Prevencinės priemonės kovai su fišingu 4-sios pramonės revoliucijos amžiuje (CyberPhish)

A2: Įgyvendinimo gairės

Projekto trukmė: 2020 Lapkritis – 2022 Lapkritis

Projekto 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..

TURINYS

1. ĮVADAS 4
2. KIBERNETINIS SAUGUMAS, SUKČIAVIMAS IR SOCIALINĖ INŽINERIJA 5
2.1 Kibernetinis saugumas ir sukčiavimas studijų programose 5
2.2. Sukčiavimo ir socialinės inžinerijos atpažinimas 5
3. MOKYMO KURSO „CYBERPHISH" PROGRAMA 6
4. KURSO „CYBERPHISH" PILOTINIŲ MOKYMŲ ORGANIZAVIMAS 7
5. PILOTINIŲ MOKYMŲ REZULTATAI 8
Klausimynas prieš pilotinius mokymus 8
Internetinė mokymosi aplinka 11
6. PILOTINIAI MOKYMAI ŠALYSE PARTNERĖSE 26
Lietuva 26
Estija 27
Malta 28
Kipras 29
Latvija 30
Išvados 31
Šaltiniai 32
Priedas 1 33
„CYBERPHISH" MOKYMO(SI) APLINKA 33
Registracija el. mokymosi aplinkoje 33
Vartotojo paskyra 35
Mokomoji medžiaga 37
Savitikros testai 38
Simuliacijos 39
Vartotojo reitingai 42

Paveikslų sąrašas

pav. 1 Pilotinių mokymų dalyvių pasiskirstymas pagal šalis ... 8
pav. 2 Pilotinių mokymų dalyvių žinios prieš mokymus ... 8
pav. 3 Pilotinių mokymų dalyvių žinių, įvertintų balais pasiskirstymas ... 9
pav. 4 Internetinė mokymosi aplinka ... 11
pav. 5 Mokomosios medžiagos pateikimas internetinėje mokymosi aplinkoje ... 11
pav. 6 Sistemos administratoriaus langas ... 12
pav. 7 Vietinio administratoriaus langas ... 12
pav. 8 Kurso dalyvio mokymosi aplinkos langas ... 13
pav. 9 Registruoto kurso dalyvio asmeninės informacijos nustatymo langas ... 13
pav. 10 Registruoto kurso dalyvio savitikros testų istorijos langas ... 14
pav. 11 Registruoto kurso dalyvio simuliacijų istorijos langas ... 14
pav. 12 Ženklelių pavyzdžiai ... 15
pav. 13 Registruotų kurso dalyvių reitingai ... 15
pav. 14 Kurso dalyvio aplinkos savitikros testo mygtukas ... 17
pav. 15 Savitikros testo fragmentas ... 17
pav. 16 Simuliacijos modelis sudarytas sprendimų medžio principu ... 18
pav. 17 Simuliacijų kategorijos ... 18
pav. 18 Simuliacijų pasirinkimas kategorijoje „Liking" ... 18
pav. 19 Simuliacijos sprendimo pavyzdys ... 19
pav. 20 Simuliacijos sprendimas ... 19
pav. 21 Simuliacijos sprendimo metu vartotojui pateikiamas grįžtamasis ryšys ekrane ... 20
pav. 22 Pabaigtos spręsti simuliacijos langas ... 20
pav. 23 Žinių patikrinimo testo klausimo pavyzdys ... 20
pav. 24 Žinių vertinimo testo gautų rezultatų lango pavyzdys ... 21
pav. 25 Savitikros testo klausimo pavyzdys ... 22
pav. 26 Savitikros testo rezultatų pavyzdys ... 22
pav. 27 Žinių patikrinimo testo pradinis langas ... 23
pav. 28 Žinių patikrinimo testo klausimo pavyzdys ... 24
pav. 29 Išlaikyto žinių patikrinimo testo langas ... 24
pav. 30 Sertifikato formavimo langas ... 25
pav. 31 Mokymus užbaigusių dalyvių statistika ... 25
pav. 32 Dalyvių žinios apie kibernetinį saugumą ir sukčiavimą prieš pilotinius mokymus ir po jų ... 26

Lentelių sąrašas

lentelė 1. Penki lengviausi klausimyno prieš mokymus klausimai ... 10
lentelė 2. Penki sudėtingiausi klausimyno prieš klausimai ... 11
lentelė 3. Mokymo medžiagos santrauka ... 16
lentelė 4. Savitikros testų klausimų specifikacija ... 21
lentelė 5. Žinių patikrinimo testų klausimų specifikacija ... 23

1. ĮVADAS

Ketvirtosios pramonės revoliucijos amžiuje kibernetinis saugumas tampa vienu iš didžiausių iššūkių. Plačiai paplitęs skaitmeninių įrenginių ir informacinių sistemų naudojimas tampa vis patrauklesnis kibernetiniams nusikaltėliams. Eurostato duomenimis, „...2019 m. maždaug kas trečias 16-74 metų amžiaus ES pilietis per pastaruosius 12 mėnesių pranešė apie su saugumu susijusius incidentus, kai 2019 m. asmeniniais tikslais naudojosi internetu. Per šį laikotarpį 2019 m. dažniausias su saugumu susijęs incidentas, apie kurį pranešta, buvo sukčiavimas (*angl*. phishing)". Praktiškai jokia informacinė sistema ar saugumo programinė įranga negali užtikrinti 100 proc. apsaugos nuo sukčiavimo atakų. Kova su šiomis grėsmėmis susijusi ne tik su aparatinės ir programinės įrangos saugumo sprendimais, bet ir su naudotojų atsparumu tokioms grėsmėms ir gebėjimu jas atpažinti.

Kibernetinės atakos taip pat nukreiptos prieš Europos įmones. 2017 m. pasaulinės informacijos saugumo būklės tyrimo duomenimis, apie 80 proc. Europos įmonių patyrė bent vieną kibernetinio saugumo incidentą, o 27 proc. visų kibernetinio saugumo incidentų sukėlė darbuotojai.

Taigi tik žmogus - naudotojas, kuris supranta, kaip veikia kibernetiniai nusikaltėliai, ir moka atpažinti įspėjamuosius kenkėjiškos veiklos požymius, gali padėti užkirsti kelią kibernetinėms atakoms, pvz., sukčiavimui.

ENISA[1] duomenimis, su kibernetine sritimi susiję dalykai yra nepakankamai atstovaujami tarp netechninių programų studentų. Todėl aktualu parengti ir visuomenei pasiūlyti plačiai prieinamą internetinį mokymo kursą apie tai, kaip atpažinti sukčiavimą (*angl*. phishing).

Dėl šių priežasčių buvo inicijuotas ir įgyvendintas tarptautinis projektas „Prevencinės priemonės kovai su fišingu 4-sios pramonės revoliucijos amžiuje" (CyberPhish). Projektą finansavo Europos Sąjunga pagal programą „Erasmus+". Projekto koordinatorius Vilniaus universiteto Kauno fakultetas. Projekto partneriai: Tartu universitetas (Estija), Dorea švietimo centras (Kipras), MECB (Malta), Altacom (Latvija) ir Informacinių technologijų institutas (Lietuva). Projekto trukmė: nuo 2020 m. lapkričio mėn. iki 2022 m. lapkričio mėn.

Pagrindinis projekto „CyberPhish" tikslas – edukuoti aukštųjų mokyklų studentus, dėstytojus, universitetų darbuotojus (bendruomenės narius), švietimo centrus ir verslo sektorių (darbdavius ir darbuotojus) bei skatinti tikslinės grupės kritinį mąstymą kibernetinio saugumo srityje.

Projekto „CyberPhish" uždaviniai – parengti mokymo programą, el. mokymosi medžiagą, mišrią mokymosi aplinką, simuliacijas, savitikros ir žinių įvertinimo testus. Sukurtas „CyberPhish" kursas leidžia naudotojams apsisaugoti nuo sukčiavimo atakų. Vartotojai įgyja kompetencijų, kurios padės jiems atkreipti dėmesį į grėsmes ir imtis būtinų prevencijos priemonių.

Projekto metu sukurtas intelektinis produktas – mokymo(si) kursas, skirtas vartotojų kritiniam mąstymui ir įgūdžiams lavinti atpažįstant sukčiavimo atvejus internete. Vartotojai mokomi kibernetinio saugumo įgūdžių, pagrindinių sukčiavimo požymių atpažinimo, supažindinami su socialinės inžinerijos metodais. Taikant mišraus mokymosi metodą ir (arba) koncepciją, naudotojai gali pasirengti žinių patikrinimo testui ir gauti baigimo pažymėjimą.

Projekto partneriai, vykdydami pilotinius mokymus penkiose šalyse partnerėse, naudojo internetinę mokymosi platformą, apimančią mokymo(si) medžiagą, simuliacijas, savitikros testus ir žinių patikrinimo testus. Remiantis šia patirtimi buvo parengtos šios gairės.

Gairių tikslas

Šiose gairėse siekiama pristatyti projekto rezultatus, geriausią pilotinių mokymų praktiką ir metodiką, kaip parengti „CyberPhish" mokymo kursą tikslinei auditorijai ir suinteresuotosioms šalims. Gairės skirtos organizacijoms, suinteresuotoms pritaikyti ir naudoti parengtą el. medžiagą interneto naudotojams mokyti atpažinti sukčiavimo atvejus: aukštojo mokslo įstaigoms, suaugusiųjų švietimo ir (arba) mokymo centrams, verslo sektoriui.

Gairių uždaviniai

Pagrindinis „CyberPhish" įgyvendinimo gairių uždavinys – pristatyti mokymo priemones, turinį ir organizavimo procesą. Šio proceso metu dalyviai įgyja žinių ir įgūdžių, reikalingų atpažinti sukčiavimo atakas darbe ir asmeniniame gyvenime, bei pasiruošia žinių patikrinimui. Sėkmingai baigę mokymus gaus pažymėjimą. Įgyvendinimo procesas grindžiamas dalyvaujančių šalių partnerių patirtimi.

[1] ENISA - Europos Sąjungos tinklų ir informacijos apsaugos agentūra https://www.enisa.europa.eu/

2. KIBERNETINIS SAUGUMAS, SUKČIAVIMAS IR SOCIALINĖ INŽINERIJA

2.1 Kibernetinis saugumas ir sukčiavimas studijų programose

Nuo 2013 m. Europos Komisija vis labiau pabrėžia kibernetinio saugumo svarbą. Pirmojoje kibernetinio saugumo strategijoje informuotumo didinimas ir įgūdžių ugdymas išskiriami kaip pagrindiniai strateginiai tikslai. 2017 m. ENISA ataskaitoje taip pat išskiriama kibernetinio saugumo svarba. Ataskaitoje rekomenduojama ES valstybėms narėms stiprinti švietimą ir įgūdžius kibernetinio saugumo srityje (ENISA, 2019, p. 23). Todėl visos ES valstybės narės parengė ir paskelbė savo nacionalines kibernetinio saugumo strategijas (NKSS).

2021 m. kovo mėn. Europos Vadovų Taryba priėmė naujas išvadas dėl ES kibernetinio saugumo strategijos[2]. Išvadose pripažįstama, kad trūksta skaitmeninių ir kibernetinio saugumo įgūdžių, ir pabrėžiama, kad reikia patenkinti rinkos paklausą toliau plėtojant švietimo ir mokymo programas.

Vykdant projektą „CyberPhish" apžvelgtos šalyse partnerėse – Estijoje, Latvijoje, Lietuvoje, Kipre ir Maltoje – galiojančios mokymo programos ir mokymo planai kibernetinio saugumo ir sukčiavimo klausimais. Tyrimui vadovavo DOREA švietimo institutas. Pagrindinės tyrimo išvados:

- Visose projekto šalyse partnerėse, išskyrus Estiją, aukštojo mokslo studijų programų analizė neapima sukčiavimo ir socialinės inžinerijos temų kaip atskirų modulių. Tačiau informacija šiomis temomis gali būti įtraukta į kitus kurso modulius. Dvi Estijos aukštojo mokslo studijų programos apima studijų modulius, orientuotus į socialinę inžineriją. Vidutinė tokių modulių trukmė yra 4,5 ECTS.
- Analizuojamos aukštojo mokslo studijų programos Estijoje, Latvijoje ir Maltoje apima „minkštųjų įgūdžių" kursus, tokius kaip bendravimo įgūdžiai, verslumas, psichologija ir kt. Priešingai, Kipro ir Lietuvos aukštojo mokslo studijų programos daugiausia orientuotos į „kietuosius įgūdžius", mažiau akcentuojant „minkštųjų įgūdžių" svarbą.
- Visose šalyse partnerėse yra keletas viešųjų ir privačių organizacijų, siūlančių kibernetinio saugumo mokymo kursus, skirtus kibernetinio saugumo ir IT specialistams, įmonėms, darbuotojams ir plačiajai visuomenei. Trumpesnės trukmės mokymų kursuose daugiausia dėmesio skiriama tik įvairių rūšių grėsmėms, įskaitant sukčiavimą, socialinę inžineriją ir apsisaugojimo būdus, tačiau ilgesnės trukmės mokymų kursai suteikia platesnę kibernetinio saugumo perspektyvą. Taip pat yra keletas organizacijų, siūlančių įsiskverbimo (*angl*. penetration) ir socialinės inžinerijos testus, skirtus įmonėms ir jų darbuotojams.

Apklausos metu surinkti duomenys padėjo nustatyti įgūdžių trūkumus ir parengti rekomendacijas naujai mokymo programai „CyberPhish". Šia programa siekiama pagerinti interneto naudotojų įgūdžius ir informuotumą bei supažindinti juos su naujausiomis kibernetinio saugumo problemomis ir grėsmėmis, visų pirma sukčiavimu (*angl*. phishing).

2.2. Sukčiavimo ir socialinės inžinerijos atpažinimas

Kibernetinis saugumas taip pat yra Europos įmonių problema. Įmonės vis dažniau tampa kibernetinių atakų taikiniais. Nusikaltėliams tobulėjant, kibernetines atakas darosi vis sunkiau aptikti ir užkirsti joms kelią, o tokioms atakoms vykdyti naudojami nauji metodai ir platformos. 2017 m. pasaulinės informacijos saugumo būklės apklausos duomenimis, maždaug 80 % Europos įmonių tais metais patyrė bent vieną kibernetinio saugumo incidentą. Apklausos duomenimis, 27 % visų kibernetinio saugumo incidentų sukelia darbuotojai. Vien 2019 m. pirmąjį ketvirtį bendrovės visame pasaulyje 120 %. dažniau nei 2018 m. susidūrė su kibernetinėmis atakomis ir patyrė didžiulius nuostolius (22,2 mlrd. eurų).

Kaip teigiama „Human Factor Report 2019" ataskaitoje, daugiau nei 99 % el. laiškų, kuriuose platinamos kenkėjiškos programos, reikalauja žmogaus įsikišimo, t. y. nuorodų spustelėjimo, dokumentų atidarymo, saugumo įspėjimų priėmimo ir kitų veiksmų [5]. Todėl labai svarbu ugdyti ir didinti informuotumą šioje srityje. Kyla poreikis paaiškinti ir (arba) išmokyti, kaip atpažinti sukčiavimą daugeliui žmonių suprantamu ir prieinamu būdu. Žinodami požymius,

[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 09/09/2022)

įspėjamuosius ženklus ir suprasdami nusikaltėlių metodus, interneto naudotojai, pirma, galės labiau pasitikėti savimi ir jaustis saugūs, antra, galės užkirsti kelią tokioms atakoms arba bent jau sulėtinti jų plitimą.

Sukčiavimas (*angl*. phishing) yra neteisėtas būdas išvilioti naudotojo asmeninius duomenis (prisijungimo duomenis, kredito kortelių informaciją ir pan.) naudojant socialinės inžinerijos metodus. Nusikaltėliai aktyviai naudojasi socialiniais tinklais, siunčia el. laiškus ir skambina telefonu. Šiais pranešimais siekiama įtikinti naudotoją atidaryti kenkėjišką priedą arba spustelėti suklastotą interneto nuorodą ir atskleisti savo slaptažodį [6].

Dažniausiai pasitaikantys sukčiavimo tipai: „Spray and pray", „Cat phishing", „Advanced fee scam", „Spear fishing", „Whaling", „Vishing", „Smishing", „Angler Phishing", „Clone Phishing" ir „Malvertising".

Informacijos saugumo kontekste socialinė inžinerija apibrėžiama kaip psichologinis manipuliavimas žmonėmis, kad jie atliktų veiksmus arba atskleistų konfidencialią informaciją. ENISA teigia, kad socialinė inžinerija tebėra didžiausia grėsmė, palengvinanti kitų rūšių kibernetinius nusikaltimus, nes 84 % kibernetinių atakų remiasi socialine inžinerija. Sukčiavimo aukų skaičius ir toliau auga, nes naudojamasi žmogiškuoju aspektu, kuris yra silpniausia grandis [6].

Socialinės inžinerijos metodai remiasi tokiomis žmogaus silpnybėmis kaip godumas, baimė, smalsumas, pasitikėjimas, empatija ir skubėjimas. Todėl kruopščiai parengtas ir suasmenintas el. laiškas, balso paštas, telefono skambutis ar tekstinė žinutė gali paveikti žmones, kad jie atskleistų savo konfidencialią informaciją, spustelėtų kenkėjišką nuorodą, atsisiųstų ir atidarytų failą su kenkėjiška programine įranga ar net pervestų pinigus nusikaltėliui.

Dr. Robert B. Cialdini savo knygoje „Influence: The Psychology of Persuasion" aprašė šešis įtikinimo principus, kurie buvo lengvai perimti ir naudojami socialinėje inžinerijoje ir sukčiavime. Vėliau jie buvo išplėsti iki septynių: skola / dėkingumas, nuoseklumas, valdžia/ autoritetas, simpatija, sutarimas, trūkumas, vieningumas. Tokiais metodais besinaudojantys sukčiai gali tikėtis sėkmingų atakų rezultatų. Todėl ypač svarbu šviesti žmones, kad jie žinotų, kaip atpažinti tokius išpuolius ir jų išvengti [7; 8; 9].

Projekto partneriai atliko apklausą, siekdami išsiaiškinti, kaip žmonės atpažįsta sukčiavimo atakas, išsiaiškinti žmonių žinias apie sukčiavimą ir skirtingus sukčiavimo tipus bei nustatyti kokių įgūdžių trūksta Kipre, Estijoje, Latvijoje, Lietuvoje ir Maltoje. Su tyrimo rezultatais galima susipažinti tyrimo ataskaitoje „Sukčiavimo atpažinimas ir įgūdžių spragos" [7].

Apklausoje dalyvavo 514 žmonių, iš kurių 259 buvo moterys, 248 vyrai ir 7 žmonės pageidavo nenurodyti savo lyties. Daugiausia respondentų buvo studentai (304), toliau seka darbuotojai (139), įmonių savininkai (53), bedarbiai (10) ir savarankiškai dirbantys asmenys (8). Dauguma apklausos respondentų turėjo aukštąjį išsilavinimą: dauguma respondentų (38 %) turėjo bakalauro laipsnį, toliau seka magistro laipsnis (23 %) ir daktaro laipsnis (6 %).

Įdomu tai, kad beveik kas penktas respondentas nurodė praeityje tapęs sukčiavimo atakos auka. Dažniausiai sukčiavimo atakos įvykdavo paspaudus nuorodas el. laiškuose ar žinutėse, atidarius priedus ar atsakant į el. laiškus ir pateikiant konfidencialius duomenis. Dažniausios šių išpuolių priežastys buvo išsiblaškymas, smalsumas arba skubėjimas. Dauguma respondentų (74 %) nėra dalyvavę jokiuose kibernetinio saugumo mokymuose ar seminaruose. Daugiau nei pusė respondentų (54 %) nurodė, kad šia sritimi susidomėjo savarankiškai. Visa tai rodo, kad žinių apie sukčiavimą ir kibernetinį saugumą poreikis auga.

3. MOKYMO KURSO „CYBERPHISH" PROGRAMA

Remdamasis poreikių analize, partnerių konsorciumas parengė mokymo programą apie kibernetinį saugumą, kibernetines atakas, socialinę inžineriją, ypač daug dėmesio skiriant sukčiavimo atpažinimui ir prevencijai.

Mokymo programos tikslas – supažindinti su kibernetiniu saugumu, daugiausia dėmesio skiriant sukčiavimo atakoms. Kurso programa skirta asmenims, studentams, verslininkams, organizacijų darbuotojams ir padės pasirengti ketvirtosios pramonės revoliucijos amžiaus saugumo grėsmėms. Kurso metu besimokantieji įgis įgūdžių, kaip atpažinti ir valdyti kibernetines atakas bei apsaugoti turimus skaitmeninius įrenginius ir asmens duomenis.

Mokymo programa sukurta mišriam mokymuisi, tačiau dėl savo struktūros ji yra lanksti ir gali būti naudojama tiek nuotoliniam, tiek tiesioginiam mokymui. Visą mokymo programą sudaro 30 valandų, atitinkančių 1 ECTS. Siūloma, kad toks pat valandų skaičius kiekvienam moduliui būtų skirtas savarankiškam mokymuisi ir žinių įsivertinimui.

Mokymo programą sudaro keturios atskiros dalys (moduliai):

1. Kibernetinio saugumo įvadas;
2. Kibernetinė sauga Europos Sąjungoje (ES);
3. Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (*angl*. phishing);
4. Kibernetinių atakų atpažinimas ir apsauga.

Visą mokymo programą galima rasti „CyberPhish" svetainėje adresu: https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A2_Extended-version-of-curricula_LT.pdf

4. KURSO „CYBERPHISH" PILOTINIŲ MOKYMŲ ORGANIZAVIMAS

Pilotinių mokymų tikslas – išmokyti dalyvius atpažinti sukčiavimo atakas, suprasti socialinę inžineriją, įgyti naujų ir patobulinti turimus įgūdžius. Paraiškoje nurodyta, kad projekto metu sukurti produktai turi būti išbandyti, kad būtų galima įvertinti rezultatus ir prireikus juos pakoreguoti atsižvelgiant į dalyvių ir mokytojų (mentorių) pastabas ir atsiliepimus.

Pilotinių mokymų dalyviai. Pilotiniai mokymai vyko visose projekto partnerių šalyse: Kipre, Estijoje, Latvijoje, Lietuvoje ir Maltoje. Dalyvavo:

- aukštųjų mokyklų studentai,
- aukštųjų mokyklų ir organizacijų darbuotojai,
- suaugusiųjų švietimo centrų mokytojai ir darbuotojai.

Kiekviena organizacija partnerė savo šalyje apmokė mažiausiai 24 dalyvius, taip išplėsdama projekto poveikį už savo organizacijos ribų.

Trukmė. Partnerių susitarimu pilotiniai mokymai truko kelis mėnesius (gegužės-rugsėjo mėn.), atsižvelgiant į kiekvieno partnerio vasaros atostogas. Kai kurie partneriai galėjo surengti pilotinius mokymus mokslo metų pabaigoje, t. y. gegužės mėnesį, baigiantis pavasario semestrui. Kiti partneriai galėjo pradėti nuo mokslo metų pradžios, rugsėjo mėn. ir pilotinių mokymų dalyvius surinkti iki rugsėjo pabaigos.

Būdas. Pilotiniai mokymai gali būti vykdomi kaip mišrus mokymosi kursas arba, atsižvelgiant į Covid-19 pandemijos apribojimus, gali vykti nuotoliniu būdu.

Vilniaus universitetas ir Tartu universitetas pilotinius mokymus vykdė savo organizacijose, integruodami „CyberPhish" kursą į mokomuosius dalykus. Kiti partneriai – Altacom, Dorea ir MECB – pilotinius mokymus vykdė bendradarbiaudami su kitomis aukštosiomis mokyklomis arba kviesdami į mokymus dalyvius iš išorės.

Mokymosi platforma. Projekto metu sukurta internetinė mokymosi platforma https://cyberphish.vuknf.lt buvo testuojama penkiomis kalbomis, t. y. anglų, estų, graikų, latvių ir lietuvių. Dalyviai turėjo susipažinti su parengta mokymo medžiaga, atlikti savitikros testus po kiekvienos modulio temos, spręsti simuliacijas ir laikyti galutinį žinių patikrinimo testą.

Pilotinių mokymų organizavimas

Prieš pilotinius mokymus penkių šalių partneriai susitarė, jog organizuodami mokymus savo šalyse užtikrins, kad:

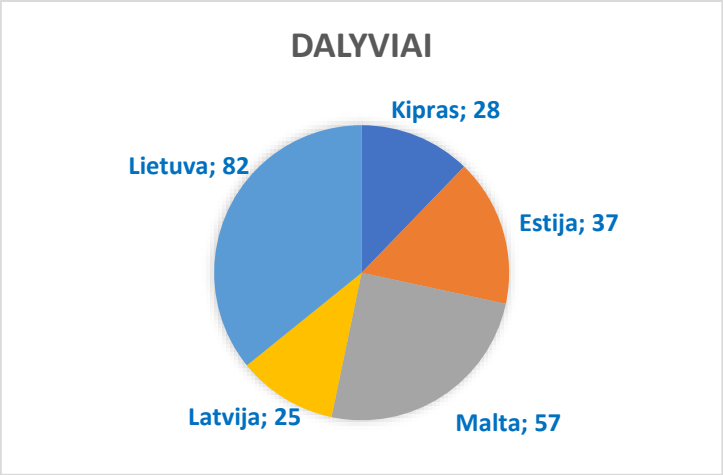
- pilotinius mokymus užbaigs ne mažiau kaip 24 dalyviai iš kiekvienos šalies partnerės (iš viso mažiausiai 120 dalyvių per visas šalis);
- pilotinių mokymų dalyviai užpildys klausimyną prieš pilotinius mokymus, t. y. įvertins savo turimas žinias prieš mokymus (iš viso ne mažiau kaip 120 užpildytų klausimynų);
- galutinis žinių patikrinimo testas laikomas išlaikytu, kai mokymų dalyvis surenka ne mažiau kaip 75%;
- pilotinių mokymų pabaigoje klausytojai užpildys klausimyną, t. y. įvertins savo turimas žinias po mokymų. Tai leis organizatoriams/ partneriams stebėti besimokančiųjų pažangą (iš viso ne mažiau kaip 120 užpildytų klausimynų);
- bent vienas instruktorius/mentorius iš kiekvienos šalies partnerės taip pat užpildytų klausimyną apie mokymus. Tai suteiks partneriams grįžtamąjį ryšį apie kurso mokomosios medžiagos struktūrą ir turinį, mokymų trukmę, temų atitikimą tikslinei auditorijai, kurso modulių išsamumą, sužinoti kiek kursas pasiekė savo tikslą supažindinti klausytojus su kibernetiniu saugumu ir sukčiavimu (iš viso ne mažiau kaip 5 užpildyti klausimynai). Svarbiausias klausimas – kiek kursas pasiekė savo tikslą supažindinti klausytojus su kibernetiniu saugumu ir sukčiavimu;
- pasibaigus pilotiniams mokymams, kiekvienas partneris koordinatoriui pateiks pilotinių mokymų santrauką. Koordinatorius šią informaciją pritaikys rengdamas IO6 ataskaitą. Apibendrinus pilotinių mokymų rezultatus bus atlikti intelektinių rezultatų (IO2, IO3, IO4 ir IO5) atnaujinimai.

5. PILOTINIŲ MOKYMŲ REZULTATAI

Pilotiniai mokymai vyko penkiose šalyse partnerėse: Kipre, Estijoje, Latvijoje, Lietuvoje ir Maltoje. Iš viso mokymuose dalyvavo 229 dalyviai. Šimtas septyniasdešimt penki (175) dalyviai mokymus baigė surinkę 75 % ar daugiau balų.

Klausimynas prieš pilotinius mokymus

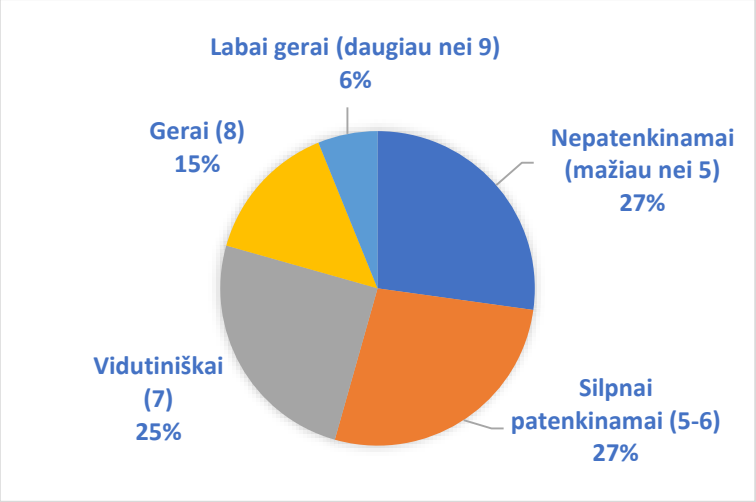
Prieš prasidedant pilotiniams mokymams, visi mokymų dalyviai užpildė klausimyną, siekiant įvertinti jų pradines žinios apie sukčiavimą ir kibernetinį saugumą. Iš viso tokius išankstinius klausimynus užpildė 229 dalyviai. Dalyvių pasiskirstymas pagal šalis parodytas toliau pateiktame paveikslėlyje.



pav. 1 Pilotinių mokymų dalyvių pasiskirstymas pagal šalis

Pradinis dalyvių žinių lygis prieš mokymus

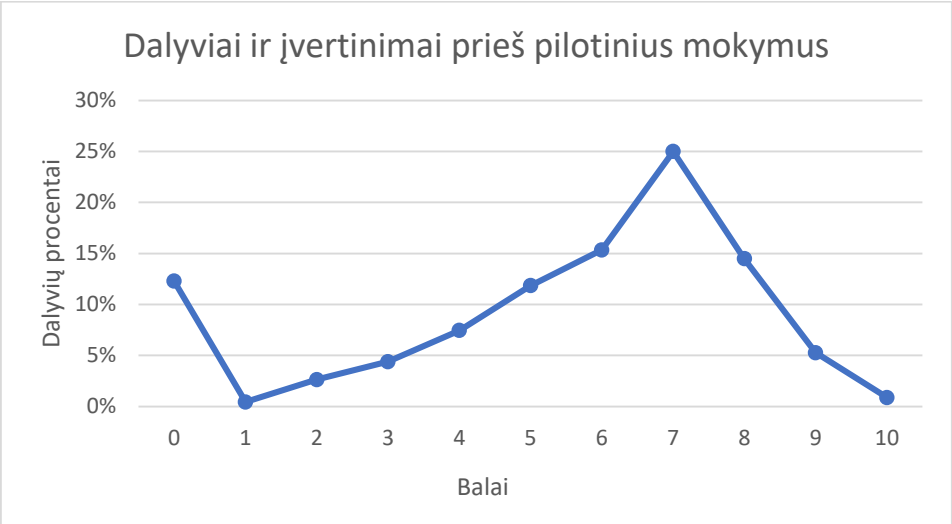
Paveikslas pateiktas žemiau vaizduoja dalyvių pasiskirstymą pagal gautus įvertinimus (balus). Penktadalio (21%) dalyvių žinios įvertintos „Nepatenkinamai", t.y. mažiau nei 5 balais, trečdalis dalyvių gavo įvertinimą „Silpnai patenkinamai" (5-6 balai), maždaug tiek pat dalyvių gavo įvertinimą „Vidutiniškai" (7 balai), 15 % dalyvių gavo įvertinimą „Gerai" (8 balai), ir tik 6 % dalyvių gavo įvertinimą „Labai gerai" (9 ir daugiau balų). Dalyvių žinios buvo vertinamos dešimties balų sistemoje.



pav. 2 Pilotinių mokymų dalyvių žinios prieš mokymus

Žemiau esantis paveikslas vaizduoja dalyvių žinių (įvertintų balais) prieš pilotinius mokymus pasiskirstymą dešimties balų skalėje. Ir čia matote, kad tik vieno dalyvio žinios prieš mokymus buvo įvertintos 10 balų.

Skalėje balai pateikiami dešimties balų sistemoje, nepriklausomai nuo universiteto vertinimo būdo.



pav. 3 Pilotinių mokymų dalyvių žinių, įvertintų balais pasiskirstymas

Klausimų sudėtingumas: penki lengviausi klausimai

Mokymo dalyvių klausimynų analizė parodė, kurie klausimai buvo labai sudėtingi, o kurie pakankamai lengvi. Remdamiesi dalyvių pateiktais atsakymais, išskirti penki lengviausi klausimai. Į šiuos klausimus atsakė teisingai maždaug 70-75 % visų dalyvių. Šie klausimai pateikti žemiau esančioje lentelėje:

1 klausimas. Ar tiesa, kad sukčiavimo atakos vykdomos tik el. paštu?

Ne
Taip

2 klausimas. Kokiais veiksmais galima apsisaugoti nuo socialinės inžinerijos atakų?

Visi išvardyti
Žinoti, kokia jūsų asmeninė informacija prieinama internete
Naudoti daugiapakopį autentifikavimą
Įjungti nepageidaujamų laiškų filtrą
Atnaujinti programinę įrangą

3 klausimas. Kuris iš išvardintų atsakymų geriausiai atspindi sąvokos „kibernetinė ataka" taikymo sritį?

Bet kokia kenkėjiška veikla kibernetinėje erdvėje, net jei ji nesėkminga
Žalingi veiksmai internete
Virusų ir „Trojos arklių" siuntimas el. paštu arba SMS žinutėmis
Sėkmingos sukčiavimo atakos

4 klausimas. Socialinė inžinerija yra...

manipuliavimas žmonėmis, dažniausiai psichologiškai įtikinant, siekiant gauti prieigą prie informacinių sistemų ar duomenų
ataka, kurios metu naudojama kenkėjiška programa, paslėpta iš pirmo žvilgsnio teisėtoje programoje
kenkėjiška programinė įranga, grasinanti paskelbti aukos asmeninius duomenis arba visam laikui užblokuoti prieigą prie jų, jei nebus sumokėtas mokestis
kai užpuolikas perima dviejų šalių sandorius, įsiterpdamas tarp jų

tam tikros rūšies programa, įdiegta rinkti informaciją apie naudotojus, jų sistemas ar naršymo įpročius, siunčiant duomenis nutolusiam naudotojui

5 klausimas. Kokia taktika naudojama sukčiavimo el. laiškuose?

Prašymas siųsti konfidencialią informaciją el. paštu
Prašymas spustelėti el. laiške esančią nuorodą
Informacijos apie per praėjusiais metais sėkmingai įvykdytų sukčiavimo atakų skaičių ir rezultatus pateikimas
Prašymas paaukoti lėšų vandenyno valymui
Prašymas susisiekti su siuntėju telefonu

lentelė 1. Penki lengviausi klausimyno prieš mokymus klausimai

Pirmasis klausimas yra apie sukčiavimo priemones; antrasis - apie prevencijos priemones; trečiasis - apie kibernetinių atakų apibrėžtį; ketvirtasis - apie socialinę inžineriją; o penktasis - apie el. laiškuose naudojamą sukčiavimo taktiką.

Taigi galime matyti, kokių žinių dalyviai turėjo pakankamai prieš mokymus.

Klausimų sudėtingumas: penki sudėtingiausi klausimai

Analizuojant dalyvių pateiktus atsakymus nustatyti klausimai į kuriuos dalyviams atsakyti buvo sunkiausia. Į šiuos klausimus neatsakė arba atsakė prastai 60-80 % dalyvių. Šie klausimai pateikti žemiau esančioje lentelėje:

1 klausimas. Koks yra kibernetinio saugumo sertifikavimo sistemos tikslas?

Sertifikuoti IRT produktus, procesus ir paslaugas
Suteikti visoje ES pripažįstamą kibernetinio saugumo kompetencijų sertifikavimą
Teikti IRT sertifikavimą, pripažįstamą už ES ribų
Nė vienas iš pateiktų atsakymų

2 klausimas. Kuri direktyva buvo pirmasis ES kibernetinio saugumo teisės aktas, kuriame saugumo reikalavimai buvo nustatyti kaip teisiniai įpareigojimai skaitmeninių paslaugų teikėjams ir esminių paslaugų operatoriams?

El. privatumo direktyva
ES kibernetinio saugumo aktas
NIS direktyva
Europos elektroninių ryšių kodekso direktyva

3 klausimas. Kurie teiginiai apie telefoninius apgavikus yra teisingi?

Telefoniniai apgavikai (*angl*. phone phreaks) išmoko valdyti telefono linijas klausydamiesi garsų, kai operatoriai sujungdavo skambučius
Telefoniniai apgavikai (*angl*. phone phreaks) skaitė telefonų bendrovės techninius žurnalus
Telefoniniai apgavikai (*angl*. phone phreaks) neįsilaužinėjo į biurus, kad sukurtų savo techninę įrangą
Telefoniniai apgavikai (*angl*. phone phreaks) nekraustė telefonų bendrovės šiukšlių dėžių, ieškodami „slaptų" dokumentų

4 klausimas. Kuo skiriasi kibernetinis saugumas nuo kompiuterių saugumo?

Kibernetinis saugumas apima skirtingas IT sritis
Tai tas pats
Kibernetinis saugumas yra kompiuterių saugumo dalis
Kibernetinis saugumas susijęs tik su interneto grėsmėmis
Kibernetinis saugumas susijęs su virusais ir pan.

5 klausimas. Kurie teiginiai apie sukčiavimo atakas (*angl*. phishing) yra teisingi?

Sukčiavimas - tai socialinės inžinerijos apgaulė, dėl kurios žmonės ir organizacijos gali prarasti duomenis, pakenkti reputacijai, prarasti tapatybę, pinigus ir patirti daug kitos žalos.

Sukčiavimas paprastai prasideda elektroniniu laišku, kuriuo bandoma įgyti potencialios aukos pasitikėjimą ir įtikinti ją atlikti užpuoliko pageidaujamus veiksmus Sukčiavimas – tai sistemos turto savybė, kuri gali būti silpnoji vieta arba sistemos saugumo trūkumas Sukčiavimas apibūdina standartinę priemonę, kuria grėsmės agentas vykdo grėsmę

lentelė 2. Penki sudėtingiausi klausimyno prieš klausimai

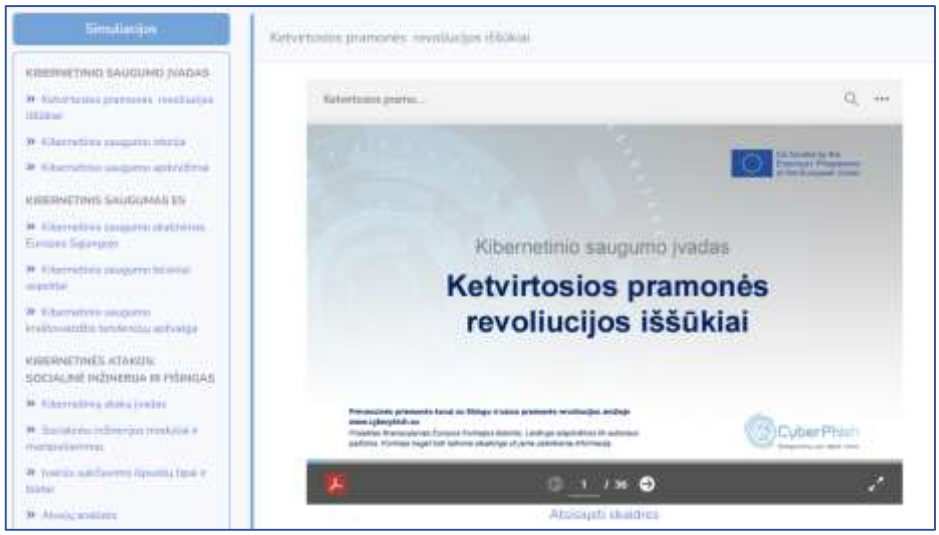
Pirmasis klausimas buvo susijęs su kibernetinio saugumo sertifikavimo sistemos tikslu; antrasis klausimas – su NIS direktyva; trečiasis klausimas – su telefoniniais sukčiais; ketvirtasis klausimas apie kibernetinio ir kompiuterinio saugumo skirtumus; penktuoju klausimu – prašoma pažymėti teisingus teiginius apie sukčiavimo atakas.

Kaip matome, klausimai buvo susiję arba su techninėmis temomis, arba su konkrečiomis temomis, pavyzdžiui, kibernetinio saugumo sistema arba direktyva.

Internetinė mokymosi aplinka

Pilotiniai mokymai buvo vykdomi projekto koordinatoriaus Vilniaus universiteto sukurtoje ir palaikomoje internetinėje sistemoje. Sistema pasiekiama adresu https://cyberphish.vuknf.lt/. Šia mokymosi platforma naudotis gali tiek registruoti mokymų dalyviai, tiek ir neregistruoti vartotojai. Nesiregistruodami vartotojai gali peržiūrėti bendrą informaciją apie mokymo kursą, peržiūrėti reitingų lenteles ir peržiūrėti arba atsisiųsti mokymo medžiagą visomis partnerių kalbomis: anglų, estų, graikų, latvių ir lietuvių.

pav. 4 Internetinė mokymosi aplinka

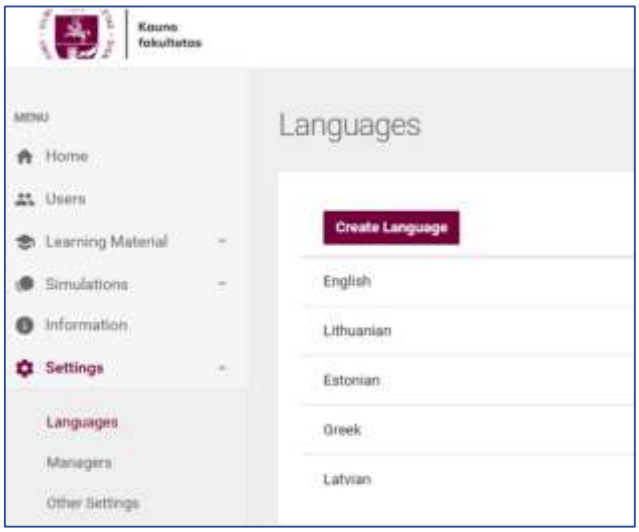


pav. 5 Mokomosios medžiagos pateikimas internetinėje mokymosi aplinkoje

Trys internetinės mokymosi aplinkos vaidmenys

Internetinėje mokymosi aplinkos sistemoje veikia trys vartotojų vaidmenys: sistemos administratorius, vietinis administratorius ir kurso dalyvis.

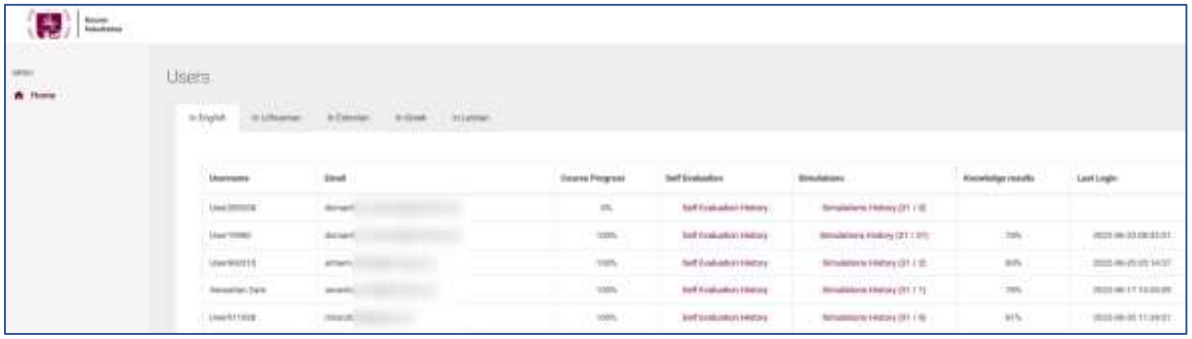
Sistemos administratoriaus gali peržiūrėti visų vartotojų statistinę informaciją, pavyzdžiui, paskutinį prisijungimą, IP adresą, būseną, el. pašto adresą.



pav. 6 Sistemos administratoriaus langas

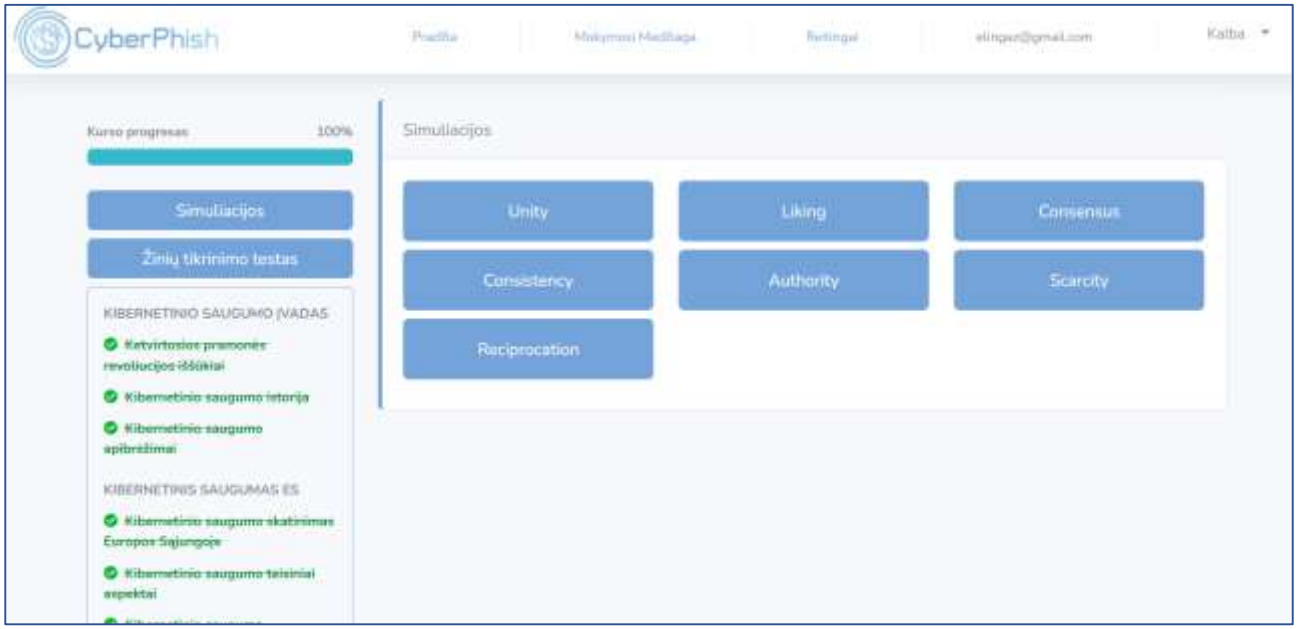
Sistemos administratorius gali įkelti mokymo medžiagą, importuoti ir redaguoti simuliacijas, kurti vietinius administratoriaus vartotojus ir nurodyti kitus su el. platforma susijusius veiksmus, kurie kitiems naudotojams nėra prieinami.

Vietinis administratorius gali matyti statistinę informaciją apie vartotojų pažangą, taip pat informaciją apie atliktus savitikros testus, išspręstas simuliacijas, informaciją apie paskutinį prisijungimą prie kurso ir žinių patikrinimo testų rezultatus. Jis taip pat gali peržiūrėti išspręstus savitikros klausimus ir scenarijus, matyti, kaip dalyvis išsprendė konkretų scenarijų ir kiek taškų surinko už kiekvieną atsakymą. Žemiau, 7 paveiksle vaizduojamas vietinio administratoriaus lango pavyzdys.



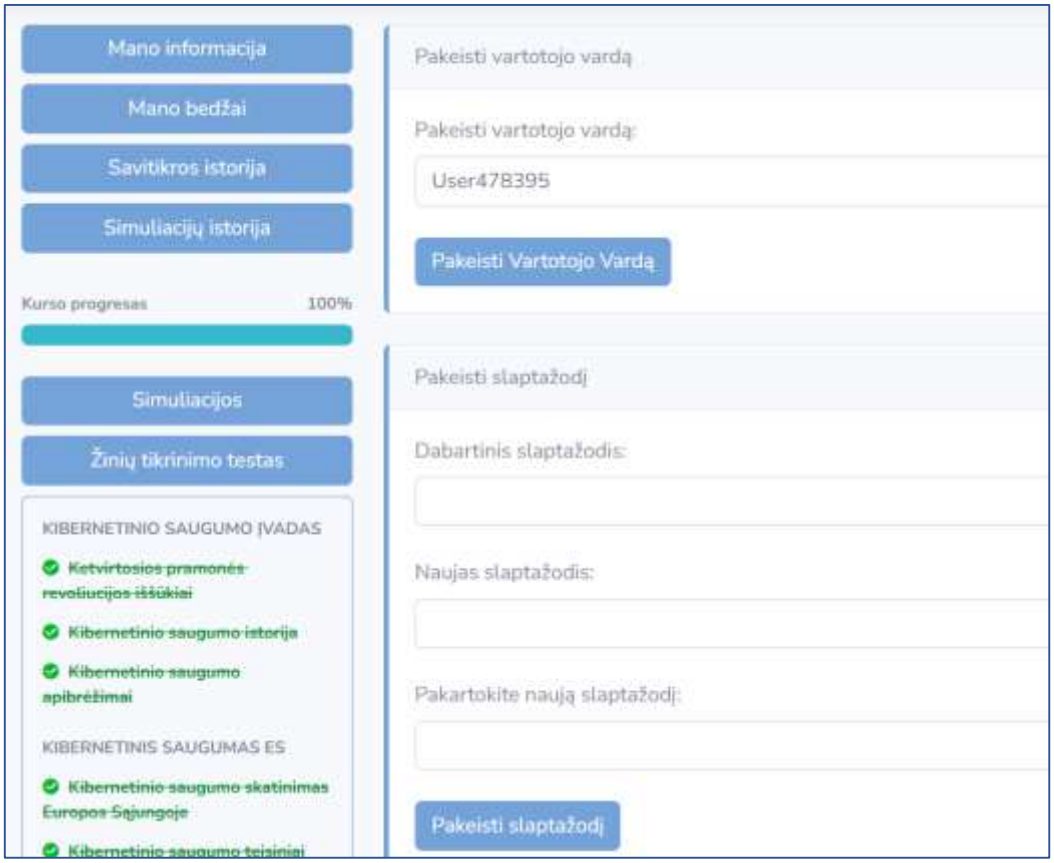
pav. 7 Vietinio administratoriaus langas

Registruotas kurso dalyvis gali naudotis mokymosi aplinka mokymosi tikslais. Žemiau esančiame 8 paveiksle pateiktas kurso dalyvio lango pavyzdys.



pav. 8 Kurso dalyvio mokymosi aplinkos langas

Registruotas kurso dalyvis gali keisti informaciją apie save. Jam suteikiama galimybė pasikeisti vartotojo vardą, prisijungimo prie sistemos slaptažodį (žr. 9 pav.).



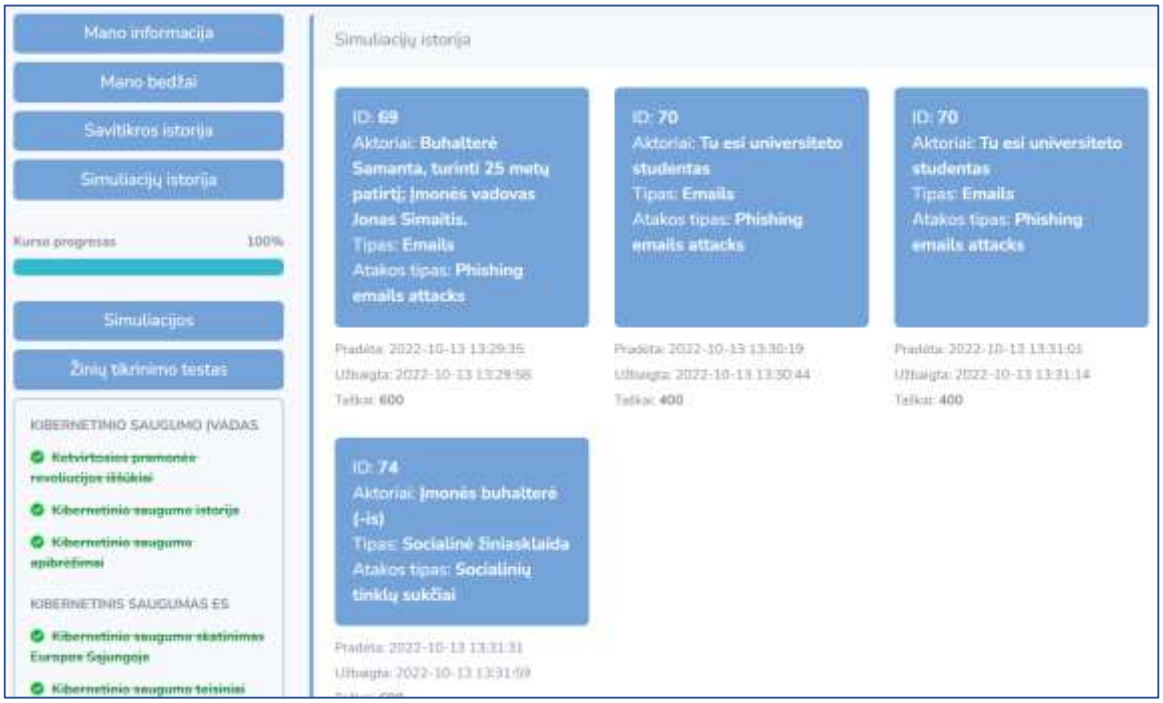
pav. 9 Registruoto kurso dalyvio asmeninės informacijos nustatymo langas

Registruotas kurso dalyvis gali stebėti atliktų savitikros testų istoriją, žinių patikrinimo testų istoriją, peržiūrėti, kiek ženklelių surinko (žr. 10 pav.).

pav. 10 Registruoto kurso dalyvio savitikros testų istorijos langas

Registruotas kurso dalyvis gali stebėti savo atliktų ir (arba) išspręstų simuliacijų istoriją:

- kada ir kaip atsakė į klausimus;
- kokius scenarijus išsprendė;
- kiek taškų surinko už kiekvieną iš jų.



pav. 11 Registruoto kurso dalyvio simuliacijų istorijos langas

Ženkleliai (*angl*. Badges)

Prieš pilotinius mokymus partneriai susitarė dėl šešių ženklelių, tačiau projekto metu buvo sukurti aštuoni ženkleliai, kurie skiriami:

- už testo išlaikymą,
- už kurso baigimą,
- už visų simuliacijų įveikimą,

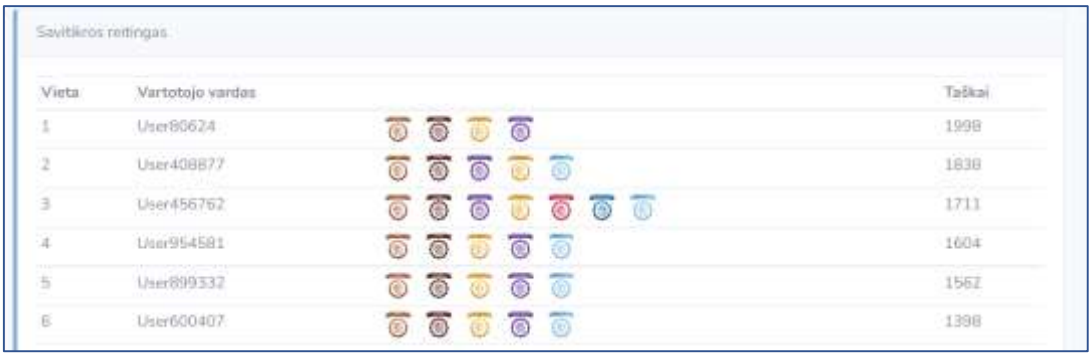
- už pirmojo savitikros testo išlaikymą,
- už modulio ir temos užbaigimą,
- už visų modulių užbaigimą,
- už visų pateikčių peržiūrėjimą,
- už kasdienį prisijungimą prie sistemos dešimties dienų laikotarpyje.

Žemiau pateikiami ženklelių pavyzdžiai:

pav. 12 Ženklelių pavyzdžiai

Taškų rinkimas

Pagal partnerių sutartas taisykles registruoti kurso dalyviai gali rinkti taškus už savitikros testus. Šie surinkti taškai vaizduojami savitikros reitingų lentelėje.



Savitikros reitingas

Vieta	Vartotojo vardas	Taškai
1	User80624	1998
2	User408877	1838
3	User456762	1711
4	User954581	1604
5	User899332	1562
6	User600407	1398

pav. 13 Registruotų kurso dalyvių reitingai

Kurso dalyvio vardas/slapyvardis ir jo surinkti taškai ir ženkleliai vaizduojami kartu.

Mokymo medžiaga internetinėje mokymosi aplinkoje

Partnerių konsorciumas parengė internetinę mokymo medžiagą pagal „CyberPhish" mokymo programą, atsižvelgdamas į ketvirtosios pramonės revoliucijos poreikius. Sukurtą mokymo medžiagą gerai įvertino nepriklausomi ekspertai (po vieną iš kiekvienos šalies partnerės).

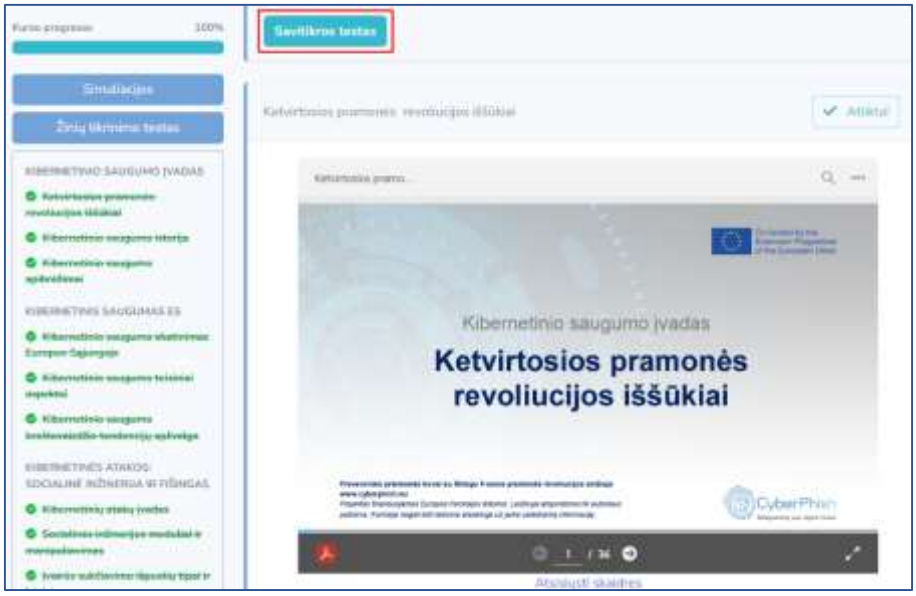
Žemiau esančioje lentelėje pateikiama parengtos mokymo medžiagos santrauka.

Moduliai ir temos				Skaidrių skaičius
1	**Kibernetinio saugumo įvadas**	1.1	Ketvirtosios pramonės revoliucijos iššūkiai	40
		1.2	Kibernetinio saugumo istorija	31
		1.3	Kibernetinio saugumo apibrėžimai	15
2	**Kibernetinė sauga Europos Sąjungoje (ES)**	2.1	Kibernetinio saugumo ugdymas Europos Sąjungoje	31
		2.2	Kibernetinio saugumo teisiniai aspektai	14
		2.3	Kibernetinio saugumo tendencijų apžvalga	41
3	**Kibernetinės atakos: socialinė inžinerija ir sukčiavimas**	3.1	Kibernetinių atakų įvadas	20
		3.2	Socialinės inžinerijos moduliai ir manipuliacija	73
		3.3	Skirtingi sukčiavimo atakų tipai ir kategorijos	37
		3.4	Konkrečių pavyzdžių nagrinėjimas	37
4	**Kibernetinių atakų atpažinimas ir apsauga**	4.1	Pagrindinės žinios apie e. saugumą	22
		4.2	Prevencinės priemonės	59
		4.3	Kibernetinių atakų atpažinimas	108
		4.4	Kibernetinių atakų valdymas	87
		4.5	Žalos sumažinimas pasinaudojant incidento valdymo planu	34
			Iš viso:	**649**

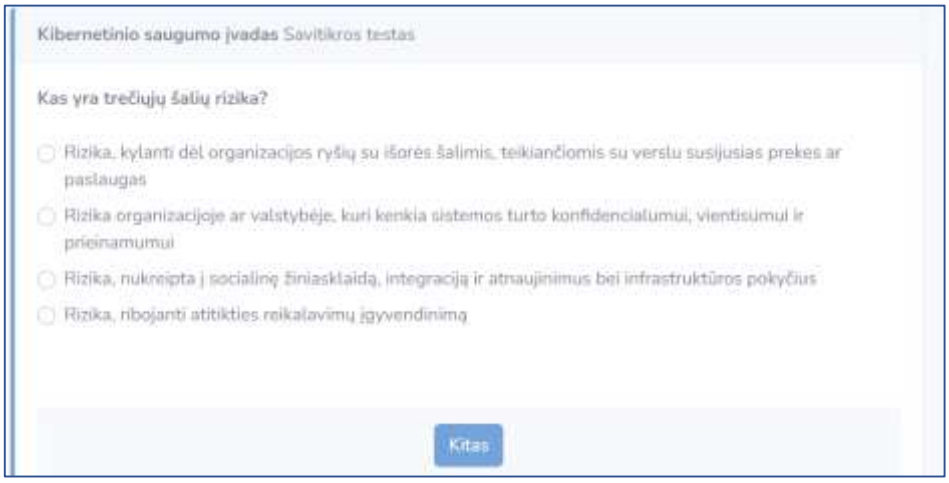
lentelė 3. Mokymo medžiagos santrauka

Užduotys internetinėje mokymosi aplinkoje

Mokymosi kurso turinį galima peržiūrėti ekrane ir (arba) atsisiųsti pateiktis.pdf formatu. Registruotas kurso dalyvis, peržiūrėjęs visą tam tikros temos mokymo medžiagą, gali pasitikrinti savo žinias, spręsdamas savitikros testus. Už tai jam bus skiriami taškai.



pav. 14 Kurso dalyvio aplinkos savitikros testo mygtukas



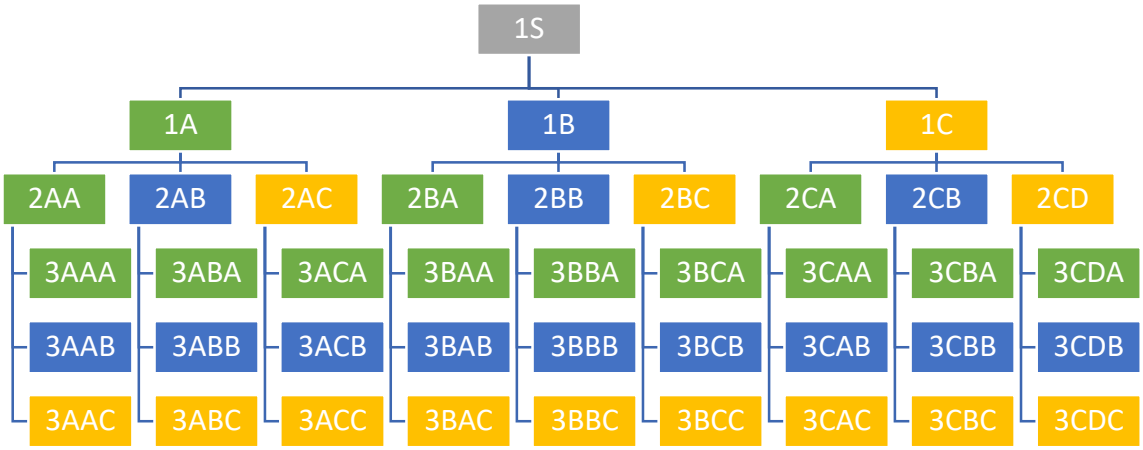
pav. 15 Savitikros testo fragmentas

Simuliacijos

Simuliacija imituoja tikras sukčiavimo atakas, pateikiant besimokančiajam šį procesą žaisminga forma. Simuliacijos tikslas – padėti žmonėms pagerinti kritinį mąstymą, susijusį su kibernetiniu saugumu ir sukčiavimu, atpažįstant sukčiavimo, nepageidaujamų elektroninių laiškų, kibernetinių patyčių ir kitus atvejus. Projekto metu partneriai sukūrė 55 simuliacijas.

Simuliaciją sudaro situacijos aprašymas, tikslas, veikėjai, atakos tipas ir keli (3-4) atsakymų variantai vartotojo elgesio pasirinkimui.

Visos simuliacijos sudarytos sprendimų medžio principu. 16 paveiksle pavaizduotas simuliacijos modelis. Kiekviena simuliacija turi tris lygmenis. Bendras parinkčių (galimų pasirinkimų) skaičius - ne mažiau kaip 50, ir ne daugiau kaip 84 parinktys.



pav. 16 Simuliacijos modelis sudarytas sprendimų medžio principu

Sprendžiant simuliaciją kiekvienas vartotojo pasirinktas atsakymas veda prie sekančio lygmens galimų atsakymų pasirinkimų. Simuliacijoje yra trijų tipų atsakymai: teisingi, dalinai teisingi ir neteisingi. Už kiekvieną atsakymą sistema skiria tam tikrą taškų skaičių. Pasirinkus iš dalies teisingą arba neteisingą atsakymą, sistema pateikia komentarą apie pasirinkimą.

Kurso dalyvis gali pasirinkti simuliacijas pagal kategorijas.

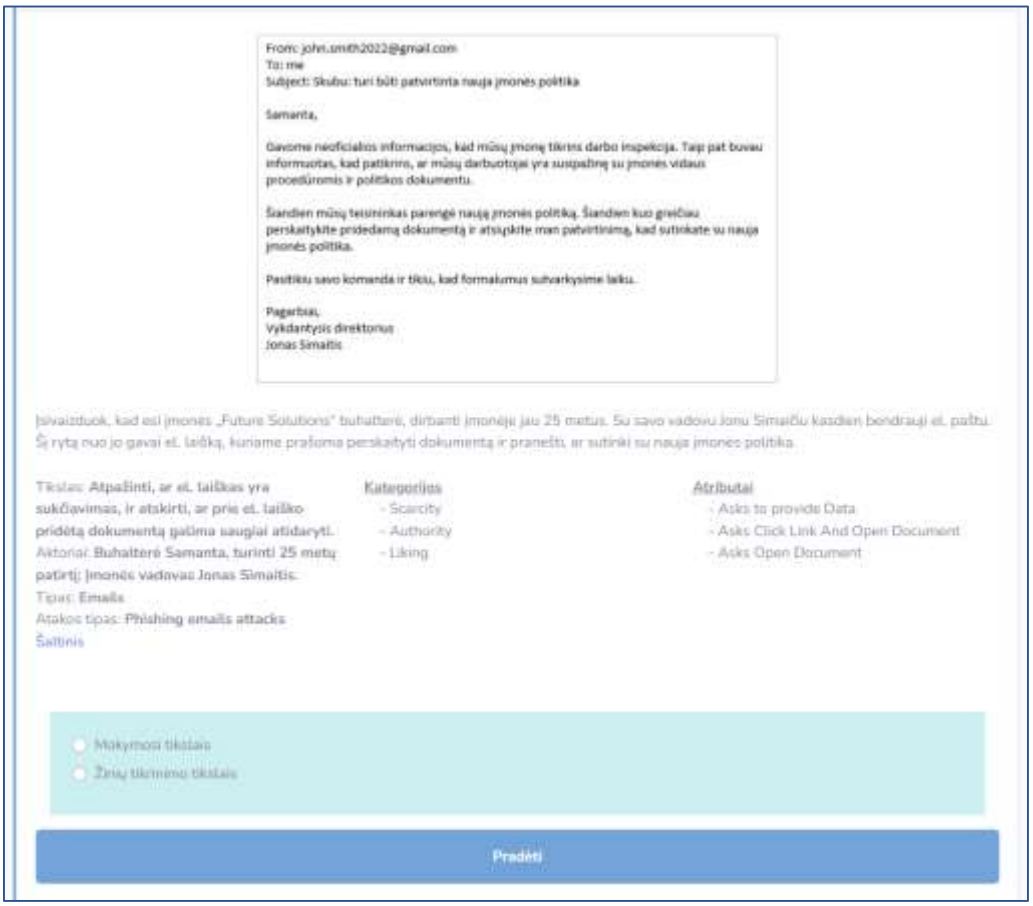
pav. 17 Simuliacijų kategorijos

Simuliacijas galima spręsti dviem būdais: mokymosi tikslais ir žinioms patikrinti. Vienu atveju grįžtamasis ryšys kurso dalyviui pateikiamas po kiekvienos situacijos, o kitu atveju – grįžtamasis ryšys pateikiamas tik pasibaigus visam simuliacijos scenarijui. Už kiekvienos simuliacijos išsprendimą skiriami taškai, o už visų scenarijų išsprendimą skiriamas ženklelis.

pav. 18 Simuliacijų pasirinkimas kategorijoje „Liking"

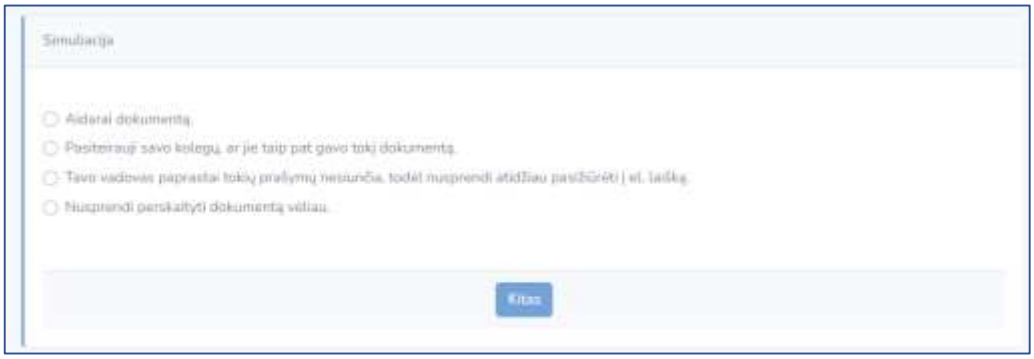
Pasirinkus simuliaciją kurso dalyviui rodomas situacijos aprašymas, simuliacijos tikslas, veikėjai, sukčiavimo atakos tipas ir kiti atributai. Dažnai (bet ne visuomet) pateikiamas paveikslėlis įspūdžiui sustiprinti, kad dalyvis labiau įsijaustų į situaciją.

Tada yra galimybė pasirinkti, kuriuo tikslu sprendžiama simuliacija: mokymosi tikslu ar žinioms patikrinti.



pav. 19 Simuliacijos sprendimo pavyzdys

Pradėjus spręsti simuliaciją, kurso dalyviui pateikiami galimi sprendimo pasirinkimai. Jis turi pasirinkti, kaip elgtųsi tokioje situacijoje. Žemiau esančiame paveiksle pateikiamas simuliacijos sprendimo pavyzdys.

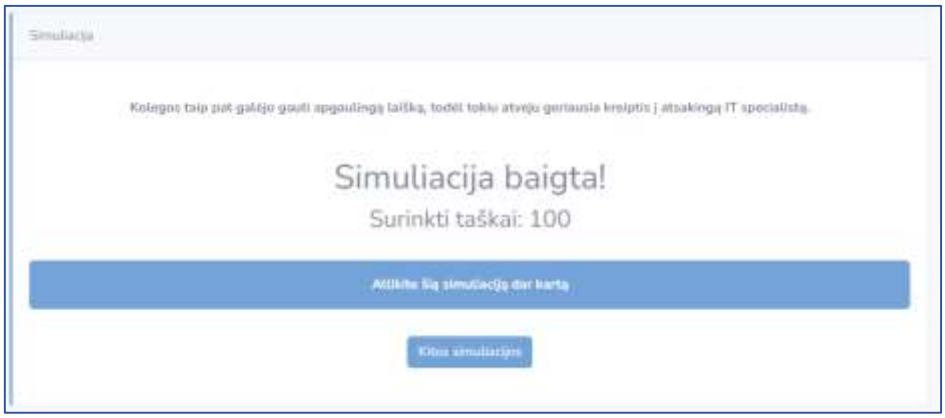


pav. 20 Simuliacijos sprendimas

Simuliacijos sprendimo metu kurso dalyvis gauna grįžtamąjį ryšį ekrane, kai pasirenkamas neteisingas arba iš dalies teisingas atsakymas. 21 paveiksle pavaizduotas grįžtamasis ryšys ekrane simuliacijos sprendimo metu.

pav. 21 Simuliacijos sprendimo metu vartotojui pateikiamas grįžtamasis ryšys ekrane

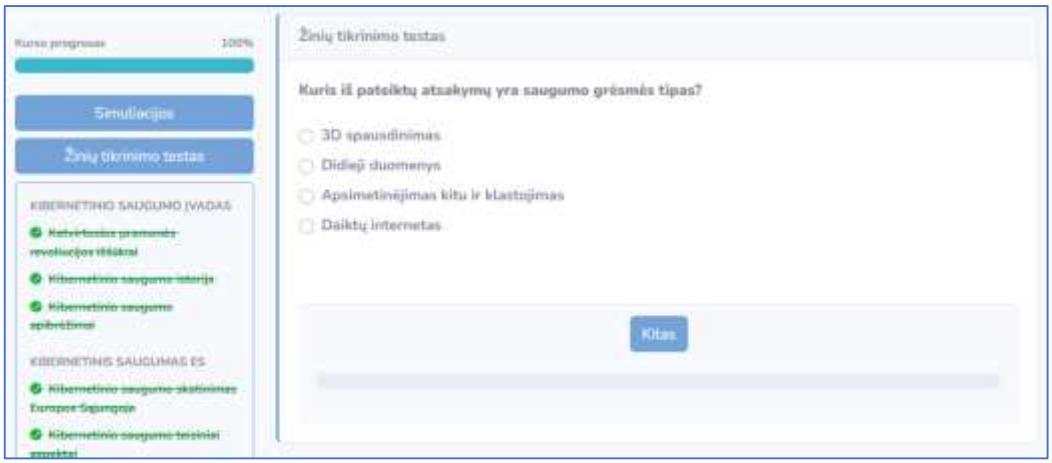
Pabaigus spręsti simuliaciją vartotojui pateikiamas pranešimas, kuriame rodomas surinktų taškų skaičius ir kvietimas spręsti kitas simuliacijas. Jei simuliacija buvo išspręsta neteisingai, pateikiama rekomendacija spręsti simuliaciją dar kartą (žr. pav. 22).



pav. 22 Pabaigtos spręsti simuliacijos langas

Žinių patikrinimo testas

Išmokus mokymo medžiagą (atlikus savikontrolės testus ir simuliacijas), dalyviui mokymosi aplinkoje rodomas mygtukas „Žinių tikrinimo testas“. Pilotinių mokymų metu žinių patikrinimo testą galima atlikti tris kartus.



pav. 23 Žinių patikrinimo testo klausimo pavyzdys

Žinių tikrinimo testo pabaigoje kurso dalyvis mato savo žinių įvertinimo rezultatą procentais.

pav. 24 Žinių vertinimo testo gautų rezultatų lango pavyzdys

Pastaba: žinių patikrinimo testas skirtas žinioms įvertinti. Šis testas nėra skirtas mokymosi tikslams. Žinių patikrinimo testai dalyviams, mentoriams ir (arba) mokytojams viešai neskelbiami. Klausimai tekstiniu formatu prieinami visiems projekto partneriams ir (arba) kūrėjams, o sistema nesuteikia prieigos prie išsamių testo rezultatų. Kiti mentoriai ir (arba) mokytojai taip pat negalės matyti išsamių testo rezultatų.

Žinių patikrinimo testai

Partneriai susitarė, kad pagal paraiškoje pateiktą informaciją parengs klausimus savitikros testams ir klausimus žinių patikrinimo testams. Klausimai bus kelių tipų.

Savitikros testuose bus trijų tipų klausimai:

- klausimai su keliais atsakymų variantais ir vienu teisingu atsakymu (galimų atsakymų skaičius: 3-6),

- klausimai su keliais atsakymų variantais (4-6 galimi atsakymai),

- „taip” ir „ne” klausimai.

Partneriai susitarė dėl klausimų kiekio kiekvienai mokymosi medžiagos temos. Pavyzdžiui, sukurti po 8-14 klausimų iš modulių „Kibernetinio saugumo įvadas” ir „Kibernetinė sauga Europos Sąjungoje (ES)” temų. Sukurti po 12-20 klausimų iš modulių „Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (*angl*. Phishing)”, „Kibernetinių atakų atpažinimas ir apsauga”.

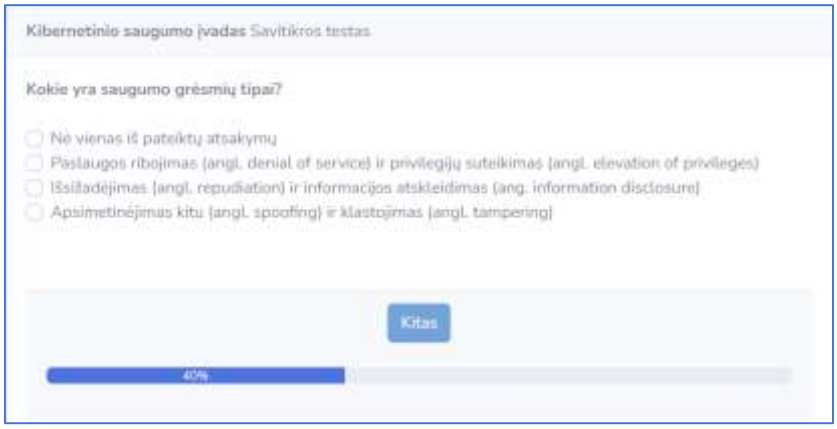
Savitikros testų klausimų **specifikacija**:

Moduliai	Sukurta savitikros klausimų (vnt.)
Kibernetinio saugumo įvadas	13
Kibernetinė sauga Europos Sąjungoje (ES)	12
Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (*angl*. phishing)	16
Kibernetinių atakų atpažinimas ir apsauga	19
Iš viso:	**60**

lentelė 4. Savitikros testų klausimų specifikacija

Mygtukas „Savitikros testas” mokymosi aplinkoje atsiranda kai peržiūrimos visos tam tikro modulio temos. Testą sudaro penki klausimai. Klausimai atsitiktine tvarka parenkami iš esamo modulio klausimų banko.

Savitikros testo metu ekrano apačioje rodoma pažangos juosta, rodanti atsakytų klausimų procentinę dalį ir likusių klausimų skaičių.



pav. 25 Savitikros testo klausimo pavyzdys

Savitikros testo pabaigoje dalyviui parodomi teisingi ir neteisingi atsakymai. Kurso dalyvio pažymėti atsakymai paryškinti žalia spalva. Dalyvis mato testo pradžios datą ir laiką, pabaigos datą ir laiką, taip pat surinktų taškų skaičių viršutinėje dešinėje ekrano pusėje.

Savitikros testų atlikimo skaičius neribojamas. Kurso dalyvis gali atlikti jį tiek kartų, kiek nori. Sprendžiant testą kitą kartą jam bus pateikti kiti atsitiktinai parinkti klausimai. Dalyviams taip pat suteikiamas ženklelis pagal partnerių sutartą taisyklę.

pav. 26 Savitikros testo rezultatų pavyzdys

Žinių patikrinimo testai. Partneriai taip pat susitarė dėl klausimų skaičiaus Žinių patikrinimo testuose:

-Visi klausimai turės keturis atsakymus, iš kurių tik vienas bus teisingas.

-Sukurti 144 žinių patikrinimo klausimus.

Žinių patikrinimo testą sudarys 36 klausimų rinkinys. Testo sprendimo trukmė neviršys 45 minučių. Testo išlaikymo procentas - 75 %.

Partneriai susitarė dėl klausimų skaičiaus iš kiekvienos mokymosi medžiagos temos. Pavyzdžiui, sukurti po 20-25 klausimų iš modulių „Kibernetinio saugumo įvadas" ir „Kibernetinio saugumo ES apžvalga". Sukurti po 45-65 klausimų iš modulių „Kibernetinės atakos - socialinė inžinerija ir sukčiavimas (*angl*. phishing)" ir „Kibernetinių atakų supratimas ir valdymas".

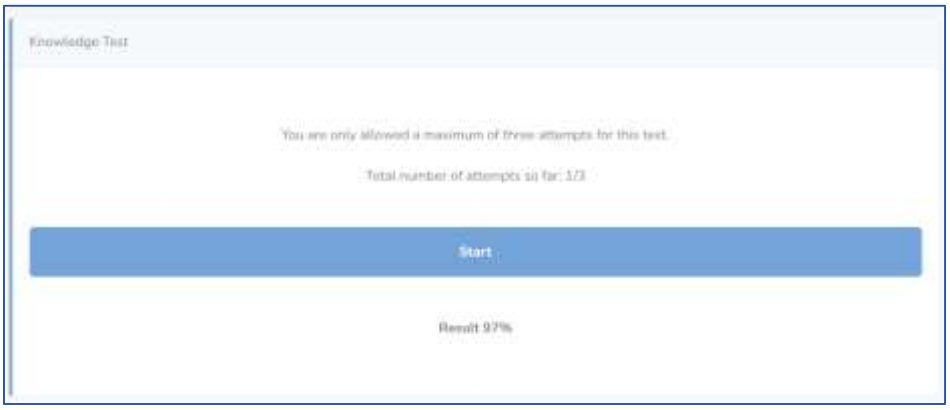
Žinių vertinimo testų klausimų **specifikacija:**

Moduliai	Sukurta žinių patikrinimo klausimų (vnt.)
Kibernetinio saugumo įvadas	24
Kibernetinė sauga Europos Sąjungoje (ES)	20
Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (*angl*. phishing)	62
Kibernetinių atakų atpažinimas ir apsauga	46
Iš viso:	**152**

lentelė 5. Žinių patikrinimo testų klausimų specifikacija

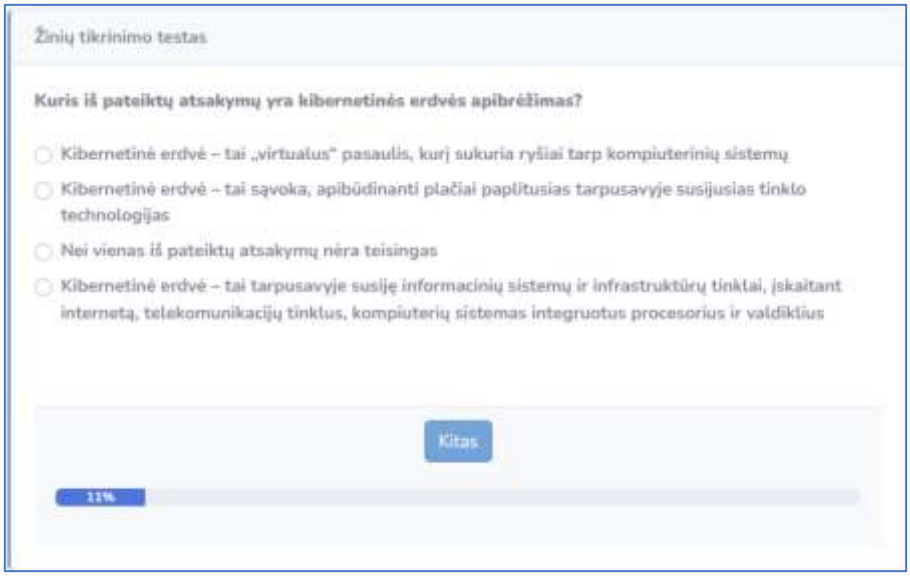
Pilotinių mokymų metu žinių patikrinimo testo sprendimų skaičius buvo ribotas. Didžiausias galimas šio testo laikymo kartų skaičius yra 3.

Mokymosi aplinkoje žinių patikrinimo testo mygtukas rodomas, kai baigiamas visas mokymosi kursas. Paspaudus testo mygtuką, parodoma, kiek kartų dalyvis bandys atlikti testą. Jei testas buvo atliktas anksčiau, rodomas ankstesnio testo rezultatas procentais.



pav. 27 Žinių patikrinimo testo pradinis langas

Žinių patikrinimo testą sudaro 36 atsitiktinai parinkti klausimai. Nustatyta taisyklė, kiek klausimų iš kiekvienos kategorijos turi būti atrinkta atsitiktine tvarka. Testo metu pažangos juostoje rodoma atsakytų klausimų procentinė dalis ir likusių klausimų skaičius. Testo pabaigoje rodomas testo rezultatas, tačiau dalyvis nemato, kaip atsakė į klausimus, nes tai yra žinių vertinimo testas.



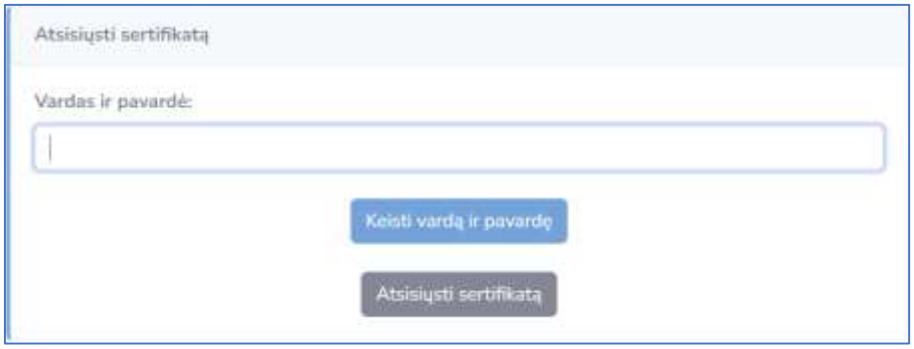
pav. 28 Žinių patikrinimo testo klausimo pavyzdys

Jei dalyviui nepavyksta išlaikyti testo, jis gali bandyti pakartoti mokymo medžiagą, atlikti savitikros testus, ir vėl bandyti atlikti žinių patikrinimo testą. Jei testas išlaikomas sėkmingai, dalyviui suteikiama galimybė įrašyti savo vardą ir pavardę ir atsisiųsti sertifikatą.pdf formatu (žr. 29 pav.).

pav. 29 Išlaikyto žinių patikrinimo testo langas

Sertifikatas

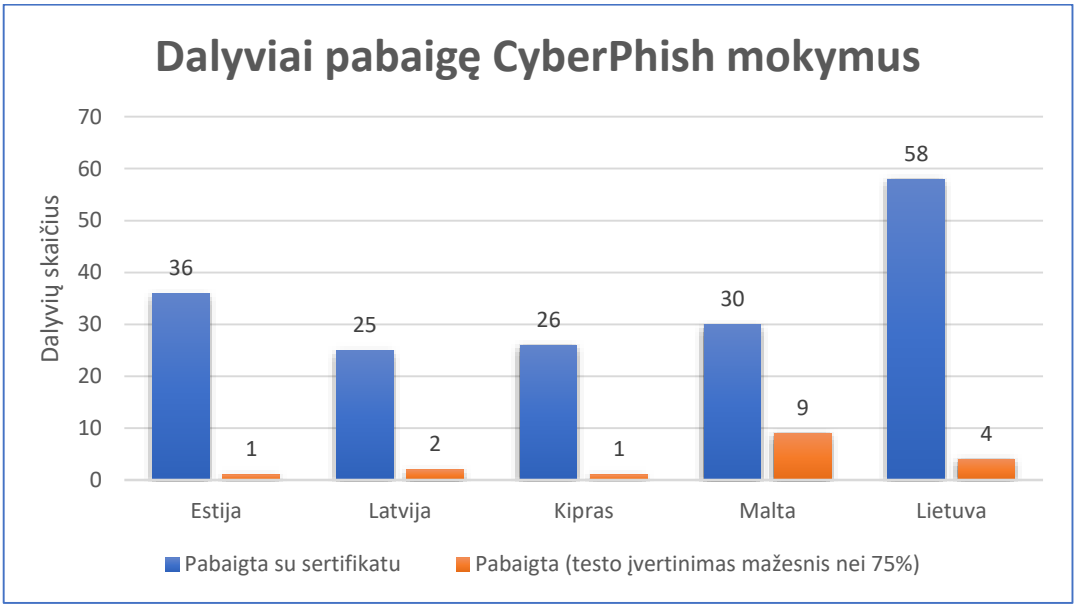
Išlaikęs žinių patikrinimo testą kurso dalyvis gauna nuorodą, klausimynui po testo užpildyti, po kurio gali įrašyti savo vardą ir pavardę ir atsisiųsti sertifikatą PDF formatu. Toks sertifikato išdavimo būdas palengvina sertifikato išdavimo procesą.



pav. 30 Sertifikato formavimo langas

Mokymus baigę dalyviai

Toliau pateiktas paveikslėlis vaizduoja kurso „CyberPhish" pilotinių mokymų rezultatus. Šimtas septyniasdešimt penki dalyviai baigė (175) mokymo kursą ir gavo pažymėjimus: 36 Estijoje, 25 Latvijoje, 26 Kipre, 30 Maltoje ir 58 Lietuvoje. Dar 17 dalyvių kursus baigė be pažymėjimo, t. y. jų žinių patikrinimo rezultatas buvo mažesnis nei 75 %.



pav. 31 Mokymus užbaigusių dalyvių statistika

Klausimynus po pilotinių mokymų užpildė ir pateikė 139 dalyviai: 31 iš Estijos, 24 iš Latvijos, 16 iš Kipro, 27 iš Maltos, ir 40 iš Lietuvos.

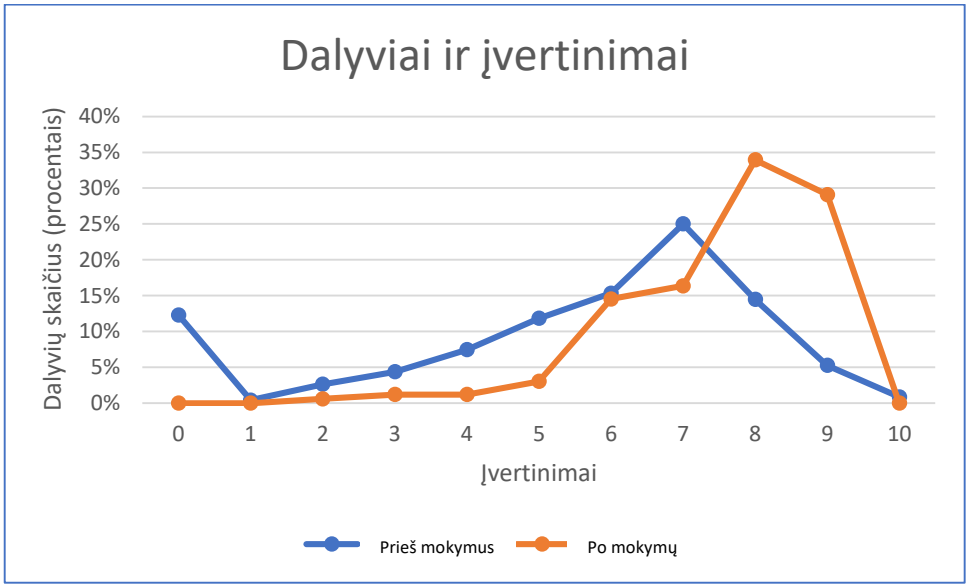
Taip pat klausimynus po mokymų užpildė 8 mokytojai/mentoriai: 2 Maltoje, 3 Lietuvoje ir po 1 Estijoje, Latvijoje ir Kipre. Mokytojai sutiko, kad kursų tikslas - supažindinti mokinius su kibernetinio saugumo ir sukčiavimo (*angl*. phishing) problemomis - buvo pasiektas. Vienodas procentas respondentų nurodė, kad „sutinka" ir, kad „visiškai sutinka" su šiuo teiginiu. Respondentai pritaria, kad programoje pateiktų temų išsamumas buvo tinkamas („sutinka" 62,5% ir „visiškai sutinka" 37,5%). Dauguma mokytojų (62,5 %) visiškai sutinka su teiginiais: „Dalyviams buvo skirta pakankamai laiko bandomajam kursui baigti" ir „Kursų metu nagrinėtų temų sritys buvo tinkamos tikslinei auditorijai".

Mokytojų teigimu kursas yra gerai parengtas ir ugdo dalyvių sąmoningumą bei kritinį mąstymą. Kursą diegtinas (iš dalies arba pilna apimtimi) ne tik su IRT susijusiuose kursuose, bet ir kituose kursuose. Daugiausia teigiamų atsiliepimų sulaukė scenarijų sprendimai.

Dalyvių žinių palyginimas prieš pilotinius mokymus ir po jų

Palyginus dalyvių žinias (atliktą žinių vertinimą) prieš mokymus ir po jų, paaiškėjo, kad dalyviai ženkliai patobulino savo žinias apie kibernetinį saugumą ir sukčiavimą. Toliau pateiktame paveiksle vaizduojama, kaip atrodė dalyvių žinios apie kibernetinį saugumą ir sukčiavimą prieš pilotinius mokymus ir po jų. Horizontalioje ašyje nurodyti įvertinimai (balais), o vertikalioje ašyje - atitinkamą balą surinkusių dalyvių skaičius išreikštas procentais.

Taigi iš paveikslo matyti, kad po „CyberPhish" kurso mokymų dalyvių rezultatai ženkliai pagerėjo (t. y. daugiau besimokančiųjų gavo 8 ir aukštesnius įvertinimus). Tuo tarpu, mokymų dalyvių neišlaikiusiųjų žinių patikrinimo testo (t. y. gavusiųjų įvertinimą nuo 0 iki 6 balų), dalyvių skaičius sumažėjo.



pav. 32 Dalyvių žinios apie kibernetinį saugumą ir sukčiavimą prieš pilotinius mokymus ir po jų

6. PILOTINIAI MOKYMAI ŠALYSE PARTNERĖSE

Šiame skyriuje pateikiama projekto šalių partnerių iš Estijos, Kipro, Latvijos, Lietuvos ir Maltos patirtis įgyvendinant „CyberPhish" mokymo programą. Kiekviena šalis pateikia informaciją apie mokymo kurso dalyvių informavimą ir atrankos procesą, dalyvių profilį, jų motyvaciją dalyvauti pilotiniuose mokymuose, mokymo proceso organizavimą ir dalyvių nuomonę apie mokymo kurso turinį.

Lietuva

Dalyvių informavimo ir atrankos procesas

Siekdami įvertinti parengto mokymo kurso „CyberPhish" kokybę, projekto partneriai savo šalyse surengė pilotinius mokymus. Lietuvoje pilotiniai mokymai buvo vykdomi kviečiant VU Kauno fakulteto bendruomenės narius, daugiausia studentus. Kvietimai buvo paskelbti fakulteto facebook puslapyje ir interneto svetainėje. Dėstytojai projektą studentams pristatė paskaitų metu. Projekto partneris Informacinių technologijų institutas parengė mokymų įgyvendinimo gaires, o taip pat parengė klausimynus mokymų dalyviams prieš ir po mokymų, stebėjo visų partnerių pilotinių mokymų eigą, o susisteminus mokymų duomenis teikė partneriams statistinę informaciją.

Dalyvių profilis

Pilotinių mokymų dalyviai buvo 20-23 metų amžiaus, o vyrų buvo šiek tiek daugiau nei moterų (60 % dalyvių buvo vyrai).

Dalyvių motyvacija prisijungti prie pilotinių mokymų

Studentai buvo motyvuojami tuo, kad pastaruoju metu padažnėjus kibernetinėms atakoms ir asmeninių duomenų vagystėms, kiekvienas privalo gerai išmanyti kibernetinį saugumą, išsiugdyti kibernetinė higienos įgūdžius, suprasti kaip veikia sukčių atakos ir kas yra socialinė inžinerija. Visa tai didina mūsų pačių atsparumą kibernetiniams nusikaltėliams. Štai kodėl studentai noriai prisijungė prie nuotolinio mokymosi kurso „CyberPhish". Kursą baigusiems ir sertifikatą

gavusiems studentams buvo suteikiamas papildomas balas prie dalyko kurso įvertinimo. „CyberPhish" mokymų kursas buvo privalomas laboratorinis darbas studijuojantiems Informacines sistemas ir kibernetinę saugą. Studentai buvo skatinami ne tik susipažinti su kurso medžiaga ir išbandyti simuliacijas, bet ir stebėti galimus sistemos netikslumus bei paliktas klaidas. Už šią veiklą jie taip pat buvo skatinami.

Mokymo proceso organizavimas

Lietuvoje vykusiuose pilotiniuose mokymuose dalyvavo Ekonomikos ir vadybos, Lietuvių filologijos ir reklamos, Finansų ir apskaitos taikomųjų sistemų, Informacinių sistemų ir kibernetinės saugos studentai. Buvo nuspręsta pakviesti studentus iš įvairių studijų programų, siekiant gauti kuo daugiau grįžtamojo ryšio, įvertinant ne tik mokymo medžiagą, mokymosi aplinkos patogumą, bet ir kurso kokybę. Projekto paraiškoje buvo numatyta pakviesti ne mažiau kaip po 24 dalyvius iš kiekvienos šalies partnerės. Pažymėtina, kad pilotinių mokymų metu Lietuvoje dalyvių skaičius buvo gerokai didesnis - prie „CyberPhish" kurso prisijungė daugiau nei 90 dalyvių, iš kurių 58 baigė kursą ir jiems buvo išduotas kurso baigimo pažymėjimas.

Dalyvių nuomonė apie mokymų kurso turinį

Pagrindinis „CyberPhish" pilotinių mokymų dalyvių siekis buvo pasitikrinti ir įsivertinti savo žinias apie sukčiavimą internete. Džiugu, kad dauguma pilotinių mokymų dalyvių Lietuvoje liko patenkinti parengtu „CyberPhish" kursu. 43% dalyvių teigė, kad simuliacijos, kurios yra integruotos „CyberPhish" kurse, pagerino jų gebėjimus atpažinti sukčiavimo atakas internete, o dar 52% nurodė, kad net labai pagerino savo gebėjimus atpažinti tokias atakas.

40-60% kursą baigusių dalyvių teigė, kad sužinojo daug naujų dalykų. Ypatingai gerai dalyviai vertino sukurtus kurso modulius ir teigė, kad išmoko daug naujo temose: „Kibernetinių atakų valdymas", „Kibernetinio saugumo teisiniai aspektai", „Skirtingi sukčiavimo (*angl*. phishing) atakų tipai ir kategorijos" ir „Socialinės inžinerija ir manipuliavimas".

Įvertinus „CyberPhish" pilotinių mokymų dalyvių pateiktą grįžtamąjį ryšį, galima teigti, kad pasitvirtino partnerių siekis „CyberPhish" kursu prisidėti prie kibernetinio saugumo įgūdžių tobulinimo ir saugesnės visuomenės sąmoningumo ugdymo.

Estija

Dalyvių informavimo ir atrankos procesas

Dalyviai išklausė kursą „Saugios programinės įrangos projektavimo principai" Tartu universitete. Pilotiniai mokymai buvo šio kurso dalis. Dalyviai daugiausia buvo Tartu universiteto (UT) ir Talino technologijos universiteto (TalTech) bendrai dėstomos kibernetinio saugumo mokymo programos studentai. Be to, pilotiniuose mokymuose dalyvavo keli "Erasmus+" studentai, kurie taip pat mokėsi minėtame kurse.

Atranka: pilotinis mokymo kursas „CyberPhish" buvo įtrauktas į šį kursą dėl šių priežasčių:

1. Kadangi neseniai paskelbta, kad sukčiavimas (*angl*. Phishing) yra didžiausia saugumo rizika Estijoje, būsimieji kibernetinio saugumo specialistai turi žinoti apie šią riziką, būti pasirengę reaguoti ir gebėti mokyti kitus apie jos poveikį;

2. Dalyvių išsilavinimas yra labai tinkamas tokio pobūdžio pilotiniams kursams. Jie yra jauni specialistai tiek kibernetinio saugumo, tiek informatikos srityje ir gali pakomentuoti tiek kurso turinio, tiek sukurtos internetinės mokymosi platformos trūkumus.

3. Kurso turinys papildė „Saugios programinės įrangos projektavimo principai" medžiagą. Sukčiavimas yra dar viena atakų rūšis. Taigi, panašūs principai (kaip ir kitų saugumo rizikų atveju) buvo iliustruojami per pateiktas pilotines paskaitas, simuliacijas ir rizikos atpažinimą.

Dalyvių profilis

Pilotų mokymų dalyvių amžiaus vidurkis buvo 31 metai, vyriausiam dalyviui - 47 metai, o jauniausiam - 22 metai. Dalyvių vyrų buvo šešis kartus daugiau nei moterų (31 vyras ir 5 moterys). Visi dalyviai buvo Kibernetinio saugumo programos pirmo kurso magistrantūros studentai, studijuojantys II semestre. Estų ir dalyvių, nurodžiusių kitas šalis, buvo po lygiai (po 18 dalyvių).

Dalyvių motyvacija prisijungti prie pilotinių mokymų

Pilotiniai mokymai buvo kurso "Saugios programinės įrangos projektavimo principai" dalis. Už kurso įvertinimą studentai galėjo gauti iki 10 balų (priklausomai nuo galutinio žinių patikrinimo testo rezultatų).

Mokymo proceso organizavimas

Mokymai buvo vykdomi internetu. Įvadinė paskaita vyko gegužės 5 d. Likusi mokymų dalis buvo pateikta kaip savarankiško mokymosi užduotis. Klausimus ir atsiliepimus studentai galėjo siųsti elektroniniu paštu arba klausti apie mokymus per kitas kurso paskaitas.

Dalyvių nuomonė apie mokymų kurso turinį

Po pilotinių mokymų atlikta studentų apklausa parodė, kad visi dalyviai patobulino savo žinias apie sukčiavimą. Ypatingai žinios patobulintos kurso „CyberPhish" temose: „Kibernetinio saugumo teisiniai aspektai", „Kibernetinių atakų valdymas", „Kibernetinio saugumo tendencijų apžvalga", „Skirtingi sukčiavimo (*angl*. Phishing) atakų tipai ir kategorijos", „Socialinė inžinerija ir manipuliavimas" bei „Kibernetinių atakų atpažinimas". Visi dalyviai, baigę „CyberPhish" kursą, buvo patenkinti savo kibernetinio saugumo dalykų žiniomis. Beveik visi studentai sutiko, kad simuliacijos padėjo patobulinti sukčiavimo atpažinimo įgūdžius. Visi dalyviai tvirtai sutiko, kad nuotolinis/internetinis metodas buvo tinkamas šiam kursui, kad mokymams baigti skirto laiko pakako, ir kad jie rekomenduotų šį kursą kitiems žmonėms. Dauguma studentų sutiko, kad jie aiškiai suprato kurso tikslus; kad kurso turinys atitiko kurso tikslus; ir kad pagalba pilotinių mokymų metu buvo tinkama.

Malta

Dalyvių informavimo ir atrankos procesas

Kibernetinis sukčiavimas daro poveikį įvairiose srityse, ne tik tose, kurios susijusios su informacinėmis technologijomis. Todėl vykdant pilotinius mokymus buvo orientuojamasi į skirtingų studijų programų studentus. MECB per savo socialinius partnerius pakvietė dalyvauti studentus iš kelių aukštųjų mokyklų. Pilotiniuose mokymuose dalyvavo studentai iš Maltos menų, mokslo ir technologijų koledžo MCAST (pagrindinė profesinio mokymo įstaiga Maltoje), ir Maltos universiteto (UoM) Jaunesniojo koledžo studentai. MECB Ltd į pilotinius mokymus taip pat kvietė ir į kitas suinteresuotąsias šalis, tokius kaip ekspertai, politikai ir mokytojai. Kvietimas registruotis į pilotinius mokymus buvo skelbiamas MECB interneto svetainėje. Pilotinių mokymų metu buvo naudojama projekto „CyberPhish" metu parengta mokymo medžiaga, scenarijai, savitikros ir žinių patikrinimo testai. Dalyviai atsakė į klausimynus skirtus mokymų dalyviams prieš ir po mokymų.

MECB į pilotinius mokymus pakvietė aukštųjų mokyklų darbuotojus būti mentoriais, kurie padėtų įvykdyti pilotinius mokymus. Prieš prasidedant pilotiniams mokymams mentoriai buvo supažindinti su visu „CyberPhish" projektu, įskaitant projekto metu atliktus tyrimus (IO1), parengtą „CyberPhish" mokymo programą (IO2), sukurtą mokymo medžiagą (IO3), simuliacijas (IO4) bei testus (IO5). Tokiu būdu buvo siekiama mentoriams suteikti kuo daugiau informacijos, kad jie galėtų pilotinių mokymų metu padėti dalyviams išspręsti iškilusius sunkumus. Be to, mentoriams buvo pademonstruota, kaip naudotis e. platforma, savitikros ir žinių patikrinimo testais. Prieš pilotinius mokymus taip pat buvo suorganizuota diskusija, pristatyti mokymo(si) metodai. Šio renginio metu mentoriams buvo pateiktos metodinės gairės, o taip pat gairės studentams. Mentoriai prieš mokymus dalyviams išsamiai pristatė projektą „CyberPhish" ir teikė konsultacijas pilotinių mokymų dalyviams.

Dalyvių profilis

Pilotiniuose mokymuose dalyvavo 43 dalyviai. Daugiau nei du trečdaliai dalyvių buvo vyrai (71,4%) ir beveik trečdalis - moterys (28,6%). Dauguma dalyvių buvo darbuotojai (60,7%), 21,4% - studentai, o dešimtadalis (10,7%) - verslininkai. Likusieji dalyviai nurodė, kad jie dirba savarankiškai ir kt.

Mokymo proceso organizavimas

Iš viso Maltoje buvo surengti treji pilotiniai mokymai:

1) tiesioginiai mokymai (MCAST Verslo vadybos ir komercijos instituto (IBMC) studentams);

2 nuotoliniai mokymai internetu (studentams, besimokantiems informacinių technologijų kursuose UoM Junior College);

3) atviri kursai (į juos pakviesti visi suinteresuotieji subjektai, įskaitant besimokančiuosius, ekspertus, politikos formuotojus ir mokytojus).

Mokymosi sistemoje užsiregistravo 75 besimokantieji, iš kurių 57% (43) pilnai baigė kursą. Iš jų 67% bandė atlikti simuliacijas, o 91% atliko žinių tikrinimo testą. Trisdešimt besimokančiųjų išsprendė žinių patikrinimo testą surinkdami 75% ir daugiau.

Dalyvių nuomonė apie turinį

Po pilotinių mokymų atlikta dalyvių apklausa parodė, kad jie patobulino savo žinias apie sukčiavimą visose „CyberPhish" kurso moduliuose. Dalyviai taip pat pažymėjo, kad įgijo daug naujų žinių apie sukčiavimą. Visi dalyviai buvo patenkinti savo kibernetinio saugumo dalykų žiniomis baigę „CyberPhish" kursą. Beveik visi dalyviai sutiko, kad simuliacijos padėjo patobulinti jų įgūdžius atpažįstant sukčiavimą. Dauguma respondentų sutiko arba visiškai sutiko su teiginiais:

- laiko, skirto mokymo kursui pabaigti buvo pakankamai;
- mokymas ir pagalba viso kurso metu buvo tinkami;
- jie aiškiai suprato kurso tikslus;
- kurso turinys atitiko kurso tikslus;
- internetinis mokymosi metodas buvo tinkamas šiam kursui;
- jie rekomenduotų šį kursą kitiems žmonėms.

Kipras

Dalyvių informavimo ir atrankos procesas

Pilotiniuose mokymuose Kipre dalyvavo įvairių studijų programų studentai, t. y. IT studijų, Europos studijų, Rinkodaros studijų ir kt. DOREA taip pat pakvietė organizacijas (kitas suaugusiųjų švietimo įstaigas, taip pat MVĮ ir jų darbuotojus iš jų tinklo) dalyvauti pilotiniuose mokymuose.

DOREA paskelbė atvirą kvietimą ir pakvietė visus norinčius prisijungti prie kurso pilotinių mokymų, nes šiuos įgūdžius turi turėti kiekvienas žmogus, ne tik IT programų studentai. Kvietimai buvo siunčiami elektroniniu paštu, skambinant telefonu ir susitinkant asmeniškai.

Dalyvių profilis

Pilotiniuose mokymuose dalyvavo 26 dalyviai. Dauguma dalyvių buvo dvidešimtmečiai studentai (92,3%), o likusieji 7,7% - darbuotojai. Daugiau nei du trečdaliai dalyvių buvo moterys (76,9%) ir beveik trečdalis - vyrai (23,1%).

Mokymo proceso organizavimas

Mokymai Kipre daugiausia buvo organizuojami internetu, o instruktorius teikė grįžtamąjį ryšį ir pagalbą internetu/ per nuotolį. Kai kuriais atvejais vyko ir tiesioginės konsultacijos.

Kiekvienas asmuo išreiškęs norą dalyvauti pilotiniuose mokymuose, kurie buvo organizuojami internetu, gavo el. laišką su instrukcijomis kaip užsiregistruoti į mokymus. Prieš užsiregistruojant į „CyberPhish" mokymo kursą visi dalyviai buvo pakviesti atsakyti į klausimyno prieš mokymus klausimus, siekiant nustatyti dalyvių pradinį žinių lygį.

Kurso metu mokymų vadovas konsultavo dalyvius el. laiškais, skambučiais, internetiniais/nuotoliniais ir kontaktiniu būdu (kai buvo įmanoma), teikė jiems rekomendacijas, atsakinėjo į klausimus arba nurodė papildomus informacijos šaltinius.

Dauguma dalyvių lankė kursus, nes apskritai domėjosi šia tema, o kiti buvo įsitikinę, kad gautas pažymėjimas bus naudingas ateityje. Dvidešimt penki iš 26 dalyvių pilnai baigė kursus ir gavo pažymėjimus.

Dalyvių nuomonė apie mokymų kurso turinį

Visi dalyviai nurodė, kad įgijo daug naujų žinių arba patobulino jau turimas žinias visose kurso „CyberPhish" modulių temose. Dauguma dalyvių nurodė, kad ypač daug naujų žinių įgijo temose: „Socialinės inžinerija ir manipuliavimas". „Skirtingi sukčiavimo (*angl*. phishing) atakų tipai ir kategorijos"; patobulino savo žinias temose: „Kibernetinio saugumo teisiniai aspektai", "Prevencinės priemonės" ir „Kibernetinių atakų valdymas". Tik vienas dalyvis nurodė, kad nieko naujo nesužinojo temoje „Kibernetinių atakų atpažinimas".

Dauguma dalyvių nurodė, kad baigę kursą yra patenkinti savo žiniomis apie kibernetinio saugumo dalykus. Nedidelė dalis dalyvių (nuo 3,8% iki 11,5%) savo žinias vertino neutraliai. Tai gali reikšti, kad, nors jie manė įgiję daug žinių, vis dar turi kur tobulėti. Dauguma dalyvių nurodė, kad simuliacijos jiems „labai padėjo" arba „padėjo" suprasti dėstomus kibernetinius dalykus. Dauguma dalyvių buvo patenkinti kursu, nes suprato kurso tikslus. Internetinis mokymosi

metodas ir kurso turinys jiems pasirodė tinkami, jiems pakako laiko kursui baigti ir pan. Vienas dalyvis vis dėlto nurodė, kad nesutinka, jog internetinis mokymosi metodas buvo tinkamas šiam kursui. Vienam dalyviui nurodė, kad internetine platforma sudėtinga naudotis, o vienas asmuo nerekomenduotų šio kurso kitiems žmonėms.

„CyberPhish" instruktorė teigė, kad kursas yra labai informatyvus ir apima visas pagrindines temas, kurios būtinos, kad besimokantieji suprastų kibernetinio saugumo problemas, ypač sukčiavimo, ir žinotų, kaip apsisaugoti. Ji pabrėžė, kad kursas neabejotinai naudingas ne tik IT studentams, norintiems atnaujinti savo įgūdžius ir žinias, bet ir kitų sričių studentams, darbuotojams ir visai visuomenei.

Latvija

Dalyvių informavimo ir atrankos procesas

Pilotiniai mokymai buvo vykdomi kartu su socialiniais partneriais Rygos technikos universitetu (RTU) ir Latvijos kultūros kolegija (LKK), todėl dalyvauti buvo pakviesti šių aukštųjų mokyklų studentai. Altacom surengė atskirus susitikimus su RTU ir LKK studentų atstovybėmis, kuriuose pristatė projektą „CyberPhish" ir numatytus pilotinius mokymus. Po susitikimo studentus kuravo asmenys, atsakingi už neformalųjį švietimą jų aukštosiose mokyklose. Socialiniai partneriai ir atsakingi asmenys iš Latvijos kultūros kolegijos, kvietė į pilotinius mokymus išsiųsdami kvietimus studentams (daugiausia iš ne IT fakultetų).

Dalyvių profilis

Pilotiniuose mokymuose dalyvavo 27 dalyviai. Dalyvių amžiaus vidurkis buvo 23 metai, vyriausiam - 26, o jauniausiam - 19 metų. Dalyvių vyrų buvo pusantro karto daugiau nei moterų (60% vyrų ir 40 % moterų). Apskritai dalyviai buvo technikos ir kultūros sričių studentai. Dauguma dalyvių buvo latviai, tuo metu gyvenantys Rygoje, tačiau buvo ir Latvijoje studijuojančių mainų studentų iš įvairių šalių.

Dalyvių motyvacija prisijungti prie pilotinių mokymų

Pilotiniai „CyberPhish" mokymai pristatyti kaip nauja papildoma neformaliojo ugdymo priemonė, padedanti besimokantiesiems įgyti vertingų teorinių žinių ir praktinių kibernetinio saugumo įgūdžių. Šiais laikais tokie įgūdžiai yra labai naudingi ne tik asmeniniam naudojimui, bet ir beveik visose darbo vietose, kur naudojami kompiuteriai. Todėl, kai kurie iš pakviestųjų nusprendė, kad dalyvavimas pilotiniuose mokymuose jiems gali būti tikrai naudingas, ir sutiko prisijungti.

Mokymo proceso organizavimas

Pagrindinė informacija apie pilotinius mokymus buvo pateikta per susitikimą su RTU ir LKK studentų atstovybėmis ir kvietime į mokymus. Be to, dalyviai galėjo užduoti rūpimus klausimus ir teikti savo atsiliepimus tiesiogiai el. paštu arba kitais kanalais (pvz., žinutėmis socialiniame tinkle).

Mokymosi platformoje užsiregistravo 45 dalyviai. Žinių tikrinimo testą išlaikė 25 dalyviai, surinkę įvertinimą daugiau nei 75%. Du dalyviai išlaikė žinių testą (latvių kalba), surinkę mažiau nei 75% balų.

Dalyvių nuomonė apie mokymų kurso turinį

Atlikus dalyvių apklausą po pilotinių mokymų paaiškėjo, kad dalyviai įgijo daug žinių apie sukčiavimą beveik visose „CyberPhish" kurso kibernetinio saugumo temose. Dalyviai patobulino žinias apie sukčiavimą šiuose moduliuose: „Kibernetinio saugumo teisiniai aspektai", „Kibernetinio saugumo tendencijų apžvalga", "Prevencinės priemonės" ir „Kibernetinių atakų valdymas". Dauguma dalyvių, baigusių „CyberPhish" kursą, buvo patenkinti savo žiniomis apie kibernetinio saugumo dalykus, ypač moduliuose „Skirtingi sukčiavimo (*angl*. phishing) atakų tipai ir kategorijos" ir „Kibernetinių atakų valdymas". Beveik visi dalyviai sutiko, kad simuliacijos padėjo patobulinti įgūdžius atpažįstant sukčiavimą. Dauguma apklaustųjų sutiko arba visiškai sutiko su teiginiais:

- jie rekomenduotų šį kursą kitiems žmonėms;
- mokymas ir parama viso kurso metu buvo tinkami;
- internetine mokymosi platforma buvo lengva naudotis;
- kursui baigti buvo skirta pakankamai laiko;
- kurso turinys atitiko kurso tikslus;
- jie aiškiai suprato kurso tikslus;
- internetinis mokymosi metodas buvo tinkamas šiam kursui.

IŠVADOS

Partnerių konsorciumas, remdamasis poreikių analize, parengė mokymo programą apie kibernetinį saugumą, kibernetines atakas, socialinę inžineriją, ypač daug dėmesio skirdamas sukčiavimo atpažinimui ir jo prevencijai. Mokymo programa pritaikyta naudoti mišriam mokymui(si), tačiau kursas gali būti naudojamas tiek nuotoliniams, tiek ir tiesioginiams mokymams. Visos mokymo programos apimtis yra 30 valandų ir tai atitinka 1 ECTS.

Mokymo programą sudaro keturios atskiros dalys (moduliai): Kibernetinio saugumo įvadas; Kibernetinė sauga Europos sąjungoje (ES); Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (angl. phishing); Kibernetinių atakų atpažinimas ir apsauga.

Partnerių konsorciumas parengė internetinę mokymo medžiagą pagal „CyberPhish" mokymo programą, atsižvelgiant į 4-osios pramonės revoliucijos poreikius. Mokomąją medžiagą sudaro skaidrės, užduotys, nuorodos į išorinius šaltinius bei vaizdo įrašus. Sukurtą mokymosi medžiagą gerai įvertino išoriniai ekspertai.

Parengta mokymo programa, mokymo medžiaga ir mokymosi aplinka gali būti naudojamos įvairioms tikslinėms grupėms, pavyzdžiui, studentams, pedagogams, universitetų darbuotojams (bendruomenės nariams), suaugusiųjų centrams ir verslo sektoriui (darbdaviams ir darbuotojams).

Sukurta internetinė mokymosi medžiaga, mišri mokymosi aplinka ir simuliacijos pilotinių mokymų metu buvo integruoti į dalyvaujančių universitetų mokomuosius dalykus.

Projekto metu sukurta mokymo medžiaga, simuliacijos, savitikros testai ir žinių patikrinimo testai padeda stiprinti dalyvių kritinį mąstymą ir kibernetinio saugumo įgūdžius, kuriuos jie galės pritaikyti savo profesinėje veikloje. Kursas „CyberPhish" gali būti sėkmingai naudojamas organizuojant mokymus ir kitoms tikslinėms grupėms, o taip pat gali būti adaptuojamas kitose Europos šalyse, kadangi kursas yra parengtas ir anglų kalba.

Palyginus pilotinio mokymo dalyvių žinias prieš mokymus ir po jų, paaiškėjo, kad dalyviai gerokai patobulino savo žinias apie kibernetinį saugumą ir sukčiavimą, ženkliai pagerėjo dalyvių rezultatai, t. y. daugiau besimokančiųjų gavo įvertinimą 8 ir aukštesnius įvertinimus.

Šimtas septyniasdešimt penki dalyviai baigė (175) mokymo kursą ir jiems buvo išduoti pažymėjimai: iš jų 36 Estijoje, 25 Latvijoje, 26 Kipre, 30 Maltoje ir 58 Lietuvoje. Dar 17 dalyvių kursus baigė be pažymėjimo, t. y. jų žinių patikrinimo rezultatai buvo mažesni nei 75 %.

ŠALTINIAI

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/2022/12/IO1-A2-Report_Analysis-of-existing-Cybersecurity-training-programmes_LT.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/2022/12/IO1-A1-Report_Recognising-Phishing-and-Skills-Gaps_LT.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

PRIEDAS 1

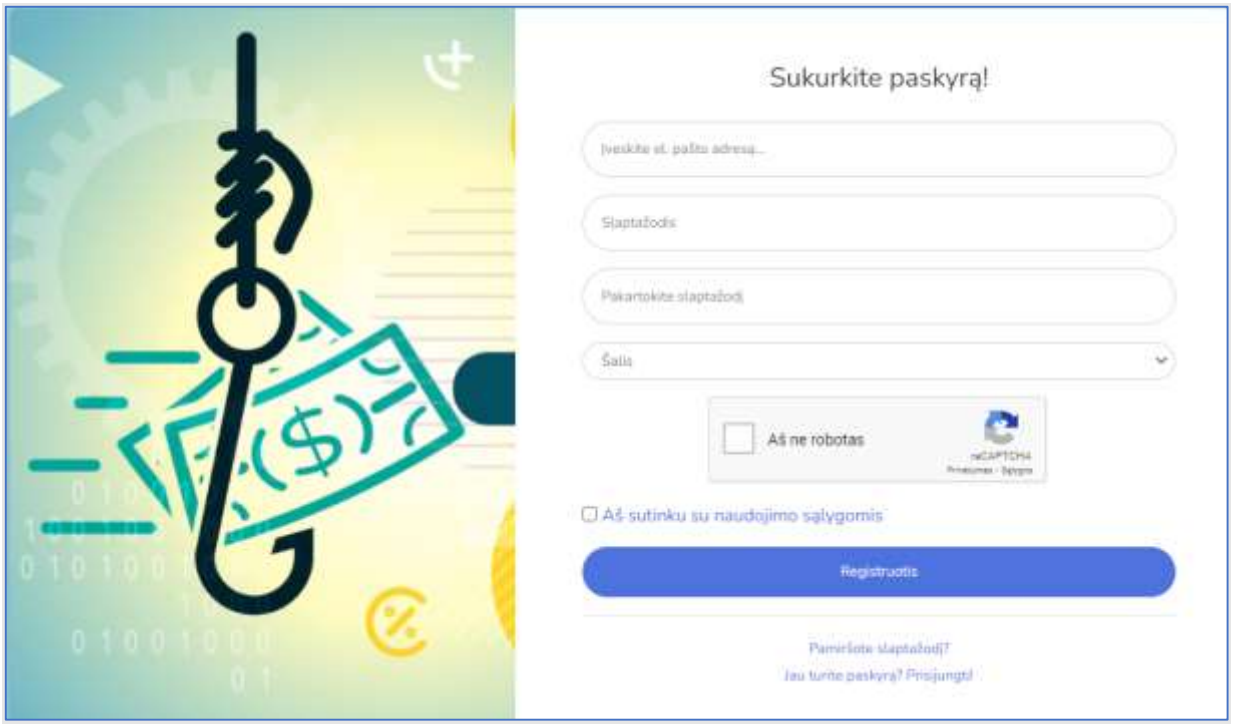
„CYBERPHISH" MOKYMO(SI) APLINKA

„CyberPhish" kurso mokymosi medžiaga yra prieinama visiems vartotojams ir yra nemokama. Ji pasiekiama adresu https://cyberphish.vuknf.lt. Mokymosi medžiaga pateikiama penkiomis kalbomis: anglų, estų, graikų, latvių ir lietuvių. Neregistruoti lankytojai gali tik peržiūrėti mokymosi medžiagą, tačiau jie negali atlikti savitikros testų, žinių patikrinimo testų, pelnyti ir rinkti ženklelių, spręsti simuliacijų ir gauti sertifikatų. Norint tapti registruotu mokymosi aplinkos vartotoju, būtina užsiregistruoti.

Registracija el. mokymosi aplinkoje

Norint tapti registruotu vartotoju, susikurkite paskyrą spustelėję mygtuką **Registruotis**.

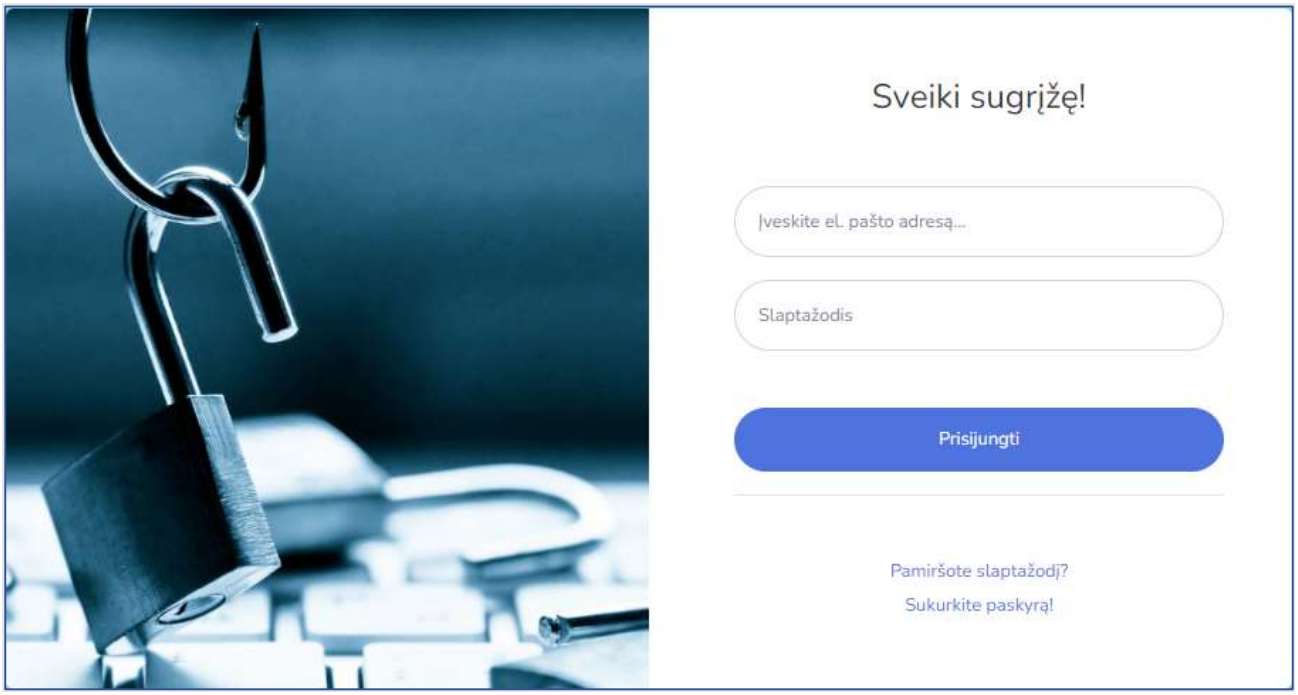
Puslapio viršuje spustelėję mygtuką **Registruotis** įveskite savo el. pašto adresą, sugalvotą slaptažodį, pakartokite slaptažodį ir pasirinkite savo šalį. Taip pat patvirtinkite (t. y. pažymėkite varnelę), kad nesate robotas ir, kad sutinkate su taisyklėmis bei sąlygomis, tada spustelėkite mygtuką **Registruotis**.



Patvirtinimo nuoroda bus išsiųsta į el. paštą, kurio adresą nurodėte kurdami paskyrą. Pasitikrinkite el. paštą ir spustelėkite atsiųstą nuorodą.

Pastaba: Jei negavote el. laiško su patvirtinimo nuoroda iš sistemos, būtina pasitikrinti nepageidaujamų laiškų aplanką. Gali atsitikti, kad patvirtinimo el. laiškas atsidurs nepageidaujamų laiškų / šiukšlių aplanke.

Paspauskite patvirtinimo nuorodą ir prisijunkite prie sistemos.

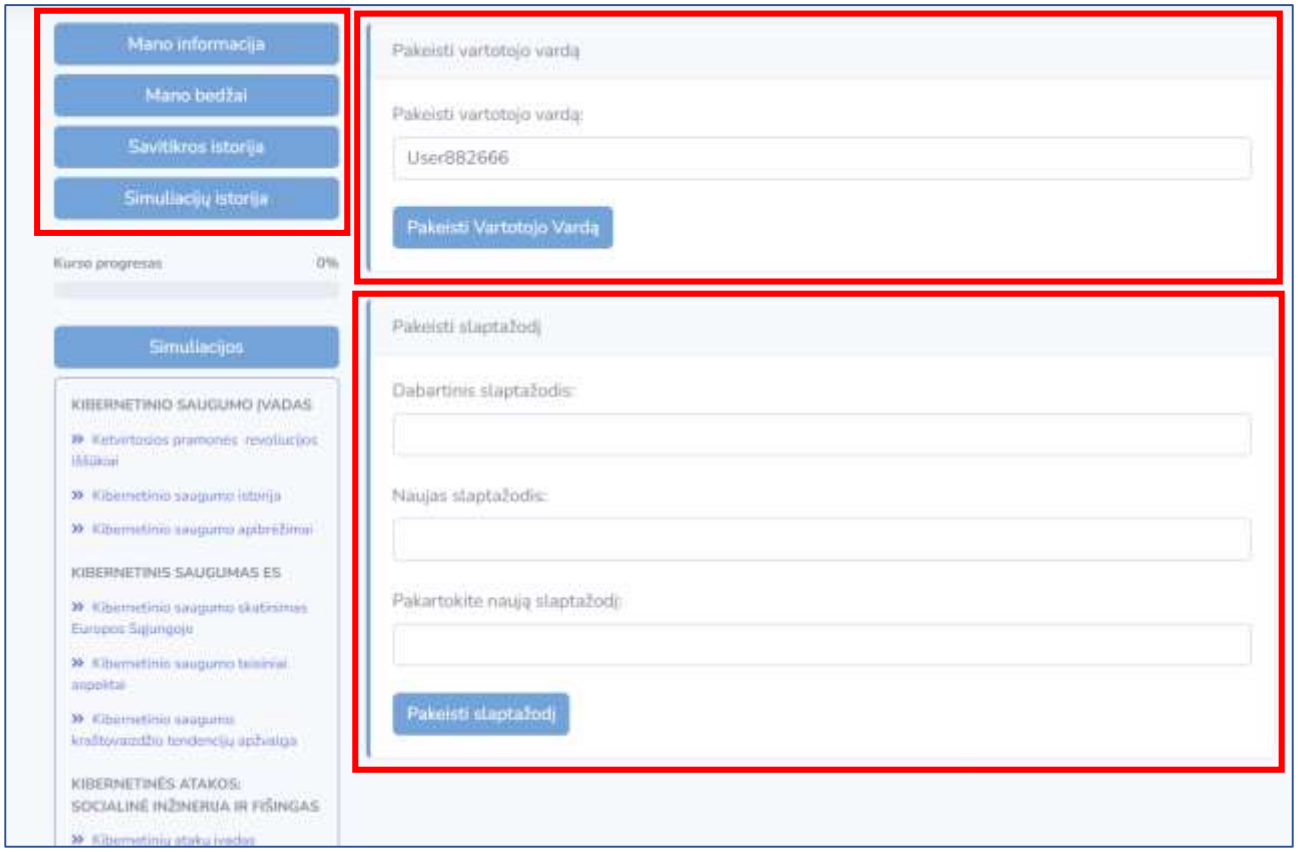


Vartotojo paskyra

Prisijungę, puslapio viršuje matysite meniu juostą. Spustelėkite savo el. pašto adresą ir pasirinkite **Mano informacija**.

Kairėje puslapio **Mano informacija** pusėje matysite pagrindinį naudotojo meniu, kuriame pateikiami mygtukai nukreipiantys į puslapius **Mano informacija** (t. y. esamą puslapį), puslapį **Mano ženkleliai**, puslapį **Savitikros istorija** ir puslapį **Simuliacijų istorija**.

Puslapyje **Mano informacija** galite pakeisti vartotojo vardą ir slaptažodį.



Puslapyje **Mano ženkleliai** matysite visus ženklelius, kuriuos surinkote už įvairias atliktas užduotis.

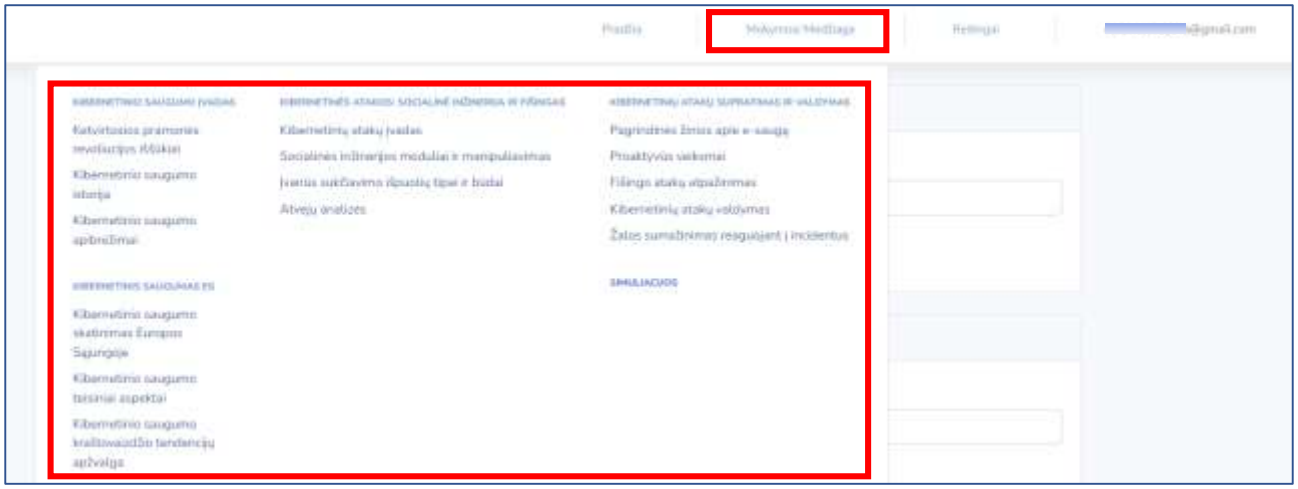
Puslapyje **Savitikros istorija** galėsite matyti visų pradėtų ir pabaigtų spręsti savitikros testų istoriją. Jei savitikros testas nebaigtas, tai jį pabaigti spręsti galite spustelėję testo pavadinimą. Jei testas baigtas, spustelėję ant jo galite pamatyti rezultatus.

Puslapyje **Simuliacijų istorija** galite peržiūrėti pradėtų ir užbaigtų simuliacijų istoriją. Jei simuliacija nebuvo pabaigta, tai galite ją pabaigti spręsti spustelėję simuliacijos pavadinimą. Jei simuliacija baigta, tuomet jos rezultatus galite peržiūrėti spustelėję ant jos pavadinimo.

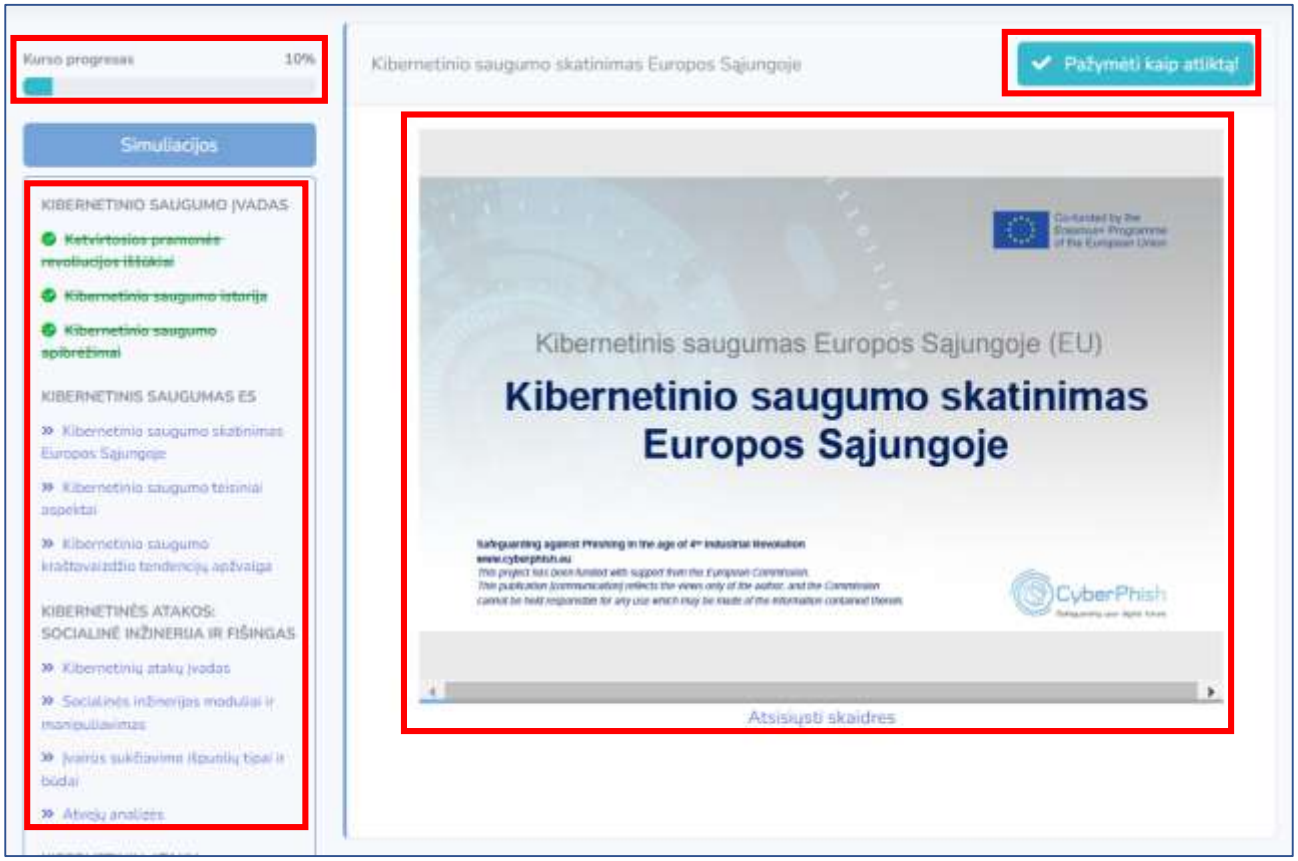
Mokomoji medžiaga

Mokymosi medžiagą pasiekiama per puslapio viršuje esantį meniu punktą **Mokymosi medžiaga** ir pasirinkus jus dominančią temą*.

**Visa mokymosi medžiaga pasiekiama be registracijos, tačiau kai kurios funkcijos gali būti ribotos. Besimokantysis gali skaityti mokomąją medžiagą neprisijungęs prie sistemos, tačiau jis negalės patvirtinti mokomosios medžiagos peržiūros būsenos, taip pat neturės prieigos prie testų ir simuliacijų.*



Pasirinkus temą, pagrindinėje puslapio dalyje matysite tos temos skaidres, o puslapio kairėje - nuorodas į visas kurso „CyberPhish" temas. Jei esate prisijungę kaip registruotas vartotojas, galite pažymėti temas kaip užbaigtas paspausdami mygtuką **Pažymėti kaip atlikta!** puslapio viršuje dešinėje pusėje. Puslapio kairėje pusėje virš mygtuko **Simuliacijos**, matysite savo **kurso progresą**.



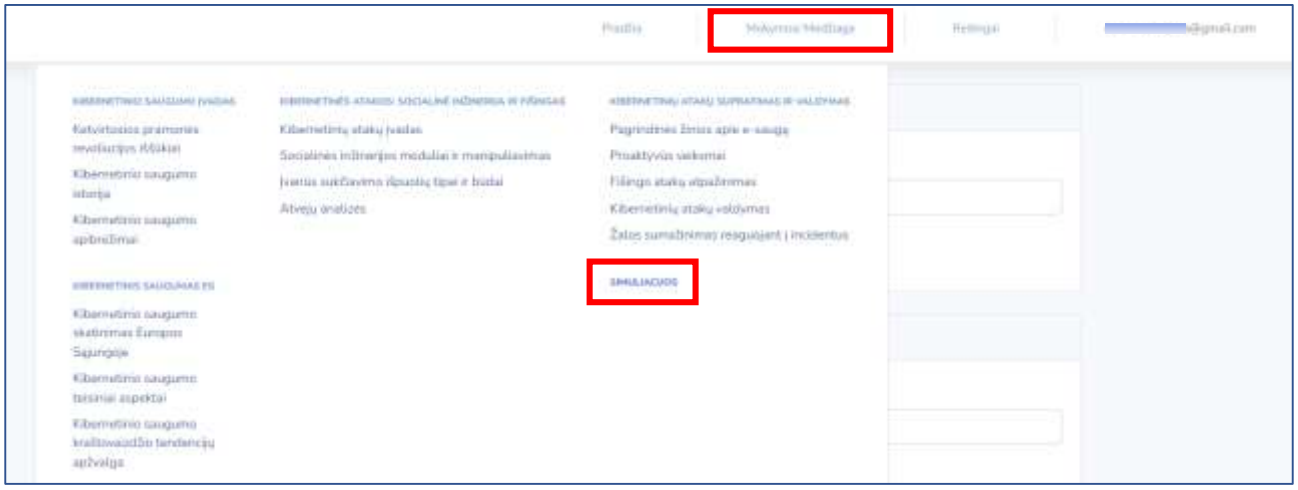
Savitikros testai

Norint pasiekti savitikros klausimus, reikia kiekvieną modulio temą **Pažymėti kaip atlikta!** Tuomet pagrindinio puslapio viršuje pamatysite mygtuką **Savitikros testas**. Norėdami pasiekti savitikros testus, turite būti prisijungę prie sistemos.

Spustelėjus mygtuką **Savitikros testas**, gausite penkis to modulio klausimus savo žinioms įvertinti.

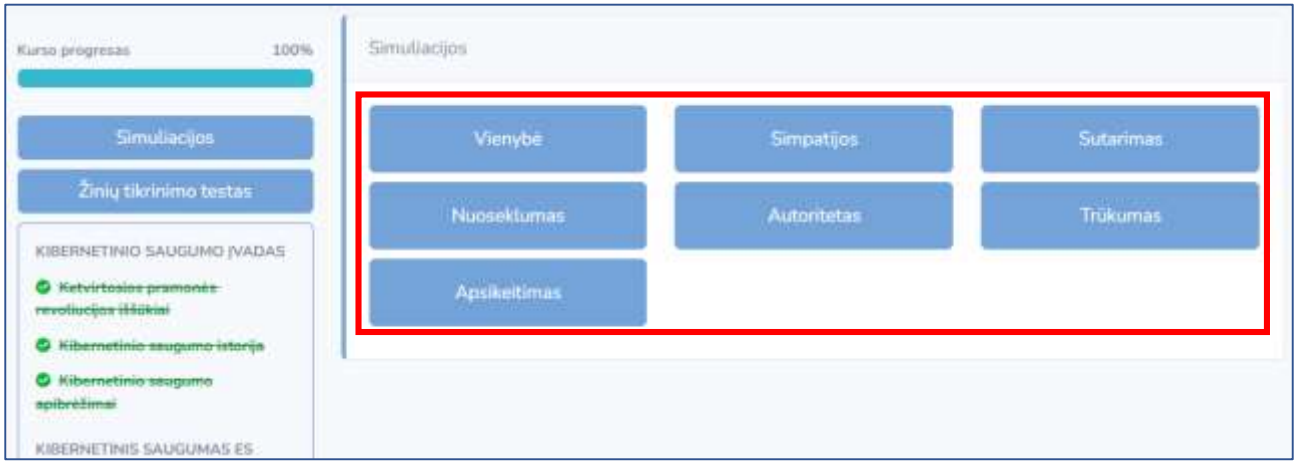
Simuliacijos

Simuliacijas pasiekti gali tik prisijungę vartotojai. Spustelėkite meniu punktą **Mokomoji medžiaga** ir pasirinkite **Simuliacijos**.

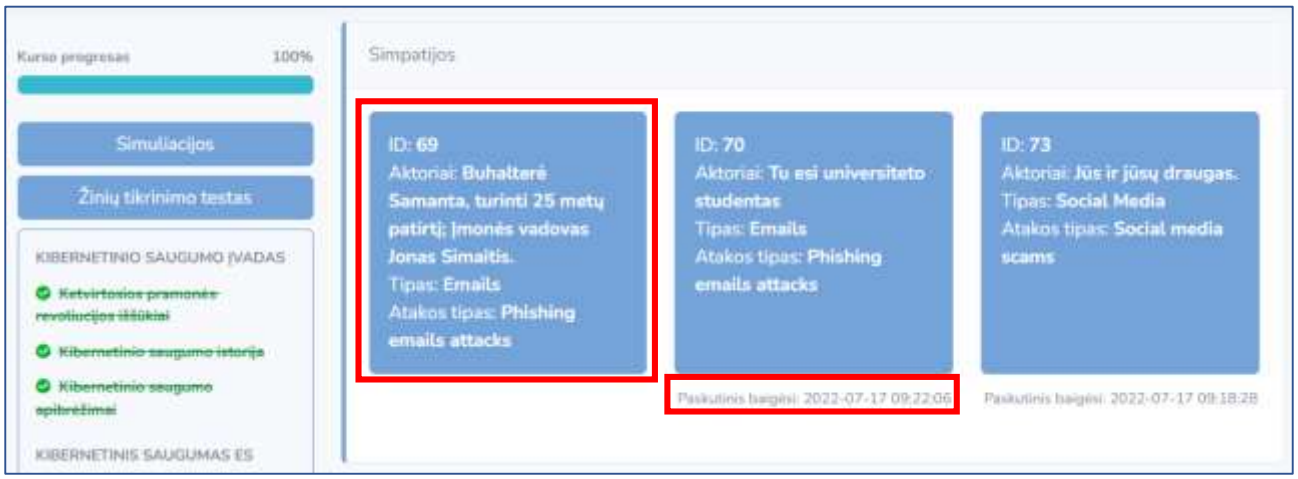


Taip pat simuliacijas galite pasiekti ir iš bet kurio pasirinktos mokymosi medžiagos temos puslapio.

Spustelėję mygtuką **Simuliacijos**, turite pasirinkti simuliacijų kategoriją. Yra septynios kategorijos: Vienybė, Simpatijos, Sutarimas, Nuoseklumas, Autoritetas, Trūkumas ir Apsikeitimas. Ta pati simuliacija gali būti įtraukta į keletą kategorijų.



Paspaudus kategorijos mygtuką galėsite pasirinkti iš tos kategorijos simuliacijų. Jei jau esate sprendę tam tikrą simuliaciją, po ja matysite laiko žymą.

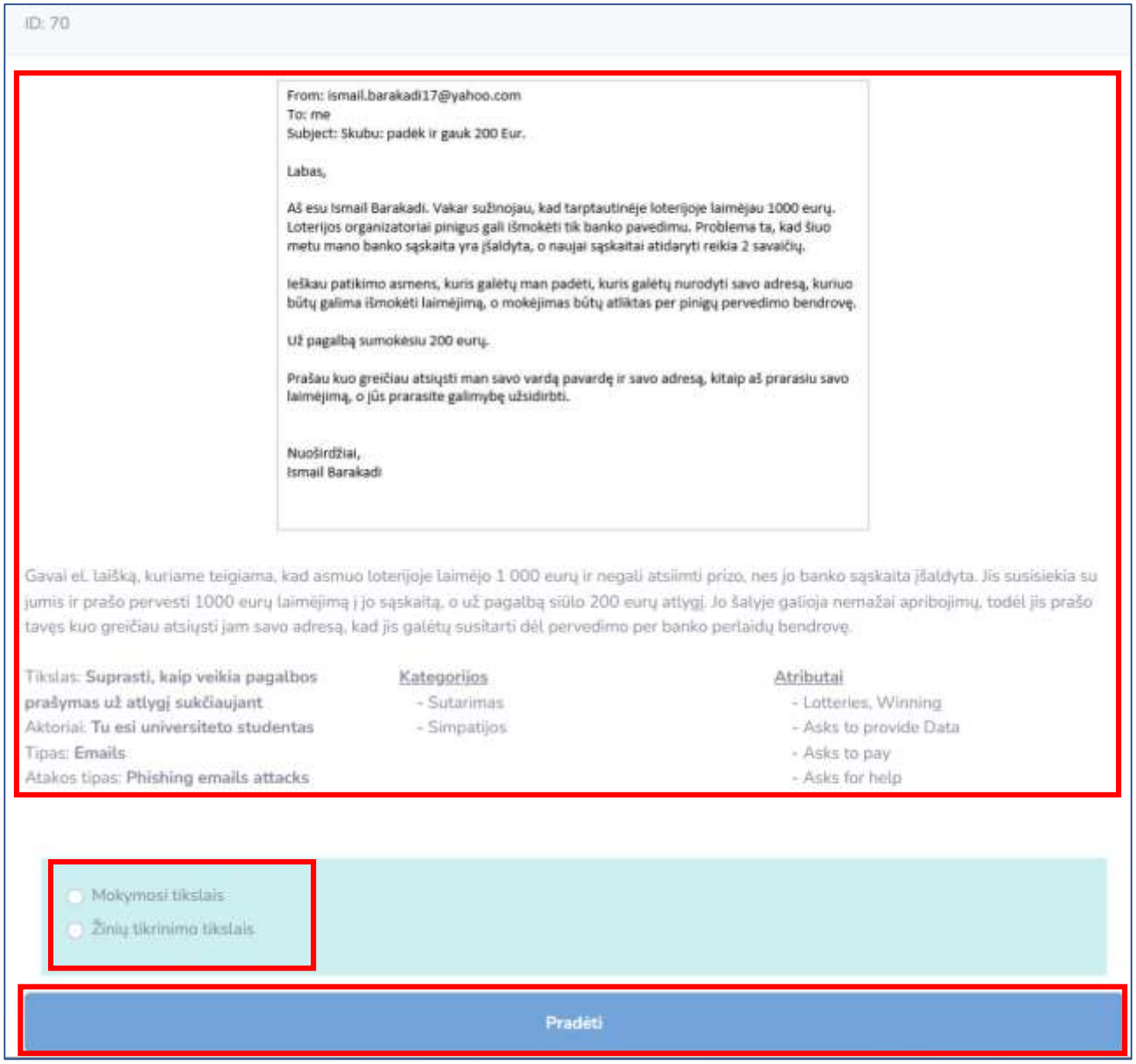


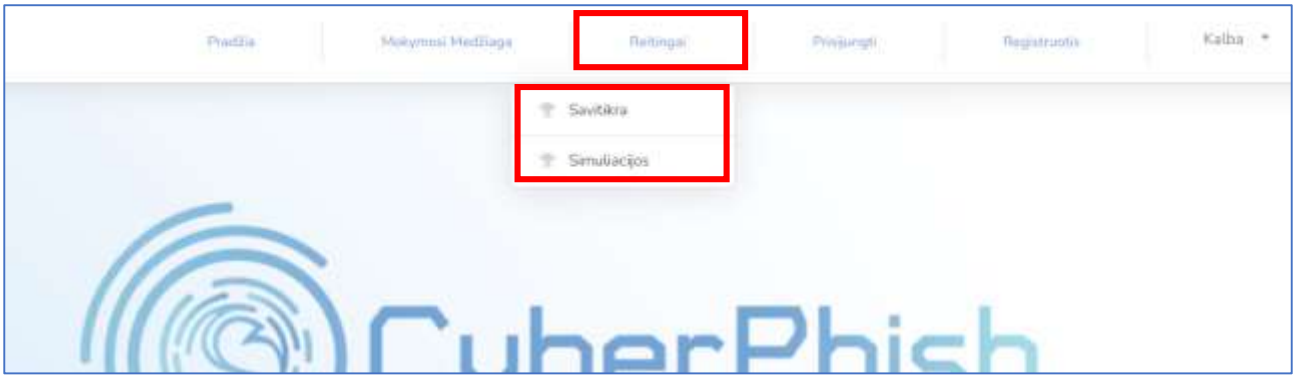
Pasirinkus simuliaciją matysite situacijos aprašymą. Prieš pradėdami turite pasirinkti, ar norite spręsti **Mokymosi tikslais**, ar **Žinių tikrinimo tikslais**.

Jei pasirinksite **Mokymosi tikslais**, po kiekvieno atsakyto klausimo matysite grįžtamąjį ryšį.

Jei pasirinksite **Žinių tikrinimo tikslais**, grįžtamąjį ryšį matysite tik pabaigę simuliaciją.

Spustelėkite mygtuką **Pradėti**.



Vartotojo reitingai

Ši parinktis vartotojus išrikiuoja pagal geriausius **Savitikros testų** ir **Simuliacijų** rezultatus. Naudotojų reitingus galite pasiekti puslapio viršuje spustelėję **Reitingai** ir pasirinkę **Savitikra** arba **Simuliacijos**.