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

A1: Metodiskie norādījumi pasniedzējiem

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

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

Funded by the Erasmus+ Programme of the European Union

Šis projekts ir finansēts ar Eiropas Komisijas atbalstu. Šī publikācija [ziņojums] atspoguļo tikai autora uzskatus, un Komisija nevar būt atbildīga par jebkādu tajā ietvertās informācijas izmantošanu.

Saturs

PAR PROJEKTU

Krāpšana ir viena no pēdējā laika lielākajām problēmām, jo kibernoziedznieki izmanto ātrākas un inovatīvākas tehnoloģijas, lai īstenotu krāpšanas kampaņas. Cilvēku vadītas pikšķerēšanas aizsardzības izstrādei ir nepieciešama lietotāju izglītošana, lai viņi varētu atpazīt pikšķerēšanas uzbrukumus un atbilstoši reaģēt uz tiem.

Projekta mērķis ir izglītot augstākās izglītības iestāžu studentus, pedagogus, augstskolu darbiniekus (sabiedrības locekļus), izglītības centrus un uzņēmējdarbības sektoru (darba devējus un darbiniekus). Turklāt projekta mērķis ir arī rosināt mērķa grupas kritisko domāšanu kiberdrošības jomā.

Projekta komanda ir izstrādājusi mācību programmu, e-mācību materiālu, jauktu mācību vidi, pašnovērtējuma testus, zināšanu novērtēšanas un vērtēšanas sistēmu, kā arī uz spēlēm balstītas simulācijas skolēniem un citiem lietotājiem, lai aizsargātu pret pikšķerēšanas uzbrukumiem, kā arī attīstītu iemaņas, kas viņiem palīdzēs apzināties draudus un veikt atbilstošus profilakses pasākumus.

Galvenie intelektuālie rezultāti ir:

1. Pētījuma analīze un ieteikumi: Izvairīšanās no pikšķerēšanas uzbrukumiem un kritiskās domāšanas uzlabošana;

2. Kursa programma;

3. Tiešsaistes mācību materiāli;

4. Izglītības simulācijas (spēļu veidošana);

5. Pašnovērtējuma un zināšanu vērtēšanas sistēmas;

6. Metodiskie norādījumi pasniedzējiem un Kiberpikšķerēšanas moduļa ieviešana.

APMĀCĪBU ORGANIZĒŠANAS VADLĪNIJAS

Ieteikumi un norādījumi par apmācību organizēšanu Kiberpikšķerēšanas moduļa dalībniekiem.

Kiberpikšķerēšanas kursu var organizēt, izmantojot jauktās mācīšanās pieeju, apvienojot tiešsaistes un klātienes mācību metodes. Tas nozīmē, ka zināšanu un prasmju apguves procesa pamatā ir gan klātienes, gan tiešsaistes mācības: lektora vadīti semināri, dalībnieku patstāvīgais darbs, izmantojot tiešsaistes mācību materiālus, un vingrinājumi grupās.

Ir svarīgi, lai dalībnieki varētu saņemt pasniedzēja atbalstu jebkurā mācību procesa posmā (izņemot galīgo zināšanu vērtēšanu), t.i., varētu uzdot interesējošos jautājumus, lūgt palīdzību, ja neizdodas vai nesaprot, kā veikt uzdevumu, un saņemt atbalstu un atsauksmes no pasniedzējiem.

Mērķa grupa. Augstākās izglītības iestāžu studenti ir šī projekta galvenā mērķa grupa. Izmēģinājuma apmācību laikā studenti tika izvēlēti no dažādām studiju programmām. Viņi izmantoja uzlabotus mācību materiālus, praktizēja uz spēlēm balstītas simulācijas un veica pašnovērtējumu un zināšanu novērtēšanas testus, lai noteiktu savu zināšanu līmeni pirms un pēc kursa. Dalībniekiem jābūt digitālām pamatprasmēm. Bez tam nav citu priekšnoteikumu studentu zināšanām vai prasmēm.

Pasniedzējiem bija arī iespēja piekļūt mūsdienīgai kursu mācību programmai, kas balstīta uz jaunākajiem pētījumiem partnervalstīs; savas jomas ekspertu izstrādāti e-mācību materiāli, kas papildināti ar vingrinājumiem studentiem, saitēm uz papildu lasāmvielu (jaunāko literatūru), un saistītiem video resursiem. Šādi viņi atjaunina un uzlabo esošās zināšanas. Pasniedzēji varēja uzzināt par inovatīvām mācību un mācīšanās metodēm, piemēram, pašnovērtējuma testiem un zināšanu testiem tiešsaistes vidē, kā arī simulācijām, kas atraktīvi un rotaļīgi simulē reālas situācijas.

Citi projekta labumu ieguvēji ir pedagogi, augstskolu darbinieki, izglītības centri un uzņēmējdarbības sektors (darba devēji un darbinieki). Viņi arī gūs labumu, paplašinot un padziļinot savas esošās zināšanas un kompetences, jūtoties drošāk tiešsaistē, izvairoties no sensitīvas/personiskas informācijas noplūdes un izvairoties no finansiāliem zaudējumiem gan personīgi, gan savās organizācijās.

Galvenā mērķa grupa	AUGSTĀKĀS IZGLĪTĪBAS STUDENTI

- Izmantot izstrādāto materiālu
- Praktizēt uz spēlēm balstītas simulācijas
- Veikt pašnovērtējuma un zināšanu vērtēšanas testus

Sekundārā mērķa grupa	PASNIEDZĒJI/ TRENERI

- Pieeja izstrādātajai mūsdienīgai kursu mācību programmai un e-mācību materiāliem
- Uzzināt par novatoriskām pasniegšanas un mācīšanās metodēm, piemēram, pašnovērtējuma testiem, zināšanu testiem un simulācijām

Cita mērķa grupa	PEDAGOGI, UNIVERSITĀTES PERSONĀLS, IZGLĪTĪBAS CENTRI UN UZŅĒMĒJDARBĪBAS SEKTORS (DARBA DEVĒJI UN DARBINIEKI)

- Pieeja izstrādātajiem e-mācību materiāliem
- Uzlabot esošās zināšanas un kompetences kiberdrošības jomā

Attēls Nr. 1 Projekta mērķa grupas

Apmācības ilgums. Ieteicamais apmācības ilgums ir 4-6 nedēļas. Visa mācību programma ir 30 stundas; tā ir līdzvērtīga 1 ECTS. Iesakām veltīt pašmācībai un vērtēšanai tādu pašu stundu skaitu vienam modulim. Kursa laikā dalībniekiem ieteicams pavadīt 2-3 stundas nedēļā (apmācības materiāla lasīšanai, testu un scenāriju risināšanai).

Paredzamais apmācības laiks var atšķirties atkarībā no apmācības. Piedāvātās tēmas un vingrinājumi/scenāriji ir sadalīti vienas dienas sesijās. Atvēlētais laiks ir elastīgs; tāpēc precīzs grafiks katrai dienai nav sniegts.

Trenerim iepriekš jāpārskata materiāls un jāplāno laiks, lai tas atbilstu konkrētajām apmācības vajadzībām.

Kursa struktūra. Kursa programma ir sadalīta četrās daļās:

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

1. Ievads kiberdrošībā	• Šī daļa iepazīstina ar kiberuzbrukumu izaicinājumiem uzņēmumiem Nozares 4.0 laikmetā, piemēram, plaša mobilo tehnoloģiju, mākoņdatošanas, lietiskā interneta (IoT) un lielo datu izmantošana, trešo pušu riski un pieaugošs draudu daudzums, tostarp draudi atsevišķām valstīm. Šajā daļā ir sniegtas arī kiberdrošības jomā izmantojamās un atrodamās definīcijas.
2. Pārskats par kiberdrošību ES	• Šis modulis iepazīstina ar esošajām ES politikām un iniciatīvām, kuru mērķis ir veicināt kiberdrošības koncepciju. Tajā arī apspriesti kiberdrošības juridiskie aspekti gan ES, gan visā pasaulē
3. Kiberuzbrukumi — sociālā inženierija un pikšķerēšana	• Šis modulis iepazīstina ar kiberuzbrukumiem, īpašu uzmanību pievēršot pikšķerēšanai. Tajā ir arī detalizēti aplūkots sociālās inženierijas un reversās sociālās inženierijas jēdziens un sociālās inženierijas ciešā saikne ar kiberuzbrukumiem. Modulis piedāvā arī dažādus pikšķerēšanas uzbrukumu veidus un paņēmienus, kā arī reālus gadījumu izpētes piemērus.
4. Kiberuzbrukumu izpratne un to risināšana	• Šis modulis koncentrējas uz e-drošības jēdzienu un proaktīvas pieejas nozīmi kiberdraudiem, izmantojot kiberhigiēnas koncepciju. Tajā ir arī sniegta detalizēta pieeja kiberuzbrukumu atpazīšanai un apstrādei, incidentu reaģēšanas plānu izstrādei un ieviešanai, lai mazinātu kiberuzbrukumu sekas.

Attēls Nr. 2 Kursa struktūra

Detalizētu mācību programmu var atrast projekta tīmekļa vietnē www.cyberphish.eu

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

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

KOPĒJĀS APMĀCĪBAS PROCEDŪRAS

Šajā daļā sniegti norādījumi par apmācību organizēšanu. Šeit ir iekļauti arī labās prakses ieteikumi, kas izmantoti Kiberpikšķerēšanas izmēģinājuma apmācībā, tostarp anketa pirms apmācības, prasības dalībnieka reģistrācijai, mācību process un zināšanu testu nosacījumi.

Uzaicinājums uz apmācībām

Pieņemsim, ka apmācība tiek organizēta kā atsevišķs kurss, kas nav iekļauts augstākās izglītības iestādes mācību programmā. Tādā gadījumā ieteicams mājas lapā un/vai sociālajos tīklos publicēt sludinājumu ar dalībnieku uzaicināšanu uz izmēģinājuma apmācībām vai nosūtīt personīgu ielūgumu potenciālajiem dalībniekiem pa e-pastu. Šis ielūgums informē potenciālo dalībnieku par apmācību primāro mērķi, kursa ilgumu, kompetencēm, kas tiks attīstītās vai iegūtas, pikšķerēšanas uzbrukumu atpazīšanā un sertifikāciju pēc kursa pabeigšanas. Tajā var būt arī saite uz reģistrācijas veidlapu.

Uzaicinājuma piemērs ir sniegts pielikumā Nr.1. Faili ppt un pdf formātos ir pieejami vietnē https://wiki.cyberphish.eu/.

Ievadsanāksme

Kursa sākumā, pirmajā tikšanās reizē, ir svarīgi veidot uzticību starp pasniedzēju un dalībniekiem, motivēt viņus un ļaut vienam otru iepazīt. Informējiet par konsultācijas formu (klātienē/attālināti) un biežumu, piemēram, reizi nedēļā, trīs reizes kursa laikā (sākumā, beigās un vidū). Ieteicams informēt par problēmām, ar kurām var saskarties reģistrācijas laikā platformā (piemēram, apstiprinājuma e-pasta ziņojums nonāk surogātpasta mapē).

Tikšanās laikā izskaidrojiet dalībniekiem, kā izmantot e-studiju vidi, ļaujiet to izmēģināt un aiciniet viņus dalīties ar radušajām problēmām, lai vēlāk nebūtu neskaidrību, kad kurss jau sāksies. Sanāksme ietver arī ievadu Kiberpikšķerēšanas kursā.

Anketa pirms apmācības

Lai novērtētu apmācību ietekmi uz dalībnieku zināšanu progresu, pirms apmācību sākuma ieteicams izmantot anketu. Izmēģinājuma apmācības laikā partneri izmantoja anketas, kas sastāvēja no 20 jautājumiem. Anketa tika izstrādāta angļu valodā un lokalizēta partnervalstu valodās: igauņu, grieķu, latviešu un lietuviešu.

Jautājumi tika atlasīti no pašvērtējuma jautājumiem (20 no 60). Visiem dalībniekiem tika uzdoti vienādi jautājumi, bet citā secībā. Šī anketa neietekmē dalībnieka rezultātus, bet ļauj izmērīt izmaiņas dalībnieka zināšanās.

Anketas aizpildīšana aizņem no 20 līdz 25 minūtēm. Pirms anketas aizpildīšanas dalībniekiem jānorāda sava e-pasta adrese. Reģistrējoties kursa mācību vidē (www.cyberphish.vukhf.lt) ieteicams izmantot to pašu e-pasta adresi. Dalībnieki ir jāinformē, ka viņiem ir jāizmanto derīga e-pasta adrese. Mācību vidē ir jāizmanto tā pati e-pasta adrese, kas norādīta dalībnieka reģistrācijas veidlapā.

Jāņem vērā, ka pirmsapmācības anketas aizpildīšana nav obligāta. Tas ir tikai ieteikums, taču šo praksi var izmantot, ja vēlaties novērtēt apmācību kursa ietekmi uz dalībniekiem.

Tiešsaistes apmācība

Pēc īsa ievada posma tiešsaistes apmācība sākas un ilgst apmēram vienu mēnesi (4-6 nedēļas). Apmācību procesā dalībnieki tiek iesaistīti dažādās mācību aktivitātēs, izmantojot dažādas apmācību metodes un formas, kas ietver, bet ne tikai, e-mācību materiāla apguvi, papildmateriālu lasīšanu, ar tēmām saistītu video skatīšanos, pašnovērtējuma testu veikšanu un zināšanu novērtēšanas testi un simulāciju risināšana. Šajā laikā dalībnieki mācās par kiberdrošību, izprot kiberuzbrukumus un sociālo inženieriju, uzzina, kā atpazīt galvenās pikšķerēšanas pazīmes, izprot kiberuzbrukumu risināšanu, mācās samazināt zaudējumus, reaģējot uz incidentiem. Veiksmīga dalība apmācībās ir atkarīga no dalībnieku spējas plānot savu laiku un aktivitātes, kā arī sadarbības ar treneriem un citiem komandas locekļiem.

Apmācības rezultātā ir sekmīgi jānokārto zināšanu vērtēšanas tests (rezultāts vismaz 75%) un jāsaņem automātiski ģenerēts sertifikāts. Apmācību noslēgumā dalībnieki iegūst jaunas zināšanas un prasmes, ko var izmantot savā ikdienā (piemēram, meklēšana internetā, personiskā saziņa sociālajos tīklos, saruna pa telefonu ar svešiniekiem, mācībās, savās darbavietās utt.). Turklāt viņi arī vairo savu pārliecību.

E-studiju vides struktūra

Cyberphish.vuknf.lt mācību platforma nodrošina atvērtu piekļuvi mācību materiāliem. Materiālu var brīvi apgūt visas personas, kas to vēlas. Reģistrācija nav nepieciešama. Taču, lai varētu atrisināt simulācijas, kas māca atpazīt pikšķerēšanas uzbrukumus, veikt pašpārbaudes, zināšanu novērtējuma testu un iegūt sertifikātu, ir jābūt reģistrētam lietotājam.

Mācību materiāls. Izvēlņu joslā noklikšķinot uz pogas Mācību materiāls, lietotājs var redzēt kursu moduļus ekrāna kreisajā pusē. Ir četri moduļi: Ievads kiberdrošībā; Pārskats par kiberdrošību ES; Kiberuzbrukumi — sociālā inženierija un pikšķerēšana; Kiberuzbrukumu izpratne un risināšana. Katrs modulis sastāv no vairākām tēmām. Izvēloties gadījumu, mācību materiāls parādīsies ekrāna centrālajā daļā. Lietotājs var lejupielādēt materiālus lietotāja datorā, noklikšķinot uz saites *Lejupielādēt slaidus*.

Pašnovērtējumu testi. Reģistrētiem lietotājiem ir vairāk iespēju. Viņiem ir iespēja kārtot pašnovērtējuma testu mācību nolūkos. Pašnovērtējuma testa poga parādās, kad students ir apguvis moduļa materiālu. Tāpēc studentam ir jānoklikšķina uz pogas *Izpildīts*, kad viņš ir iepazinies ar katru moduļa tēmu. Kad visas tēmas modulī ir atzīmētas kā *Izpildītas*, kas nozīmē, ka materiāls šajā modulī ir apgūts, tad ir iespēja kārtot pašnovērtējuma testu, noklikšķinot uz pogas Pašnovērtējuma tests. Testa laikā studentam tiek uzdoti pieci nejauši izvēlēti jautājumi no šī moduļa.

Pēc testa sistēma parāda testa rezultātus, parādot studenta izvēlētās atbildes, pareizās un nepareizās atbildes, testa atbildēm patērēto laiku un iegūtos punktus. Students var atkārtoti kārtot testu, noklikšķinot uz pogas *Atkārtot*. Atkārtoti kārtojot testu, tiek uzrādīti 5 nejauši jautājumi. Pašnovērtējuma testu students var kārtot neierobežotu skaitu reižu.

Simulācijas. Reģistrētie lietotāji var risināt simulācijas. Šīs simulācijas ir faktisko situāciju makets. Ekrāna kreisajā pusē virs moduļa tēmām ir poga *Simulācijas*. Students jebkurā laikā var tos atrisināt. Simulācijas ir sagrupētas 7 grupās: Vienotība, patika, vienprātība, konsekvence, autoritāte, trūkums un savstarpējība. Izvēloties simulāciju, tiek sniegts situācijas apraksts. Simulācijas var darboties divos režīmos: mācību nolūkos un zināšanu pārbaudes nolūkos. Pirmajā režīmā simulāciju mācību nolūkos, students redz savāktos punktus un kopējo secinājumu simulācijas beigās. Simulācijā zināšanu pārbaudei students apsver simulācijas laikā izdarītās izvēles beigās un saņem atgriezenisko saiti ar komentāriem. Mentoram jāizlemj, cik simulācijas dalībniekam ir jāatrisina. Piemēram, izmēģinājumā laikā katram dalībniekam bija jāatrisina vismaz 20 simulācijas pēc paša izvēles.

Zināšanu vērtēšanas tests. Reģistrētie lietotāji var nokārtot zināšanu testu un saņemt sertifikātu. Poga *Zināšanu tests* parādās ekrāna kreisajā pusē virs kursa moduļiem, kad students ir apguvis visu materiālu un atzīmējis visas tēmas kā izpildītas. Tests tiek uzskatīts par nokārtotu, ja ir sasniegts vismaz 75% punktu skaits. Dalībnieki, kuri nokārtos šo gala testu, saņems sertifikātu. Ja dalībnieks neiztur pārbaudījumu, viņš vai viņa var atkārtot tēmas un, vēl kādu laiku veltot mācībām, var atkārtoti kārtot gala Zināšanu testu. Zināšanu testu var kārtot trīs reizes.

Reitingi. Sistēma aprēķina reitingus, lai padarītu mācību procesu pievilcīgāku studentiem. Kursa dalībnieks savu reitingu un savāktos punktus var redzēt kopvērtējuma tabulā. Reitingi ir balstīti uz pašnovērtējuma testiem un simulācijām. Reitingiem var piekļūt, izmantojot izvēlnes vienumu Reitingi ekrāna augšdaļā. Studenta simulācijas reitings tiek aprēķināts, summējot visu atrisināto simulāciju labākos rezultātus. Attiecīgi studenta pašnovērtējuma testa reitings tiek aprēķināts, summējot visu kārtoto testu labākos punktus.

Studenti var arī redzēt savu mācību progresu. Tas tiek parādīts virs kursa moduļiem ekrāna kreisajā pusē un lietotāja izvēlnē ekrāna augšdaļā Izmantojot lietotāja izvēlni, students var mainīt lietotājvārdu un paroli, skatīt savāktās nozīmītes, pašnovērtējuma testu vēsturi un simulāciju vēsturi.

Sertifikāti. Sertifikāti (PDF formātā) automātiski ģenerējas visiem dalībniekiem, kuri ir pabeiguši kursu un nokārtojuši zināšanu novērtējuma testu vismaz par 75%. Sertifikāta piemērs ir sniegts pielikumā Nr.2.

Pēc kursa pabeigšanas visi dalībnieki saņems sertifikātus. Pabeidzot Kiberpikšķerēšanas kursu, akadēmiskie kredītpunkti netiek piešķirti.

Pieejamība

Izstrādātais e-kurss ir pieejams četrās valodās: Angļu, igauņu, grieķu, latviešu un lietuviešu. Tas ir pieejams vietnē https://cyberphish.vuknf.lt/. Tālāk ir sniegts mācību platformas galvenā ekrāna attēls.

Attēls Nr. 3 Mācību platformas galvenais ekrāns

Labas prakses ieteikumi no Izmēģinājuma apmācības. Ieteicams izstrādāt noteikumus un norādījumus studentiem. Aptaujas anketas kursa sākumā un beigās nav obligātas. Citus rīkus var izmantot kā parastajā apmācībā.

Norādījumi studentiem

Šajā daļā mēs aprakstām soļus, organizējot apmācību:

1. solis. Anketa pirms apmācības. Pirms apmācības aizpildiet anketu. Norādiet derīgu e-pasta adresi, kas tiks izmantota arī e-apmācības sistēmā, aizpildot šo anketu.

2. solis. Pierakstieties e-mācību vidē. Pierakstieties e-mācību vidē vietnē https://cyberphish.vuknf.lt/login ar to pašu e-pasta adresi, kuru norādījāt anketā.

Piezīme: Ja skolēns nav saņēmis apstiprinājuma e-pastu no sistēmas, nepieciešams pārbaudīt surogātpasta mapi. Apstiprinājuma e-pasts var nonākt surogātpasta/surogātpasta mapē.

3. solis. Piesakieties e-mācību vidē.

Piesakieties vietnē https://cyberphish.vuknf.lt ar personīgajiem akreditācijas datiem.

4. solis. Mācību materiāla apguve.

Pēc pieteikšanās izpētiet visu mācību materiālu, t.i., četras tēmas un apakštēmas (skat. zemāk). Atzīmējiet kā *izpildītu* pēc katras tēmas izskatīšanas.

Tēmas un apakštēmas:

1. Ievads kiberdrošībā;
1.1. Priekšvēsture – 4. industriālās revolūcijas izaicinājumi;
1.2. Kiberdrošības vēsture;
1.3. Kiberdrošības definīcijas
2. Pārskats par kiberdrošību ES;
2.1. Kiberdrošības veicināšana Eiropas Savienībā;
2.2. Kiberdrošības juridiskie aspekti;
2.3. Pārskats par kiberdrošības vides tendencēm;
3. Kiberuzbrukumi — sociālā inženierija un pikšķerēšana;
3.1. Ievads kiberuzbrukumos;
3.2. Sociālās inženierijas moduļi un manipulācijas;
3.3. Dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni;
3.4. Gadījumu izpēte;
4. Kiberuzbrukumu izpratne un to risināšana.
4.1. Pamatzināšanas par e-drošību;
4.2. Proaktīvas darbības;
4.3. Pikšķerēšanas uzbrukumu atpazīšana;
4.4. Kiberuzbrukumu risināšana;
4.5. Bojājumu samazināšana līdz minimumam, reaģējot uz incidentiem,

5. solis. Izpildiet četrus pašnovērtējuma testus. Pēc katras tēmas apguves aizpildiet pašnovērtējuma testu.

6. solis. Palaist/atrisināt/veikt simulācijas. Mācību laikā veiciet simulācijas kā studiju procesa sastāvdaļu.

7. solis. Veiciet zināšanu novērtēšanas testu. Visbeidzot nokārtojiet pēdējo testu ar vismaz 75%.

8. solis. Pēc pēdējā testa nokārtošanas aizpildiet **Pēckursa anketu dalībniekiem** par izmēģinājuma apmācību.

Piezīme: šis rīks tika izmantots izmēģinājuma apmācības laikā, bet citus rīkus var izmantot kā parastajās apmācībās.

Noslēguma tikšanās

Noslēguma sanāksmei ir vairāki mērķi: pirmkārt, tās laikā dalībnieki var aizpildīt pēcapmācības anketu, otrkārt, dalībnieki var izteikt savu viedokli par kursu. Noslēgumā var apspriest zināšanu novērtēšanas testa norisi, grūtības un izaicinājumus atbildot uz jautājumiem un citus jautājumus.

Aptaujas pēc kursa

Izmēģinājumā dalībniekiem tika lūgts aizpildīt pēckursa anketu pēc pēdējā testa nokārtošanas. Anketa sastāv no punktiem, kuros tiek lūgts sniegt vispārīgu informāciju, piemēram, e-pastu, dzimumu, nodarbošanos un jautājumiem par dalībnieka zināšanu novērtējumu konkrētos kiberdrošības jautājumos pēc Kiberpikšķirēšanas apmācības kursa pabeigšanas, dalībnieka pieredzi, izmantojot simulācijas. Tiek uzdoti arī jautājumi par kursa mērķiem, tiešsaistes formāta pieejas piemērotību, kursa saturu, laika ilgumu, apmācību un atbalstu, mācību platformas lietojamību. Anketas piemērs ir sniegts pielikumā Nr.3.

Treneriem un mentoriem arī tika lūgts aizpildīt **pēckursa anketu** pēc izmēģinājuma. Anketa sastāv no punktiem, kuros tiek lūgts sniegt vispārīgu informāciju, piemēram, e-pastu, vārdu, uzvārdu, valsti, kā arī jautājumiem par kursa struktūru un saturu, laika ilgumu, tēmu atbilstību mērķauditorijai, kursa tēmu pilnīgumu, cik lielā mērā kurss ir sasniedzis savu mērķi iepazīstinot studentus ar kiberdrošību un pikšķerēšanu. Anketas piemērs ir sniegts pielikumā Nr.4.

APRAKSTI, KĀ STRĀDĀT AR E-PLATFORMU

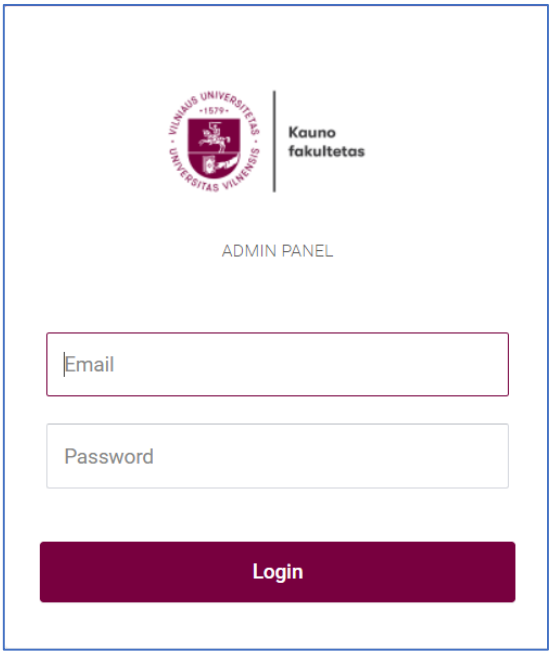
Mācību materiāli, kas izvietoti e-mācību vidē https://cyberphish.vuknf.lt ir pieejami visiem apmeklētājiem un ir bez maksas. Mācību materiāls ir pieejams piecās valodās: Angļu, igauņu, grieķu, latviešu un lietuviešu. Nereģistrēti apmeklētāji var tikai apskatīt mācību materiālu, bet nevar pildīt pašnovērtējuma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

Lietotāja rokasgrāmata ir pieejama dokumentā **User_Manual_for_training-Participants.pdf** vietnē https://wiki.cyberphish.eu/. Šajā dokumentā ir aprakstīts, kā izmantot mācību platformu.

Pasniedzēju vide

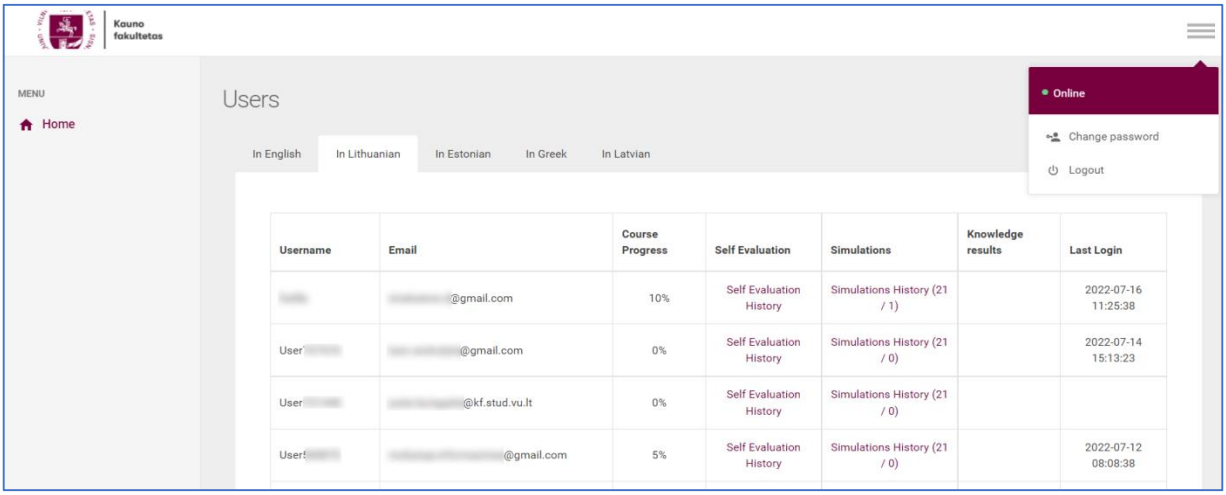
Pasniedzēju vidē var sekot līdzi mācību sistēmā reģistrētajiem dalībniekiem, viņu mācību gaitai procentos, apskatīt veikto pašnovērtējuma testu vēsturi, simulāciju vēsturi, zināšanu testu atzīmes, kā arī pēdējās pieteikšanās datumu un laiku.

Pasniedzēju vides pieteikšanās adrese: https://cyberphish.vuknf.lt/admin-panel. Pieteikšanās logs ir parādīts zemāk:



Attēls Nr. 4 Pasniedzēju vides pieteikšanās logs

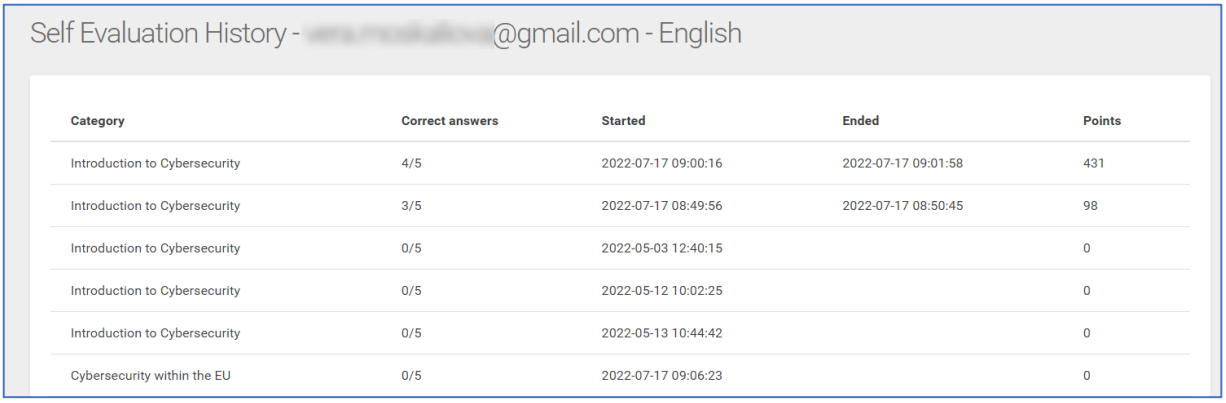
Kad pieteikšanās dati ir ievadīti, sistēma pasniedzējam nodrošina dalībnieku sarakstu. Pasniedzējs var sekot līdzi dalībnieku mācību progresam pa valodām (angļu, lietuviešu, igauņu, grieķu un latviešu). Pasniedzēja vides galvenais logs ir parādīts zemāk:



Attēls Nr. 5 Pasniedzēja vides galvenais logs

Pašnovērtējumu pārbaužu vēsture

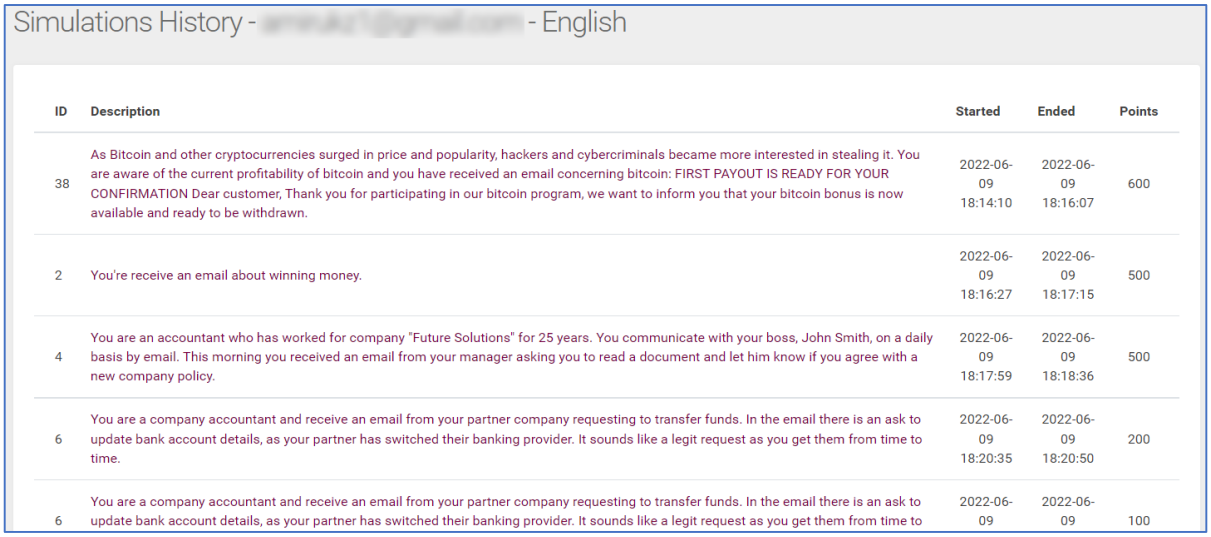
Šo informāciju var apskatīt, noklikšķinot uz dalībnieka pašnovērtējuma vēsturi:



Attēls Nr. 6 Dalībnieka pašnovērtējuma vēsture

Simulāciju vēsture

Šo informāciju var apskatīt, noklikšķinot uz dalībnieka simulāciju vēsturi:



Attēls Nr. 7 Dalībnieka simulāciju vēsture

DARBS AR INOVATĪVĀM METODĒM (T.I., SIMULĀCIJAS METODES, LEKCIJAS, SEMINĀRI, PRAKTISKĀS APMĀCĪBAS, INTERNETA RĪKU LIETOŠANA U.C.)

Simulācija imitē reālus pikšķerēšanas uzbrukumus, parādot procesu lietotājam rotaļīgā formā.

Simulācijas galvenais mērķis ir palīdzēt cilvēkiem uzlabot kritisko domāšanu saistībā ar kiberdrošību un pikšķerēšanu, atpazīstot pikšķerēšanas, surogātpasta, kiberhuligānisma u.c. gadījumus. Pamatojoties uz IO1, tika izstrādāti ieteikumi simulācijām, koncentrējoties uz reālās dzīves gadījumu izpētes pielāgošanu mācību procesam.

Simulācija ietver situācijas aprakstu, mērķi, varoņus, uzbrukuma veidu un vairākas (3-4) atbildes iespējas lietotāja rīcībai. Simulācijas tika izstrādātas, lai novērtētu iespējamo/varbūtējo lietotāja rīcību, viņa iespējamos apsvērumus/bažas un lēmumus šādā situācijā. Piedāvātās simulācijas sastāv no trim dziļuma līmeņiem. Kad ir izvēlēts viens no problēmas/situācijas variantiem, tiek ietekmēti un parādīti turpmākie iespējamie risināmā gadījuma varianti.

Tiek īstenota simulācija mācību un zināšanu pārbaudes nolūkos. Atrisinot simulāciju mācību nolūkos, students redz savāktos punktus un kopējo secinājumu simulācijas beigās. Atrisinot simulāciju zināšanu pārbaudes nolūkā, students redz simulācijas laikā izdarītās izvēles un simulācijas beigās saņem atgriezenisko saiti ar komentāriem. Ja simulācija tika atrisināta nepareizi, lietotājam ieteicams simulāciju atrisināt vēlreiz.

SECINĀJUMI UN IETEIKUMI

Šis dokuments ir izstrādāts visiem pasniedzējiem un mentoriem, kuri sniedz padomus un apmāca studentus. Projekta konsorcijs cer, ka viņi atradīs noderīgus norādījumus par to, kā lietot sistēmu un kā nodrošināt apmācību cilvēkiem, kuri vēlas uzzināt par kiberuzbrukumiem, jo īpaši pikšķerēšanu un sociālo inženieriju, kā arī uzzināt, kā atpazīt galvenās šādu draudu pazīmes. Potenciālajiem lietotājiem ir nepieciešamas pamata digitālās prasmes. Citu priekšnoteikumu attiecībā uz lietotāja zināšanām vai prasmēm nav.

Studentiem un darbiniekiem trūkst zināšanu par pikšķerēšanu, sociālo inženieriju, kiberuzbrukumiem un viņu datu drošību, liecina projekta partneru 2020. gadā Igaunijā, Kiprā, Latvijā, Lietuvā un Maltā veiktais pētījums (sk. https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EN_CYBERPHISH-REPORT_survey-results.pdf). Tas noved ne tikai pie personas datu un personīgo finanšu zaudēšanas pikšķerēšanas vai kiberuzbrukuma gadījumā, bet arī uzņēmumu/organizāciju sensitīvas informācijas un finanšu resursu zaudēšanas.

Pamatojoties uz partnervalstīs veikto pētījumu (sk. https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A2_EN_CYBERPHISH-REPORT_study-analysis.pdf) par augstākās izglītības programmām, kas saistītas ar kiberdrošību, kā arī par privāto uzņēmumu piedāvātajām kiberdrošības apmācību programmām, ir izstrādāta mācību programma, kas aptver četrus moduļus:

- Ievads kiberdrošībā;
- Pārskats par kiberdrošību ES;
- Kiberuzbrukumi — sociālā inženierija un pikšķerēšana;
- Kiberuzbrukumu izpratne un to risināšana

Lai iegūtu papildinformāciju par to, kā sagatavot pasniedzējus un mentorus apmācībām, skatiet pilnu Kiberpikšķerēšanas kursa mācību programmu (sk. https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EN_Cyberphish-Full-Curriculum-Final.pdf)

Kiberpikšķerēšanas apmācības kursu izmēģinājuma apmācības dalībnieki novērtēja atzinīgi. Viņi atzina tā lietderību ikdienas ar IT saistītajās darbībās gan parastajiem lietotājiem, gan uzņēmuma darbiniekiem. Plašāka informācija tiks sniegta ziņojumā IO6 A2: Kursa īstenošanas vadlīnijas.

Tiešsaistes mācību kurss integrē apmācību materiālu PDF formātā – kodolīgi un skaidri, nepārslogojot apmācāmos ar apjomīgu lasāmo materiālu. Tiem, kas vēlas uzzināt vairāk par konkrētu tēmu, katra PDF dokumenta beigās ir norādītas saites uz ārējiem avotiem.

Pašnovērtējuma testi un simulācijas tiek izmantoti, lai palīdzētu dalībniekiem labāk asimilēt mācību materiālu. Simulācijas nodrošina atgriezenisko saiti, kas palīdz vai nu pārskatīt mācību materiālu, vai apgūt jaunas lietas. Turklāt kursa laikā simulācijas var izmantot divos režīmos: mācībām un zināšanu pārbaudei.

Kurss var būt paredzēts studentiem kā kursa daļa, kā papildmateriāls vai kā atsevišķs modulis/kurss.

INFORMĀCIJAS AVOTI

1. IO1 A1: Ziņojums par pikšķerēšanas un prasmju trūkumu atpazīšanu
   https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EN_CYBERPHISH-REPORT_survey-results.pdf
2. IO1 A2: Esošo kiberdrošības apmācību programmu analīze.
   https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A2_EN_CYBERPHISH-REPORT_study-analysis.pdf
3. IO2 A1: Īsā mācību programmu versija izplatīšanai
   https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A1_EN_Cyberphish-Short-Curriculum-Final.pdf
4. IO2 A2: Paplašināta mācību programmu versija mācību materiālu izstrādei un apmācībām
   https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EN_Cyberphish-Full-Curriculum-Final.pdf
5. User_Manual_for_training-Participants.pdf
   [saite]

Pielikumi

Pielikums Nr. 1. Tiešsaistes uzaicinājuma uz Kiberpikšķerēšanas kursu piemērs

Izdrukāta uzaicinājuma uz Kiberpikšķerēšanas kursu piemērs

We kindly invite you to participate in the online course about phishing!

Registration to online course:

Name and Surname _____

Name of education institution _____

Email _____

Duration of pilot training **4-6 week**.

You will learn about **phishing attacks** through an online training material and a scenarios in which you will have to recognise whether or not it is a phishing case and what actions you would take in such a situation.

The scenarios tool will help you **better understand fraud** and **gain knowledge interactively**.

All course participants completed the course will be **awarded certificates**.
Participants completed course with highest scores will be **awarded prizes**.

Course participants will develop competences that will help them to highlight threats and take appropriate preventive measures.

Trainings are organized in the framework of the CyberPhish (Safeguarding against Phishing in the age of 4th Industrial Revolution) project which is funded under the Erasmus+ programme.

All personal data contained in this document is collected during the implementation of the Erasmus + Program (2014-2020), according to the European Commission's regulations. These will be stored and processed by Program Beneficiary Organizations, NA, EC in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of these data and repealing Directive 95/46 / EC (General Data Protection Directive - GDPR). The beneficiary organizations of the Program, EC, NA will store and process these data according to Regulation (EC) no. No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. During the event, photographs and / or films will be taken for purposes of promoting and disseminating the results of Erasmus + funded projects. The materials will not affect your personal or institutional image. By registering to this event you consent to being filmed and / or photographed for the aforementioned reasons.

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Pielikums Nr. 2. Kiberpikšķerēšanas kursa pabeigšanas sertifikāta piemērs

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

Pielikums Nr. 3. Pēckursa anketas piemērs Kiberpikšķerēšanas kursa dalībniekiem

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Post-Course Questionnaire for participants

This survey is part of an EU funded CyberPhish 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 course participants who have completed the CyberPhish course. The data will only be used for the purpose of the project.

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

Thank you for your cooperation and your time.m

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

*Privaloma

Gender *

- ◯ Male
- ◯ Female
- ◯ Other

Occupation *

- ◯ Student
- ◯ Employee
- ◯ Self-employed
- ◯ Business owners
- ◯ Other

How would you evaluate your knowledge on these cybersecurity subjects after finishing the CyberPhish course *

	I have gained a lot of new knowledge about phishing	I have improved my knowledge about phishing	I haven't learnt anything new
Legal Aspects of Cybersecurity	○	○	○
The tendencies of Cybersecurity landscape	○	○	○
Social engineering	○	○	○
Psychological aspects of social engineering	○	○	○
Types of Phishing Attacks and Techniques	○	○	○
Recognising Phishing Attacks	○	○	○
Proactive actions of cyber incidents	○	○	○
Handling Cyber-attacks	○	○	○

How would you evaluate your knowledge on these cybersecurity subjects after finishing the CyberPhish course *

	Satisfied	Neutral	Dissatidfied	I have no opinion
Introduction to Cybersecurity	○	○	○	○
Overview of Cybersecurity within the EU	○	○	○	○
Cyber-attacks – Social Engineering and Phishing	○	○	○	○
Understanding and Handling Cyber-attacks	○	○	○	○

Your experience using simulations *

	Strongly helped	Helped	Not helped	I have no opinion
Did the simulations help to improve your skills recognising phishing?	○	○	○	○

Please rate your experience of the following elements of the CyberPhish course? *

	Strongly agree	Agree	Disagree	Strongly disagree
I had a clear understanding of the course objectives	○	○	○	○
I found the online approach to learning was suitable for the course	○	○	○	○
I found the course content covered the course objectives	○	○	○	○
I found the amount of time given to complete the course to be ample	○	○	○	○
I found the training and support throughout the course to be appropriate	○	○	○	○

I would recommend this course to other people	○	○	○	○
The online learning platform was easy to use	○	○	○	○

What are the main benefits you gained from completing the CyberPhish course? (Please provide one or two sentences)

Jūsų atsakymas

Was there anything missing from the course or anything that could have been improved? (Please provide one or two sentences)

Jūsų atsakymas

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

Pateikti Puslapis 1 iš 1 Valyti formą

Pielikums Nr. 4. Pēckursa anketas piemērs Kiberpikšķerēšanas kursa pasniedzējiem, konsultantiem un mentoriem

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!