Andmepüügi vastu kaitsemine 4. tööstusrevolutsiooni ajastul (CyberPhish)

A1: Metoodilised juhised koolitajatele

Project periood: November 2020 – November 2022

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

Funded by the Erasmus+ Programme of the European Union

Dokumendi ajalugu			
Versioon #	**Versiooni kuupäev**	**Kirjeldus**	**Ees ja Perenimi**
1	**2022-07-03**	**Original Draft**	**Vera Moskaliova (VU)**
2	**2022-07-13**	**Updated Draft**	**Vera Moskaliova (VU)**
3	**2022-07-18**	**Updated Draft**	**Vera Moskaliova (VU)**
3.1	**2022-07-23**	**Commented Draft**	**Raimundas Matulevicius (UT)**
3.2	**2022-07-23**	**Commented Draft**	**Viktorija Triuskaite (Dorea)**
4	**2022-08-05**	**Updated**	**Vera Moskaliova (VU)**

Sisukord

PROJEKTI KIRJELDUS

Pettused on viimasel ajal üks suuremaid probleeme, kuna küberkurjategijad kasutavad petukampaaniate läbiviimiseks kiiremaid ja uuenduslikumaid tehnoloogiaid. Inimjõul töötava andmepüügikaitse arendamine nõuab kasutajate harimist, et nad oskaksid andmepüügirünnakuid ära tunda ja neile asjakohaselt reageerida.

Projekti eesmärk on koolitada kõrgkoolide üliõpilasi, õppejõude, ülikoolide töötajaid (kogukonna liikmeid), hariduskeskusi ja ettevõtlussektorit (tööandjaid ja töötajaid). Lisaks on projekti eesmärk ergutada ka sihtrühma kriitilist mõtlemist küberturvalisuse vallas.

Projektimeeskond on õpilastele ja teistele kasutajatele välja töötanud õppekava, e-õppematerjali, segaõppe keskkonna, enesehindamise testid, teadmiste hindamis- ja hindamissüsteemi ning mängupõhised simulatsioonid, et kaitsta andmepüügirünnakute eest. Samuti ehitada pädevused, mis aitavad neil ohtudest teadlikud olla ja võtta asjakohaseid ennetusmeetmeid.

Peamised intellektuaalsed väljundid on:

1. Uuringu analüüs ja soovitused: Andmepüügirünnakute vältimine ja kriitilise mõtlemise parandamine;

2. Kursuse õppekava;

3. Veebipõhine õppematerjal;

4. Andmepüügi simulatsioonid (mängimine);

5. Enese- ja teadmiste hindamise süsteemid;

6. Metoodilised juhised koolitajatele ja CyberPhishi mooduli rakendamine..

KOOLITUSE KORRALDAMISE JUHEND

Soovitused ja juhised koolituse korraldamiseks CyberPhishi moodulis osalejatele.

Cyberphishi kursust võiks korraldada kombineeritud õppemeetodil, kombineerides veebipõhiseid ja näost näkku õpetamise meetodeid. See tähendab, et teadmiste ja oskuste omandamise protsess põhineb nii silmast-silma kui ka veebipõhisel õppetööl: lektori juhitud seminarid, osalejate iseseisev töö veebipõhise õppematerjalide abil ning rühmakoostöö harjutused.

On oluline, et osalejad saaksid õppejõu tuge igal õppeprotsessi etapil (v.a teadmiste lõplik hindamine), st nad saaksid esitada huvipakkuvaid küsimusi, küsida abi, kui nad ei suuda või ei mõista, kuidas ülesannet täita, ja saada õppejõududelt tuge ja tagasisidet.

Sihtgrupp. Kõrgkooliõpilased on selle projekti peamine sihtrühm. Pilootkoolituse käigus valiti üliõpilased erinevatelt õppekavadelt. Nad kasutasid ja täiustatud koolitusmaterjale, harjutasid mängupõhiseid simulatsioone ning viisid läbi enese- ja teadmiste hindamise teste, et teha kindlaks oma teadmiste tase enne ja pärast kursust. Osalejatel peavad olema digitaalse kirjaoskuse põhioskused. Peale selle ei ole õpilaste teadmistel ega oskustel muid eeldusi.

Samuti on õpetajatel olnud juurdepääs partnerriikide viimastel uuringutel põhinevale kaasaegsele kursuse õppekavale; oma ala ekspertide poolt välja töötatud e-õppematerjalid, mida on rikastatud õpilastele mõeldud harjutuste, lisalugemismaterjalide (teaduskirjanduse) linkide ja seotud videoressurssidega. Seega uuendavad ja täiustavad osalejad oma olemasolevaid teadmisi. Õpetajad said tutvuda uudsete õpetamis- ja õppimismeetoditega, nagu enesetestid ja teadmiste testid veebikeskkonnas, aga ka simulatsioonid, mis atraktiivselt ja mänguliselt simuleerivad päriselu olukordi.

Muud projektist mõjutatud kasusaajad on haridustöötajad, ülikoolide töötajad, hariduskeskused ja ärisektor (tööandjad ja töötajad). Samuti saavad koolitatavad kasu oma olemasolevate teadmiste ja pädevuste avardamisest ja süvendamisest, tunnevad end veebis turvalisemalt, väldivad tundliku/isikliku teabe leket ja rahalisi kaotusi nii isiklikult kui ka organisatsioonides..

Peamine sihtrühm KÕRGHARIDUSE TUDENGID

- Kasutavad projekti käigus arendatud väljatöötatud materjali
- Harjutavad mängupõhiseid simulatsioone
- Teevad enesehinnangu ja teadmiste hindamise teste

Teisene sihtrühm ÕPETAJAD / KOOLITAJAD

- Juurdepääs kaasaegsele kursuse õppekavale ja e-õppematerjalidele
- Õpivad tundma uuenduslikke õpetamis- ja õppimismeetodeid, nagu enesetestid, teadmiste testid ja simulatsioonid

Muu sihtrühm ÕPETAJAD, ÜLIKOOLI TÖÖTAJAD, ÜLIKOOLI TÖÖTAJAD, HARIDUSKESKUSED JA ÄRISEKTOR (TÖÖANDJAD JA TÖÖTAJAD)

- Juurdepääs arendatud e-õppematerjalidele
- Täiustavad olemasolevaid teadmisi ja pädevusi küberturvalisuse valdkonnas

Joonis 1 Projekti sihtrühma analüüs

Koolituse kestus. Soovitatav koolituse kestus on 4-6 nädalat. Kogu õppekava on 30 tundi; see võrdub 1 EAP-ga. Iseõppimisel ja hindamisel soovitatakse arvestada sama palju tunde mooduli kohta. Osalejatel on soovitatav kulutada kursuse jooksul 2-3 tundi nädalas (koolitusmaterjali lugemine, testide ja stsenaariumide lahendamine).

Eeldatav treeningaeg võib olenevalt treeningust erineda. Pakutavad teemad ja harjutused/stsenaariumid on jagatud ühepäevasteks seanssideks. Eraldatud aja maht on paindlik; seetõttu pole iga päeva kohta täpset ajakava esitatud.

Koolitaja peaks materjali eelnevalt üle vaatama ja planeerima aja vastavalt konkreetsetele koolitusvajadustele.

Kursuse struktuur. Kursuse õppekava on üles ehitatud neljaks osaks:

1. Sissejuhatus küberturvalisusesse;
2. Ülevaade küberturvalisusest EL-is
3. Küberrünnakud – sotsiaalsed ründed ja andmepüük
4. Küberrünnakute mõistmine ja nendega toime tulemine

1. Sissejuhatus küberturvalisusesse	• See osa tutvustab tööstus 4.0 ajastul ettevõtete jaoks küberrünnakute väljakutseid, nagu mobiilsete tehnoloogiate, pilvandmetöötluse, asjade Interneti (IoT) ja suurandmete laialdast kasutamist, kolmandate osapoolte riske ja kasvavaid ohte, sealhulgas riiklikke ohte. Tutvustatakse ka küberturvalisuse valdkonnas kasutatud ja leitud definitsioone.
2. Ülevaade küberturvalisusest ELis	• See moodul tutvustab olemasolevaid ELi poliitikaid ja algatusi, mille eesmärk on edendada küberjulgeoleku kontseptsiooni. Samuti arutatakse küberturvalisuse õiguslikke aspekte nii ELis kui ka kogu maailmas.
3. Küberrünnakud – sotsiaalsed ründed ja andmepüük	• See moodul tutvustab küberrünnakuid, keskendudes eelkõige andmepüügile. Samuti käsitletakse üksikasjalikult sotsiaalsete rünnakute ja pööratud sotsiaalsete rünnete kontseptsiooni ning sotsiaalsuse tugevat seost küberrünnakutega. Moodul tutvustab ka erinevat tüüpi andmepüügirünnakuid ja tehnikaid koos reaalsete juhtumiuuringute näidetega.
4. Küberrünnakute mõistmine ja nendega toimetulek	• See moodul keskendub e-ohutuse kontseptsioonile ja küberohtudele ennetava lähenemise olulisusele küberhügieeni kontseptsiooni kaudu. Samuti pakub see üksikasjalikku lähenemist küberrünnakute äratundmisele ja käsitlemisele ning intsidentidele reageerimise plaanide väljatöötamisele ja rakendamisele, et minimeerida küberrünnakute mõju.

Joonis 2 Kursuse struktuur

Täpsem õppekava on leitav projekti veebilehel www.cyberphish.eu

Lühike versioon: https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A1_EST_Cyberphish-Short-Curriculum-Final.pdf

Pikk versioon: https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EST_Cyberphish-Full-Curriculum-Final.pdf

KOOLITUSTE KORRALDUSE SOOVITUSED

See osa juhendab koolituse korraldamist. Siin on ka CyberPhishi pilootkoolituse ajal kasutatud heade tavade soovitused, sealhulgas küsimustik enne koolitust, osaleja registreerimisnõuded, õppeprotsess ja teadmiste testi tingimused.

Koolituse reklaam

Oletame, et koolitus korraldatakse eraldi kursusena, mis ei sisaldu kõrgkooli õppekavas. Sel juhul on soovitatav avaldada pilootkoolitusele osalejaid kutsuv teadaanne veebilehel ja/või suhtlusvõrgustikes või saata potentsiaalsetele osalejatele personaalne kutse meili teel. Kutse teavitab potentsiaalset osalejat koolituse peamisest eesmärgist, kursuse kestusest, väljatöötatud või omandatud pädevustest andmepüügirünnakute äratundmisel ja sertifitseerimisest pärast kursuse läbimist. See võib sisaldada ka linki registreerimisvormile.

Kutse näide on toodud lisas 1. Failid ppt- ja pdf-vormingus on saadaval aadressil https://wiki.cyberphish.eu/ .

Sissejuhatav koosolek

Kursuse alguses, esimesel kohtumisel on oluline tekitada koolitaja ja osalejate vahel usaldust, motiveerida neid ning lasta neil üksteist tundma õppida. Tutvustage konsultatsiooni vormi (kontakt/veebipõhine) ja sagedust, näiteks kord nädalas, kolm korda kursuse kohta (alguses, lõpus ja keskel). Soovitatav on mainida väljakutseid, mis võivad tekkida platvormile registreerumisel (nt kinnitusmeil rämpsposti kausta).

Kohtumisel selgitatakse osalejatele, kuidas kasutada e-õppe keskkonda, lubatakse seda katsetama ja kutsutakse üles jagama probleeme, mis neil võivad tekkida, nii et hiljem pole kursuse alguses kahtlusi. Kohtumisel tutvustatakse ka CyberPhishi kursust.

Enne koolitust küsimustik

Koolituse mõju hindamiseks osalejate teadmiste edenemisele on soovitatav enne koolituse algust kasutada küsimustikku. Pilootkoolituse käigus kasutasid partnerid küsimustikke, mis koosnesid 20 küsimusest. Küsimustik töötati välja inglise keeles ja lokaliseeriti partnerite riikide keeltesse: eesti, kreeka, läti ja leedu keelde.

Küsimused valiti välja enesehinnanguküsimuste hulgast (20 60-st). Kõigile osalejatele esitati samad küsimused, kuid erinevas järjekorras. See küsimustik ei mõjuta osaleja tulemusi, kuid võimaldab mõõta osaleja teadmiste muutust.

Küsimustiku täitmine võtab aega 20–25 minutit. Enne küsimustiku täitmist peavad osalejad esitama oma e-posti aadressi. Kursuse õppekeskkonda (www.cyberphish.vukhf.lt) registreerumisel on soovitatav kasutada sama meiliaadressi. Osalejaid tuleks teavitada, et nad peavad kasutama kehtivat e-posti aadressi. Õpikeskkonnas tuleb kasutada sama meiliaadressi, mis osaleja registreerimisankeedil.

Tuleb märkida, et koolituseelse küsimustiku täitmine ei ole kohustuslik. See on ainult soovitus, kuid seda praktikat võiks kasutada juhul, kui olete huvitatud koolituse mõjust osalejatele.

Veebipõhine koolitus

Pärast lühikest sissejuhatavat etappi algab veebipõhine koolitus ja see kestab umbes kuu (4-6 nädalat). Koolitusprotsessi käigus kaasatakse osalejad erinevatesse õppetegevustesse, kasutades erinevaid koolitusmeetodeid ja vorme, mis hõlmavad näiteks: e-õppematerjaliga tutvumist, lisamaterjali lugemist, teemakohaste videote vaatamist, enesehinnangu testide tegemist ja teadmiste hindamise testid ja simulatsioonide lahendamine. Selle aja jooksul õpivad osalejad tundma küberturvalisust, mõistavad küberrünnakuid ja sotsiaalset manipuleerimist, õpivad ära tundma peamisi andmepüügi märke, mõistavad küberrünnakute käsitlemist, õpivad intsidentidele reageerimise kaudu kahjusid minimeerima. Edukas koolitusel osalemine sõltub osalejate oskusest oma aega ja tegevusi ise planeerida ning koostööst koolitajate ja teiste meeskonnaliikmetega.

Koolituse tulemuseks peaks olema teadmiste hindamise testi edukas sooritamine (hindega vähemalt 75%) ja automaatselt genereeritud tunnistuse väljastamine. Koolituse lõpus saavad osalejad uusi teadmisi ja oskusi, mida nad saavad kasutada oma igapäevaelus (näiteks Internetis otsimine, isiklik suhtlus suhtlusvõrgustikes, võõrastega telefonis rääkimine, õppimine, töökohal jne). Lisaks tõstavad nad ka iseenda enesekindlust.

Veebipõhise õppekeskkonna struktuur

Cyberphish.vuknf.lt õppeplatvorm pakub avatud juurdepääsu õppematerjalidele. Materjaliga saavad kõik soovijad vabalt tutvuda. Registreerimist ei nõuta. Andmepüügirünnakute äratundmist, enesetestide, teadmiste hindamise testi ja sertifikaadi saamiseks õpetavate simulatsioonide lahendamiseks on aga vajalik olla registreeritud kasutaja.

Õppematerjal. Menüüribal nupule *Õppematerjal* vajutades näeb kasutaja ekraani vasakus servas kursuse mooduleid. Mooduleid on neli: Sissejuhatus küberturvalisusesse; Ülevaade küberturvalisusest EL-is; küberrünnakud – sotsiaalsed ründed ja andmepüük; Küberrünnakute mõistmine ja nendega toime tulemine. Iga moodul koosneb mitmest teemast. Kui juhtum on valitud, kuvatakse õppematerjal ekraani keskosas. Kasutaja saab materjali alla laadida kasutaja arvutisse, klõpsates lingil *Laadi slaidid alla*.

Enesekontrolli testid. Registreeritud kasutajatel on rohkem võimalusi. Neil on võimalus sooritada õppimise eesmärgil enesehindamise teste. *Enesehinnangu* testi nupp ilmub siis, kui üliõpilane on mooduli materjali selgeks saanud. Seetõttu peab üliõpilane vajutama nuppu *Lõpetatud*, kui ta on iga mooduli teemaga kursis. Kui moodulis on kõik teemad märgitud Lõpetatuks, mis tähendab, et selle mooduli materjal on õpitud, siis avaneb enesehinnangu testi sooritamise võimalus vajutades nupule Enesehinnangu test. Testi käigus esitatakse õpilasele viis juhuslikku küsimust sellest moodulist.

Pärast testi kuvatakse süsteemis testi tulemused, kus on näha õpilase valitud vastused, õiged ja valed vastused, testi lahendamiseks kulunud aeg ja kogutud punktid. Õpilane saab testi uuesti sooritada, klõpsates nuppu Tee uuesti. Testi uuesti sooritamisel esitatakse 5 juhuslikku küsimust. Enesehindamise testi saab üliõpilane sooritada piiramatu arv kordi.

Simulatsioonid. Registreeritud kasutajad saavad simulatsioone lahendada. Need simulatsioonid on tegelike olukordade maketid. Ekraani vasakus servas on mooduliteemade kohal nupp Simulatsioonid. Õpilane saab neid igal ajal lahendada. Simulatsioonid on rühmitatud 7 rühma: ühtsus, meeldimine, konsensus, järjepidevus, autoriteet, nappus ja vastastikmõju. Simulatsiooni valimisel antakse olukorra kirjeldus. Simulatsioonid võivad töötada kahes režiimis: õppimise ja teadmiste kontrollimise eesmärgil. Esimeses režiimis näeb õpilane kogutud punkte ja üldist järeldust simulatsiooni lõpus. Teadmiste kontrollimise simulatsioonis arvestab õpilane lõpus simulatsiooni käigus tehtud valikuid ja saab tagasisidet koos kommentaaridega. Mentor peaks otsustama, mitu simulatsiooni osaleja peab lahendama. Näiteks piloodi käigus pidi iga osaleja lahendama vähemalt 20 enda valitud simulatsiooni..

Teadmiste kontroll. Registreeritud kasutajad saavad sooritada teadmiste testi ja saada sertifikaadi. Teadmiste testi nupp ilmub ekraani vasakusse serva kursuse moodulite kohale, kui üliõpilane on kogu materjali selgeks õppinud ja kõik teemad lõpetatuks märkinud. Test loetakse sooritatuks, kui tulemus on vähemalt 75%. Selle lõputesti läbinud osalejad saavad tunnistuse. Kui osaleja testi ei soorita positiivselt, saab ta teemasid korrata ja pärast õppimiseks kuluvat aega uuesti sooritada teadmiste lõputesti. Teadmiste testi saab sooritada kolm korda.

Hinnangud. Süsteem arvutab hinnanguid, et muuta õppeprotsess õpilastele atraktiivsemaks. Kursusel osaleja näeb oma hinnangut ja kogutud punkte üldhinnangu tabelis. Hinnangud põhinevad ennast hindavatel testidel ja simulatsioonidel. Reitingutele pääseb ligi ekraani ülaosas olevast menüüpunktist Reitingud. Õpilase simulatsioonireiting arvutatakse kõigi lahendatud simulatsioonide parimate tulemuste liitmisel. Vastavalt sellele arvutatakse õpilase enesehindamise testi hinne kõigi sooritatud enesetestide parimate punktisummade liitmise teel. Õpilased näevad ka oma õppimise edenemist. Seda kuvatakse kursuse moodulite kohal ekraani vasakus servas ja ekraani ülaosas oleva kasutajamenüü kaudu. Kasutajamenüü kaudu saab õpilane muuta kasutajanime ja parooli, näha kogutud märke, enesetestide ajalugu ja simulatsioonide ajalugu.

Tunnistus. Sertifikaadid (PDF-vormingus) genereeritakse automaatselt kõikidele osalejatele, kes on läbinud kursuse ja sooritanud Teadmiste-hindamistesti vähemalt 75%. Sertifikaadi näidis on toodud lisas nr 2.

Kursuse läbimisel antakse kõigile osalejatele tunnistused. CyberPhishi kursuse läbimine ei anna akadeemilist ainepunkti.

Ligipääsetavus

Väljatöötatud e-kursus on saadaval viies keeles: inglise, eesti, kreeka, läti ja leedu keeles. Seda majutatakse aadressil https://cyberphish.vuknf.lt/ . Pilt õppeplatvormi põhiekraanist on toodud allpool.

Joonis 3 Õppeplatvormi ekraanikuva

Heade tavade soovitused proovikoolitusest. Soovitatav on õpilastele välja töötada reeglid ja juhised. Küsimustikud kursuse alguses ja lõpus on vabatahtlikud. Muid vahendeid saab kasutada nagu tavakoolituses.

Juhised õpilastele

Selles osas anname koolituse korraldamiseks soovituslikud sammud:

1. samm. Koolituse eelne küsimustik. Enne koolitust täitke küsimustik. Esitage kehtiv e-posti aadress, mida kasutatakse hiljem ka e-õppe süsteemis.

2. samm. Looge kasutaja e-õppekeskkonda. Logige e-õppekeskkonda sisse aadressil https://cyberphish.vuknf.lt/login sama e-posti aadressiga, mida kasutasite küsimustikus.

Märkus: Kui õpilane ei ole süsteemist kinnituskirja saanud, on vaja kontrollida rämpsposti kausta. Kinnitusmeil võib sattuda rämpsposti kausta..

3. samm Sisenege e-õppe keskkonda.

Logige sisse saidil https://cyberphish.vuknf.lt isiklike mandaatidega.

4. samm. Õppematerjaliga tutvumine.

Pärast sisselogimist tutvuge kogu koolitusmaterjaliga ehk nelja teema ja alateemaga (vt allpool). Pärast iga teema läbimist märkige see lõpetatuks.

Teemad ja alateemad:

1. Sissejuhatus Küberturvalisusesse;
1.1. Taust - neljanda tööstusrevolutsiooni väljakutsed;
1.2. Küberturvalisuse ajalugu;
1.3. Küberturvalisuse mõisted;
2. Ülevaade küberturvalisusest ELis;
2.1. Küberturvalisuse edendamine Euroopa Liidus;
2.2. Küberjulgeoleku õiguslikud aspektid;
2.3. Ülevaade küberturvalisuse valdkonna tendentsidest;
3. Küberrünnakud –andmepüük ja sotsiaalsed ründed;
3.1. Sissejuhatus küberrünnakutesse;
3.2. Sotsiaalse ründe tehnikad ja manipuleerimine;
3.3. Suhtlusrünnaku tüübid ja tehnikad;
3.4. Juhtumiuuringud;
4. Küberrünnakute mõistmise ja nende toimetuleku ülevaade.
4.1. Alusteadmised e-turvalisusest;
4.2. Ennetavad tegevused;
4.3. Andmepüügirünnakute äratundmine;
4.4. Küberrünnakutega toimetulemine;
4.5. Kahjude minimeerimine juhtumitele reageerimise kaudu.

5. samm. Täitke neli enesehinnangu testi. Pärast iga teema õppimist täitke enesehinnangu test.

6. samm Käivitage/lahendage/sooritage simulatsioonid. Õppe käigus sooritada õppeprotsessi osana simulatsioone.

7. samm. Täitke teadmiste hindamise test. Lõpuks sooritage lõputest vähemalt 75% tulemusega.

8. samm. Pärast viimase testi sooritamist täitke osalejatele kursusejärgne küsimustik tkoolituse kohta.

Märkus: Järgnevaid tööriistu kasutati pilootkoolituse ajal, kuid tööriistu saab kasutada ka tavakoolituses.

Lõpukohtumine

Lõpu koosolekul on mitu eesmärki: esiteks võimaldab see osalejatel täita koolitusjärgset küsimustikku, teiseks võimaldab see osalejatel kursuse kohta arvamust avaldada. Lõpuks võiks arutada teadmiste hindamise testide protsessi, küsimustele vastamise raskusi ja väljakutseid ning muid küsimusi.

Kursusejärgsed küsimustikud

Pilootprojektis paluti osalejatel pärast viimase testi sooritamist täita osalejate jaoks kursusejärgne küsimustik. Küsimustik koosneb punktidest, milles palutakse esitada üldist teavet, nagu e-post, sugu, amet ja küsimused osalejate teadmiste hindamise kohta konkreetsetes küberjulgeoleku teemades pärast CyberPhishi koolituskursuse lõpetamist, osaleja kogemusi simulatsioonide kasutamisega. Lisaks esitatakse küsimusi kursuse eesmärkide, veebivormingu lähenemisviisi sobivuse, kursuse sisu, kestuse, koolituse ja toe ning õppeplatvormi kasutatavuse kohta. Ankeedi näide on toodud lisas nr 3.

Koolitajatel ja mentoritel paluti täita ka pärast pilooti koolitajate jaoks kursusejärgset küsimustikku. Küsimustik koosneb punktidest, milles palutakse esitada üldist teavet, nagu e-posti aadress, nimi, riik, samuti küsimusi kursuse ülesehituse ja sisu, aja kestuse, teemade asjakohasuse kohta sihtrühma jaoks, kursuse teemade terviklikkuse, ulatuse kohta. kursus on saavutanud oma eesmärgi tutvustada õpilastele küberturvalisust ja andmepüügi. Ankeedi näide on toodud lisas nr 4.

JUHTNÖÖRID ÕPPEPLATVORMI KASUTAMISEKS

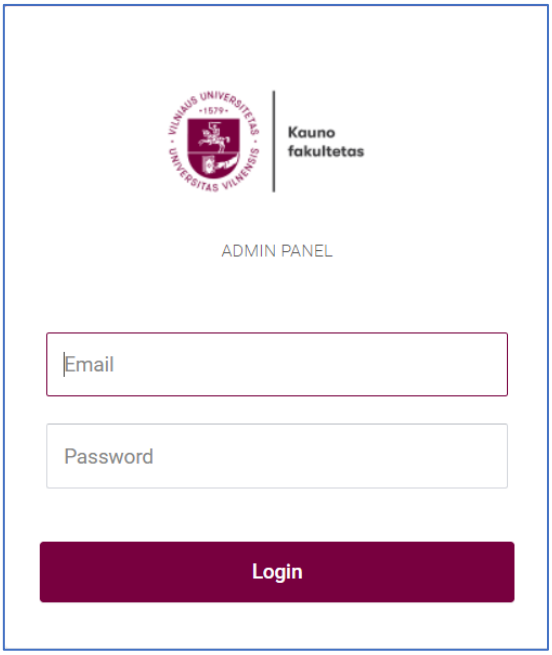
E-õppekeskkonnas aadressil https://cyberphish.vuknf.lt majutatud õppematerjalid on kõigile külastajatele kättesaadavad ja tasuta. Õppematerjal on saadaval viies keeles: inglise, eesti, kreeka, läti ja leedu keeles. Registreerimata külastajad saavad ainult vaadata õppematerjali, kuid nad ei saa sooritada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

Kasutusjuhend on esitatud veebisaidil https://wiki.cyberphish.eu/ dokumendis *User_Manual_for_training-Participants.pdf*. See dokument kirjeldab õppeplatvormi kasutamist.

Õpetajate keskkond

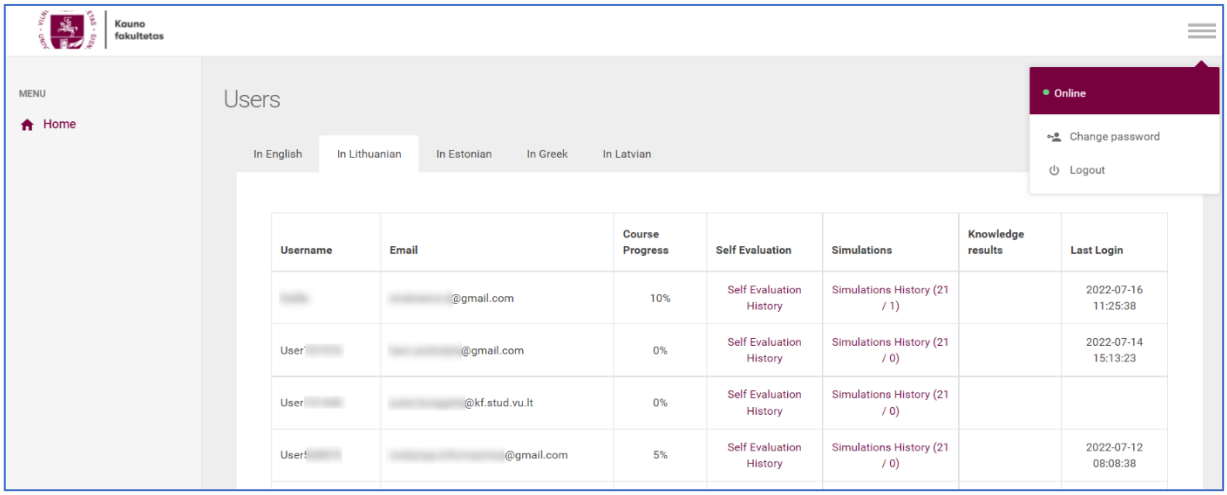
Õpetaja keskkonnas saab jälgida õppesüsteemi registreerunud osalejaid, nende õppimise edenemist protsentides, sooritatud enesetestide ajalugu, simulatsioonide ajalugu, teadmiste kontrolli hindeid ning testimise kuupäeva ja kellaaega. viimane sisselogimine.

Õpetajate keskkonna sisselogimisaadress: https://cyberphish.vuknf.lt/admin-panel . Sisselogimisaken on toodud allpool:



Joonis 4 Õppejõu vaatesse sisenemine

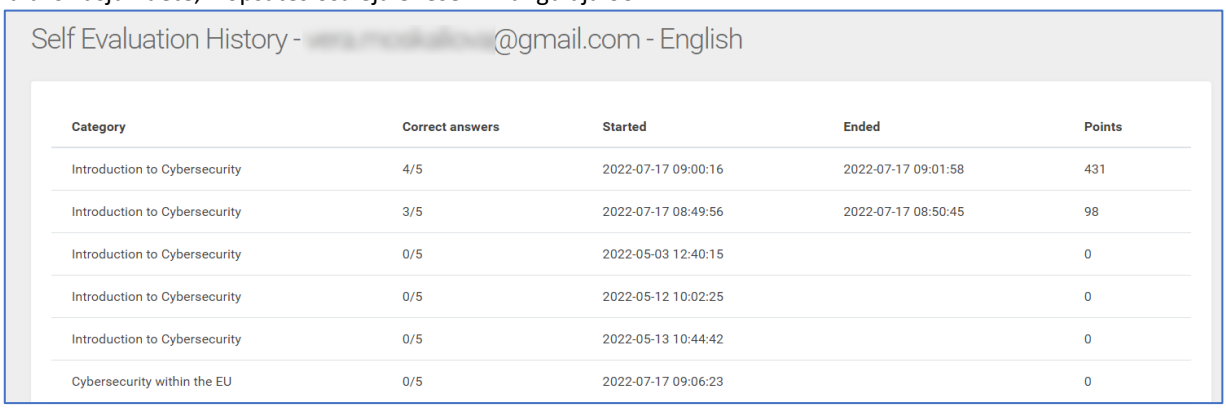
Kui sisselogimisandmed on sisestatud, kuvab süsteem õpetajale osalejate nimekirja. Õpetaja saab jälgida osalejate õppimise edenemist keelte kaupa (inglise, leedu, eesti, kreeka ja läti keel). Allpool on toodud õpetaja keskkonna põhiekraan:



Joonis 5 Õppejõu keskkonna põhivaate näide

Enesehindamise testide ajalugu

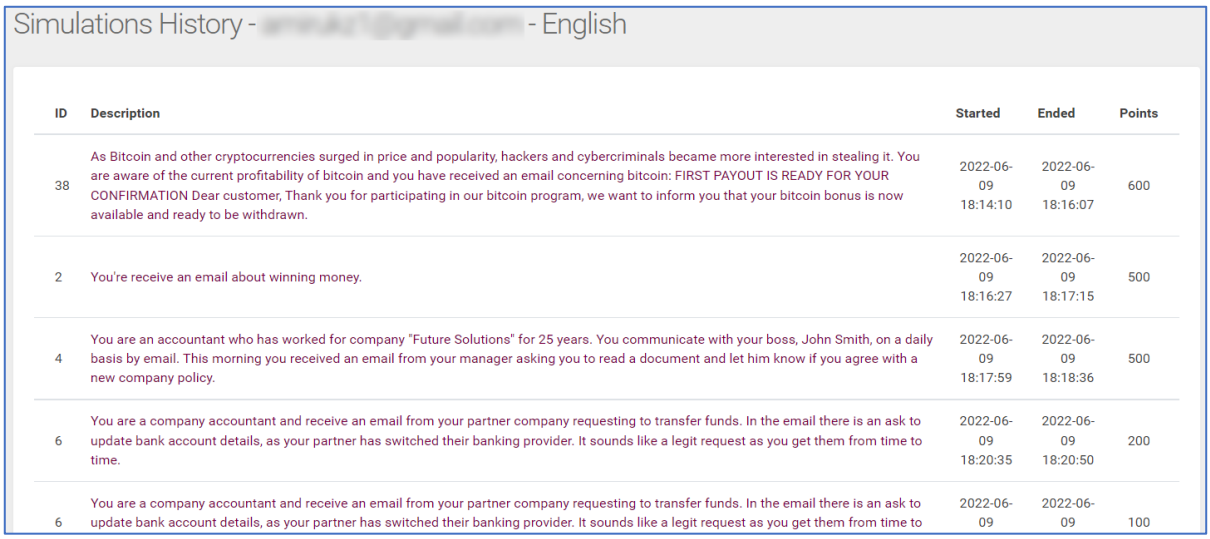
Neid üksikasju näete, klõpsates osaleja enesehinnangu ajalool:



Joonis 6 Osaleja enesehinnangu testide ajalugu

Simulatsioonide ajalugu

Neid üksikasju näete, klõpsates osaleja simulatsioonide ajalool:



Joonis 7 Osaleja simulatsioonide ajaloo vaate näide

TÖÖ UUENDUSLIKUTE MEETODITEGA (SIMULATSIOONID, LOENGUD, SEMINARID, PRAKTILISED KOOLITUSED, INTERNETITÖÖRIISTADE KASUTAMINE JMS)

Simulatsioon imiteerib tegelikke andmepüügirünnakuid, esitades protsessi kasutajale mängulises vormis. Simulatsiooni põhieesmärk on aidata inimestel parandada küberturvalisuse ja andmepüügiga seotud kriitilist mõtlemist, tuvastades andmepüügi, rämpsposti, küberkiusamise jms juhtumeid. IO1 põhjal töötati välja soovitused simulatsioonide jaoks, mis keskenduvad reaalse elu juhtumiuuringute kohandamisele õppeprotsessis.

Simulatsioon sisaldab olukorra kirjeldust, eesmärki, tegelasi, rünnaku tüüpi ja mitmeid (3-4) vastusevariante kasutaja käitumisele. Simulatsioonid olid mõeldud selleks, et hinnata kasutaja võimalikku/tõenäolist käitumist, tema võimalikke kaalutlusi/muresid ja otsuseid sellises olukorras. Esitatud simulatsioonid koosnevad kolmest sügavuse tasemest. Kui üks probleemi/olukorra valikutest on valitud, mõjutatakse ja esitatakse edasised võimalikud lahendused juhtumi lahendamiseks.
Rakendatakse simulatsiooni õppimise ja teadmiste kontrollimise eesmärgil. Õppimise eesmärgil simulatsiooni lahendamisel näeb õpilane kogutud punkte ja simulatsiooni lõpus üldist järeldust. Teadmiste testimise eesmärgil simulatsiooni lahendades näeb õpilane simulatsiooni käigus tehtud valikuid ja saab simulatsiooni lõpus tagasisidet koos kommentaaridega. Kui simulatsioon lahendati valesti, on kasutajal soovitatav simulatsioon uuesti lahendada.

JÄRELDUSED JA SOOVITUSED

See dokument on välja töötatud kõigile koolitajatele ja mentoritele, kes pakuvad õpilastele nõu ja koolitust. Projekti konsortsium loodab, et nad leiavad kasulikke juhiseid selle kohta, kuidas süsteemi kasutada ja kuidas pakkuda koolitust inimestele, kes soovivad õppida tundma küberrünnakuid, eelkõige andmepüügi ja sotsiaalse manipuleerimise kohta, ning õppida ära tundma küberrünnakute peamised tunnused. Potentsiaalsetelt kasutajatelt nõutakse digitaalse kirjaoskuse põhioskusi. Muid eeldusi kasutaja teadmistel või oskustel pole.

Õpilastel ja töötajatel puuduvad teadmised andmepüügist, sotsiaalsest manipuleerimisest, küberrünnakutest ja nende andmete turvalisusest, selgub projekti partnerite poolt 2020. aastal Eestis, Küprosel, Lätis, Leedus ja Maltal läbi viidud uuringust (vt https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EST_CYBERPHISH-REPORT_survey-results.pdf). See toob kaasa mitte ainult isikuandmete ja isiklike rahaliste vahendite kadumise andmepüügi või küberrünnaku korral, vaid ka ettevõtete/organisatsioonide tundliku teabe ja rahaliste ressursside kadumise.

Tuginedes partnerriikides läbi viidud uuringule (vt https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A2_EST_CYBERPHISH-REPORT_study-analysis.pdf) küberturvalisusega seotud kõrghariduse õppekavade kohta nagu ka eraettevõtete pakutavate küberjulgeoleku koolitusprogrammide puhul, on välja töötatud nelja moodulit hõlmav õppekava:

- Sissejuhatus küberturvalisusesse;
- Küberturvalisuse Euroopa Liidus;
- Küberrünnakud: Andmepüük ja sotsiaalsed ründed;
- Küberrünnakute mõistmine ja nendega toimetuleku ülevaade

Lisateavet koolitajate ja mentorite koolituseks ettevalmistamise kohta leiate kogu CyberPhishi kursuse õppekavast (vt https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EST_Cyberphish-Full-Curriculum-Final.pdf)

Pilootkoolitusel osalejad võtsid CyberPhishi koolituskursuse hästi vastu. Nad tunnistasid selle kasulikkust nii tavakasutajate kui ka ettevõtte töötajate igapäevastes IT-alastes tegevustes. Lisateavet leiate *aruandest IO6 A2: Kursuse rakendamise juhised*.

Veebiõppekursus integreerib koolitusmaterjali PDF-vormingus – kokkuvõtlikult ja selgelt, ilma et koolitatavaid rohke lugemisega üle koormataks. Neile, kes soovivad konkreetse teema kohta rohkem teada saada, on iga PDF-dokumendi lõpus lingid välistele allikatele.

Enesehindamise teste ja simulatsioone kasutatakse selleks, et aidata osalejatel koolitusmaterjali paremini omastada. Simulatsioonid annavad tagasisidet, mis aitab kas koolitusmaterjali üle vaadata või uusi asju õppida. Lisaks saab kursuse jooksul kasutada simulatsioone kahes režiimis: õppimiseks ja teadmiste kontrollimiseks.

Kursus võib olla mõeldud üliõpilastele kursuse osana, lisamaterjalina või eraldi moodulina/kursusena.

VIITED

1. IO1 A1: Recognising Phishing and Skills Gaps report
   https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EN_CYBERPHISH-REPORT_survey-results.pdf
2. IO1 A2: Analysis of existing Cybersecurity training programmes report.
   https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A2_EN_CYBERPHISH-REPORT_study-analysis.pdf
3. IO2 A1: Short version of curricula for dissemination
   https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A1_EN_Cyberphish-Short-Curriculum-Final.pdf
4. IO2 A2: Extended version of curricula for training material development and for trainings
   https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EN_Cyberphish-Full-Curriculum-Final.pdf
5. User_Manual_for_training-Participants.pdf
   [link]

LISAD

Lisa 1. Näide veebipõhisest kutsest CyberPhishi kursusele

Näide prinditud CyberPhishi kursuse kutse vormist

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.

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Lisa 2. CyberPhishi kursuse läbimise tunnistuse näide

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

Lisa 3. Kursusejärgse küsimustiku näide CyberPhishi kursustel osalejatele

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

Lisa 4. Kursusejärgse küsimustiku näide CyberPhishi kursuste koolitajatele, konsultantidele ja mentoritele

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!