele manipuleerimisele ja enesekaitse viisidele, siis pikemaajalised koolitused pakuvad küberturvalisusele laiemat perspektiivi. Samuti on mõned organisatsioonid, mis pakuvad ettevõtetele ja nende töötajatele suunatud läbitungimise ja sotsiaalse manipuleerimise teste.

Küsitlusest kogutud andmed aitasid tuvastada puudujääke oskustes ja koostada soovitusi uue koolitusprogrammi CyberPhish jaoks. Käesoleva programmi eesmärk on parandada Interneti-kasutajate oskusi ja teadlikkust ning harida neid uusimate küberturvalisuse probleemide ja ohtude, eriti andmepüügi kohta.

2.2. Andmepüügi ja sotsiaalse manipuleerimise äratundmine

Küberturvalisus on probleem ka Euroopa ettevõtete jaoks. Ettevõtted muutuvad üha enam küberrünnakute sihtmärkideks. Kuna kurjategijad muutuvad osavamaks, muutub küberrünnakute avastamine ja ennetamine keerulisemaks ning selliste rünnakute läbiviimiseks kasutatakse uusi meetodeid ja platvorme. 2017. aasta ülemaailmse infoturbe olukorra uuringu kohaselt koges umbes 80% Euroopa ettevõtetest aastas vähemalt ühte küberturvalisuse intsidenti. Uuringu kohaselt vastutavad töötajad 27% kõigist küberjulgeolekuintsidentidest. Ainuüksi 2019. aasta esimeses kvartalis sattusid ettevõtted üle maailma küberrünnakute sihtmärgiks 120% sagedamini kui 2018. aastal ja kandsid tohutut kahju (22,2 miljardit eurot).

2019. aasta inimfaktori aruande kohaselt nõuab enam kui 99% pahavara levitavatest meilidest inimese sekkumist, st linkide jälgimist, dokumentide avamist, turvahoiatuste aktsepteerimist ja muud käitumist [5]. Seetõttu on oluline andmepüügi valdkonnas harida ja tõsta teadlikkust. Küberhügieen nõuab andmepüügi tuvastamise selgitamist/õpetamist viisil, mis on enamikule inimestele arusaadav ja juurdepääsetav. Hoiatusmärkide tundmine ja kurjategijate meetodite mõistmine muudab internetikasutajad esiteks enesekindlamaks ja turvalisemaks ning teiseks aitab neil ennetada või vähemalt pidurdada selliste rünnakute levikut.

Andmepüük on illegaalne kasutaja isikuandmete (sisselogimismandaatide, krediitkaarditeabe jne) väljapressimine sotsiaalse manipuleerimise tehnikate abil. Kurjategijad on aktiivsed sotsiaalvõrgustikes, saadavad meile ja helistavad. Nende sõnumite eesmärk on veenda kasutajat avama pahatahtlikku manust või klõpsama võltsitud veebilingil, paljastades tema parooli. [6] Levinuimad andmepüügi tüübid on *Spray and pray, Cat phishing, Advanced fee scam, Spear phishing, Whaling, Vishing, Smishing, Angler Phishing, Clone Phishing ja Malvertising*.

Infoturbe kontekstis määratletakse sotsiaalset manipuleerimist kui inimeste psühholoogilist manipuleerimist tegevuste sooritamiseks või konfidentsiaalse teabe avaldamiseks. ENISA väidab, et sotsiaalsed ründed on endiselt peamine oht muud tüüpi küberkuritegevuse hõlbustamiseks, kuna 84% küberrünnakutest tuginevad sotsiaalsele manipuleerimisele. Andmepüügiohvrite arv kasvab jätkuvalt, kuna see kasutab ära inimlikku mõõdet, mis on enamasti turvalisuse nõrgim lüli [6].

Sotsiaalse rünnaku tehnikad põhinevad inimlikel nõrkustel, nagu ahnus, hirm, uudishimu, usaldus, empaatia ja kiirustamine. Seetõttu võib hoolikalt koostatud ja isikupärastatud e-kiri, kõnepost, telefonikõne või tekstisõnum mõjutada inimesi avaldama oma konfidentsiaalset teavet, klõpsama pahatahtlikul lingil, laadima alla ja avama pahavara sisaldava faili või isegi kandma kurjategijale raha üle.

Dr Robert B. Cialdini kirjeldas oma raamatus "Mõju: veenmise psühholoogia" kuut veenmise põhimõtet, mis võeti hõlpsasti kasutusele ja kasutati sotsiaalses manipuleerimises ja andmepüügis. Hiljem laiendati neid seitsmele: vastutasu, defitsiit, autoriteet, järjepidevus, üksmeel, meeldiv ja ühtsus. Selliseid tehnikaid kasutavad petturid võivad oma loodud rünnakutelt oodata edukaid tulemusi. Seetõttu on eriti oluline inimesi harida, et nad teaksid, kuidas selliseid rünnakuid ära tunda ja vältida. [7; 8; 9]

Projekti partnerid viisid läbi küsitluse, et selgitada välja, kuidas inimesed andmepüügirünnakuid ära tunnevad, inimeste teadlikkust andmepüügist ja erinevatest andmepüügiliikidest ning oskuste puudujääke partnerriikides Küprosel, Eestis, Lätis, Leedus ja Maltal. Uuringu tulemused on kättesaadavad uuringuaruandes “Andmepüügi ja oskuste lünkade tuvastamine”. [7]

Küsitluses osales viissada neliteist inimest, kellest 259 olid naised, 248 mehed ja 7 inimest eelistas oma sugu mitte tuvastada. Enim on vastajaid üliõpilased (304), järgnevad palgatöötajad (139), ettevõtete omanikud (53), töötud (10) ja füüsilisest isikust ettevõtjad (8). Enamik küsitlusele vastanutest on kõrgelt haritud – enamikul vastajatest (38%) on bakalaureusekraad, järgnesid magistrikraad (23%) ja doktorikraad (6%).

Huvitav on see, et peaaegu iga viies vastaja teatas, et on minevikus olnud andmepüügi rünnaku ohver. Kõige tavalisemad andmepüügirünnakud on aset leidnud meilides või sõnumites olevatel linkidel klõpsamisel, manuste avamisel või meilidele vastamisel ja konfidentsiaalsete andmete esitamisel. Nende rünnakute kõige levinumad põhjused olid tähelepanu hajumine, uudishimu või kiirustamine. Enamik vastajaid (74%) ei ole käinud ühelgi küberturvalisuse koolitusel ega seminaril. Üle poole vastanutest (54%) märkis, et neil on tekkinud huvi selle valdkonna vastu iseseisvalt. Kõik eelnev illustreerib kasvavat vajadust andmepüügi ja küberturvalisuse alaste teadmiste järele.

3. CYBERPHISHI ÕPPEKAVA

Partnerite konsortsium on vajaduste analüüsi põhjal välja töötanud küberjulgeoleku, küberrünnakute, sotsiaalse rünnakute koolituse õppekava, keskendudes eelkõige andmepüügi tuvastamisele ja ennetamisele.

Õppekava eesmärk on tutvustada küberturvalisust, keskendudes andmepüügirünnakutele. Kursuse programm on suunatud üksikisikutele, üliõpilastele, ettevõtjatele, organisatsioonide töötajatele ning valmistab osalejaid ette neljanda tööstusrevolutsiooni ajastu julgeolekuohtudeks. Kursus annab õppijatele oskused küberrünnakute tuvastamiseks ja haldamiseks ning seadmete ja andmete kaitsmiseks.

Õppekava on loodud segaõppeks, kuid selle ülesehitus muudab selle paindlikuks ja seda saab kasutada nii kaugõppeks kui ka silmast silma koolituseks. Täielik koolitusprogramm koosneb 30 tunnist, mis vastab 1 EAP-le. Iseõppimisel ja hindamisel soovitatakse arvestada sama palju tunde mooduli kohta.

Õppekava koosneb neljast erinevast osast (moodulist).:

1. Sissejuhatus küberturvalisusesse;
2. Ülevaade küberturvalisusest ELis;
3. Küberrünnakud – sotsiaalsed ründed ja andmepüük;
4. Küberrünnakute mõistmine ja nendega toimetulek.

Täieliku õppekava leiate CyberPhishi veebilehelt: https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EST_Cyberphish-Full-Curriculum-Final.pdf

4. CYBERPHISH PILOOTKOOLITUSTE KORRALDAMINE

Pilootkoolituse eesmärk on õpetada osalejaid tuvastama andmepüügirünnakuid, mõistma sotsiaalset manipuleerimist ning õppima uusi ja täiustama olemasolevaid oskusi. Projekti taotluses on täpsustatud, et projekti käigus välja töötatud tooteid tuleb piloteerida, et tulemusi hinnata ning vajadusel osalejate ja õpetajate/mentorite kommentaaride ja tagasiside valguses kohendada.

Osalejad. Pilootkoolitus toimus kõigis projekti partnerriikides – Küprosel, Eestis, Lätis, Leedus ja Maltal.

Pilootkoolitustel osalejateks olid:

- kõrghariduse üliõpilased,
- kõrgkoolide ja organisatsioonide töötajad,
- Täiskasvanute koolituskeskuste õpetajad ja töötajad.

Iga partnerorganisatsioon koolitas oma riigis vähemalt 24 osalejat, laiendades seega projekti mõju oma organisatsioonist kaugemale.

Kestus. Partnerite kokkuleppel kestis pilootkoolituste periood mitu kuud (mai-september), arvestades iga partneri suvepuhkust. Mõned partnerid said pilootkoolituse läbi viia õppeaasta lõpus, s.o maikuus, kevadsemestri lõpus. Teised partnerid alustasid õppeaasta alguses septembris ja kogusid osalejate tagasiside pilootkoolitusele septembri lõpuks.

Vorm. Pilootkoolitus viidi läbi segaõppe kursusena või Covid-19 pandeemia piiranguid arvestades kaugõppena.

Vilniuse Ülikool ja Tartu Ülikool piloteerisid koolitust oma organisatsioonides, integreerides Cyberphishi kursuse oma õppeainetesse. Teised partnerid Altacom, Dorea ja MECB viisid pilootkoolituse läbi koostöös teiste kõrgkoolidega või väliseid osalejaid kutsudes.

Õppeplatvorm. Õppeplatvorm CyberPhish töötati välja ja testiti viies keeles – inglise, eesti, kreeka, läti, leedu ja leedu keeles. Osalejad pidid tutvuma väljatöötatud õppematerjaliga, sooritama iga kursuse teema järel enesehinnanguteste, lahendama simulatsioone ja sooritama teadmiste lõpukontrolli.

Pilootkoolituste korraldamine

Enne pilootkoolitust leppisid viis partnerit kokku koolituse korraldamise tingimustes oma riigis tagamaks, et:

- pilootkoolituse läbib vähemalt 24 osalejat igast partnerriigist (kokku vähemalt 120 osalejat kõigis riikides kokku);

- osalejad täidavad eelpiloodi küsimustiku, s.t hindavad enne koolitust oma olemasolevaid teadmisi (kokku vähemalt 120 täidetud ankeeti);

- teadmiste lõpukontroll loetakse sooritatuks, kui osaleja saavutab vähemalt 75%;

- osalejad täidavad pilootkoolituse lõpus ankeedi, s.t hindavad pärast koolitust oma olemasolevaid teadmisi (kokku vähemalt 120 täidetud ankeeti);

- vähemalt üks koolitaja igast partnerriigist täidab ka koolituse kohta ankeedi (vähemalt 5 ankeeti). Küsimustik aitab hinnata pilootkoolitust koolitaja vaatest. Koolitajate antud vastused (tagasiside) annavad infot väljatöötatud kursuse kvaliteedi, s.o teemade asjakohasuse kohta sihtrühmale, kursuse teemade terviklikkuse, kursuse materjali ülesehituse ja sisu kohta ning koolituse pikkus. Olulisim küsimus saab olema, mil määral on kursus saavutanud oma eesmärgi tutvustada kuulajatele küberturvalisust ja pettusi.

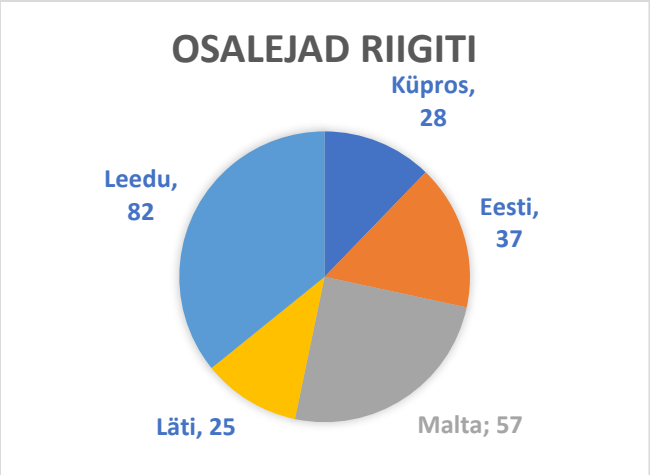
- Pilootkoolituse lõpus esitab iga partner koordinaatorile pilootkoolituse kokkuvõtte. Koordinaator kasutab seda teavet IO6 aruande koostamiseks. Partnerid värskendavad intellektuaalseid tulemusi (IO2, IO3, IO4 ja IO5) pärast pilootkoolituse tulemuste sünteesi.

5. PILOOTKOOLITUSTE TULEMUSED

Pilootkoolitus toimus viies partnerriigis – Küprosel, Eestis, Lätis, Leedus ja Maltal. Kokku osales koolitusel 229 osalejat. Sada seitsekümmend viis (175) osalejat läbisid koolituse 75% või kõrgema tulemusega.

Piloodieelne küsimustik

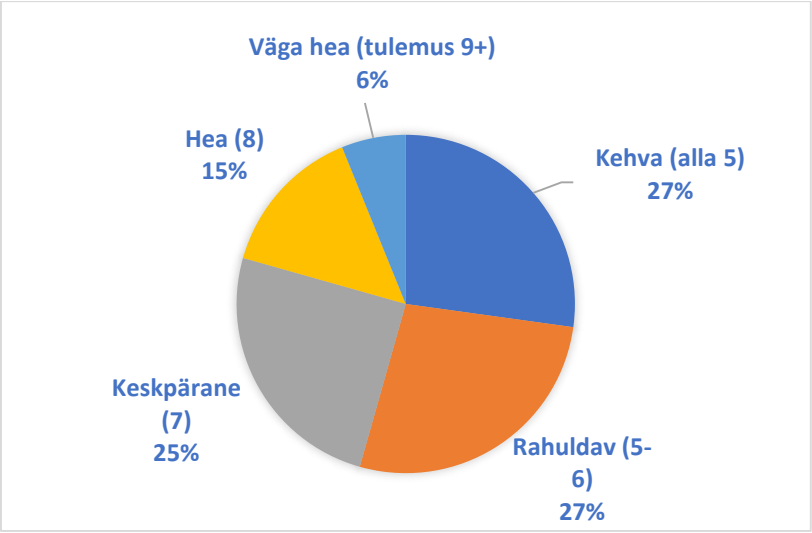
Enne pilootkoolituse algust täitsid kõik osalejad koolituseelse küsimustiku, et hinnata oma esmaseid teadmisi pettuste ja küberturvalisuse kohta. Selliseid eelankeete täitis kokku 229 osalejat. Osalejate jaotus riikide kaupa on näidatud alloleval joonisel 1.



Joonis 1. Pilootkoolitusel osalejad riigiti

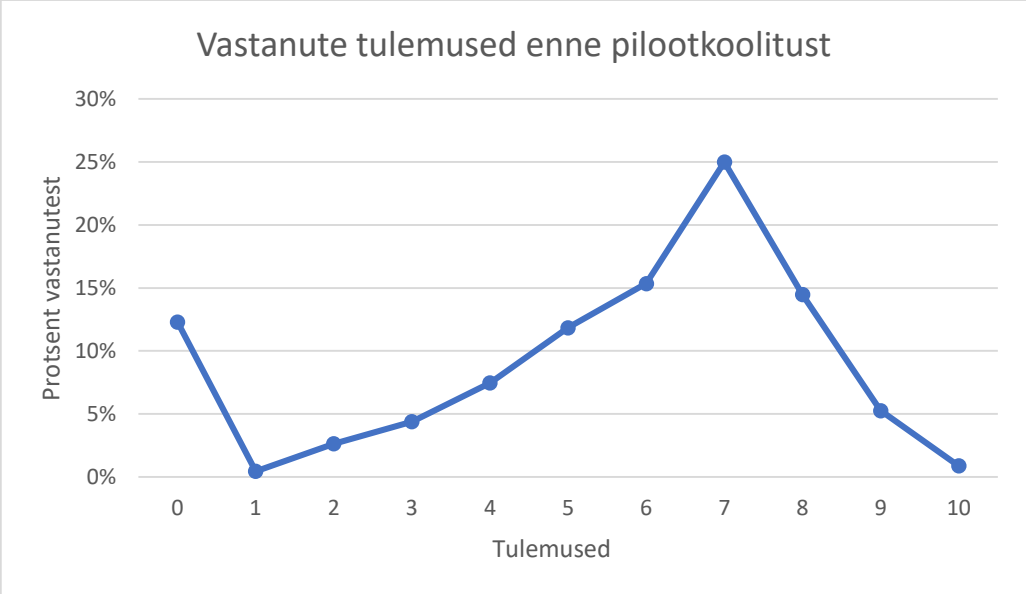
Osalejate teadmiste esialgne tase enne koolitust

Ankeete analüüsiti, et hinnata pilootkoolituses osalejate koolituseelseid teadmisi. Joonisel 2 on näidatud osalejate jaotus vastavalt saadud punktisummadele. 27% osalejate teadmised andmepüügist olid kehvad (skoor on alla 5 punkti). Samal osal (27%) osalejatest olid vaid algteadmised (s.o hind 5-6 punkti). 25% osalejatest oli hindeks "keskmine" (7 punkti). 15% osalejatest olid teadmised hinnatud "heaks" (s.o 8 punkti), kui vaid 6% osalejatest oli hindeks "väga hea" (9 punkti või rohkem). Osalejate teadmisi hinnati kümnepalliskaalal.



Joonis 2. Pilootkoolitusel osalejate andmepüügialased teadmised enne koolitust

Joonisel 3 on näidatud osalejate teadmiste jaotus (skoorina) enne pilootkoolitust kümnepallisel skaalal. On näha, et veidi üle viiendiku vastajatest saavutas kõrge hinde (s.o hinded 8, 9 ja 10)..



Joonis 3. Teadmiste tulemuse jaotus pilootkoolitusel osalejate lõikes.

Küsimuste raskusaste: 5 kõige lihtsamat küsimust

Osalejate küsimustike analüüsimine näitas, millised küsimused olid rasked ja millised piisavalt lihtsad. Osalejate antud vastuste põhjal oleme välja selgitanud viis kõige otsesemat küsimust. Ligikaudu 70–75% kõigist osalejatest vastas neile küsimustele õigesti. Need küsimused on toodud allolevas tabelis.

Lihtne 1. 15. Kas vastab tõele, et andmepüügirünnak toimub ainult e-maili teel?

EI
JAH

Lihtne 2. 13 Millised tegevused võivad sotsiaalse manipuleerimise rünnakuid ära hoida?

Kõik loetletud
Teadmine, millised teie isikuandmed on Internetis saadaval
Kasutate mitmefaktorilist autentimist
Lubate rämpspostifilter
Hoiate tarkvara ajakohasena

Lihtne 3. 5. Milline järgnevatest vastustest katab kõige paremini mõiste "küberrünnak" ulatust?

Mis tahes pahatahtlik tegevus küberruumis, isegi kui see ebaõnnestub
Kahjulikud tegevused Interneti kaudu
Viiruste ja troojalaste saatmine e-posti või SMS-i teel
Edukad andmepüügirünnakud

Lihtne 4. 12. Sotsiaalne rünnak on …

Inimeste manipuleerimine, tavaliselt psühholoogilise veenmise teel, et saada juurdepääs infosüsteemidele või andmetele.

Rünnak, mis kasutab pahatahtlikku programmi, mis on peidetud näiliselt vajaliku programmi sisse
Pahavara, mis ähvardab avaldada ohvri isikuandmeid või blokeerida neile püsivalt juurdepääsu, kui tasu ei maksta
Teatud tüüpi programm, mis on installitud kasutajate, nende süsteemide või sirvimisharjumuste kohta teabe kogumiseks, mis saadab andmed kaugkasutajale.

Lihtne 5. 14. Milliseid taktikaid kasutatakse andmepüügimeilide puhul?

Konfidentsiaalse teabe saatmise taotlus e-posti teel
Palun klõpsake meilis oleval lingil
Teabe edastamine eelmisel aastal edukalt sooritatud andmepüügirünnakute arvu ja tulemuste kohta
Palutakse annetada ookeani puhastamiseks
Palve saatjaga telefoni teel ühendust võtta

Tabel 1. Lihtsamad küsimused osalejatele (5 lihtsamat)

Esimene küsimus puudutab pettusvahendeid. Teine puudutab ennetusmeetmeid. Kolmas puudutab küberrünnakute määratlust. Neljas käsitleb sotsiaalset manipuleerimist ja viies meilides kasutatavat pettuse taktikat.

Seega saame järeldada, et osalejatel oli enne koolitust piisavalt teadmisi.

Pilootkoolitus: küsimuste keerukus: 5 kõige keerulisemat küsimust.

Osalejate antud vastuste analüüs tõi välja küsimused, millele vastati kõige kehvemini. Nendele küsimustele ei vastanud või vastasid halvasti 60–80% osalejatest. Need küsimused on toodud allolevas tabelis.

Keeruline 1. 7. Mis on küberturvalisuse sertifitseerimisraamistiku eesmärk?

Sertifitseerida IKT tooteid, protsesse ja teenuseid
Anda omandatud küberjulgeolekualaste pädevuste sertifikaat, mis on äratuntav kogu ELis
Anda väljaspool EL-i äratuntav IKT sertifikaat
Ükski vastustest ei ole õige

Keeruline 2. 8. Milline direktiiv oli esimene kogu ELi hõlmav küberjulgeolekualane õigusakt, mis kehtestas digitaalteenuste pakkujate (DSP) ja oluliste teenuste operaatorite (OES) juriidiliste kohustustena turvanõuded?

E-privaatsuse direktiiv
EL küberjulgeoleku seadus
NIS-direktiiv
Euroopa elektroonilise side koodeksi direktiiv

Keeruline 3. 3. Millised väited Phone Phreaks kohta on õiged?

Phone Phreaks õppis telefoniliine juhtima, kuulates helisid, kui operaatorid kõnesid ühendasid
Phone Phreaks lugesid telefonifirma tehnilisi ajakirju
Phone Phreaks ei tunginud kontoritesse oma riistvara arendamiseks
Phone Phreaks ei kaevanud "salajaste" dokumentide leidmiseks telefonifirma prügikastidess

Keeruline 4. 4. Mis vahe on küberturvalisusel ja arvutiturvalisusel?

Küberturvalisus haarab IT erinevad valdkonnad
need on samad
küberturvalisus on osa arvutiturbest
küberturvalisus tegeleb ainult Interneti-ohtudega
küberturvalisus on seotud viirustega jne.

Keeruline 5. 11. Millised väited andmepüügirünnaku kohta on õiged?

Andmepüük on sotsiaalse manipuleerimise pettus, mille tagajärjeks võib olla andmete kadu, maine kahjustamine, identiteedivargus, rahakaotus ja palju muud kahju inimestele ja organisatsioonidele.

Andmepüügipettus algab tavaliselt e-kirjaga, mis püüab võita potentsiaalse ohvri usaldust ja veenda teda ründaja soovitud toiminguid tegema. Andmepüük on süsteemivara omadus, mis võib kujutada endast süsteemi turvalisuse nõrkust või viga Andmepüük kirjeldab standardset vahendit, mille abil ohuagent ähvardab

Tabel 2. Kõige keerulisemad küsimused osalejatele (5 keerulisemat)

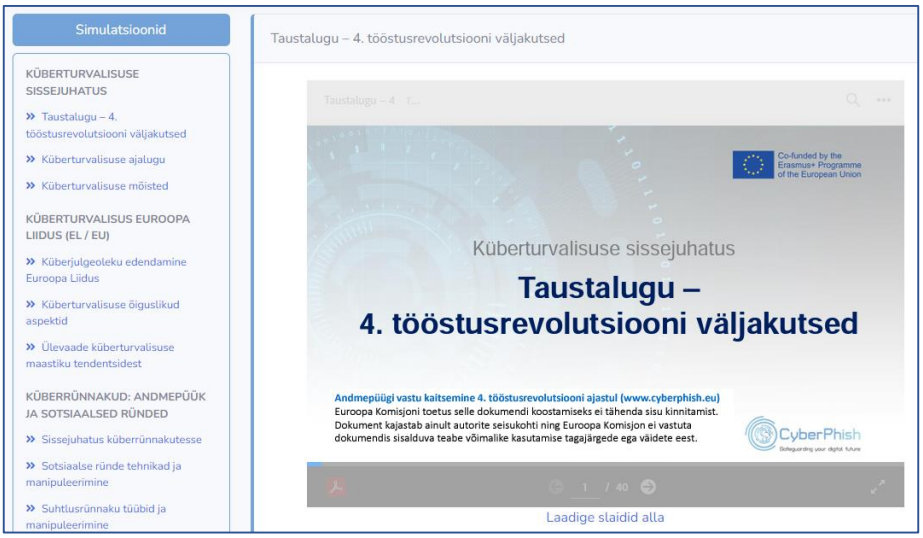
Esimene küsimus puudutas küberturvalisuse sertifitseerimisskeemi eesmärki; teine küsimus puudutas krüptimise eeliseid; kolmas küsimus puudutas kahjustatud seadme omadusi; neljas küsimus puudutas võrgu- ja infoturbe direktiivi; viies küsimus esitati küber- ja arvutiturbe erinevuste kohta.

Nagu näha, puudutasid küsimused kas tehnilisi teemasid või spetsiifilisi küsimusi, nagu küberturvalisuse raamistik või direktiiv.

Veebipõhine õppekeskkond

Pilootkoolitus viiakse läbi süsteemis, mille on välja töötanud ja hooldanud projekti koordinaator Vilniuse Ülikool. Süsteemi pääseb ligi lingi https://cyberphish.vuknf.lt/ kaudu. Õppeplatvormi saavad kasutada nii registreerunud kui ka registreerimata osalejad. Registreerimata osalejad saavad vaadata üldteavet koolituse kohta, vaadata reitingutabeleid ja vaadata või alla laadida koolitusmaterjale kõigis partnerkeeltes: inglise, eesti, kreeka, läti ja leedu keeles.

Joonis 4. Veebipõhine õppekeskkond

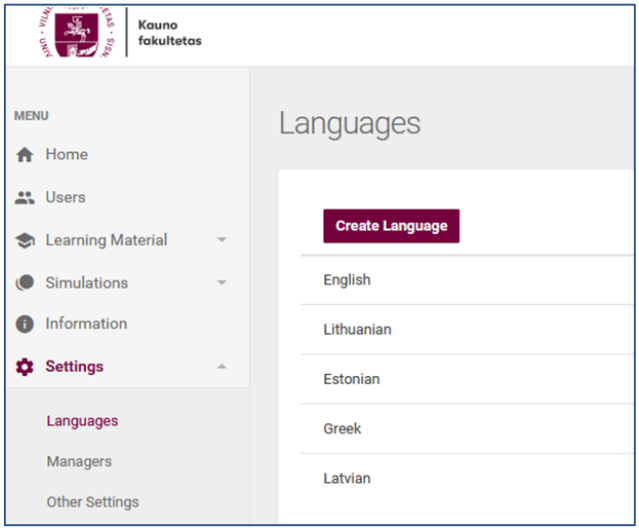


Joonis 5. Õppematerjal veebipõhises õppekeskkonnas

Veebipõhise õppekeskkonna kolm rolli

Veebipõhises õppekeskkonnas on kolm kasutajarolli: administraator, kohalik administraator ja kursusel osaleja.

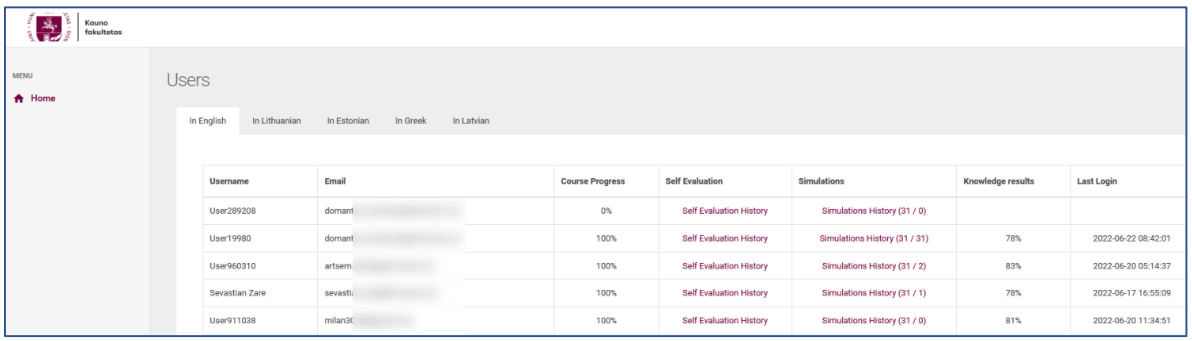
Administraator saab vaadata kõigi kasutajate statistilist teavet, nagu viimane sisselogimine, IP-aadress, olek ja e-posti aadress. (Joonis 6)



Joonis 6. Administraatori vaade

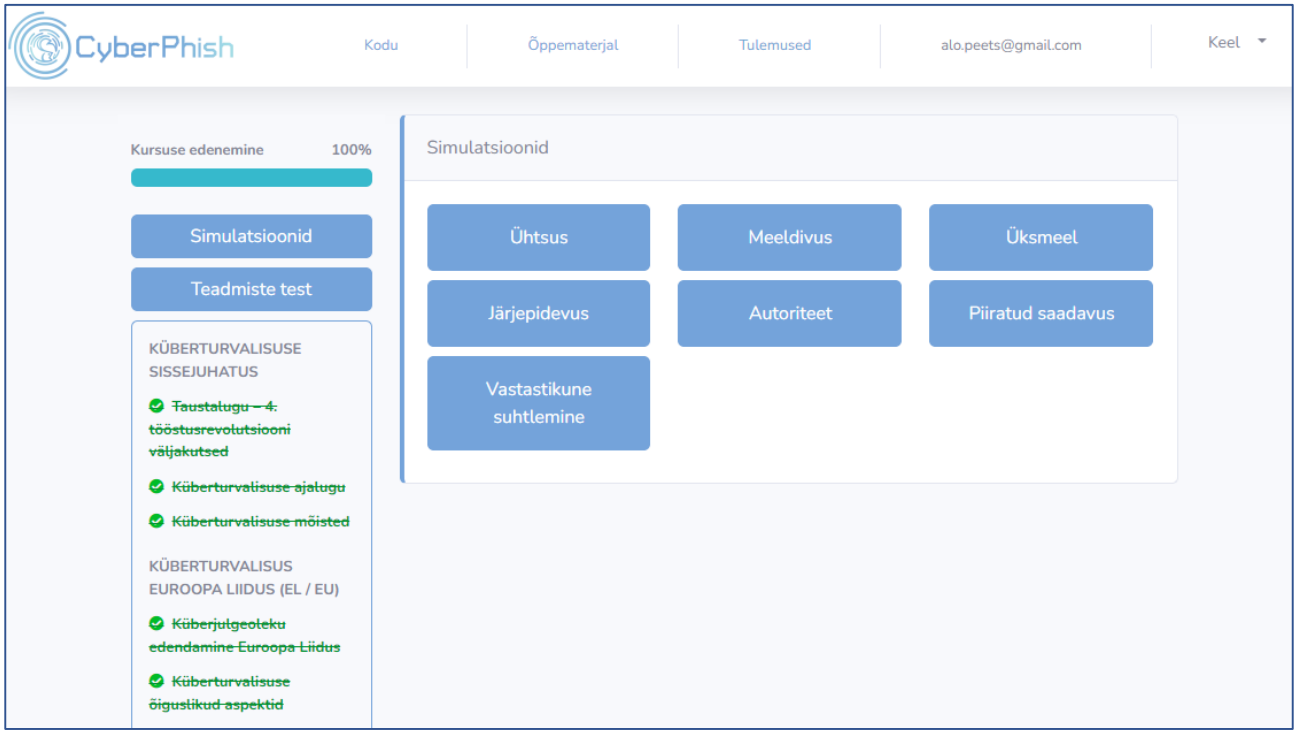
Administraator saab laadida üles koolitusmaterjale, importida ja redigeerida simulatsioone, luua kohalikke administraatorkasutajaid ning määrata muid e-platvormiga seotud toiminguid, mis pole teistele kasutajatele kättesaadavad.

Kohalik administraator näeb statistilist teavet kasutajate edusammude kohta, samuti teavet sooritatud enesehinnangu testide ja lahendatud simulatsioonide, viimase sisselogimise ja teadmiste hindamise testi tulemuste kohta. Samuti saab kasutaja vaadata lahendatud enesehindamise küsimusi ja stsenaariume, näha, kuidas osaleja konkreetse stsenaariumi lahendas ja kui palju punkte iga vastuse eest kogus. (Joonis 7)



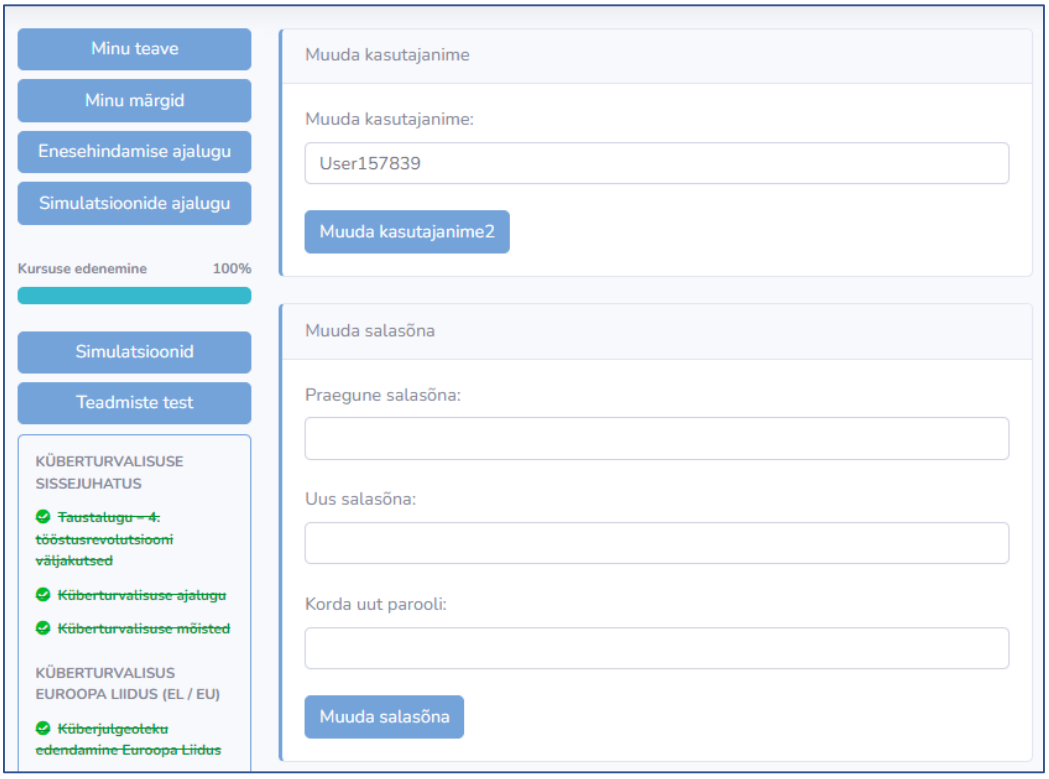
Joonis 7. Kohaliku administraatori vaade

Registreerunud kursusel osaleja saab kasutada õpikeskkonda õppimise eesmärgil. Joonisel 8 on näide kursusel osalejate vaatest.



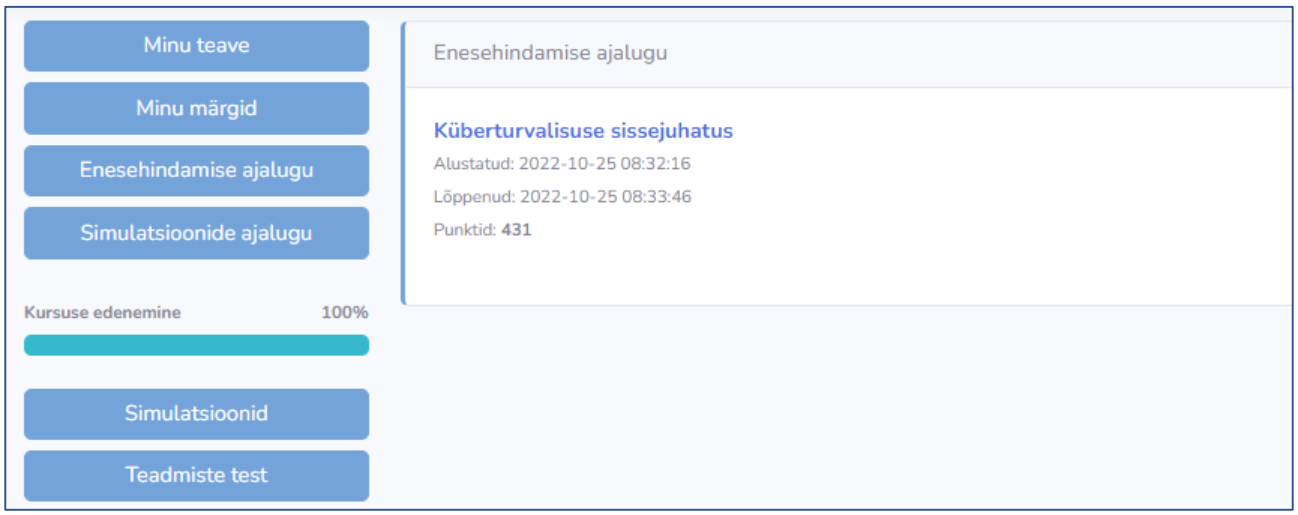
Joonis 8. Kursusel osaleja õpikeskkonna vaade

Pärast kursusele registreerumist saab osaleja muuta enda kohta käivat teavet, st kasutajanime ja parooli (vt joonis 9).



Joonis 9. Kursusel osaleja isikuandmete muutmise aken

Registreeritud kursusel osalejana saate jälgida oma enesetestide ajalugu ja teadmiste kontrolli ajalugu ning vaadata, kui palju märke olete teeninud (vt joonis 10).



Joonis 10. Kursusel osaleja enesehindamise testi ajaloo vaade

Registreerunud kursusel osalejana saad jälgida enda läbitud/lahendatud simulatsioonide ajalugu:

- millal ja kuidas küsimustele vastasite;
- millised stsenaariumid lahendasite;
- Kui palju punkte sa igaühe eest said.

Joonis 11. Kursusel osalejate simulatsiooni ajaloo vaade

Märgid

Enne pilootkoolitust leppisid partnerid kokku kuus rinnamärki. Siiski valmis projekti käigus **kaheksa märki**:

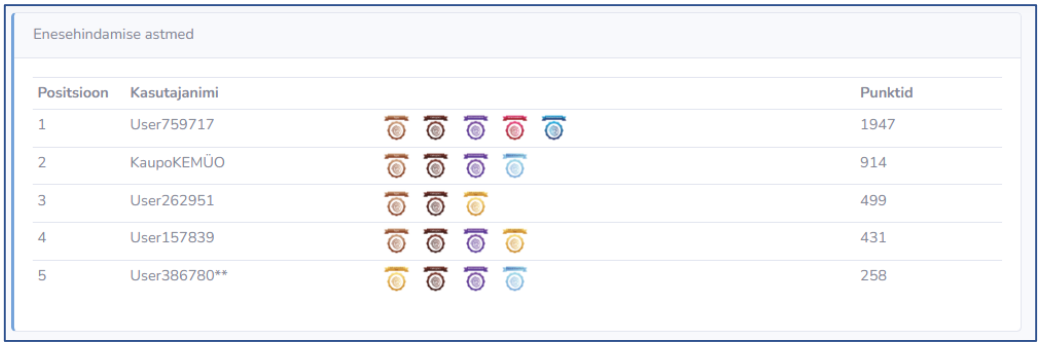
- testi sooritamine;
- kursuse läbimine;
- kõigi simulatsioonide lahendamine;
- esimese enesehinnangu testi sooritamine;
- kategooria ja teema täitmine;
- kõikide esitluste läbimine;
- iga päev kümne päeva jooksul süsteemi sisse logides.

Joonisel 12 leiate märkide näited.

Joonis 12. Märkide näited

Tulemused

Registreerunud kursusel osalejad saavad enesetestide eest punkte koguda vastavalt partneritega kokkulepitud reeglitele. Need tulemused kuvatakse enesehinnangu edetabelite tabelis. Kursusel osaleja nimi ja kogutud puntid kuvatakse tulemuste tabelis..



Joonis 13. Registreerunud kursusel osalejate pingeread

Õppematerjal veebipõhises õpikeskkonnas

Partnerite konsortsium töötas välja veebipõhise koolitusmaterjali, järgides CyberPhishi õppekava ja vastavalt 4. tööstusrevolutsiooni vajadustele. Sõltumatud eksperdid hindasid väljatöötatud õppematerjali heaks (üks partnerriigi kohta). Allolevas tabelis 4 on välja töötatud koolitusmaterjalide kokkuvõte.

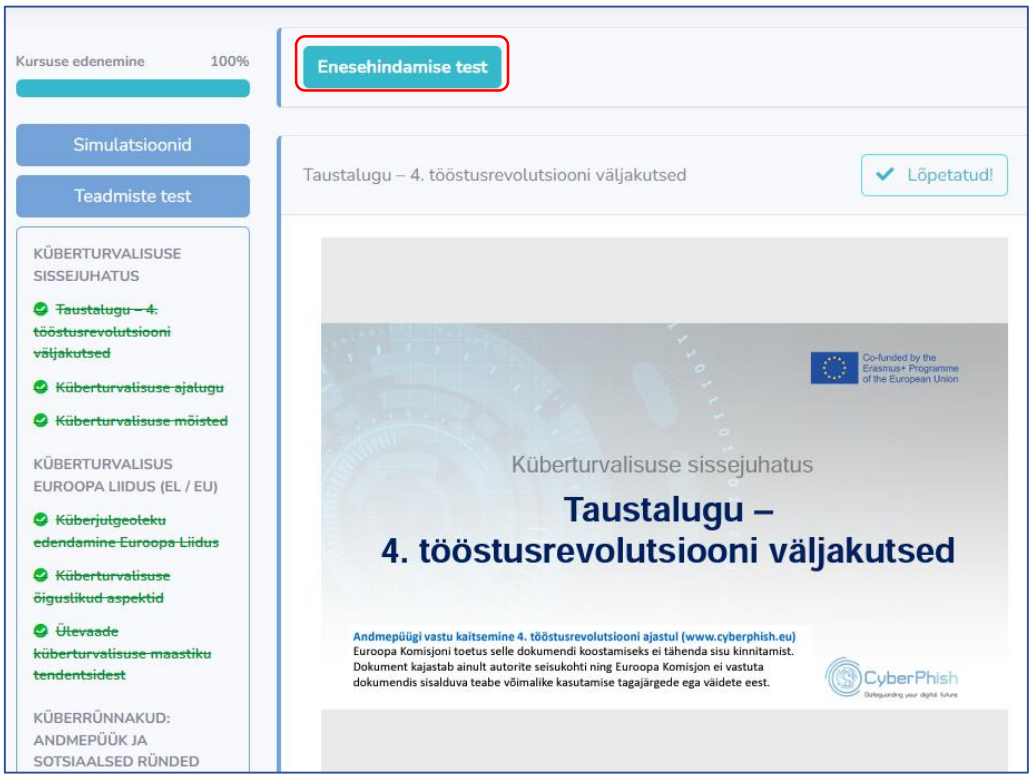
Mooduli ja alamteemade nimetus				Slaidide arv
1	**Küberturvalisuse sissejuhatus**	1.1	Taustalugu – 4. tööstusrevolutsiooni väljakutsed	40
		1.2	Küberturvalisuse ajalugu	31
		1.3	Küberturvalisuse mõisted	15
2	**Küberturvalisus Euroopa Liidus (EL / EU)**	2.1	Küberjulgeoleku edendamine Euroopa liidus	31
		2.2	Küberturvalisuse õiguslikud aspektid	14
		2.3	Ülevaade küberturvalisuse maastiku tendentsidest	41
3	**Küberrünnakud: andmepüük ja sotsiaalsed ründed**	3.1	Sissejuhatus küberrünnakutesse	20
		3.2	Sotsiaalse ründe tehnikad ja manipuleerimine	73
		3.3	Suhtlusrünnaku tüübid ja manipuleerimine	37

		3.4	Juhtumiuuringud	37
4	**Küberrünnakute mõistmise ja nendega toimetuleku ülevaade**	4.1	Alusteadmised e-turvalisusest	22
		4.2	Ennetavad tegevused	59
		4.3	Andmepüügirünnakute äratundmine	108
		4.4	Küberrünnakutega toimetulemine	87
		4.5	Kahjude minimeerimine juhtumitele reageerimise kaudu	34
			Kokku:	**649**

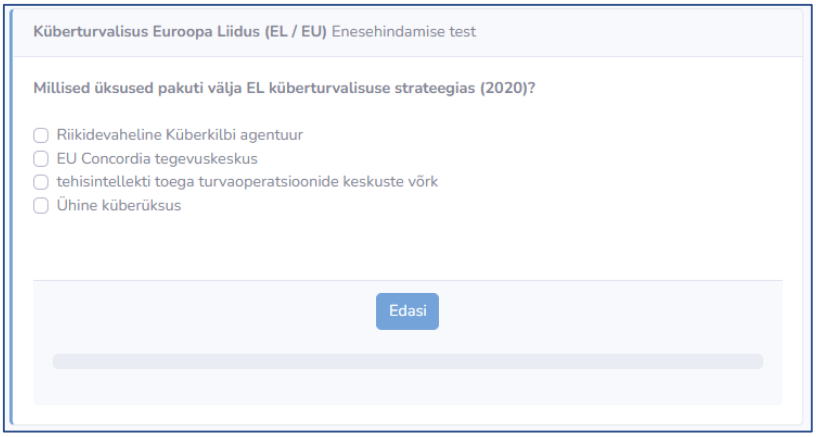
Tabel 3. Kokkuvõte õppematerjalist

Ülesanded veebipõhises õppekeskkonnas

Kursuse sisu on võimalik vaadata ekraanilt ja/või alla laadida PDF formaadis. Kui registreerunud osaleja on läbi vaadanud kõik konkreetse teema koolitusmaterjalid, saab ta oma teadmisi proovile panna enesetesti sooritades. Kursuse osade läbimise eest antakse punkte.



Joonis 14. Enesehindamise testi nupp kursusel osaleja keskkonnas

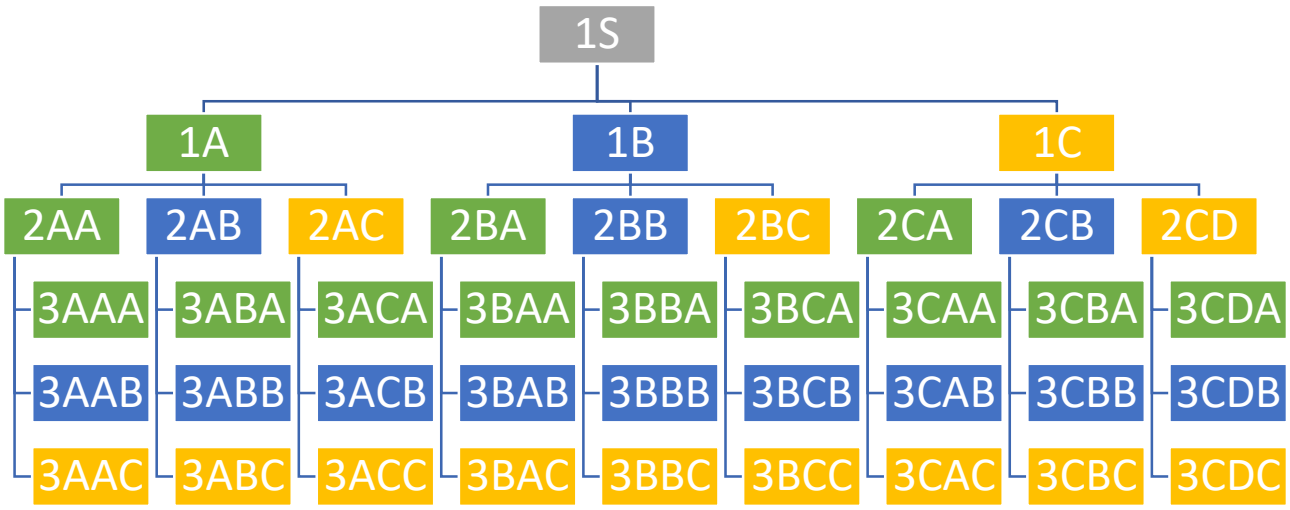


Joonis 15. Enesehinnangu testi näidis

Simulatsioonid

Simulatsioon simuleerib tegelikke pettuste rünnakuid, esitades protsessi kasutajale mänguliselt. Simulatsiooni eesmärk on aidata inimestel parandada küberturvalisuse ja pettuste kriitilist mõtlemist, tuvastades andmepüügi, rämpsposti, küberkiusamise ja muud juhtumid. Projektipartnerid töötasid välja 55 simulatsiooni.

Simulatsioon koosneb olukorra kirjeldusest, eesmärgist, osalejatest, ründe tüübist ja mitmest (3-4) vastusevariandist kasutaja käitumise valimiseks. Kõik simulatsioonid põhinevad otsustuspuul. Joonisel 15 on näidatud simulatsioonimudel. Igal simulatsioonil on kolm taset. Optsioonide (võimalike valikute) koguarv peab olema vähemalt 50, maksimaalselt 84 optsiooni.



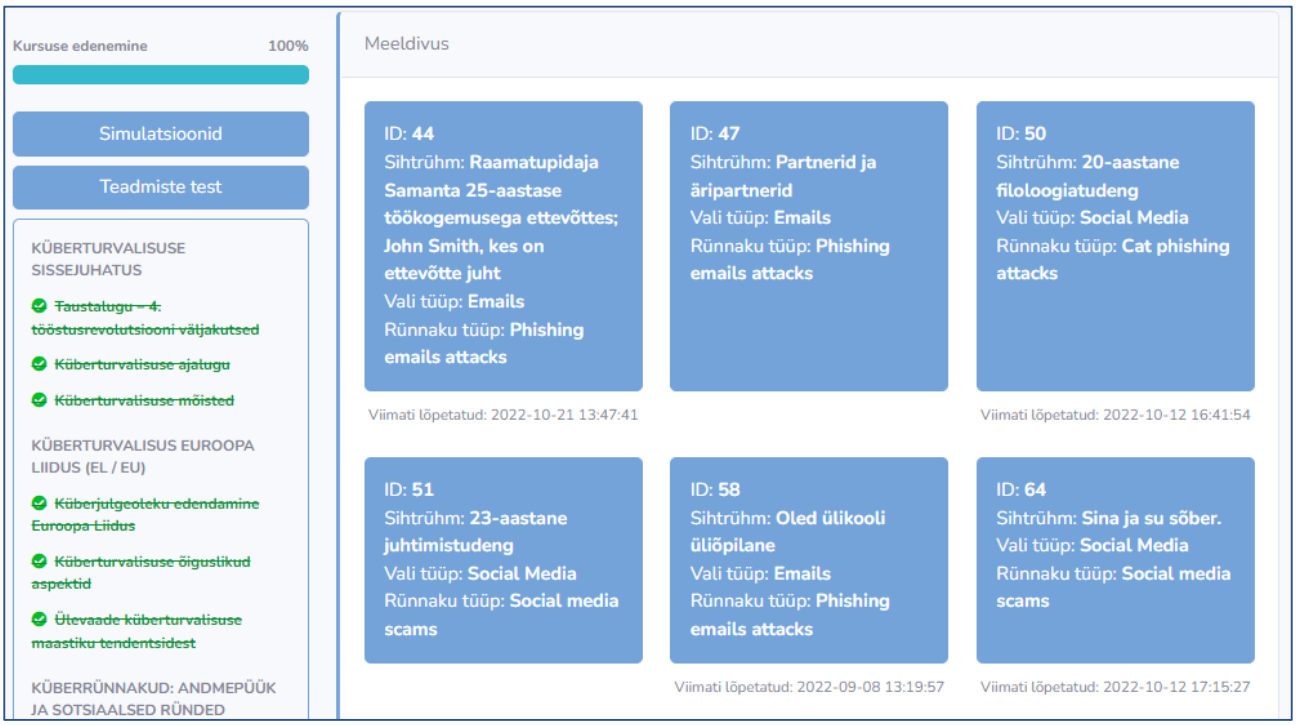
Joonis 16. Simulatsioonimudel põhineb otsustuspuul

Simulatsioonis viib iga kasutaja valitud vastus võimalike vastusevalikute järgmisele tasemele. Simulatsioonil on kolme tüüpi lahendusi: õige, osaliselt õige ja vale. Iga vastuse eest annab süsteem kursusel osalejale teatud arvu punkte. Süsteem annab ekraanile tagasisidet, kui valitakse osaliselt õige või vale vastus. Samuti antakse ettepanekuid, millist materjali osa peaks õpilane kordama ja millist teemat edasi uurima. Simulatsioonide valimine toimub kategooriate kaupa.

Joonis 17. Simulatsiooni kategooriad/teemad

Simulatsioone saab kasutada kahel viisil: õppimiseks ja teadmiste kontrollimiseks. Ühel viisil antakse koolitatavale tagasisidet pärast igat olukorda, teiselt poolt aga alles pärast kogu simulatsioonistsenaariumi läbimist. Simulatsioonide lahendamise eest antakse punkte, kõigi stsenaariumide lahendamise eest antakse märk.

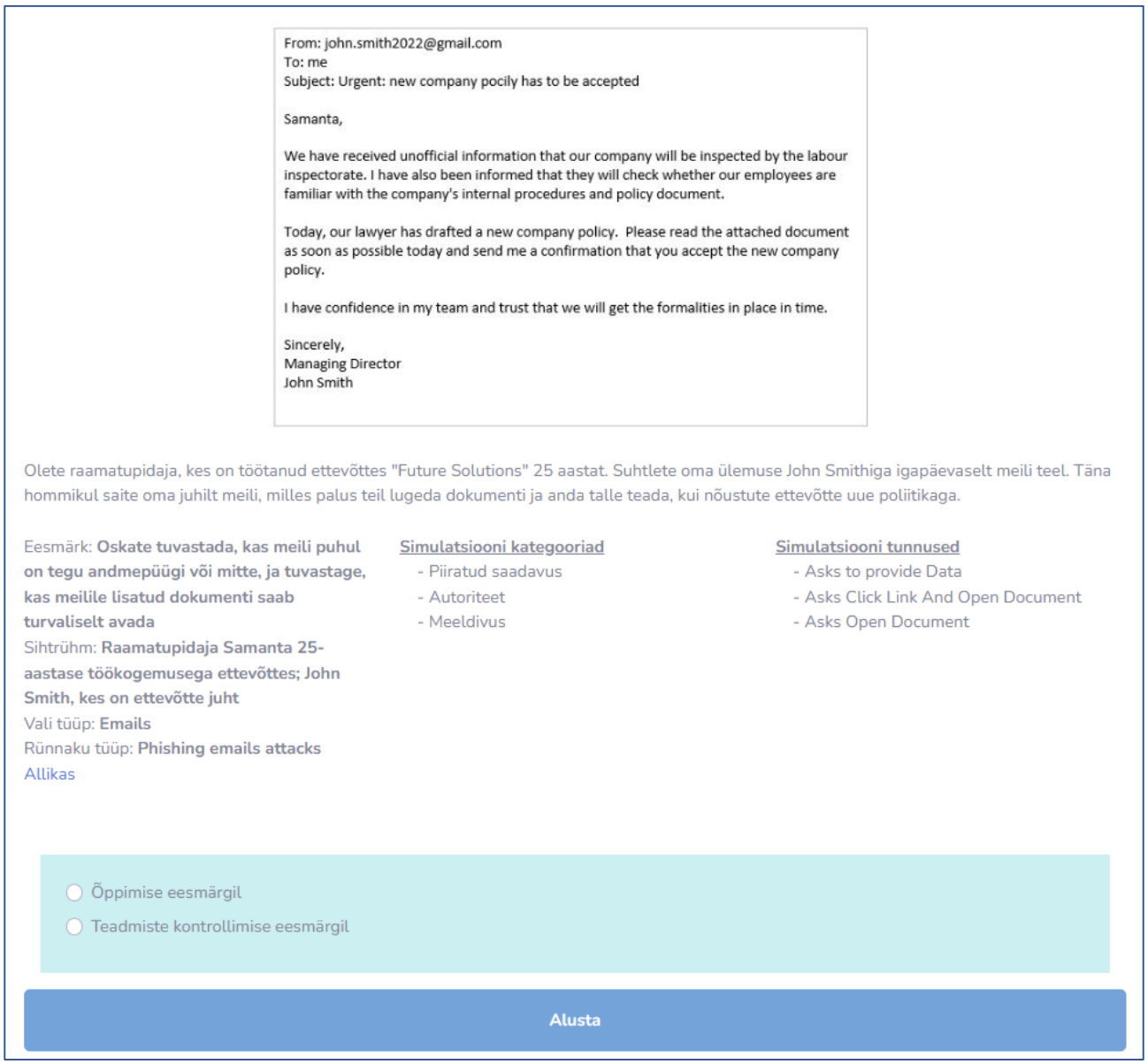
.



Joonis 18. Simulatsioonide valik teemas Meeldimine

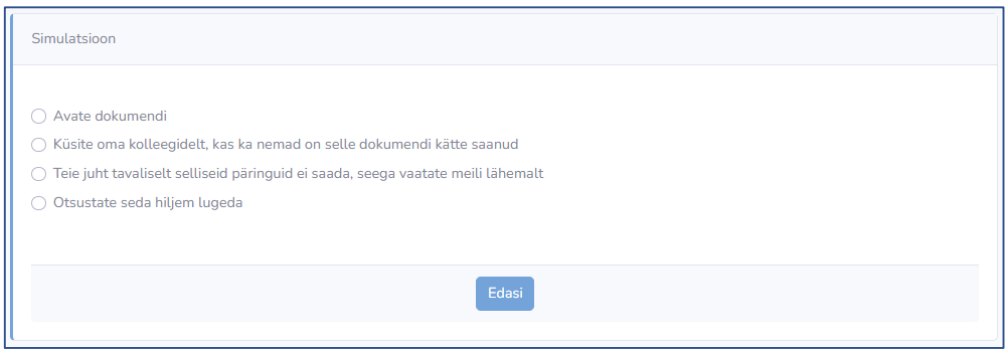
Pärast simulatsiooni valimist näidatakse kursusel osalejale olukorra kirjeldust, simulatsiooni eesmärki, tegelasi, andmepüügi rünnaku tüüpi ja muid atribuute. Sageli (kuid mitte alati) näidatakse pilti mulje suurendamiseks (et osaleja empaatiavõimelisemaks muuta).

Seejärel on võimalus valida simulatsiooni eesmärk: õppimise eesmärgil või teadmiste kontrollimiseks.



Joonis 19. Simulatsioonilahenduse näide

Kui simulatsioon on alanud, esitatakse osalejale valikud. Nad peavad valima, kuidas ta sellises olukorras käitub. Alloleval joonisel on näide simulatsioonilahendusest.

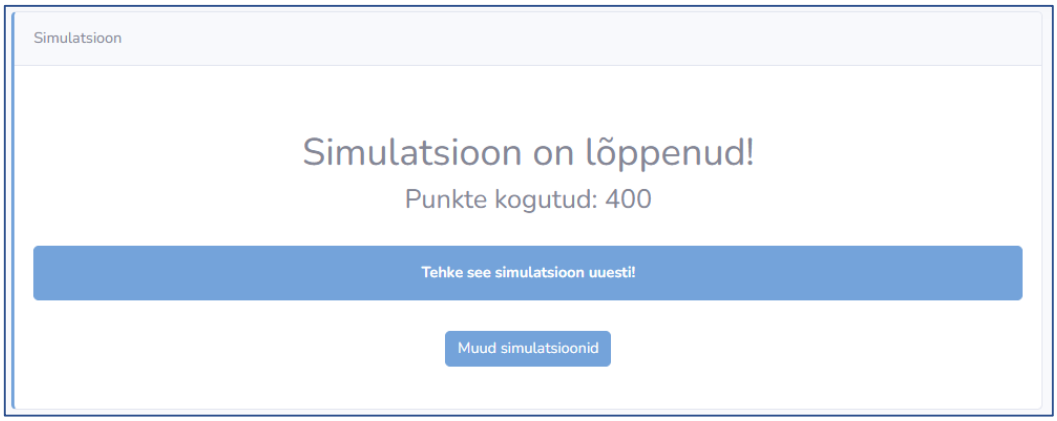


Joonis 20. Simulatsiooni lahendamine

Simulatsiooni käigus saab kasutaja vale või osaliselt õige vastuse valimisel ekraanil tagasisidet. Joonis 21 illustreerib kasutajale kuvatavat tagasisidet simulatsioonilahenduse ajal.

Joonis 21. Ekraanil tagasiside kasutajale simulatsioonilahenduse ajal

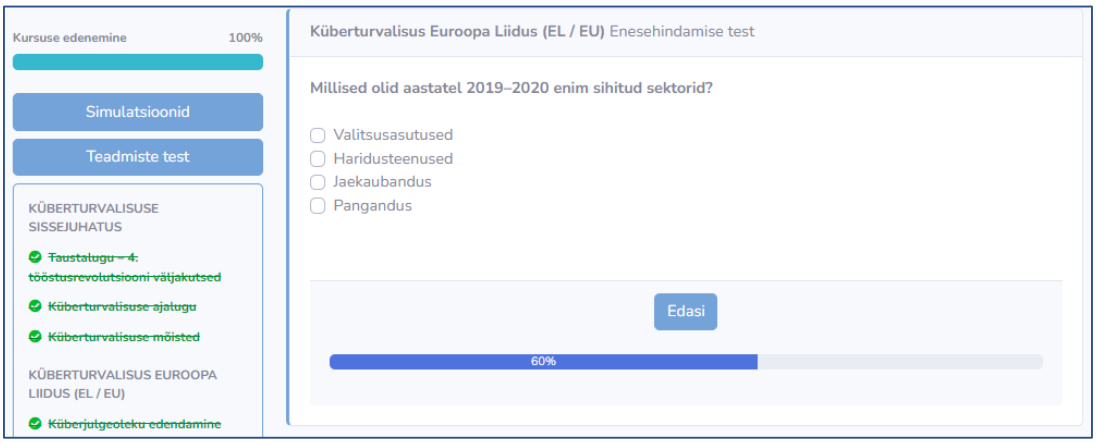
Kui simulatsioon on lõppenud, kuvatakse kasutajale teade, mis näitab kogutud punktide arvu ja kutsub üles teisi simulatsioone lahendama. Kui simulatsioon lahendati valesti, antakse soovitus simulatsioon uuesti lahendada (vt joonis 22).



Joonis 22. Lõpetatud simulatsiooni aken

Teadmiste hindamise test

Pärast koolitusmaterjaliga tutvumist (enesetestid ja simulatsioonid) esitatakse osalejale õpikeskkonnas nupp teadmiste testi sooritamiseks. Pilootkoolituse käigus saab teadmiste kontrolli sooritada kolm korda.



Joonis 23. Teadmiste hindamise testi küsimuse näide

Teadmiste kontrolli lõpus näeb kursuslane oma teadmiste hindamise protsenti.

Joonis 24. Teadmiste hindamise testi hindamisakna näide

Märkus. Teadmiste test on mõeldud teadmiste hindamiseks. See test ei ole mõeldud õppimiseks. Teadmiste teste ei avaldata avalikult osalejatele, mentoritele ja/või õpetajatele. Küsimused on tekstivormingus kättesaadavad kõikidele projektipartneritele/arendajatele ning süsteem ei võimalda ligipääsu üksikasjalikele testitulemustele. Ka teised mentorid/õpetajad ei saa kõiki testitulemusi vaadata.

Teadmiste testid

Partnerid on leppinud kokku, et töötavad välja enesetestide küsimused ja teadmiste kontrolli küsimused taotluses toodud info põhjal. Küsimused on järgmist tüüpi.

Enesehindamise testides on kolme tüüpi küsimusi:

- ühe õige vastusega valikvastustega küsimused (võimalike vastuste arv: 3-6),

- valikvastustega küsimused (4-6 võimalikku vastust),

- jah/ei Küsimused.

Partnerid on kokku leppinud/otsustanud küsimuste hulga/küsimuste koguse õppematerjali teema kohta. Näiteks 8-14 küsimust teemadest "Küberturvalisuse sissejuhatus" ja "Ülevaade küberturvalisusest EL-is". Partnerid lõid 12–20 küsimust teemadest " Küberrünnakud: andmepüük ja sotsiaalsed ründed" ning " Küberrünnakute mõistmise ja nendega toimetuleku ülevaade".

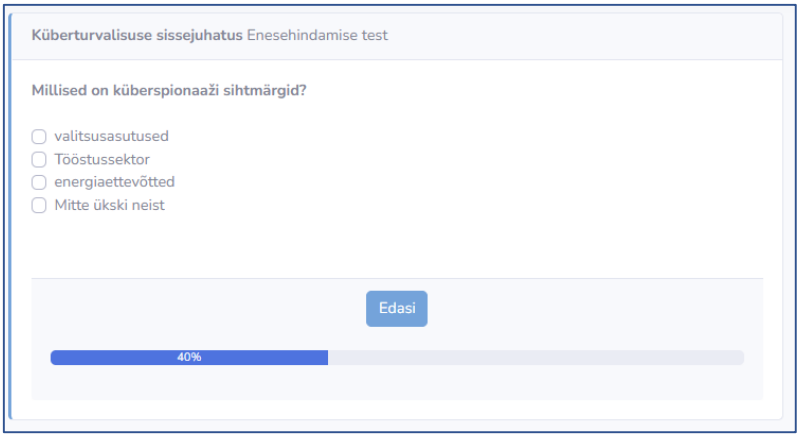
Enesehindamise küsimuste jaotus**:**

Mooduli nimetus	Enesehindamise küsimused
Küberturvalisuse sissejuhatus	13
Ülevaade küberturvalisusest EL-is	12
Küberrünnakud: andmepüük ja sotsiaalsed ründed	16
Küberrünnakute mõistmise ja nendega toimetuleku ülevaade	19
Total:	**60**

Tabel 4. Enesehindamise testi küsimuste jaotus

Kui kõik konkreetse mooduli alateemad on läbi vaadatud, ilmub õpikeskkonda nupp "Enesehindamise test". Test koosneb viiest küsimusest. Küsimused valitakse juhuslikult praeguse kategooria küsimuste pangast.

Enesehinnangu testi ajal kuvatakse ekraani allosas edenemisriba, mis näitab vastatud küsimuste protsenti ja järelejäänud küsimuste arvu.

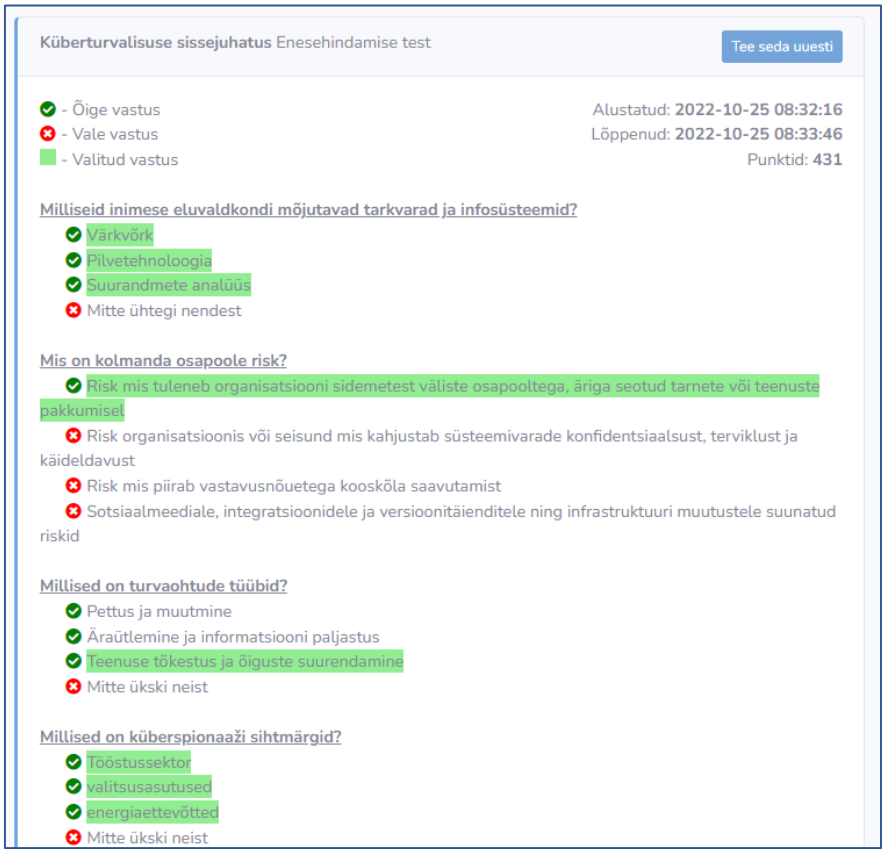


Joonis 25. Näide enesehinnangu testi küsimusest kategoorias "Küberturvalisuse sissejuhatus"

Enesehinnangu testi lõpus näidatakse osalejale õiged ja valed vastused. Õppija poolt märgitud vastused on esile tõstetud rohelisega. Osaleja näeb ekraani paremas ülanurgas alguskuupäeva ja kellaaega, lõppkuupäeva ja -kellaaega ning kogutud punktide arvu.

Enesehindamise testide arv ei ole piiratud. Kursusel osalejad võivad seda võtta nii tihti kui soovivad. Järgmine kord, kui nad testi sooritavad, esitatakse neile muid juhuslikult valitud küsimusi.

Osalejaid autasustatakse ka märgiga vastavalt partnerite vahel kokkulepitud reeglile.



Joonis 26. Näide enesetesti tulemustest

Teadmiste testid. Samuti on partnerid kokku leppinud teadmiste testides esitatavate küsimuste arvus.

- Kõigil küsimustel on neli vastust, millest ainult üks on õige.

- Loodi 144 teadmiste testi küsimust.

Teadmiste test koosneb 36 küsimusest. Testi täitmiseks kulub kuni 45 minutit. Läbimise protsent on 75%.

Partnerid on kokku leppinud küsimuste arvu iga õppematerjali teema kohta. Näiteks 20-25 küsimust teemadest "Küberturvalisuse sissejuhatus" ja "Ülevaade küberturvalisusest EL-is". Töötati välja 45–65 küsimust teemadel "Küberrünnakud – sotsiaalne manipuleerimine ja andmepüük" ning "Küberrünnakute mõistmine ja juhtimine".

Teadmiste hindamise testide küsimuste täpsustamine:

Mooduli nimetus	Teadmiste testi küsimusi
Küberturvalisuse sissejuhatus	24
Ülevaade küberturvalisusest EL-is	20
Küberrünnakud: andmepüük ja sotsiaalsed ründed	62
Küberrünnakute mõistmise ja nendega toimetuleku ülevaade	46
Kokku:	**152**

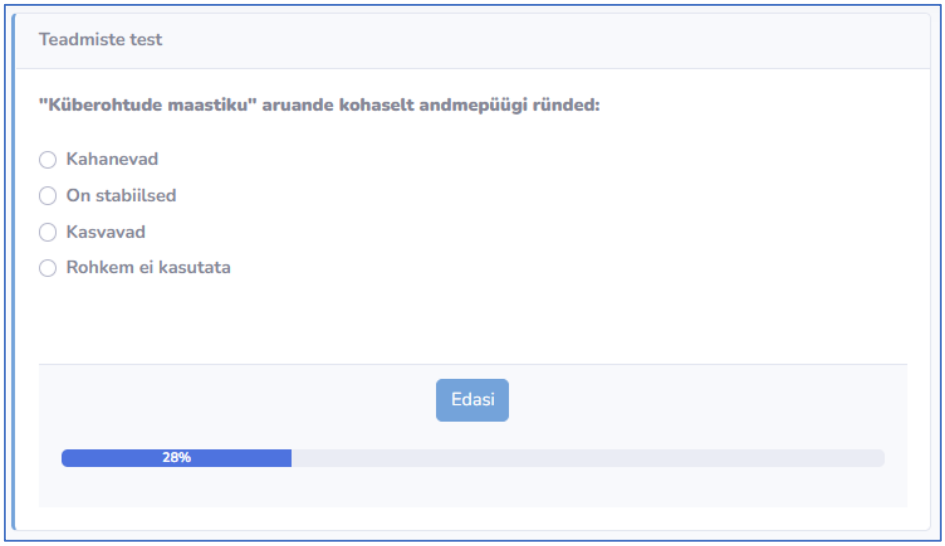
Tabel 5. Teadmiste hindamise testide küsimuste jaotus

Pilootkoolituse käigus oli teadmiste kontrollide arv piiratud. Seda testi saab sooritada kuni 3 korda.

Õpikeskkonnas kuvatakse teadmiste kontrolli nupp, kui kogu kursus on läbitud. Testi nupul klõpsamine näitab katsete arvu, mida osaleja testi sooritamiseks teeb. Kui test on varem tehtud, näidatakse eelmise testi tulemus protsentides.

Joonis 27. Teadmiste testi algusaken

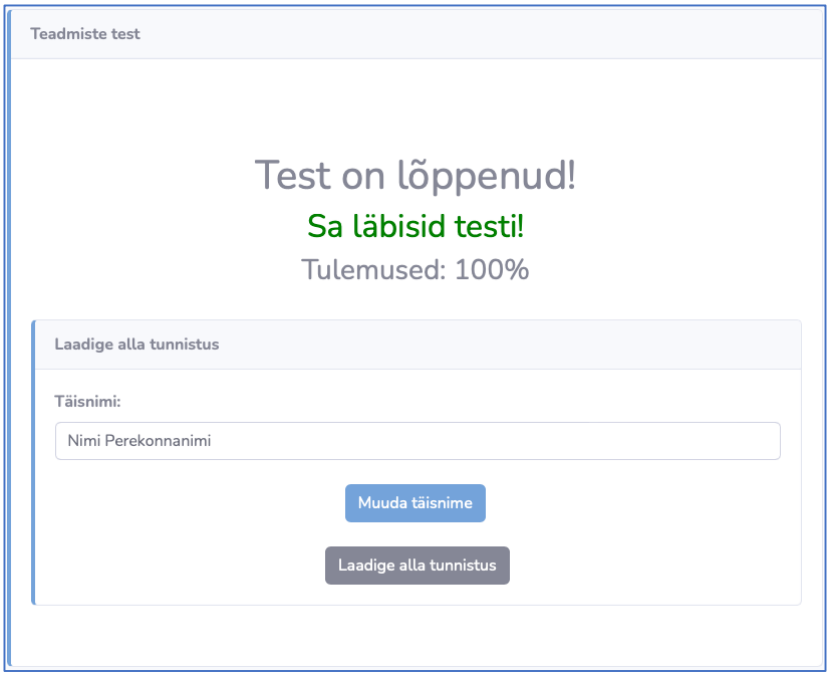
Teadmiste test koosneb juhuslikust valikust 36 küsimusest. Igast kategooriast juhuslikult valitavate küsimuste arvu jaoks on kehtestatud reegel. Testi ajal näitab edenemisriba vastatud küsimuste protsenti ja järelejäänud küsimuste arvu. Testi lõpus kuvatakse testi tulemus, kuid osaleja ei näe, kuidas ta on küsimustele vastanud, kuna tegemist on teadmiste hindamise testiga.



Joonis 28. Teadmiste testi küsimuse näide

Kui osalejad testi läbi kukuvad, võivad nad proovida koolitusmaterjali korrata, sooritada enesehinnangutestid ja proovida uuesti teadmiste testi läbimist.

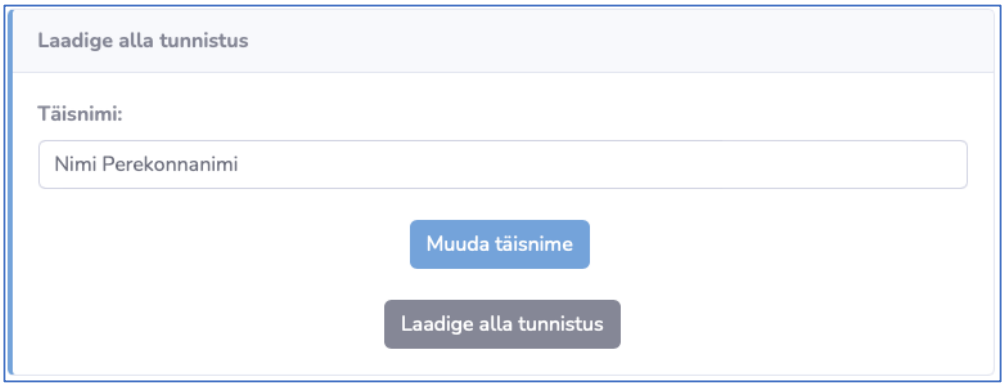
Õnnestumise korral antakse osalejale võimalus sisestada oma nimi ja alla laadida tunnistus PDF formaadis.



Joonis 29. Läbitud teadmiste testi aken

Tunnistus

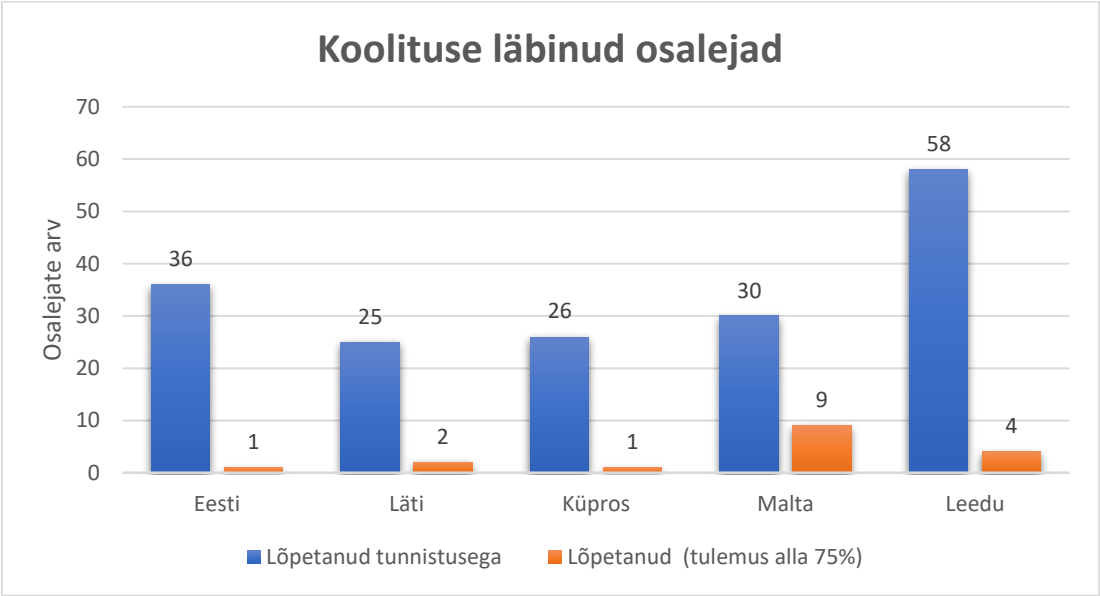
Pärast testi sooritamist saab osaleja lingi testijärgse küsimustiku täitmiseks, mille järel saab täita oma nime ja tunnistuse PDF-vormingus alla laadida. Automaatne tunnistuse väljastamise viis hõlbustab sertifikaadi väljaandmise protsessi.



Joonis 30. Lõputunnistuse loomise vaade

Koolituse läbinud osalejad

Alloleval joonisel on näidatud koolituse tulemused. Sada seitsekümmend viis (175) osalejat läbisid koolituse ja said tunnistuse: 36 Eestis, 25 Lätis, 26 Küprosel, 30 Maltal ja 58 Leedus. Veel 17 osalejat läbisid kursuse ilma tunnistuseta, st nende teadmiste testi tulemus oli alla 75%.



Joonis 31. Statistika koolituse läbinud kasutajate kohta

Koolitusjärgsed küsimustikud täitsid ja esitasid 139 osalejat: 31 Eestist, 24 Lätist, 16 Küproselt, 27 Maltalt ja 40 Leedust.

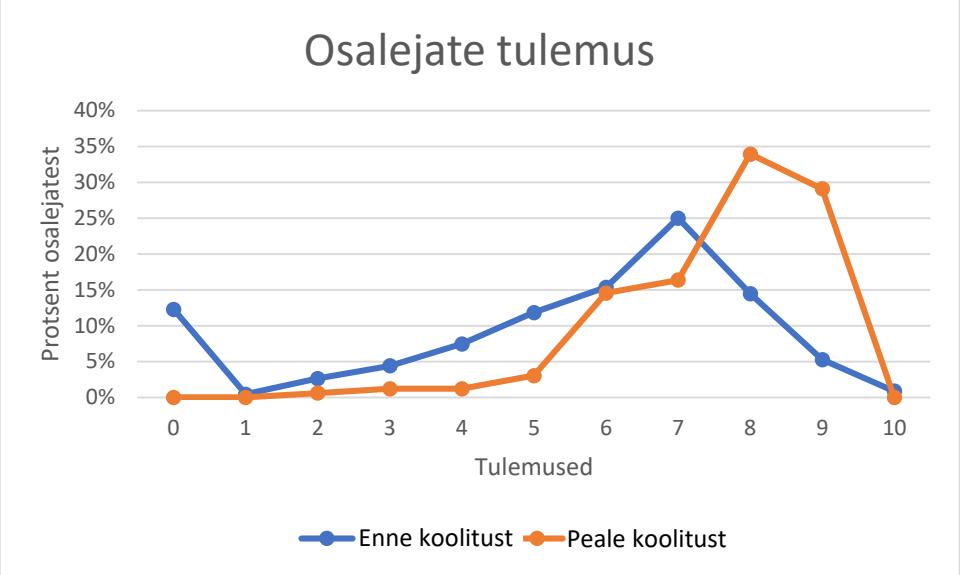
Koolitusjärgsed küsimustikud täitsid 8 õpetajat: 2 Maltalt, 3 Leedust ja 1 Eestist, Lätist ja Küproselt. Õpetajad nõustusid, et kursus saavutas oma eesmärgi tutvustada õpilastele küberturvalisust ja õngitsemist (sama protsent vastanutest märkis, et nõustub väitega ja nõustub igati). Vastajad nõustuvad (62,5%) ja nõustuvad täielikult (37,5%), et programmis käsitletud teemade detailsus oli asjakohane. Valdav osa õpetajatest (62,5%) nõustub täielikult väidetega „Pilootkursuse läbimiseks oli osalejatele piisav aeg“ ja „Kursusega käsitletud teemavaldkonnad olid sihtrühmale sobivad“.

Õpetajad kommenteerisid, et kursus on hästi kavandatud ning arendab osalejate teadlikkust ja kriitilist mõtlemist. Selle sissejuhatus ei tohiks piirduda IKT-ga seotud kursustega, vaid see tuleks kas osaliselt või täielikult sisse viia erinevatele kursustele. Kõige positiivsemat tagasisidet said stsenaariumilahendused.

Osalejate teadmiste võrdlus enne ja pärast pilootkoolitust

Koolituseelse ja -järgse teadmiste hindamise võrdlemine näitas, et osalejad parandasid oluliselt oma teadmisi küberturvalisusest ja andmepüügist. Allolev graafik näitab, kuidas nägid välja osalejate teadmised küberturvalisusest ja pettustest enne ja pärast pilootkoolitust. Horisontaalne telg näitab hindevahemikke (hindeid) ja vertikaaltelg vastava punktisumma saanud õpilaste protsenti.

Seega on jooniselt näha, et pärast CyberPhishi koolitust paranes osalejate sooritus oluliselt, st rohkem õpilasi sai hinded 8 või kõrgemad. Samal ajal vähenes nende osalejate arv, kes sooritasid teadmiste kontrolli kehvasti, s.o hinded vahemikus 0 kuni 6.



Joonis 32. Osalejate teadmised küberturvalisusest ja andmepüügist enne ja pärast pilootkoolitust

6. PILOOTIKOOLITUS PARTNERRIIKIDES

See peatükk tutvustab partnerriikide – Eesti, Küprose, Läti, Leedu ja Malta – kogemusi koolitusprogrammide rakendamisel. Iga riik pakub teavet valdkondade kohta, sealhulgas osalejate teave ja valikuprotsess, osalejate profiil, õpilaste motivatsioon pilootkoolitusega liituda, koolitusprotsessi korraldus ja osalejate arvamus sisu kohta.

Leedu

Osalejate kirjeldus ja valikuprotsess

CyberPhishi kursuse kvaliteedi hindamiseks viisid projektipartnerid oma riikides läbi pilootkoolituse. Leedus viidi pilootkoolitus läbi, kutsudes kohale Vilniuse Ülikooli Kaunase teaduskonna liikmeid, peamiselt üliõpilasi. Kutsed postitati teaduskonna Facebooki lehele, kodulehele ning õppejõud tutvustasid projekti oma loengutel. Projekti partner Infotehnoloogia Instituut koostas juhendid, töötas välja küsimustikud enne ja pärast koolitust, jälgis kõikide partnerite pilootkoolituse kulgu ning edastas pärast koolitusandmete süstematiseerimist partneritele statistilist teavet.

Osalejate profiil

Pilootkoolitusel osalejad olid vanuses 20-23 aastat ning mehi oli veidi rohkem kui naisi (60% osalejatest olid mehed).

Õpilaste motivatsioon liituda pilootkoolitusega

Õpilasi motiveeris asjaolu, et viimasel ajal sagenenud küberrünnakute ja isikuandmete varguste puhul peavad kõigil olema head teadmised küberturvalisusest. Kõik peaksid mõistma küberhügieeni, andmepüügirünnakute toimimist ja mis on sotsiaalne manipuleerimine. Kõik see suurendab meie endi vastupanuvõimet küberkurjategijate suhtes. Seetõttu olid õpilased innukad Cyberphishi kaugõppekursusega liituma. Kursuse läbinud ja tunnistuse saanud õpilased saavad kursuse tulemuse eest lisapunkti. Kursus oli kohustuslik laboriharjutus infosüsteemide ja küberturvalisuse õppijatele. Õpilasi julgustati mitte ainult tutvuma kursuse materjaliga ja katsetama simulatsioone, vaid ka jälgima süsteemi võimalikke ebatäpsusi ja vigu. Vigade raporteerimise eest said nad ka tasu.

Koolitusprotsessi korraldamine

Leedu pilootkoolitusel osalesid majanduse ja juhtimise, Leedu filoloogia ja edutamise, rahanduse ja raamatupidamise rakendussüsteemide ning infosüsteemide ja küberturvalisuse üliõpilased. Otsustati kutsuda tudengeid väga erinevatelt õppekavadelt, et saada võimalikult palju tagasisidet, hinnates mitte ainult koolitusmaterjali, õpikeskkonna

kasutajasõbralikkust, vaid ka kursuse kvaliteeti. Projektitaotlus nägi ette kutsuda igast partnerriigist vähemalt 24 osalejat. Märkimisväärne on see, et Leedus on pilootkoolitusel osalejate arv olnud oluliselt suurem, praeguseks on CyberPhishi kursusega liitunud üle 90 osaleja, kellest 58 on kursuse läbinud ja neile on väljastatud kursuse läbimise tunnistus.

Osalejate arvamus sisu kohta

CyberPhishi pilootkoolituse peamine eesmärk oli testida ja hinnata nende teadmisi võrgupettuste kohta. On julgustav, et enamik Leedus toimunud pilootkoolitusel osalejaid jäid CyberPhishi kursusega rahule. 43% osalejatest väitis, et CyberPhishi kursusega integreeritud simulatsioonid parandasid nende suutlikkust tuvastada võrgupettuse rünnakuid ja veel 52% märkisid, et nad parandasid palju oma võimet tuvastada võrgupettusi.

40–60% kursuse läbinud osalejatest ütles, et on õppinud palju uusi asju. Osalejad olid järgmiste teemade osas väga optimistlikud. Nad väitsid, et on õppinud palju uut: "Küberrünnakute käsitlemine", "Küberturvalisuse õiguslikud aspektid", "Erinevad andmepüügirünnakute tüübid ja tehnikad" ning "Sotsiaaltehnoloogia moodulid ja manipuleerimine".

CyberPhishi pilootkoolitusel osalejate tagasiside on kinnitanud partnerite ambitsiooni panustada läbi CyberPhishi kursuse küberturvalisuse oskuste arendamisse ja turvalisema ühiskonna kujundamisse.

Eesti

Osalejate kirjeldus ja valikuprotsess

Osalejad läbisid Tartu Ülikoolis kursuse “Turvalise tarkvara disaini põhimõtted”. Pilootkoolitus oli kursuse/aine osa. Osalesid peamiselt Tartu Ülikooli (TÜ) ja Tallinna Tehnikaülikooli (TalTech) ühiselt antava küberturvalisuse õppekava üliõpilased. Lisaks osales piloodil paar Erasmus+ tudengit, kes samuti eelnimetatud ainet läbisid.

Valik: piloot kaasati selle aine osana järgmistel põhjustel:

1. Kuna andmepüügist teatatakse viimasel ajal Eestis turvariskina number 1, peavad tulevased küberjulgeoleku spetsialistid sellest riskist teadlikud olema, olema valmis reageerima ja oskama teistele selle mõjusid õpetada;

2. Osalejate taust on seda tüüpi kursuse piloteerimiseks väga sobiv. Nad on noored spetsialistid nii küberturvalisuse kui informaatika vallas ning oskavad kommenteerida nii kursuse sisu kui ka arendatud tarkvaraplatvormi puudujääke.

3. Kursuse sisu täiendas “Turvalise tarkvara disaini põhimõtted” materjali. Andmepüük on veel üks teist tüüpi rünnak. Seega näitlikustati sarnaseid põhimõtteid (nagu ka teiste turvariskide puhul) läbi pilootloengute, stsenaariumide ja riskide äratundmise.

Osalejate profiil

Pilootkoolitusel osalejate keskmine vanus oli 31 aastat, neist vanim — 47 ja noorim — 22 aastat. Osalenud mehi oli kuus korda rohkem kui naisi (31 meest ja viis naist). Kõik osalejad olid küberturvalisuse programmi 2. semestri 1. aasta magistrandid. Eestlasi ja osalejaid teistest riikidest oli võrdselt (mõlemaid 18 osalejat).

Õpilase motivatsioon liituda pilootkoolitusega

Piloot oli osa ainest “Turvalise tarkvara kujundamise põhimõtted“. Aine lõpphindest võisid õpilased teenida kuni 10 protsenti (olenevalt teadmiste lõputestist).

Koolitusprotsessi korraldamine

Koolitus viidi läbi veebis. Initsialiseerimisloeng peeti 5. mail. Ülejäänu anti iseõppimise ülesandena. Õpilased said küsimusi küsida ja tagasiside e-posti teel või küsida koolituse kohta teiste aine loengute ajal.

Osalejate arvamus sisu kohta

Õpilaste küsitlus pärast pilootkoolitust näitas, et kõik õpilased parandasid oma teadmisi andmepüügist. Teadmiste paranemist täheldati eelkõige küberjulgeoleku juriidiliste aspektide, küberrünnakute käsitlemise, küberturvalisuse maastiku tendentside, andmepüügirünnete tüüpide ja tehnikate, sotsiaalse manipuleerimise ning andmepüügirünnakute äratundmise osas. Kõik osalejad jäid pärast CyberPhishi kursuse läbimist oma teadmistega küberturvalisuse teemadel rahule. Peaaegu kõik õpilased nõustusid, et simulatsioonid aitasid parandada nende oskusi andmepüügi äratundmisel. Kõik osalejad nõustusid kindlalt, et veebipõhine lähenemine sobib kursuse ainega, et kursuse läbimiseks antud aeg on piisav ning nad soovitavad seda kursust ka teistele inimestele. Enamik õpilasi nõustus, et neil

on selge arusaam kursuse eesmärkidest, et kursuse sisu hõlmas kursuse eesmärke ja et toetus kursuse kaudu oli asjakohane.

Malta

Osalejate kirjeldus ja valikuprotsess

Küberandmepüük mõjutab mitmeid valdkondi, mitte ainult infotehnoloogiat. Sellega seoses võeti sihikule erinevate õppekavade üliõpilased. MECB kutsus oma sotsiaalpartnerite kaudu osalema kõrgkoolide (HEI) üliõpilasi. Pilootkoolituses osalesid üliõpilased Malta Kunsti-, Teadus- ja Tehnoloogiakolledžist (MCAST), mis on saare peamine kutsehariduse ja -koolituse (VET) pakkuja, ja Malta ülikoolist (UoM) – Junior College. Lisaks õpilastele keskendus MECB Ltd ka teistele sidusrühmadele, sealhulgas, kuid mitte ainult, eksperdid, poliitikakujundajad ja õpetajad. Neid kutsuti osalema MECB veebisaidi kaudu. Sidusrühmade teadmiste taseme tuvastamiseks enne ja pärast kursust kasutati ka CyberPhishi projekti käigus välja töötatud koolitusmaterjale, stsenaariume, enesehindamist ja teadmiste hindamise teste.

Samuti valiti välja koolitajad ja juhendajad kõrgkoolist ja MECB Ltd-st, et anda CyberPhishi projekti kohta üksikasju ja jälgida pilootkoolitust. Enne pilooti teavitati koolitajaid üldisest CyberPhishi projektist, sealhulgas, kuid mitte ainult, uuringust (IO1), CyberPhishi õppekavast (IO2) ja kursuse materjalist (IO3) ning väljatöötatud stsenaariumidest (IO4). Nii sooviti tõsta projektiteadlikkust ja võimaldada koolitajatel aidata sidusrühmi mis tahes raskustes. Lisaks näidati, kuidas kasutada e-platvormi, enesehindamise ja teadmiste hindamise teste. Enne pilooti toimus ka arutelu ja tutvustati õppemeetodeid, mida saaks kasutada tõhusaks tööks sidusrühmadega. Tutvustava sessiooni käigus anti koolitajatele spetsiaalselt koolitajatele välja töötatud metoodilised juhised ja materjalid ning tutvustati õpilaste juhiseid, mis jagati õpilastele pilootkoolituse alguses.

Osalejate profiil

Pilootkoolitusel osales 43 osalejat. Üle kahe kolmandiku osalejatest olid mehed (71,4%) ja ligi kolmandiku moodustasid naised (28,6%). Enim osalesid töötajad (60,7%), 21,4% üliõpilased ja kümnendik (10,7%) ärimehed. Ülejäänud osalejad märkisid, et nad on füüsilisest isikust ettevõtjad ja muud valikud.

Koolitusprotsessi korraldamine

Kokku toimus Maltal kolm piloodikoolitust järgmiselt:

1) Näost näkku (MCAST-i ärijuhtimise ja kaubanduse instituudi (IBMC) üliõpilased)
2) Internetis (üliõpilased, kes järgivad infotehnoloogia kursusi Junior College UoM-is)
3) Avatud kursus (kutsutakse kõik sidusrühmad, sealhulgas õppijad, eksperdid, poliitikakujundajad ja õpetajad)

Kokku registreerus süsteemi 75 õppijat, kellest 57% (43) lõpetas lõpukursuse täielikult. Neist 67% proovis simulatsioone ja 91% proovis sooritada lõpliku teadmiste testi. Kolmkümmend hindamist proovinud õppijat said 75% ja rohkem koguhindest ehk lõpetasid kursuse positiivse tulemusega.

Osalejate arvamus sisu kohta

Osalejate küsitlus pärast pilootkoolitust näitas, et nad täiendasid oma teadmisi andmepüügist kõigis CyberPhishi kursuse küberturvalisuse teemades. Osalejad märkisid ka, et said andmepüügi kohta palju uusi teadmisi. Kõik osalejad jäid pärast CyberPhishi kursuse läbimist oma teadmistega küberturvalisuse teemadel rahule. Peaaegu kõik õpilased nõustusid, et simulatsioonid aitasid parandada nende oskusi andmepüügi äratundmisel. Suurem osa vastajatest nõustus väidetega või nõustus nendega täielikult:

- kursuse läbimiseks antud aeg oli piisav;
- koolitus ja toetus kogu kursuse jooksul olid asjakohased;
- neil oli selge arusaam kursuse eesmärkidest;
- kursuse sisu hõlmas kursuse eesmärke;
- kursusele sobis veebipõhine õppimisviis;
- nad soovitaksid seda kursust teistele inimestele.

Küpros

Osalejate kirjeldus ja valikuprotsess

Küprose pilootkoolitusel olid sihiks erinevate õppekavade tudengid – nimelt IT-õpingud, Euroopaõpingud, Turundusõpingud ja nii edasi. DOREA on kutsunud pilootkursusel osalema ka organisatsioone (teisi täiskasvanute koolitusasutusi, aga ka ettevõtteid ja nende töötajaid meie võrgustikust).

DOREA tegi avatud üleskutse ja kutsus kõiki huvilisi pilootkursusega liituma, arvestades, et need oskused peavad olema igal inimesel, mitte ainult IT-programmide õppuritel. Kutsed tehti e-posti, telefonikõnede ja silmast-silma kohtumiste teel.

Osalejate profiil

Pilootkoolitusel osales 26 osalejat. Valdav osa osalejatest olid 20. eluaastates üliõpilased (92,3%) ja ülejäänud 7,7% töötajad. Üle kahe kolmandiku osalejatest olid naised (76,9%) ja ligi kolmandiku olid mehed (23,1%).

Koolitusprotsessi korraldamine

Koolitus Küprosel korraldati enamasti veebipõhiselt, koolitaja veebipõhise tagasiside/abiga. Mõnel korral toimusid ka silmast silma konsultatsioonid.

Veebikoolituse puhul sai iga osaleja, kes avaldas huvi osaleda, e-kirja koos juhiste ja sammudega kursusele registreerumiseks. Kõik õpilased kutsuti enne kursusele registreerumist ja pärast kursusel osalemist täitma enesehindamise testi.

Kursuse ajal konsulteeris koolitaja osalejatega e-kirjade, kõnede ning veebi- ja näost-näkku kohtumiste osas (võimaluse korral), juhendades neid, vastates nende küsimustele või pakkudes täiendavaid teabeallikaid.

Enamik osalejaid osales kursusel, kuna oli üldiselt teemast huvitatud ja teised on selgitanud, et nende arvates on saadud tunnistusest tulevikus kasu. 26 osalejast 25 on kursuse täielikult läbinud ja saanud tunnistuse.

Osalejate arvamus sisu kohta

Kõik osalejad märkisid, et on saanud palju uusi teadmisi või täiendanud oma teadmisi kõikides valdkondades. Suurem osa osalejatest on märkinud, et eriti palju uusi teadmisi said nad teemadel „Sotsiaaltehnoloogia“ ja „Andmepüügi rünnakute tüübid ja tehnikad“. Enamik osalejaid on täiendanud oma teadmisi teemadel „Küberturvalisuse juriidilised aspektid“, „Küberintsidentide ennetavad meetmed“ ja „Küberintsidentide käsitlemine“. Vaid üks osaleja oli märkinud, et ta ei saanud õngitsemisrünnakute äratundmisest midagi uut teada.

Suurem osa osalejatest märkis, et on pärast kursuse läbimist rahul oma teadmistega küberturvalisuse teemadel. Väike arv osalejatest (vahemikus 3,8% kuni 11,5%) oli oma teadmisi hinnates neutraalne. See võib viidata sellele, et kuigi nad on uskunud, et nad on saanud palju teadmisi, on veel arenguruumi. Enamik osalejaid on märkinud, et simulatsioonid kas „aitasid tugevalt” või „aitasid” neil õpetatavatest küberteemadest aru saada. Enamikul osalejatest oli kursusel suurepärane kogemus kursuse eesmärkide mõistmise, veebipõhise lähenemisviisi ja sisu sobivaks leidmise, kursuse läbimiseks piisavalt aega jms osas. Üks osaleja märkis, et tema arvates ei sobinud veebipõhine õppimisviis sobivaks. kursuse puhul oli ühel osalejal platvormi raske kasutada ja üks inimene ei soovitaks seda kursust teistele inimestele.

CyberPhishi koolitaja nendib, et kursus on väga informatiivne ja hõlmab kõiki suuremaid teemasid, mis on vajalikud, et õpilased saaksid aru küberjulgeoleku probleemidest, eelkõige andmepüügist, aga ka õppida end kaitsma. Ta rõhutas, et kursus on kindlasti kasulik mitte ainult IT-tudengile oma oskuste ja teadmiste värskendamiseks, vaid ka teiste valdkondade üliõpilastele, töötajatele ja ühiskonnale.

LÄTI

Osalejate kirjeldus ja valikuprotsess

Pilootkoolitus viidi ellu koos partneritega Riia Tehnikaülikooli (RTU) ja Läti Kultuurikolledžiga, mistõttu kutsuti osalema ka nende kõrgkoolide üliõpilased. Altacom korraldas eraldi kohtumised RTU ja LKK üliõpilasomavalitsustega, et tutvustada CyberPhishi projekti ja kavandatavat pilootkoolitust. Pärast kohtumist suunati üliõpilased nende kõrgkooli mitteformaalse hariduse eest vastutava isiku juurde. Partnerid ja kontaktid Läti kultuurikolledžist, saatsid välja kutsed üliõpilastele (enamasti mitte-IT teaduskondadest).

Osalejate profiil

Pilootkoolitusel osales 27 osalejat. Piloodikoolitusel osalejate keskmine vanus oli 23 aastat, neist vanim — 26 ja noorim — 19 aastat vana. Osalenud mehi oli poolteist korda rohkem kui naisi (60% mehi ja 40% naisi). Üldiselt olid osalejad tehnika- ja kultuurivaldkonna tudengid. Enamik osalejaid olid praegu Riias elavad lätlased, kuid on ka Lätis õppivaid vahetusõpilasi erinevatest riikidest.

Õpilaste motivatsioon pilootkoolitusega liituda

Pilootkoolitust tutvustati uue mitteformaalse hariduse lisavahendina, mis aitab õpilastel omandada väärtuslikke teoreetilisi ja praktilisi oskusi küberturvalisuse vallas. Tänapäeval on need oskused väga kasulikud mitte ainult isiklikuks kasutamiseks, vaid ka peaaegu kõigil töökohtadel, kus arvutit kasutatakse. Seetõttu otsustasid mõned kutsutud õpilased, et piloodil osalemine võib neile tõesti kasulik olla, ja nõustusid sellega liituma.

Koolitusprotsessi korraldamine

Põhiinfo pilootkoolituse kohta on antud RTU ja LKK üliõpilasomavalitsustega kohtumisel ning kutses. Lisaks said osalejad oma küsimuste ja tagasisidega otse ühendust võtta e-posti või muude kontaktide kaudu (nt sõnum sotsiaalvõrgustikus).

Õppeplatvormil oli registreerunud 45 osalejat. 25 osalejat läbis teadmiste testi tulemustega üle 75%. Teadmiste testi (läti keeles) sooritas 2 osalejat hindega alla 75%.

Osalejate arvamus sisu kohta

Osalejate küsitlus pärast pilootkoolitust näitas, et nad said palju teadmisi andmepüügist peaaegu kõigis CyberPhishi kursuse küberturvalisuse teemades. Osalejad täiendasid oma teadmisi andmepüügist moodulites "Küberturvalisuse juriidilised aspektid", "Küberturvalisuse tendentsid", "Küberturvalisuse ennetavad tegevused" ja "Küberrünnakute käsitlemine". Enamik osalejaid jäid pärast CyberPhishi kursuse läbimist rahule oma teadmistega küberjulgeoleku teemadel, eriti moodulitega „Küberrünnakud – andmepüük ja sotsiaalsed ründed“ ning „Küberrünnakute mõistmine ja käsitlemine“. Peaaegu kõik õpilased nõustusid, et simulatsioonid aitasid parandada nende oskusi andmepüügi äratundmisel. Enamik vastajatest nõustus väidetega või nõustus nendega täielikult:

- nad soovitaksid seda kursust teistele inimestele,
- koolitus ja toetus kogu kursuse jooksul oli asjakohased;
- veebipõhist õppeplatvormi oli lihtne kasutada;
- kursuse läbimiseks antud aeg oli piisav;
- kursuse sisu hõlmas kursuse eesmärke;
- osalejail oli selge arusaam kursuse eesmärkidest;
- kursusele sobis veebipõhine õppimisviis.

KOKKUVÕTE

Partnerite konsortsium on vajaduste analüüsi põhjal välja töötanud küberjulgeoleku, küberrünnakute, sotsiaalse rünnakute koolituse õppekava, keskendudes eelkõige andmepüügi tuvastamisele ja ennetamisele. Õppekava oli koostatud segaõppeks, kuid selle ülesehitus muudab selle paindlikuks ja seda saab kasutada nii kaugõppeks kui ka silmast silma koolituseks. Täielik koolitusprogramm koosneb 30 tunnist, mis vastab 1 EAP-le.

Õppekava koosneb neljast erinevast osast (moodulist): Küberturvalisuse sissejuhatus; Ülevaade küberturvalisusest EL-is; Küberrünnakud: andmepüük ja sotsiaalsed ründed; Küberrünnakute mõistmise ja nendega toimetuleku ülevaade.

Partnerite konsortsium töötas välja veebipõhise koolitusmaterjali, järgides CyberPhishi õppekava ja vastavalt 4. tööstusrevolutsiooni vajadustele. Projekti käigus lõid partnerid õppematerjali, mis koosneb slaididest, testidest ning linkidest välistele allikatele ja videotele. Sõltumatud eksperdid hindasid väljatöötatud õppematerjali positiivse tagasisidega.

Väljatöötatud õppekavasid, koolitusmaterjale ja õpikeskkonda saab kasutada erinevatele sihtrühmadele, näiteks üliõpilastele, haridustöötajatele, ülikooli töötajatele (kogukonnaliikmetele), täiskasvanute keskustele ja ettevõtlussektorile (tööandjad ja töötajad).

Väljatöötatud e-õppematerjalid, segaõppe keskkond ja simulatsioonid lõimiti osalevates ülikoolides pilootkoolituse käigus õppeainetesse.

Väljatöötatud koolitusmaterjal, simulatsioonid, enesehindamise testid ja teadmiste hindamise testid aitavad arendada osalejate kriitilist mõtlemist ning küberturvalisuse alastes oskustes, mida oma tööpraktikas rakendada. Kursust CyberPhish saab edukalt kasutada ka teistele sihtrühmadele suunatud koolituste korraldamiseks mitte ainult pilootkoolituse käigus osalevates riikides, vaid ka läbi kohandamise teistes Euroopa riikides.

Koolituseelse ja -järgse teadmiste hindamise võrdlemine näitas, et osalejad parandasid oluliselt oma teadmisi küberturvalisusest ja andmepüügist. Andmed näitavad, et osalejate tulemused paranesid oluliselt, st rohkem õpilasi sai hinde 8 või kõrgema tulemuse.

Sada seitsekümmend viis osalejat läbisid (175) koolituse ja said tunnistuse: 36 Eestist, 25 Lätist, 26 Küproselt, 30 Maltalt ja 58 Leedust. Veel 17 osalejat läbisid kursuse ilma tunnistuseta, st nende teadmiste testi tulemus oli alla 75%.

VIITED

1. ENISA (2019): Cybersecurity skills development in the EU. European Union Agency for Security. December, 2019. URL: Cybersecurity Skills Development in the EU — ENISA (europa.eu) (accessed 09/08/2022)
2. Council of the European Union (2021): Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade, 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 (accessed 09/08/2022)
3. Good practices in innovation on Cybersecurity under the NCSS, November 19, 2019
4. IO1 A2: Results "Analysis of Existing Cybersecurity training programmes", 2021, URL:https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A2_EN_CYBERPHISH-REPORT_study-analysis.pdf
5. Proofpoint (2019): Human Factor Report 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor
6. European Union Agency for Cybersecurity (2020): Phishing - ENISA threat landscape 2019-2020
7. IO1 A1 "RECOGNISING PHISHING AND SKILLS GAPS", 2021, URL:https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EN_CYBERPHISH-REPORT_survey-results.pdf
8. Robert B. Cialdini (2006) The Psychology of Persuasion. Harper Business, 336p. ISBN: 978-0061241895
9. NCC group (2020) :Psychology of the Phish: Leveraging the Seven Principles of Influence, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433

LISA 1

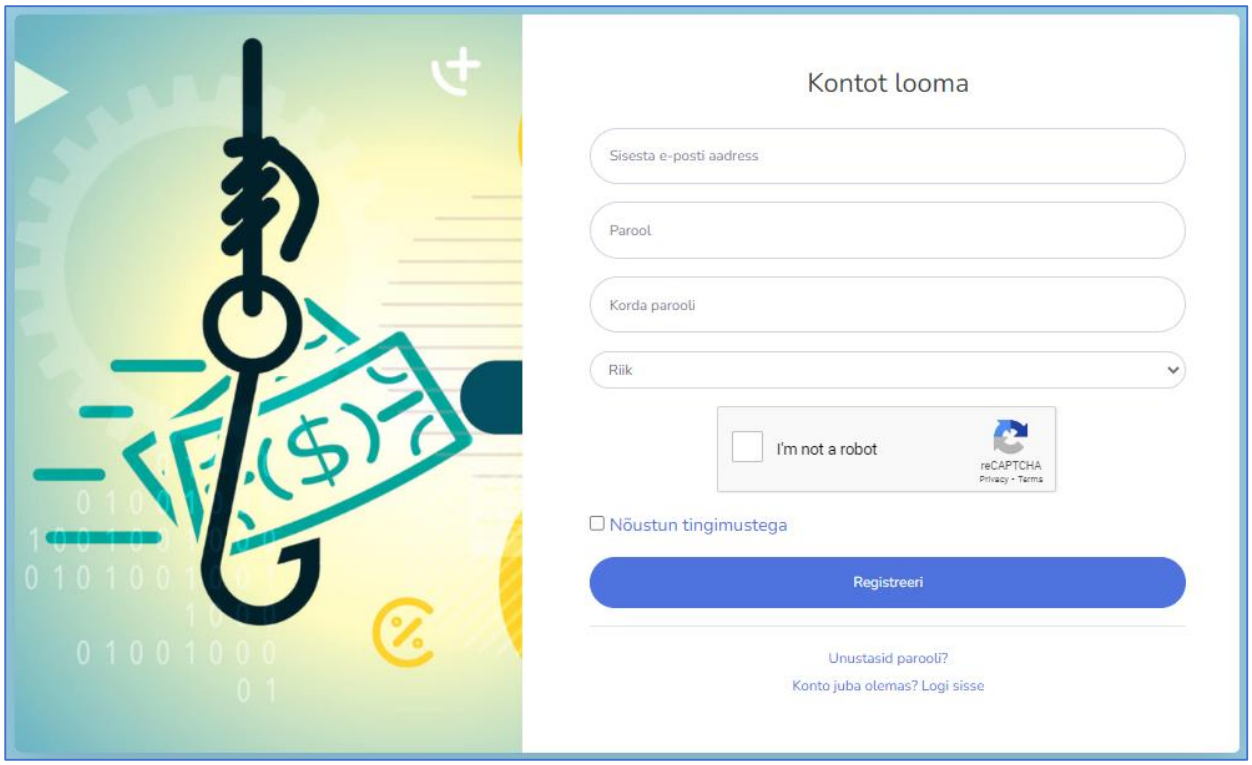
CYBERPHISHI ÕPPEKESKKOND

E-õppekeskkonnas aadressil https://cyberphish.vuknf.lt majutatud õppematerjalid on kõigile külastajatele kättesaadavad ja tasuta. Õppematerjal on saadaval viies keeles: inglise, eesti, kreeka, läti ja leedu keeles. Registreerimata külastajad saavad ainult vaadata õppematerjali, kuid nad ei saa sooritada eneseteste, teadmiste teste, teenida ja koguda märke, teha simulatsioone ega saada sertifikaate. Veebilehe registreeritud külastajaks saamiseks tuleb registreeruda e-mailiga.

Registreerumine e-õppe keskkonda

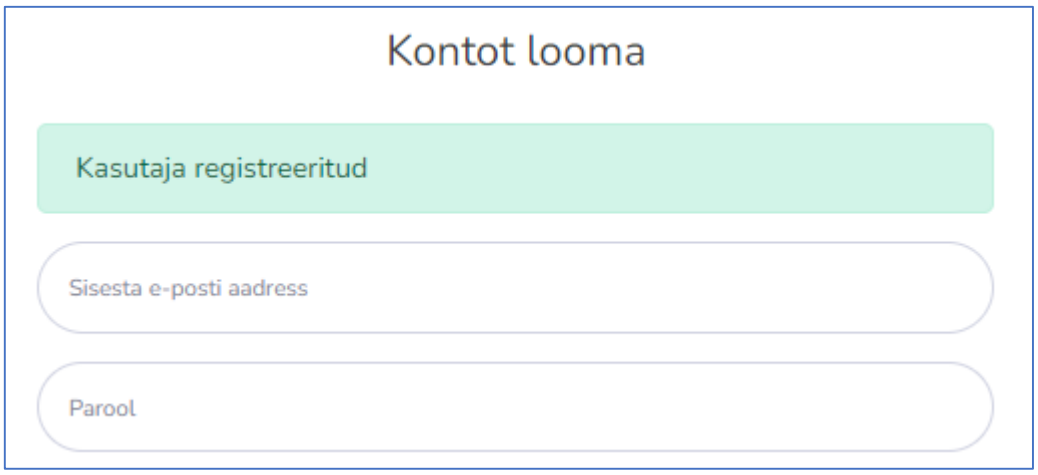
Registreeritud kasutajaks saamiseks looge konto, klõpsates nuppu "Registreeri".

Pärast lehe ülaosas nupul „**Registreeru**“ klõpsamist sisestage oma e-post, parool, korrake oma parooli ja valige oma riik. Samuti peate kinnitama, et te ei ole robot ja nõustute tingimustega ning seejärel klõpsake nuppu „Registreeru“.

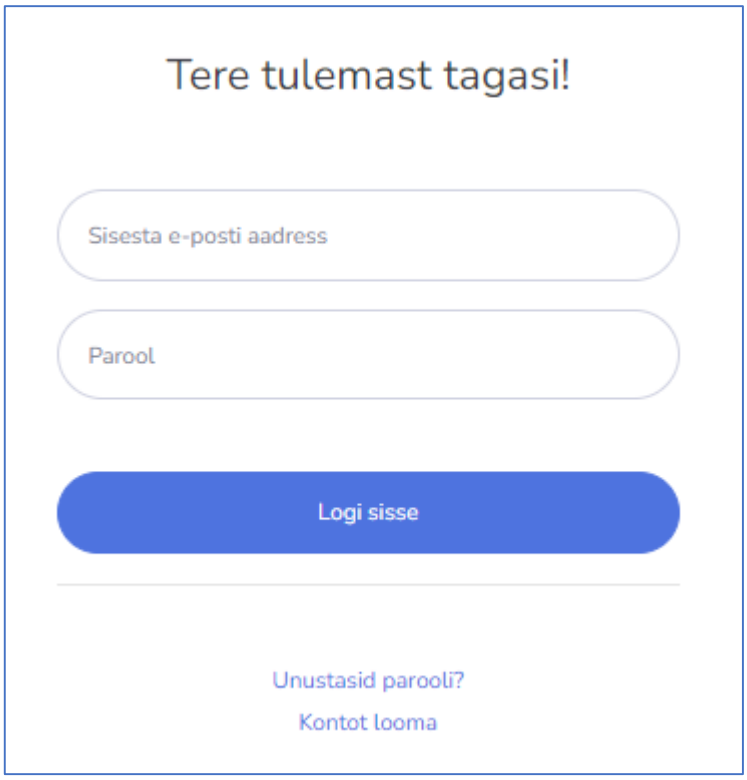


Kui olete registreerunud, saadetakse teile e-posti teel kinnituslink. Klõpsake lingil.

Märkus: Kui üliõpilane ei ole süsteemist kinnituskirja saanud, on vaja kontrollida rämpsposti. Võimalik, et kinnitusmeil satub rämpsposti/rämpsposti kausta.

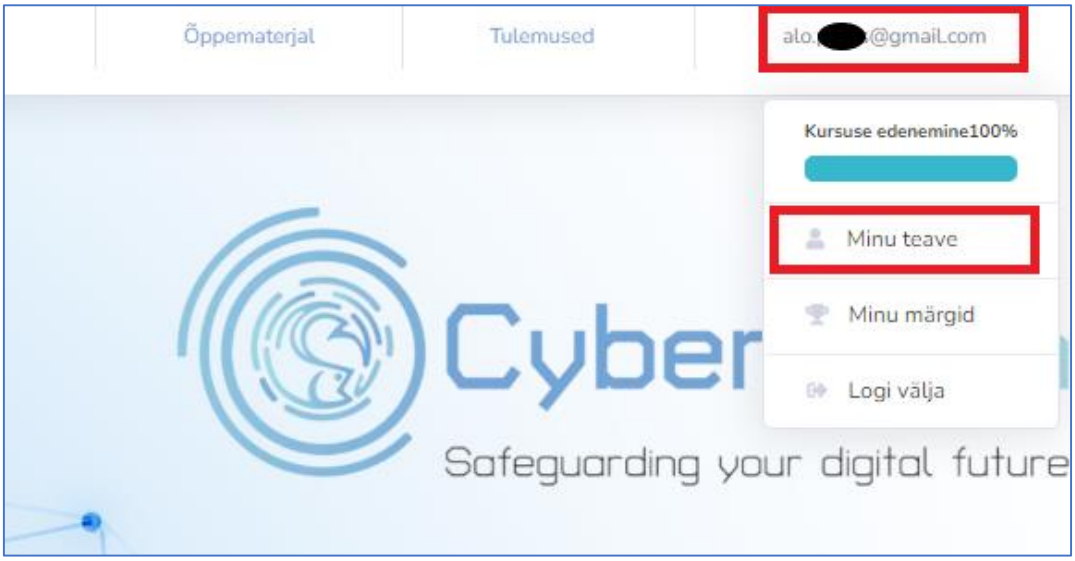


Süsteemi sisselogimiseks klõpsake kinnituslingil.



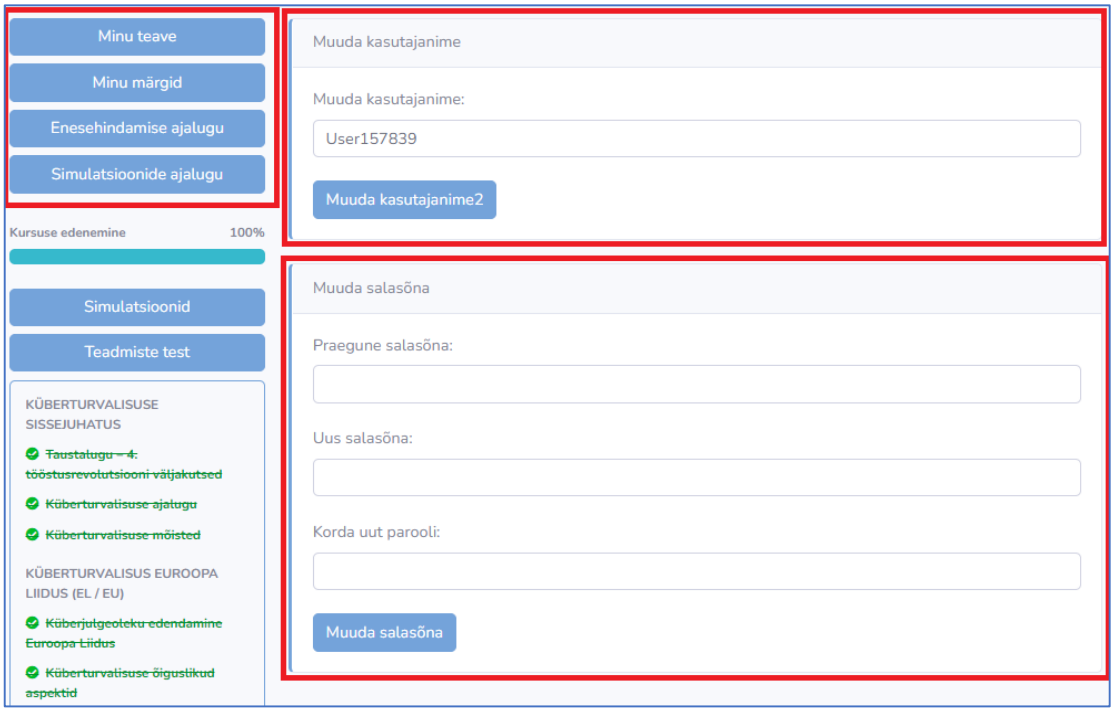
Kasutajakonto

Kui olete sisse loginud, klõpsake lehe ülaosas oma e-posti aadressi ja klõpsake üksust „**Minu teave**“.



Lehe **Minu teave** vasakus servas näete kasutaja põhimenüüd, mis viitab lehele **Minu teave** (teie praegune leht), **Minu märgid, Enesehindamise ajalugu ja Simulatsioonide ajalugu**..

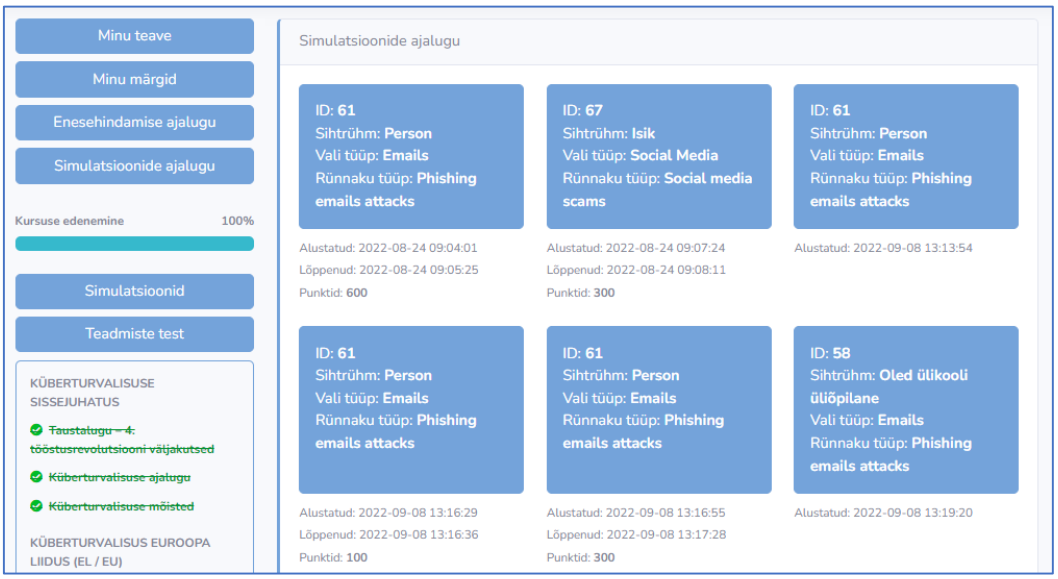
Oma kasutajanime ja parooli saate muuta lehel Minu teave.



Minu märgid lehel näete kõiki märke, mille olete erinevate sooritatud ülesannete jaoks kogunud.

Lehel **Enesehindamise ajalugu** näete kõigi alustatud või lõpetatud enesehinnangu testide ajalugu. Kui enesehinnangu test on puudulik, saate seda teha, klõpsates testi nimel. Kui test on lõpetatud, võite tulemuste nägemiseks sellel klõpsata.

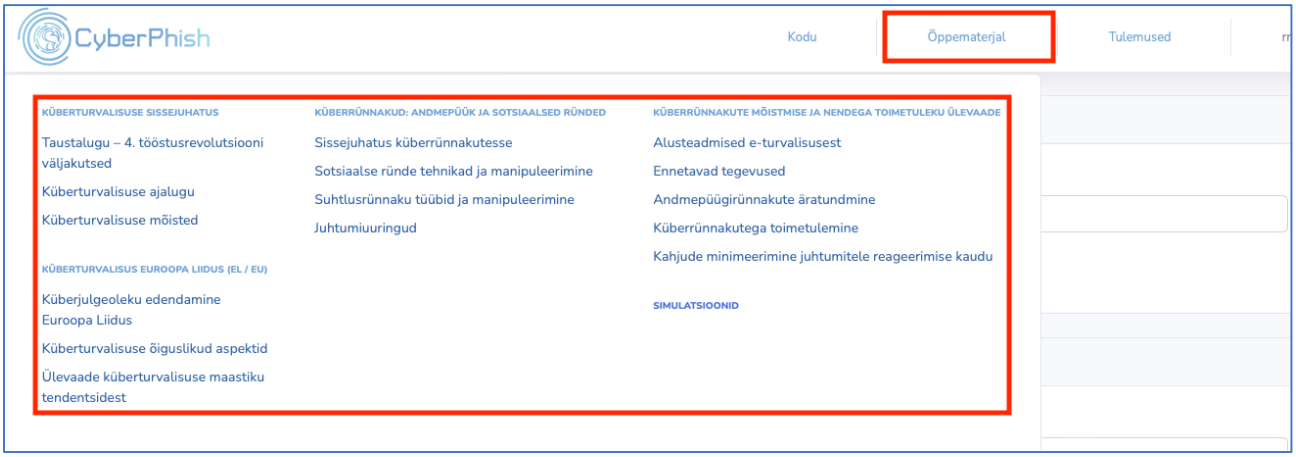
Simulatsioonide ajaloo lehel saate vaadata alustatud või lõpetatud simulatsioonide ajalugu. Kui simulatsioon pole lõpetatud, saate seda teha, klõpsates simulatsiooni nimel. Kui simulatsioon on lõppenud, näete tulemusi sellel klõpsates.



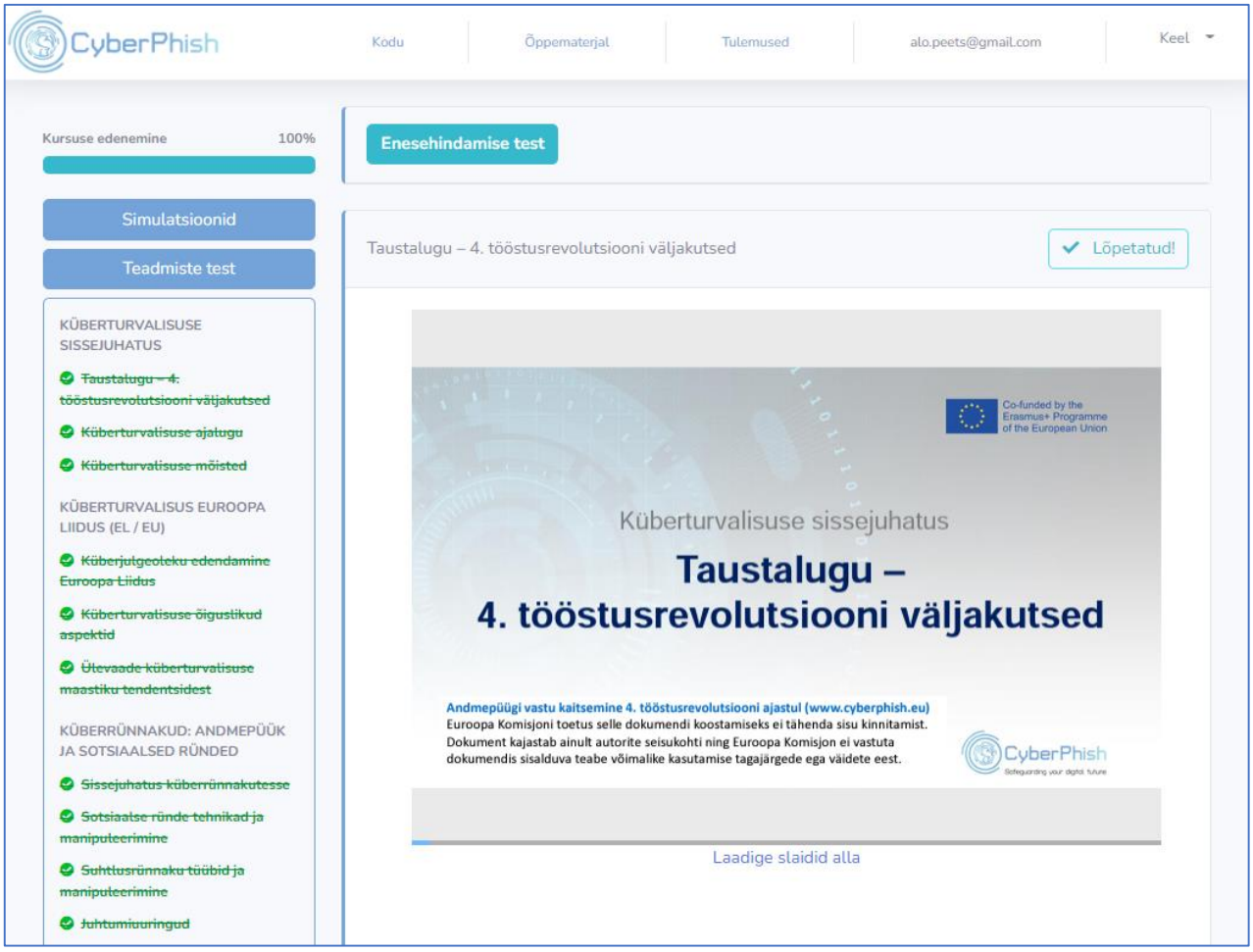
Õppematerjal

Õppematerjalidele pääsete ligi lehe ülaosas, valides menüükäsu **Õppematerjal** ja valides teid huvitava teema*.

*Kõigile toetuvatele materjalidele pääseb juurde ilma registreerimiseta, kuid mõned funktsioonid võivad olla piiratud. Koolitatav saab lugeda koolitusmaterjali ilma süsteemi sisse logimata, kuid ta ei saa kinnitada koolitusmaterjali vaatamise olekut, samuti puudub juurdepääs testidele ja simulatsioonidele.

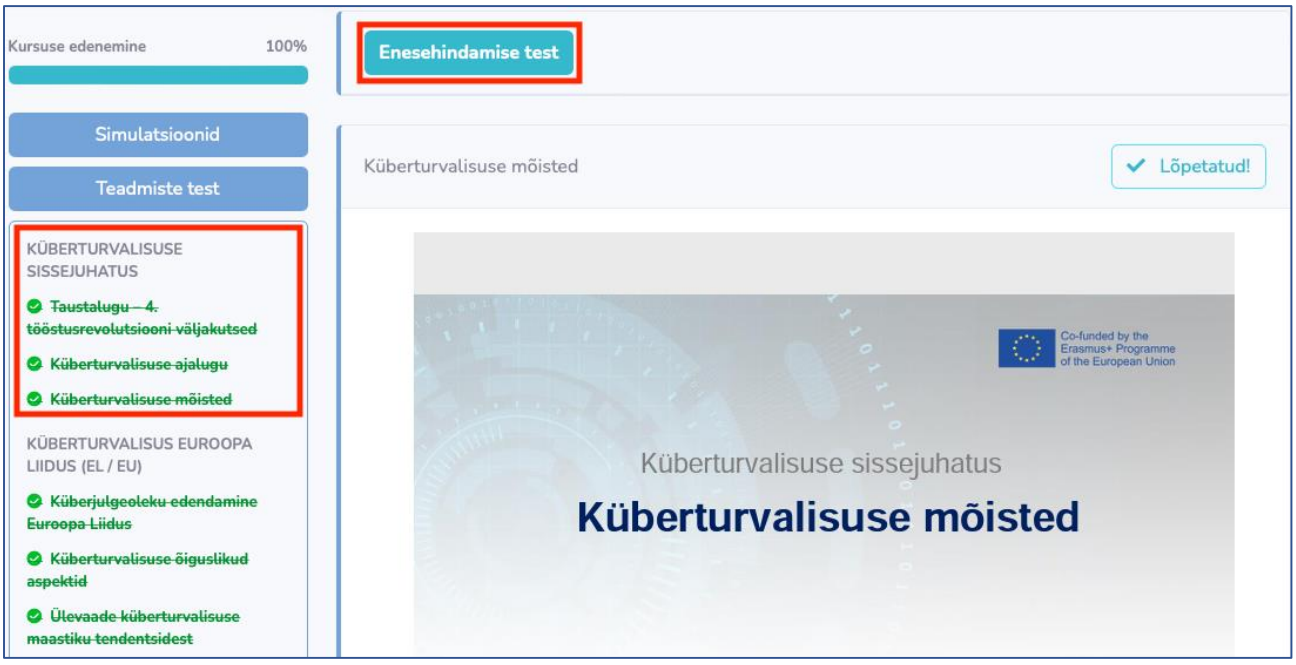


Kui valite mõne teema, näete selle teema slaide lehe põhiosas ja linke kõigile teemadele lehe vasakus servas. Kui olete sisse logitud, saate teemad lõpetatuks märkida, vajutades nuppu Märgi lõpetatuks! lehe ülaosa paremas servas ja vaadake oma kursuse edenemist lehe vasakus servas.

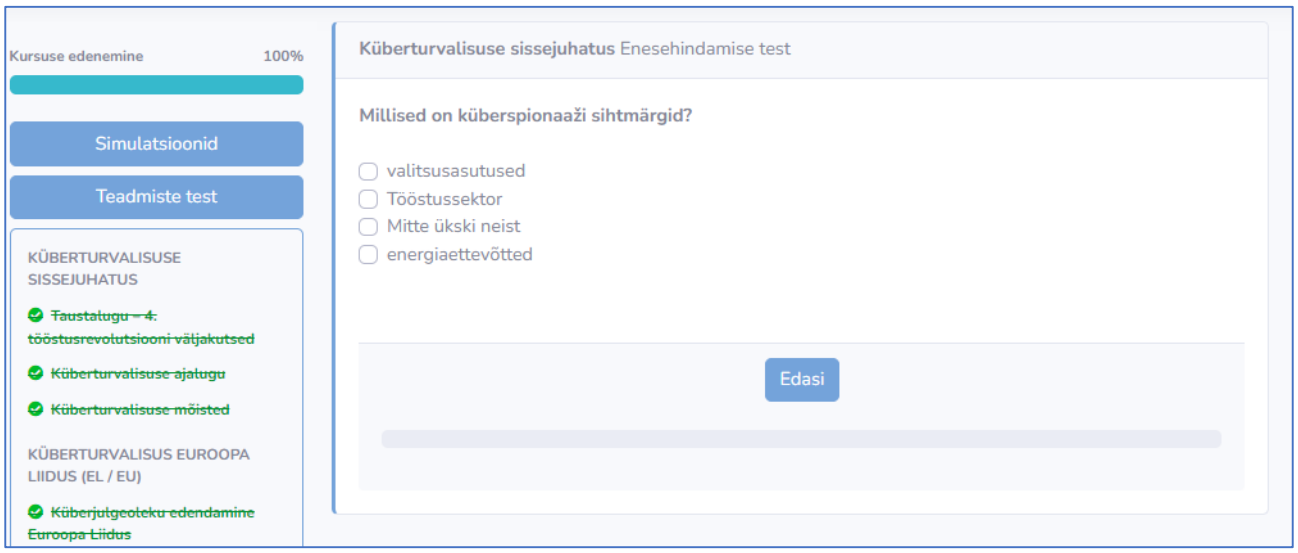


Enesehinnangu test

Enesehinnangu küsimustele juurdepääsuks peate märkima iga teema kategoorias lõpetatuks. Seejärel näete avalehe ülaosas nuppu Enesehindamise test. Enesehinnangu testile pääsemiseks peate olema sisse logitud.



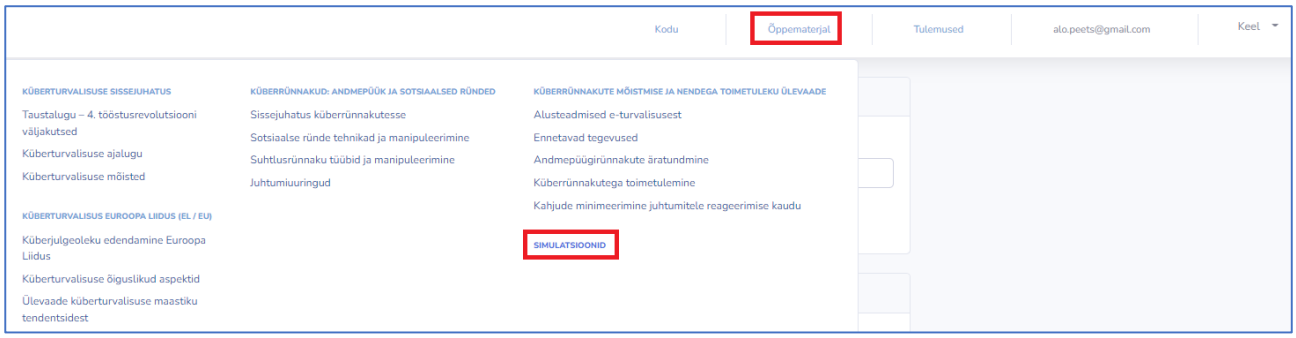
Kui klõpsate nupul Enesehinnangu test, saate selle kategooria kohta 5 küsimust oma teadmiste hindamiseks.



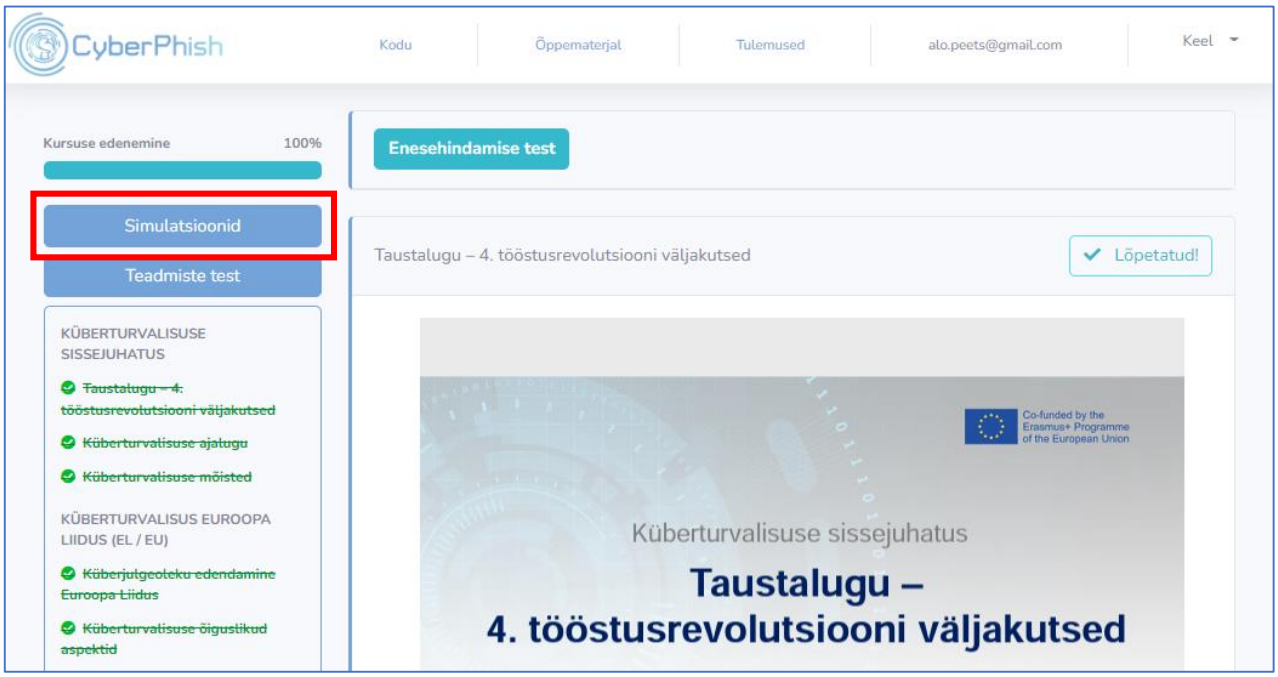
Simulatsioonid

Kasutajad pääsevad simulatsioonidele juurde ainult sisse logides.

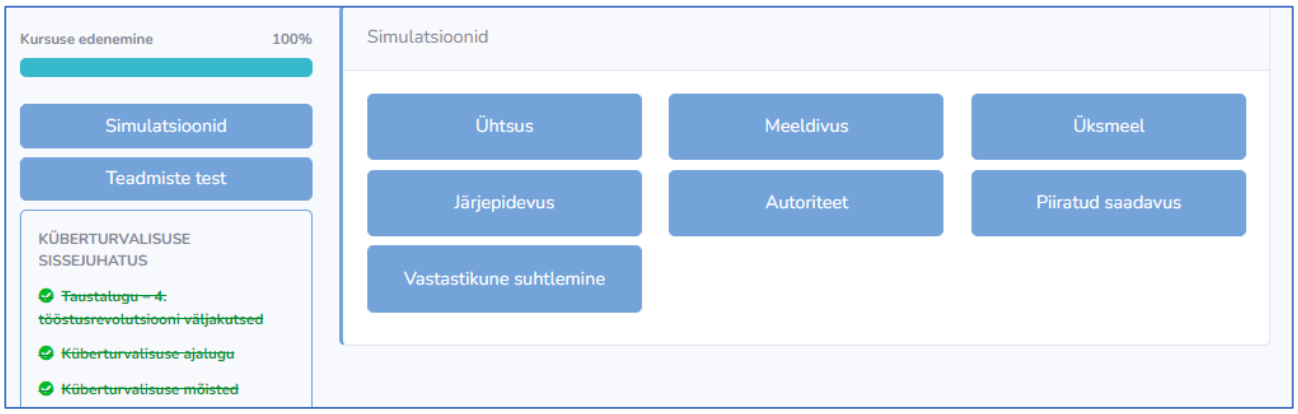
Simulatsioonidele pääsete juurde, klõpsates **õppematerjalil** ja valides **Simulatsioonid**.



Simulatsioonidele pääsete juurde ka mis tahes valitud õppematerjalide teemalehelt.



Kui klõpsate Simulatsioonid, peate valima simulatsioonide kategooria. Üks simulatsioon saab kuuluda mitmesse kategooriasse.



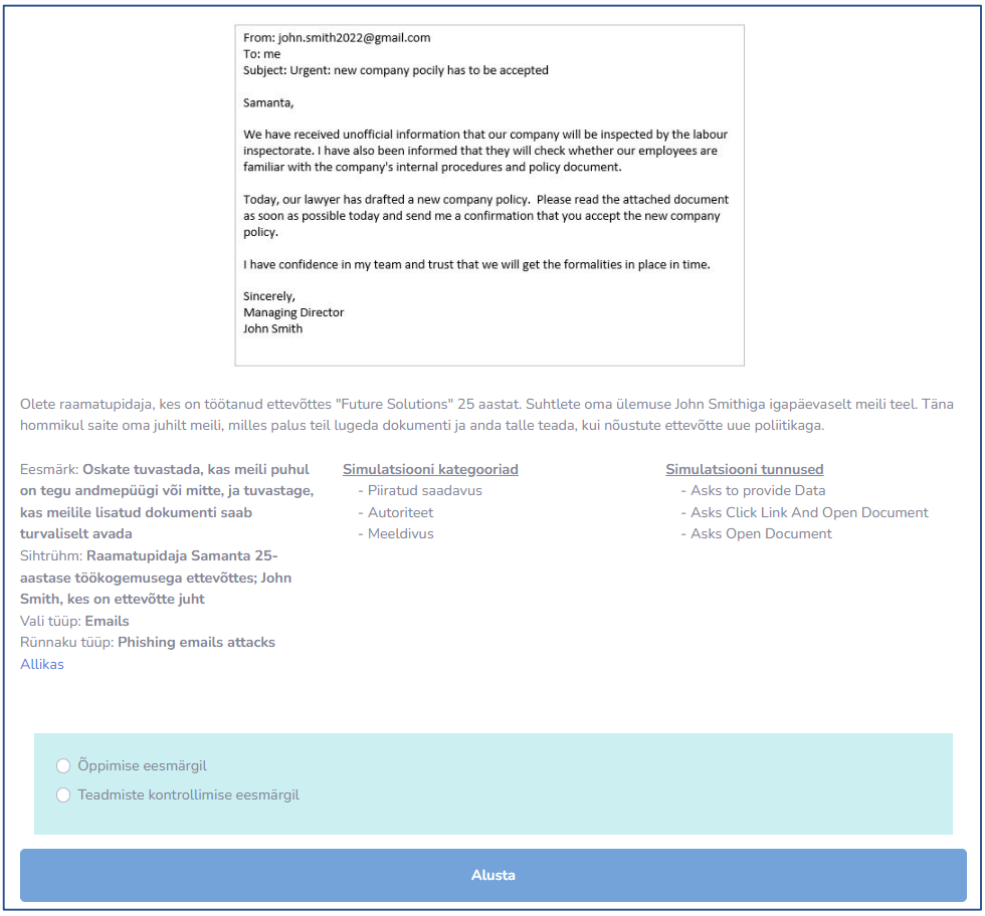
Kui valite kategooria Simulatsioonid, saate valida selle kategooria simulatsioone. Kui olete varem konkreetse simulatsiooni lõpetanud, näete selle simulatsiooni all ajatemplit.

Kui valite mis tahes simulatsiooni, näete enne selle lahendamise alustamist olukorra kirjeldust. Enne alustamist peate valima, kas soovite seda teha õppimise või teadmiste kontrollimise eesmärgil.

Kui valite õppimise eesmärgil, näete tagasisidet pärast iga vastatud küsimust.

Kui valite teadmiste kontrollimise eesmärgil, näete tagasisidet alles pärast simulatsiooni lõpetamist.

Klõpsake nuppu „**Alusta**“.



Kasutajate auastmed

See valik reastab kasutajad nende parimate enesehindamistestide ja simulatsioonide tulemuslikkuse järgi. Kasutajate edetabelitele pääsete juurde, klõpsates lehe ülaosas valikul Auastmed ja valides kas Enesehindamine või Simulatsioonid.