Andmepüügi vastu kaitsemine 4. tööstusrevolutsiooni ajastul (CyberPhish)

CyberPhish laiendatud õppekava

Projekti periood: November 2020 – November 2022

Projekti number.: 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.

Sisukord

SISSEJUHATUS

Cyberphishi laiendatud õppekava eesmärk on pakkuda kokkuvõtlikke, kuid kaugeleulatuvaid küberturvalisuse mooduleid, pöörates erilist tähelepanu andmepüügile. Dokument on jagatud kolmeks põhiosaks, nimelt:

- **Koolitaja ettevalmistamise kursus** - tutvustab õppekava edastamiseks õiget mõtteviisi ja kontrollib koolitajale seatud nõudeid.
- **Näost näkku / veebikoolitus** – tutvustab koolituse sius, vormi ja läbiviimise korda.
- **Õppekava (e-õppe mooduli) struktuur** - kirjeldab üksikasjalikult õppekava ülesehitust

Oluline on märkida, et kuigi õppekava läbiviimine on mõeldud hübriid-õppimise lähenemisviisina, võimaldab selle ülesehitus paindlikkust õppetöös. Õppekava tegeleb küberturvalisuse tutvustamisega, pöörates erilist tähelepanu andmepüügile (*phishing*). See on suunatud ettevõtetele ja üksikisikutele laiemalt ning on mõeldud nii tööstuse 4.0 kui ka selle võimalike julgeolekuprobleemide saavutamiseks. Õppekava edastamise kaudu omandavad õppijad oskused küberrünnakute tuvastamiseks ja käsitlemiseks ning kuidas kaitsta seadmeid ja andmeid toore jõu rünnakute eest.

1. KOOLITAJA ETTEVALMISTAMISE KURSUS

Koolituskursuse ülesehitus on loodud nii näost näkku klassiruumis kui ka veebis läbiviimiseks. Soovitatav kestus võib varieeruda sõltuvalt osalejate arvust ja läbiviimise nõuetest. Koolitaja koolituskursuse praktilise olemuse tõttu soovitatakse, et koolitusrühmas oleks maksimaalselt kuni kaksteist osalejat (tulevast koolitajat).

Koolitusprogrammi struktuur on toodud allolevas tabelis. Tabelis on välja toodud soovitatavad teemad ja soovitatav kestus. Koolitusorganisatsiooni ja treeneri otsustada on kasutada, pikendada, vähendada või suurendada koolitaja programmi kestust ja sisu vastavalt olukorrale ning vastavalt koolitaja ja õppijate varasemale kogemusele.

On asjakohane märkida, et kursus koolitajate ettevalmistamiseks on mõeldud osalejatele, kes on juba küberturvalisuse teemaga kursis. Ürituse korraldajad võiksid enne kursust koolitajatele saata küsimustiku, et koguda osalejate taseme ja ootuste kohta infot. Küsimustiku tagasiside põhjal võiksid läbiviijad koolitusürituste kava vastavalt sellele kohandada.

Struktuur	Koolitaja ettevalmistamise 4 päevane kursus on mõeldud varasema kogemuse ja kübervaldkonna teadmistega osalejale.	
Eesmärk	Koolituse eesmärk on anda osalejaile teadmised ja oskused andmepüügi küberturvalisuse valdkonna koolituse läbiviimiseks.	
Kava		
1. päev	Päev õpilase elus	
Kirje nr	*Teema*	*Soovituslik kestus*
D1-01	Sissejuhatus ja üksteise tundmaõppimise seanss • Tutvumise või meeskonnatöö harjutus - *Low Tech Social Network (jäämurdja)* - *Marshmallow Challenge (meeskonnatöö)*	0.5 tundi
D1-02	Erinevate õpistiilide mõistmine ja nendega tegelemine • Lühike sissejuhatus erinevatesse õppimisstiili mudelitesse - *Erinevate õpistiilide (nt 7 õppimisstiili, Kolbi õppetsükkel) tutvustamine.*	0.5 tundi

D1-03	Koolitaja õppijana – Õppemetoodikate kogemine (1. osa) Selle seansi eesmärk on kaasata koolitajad õpilastena erinevate pedagoogiliste olukordadesse, õpetamismeetodite mõistmisse ja kogemisse. Tulevased koolitajad tegutsevad õpilaste rollis auditoorselt või virtuaalselt (veebiklassis). • Sissejuhatus erinevatesse pedagoogilistesse seadetesse ja õpetamismeetoditesse - *Seansi esimeses osas tutvustab peakoolitaja mitmeid erinevaid pedagoogilisi olukordi ja materjali edastusviise. (nt töötoad, praktilised harjutused, arutelud, väitlus, juhtumianalüüsid jne)* • Erinevate õppemeetodite kogemine - *Seansi teises osas puutuvad koolitajad / õppijad kokku erinevate õpetamismetoodikatega.*	3 tundi
D1-04	Võrgustumise paus	0.5 tundi
D1-05	Koolitaja kui üliõpilane - õppemetoodikate kogemine (2. osa) • Arutelu, tagasiside ja parimate tavade jagamine *- tunnete, hoiakute ja tagasiside jagamine 1. osa kogemuste kohta* *- parimate tavade jagamine õpilaste õpikogemuse parandamiseks*	1 tundi
D1-06	1. päev – kokkuvõte ja järeldused	0.5 tundi
2. päev	Oluliste pehmete oskuste värskendamine	
Kirje nr	*Teema*	*Soovituslik kestus*
D2-01	2. päeva sissejuhatus - pehmete oskuste tähtsus • Lühike tutvustus pehmete oskuste olulisusest õppetunni andmisel - *Lühitutvustus, mis keskendub peamiselt teema esitlusele, soodsa õppimiskeskkonna loomisele, klassiruumi haldamisele ja konstruktiivse tagasiside andmisele*	0.5 tundi
D2-02	Olulised pehmed oskused treeningute läbiviimiseks (1. osa) • Ettekande oskused - *esitluse struktureerimine (nt slaidide arv ja formaat, veebitööriistade kasutamine)* - *esinemise aspektid (nt kehakeel, hääle tonaalsus)* - *lühikeste esitluste harjutamine (näost näkku või veebis) koos vastastikuse tagasiside ja kommentaaridega* • Hõlbustamise oskused - *rühmaarutelu hõlbustamine (nt küsimuste uurimine, ümbersuunamine ja sõnastamine)* - *koostöö hõlbustamine (nt ajurünnak, mõttekaart, kuus mõttemütsi)* • Digitaalsete tööriistade kasutamine sotsiaalsete oskuste toetamiseks - *Digitaalsete tööriistade kasutamine esitluste ja arutelude hõlbustamiseks* - *Sissejuhatus digitaalsetesse / veebitööriistadesse, sealhulgas, kuid mitte ainult, MS Teams, Zoom, Skype, Google Meet, Mentimeter, Kazoom ja nii edasi.*	2 tundi
D2-03	Võrgustumise paus	0.5 tundi
D2-04	Olulised pehmed oskused treeningute läbiviimiseks (2. osa) • Klassiruumi haldamine - *Parimate tavade jagamine õppijate kontrollimiseks, vaimustamiseks ja kaasamiseks nii näost näkku kui ka veebis* • Tõhusa ja konstruktiivse tagasiside andmine	2 tundi

	- *Lühike rühmavestlus (näost-näkku või veebis toimuv seminar), milles analüüsitakse tõhusaid ja konstruktiivseid tagasiside võtteid*	
D2-05	2. päev – kokkuvõte ja järeldused	0.5 tundi
Day 3	Õppekava tutvustus	
Kirje nr	*Teema*	*Soovituslik kestus*
D3-01	Sissejuhatus õppekava ülesehitusse ja õpetamise viisidesse *Lühike näost näkku või veebis toimuv sessioon, kus tutvustatakse õppekava struktuuri, sealhulgas õpitulemuste olulisust koos õpetamise viisidega.*	1 tundi
D3-02	Õppekava teemade üksikasjalik analüüs (1. osa) *Seletus õppekava kahe esimese sissejuhatava mooduli kohta*	1 tundi
D3-03	Võrgustumise paus	0.5 tundi
D3-04	Õppekava teemade üksikasjalik analüüs (2. osa) *Seletuskoht õppekava kahe viimase mooduli kohta*	3 tundi
D3-05	3. päev – kokkuvõte ja järeldused	0.5 tundi
Day 4	Lõppseminar - oluliste pehmete oskuste hindamine õppekava abil	
Kirje nr	*Teema*	*Soovituslik kestus*
D4-01	Töötoa tutvustus *Viimane päev koosneb töötoast, kus eeldatakse, et kõik osalejad mõtlevad 1. päeval kogutud kogemustele, harjutavad 2. päeval omandatud oskusi ja kasutavad 3. päeval selgitatud õppekava. Hindamine toimub teiste osalevate koolitajate tagasiside vormis. Töötoa kestus sõltub osalejate arvust.*	0.5 tundi
D4-02	Esitlusoskuste hindamine *Koolitajatel palutakse koostada ja pidada 10-minutiline ettekanne, valides kavandatud õppekavast mis tahes teema. Igale ettekandele järgneb vastastikune hinnang ja tagasiside esitluse kohta, sealhulgas kasutatud uudsed tehnikad.* Treeneri äranägemisel võidakse kasutada muid hindamisviise	0.25 tundi osaleja kohta (maksimaalselt 3h)
D4-03	Võrgustumise paus	0.5 tundi
D4-04	Hõlbustusoskuste hindamine *Koolitajatel palutakse hõlbustada 10-minutilist seanssi, valides mis tahes teema kavandatud õppekavast. Igale sessioonile järgneb vastastikune hindamine ja tagasiside nii hõlbustusoskuste kui ka klassi juhtimise kohta.* Treeneri äranägemisel võidakse kasutada muid hindamisviise.	0.25 tundi osaleja kohta (maksimaalselt 3h)
D4-05	4. päev – kokkuvõte ja järeldused	0.5 tundi

2. NÄOST NÄKKU / VEEBIKOOLITUS

Õppijate integreerimisel õppimiskogemusse kasutatakse neljaastmelist lähenemisviisi. Lühidalt

VEEBIPÕHINE ORIENTEERUMISSESSIOON	AVAÜRITUS	MOODULI ÕPETAMINE	LÕIMIMISE TÖÖTUBA	MOODULI ÕPETAMINE	KURSUSE ARUANDLUS	KOKKUVÕTTEV VÕRGUSTUMINE
Teave koolitusasutuse kohta - *Eesmärgid* - *Poliitika* - *Reeglid*	Koolitaja tutvustus Koolitusasutuse juhtimise infosüsteem (MIS) - *Süsteemi tutvustus* - *Kasutaja / parool* - *Ressursid* - *Litsentsi info* - *KKK / tõrkeotsing* Ametlik kursuse õppekava Hindamise metoodika Suhtluskanalite tutvustus	Koolituse sisuline läbiviimine. Täpne päevade arv sõltub koolituspäeva pikkusest. Esimene osa (15 tundi)	Veebi tagasiside vorm aktuaalsete heade tavade ja muude lahendamist vajavate tavade kohta. Arutelu osalejatega	Koolituse sisuline läbiviimine. Täpne päevade arv sõltub koolituspäeva pikkusest. Teine osa (15 tundi)	Andmete kogumine - *Koolitaja tagasiside aruanne* - *Osalejate tagasiside vormi vastuste analüüs.*	Fookussessioon - *Koolituse analüüs* - *Kokkuvõte* - *Järgmised sammud*
JÄRJEPIDEV KOOLITAJA TUGI OSALEMISEL						
JÄRJEPIDEV SÜSTEEMI TUGI KOOLITUSE LÄBIVIIMISEL						

i. Isejuhitav virtuaalse orientatsiooni seanss

Esimene samm alustamiseks on osalemine veebipõhisel orienteerumisseansil. Seanss on läbitav osalejale sobivas tempos, mis võimaldab osalejal paindlikult õppida õppeteenust pakkuva asutuse (koolitusasutuse) kohta.

Huvitatud õppijatel on võimalus tutvuda koolitusasutuse ja konkreetse osakonnaga seotud (kuid mitte ainult) teabega. Esile tuuakse osakondade eesmärgid, põhimõtted ja protseduurid ning koolitusasutuse visioon. Nägemis- ja kuulmispuudega õpilaste toetamiseks peavad kõik juhendmaterjalid ja esitlused olema pealkirjaga ja ekraanilugejaile kättesaadavad.

ii. Avaüritus

Iga uut gruppi õpilasi tervitatakse avaüritusel, mis võib toimuda näost näkku väi veebi vahendusel. Avaürituse eesmärk on koolitaja tutvumine õpilastega ja osalejate omavaheline tutvumine. Samuti tutvustatakse kursuse ülesehtust ja läbimise tingimusi.

Kui koolitaja on saanud loa kasutada koolitusasutuse infosüsteemi, esitab ta lühikese tutvustuse kasutatava süsteemi kohta. Õppijatele antakse kasutajatunnused ja nad läbivad paroolide seadistamise. Lisaks antakse juhiseid juurdepääsuks ressurssidele, mida õppijatel on lubatud kasutada. Sellega seoses loetakse läbi ja allkirjastatakse kasutuspoliitika. Tunnistades, et see võib tunduda rohke tehnilise teabena, tehakse edaspidiseks kasutamiseks kättesaadavaks dokument KKK ja tõrkeotsing. Koolitaja lõpetab kohtumise joonistades täpse pildi ametlikust kursuse õppekavast, hindamismetoodikast ja suhtluskanalitest.

iii. Õppijate võimestamine pideva toetuse kaudu

Lisaks küberjulgeoleku õppekursusega õppijate teadmiste, oskuste ja hoiakute arendamisele möönab koolitusasutus õppijate muutuvate vajaduste tuvastamise ja neile reageerimise olulisust. Ühe näitena on koolitajad regulaarselt kättesaadavad õpilastega positiivseks suhtlemiseks kursuse vältel.

Pärast ettemääratud arvu lõpetatud õppeseansse korraldatakse lõimimise töötuba. Kogutakse ja arutatakse õppijate tagasisidet, et teha kindlaks, kui hästi kursuse edasijõudmine vastab õpilaste ootustele ja koolitusasutuse standarditele.

Enne lõimumise töötuba võib andmete kogumise hõlbustamiseks kasutada erinevaid koolituse hindamise tööriistu. Lõimumise töötoas tuvastatud edukuse näitajad on muuhulgas õpilaste uute oskuste ja teadmiste omandamine, positiivne suhtumine õppimiskogemusse ja õppimise efektiivsus. Seda teavet kasutatakse omakorda kursuse programmi kvaliteedi paranemise tagamiseks.

iv. Kursuse aruandlus

Kursuse lõpetamine on oma olemuselt märkimisväärse saavutuse tunnustamise hetk.

Kokkuvõttev võrgustumine aitab osalistel jagada enda osalemise ja kursuse lõpetamise positiivseid emotsioone. Ühtlasi analüüsib koolitusasutus koolituse läbiviimist ja edukust. *Kirkpatrick's nelja tasemelist koolituse hindamise mudelit*[1] kasutatakse koolituse hindamiseks.

Enne võrgustumise kohtumist kogub koolitusasutus järgneva info kokku:

- *Koolitaja aruanne ja hinded.*
  See aitab mõõta, kui palju on õppijate teadmised ja oskused pärast õppeprogrammi algust muutunud.
- *Osalejate tagasiside.*
  Digitaalne koolituse hindamise vorm, tagasiside küsimine üldise rahulolu kohta õppekogemusega ja õpingute rakendatavuse kohta töökohal (või muul viisil).

Kui need andmed on käes, toimub võrgustikusündmuse ajal fookusessioon, kus koolitusasutus saab struktureeritud paneeldiskussiooni kaudu kvalitatiivselt mõõta tulemusi, näiteks tootlikkust, kvaliteeti ja tõhusust.

3. ÕPPEKAVA (E-ÕPPIMISE) STRUKTUUR

3.1 Sissejuhatus

Õppekava on suunatud nii ettevõtetele kui ka eraisikutele, kes kogevad Tööstuse 4.0 paratamatuid positiivseid ja negatiivseid mõjusid ning kes soovivad rohkem teada saada ja paremini kaitsta ennast neljanda tööstusrevolutsiooni põhjustatud julgeolekuprobleemide eest.

Õppekava on üles ehitatud neljas erinevas osas, alustades küberturvalisuse valdkonna tutvustamisest ja sellega seotud väljakutsetest, mille on toonud Tööstus 4.0. Õppekavas käsitletakse küberturvalisust ja selle õiguslikke aspekte Euroopa tasandil ning kuidas küberturvalisust Euroopa Liidus edendatakse.

Arvestades sotsiaalsete aspektide tähtsust ja mõju ning selle seost küberrünnakutega, on õppekavas selgitatud küberrünnakute äratundmist ja seda, kuidas rünnakutega toime tulla, et vältida katastroofilisi ja pöördumatuid mõjusid.

Peale erinevate moodulite lühikese kirjelduse sisaldab õppekava struktuur ka mooduli õpitulemusi ning soovituslikku mahtu ja õppemeetodeid. On asjakohane selgitada, et kuigi õppekava sisaldab mitu tundi mooduli kohta, tuleb neid tunde pidada kontakttundideks. Õppekava on kokku 30 tundi, mis vastab 1 EAP-le. Tehakse ettepanek, et eneseõppimisel ja hindamisel tuleks arvestada sama arvu tunde mooduli kohta.

[1] Kirkpatrick, D. L. (1994). Evaluating training programs: the four levels. San Francisco: Berrett-Koehler.

Õppekava moodul	*Mooduli eesmärk*
1.0 Sissejuhatus küberturvalisusesse	Esimese mooduli eesmärk on tutvustada küberturvalisuse kursust ja selle teemasid nii koolitajatele kui ka kõrgkoolide üliõpilastele. Moodul algab küberkuritegevuse lühikese ajaloo ja selle kiire kasvu põhjuste tutvustamisega, samuti ajalooliste etappide ja praeguse olukorraga. Täiendavalt tuuakse välja küberturvalisuse väljakutsed, mida üksikisikud ja ettevõtted kogevad tööstuse 4.0 tulekuga, näiteks globaalsete piiride vähenemine, mobiilsete tehnoloogiate laialdane kasutamine, pilvandmetöötlus, asjade Internet (IoT) ja suurandmed. Muud väljakutsed hõlmavad kolmandate isikute riske ja kasvavaid ohte, sealhulgas rahvusriikide ohte. Koolitajad leiavad vajaliku materjali, et tutvustada õppuritele küberturvalisuse kontseptsiooni koos tavapäraste väljakutsetega, millega ettevõtted silmitsi seisavad, võimaluse korral reaalsete stsenaariumidega. Moodul süveneb ka arvukatesse küberturvalisuse valdkonnas kasutatavatesse definitsioonidesse ja žargooni.
2.0 Ülevaade küberturvalisusest ELis	Teises moodulis tutvustatakse õppijale olemasolevat ELi poliitikat ja algatusi, mille eesmärk on edendada küberturvalisuse kontseptsiooni. Samuti käsitletakse küberjulgeoleku õiguslikke aspekte nii ELis kui ka kogu maailmas, tutvustades õppuritele arvukaid reaalse elu stsenaariume ja juhtumiuuringuid turvalisuse valdkonnas. Moodul sisaldab ülevaadet küberturvalisuse valdkonna suundumustest, sealhulgas, kuid mitte ainult, statistikat, suundumusi, asjakohaseid ohte, õiguslikke, maine- ja finantsriske ning juhtumianalüüsi.
3.0 Küberrünnakud – sotsiaalsed ründed ja andmepüük	Kolmas moodul tutvustab õppijat küberrünnakutele, keskendudes eriti andmepüügile. Samuti süvenetakse üksikasjalikult sotsiaalsetele rünnetele ja pööratud sotsiaalse rünnaku mõistesse koos küberrünnakute näidetega. Moodul tutvustab ka erinevaid andmepüügirünnakute tüüpe ja tehnikaid koos reaalsete juhtumianalüüsi näidetega projekti partnerriikidest.
4.0 Küberrünnakute mõistmine ja nendega toimetulek	Neljandas moodulis tutvustatakse õppijale e-ohutuse mõistet ja küberhügieeni mõiste kaudu proaktiivse lähenemise olulisust küberohtudele. Moodul pakub ka üksikasjalikku lähenemist küberrünnakute äratundmisele ja käsitlemisele. Moodul tutvustab juhtumitele reageerimise plaanide väljatöötamist ja rakendamist, et minimeerida küberrünnakute mõjusid.

3.2 E-õppe mooduli struktuur üksikasjalikult

3.2.1 Sissejuhatus küberturvalisusse

Mooduli nimetus	1.0 Sissejuhatus küberturvalisusse
Mooduli maht *(Tunde / Slaide)*	3 tundi 46 – 60 Slaidi

Tarneviisid	Kontaktõpe E-õpe Hübriidõpe
Hindamine	Kohapeal aktiivne osalus / Veebitest
Õpiväljundid	• On teadlik küberturvalisuse üldisest taustast. • Mõistab küberturvalisuse väljakutseid • Mõistab küberturvalise valdkonna arengut ja suurenenud tähtsust viimastel aastatel. • Mõistab küberturvalisuse valdkonna volaatilisust ja vajadust olla pidevalt sammuke eespool ründajatest. • Tunneb ja oskab seletada küberturvalisuega seotudpeamisi mõisteid ja sõnu.
Eeldused	Eelnevad teadmised pole olulised
Mooduli kirjeldus	Esimese mooduli eesmärk on tutvustada küberturvalisuse kursust ja selle teemasid nii koolitajatele kui ka kõrgkoolide üliõpilastele. Moodul algab küberkuritegevuse lühikese ajaloo ja selle kiire kasvu põhjuste tutvustamisega, samuti ajalooliste etappide ja praeguse olukorraga. Täiendavalt tuuakse välja küberturvalisuse väljakutsed, mida üksikisikud ja ettevõtted kogevad tööstuse 4.0 tulekuga, näiteks globaalsete piiride vähenemine, mobiilsete tehnoloogiate laialdane kasutamine, pilvandmetöötlus, asjade Internet (IoT) ja suurandmed. Muud väljakutsed hõlmavad kolmandate isikute riske ja kasvavaid ohte, sealhulgas rahvusriikide ohte. Koolitajad leiavad vajaliku materjali, et tutvustada õppuritele küberturvalisuse kontseptsiooni koos tavapäraste väljakutsetega, millega ettevõtted silmitsi seisavad, võimaluse korral reaalsete stsenaariumidega. Moodul süveneb ka arvukatesse küberturvalisuse valdkonnas kasutatavatesse definitsioonidesse ja žargooni.
MOODULI ALAMTEEMAD	
1.1 Taust - neljanda tööstusrevolutsiooni väljakutsed	• Sissejuhatus küberturvalisusesse • Küberkuritegevuse arengu lühiajalugu ja selle kiire kasvu põhjused, samuti ajaloolised etapid ja hetkeseis • Probleemi taust, milles kirjeldatakse väljakutseid, mida ettevõtted küberrünnakutega seoses näevad • Ettevõtte väljakutsed tööstus 4.0 ajastul: - Piirideta; - Tehnoloogiad: tehnoloogiate laialdane kasutamine (mobiiltehnoloogiad); - Pilveandmetöötlus; - Suurandmed töötlemine;

	- Kolmandate osapooltest tulenev risk; - Asjade internet (IoT); • Kuidas saada hakkama pidevalt suureneva ohuga?; • Riiklikud ohud		
	Kestus tundides 1.5	*Minimaalselt slaidide* 23	*Maksimaalselt slaide* 30
1.2 Küberturvalisuse ajalugu	• Lühike ajalugu selle kohta, kuidas küberrünnakute lähenemisviisid on aja jooksul muutunud, mis on suurendanud ohtusid ja seega ka küberrünnakute vastaseid vastumeetmeid. • See osa võib hõlmata kohalikke / Euroopa / rahvusvahelisi juhtumianalüüse		
	Kestus tundides 1.0	*Minimaalselt slaidide* 15	*Maksimaalselt slaide* 20
1.3 Küberturvalisuse mõisted	• Jaotis küberturvalisuse žargooni / terminite ja statistika / allikate kohta		
	Kestus tundides 0.5	*Minimaalselt slaidide* 8	*Maksimaalselt slaide* 10

3.2.2 Ülevaade küberturvalisusest Euroopa Liidus (EL)

Mooduli nimetus	2.0 Ülevaade küberturvalisusest ELis
Mooduli maht *(Tunde / Slaide)*	3 tundi 48 – 67 slaidi
Tarneviisid	Kontaktõpe E-õpe Hübriidõpe Arutelud
Hindamine	Kohapeal aktiivne osalus / Veebitest
Õpiväljundid	• Küberjulgeoleku õiguslike aspektide mõistmine • ELi küberturvalisusega seotud praeguste poliitikate mõistmine • Küberjulgeolekuga seotud ELi seaduste mõistmine • Küberjulgeoleku kohalike seaduste seostamine ja võrdlemine ELi seadustega
Eeldused	Alus IT- ja äriteadmised võivad mooduli paremaks mõistmiseks olla kasulikud

<table>
<tr><td>Mooduli kirjeldus</td><td colspan="3">Teises moodulis tutvustatakse õppijale olemasolevat ELi poliitikat ja algatusi, mille eesmärk on edendada küberturvalisuse kontseptsiooni. Samuti käsitletakse küberjulgeoleku õiguslikke aspekte nii ELis kui ka kogu maailmas, tutvustades õppuritele arvukaid reaalse elu stsenaariume ja juhtumiuuringuid turvalisuse valdkonnas.

Moodul sisaldab ülevaadet küberturvalisuse valdkonna suundumustest, sealhulgas, kuid mitte ainult, statistikat, suundumusi, asjakohaseid ohte, õiguslikke, maine- ja finantsriske ning juhtumianalüüsi.</td></tr>
<tr><td colspan="4">MOODULI ALAMTEEMAD</td></tr>
<tr><td rowspan="2">2.1 Küberturvalisuse edendamine Euroopa Liidus</td><td colspan="3">• Lühitutvustus ELi poliitikate ja algatuste kohta, mille eesmärk on edendada küberturvalisuse kontseptsiooni</td></tr>
<tr><td>Kestus tundides
1.0</td><td>Minimaalselt slaidide
20</td><td>Maksimaalselt slaide
30</td></tr>
<tr><td rowspan="2">2.2 Küberjulgeoleku õiguslikud aspektid</td><td colspan="3">• Küberjulgeoleku õiguslikud aspektid kogu maailmas (üldiselt) ja eriti ELis, sealhulgas eeskirjade eiramise tagajärjed.
• Küberjulgeoleku kohalike seaduste seos, võrdlus ja vastandamine ELi seadustele.</td></tr>
<tr><td>Kestus tundides
0.5</td><td>Minimaalselt slaidide
5</td><td>Maksimaalselt slaide
7</td></tr>
<tr><td rowspan="2">2.3 Ülevaade küberturvalisuse maastiku suundumustest</td><td colspan="3">• Tegelike elustsenaariumide ja juhtumianalüüside esitamine, sealhulgas statistika, suundumused, asjakohased ohud, riskid (juriidiline, maine, finants).
• Vaade hiljutistele küberrünnakutele ja aktiivne arutelu personaalse enesetäiendamise olulisuse osas, pidades silmas küberrünnakutest tulenevaid võimalikke riske..
Märkus. Arutelu võiks toimuda näost näkku, koolitaja hõlbustades ja andes juhiseid arutelust oodatava kohta.</td></tr>
<tr><td>Kestus tundides
1.5</td><td>Minimaalselt slaidide
23</td><td>Maksimaalselt slaide
30</td></tr>
</table>

3.2.3 Küberrünnakud – sotsiaalsed ründed ja andmepüük

Mooduli nimetus	3.0 Küberrünnakud – sotsiaalsed ründed ja andmepüük
Mooduli maht *(Tunde / Slaide)*	10 tundi 150 – 200 slaidi
Tarneviisid	Kontaktõpe E-õpe Hübriidõpe Interaktiivsete tööriistade kasutamine

<table>
<tr><td></td><td colspan="3">Arutelud</td></tr>
<tr><td>Hindamine</td><td colspan="3">Kohapeal aktiivne osalus / Veebitest</td></tr>
<tr><td>Õpiväljundid</td><td colspan="3">• Mõistab küberrünnakute olemust
• Tunneb ära sotsiaalsed ja pööratud sotsiaalsed ründed
• Mõistab sotsiaalsest ründest tulenevaid ohtusid
• Teab levinuid küberrunnakute viise</td></tr>
<tr><td>Eeldused</td><td colspan="3">Alus IT- ja äriteadmised võivad mooduli paremaks mõistmiseks olla kasulikud</td></tr>
<tr><td>Mooduli kirjeldus</td><td colspan="3">Kolmas moodul tutvustab õppijat küberrünnakutele, keskendudes eriti andmepüügile. Samuti süvenetakse üksikasjalikult sotsiaalsetele rünnetele ja pööratud sotsiaalse rünnaku mõistesse koos küberrünnakute näidetega.

Moodul tutvustab ka erinevaid andmepüügirünnakute tüüpe ja tehnikaid koos reaalsete juhtumianalüüsi näidetega projekti partnerriikidest.</td></tr>
<tr><td colspan="4">MOODULI ALAMTEEMAD</td></tr>
<tr><td rowspan="2">3.1 Sissejuhatus küberrünna-kutesse</td><td colspan="3">• Lühitutvustus küberrünnakutest, eriti andmepüügirünnakutest</td></tr>
<tr><td>Kestus tundides
0.5</td><td>Minimaalselt slaidide
8</td><td>Maksimaalselt slaide
10</td></tr>
<tr><td rowspan="2">3.2 Sotsiaaltehnika moodulid ja manipuleerimine</td><td colspan="3">• Ülevaade sotsiaaltehnika mudelitest, pöörates erilist tähelepanu järgnevale:
a) "Mõjurelvad - R. Cialdini[2]
- Vastastikune suhtlemine
- Pühendumus ja järjepidevus
- Sotsiaalne tõestus
- Meeldivus
- Autoriteet
- Piiratud saadavus
b) Sotsiaaltehnoloogia psühholoogilised aspektid
c) Ülevaade sotsiaalsest pöördtehnoloogiast</td></tr>
<tr><td>Kestus tundides
4</td><td>Minimaalselt slaidide
60</td><td>Maksimaalselt slaide
80</td></tr>
<tr><td>3.3 Erinevad andmepüügi-rünnakute tüübid ja tehnikad</td><td colspan="3">• Jaotis küberrünnakute (eriti andmepüügi) eri tüüpide määratlemiseks ja nende tuvastamiseks (järgmine peatükk). Näiteks:
Kategooriad
- GDPR seotud rünnakud
- E-kirjad;
- Sõnumirakendused;</td></tr>
</table>

[2] Cialdini, R. B. (2016). Pre-Suasion: A Revolutionary Way to Influence and Persuade. New York: Simon & Schuster. ISBN 978-1501109799.

<table>
<tr><td></td><td colspan="3">- Sotsiaalvõrgustik;
- Veebilehed;
- Loterii pettused;
- SMS;
- Telefoni kõned;
- Näost näkku suhtlus;
- Üle-õla ründed;
Eri tehnikate kombinatsioon
- Spray and Pray
- Spear Phishing
- Whaling
- Vishing
- Smishing
- Angler Phishing
- Clone Phishing
- Malvertising</td></tr>
<tr><td></td><td>Kestus tundides
4</td><td>Minimaalselt slaidide
60</td><td>Maksimaalselt slaide
80</td></tr>
<tr><td>3.4 Juhtumiuuringud</td><td colspan="3">• Partnerorganisatsioonide erinevate juhtumiuuringute tutvustamine
• Veebipõhine või näost näkku vestlus väikestes rühmades (5-6 õpilast) Märkus. Arutelu toimub harjutusena, kus iga rühm leiab ja analüüsib hiljutist andmepüügirünnakut, hõlmates selliseid üksikasju nagu rünnaku kuupäev, teave ohvri kohta, rünnaku viisid, tagajärjed, saadud õppetunnid ja nii edasi. Seejärel esitab õpilane igast rühmast analüüsi tulemused kogu klassile. Samuti tuleb anda konstruktiivset tagasisidet koolitajalt ja kaaslastelt.</td></tr>
<tr><td></td><td>Kestus tundides
1.5</td><td>Minimaalselt slaidide
22</td><td>Maksimaalselt slaide
30</td></tr>
</table>

3.2.4 Küberrünnakute mõistmine ja nendega toimetulek

Mooduli nimetus	4.0 Küberrünnakute mõistmine ja nendega toimetulek
Mooduli maht *(Tunde / Slaide)*	14 tundi 210 – 255 slaidi
Tarneviisid	Kontaktõpe E-õpe Hübriidõpe
Hindamine	Kohapeal aktiivne osalus / Veebitest
Õpiväljundid	• Omandab põhiteadmisi e-ohutuse ja turvalisuse valdkonnas • Mõistab erinevat infosisu

<table>
<tr><td></td><td colspan="3">

Mõistab identiteeti ja eristab identiteediga seotud rünnakuid
Mõistab küberrünnakute tagajärgi nii eraisikutele kui ka organisatsioonidele
Mõistab küberhügieeni kui küberrünnakuid ennetava tegevuse tähtsust
Mõistab ja oskab rakendada erinevaid kaitsemeetodeid küberrünnakute vastu kaitsemiseks
Teab kuidas käituda küberrünnaku ohviks langemise korral

</td></tr>
<tr><td>Eeldused</td><td colspan="3">Eelmiste moodulite läbimine</td></tr>
<tr><td>Mooduli kirjeldus</td><td colspan="3">Neljandas moodulis tutvustatakse õppijale e-ohutuse mõistet ja küberhügieeni mõiste kaudu proaktiivse lähenemise olulisust küberohtudele.

Moodul pakub ka üksikasjalikku lähenemist küberrünnakute äratundmisele ja käsitlemisele. Moodul tutvustab juhtumitele reageerimise plaanide väljatöötamist ja rakendamist, et minimeerida küberrünnakute mõjusid.</td></tr>
<tr><td colspan="4">MOODULI ALAMTEEMAD</td></tr>
<tr><td>4.1 Põhiteadmised e-turvalisuse kohta</td><td colspan="3">

Infosisu erinevused (avatud, privaatne, äriline jne); Intellektuaalne omand; Autoriõigused;
Tunneb mõistet Identiteet; on teadlik identiteedivargustest ja varguse meetoditest. On teadlik nuhkvarast, klaviatuuri nuhkidest, pettusreklaamist ja troojalastest. Tea erinevaid viise, kuidas pahatahtlik tarkvara seadmesse pääseb.
Teab identiteedi ja isikuandmete varguste põhjusi ja tagajärgi töökohal ja Internetis (petlik teabe kasutamine, teabe kaotamise oht, sabotaaž).
Teab isikuandmete avalikustamisega seotud ohtude kohta.
Lühitutvustus küberrünnakute mõjust nii eraisikule kui ka organisatsioonile. Lisateavet punktis 4.4.

<table>
<tr><td>Kestus tundides
0.5</td><td>Minimaalselt slaidide
8</td><td>Maksimaalselt slaide
10</td></tr>
</table>
</td></tr>
<tr><td>4.2 Ennetavad toimingud</td><td colspan="3">

Küberhügieen Internetis (minimeerige inimeste kohta käivat teavet, sealhulgas isiklikud kontod sotsiaalmeedias, mida ründajad saaksid kasutada)
Küberhügieen töökohal
Tehnoloogilised tööriistad ja meetmed (andmepüügimeilide filtrid ja blokeerimine)

<table>
<tr><td>Kestus tundides
2</td><td>Minimaalselt slaidide
30</td><td>Maksimaalselt slaide
35</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>4.3</td><td>Andmepüügi-rünnakute tuvastamine</td><td colspan="3">• Juhtumianalüüs, kasutades jaotise 3.3 tehnikaid - andmepüügirünnakute erinevad tüübid ja tehnikad
• Jaotis küberrünnakute tuvastamiseks (viidates eelmise peatüki üksustele), näiteks:
- Kriitiline mõtlemine
- Õpitakse linke eelvaatama
- URL-i mõistmine
- Sõnumite analüüsimine
- Ohu märkide äratundmine</td></tr>
<tr><td colspan="2"></td><td>Kestus tundides
5</td><td>Minimaalselt slaidide
75</td><td>Maksimaalselt slaide
90</td></tr>
<tr><td>4.4</td><td>Küberrünnakute käsitlemine</td><td colspan="3">• Küberturvalisuse juhend, sealhulgas jaotis küberrünnakute poolt nii üksikisikule kui ka organisatsioonidele tekitatud kahjude kohta ning eelmise peatüki põhjal küberrünnakutega toimetulek.
• Tegevus peaks hõlmama näiteks:
- Ohutu navigeerimine
- Turvaliste paroolide kasutamine
- Rünnakute vältimine
- Turvaline veebipoodides ostlemine
- Antiviiruse kasutamine
- Sessiooniküpsistega ümberkäimine
- Tagavarakoopiate tegemine
- Andmete krüpteerimine
- Mitme tasemeline autentimine
- Pahavara
- Privaat režiimis veebisirvimine
• See jaotis sisaldab ka kohalikke / Euroopa / rahvusvahelisi juhtumianalüüse, mida on näidatud eelmistes moodulites
• See jaotis sisaldab vajaduse korral lihtsaid juhiseid samm-sammult
• See jaotis sisaldab ka küberrünnaku reaktiivset tegevust, sealhulgas taasteprotseduure, kui organisatsioon ja / või kasutaja langevad küberrünnaku ohvriks.</td></tr>
<tr><td colspan="2"></td><td>Kestus tundides
5</td><td>Minimaalselt slaidide
75</td><td>Maksimaalselt slaide
90</td></tr>
<tr><td>4.5</td><td>Kahjustuste minimeerimine intsidentidele reageerimise kaudu</td><td colspan="3">• Intsidentidele reageerimise plaanide analüüs, väljatöötamine ja rakendamine, milles on näidatud soovitatud ja parimate tavade meetodid, mida tuleb kasutada andmerikkumise juhtumi korral.
Märkus: osa jaotisest võiks kohandada vastavalt konkreetsele riigile</td></tr>
<tr><td colspan="2"></td><td>Kestus tundides
1.5</td><td>Minimaalselt slaidide
22</td><td>Maksimaalselt slaide
30</td></tr>
</table>