Andmepüügi vastu kaitsemine 4. tööstusrevolutsiooni ajastul (CyberPhish)

CyberPhish lühike 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 lühike õppekava kirjeldab üksikasjalikult õppekava ülesehitust ja selle eesmärk on pakkuda küberjulgeolekus lühikesi, kuid kaugeleulatuvaid mooduleid, pöörates erilist tähelepanu andmepüügile. Seda kasutatakse rakendamiseks kõrgharidusasutuste õppemoodulites ja levitamise eesmärgil, et osalejaid kursusele meelitada. See lühiversioon koosneb kolmest tasemeteemast: põhiteemad, alateemad ja alateemade üksused, mille peamine eesmärk on õpilased, teised kursusel osalejad ja õpetajad. Nad saavad seda õppekava tutvustust kasutada kursuse peamiste eesmärkide mõistmiseks.

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. ÕPPEKAVA (E-ÕPPIMISE) STRUKTUUR

1.1 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.

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.

1.2 E-õppe mooduli struktuur üksikasjalikult

1.2.1 Sissejuhatus küberturvalisuse

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.

<table>
<tr><td></td><td>

- Mõistab küberturvalisuse valdkonna volaatilisust ja vajadust olla pidevalt sammuke eespool ründajatest.
- Tunneb ja oskab seletada küberturvalisuega seotudpeamisi mõisteid ja sõnu.

</td></tr>
<tr><td>Eeldused</td><td>Eelnevad teadmised pole olulised</td></tr>
<tr><td>Mooduli kirjeldus</td><td>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.</td></tr>
<tr><td colspan="2">MOODULI ALAMTEEMAD</td></tr>
<tr><td>1.1 Taust - neljanda tööstusrevolutsiooni väljakutsed</td><td>

- 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

<table>
<tr><td>Kestus tundides</td><td>Minimaalselt slaidide</td><td>Maksimaalselt slaide</td></tr>
<tr><td>1.5</td><td>23</td><td>30</td></tr>
</table>

</td></tr>
</table>

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

1.2.2 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
Mooduli kirjeldus	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.

<table>
<tr><th colspan="4">MOODULI ALAMTEEMAD</th></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>

1.2.3 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 Arutelud
Hindamine	Kohapeal aktiivne osalus / Veebitest
Õpiväljundid	• Mõistab küberrünnakute olemust • Tunneb ära sotsiaalsed ja pööratud sotsiaalsed ründed • Mõistab sotsiaalsest ründest tulenevaid ohtusid

<table>
<tr><td></td><td colspan="3">• 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[1]
- 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;
- Sotsiaalvõrgustik;
- Veebilehed;
- Loterii pettused;
- SMS;
- Telefoni kõned;
- Näost näkku suhtlus;
- Üle-õla ründed;</td></tr>
</table>

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

	Eri tehnikate kombinatsioon - *Spray and Pray* - *Spear Phishing* - *Whaling* - *Vishing* - *Smishing* - *Angler Phishing* - *Clone Phishing* - *Malvertising*		
	Kestus tundides 4	*Minimaalselt slaidide* 60	*Maksimaalselt slaide* 80
3.4 Juhtumiuuringud	• 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.*		
	Kestus tundides 1.5	*Minimaalselt slaidide* 22	*Maksimaalselt slaide* 30

1.2.4 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 • 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

<table>
<tr><td></td><td colspan="3">• 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 rowspan="2">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.</td></tr>
<tr><td>Kestus tundides
0.5</td><td>Minimaalselt slaidide
8</td><td>Maksimaalselt slaide
10</td></tr>
<tr><td rowspan="2">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)</td></tr>
<tr><td>Kestus tundides
2</td><td>Minimaalselt slaidide
30</td><td>Maksimaalselt slaide
35</td></tr>
<tr><td rowspan="2">4.3 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>Kestus tundides
5</td><td>Minimaalselt slaidide
75</td><td>Maksimaalselt slaide
90</td></tr>
</table>

<table>
<tr><td>4.4</td><td>Küberrünnakute käsitlemine</td><td>

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.

<table>
<tr><td>Kestus tundides
5</td><td>Minimaalselt slaidide
75</td><td>Maksimaalselt slaide
90</td></tr>
</table>
</td></tr>
<tr><td>4.5</td><td>Kahjustuste minimeerimine intsidentidele reageerimise kaudu</td><td>

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

<table>
<tr><td>Kestus tundides
1.5</td><td>Minimaalselt slaidide
22</td><td>Maksimaalselt slaide
30</td></tr>
</table>
</td></tr>
</table>