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

A1: Metodinės rekomendacijos mokymų vadovams / mentoriams

Projekto trukmė: 2020 lapkritis – 2022 lapkritis

Projekto Nr.: 2020-1-LT01-KA203-078070

Funded by the
Erasmus+ Programme
of the European Union

Projektas finansuojamas Europos Komisijos lėšomis. Leidinyje atspindimos tik autoriaus pažiūros, Komisija negali būti laikoma atsakinga už jame pateikiamą informaciją.

Turinys

APIE PROJEKTĄ

Sukčiavimas pastaruoju metu yra viena didžiausių problemų, nes kibernetiniai nusikaltėliai sukčiavimo kampanijoms vykdyti naudoja vis greitesnes ir pažangesnes technologijas. Norint didinti žmonių sąmoningumą apie sukčiavimą internete, reikia šviesti naudotojus, kad jie galėtų atpažinti sukčiavimo atakas ir tinkamai į jas reaguoti.

Projekto tikslas yra edukuoti aukštųjų mokyklų studentus, pedagogus, universiteto darbuotojus (bendruomenės narius), suaugusiųjų švietimo centrus ir verslo sektorius bei skatinti tikslinės grupės kritinį mąstymą kibernetinio saugumo srityje.

Projekto partneriai sukūrė mokymo programą, el. mokymosi medžiagą, mišrią mokymosi aplinką, savitikros testus žinių įsivertinimui bei žinių patikrinimo testus, simuliacijų scenarijus studentams ir kitiems naudotojams, gaires mokymų vadovams / mentoriams bei rekomendacijas, kaip įsidiegti mokymo kursą, siekiant apsisaugoti nuo sukčiavimo atakų, įgyti kompetencijų, kurios padės atkreipti dėmesį į grėsmes ir imtis reikiamų prevencijos priemonių.

Pagrindiniai intelektiniai rezultatai:

1. Tyrimo analizė ir rekomendacijos: Išvengti sukčiavimo atakų ir tobulinti kritinį mąstymą;
2. Kurso programa;
3. Internetinė mokymosi medžiaga;
4. Simuliacijos;
5. Savęs vertinimo bei žinių vertinimo sistema;
6. Metodinės rekomendacijos mokymų vadovams / mentoriams ir modulio įgyvendinimui.

MOKYMO ORGANIZAVIMO GAIRĖS

Šioje dalyje pateikiami pasiūlymai ir rekomendacijos, kaip organizuoti mokymus „CyberPhish“ kurso dalyviams.

„Cyberphish“ kursas gali būti organizuojamas taikant mišriojo mokymosi būdą, derinant nuotolinio ir kontaktinio mokymo metodus. Tai reiškia, kad žinių ir įgūdžių įgijimo procesas grindžiamas ir tiesioginiu, ir nuotoliniu mokymu: dėstytojo vedami seminarai, savarankiškas dalyvių darbas naudojantis internetine mokymosi medžiaga ir grupinio bendradarbiavimo praktikos.

Svarbu, kad dalyviai bet kuriuo mokymosi proceso metu (išskyrus galutinį žinių įvertinimą) galėtų sulaukti dėstytojo pagalbos, t. y. galėtų užduoti rūpimus klausimus, prašyti pagalbos, jei nepavyksta ar nesupranta, kaip atlikti užduotį, ir gauti dėstytojų pagalbą bei grįžtamąjį ryšį.

Tikslinė grupė. Šio projekto pagrindinė tikslinė grupė yra aukštųjų mokyklų studentai. Pilotinių mokymų metu buvo atrinkti studentai iš įvairių studijų programų. Jie naudojo pažangią mokymo medžiagą, praktiškai išbandė simuliacijas – sukčiavimo atakų imitacijas ir laikė savitikros bei žinių vertinimo testus, kad nustatytų savo žinių lygį prieš mokymus ir po jų. Kurso dalyviai turėtų turėti pagrindinius skaitmeninio raštingumo įgūdžius. Kitų išankstinių reikalavimų studentų žinioms ar įgūdžiams nėra.

Dėstytojai taip pat gali naudotis modernia mokymo programa, paremta naujausiais šalių partnerių moksliniais tyrimais, savo srities ekspertų parengta e. mokymosi medžiaga, praturtinta studentams skirtomis užduotimis, nuorodomis į papildomus skaitinius (naujausią literatūrą) bei vaizdo įrašus. Tokiu būdu jie gali atnaujinti ir patobulinti savo turimas žinias. Taip pat internetinėje aplinkoje dėstytojai gali susipažinti su inovatyviais mokymo ir mokymosi metodais, tokiais kaip savitikros bei žinių įvertinimo testai bei simuliacijos, kurios patraukliai ir žaismingai imituoja realaus gyvenimo situacijas.

Kiti projekto naudos gavėjai: pedagogai, universitetų darbuotojai, švietimo centrai ir verslo sektorius (darbdaviai ir darbuotojai). Jie taip pat gali gauti naudos – praplėsdami ir pagilindami savo turimas žinias bei kompetencijas, galės jaustis saugesni internete, išvengti jautrios ir (arba) asmeninės informacijos nutekėjimo, išvengti finansinių nuostolių tiek asmeniškai, tiek savo organizacijose.

Pagrindinė tikslinė grupė	AUKŠTŲJŲ MOKYKLŲ STUDENTAI

- Naudojasi sukurta e. mokymosi medžiaga
- Sprendžia simuliacijas
- Atlieka savitikros ir žinių vertinimo testus

Antrinė tikslinė grupė	MOKYMŲ VADOVAI / MENTORIAI

- Prieina prie sukurtos modernios kurso programos ir e. mokymosi medžiagos
- Sužino apie inovatyvius mokymo ir mokymosi metodus, tokius kaip savęs bei žinių įvertinimas, simuliacijos

Kitos tikslinės grupės	PEDAGOGAI, UNIVERSITETŲ DARBUOTOJAI, UNIVERSITETŲ PERSONALAS, ŠVIETIMO CENTRAI IR VERSLO SEKTORIUS (DARBDAVIAI IR DARBUOTOJAI)

- Prieina prie sukurtos e. mokymosi medžiagos
- Pagilina turimas žinias ir kompetencijas kibernetinio saugumo srityje

Paveikslas 1. Projekto tikslinės grupės

Mokymo trukmė. Rekomenduojama mokymo trukmė – 4-6 savaitės. Visa mokymo programa trunka 30 valandų, tai atitinka 1 ECTS. Siūloma tokį patį valandų skaičių kiekvienam moduliui skirti savarankiškam mokymuisi ir įsivertinimui. Rekomenduojama, kad kursų metu dalyviai per savaitę skirtų 2-3 valandas (mokymo medžiagos skaitymui, testų ir scenarijų sprendimui).

Numatoma mokymo trukmė gali skirtis priklausomai nuo mokymo. Pateiktos temos ir pratimai / scenarijai suskirstyti į vienos dienos sesijas. Skiriamas laikas yra lankstus, todėl tikslus kiekvienos dienos tvarkaraštis nepateikiamas.

Mokymų vadovas / mentorius turėtų iš anksto peržiūrėti medžiagą ir suplanuoti laiką taip, kad jis atitiktų konkrečius mokymo poreikius.

Kurso struktūra. Kursų programą sudaro keturios dalys:

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.

1. Kibernetinio saugumo įvadas	•Šiame modulyje pristatomi kibernetinių atakų iššūkiai, su kuriais susiduria įmonės 4sios Pramonės revoliucijos amžiuje, pavyzdžiui, plačiai naudojamos mobiliosios technologijos, debesų kompiuterija, daiktų internetas (IoT) ir didieji duomenys, trečiųjų šalių keliama rizika ir augančios grėsmės, įskaitant nacionalinių valstybių grėsmes. Šioje dalyje taip pat pateikiamos kibernetinio saugumo srityje naudojami pibrėžimai.
2. Kibernetinė sauga Europos Sąjungoje (ES)	•Šiame modulyje pristatoma esama ES politika ir iniciatyvos, kuriomis siekiama skatinti kibernetinio saugumo koncepciją. Jame taip pat aptariami teisiniai kibernetinio saugumo aspektai ES ir pasaulyje.
3. Kibernetinės atakos: socialinė inžinerija ir sukčiavimas (*angl*. Phishing)	•Šiame modulyje supažindinama su kibernetinėmis atakomis, ypatingą dėmesį skiriant sukčiavimui (*angl*. Phishing). Jame taip pat išsamiai aptariama socialinės inžinerijos ir atvirkštinės socialinės inžinerijos sąvokos bei glaudus socialinės inžinerijos ryšys su kibernetinėmis atakomis. Modulyje taip pat pristatomos įvairių tipų sukčiavimo atakos ir metodai, taip pat pateikiami realūs pavyzdžiai.
4. Kibernetinių atakų atpažinimas ir apsauga	•Šiame modulyje daugiausia dėmesio skiriama e. saugumo koncepcijai ir aktyvaus požiūrio į kibernetines grėsmes svarbai taikant kibernetinės higienos koncepciją. Jame taip pat pateikiamas išsamus požiūris į tai, kaip atpažinti ir valdyti kibernetines atakas, rengti ir įgyvendinti reagavimo į incidentus planus, kad būtų sumažintas kibernetinių atakų poveikis.

Paveikslas 2. Mokymo kurso struktūra

Išsamią mokymo programą galima rasti projekto svetainėje www.cyberphish.eu

Trumpoji mokymo programos versija: https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A1_EN_Cyberphish-Short-Curriculum-Final.pdf

Pilnoji versija: https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EN_Cyberphish-Full-Curriculum-Final.pdf

BENDROJI MOKYMO TVARKA

Ši dalis skirta mokymo organizavimui. Čia taip pat pateikiamos gerosios praktikos rekomendacijos, kurios buvo naudotos pilotinių mokymų metu, įskaitant klausimyną prieš mokymus, reikalavimus dalyvių registracijai, mokymosi proceso ir žinių patikrinimo sąlygas.

Kvietimas į mokymus

Tarkime, kad mokymai organizuojami kaip atskiras kursas, neįtrauktas į aukštosios mokyklos mokymo programą. Tokiu atveju rekomenduojama interneto svetainėje ir (arba) socialiniuose tinkluose paskelbti pranešimą, kviečiantį į pilotinius mokymus, arba išsiųsti asmeninį kvietimą potencialiems dalyviams el. paštu. Šiame kvietime potencialus dalyvis informuojamas apie pagrindinį mokymo tikslą, kursų trukmę, įgyjamą kompetenciją atpažinti sukčiavimo atakas, ir sertifikavimą baigus mokymo kursą. Jame taip pat gali būti nuoroda į registracijos formą.

Kvietimo pavyzdys pateikiamas 1 priede. Failai ppt ir pdf formatais pateikiami https://wiki.cyberphish.eu/.

Įvadinis susitikimas

Kurso pradžioje, pirmojo susitikimo metu, svarbu sukurti pasitikėjimą tarp mokymų vadovo / mentoriaus ir dalyvių, motyvuoti juos ir leisti jiems susipažinti vieniems su kitais. Supažindinkite su konsultacijos forma (gyvai / nuotoliniu būdu) ir dažnumu, pavyzdžiui, kas savaitę, tris kartus per kursą (pradžioje, pabaigoje ir viduryje). Rekomenduojama paminėti problemas, kurios gali iškilti registruojantis platformoje (pvz., į nepageidaujamų laiškų aplanką patekęs patvirtinimo el. laiškas).

Susitikimo metu dalyviams paaiškinama, kaip naudotis e-mokymosi aplinka, leidžiama ją išbandyti ir kviečiama pasidalyti iškilusiais klausimais, kad vėliau, prasidėjus kursui, nekiltų neaiškumų. Susitikime taip pat pristatomas „CyberPhish“ mokymo kursas.

Klausimynas prieš mokymus

Siekiant įvertinti mokymo poveikį dalyvių žinių pažangai, prieš pradedant mokymus rekomenduojama naudoti klausimyną. Pilotinių mokymų metu partneriai naudojo klausimyną iš 20 klausimų. Klausimynas buvo parengtas anglų kalba ir lokalizuotas partnerių šalių kalbomis: estų, graikų, latvių ir lietuvių.

Klausimai buvo atrinkti iš savitikros klausimų (20 iš 60). Visiems dalyviams buvo pateikti tie patys klausimai, tačiau skirtinga tvarka. Šis klausimynas neturi įtakos dalyvio rezultatams, tačiau leidžia įvertinti dalyvio žinių pokytį.

Klausimyno pildymas trunka nuo 20 iki 25 minučių. Prieš pateikdami klausimyną dalyviai turi nurodyti savo el. pašto adresą. Rekomenduojama naudoti tą patį el. pašto adresą, koks buvo naudojamas registruojantis į kurso e-mokymosi aplinką (https://cyberphish.vuknf.lt/). Dalyviai turėtų būti informuojami, kad jie turi naudoti galiojantį el. pašto adresą. Mokymosi aplinkoje turi būti naudojamas tas pats el. pašto adresas, kuris nurodytas dalyvio registracijos formoje.

Reikėtų pažymėti, kad klausimynas prieš mokymus nėra privalomas. Tai tik rekomendacija, tačiau šia praktika galima pasinaudoti, jei norite įvertinti mokymų poveikį dalyviams.

Nuotolinis mokymas

Po trumpo įvado prasideda nuotolinis mokymas, kuris trunka apie mėnesį (4-6 savaites). Mokymo proceso metu dalyviai dalyvauja įvairioje mokymosi veikloje, naudodami įvairius mokymo metodus ir formas, kurios apima, el. mokymo medžiagos studijavimą, papildomos medžiagos skaitymą, su temomis susijusių vaizdo įrašų žiūrėjimą, savitikros ir žinių vertinimo testų atlikimą, simuliacinių užduočių sprendimą. Per šį laiką dalyviai sužino apie kibernetinį saugumą, supranta kibernetines atakas ir socialinę inžineriją, išmoksta atpažinti pagrindinius sukčiavimo (*angl*. phishing) požymius, supranta, kaip elgtis su kibernetinėmis atakomis, išmoksta sumažinti žalą reaguojant į incidentus. Sėkmingas dalyvavimas mokymuose priklauso nuo dalyvio gebėjimo pačiam planuoti savo laiką ir veiklą, taip pat nuo bendradarbiavimo su CyberPhish mokymų vadovu bei kitais komandos nariais.

Po mokymų turėtų būti sėkmingai išlaikytas žinių vertinimo testas (t. y. surinkta ne mažiau kaip 75 % taškų) ir išduotas automatiškai sugeneruotas pažymėjimas. Mokymų pabaigoje dalyviai įgyja naujų žinių ir įgūdžių, kuriuos gali panaudoti kasdieniame gyvenime (pavyzdžiui, ieškodami informacijos internete, asmeniškai bendraudami socialiniuose tinkluose, kalbėdami telefonu su nepažįstamais žmonėmis, mokydamiesi, darbo vietoje ir t. t.). Be to, jie įgyja didesnį pasitikėjimą savimi.

E-mokymosi aplinkos struktūra

Mokymosi platforma https://cyberphish.vuknf.lt/ suteikia atvirą prieigą prie mokomosios medžiagos. Medžiagą gali laisvai studijuoti visi norintys asmenys. Registruotis nereikia. Tačiau norint spręsti simuliacijas, kuriose mokoma, kaip atpažinti sukčiavimo atakas, atlikti savikontrolės testus, žinių vertinimo testą ir gauti sertifikatą, būtina būti registruotu naudotoju.

Mokymo medžiaga. Spustelėjęs meniu juostoje esantį mygtuką „Mokymosi medžiaga“, naudotojas kairėje ekrano pusėje mato kurso modulius. Yra keturi moduliai: kibernetinio saugumo įvadas; kibernetinė sauga Europos Sąjungoje (ES); kibernetinės atakos: socialinė inžinerija ir sukčiavimas (*angl*. Phishing); kibernetinių atakų atpažinimas ir apsauga. Kiekvieną modulį sudaro kelios temos. Pasirinkus temą, ekrano viduryje rodoma mokymosi medžiaga. Naudotojas gali atsisiųsti medžiagą į savo kompiuterį, spustelėjęs nuorodą „Atsisiųsti skaidres“.

Savitikros testai. Registruoti naudotojai turi daugiau galimybių. Jie turi galimybę mokymosi tikslais atlikti savitikros testus. Mygtukas *„Savitikros testas“* atsiranda, kai dalyvis išmoksta modulio medžiagą. Todėl dalyvis, susipažinęs su kiekviena modulio tema, turi spustelėti mygtuką *„Pažymėti kaip atliktą!”.* Kai visos modulio temos pažymėtos kaip *„Atlikta!*“, reiškia, kad to modulio medžiaga išmokta, tuomet galima atlikti savitikros testą, paspaudus mygtuką *„Savitikros testas*“. Testo metu dalyviui pateikiami penki atsitiktiniai klausimai iš to modulio.

Atlikus testą sistema parodo testo rezultatus: pasirinktus atsakymus, teisingus ir neteisingus atsakymus, testo sprendimo laiką ir surinktus taškus. Dalyvis gali pakartoti testą spustelėjęs mygtuką *„Atlikti iš naujo*“. Pakartotinai atliekant testą pateikiami penki atsitiktiniai klausimai iš to mdulio. Savitikros testą galima atlikti neribotą skaičių kartų.

Simuliacijos. Registruoti dalyviai gali spręsti simuliacijas. Simuliacija yra tikrų situacijų imitacija. Kairėje ekrano pusėje virš modulio temų yra mygtukas *„Simuliacijos*“. Registruotas mokymų dalyvis gali jas spręsti bet kuriuo metu. Simuliacijos suskirstytos į 7 grupes: Vienybė (Unity), Simpatijos (Liking), Sutarimas/ konsensusas (Consensus),

Nuoseklumas (Consistency), Autoritetas (Authority), Trūkumas/ stygius (Scarcity) and Apsikeitimas (Reciprocation). Pasirinkus simuliaciją, pateikiamas situacijos aprašymas ir galimi jos sprendimo variantai. Simuliacijos veikia dviem rėžimais: mokymosi ir žinių patikrinimo. Pirmu atveju (pasirinkus spręsti mokymosi tikslu), dalyvis pasirinkęs galimą situacijos sprendimo variantą, gauna grįžtamąjį ryšį, o simuliacijos pabaigoje mato surinktus balus ir bendrą išvadą. Antru atveju (sprendžiant simuliaciją žinių patikrinimo tikslu), dalyvis gauna grįžtamąjį ryšį tik simuliacijos pabaigoje. Mokymų vadovas / mentorius turėtų nuspręsti, kiek simuliacijų dalyvis turi išspręsti. Pavyzdžiui, pilotinių mokymų metu kiekvienas dalyvis turėjo išspręsti ne mažiau kaip 20 pasirinktų simuliacijų.

Žinių tikrinimo testas. Registruoti dalyviai gali atlikti baigiamąjį žinių patikrinimo testą ir gauti sertifikatą. Mygtukas *„Žinių tikrinimo testas“* pasirodo kairėje ekrano pusėje virš kurso modulių, kai dalyvis išmoksta visą medžiagą ir pažymi visas temas kaip atliktas. Testas laikomas išlaikytu, jei surenkama ne mažiau kaip 75 % taškų. Dalyviai, išlaikę baigiamąjį gauna elektroninį pažymėjimą. Jei dalyvis neišlaiko testo, jis gali pakartoti temas ir, skyręs daugiau laiko mokymuisi, pakartotinai laikyti žinių patikrinimo testą. Šį testą galima laikyti tris kartus.

Reitingai. Tam, kad mokymosi procesas būtų patrauklesnis, sistema apskaičiuoja įvertinimus/ reitingus. Kurso dalyvis savo įvertinimą/ reitingą, surinktus ženkliukus (bedžus) ir taškus gali matyti bendroje įvertinimų lentelėje, kuri pasiekiama per meniu punktą *„Reitingai“*, esantį ekrano viršuje. Dalyvio simuliacijų reitingas apskaičiuojamas susumuojant geriausius visų išspręstų simuliacijų rezultatus. Atitinkamai dalyvio savitikros testo įvertinimas apskaičiuojamas susumuojant visų atliktų savitikros testų geriausius rezultatus.

Kurso progresas. Dalyvis taip pat gali matyti savo mokymosi pažangą. Kurso progresas rodomas virš kurso modulių kairėje ekrano pusėje, o taip pat ir per naudotojo meniu ekrano viršuje. Per naudotojo meniu dalyvis gali pakeisti naudotojo vardą ir slaptažodį, matyti surinktus ženkliukus (bedžus), savitikros testų istoriją ir simuliacijų istoriją.

Sertifikatai. Visiems dalyviams, kurie baigė kursą ir išlaikė žinių įvertinimo testą surinkdami ne mažiau kaip 75 % taškų, automatiškai sugeneruojami sertifikatai (PDF formatu). Sertifikato pavyzdys pateikiamas 2 priede. Užbaigus „CyberPhish“ kursą akademiniai kreditai nesuteikiami.

Prieinamumas

Internetinis mokymo kursas sukurtas penkiomis kalbomis — anglų, estų, graikų, latvių ir lietuvių. Jis pasiekiamas adresu https://cyberphish.vuknf.lt/. Žemiau esančiame paveiksle vaizduojamas pagrindinis mokymosi aplinkos langas.

Paveikslas 3. Mokymosi aplinkos pagrindinis langas

Pilotinių mokymų gerosios praktikos rekomendacijos. Rekomenduojama parengti taisykles ir instrukcijas mokymų dalyviams. Klausimynai kurso pradžioje ir pabaigoje nėra privalomi. Kitos priemonės taip pat gali būti naudojamos, kaip ir įprastiniuose mokymuose.

Instrukcijos mokymų dalyviams

Toliau pateikiami rekomenduojami žingsniai/ etapai organizuojant CyberPhish mokymus:

1 žingsnis. Užpildyti klausimyną prieš mokymus. Prieš mokymus užpildykite klausimyną. Pateikite galiojantį savo el. pašto adresą, kuris taip pat bus naudojamas ir e-mokymosi aplinkoje.

2 žingsnis. **Užsiregistruoti e-mokymosi aplinkoje**. Užsiregistruokite e-mokymosi aplinkoje adresu https://cyberphish.vuknf.lt/login, naudodami tą patį el. pašto adresą, kurį nurodėte pildydami klausimyną.

Pastaba: negavus patvirtinimo el. laiško iš e-mokymosi sistemos, reikia patikrinti nepageidaujamų laiškų aplanką. Patvirtinimo laiškas galėjo atsidurti nepageidaujamų laiškų / šiukšlių aplanke.

3 žingsnis. Prisijungti prie e-mokymosi aplinkos. Prisijunkite adresu https://cyberphish.vuknf.lt, naudodami asmeninius prisijungimo duomenis.

4 žingsnis. Mokomosios medžiagos studijavimas. Prisijungę išstudijuokite visą mokomąją medžiagą, t. y. keturias temas ir potemes (žr. žemiau). Peržiūrėję kiekvieną temą, paspauskite mygtuką *„Pažymėti kaip atliktą*".

Temos ir potemės:

1. Kibernetinio saugumo įvadas
   1.1. Ketvirtosios pramonės revoliucijos iššūkiai
   1.2. Kibernetinio saugumo istorija
   1.3. Kibernetinio saugumo apibrėžimai
2. Kibernetinė sauga Europos Sąjungoje (ES)
   2.1. Kibernetinio saugumo skatinimas Europos Sąjungoje;
   2.2. Teisiniai kibernetinio saugumo aspektai
   2.3. Tendencijų ir kibernetinio saugumo situacijos apžvalga
3. Kibernetinės atakos: socialinė inžinerija ir sukčiavimas (*angl*. phishing)
   3.1. Kibernetinių atakų įvadas
   3.2. Socialinė inžinerija ir manipuliavimas
   3.3. Skirtingi sukčiavimo atakų tipai ir kategorijos
   3.4. Atvejų analizė
4. Kibernetinių atakų atpažinimas ir apsauga
   4.1. Bazinės e-Saugumo žinios
   4.2. Prevencinės priemonės
   4.3. Kibernetinių atakų atpažininmas
   4.4. Kibernetinių atakų valdymas
   4.5. Žalos sumažinimas pasinaudojant incidento valdymo planu

5 žingsnis. Spręsti keturis savitikros testus. Išmokę kiekvieną temą, išspręskite savitikros testą.

6 žingsnis. Spręsti simuliacijas. Mokymosi metu spręskite simuliacijas kaip mokymosi proceso dalį.

7 žingsnis. Spręskite žinių patikrinimo testą. Išspręskite baigiamąjį žinių patikrinimo testą surinkdami ne mažiau kaip 75% taškų.

8 žingsnis. Išlaikę baigiamąjį žinių patikrinimo testą, užpildykite mokymų dalyviams skirtą **klausimyną po mokymų** apie pilotinius mokymus.

Pastaba: ši priemonė buvo naudojama pilotinių mokymų metu, tačiau galima naudoti ir kitas priemones, kaip ir įprastuose mokymuose.

Baigiamasis susitikimas

Baigiamasis susitikimas turi kelis tikslus: pirma, jo metu dalyviai gali užpildyti klausimyną apie pilotinius mokymus, antra – dalyviai gali išsakyti savo nuomonę apie mokymo kursą. Galiausiai galima aptarti žinių vertinimo testo eigą, iškilusius sunkumus ir iššūkius atsakant į testo klausimus bei kitus klausimus, susijusius su mokymais.

Klausimynas po mokymo kurso

Pilotinių mokymų metu dalyvių, išlaikiusių galutinį žinių patikrinimo testą, buvo paprašyta užpildyti **klausimyną apie mokymus**. Klausimyną sudaro punktai, kuriuose prašoma pateikti bendrojo pobūdžio informaciją (pavyzdžiui, el. pašto adresą, lytį, profesiją) ir klausimai dalyviui apie savo žinių vertinimą pabaigus „CyberPhish" mokymo kursą. Prašoma įvertinti savo patirtį naudojant simuliacijas, užduodami klausimai apie kurso tikslus, nuotolinio formato metodo tinkamumą, kurso turinį, trukmę, mokymą ir pagalbą kurso metu, mokymosi platformos patogumą. Klausimyno pavyzdys pateikiamas 3 priede.

Pasibaigus pilotiniams mokymams kurso mentorių /mokymų vadovų taip pat buvo paprašyta užpildyti jiems skirtą klausimyną. Klausimyną sudaro punktai, kuriuose prašoma pateikti bendrą informaciją, pavyzdžiui, el. paštą, vardą, pavardę, šalį, taip pat klausimai apie kurso struktūrą ir turinį, trukmę, temų atitikimą tikslinei auditorijai, kurso temų

išsamumą, kiek kursas pasiekė savo tikslą supažindinti besimokančiuosius su kibernetiniu saugumu ir sukčiavimu. Klausimyno pavyzdys pateikiamas 4 priede.

DARBAS SU E-MOKYMOSI APLINKA

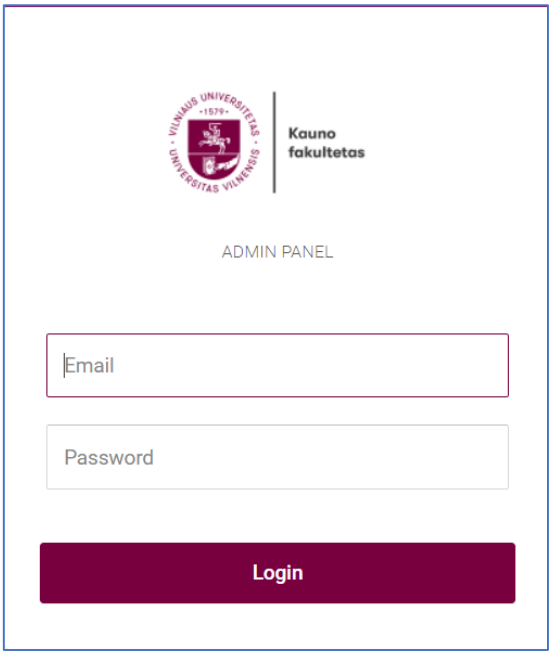
E-mokymosi aplinka pasiekiama adresu https://cyberphish.vuknf.lt. Čia patalpinta mokymosi medžiaga prieinama visiems lankytojams ir yra nemokama. Mokymosi medžiaga pateikiama penkiomis kalbomis: anglų, estų, graikų, latvių, ir lietuvių kalbomis. Neregistruoti lankytojai gali tik peržiūrėti mokymosi medžiagą, tačiau jie negali atlikti savitikros testų, žinių patikrinimo testų, pelnyti ir rinkti ženkliukų, vykdyti simuliacijų ar gauti sertifikatų. Norint tapti registruotu svetainės lankytoju, reikia joje užsiregistruoti.

Vartotojo vadovas pateikiamas dokumente **User_Manual_for_training-Participants.pdf** adresu https://wiki.cyberphish.eu/. Šiame dokumente aprašoma, kaip naudotis šia mokymosi platforma.

Mokytojo aplinka

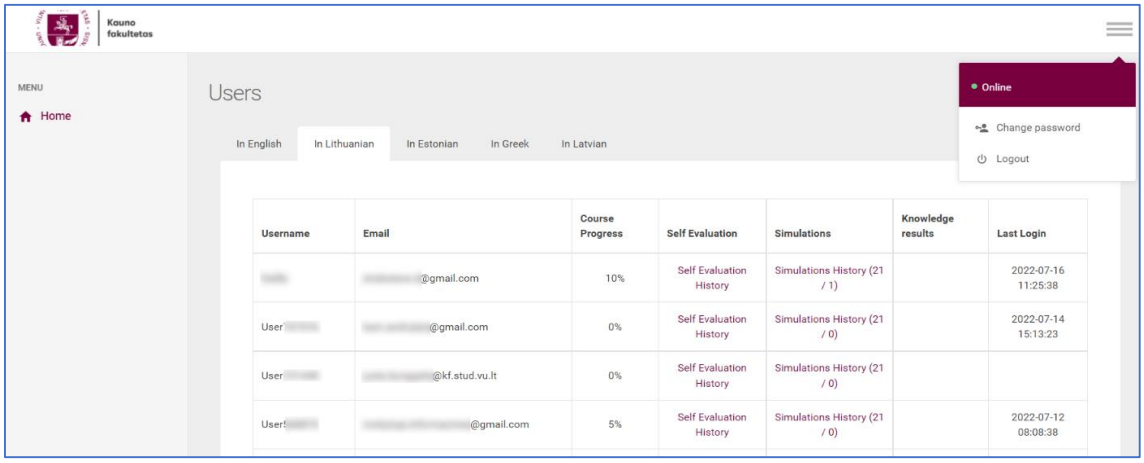
Mokytojo aplinkoje galima stebėti mokymosi sistemoje užsiregistravusius dalyvius, jų mokymosi pažangą procentine išraiška, atliktų savitikros testų istoriją, simuliacijų istoriją, žinių patikrinimo įvertinimus, paskutinio prisijungimo datą ir laiką.

Prisijungimo prie mokytojo aplinkos adresas: https://cyberphish.vuknf.lt/admin-panel. Prisijungimo langas pateikiamas žemiau:



Paveikslas 4. Mokytojo aplinkos prisijungimo langas

Įvedus mokytojo prisijungimo duomenis, sistema pateikia dalyvių sąrašą. Mokytojas gali stebėti dalyvių mokymosi pažangą pagal kalbas (anglų, lietuvių, estų, graikų ir latvių). Žemiau pateikiamas pagrindinio mokytojo aplinkos lango pavyzdys.



Paveikslas 5. Pagrindinis mokytojo aplinkos langas

Savitikros testų istorija

Pasirinkus dalyvį ir jo savitikros testų istoriją, sistema pateikia detalią informaciją: spręstų testų pradžios ir pabaigos datas ir laikus, surinktus taškus, potemes, teisingų atsakymų skaičių.

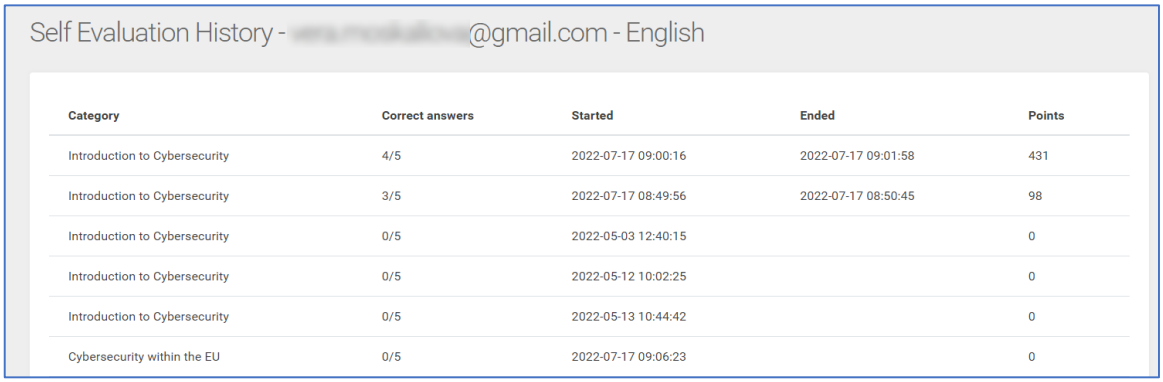
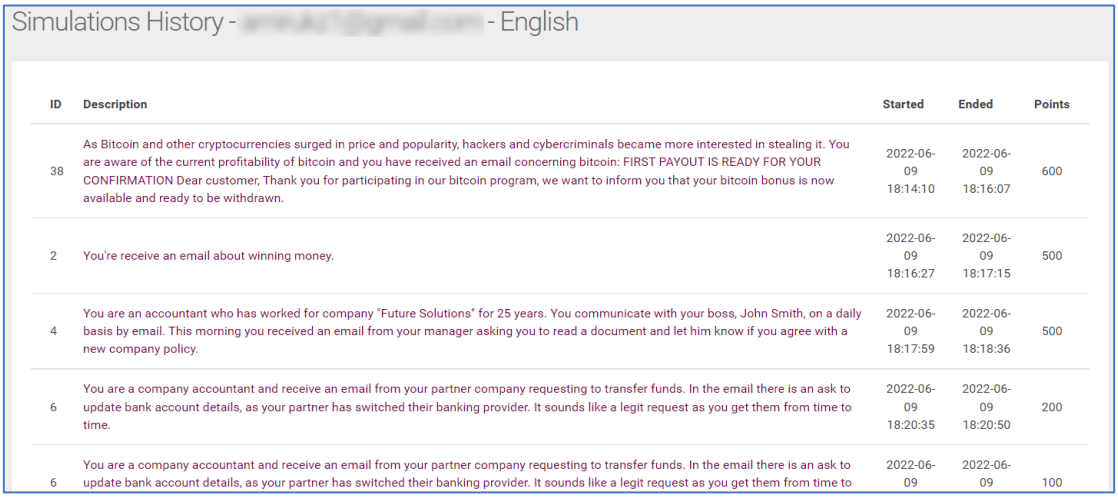


Figure 6 Dalyvio spręstų savitikros testų istorija

Simuliacijų istorija

Pasirinkus dalyvį ir jo simuliacijų istoriją sistema pateikia informaciją apie spręstas simuliacijas, sprendimo pradžios ir pabaigos datas ir laikus, surinktus taškus.



Paveikslas 7. Dalyvio spręstų simuliacijų istorija

DARBAS SU INOVATYVIAIS METODAIS (SIMULIACIJOS, PASKAITOS, SEMINARAI, PRAKTINIAI MOKYMAI, INTERNETO PRIEMONIŲ NAUDOJIMAS IR T. T.)

Simuliacija imituoja tikras sukčiavimo atakas, pateikdama naudotojui procesą žaisminga forma.

Pagrindinis simuliacijos tikslas – padėti žmonėms pagerinti kritinį mąstymą, susijusį su kibernetiniu saugumu ir sukčiavimu, atpažįstant sukčiavimo, nepageidaujamų elektroninių laiškų, kibernetinių patyčių ir kitus atvejus. Remiantis IO1 buvo parengtos rekomendacijos simuliacijoms – daugiausia dėmesio skirta realių atvejų analizei, jų pritaikymui mokymosi procesui.

Simuliaciją sudaro situacijos aprašymas, tikslas, veikėjai, atakos tipas ir keli (3-4) atsakymų variantai vartotojo elgesio pasirinkimui. Simuliacijos skirtos įvertinti galimą / tikėtiną naudotojo elgesį, jo galimus svarstymus / nuogąstavimus ir sprendimus tokioje situacijoje. Pateiktas simuliacijas sudaro trys lygmenys. Pasirinkus vieną iš problemos / situacijos variantų, paveikiami ir pateikiami kiti galimi sprendžiamo atvejo variantai.

Sukurtos simuliacijos veikia dviem režimais: mokymosi tikslais ir žinių patikrinimo tikslais. Sprendžiant simuliaciją mokymosi tikslais, simuliacijos pabaigoje studentas mato surinktus balus ir bendrą išvadą. Sprendžiant simuliaciją žinių patikrinimo tikslais, studentas mato simuliacijos metu padarytus pasirinkimus ir simuliacijos pabaigoje gauna grįžtamąjį ryšį su komentarais. Jei simuliacija buvo išspręsta neteisingai, naudotojui rekomenduojama simuliaciją spręsti iš naujo.

IŠVADOS IR REKOMENDACIJOS

Šis dokumentas skirtas visiems mokymų vadovams ir mentoriams, kurie konsultuoja bei moko studentus. Projekto konsorciumas tikisi, kad jie ras naudingų patarimų, kaip naudotis sistema ir kaip rengti mokymus žmonėms, norintiems sužinoti apie kibernetines atakas, ypač apie sukčiavimą (*angl*. phishing) ir socialinę inžineriją, taip pat norintiems išmokti atpažinti pagrindinius tokių grėsmių požymius. Iš potencialių vartotojų reikalaujama turėti skaitmeninio raštingumo pagrindus. Kitų išankstinių reikalavimų vartotojo žinioms ar įgūdžiams nėra.

Projekto partnerių 2020 metais atliktas tyrimas Estijoje, Kipre, Latvijoje, Lietuvoje ir Maltoje parodė, kad studentams ir darbuotojams trūksta žinių apie sukčiavimą, socialinę inžineriją, kibernetines atakas ir duomenų saugumą (žr. https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EN_CYBERPHISH-REPORT_survey-results.pdf). Tai lemia ne tik asmeninių duomenų ir asmeninių finansų praradimą sukčiavimo ar kibernetinės atakos atveju, bet ir konfidencialios informacijos bei įmonių / organizacijų finansinių išteklių praradimą.

Remiantis su kibernetiniu saugumu susijusių aukštojo mokslo mokymo programų ir privačių bendrovių vykdomų kibernetinio saugumo mokymo programų analize šalyse partnerėse (žr. https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A2_EN_CYBERPHISH-REPORT_study-analysis.pdf) konsorciumas parengė mokymo programą, apimančią keturis modulius:

- Kibernetinio saugumo įvadas;
- Kibernetinė sauga Europos Sąjungoje (ES);
- Kibernetinės atakos: socialinė inžinerija ir sukčiavimas (*angl*. Phishing);
- Kibernetinių atakų atpažinimas ir apsauga.

Daugiau informacijos apie tai, kaip parengti būsimuosius Cyberphish kurso lektorius/ mentorius, pateikta pilnojoje „CyberPhish“ kursų mokymo programoje (žr. https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EN_Cyberphish-Full-Curriculum-Final.pdf).

Pilotinių mokymų dalyviai gerai įvertino „CyberPhish“ mokymo kursą. Jie pripažino, kad jis naudingas tiek paprastų vartotojų, tiek įmonių darbuotojų kasdienėje su IT susijusioje veikloje. Daugiau informacijos bus pateikta ataskaitoje IO6 A2: Kurso įgyvendinimo gairės.

Mokymo medžiaga internetinėje mokymo aplinkoje pateikiama PDF formatu – glaustai ir aiškiai, neapkraunant mokymų dalyvių gausiu skaitymu. Norintiems daugiau sužinoti apie konkrečią temą ar potėmę, kiekvieno PDF dokumento pabaigoje pateikiamos nuorodos į išorinius šaltinius.

Siekiant padėti dalyviams geriau įsisavinti mokymo medžiagą, naudojami savitikros testai ir simuliacijų sprendimai. Sprendžiant simuliaciją pateikiamas grįžtamasis ryšys. Nesėkmingo sprendimo atveju besimokanysis nukreipiamas peržiūrėti mokymo medžiagą. Be to, kurso metu simuliacijas galima naudoti dviem režimais: mokymosi tikslais ir žinių patikrinimo tikslais.

Kursas gali būti skirtas besimokantiesiems kaip sudėtinė kurso dalis, kaip papildoma medžiaga arba kaip atskiras modulis / kursas.

NUORODOS

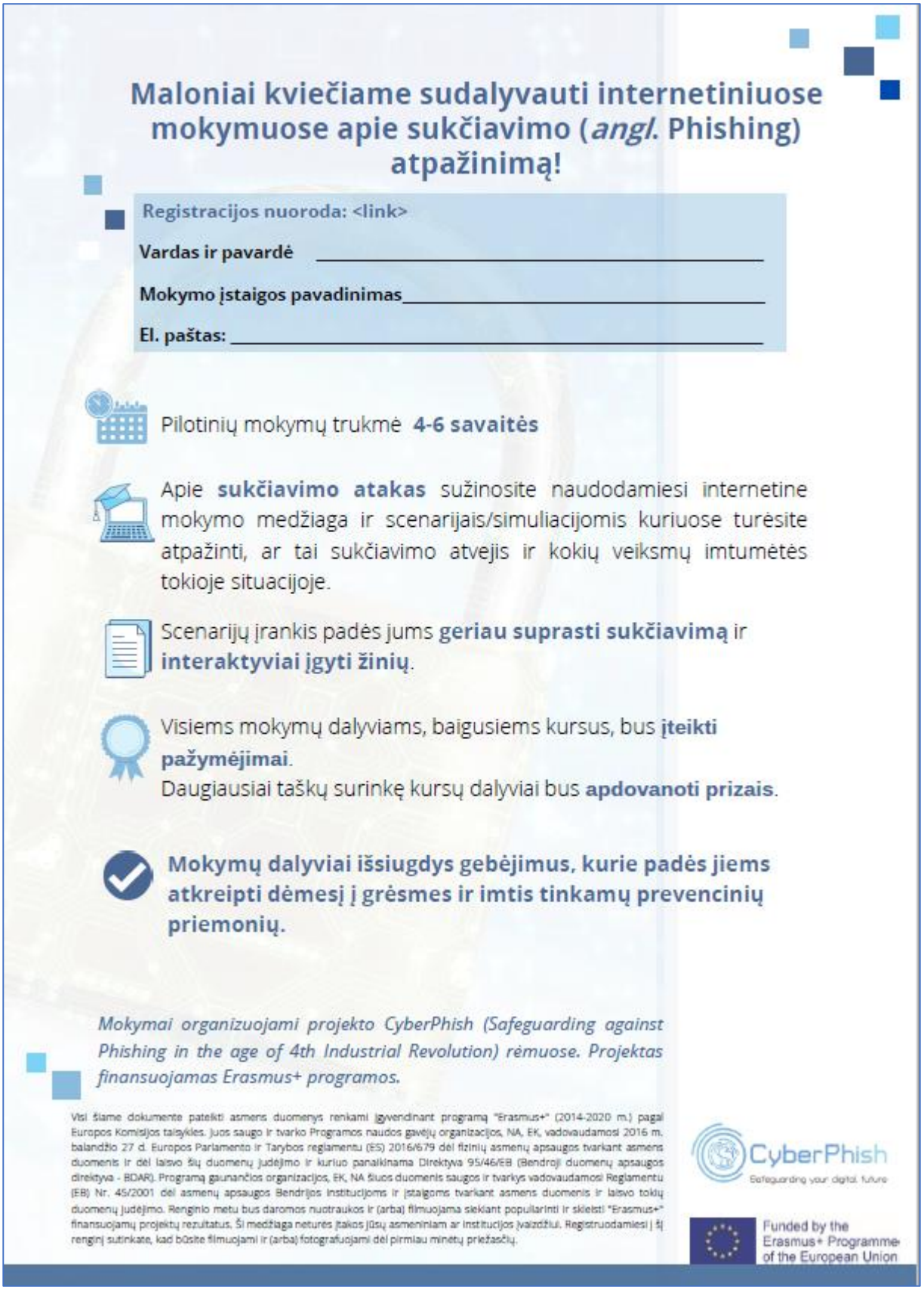
1. IO1 A1: Sukčiavimo atvejų ir įgūdžių spragų identifikavimas
   https://cyberphish.eu/wp-content/uploads/2021/10/IO1_A1_LT_CYBERPHISH-REPORT.pdf
2. IO1 A2: Kibernetinio saugumo mokymo programų analizė
   https://cyberphish.eu/wp-content/uploads/2021/10/IO1-A2_LT-CYBERPHISH-REPORT_study-analysis.pdf
3. IO2 A1: Trumpoji mokymų programos versija, skirta sklaidai
   https://cyberphish.eu/wp-content/uploads/2021/10/IO2-A1_LT_Cyberphish-Short-Curriculum.pdf
4. IO2 A2: Pilnoji mokymų programos versija, skirta mokymo medžiagai rengti ir mokymams
   https://cyberphish.eu/wp-content/uploads/2021/10/IO2-A2_LT_Cyberphish-Full-Curriculum.pdf
5. User_Manual_for_training-Participants.pdf
   [link]

Priedai

1 priedas. Kvietimo į „CyberPhish“ kursą pavyzdžiai

Kvietimo internetu į „CyberPhish“ kursą pavyzdys:

Spausdinto kvietimo į „CyberPhish“ kursą formos pavyzdys



Maloniai kviečiame sudalyvauti internetiniuose mokymuose apie sukčiavimo (*angl.* Phishing) atpažinimą!

Registracijos nuoroda: <link>

Vardas ir pavardė _____

Mokymo įstaigos pavadinimas_____

El. paštas: _____

Pilotinių mokymų trukmė **4-6 savaitės**

Apie **sukčiavimo atakas** sužinosite naudodamiesi internetine mokymo medžiaga ir scenarijais/simuliacijomis kuriuose turėsite atpažinti, ar tai sukčiavimo atvejis ir kokių veiksmų imtumėtės tokioje situacijoje.

Scenarijų įrankis padės jums **geriau suprasti sukčiavimą** ir **interaktyviai įgyti žinių**.

Visiems mokymų dalyviams, baigusiems kursus, bus **įteikti pažymėjimai**.
Daugiausiai taškų surinkę kursų dalyviai bus **apdovanoti prizais**.

Mokymų dalyviai išsiugdys gebėjimus, kurie padės jiems atkreipti dėmesį į grėsmes ir imtis tinkamų prevencinių priemonių.

Mokymai organizuojami projekto CyberPhish (Safeguarding against Phishing in the age of 4th Industrial Revolution) rėmuose. Projektas finansuojamas Erasmus+ programos.

Visi šiame dokumente pateikti asmens duomenys renkami įgyvendinant programą "Erasmus+" (2014-2020 m.) pagal Europos Komisijos taisykles. Juos saugo ir tvarko Programos naudos gavėjų organizacijos, NA, EK, vadovaudamosi 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo šių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrojі duomenų apsaugos direktyva - BDAR). Programą gaunančios organizacijos, EK, NA šiuos duomenis saugos ir tvarkys vadovaudamosi Reglamentu (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo. Renginio metu bus daromos nuotraukos ir (arba) filmuojama siekiant populiarinti ir sklaidyti "Erasmus+" finansuojamų projektų rezultatus. Šį medžiagą neturės įtakos jūsų asmeniniam ar institucijos įvaizdžiui. Registruodamiesi į šį renginį sutinkate, kad būsite filmuojami ir (arba) fotografuojami dėl pirmiau minėtų priežasčių.

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

2 priedas. „CyberPhish“ kurso baigimo sertifikato pavyzdys

CERTIFICATE

OF COMPLETION ONLINE COURSE

Name Surname

has successfully completed the online training course

Safeguarding against Phishing in the age of 4th Industrial Revolution

This certificate was awarded on 12 May, 2022

CyberPhish

Project funding source: Erasmus+ KA2 Strategic Partnerships.
CyberPhish Project No 2020-1-LT01-KA203-078070,
https://cyberphish.eu

Funded by the
Erasmus+ Programme
of the European Union

3 priedas. Klausimyno, skirto „CyberPhish“ kurso dalyviams po kurso, pavyzdys

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Dalyvių klausimynas pasibaigus kursui

Ši apklausa tai pilotinių mokymų paskutinė dalis. Nuotoliniai mokymai rengiami pagal CyberPhish projektą, kurio tikslas - sukurti nuotolinę mokymosi aplinką, kurioje pateikiama mokymo medžiaga, savitikros ir žinių patikrinimo testai bei simuliacijos, siekiant apsisaugoti nuo "phishing" atakų, atpažinti grėsmes ir užkirsti joms kelią.

Šioje apklausoje renkama informacija apie piloninių mokymų kurso dalyvius, baigusius "CyberPhish" kursą. Surinkti duomenys bus naudojami tik projekto tikslais.

Apklausos užpildymo laikas ~10 minučių.

Dėkojame už bendradarbiavimą ir jūsų laiką.

[redacted] (nebendrinama)

Perjungti paskyrą

*Privaloma

Lytis *

- ◯ Vyras
- ◯ Moteris
- ◯ Kita

Užimtumas *

- ◯ Studentas
- ◯ Darbuotojas
- ◯ Dirbantis pagal individualią sutartį ar verslo liudijimą
- ◯ Verslo atstovas
- ◯ Kita

Kaip vertinate savo žinias šiomis kibernetinio saugumo temomis baigę "CyberPhish" kursą? *

	Įgijau daug naujų žinių apie sukčiavimą (angl. phishing)	Patobulinau savo žinias apie sukčiavimą (angl. phishing)	Nieko naujo neišmokau
Kibernetinio saugumo teisiniai aspektai	◯	◯	◯
Kibernetinio saugumo tendencijų apžvalga	◯	◯	◯
Socialinė inžinerija	◯	◯	◯
Psichologiniai socialinės inžinerijos aspektai	◯	◯	◯
Sukčiavimo atakų tipai ir būdai	◯	◯	◯
Sukčiavimo atakų atpažinimas	◯	◯	◯
Kibernetinių incidentų prevencinės priemonės	◯	◯	◯
Kibernetinių atakų valdymas	◯	◯	◯

Kaip vertinate savo žinias šiomis kibernetinio saugumo temomis baigę "CyberPhish" kursą? *

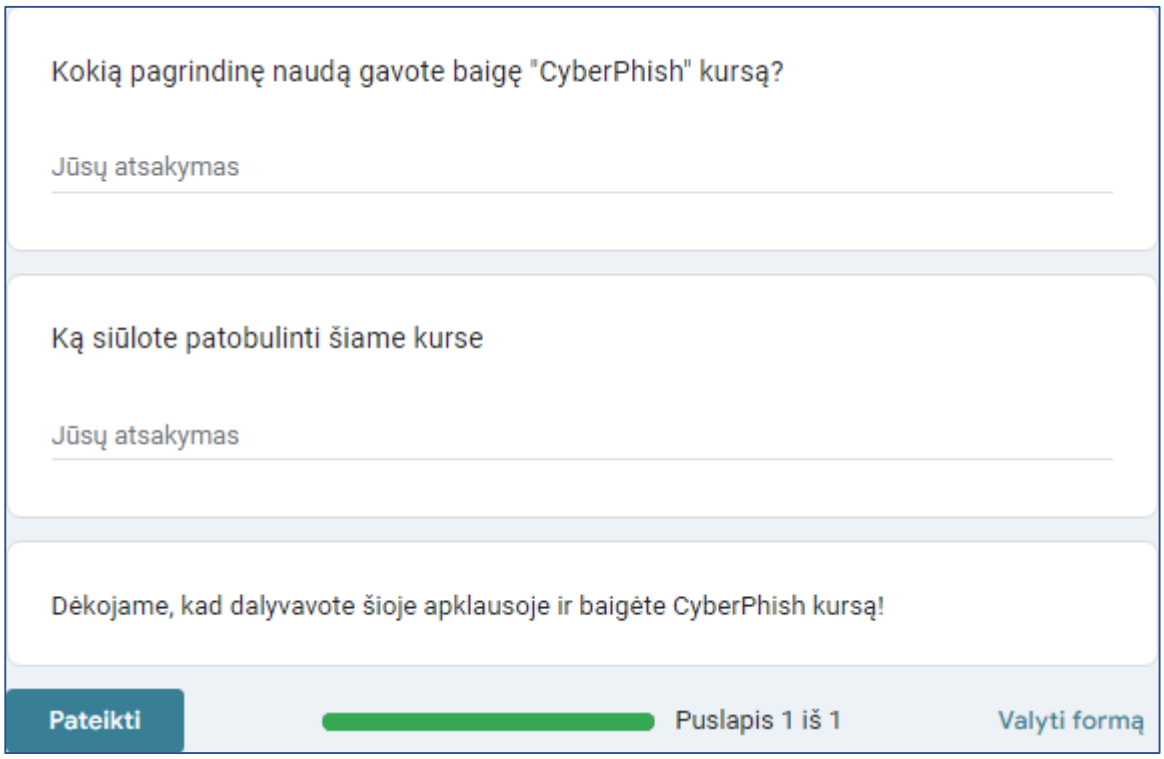
	Gerai	Vidutiniškai	Prastai	Neturiu nuomonės
Kibernetinio saugumo įvadas	◯	◯	◯	◯
Kibernetinė sauga Europos sąjungoje	◯	◯	◯	◯
Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (angl. phishing))	◯	◯	◯	◯
Kibernetinių atakų atpažinmas ir apsauga	◯	◯	◯	◯

Jūsų patirtis naudojant simuliacijas *

	Labai padėjo	Padėjo	Nepadėjo	Neturiu nuomonės
Ar simuliacijos padėjo pagerinti jūsų įgūdžius atpažįstant sukčiavimą?	◯	◯	◯	◯

Įvertinkite savo patirtį, susijusią su šiais "CyberPhish" kurso elementais? *

	Visiškai sutinku	Sutinku	Nesutinku	Visiškai nesutinku
Aiškiai supratau kurso tikslus	○	○	○	○
Manau, kad internetinis mokymosi metodas buvo tinkamas šiam kursui	○	○	○	○
Manau, kad kurso turinys atitiko kurso tikslus	○	○	○	○
Manau, kad kursui užbaigti buvo skirta pakankamai laiko	○	○	○	○
Manau, kad mokymas ir pagalba viso kurso metu buvo tinkami	○	○	○	○
Rekomenduočiau šį kursą kitiems žmonėms	○	○	○	○
Mokymosi internetu platforma buvo paprasta naudotis	○	○	○	○


Kokią pagrindinę naudą gavote baigę "CyberPhish" kursą?
Jūsų atsakymas
Ką siūlote patobulinti šiame kurse
Jūsų atsakymas
Dėkojame, kad dalyvavote šioje apklausoje ir baigėte CyberPhish kursą!
Pateikti
Puslapis 1 iš 1
Valyti formą

4 priedas. Klausimyno, skirto „CyberPhish“ kursų instruktoriams, konsultantams ir mentoriams po kursų, pavyzdys

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Post-Course Questionnaire for trainers/ consultants/ mentors

This survey is part of an EU funded project to design and develop e-learning materials, blended learning environment, knowledge and skills self-evaluation and knowledge evaluation system simulations for students and other users in order to prevent from phishing attacks, raise competencies in this area for identification and prevention of threats.

This survey will gather information from CyberPhish course teachers/consultants/mentors. This survey will help to evaluate the project's pilot trainings.

The survey should take approximately 10-15 minutes to complete.

Thank you for your cooperation and your time.

[redacted]@gmail.com (nebendrinama)
Perjungti paskyrą

*Privaloma

Name *

Jūsų atsakymas

Country *

- ◯ Lithuania
- ◯ Latvia
- ◯ Estonia
- ◯ Malta
- ◯ Cyprus

Please indicate how strongly you agree or disagree with the following statements *

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
The structure and content of the course motivated participants to complete it.	○	○	○	○	○
The time provided for participants to complete the pilot course was sufficient.	○	○	○	○	○
Areas of topics covered by the course were appropriate for the target audience.	○	○	○	○	○
The appropriate amount of detail was provided for the topics covered by the programme.	○	○	○	○	○

What other additional support or resources could have helped to organise the course

Jūsų atsakymas

Please indicate how much you agree or disagree with the following statement *

	Fully achieved	Achieved to a high extent	Achieved to a low extent	Not achieved
To what extent has CyberPhish achieved its goal of introducing cybersecurity and phishing to students	○	○	○	○

Other comments, suggestions

Jūsų atsakymas

Thank you for your participation in this survey and for completing the CyberPhish course!