

# 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

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

<b>Apie projektą</b> .....	<b>3</b>
<b>Mokymo organizavimo gairės</b> .....	<b>3</b>
<b>Bendroji mokymo tvarka</b> .....	<b>5</b>
<b>Darbas su e-mokymosi aplinka</b> .....	<b>9</b>
<b>Darbas su inovatyviais metodais (simuliacijos, paskaitos, seminarai, praktiniai mokymai, interneto priemonių naudojimas ir t. t.)</b> .....	<b>11</b>
<b>Išvados ir rekomendacijos</b> .....	<b>12</b>
<b>Nuorodos</b> .....	<b>13</b>
<b>Priedai</b> .....	<b>14</b>
1 priedas. Kvietimo į „CyberPhish“ kursą pavyzdžiai .....	14
2 priedas. „CyberPhish“ kurso baigimo sertifikato pavyzdys.....	16
3 priedas. Klausimyno, skirto „CyberPhish“ kurso dalyviams po kurso, pavyzdys.....	17
4 priedas. Klausimyno, skirto „CyberPhish“ kursų instruktoriams, konsultantams ir mentoriams po kursų, pavyzdys .....	23



## 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 internte, reikia švesti naudotojus, kad jie galėtų atpažinti sukčiavimo atakas ir tinkamai į jas reaguoti.

Projekto tikslas yra edukuoti aukštųjų mokyklų studentus, pedagogus, universiteto darbuotojus (bendruomenės narius), suaugusiuju švietimo centrus ir verslo sektorius bei skatinti tikslinės grupės kritinj 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 mokymu vadovams / mentoriams bei rekomendacijas, kaip įsidiegti mokymo kursą, siekiant apsaugoti nuo sukčiavimo atakų, igyti kompetencijų, kurios padės atkreipti dėmesį į grėsmes ir imtis reikiama prevencijos priemonių.

Pagrindiniai intelektiniai rezultatai:

1. Tyrimo analizė ir rekomendacijos: Išvengti sukčiavimo atakų ir tobulinti kritinj mąstymą;
2. Kurso programa;
3. Internetinė mokymosi medžiaga;
4. Simuliacijos;
5. Savęs vertinimo bei žinių vertinimo sistema;
6. Metodinės rekomendacijos mokymu 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 nuotolinu mokymu: dėstytojo vedami seminarai, savarankiškas dalyvių darbas naudojantis internetine mokymosi medžiaga ir grupinio bendradarbiavimo praktikos.

Svarbu, kad dalyviai bet kuriuo mokymosi proceso metu (išskyrus galutinj žinių įvertinimą) galėtų sulaukti dėstytojo pagalbos, t. y. galėtų užduoti rūpimus klausimus, prašyti pagalbos, jei nepavyksta ar nesuprantą, kaip atlikti užduotj, ir gauti dėstytojų pagalbą bei grįžtamajį 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, praktiskai išbandė simuliacijas – sukčiavimo atakų imitacijas ir laikė savitikros bei žinių vertinimo testus, kad nustatytu savo žinių lygi 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 imituoją realaus gyvenimo situacijas.

Kiti projekto naudos gavėjai: pedagogai, universitetų darbuotojai, švietimo centralai ir verslo sektorius (darbdaviai ir darbuotojai). Jie taip pat gauti naudos – praplėsdami ir pagilindami savo turimas žinias bei kompetencijas, galēs jaustis saugesni internte, 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 saveš bei žinių jvertinimas, 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 tiklinės 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 moduliu skirti savarankiškam mokymuisi ir jsivertinimui. 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 Sajungoje (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 4ios Pramonės revoliucijos amžiuje, pavyzdžiu, plačiai naudojamos mobiliosios technologijos, debesų kompiuterija, daiktų internetas (IoT) ir didieji duomenys, trečiųjų šalių keliamą rizika ir augančios grėsmės, išskaitant nacionalinių valstybių grėsmes. Šioje dalyje taip pat pateikiami kibernetinio saugumo srityje naudojami apibrėžimai.

### 2. Kibernetinė sauga Europos Sąjungoje (ES)

• Šiame modulyje pristatoma esama ES politika ir iniciatyvos, kuriomis siekiama skatinti kibernetinio saugumo konцепciją. 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 aptariamos socialinės inžinerijos ir atvirkštinės socialinės inžinerijos sąvokos bei glaudus socialinės inžinerijos ryšys su kibernetinėmis atakomis. Modulyje pristatomos įvairių tipų sukčiavimo atakos ir metodai, taip pat pateikiami realūs pavyzdžiai.

### 4. Kibernetinių atakų atpažinimas ir apsauga

• Šiame modulyje supažindinama su e. saugumo sąvoka ir aktyvaus požiūrio į kibernetines grėsmes svarba taikant kibernetinės higienos koncep ciją. Jame taip pat išsamiai aprašoma kaip atpažinti ir valdyti kibernetines atakas, rengti ir įgyvendinti reagavimo į incidentus planus, siekiant sumažinti kibernetinių atakų poveikį.

## Paveikslas 2. Mokymo kurso struktūra

Išsamią mokymo programą galima rasti projekto svetainėje [www.cyberphish.eu](http://www.cyberphish.eu)

Trumpoji mokymo programos versija: [https://cyberphish.eu/wp-content/uploads/2022/12/I02-A1\\_Short-version-of-curricula-for-dissemination\\_LT.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/I02-A1_Short-version-of-curricula-for-dissemination_LT.pdf)

Pilnoji versija: [https://cyberphish.eu/wp-content/uploads/2022/12/I02-A2\\_Extended-version-of-curricula\\_LT.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/I02-A2_Extended-version-of-curricula_LT.pdf)

## BENDROJI MOKYMO TVARKA

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

### Kvietimas į mokymus

Tarkime, kad mokymai organizuojami kaip atskiras kursas, neįtrauktas į aukštostos mokyklos mokymo programą. Tokiu atveju rekomenduojama interneto svetainėje ir (arba) socialiniuose tinkluose paskelbtį pranešimą, kviečiantį į pilotinius mokymus, arba išsiųsti asmeninį kvietimą potencialiems dalyviams el. paštu. Šiame kvietime potencialius 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 kita. Supažindinkite su konsultacijos forma (gyvai / nuotolinii būdu) ir dažnumu, pavyzdžiu, kas savaitę, tris kartus per kursą (pradžioje, pabaigoje ir viduryje). Rekomenduojama paminėti problemas, kurios gali iškilti registruojantis platformoje (pvz., į nepageidaujamų laiškų aplanką patekės patvirtinimo el. laiškas).



Susitikimo metu dalyviams paaiškinama, kaip naudotis e-mokymosi aplinka, leidžiama ją išbandyti ir kviečiama pasidalinti 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 skirtinė 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 aplinka (<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.

### Nuotlinis mokymas

Po trumpo įvado prasideda nuotlinis 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 nepažystamais 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 mokomojių medžiagų. Medžiagą gali laisvai studijuoti visi norintys asmenys. Registruotis nereikia. Tačiau norint spręsti simuliacijas, kuriose mokoma, kaip atpažinti sukčiavimo atakas, atliliki savikontrolės testus, žinių vertinimo testą ir gauti sertifikatą, būtina būti registruotu naudotoju.

**Mokymo medžiaga.** Spustelėjės meniu juosteje esantį mygtuką „Mokymosi medžiaga“, naudotojas kairėje ekrano pusėje mato kurso modulius. Yra keturi moduliai: kibernetinio saugumo įvadas; kibernetinė sauga Europos Sajungoje (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 atsisiusti medžiagą į savo kompiuterį, spustelėjės nuorodą „Atsisiusti skaidres“.

**Savitikros testai.** Registruoti naudotojai turi daugiau galimybę. Jie turi galimybę mokymosi tikslais atliliki 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 atliliki 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 spustelėjės mygtuką „Atlikti iš naujo“. Pakartotinai atliekant testą pateikiami penki atsitiktiniai klausimai iš to modulio. Savitikros testą galima atliki neribotą skaičių kartų.

**Simuliacijos.** Registruoti dalyvai 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 režimais: mokymosi ir žinių patikrinimo. Pirmu atveju (pasirinkus spręsti mokymosi tikslu), dalyvis pasirinkęs galimą situacijos sprendimo variantą, gauna grįztamajį ryšį, o simuliacijos pabaigoje mato surinktus balus ir bendrą išvadą. Antru atveju (sprendžiant simuliaciją žinių patikrinimo tikslu), dalyvis gauna grįztamajį ryšį tik simuliacijos pabaigoje. Mokymų vadovas / mentorius turėtų nuspręsti, kiek simuliacijų dalyvis turi išspręsti. Pavyzdžiu, pilotinių mokymų metu kiekvienas dalyvis turėjo išspręsti ne mažiau kaip 20 pasirinktų simuliacijų.

**Žinių tikrinimo testas.** Registrnuoti dalyviai gali atlkti baigiamajį 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 baigiamajį 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 pasiekama 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. Užsiregistrhuoti e-mokymosi aplinkoje.** Užsiregistruokite e-mokymosi aplinkoje adresu <https://cyberphish.vuknf.lt/login>, naudodamai 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 / šiukslių 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 „*Pažymeti kaip atlikta*“.

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 Sajungoje (ES)
  - 2.1.Kibernetinio saugumo skatinimas Europos Sajungoje;
  - 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.Prevenčinės priemonės
  - 4.3.Kibernetinių atakų atpažinimas
  - 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 mokymu** 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: pirmia, jo metu dalyviai gali užpildyti klausimyną apie pilotinius mokymus, antra – dalyviai gali išsakyti savo nuomonę apie mokymo kursą. Galiausiai galima aptarti žinių vertinimo teste eigą, iškilusius sunkumus ir iššūkius atsakant į teste 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 mentorų /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-MOKYMOSSI APLINKA

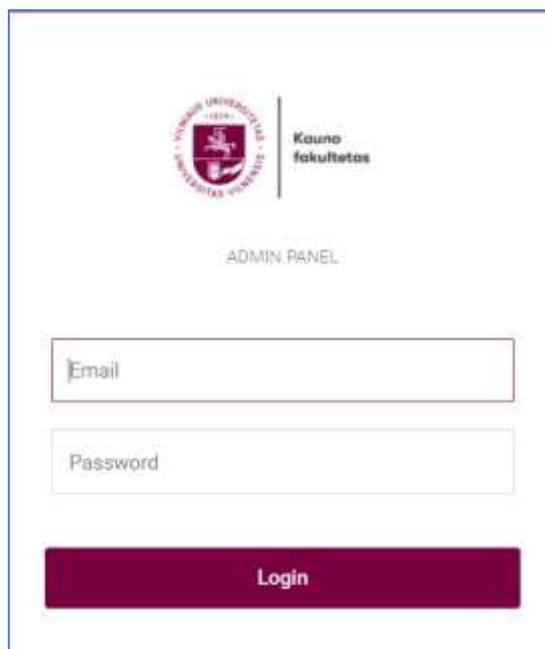
E-mokymosi aplinka pasiekiamama adresu <https://cyberphish.vuknf.lt>. Čia patalpinta mokymosi medžiaga prieinama visiems lankytojams ir yra nemokama. Mokymosi medžiaga pateikiama penkiomis kalbomis: anglų, estų, graikų, latvių, ir lietuvių kalbomis. Neregistruoti lankytojai gali tik peržiūrėti mokymosi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

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.

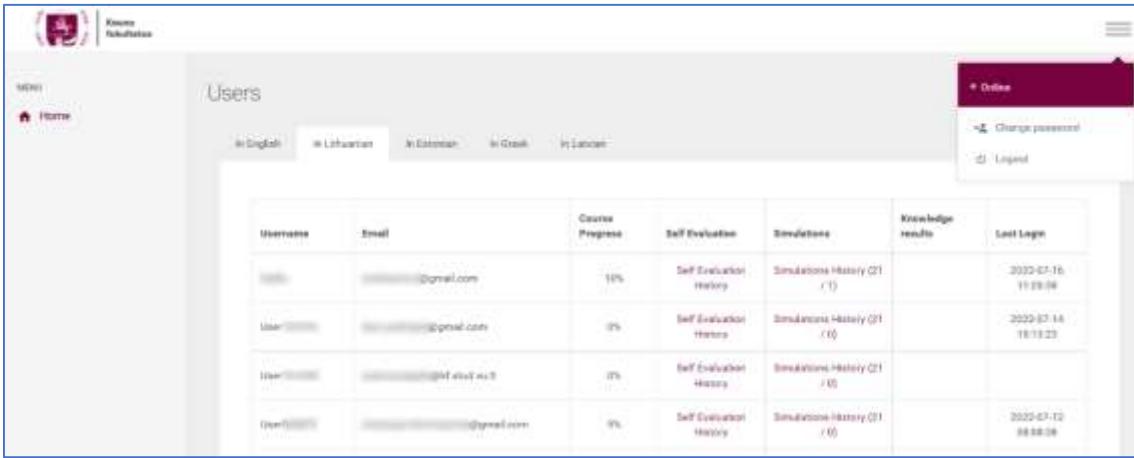
Prisijungimo prie mokytojo aplinkos adresas: <https://cyberphish.vuknf.lt/admin-panel>. Prisijungimo langas pateikiamas žemiau:



The screenshot shows a login interface for an administrator panel. At the top left is the Kaunas University of Technology logo, which includes a crest with a figure and the text 'Vilniaus UNIVERSITETAS' and '1922'. To the right of the logo is the text 'Kauno' fakultetas'. Below the logo, centered, is the text 'ADMIN PANEL.' In the center of the page is a form with two input fields: one for 'Email' and one for 'Password', both with placeholder text. Below the password field is a large, solid red rectangular button labeled 'Login' in white text.

**Paveikslas 4. Mokytojo aplinkos prisijungimo langas**

Jvedus 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.

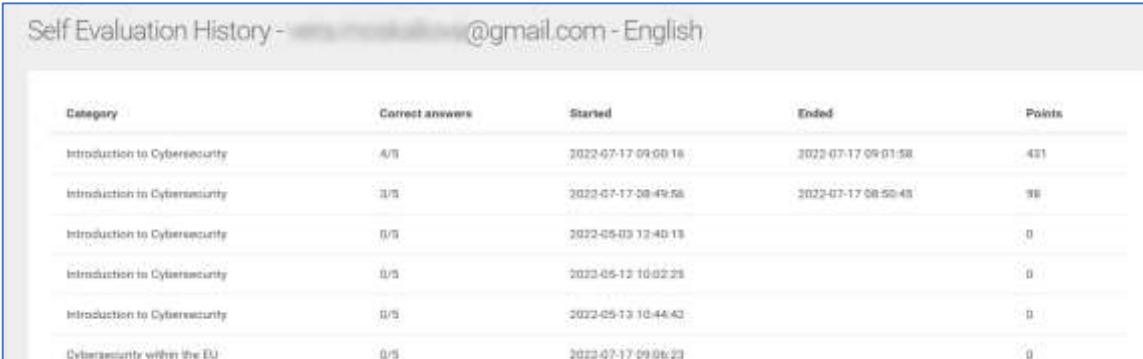


Username	Email	Course Progress	Self Evaluation History	Simulations History	Knowledge Results	Last Login
[REDACTED]	[REDACTED]@gmail.com	10%	Self Evaluation History (21 / 10)	Simulations History (21 / 10)	[REDACTED]	2022-07-16 11:19:08
User [REDACTED]	[REDACTED]@gmail.com	0%	Self Evaluation History	Simulations History (21 / 10)	[REDACTED]	2022-07-16 18:13:23
User [REDACTED]	[REDACTED]@outlook.com	0%	Self Evaluation History	Simulations History (21 / 10)	[REDACTED]	2022-07-16 18:13:23
User [REDACTED]	[REDACTED]@gmail.com	0%	Self Evaluation History	Simulations History (21 / 10)	[REDACTED]	2022-07-16 18:13:23

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.

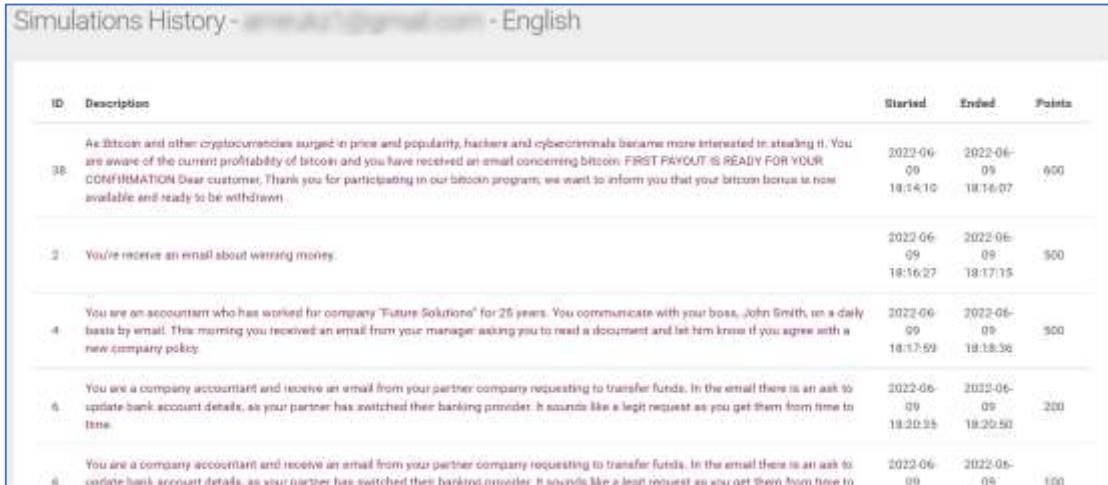


Category	Correct answers	Started	Ended	Points
Introduction to Cybersecurity	4/5	2022-07-17 09:00:18	2022-07-17 09:01:58	431
Introduction to Cybersecurity	3/5	2022-07-17 08:49:58	2022-07-17 08:50:48	18
Introduction to Cybersecurity	0/5	2022-05-03 12:40:18	2022-05-03 12:40:18	0
Introduction to Cybersecurity	0/5	2022-05-12 10:02:21	2022-05-12 10:02:21	0
Introduction to Cybersecurity	0/5	2022-05-13 10:44:42	2022-05-13 10:44:42	0
Cybersecurity within the EU	0/5	2022-07-17 09:06:23	2022-07-17 09:06:23	0

Figure 6 Dalyvio spręstų savitikros testų istorija

### Simuliacijų istorija

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



ID	Description	Started	Ended	Points
1	As Bitcoin and other cryptocurrencies surged in price and popularity, hackers and cybercriminals became more interested in stealing it. You are aware of the current profitability of Bitcoin and you have received an email concerning Bitcoin. FIRST PAYOUT IS READY FOR YOUR CONFIRMATION Dear customer, Thank you for participating in our Bitcoin program; we want to inform you that your Bitcoin balance is now available and ready to be withdrawn.	2022-06-09 18:14:10	2022-06-09 18:16:07	600
2	You've received an email about warning money.	2022-06-09 18:16:27	2022-06-09 18:17:15	500
3	You are an accountant who has worked for company "Future Solutions" for 25 years. You communicate with your boss, John Smith, on a daily basis by email. This morning you received an email from your manager asking you to read a document and let him know if you agree with a new company policy.	2022-06-09 18:17:59	2022-06-09 18:18:36	500
4	You are a company accountant and receive an email from your partner company requesting to transfer funds. In the email there is an ask to update bank account details, as your partner has switched their banking provider. It sounds like a legit request as you get them from time to time.	2022-06-09 18:20:55	2022-06-09 18:20:55	300
5	You are a company accountant and receive an email from your partner company requesting to transfer funds. In the email there is an ask to update bank account details, as your partner has switched their banking provider. It sounds like a legit request as you get them from time to time.	2022-06-09 18:20:55	2022-06-09 18:20:55	300
6	You are a company accountant and receive an email from your partner company requesting to transfer funds. In the email there is an ask to update bank account details, as your partner has switched their banking provider. It sounds like a legit request as you get them from time to time.	2022-06-09 18:20:55	2022-06-09 18:20:55	100

Paveikslas 7. Dalyvio spręstų simuliacių istorija



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

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

Pagrindinis simulacijos tikslas – padėti žmonėms pagerinti kritinį mąstymą, susijusį su kibernetiniu saugumu ir sukčiavimu, atpažstant sukčiavimo, nepageidaujamų elektroninių laiškų, kibernetinių patyčių ir kitus atvejus. Remiantis [IO1](#) buvo parengtos rekomendacijos simulacijoms – 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. Simulacijos skirtos įvertinti galimą / tikėtiną naudotojo elgesį, jo galimus svarstymus / nuogąstavimus ir sprendimus tokioje situacijoje. Pateiktas simulacijas sudaro trys lygmenys. Pasirinkus vieną iš problemos / situacijos variantų, paveikiami ir pateikiami kiti galimi sprendžiamos atvejų variantai.

Sukurtos simulacijos veikia dviem režimais: mokymosi tikslais ir žinių patikrinimo tikslais. Sprendžiant simulaciją mokymosi tikslais, simulacijos pabaigoje studentas mato surinktus balus ir bendrą išvadą. Sprendžiant simulaciją žinių patikrinimo tikslais, studentas mato simulacijos metu padarytus pasirinkimus ir simulacijos pabaigoje gauna grįztamajį ryšį su komentarais. Jei simuliacija buvo išspręsta neteisingai, naudotojui rekomenduojama simulaciją 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 tokius grėsmis 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/2022/12/I01-A1-Report\\_Recognising-Phishing-and-Skills-Gaps\\_LT.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/I01-A1-Report_Recognising-Phishing-and-Skills-Gaps_LT.pdf)). Tai lemia ne tik asmeninių duomenų ir asmeninių finansų praradimą sukčiavimo ar kibernetinės atakos atveju, bet ir konfidentialios informacijos bei įmonių / organizacijų finansinių išteklių praradimą.

Remiantis su kibernetiniu saugumu susijusių aukštojo mokslo mokymo programų ir privačių bendrovų vykdomy kibernetinio saugumo mokymo programų analize šalyse partnerėse (žr. [https://cyberphish.eu/wp-content/uploads/2022/12/I01-A2-Report\\_Analysis-of-existing-Cybersecurity-training-programmes\\_LT.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/I01-A2-Report_Analysis-of-existing-Cybersecurity-training-programmes_LT.pdf)) konsorciumas parengė mokymo programą, apimantį keturis modulius:

- Kibernetinio saugumo įvadas;
- Kibernetinė sauga Europos Sajungoje (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/2022/12/I02-A2\\_Extended-version-of-curricula\\_LT.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/I02-A2_Extended-version-of-curricula_LT.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 pateikiamas nuorodos į išorinius šaltinius.

Siekiant padėti dalyviams geriau įsisavinti mokymo medžiagą, naudojami savitikros testai ir simuliacijų sprendimai. Sprendžiant simuliaciją pateikiamas grįztamasis 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/2022/12/IO1-A1-Report\\_Recognising-Phishing-and-Skills-Gaps\\_LT.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A1-Report_Recognising-Phishing-and-Skills-Gaps_LT.pdf)
2. IO1 A2: Kibernetinio saugumo mokymo programų analizė  
[https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A2-Report\\_Analysis-of-existing-Cybersecurity-training-programmes\\_LT.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/IO1-A2-Report_Analysis-of-existing-Cybersecurity-training-programmes_LT.pdf)
3. IO2 A1: Trumpoji mokymų programos versija, skirta sklaidai  
[https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A1\\_Short-version-of-curricula-for-dissemination\\_LT.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A1_Short-version-of-curricula-for-dissemination_LT.pdf)
4. IO2 A2: Pilnoji mokymų programos versija, skirta mokymo medžiagai rengti ir mokymams  
[https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A2\\_Extended-version-of-curricula\\_LT.pdf](https://cyberphish.eu/wp-content/uploads/2022/12/IO2-A2_Extended-version-of-curricula_LT.pdf)
5. User\_Manual\_for\_training-Participants.pdf  
<https://wiki.cyberphish.eu/>



## Priedai

### 1 priedas. Kvietimo į „CyberPhish“ kursą pavyzdžiai

Kvietimo internetu į „CyberPhish“ kursą pavyzdys:

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

Registracijos nuoroda: <[link](#)>

 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.

 Scenariju įrankis padės jums **geriau suprasti sukčiavimą** ir **interaktyviai įgerti žinių**.

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

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

 Daugiau informacijos apie projektą **CyberPhish**:  
<https://cyberphish.eu/>

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

 CyberPhish  
Safeguarding your digital future

 Funded by the  
Erasmus+ Programme  
of the European Union



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 igyti žinių**.



Visiems mokymų dalyviams, baigusiems kursus, bus **iteikti 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) renginio. Projekto finansuojamas Erasmus+ programos.*

Visi šiam dokumente pateiktai asmenys duomenys renkami išgrendinant programą "Erasmus+" (2014-2020 m.) pagal Europos Komisijos taisyklės Juns 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 asmenys duomenis ir dėl laisvo šių duomenų judėjimo ir kuriuo panalinkama Direktyva 95/46/EE (Bendroji) duomenų apsaugos direktyva - BDAR). Programa gausiausčios organizacijos, EK, NA kluos duomenis saugos ir tvarkys vadovaudamosi Reglamentu (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir (arba) siejant asmenys duomenis ir laisvo tokių duomenų judėjimo. Renginio metu bus daromos nuotraukos ir (arba) filmuojama siekiant populiarinti ir skleisti "Erasmus+" finansuojamų projektų rezultatus. Ši medžiaga neturės jokių asmeninių ar institucijos įvaizdžių. Registruodamiesi į šį renginį sutinkate, kad būsite filmuojami ir (arba) fotograjuojami dėl pirmiau minėtų priežasčių.



Funded by the  
Erasmus+ Programme  
of the European Union



## 2 priedas. „CyberPhish“ kurso baigimo sertifikato pavyzdys





Funded by the  
Erasmus+ Programme  
of the European Union



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

 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 apsaugoti 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? \*

	Igijau daug naujų žinių apie sukčiavimą (angl. phishing)	Patobulinau savo žinias apie sukčiavimą (angl. phishing)	Nieko naujo neišmokau
Kibernetinio saugumo teisinių aspektai	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kibernetinio saugumo tendencijų apžvalga	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Socialinė inžinerija	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Psichologiniai socialinės inžinerijos aspektai	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sukčiavimo atakų tipai ir būdai	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sukčiavimo atakų atpažinimas	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kibernetinių incidentų prevencinės priemonės	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kibernetinių atakų valdymas	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



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

	Gerai	Viðutiniškai	Prastai	Neturiu nuomonės
Kibernetinio saugumo įvadas	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kibernetinė sauga Europos sąjungoje	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kibernetinės atakos (socialinė inžinerija ir sukčiavimas (angl. phishing))	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kibernetinių atakų atpažinimas ir apsauga	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Jūsų patirtis naudojant simuliacijas \*

	Labai padėjo	Padėjo	Nepadėjo	Neturiu nuomonės
Ar simuliacijos padėjo pagerinti jūsų įgūdžius atpažįstant sukčiavimą?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Jvertinkite savo patirtj, susijusią su šiais "CyberPhish" kurso elementais? \*

	Visiškai sutinku	Sutinku	Nesutinku	Visiškai nesutinku
Aiškiai supratau kurso tikslus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Manau, kad internetinis mokymosi metodas buvo tinkamas šiam kursui	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Manau, kad kurso turinys atitiko kurso tikslus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Manau, kad kursui užbaigtį buvo skirta pakankamai laiko	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Manau, kad mokymas ir pagalba viso kurso metu buvo tinkami	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Rekomenduočiau šį kursą kitiems žmonėms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mokymosi internetu platforma buvo paprasta naudotis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Funded by the  
Erasmus+ Programme  
of the European Union

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



Funded by the  
Erasmus+ Programme  
of the European Union



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



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 paskyra



\*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.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The time provided for participants to complete the pilot course was sufficient.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Areas of topics covered by the course were appropriate for the target audience.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The appropriate amount of detail was provided for the topics covered by the programme.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



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!