

Aizsardzība pret pikšķerēšanu 4. industriālās revolūcijas laikmetā (CyberPhish)



CyberPhish paplašinātā mācību programma

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. Šajā publikācijā [paziņojumā] atspoguļots vienīgi tās autoru viedoklis un Eiropas Komisija neuzņemas atbildību par veidu, kādā tiek izmantota tajā ietvertā informācija.



Saturs

Saturs	2
Ievads	3
1. Treneru apmācības koncepcija	3
2. Klātienēs / tiešsaistes apmācība	6
3. Mācību programmas (e-apmācības moduļa) struktūra	8
3.1 Ievads	8
3.2 Detalizēta e-apmācības moduļa struktūra	9
3.2.1 Ievads kiberdrošībā	9
3.2.2 Kiberdrošība Eiropas Savienībā (ES).....	10
3.2.3 Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana	12
3.2.4 Kiberuzbrukumu izpratne un rīcība kiberuzbrukuma gadījumā.....	14



IEVADS

Cyberphish Paplašinātās mācību programmas mērķis ir sniegt kodolīgus, taču tālejošus moduļus kiberdrošības jomā, īpašu uzmanību pievēršot kiberpikšķerēšanai. Mācību programma ir sadalīta trīs galvenajās sadaļās, proti:

- **Treneru apmācības kurss** - kas ļauj treneriem iegūt pareizu izpratni un prasmes, lai īstenotu mācību programmu.
- **Klātienēs / tiešsaistes apmācība** - nosaka kārtību, kādā tiek nodrošināta mācību programma.
- **Error! Reference source not found.** - sīki apraksta mācību programmas struktūru

Ir svarīgi atzīmēt, ka, lai gan mācību programmas īstenošanai ir paredzēta jauktas mācīšanās pieeja, tās struktūra ļauj īstenot mācību programmu elastīgi.

Mācību programma aplūko kiberdrošības jautājumus, īpaši koncentrējoties uz kiberpikšķerēšanu. Tā ir paredzēta uzņēmējiem un sabiedrībai kopumā un tā ir izstrādāta, lai sagatavotu sabiedrību ceturtajai industriālajai revolūcijai un tās radītajiem potenciālajiem drošības apdraudējumiem.

Apgūstot mācību programmu, izglītojamie apgūst prasmes, kas ļauj atpazīt kiberuzbrukumus un atbilstoši rīkoties, kā arī pasargāt ierīces un datus no pārlases uzbrukumiem.

1. TRENERU APMĀCĪBAS KONCEPCIJA

Tālāk aprakstītā treneru apmācības kursa struktūra ir izstrādāta tā, lai to varētu īstenot klātienē vai tiešsaistē. Paredzamais kursa ilgums var atšķirties atkarībā no dalībnieku skaita un īstenošanas prasībām. Ņemot vērā šī treneru apmācības kursa īpatnības, ieteicams katrā kursa grupā iekļaut ne vairāk kā divpadsmit trenerus.

Apmācības programmas struktūra ir sniegta zemāk esošajā tabulā. Tabulā ir norādītas **ieteicamās tēmas** treneru apmācības nodarbībām un ieteicamais nodarbības ilgums. Apmācības organizācija un treneris var izvēlēties izmantojamo saturu, paplašināt to, saīsināt vai pagarināt treneru apmācības programmu, kā to uzskata par nepieciešamu un ņemot vērā trenera un izglītojamo sagatavotības līmeni.

Ir lietderīgi atzīmēt, ka treneru apmācības kurss ir paredzēts treneriem, kuri jau ir informēti par kiberdrošības tēmu kopumā.

Pasākuma organizatori pirms treniņa var nosūtīt anketu treneriem, lai apkopotu informāciju par treneru sagatavotības līmeni un saprastu, ko treneri sagaida no šīm apmācībām. Izmantojot anketās norādīto informāciju, organizatori var attiecīgi pielāgot mācību programmas plānu.

Struktūra	Treneru apmācības kurss tiek īstenots īsā 4 dienu programmā, kuras mērķis ir nodrošināt trenerus ar atbilstošām prasmēm un kompetencēm	
Mērķis	Nodrošināt treneriem pamatkompetences un apmācību izstrādes prasmes, lai efektīvi īsteno kiberdrošības apmācību sesijas	
Programma		
1. diena	Diena studenta dzīvē	
Temata Nr.	Temats	Ieteicamais ilgums
D1-01	Ievads un iepazīšanās sesija <ul style="list-style-type: none"> • Iepazīšanās vai komandas veidošanas aktivitāte - Zemo tehnoloģiju sociālais tīkls (iepazīšanās) 	30 minūtes



	- Zefīru izaicinājums (komandas veidošana)	
D1-02	<p>Dažādu mācību stilu izpratne un risināšana</p> <ul style="list-style-type: none"> • Īss ievads par dažādiem mācīšanās stilu modeļiem <p>- Iepazīšanās ar dažādiem mācīšanās stiliem (piemēram, 7 mācīšanās stili, Kolba mācīšanās cikls) kā turpmāko sadaļu pamatu.</p>	30 minūtes
D1-03	<p>Treneris kā students - mācību metožu pieredze (1. daļa)</p> <p>Šīs sesijas mērķis ir iesaistīt pasniedzējus dažādu pedagoģisko apstākļu un mācību metožu izpratnē un pieredzē izglītojamo lomā. Mācības klātienē vai virtuāli (tiešsaistes klasē) ar treneriem izglītojamo lomā.</p> <ul style="list-style-type: none"> • Iepazīšanās ar dažādiem pedagoģiskajiem apstākļiem un mācīšanas metodēm <p>- Sesijas pirmajā daļā galvenais treneris iepazīstina ar vairākiem pedagoģiskajiem apstākļiem un pasniegšanas metodēm (piem., semināri, praktiskas sesijas, diskusijas, depates, gadījumu izpēte u.t.t.)</p> <ul style="list-style-type: none"> • Dažādu mācīšanas metožu pieredze <p>- Nodarbības otrajā daļā treneri / izglītojamie praktiski piedzīvo šīs dažādās mācīšanas metodes.</p>	3 stundas
D1-04	Tīklošanās pauze	30 minūtes
D1-05	<p>Treneris kā students - mācību metožu pieredze (2. daļa)</p> <ul style="list-style-type: none"> • Diskusija, atsauksmes un dalīšanās ar labāko praksi <p>- Dalīšanās ar jūtām, attieksmi, atgriezenisko saiti par 1. daļas pieredzi</p> <p>- Dalīšanās labākajā praksē, kā uzlabot studentu mācīšanās pieredzi</p>	1 stunda
D1-06	1. diena - Secinājumi un kopsavilkums	30 minūtes
2. diena	Pamata sociālo prasmju atsvaidzināšana	
Temata Nr.	Temats	Ieteicamais ilgums
D2-01	<p>2. dienas ievads - sociālo prasmju nozīme</p> <ul style="list-style-type: none"> • Īss ievads par sociālo prasmju nozīmi nodarbības pasniegšanā <p>- Īss ievads, kas galvenokārt vērsts uz prezentāciju, veicināšanu, klases pārvaldību un konstruktīvu atsauksmju sniegšanu</p>	30 minūtes
D2-02	<p>Pamata sociālās prasmes apmācību organizēšanai (1. daļa)</p> <ul style="list-style-type: none"> • Prezentācijas prasmes <p>- Prezentācijas strukturēšana (piemēram, slaidu skaits un formāts, tiešsaistes rīku izmantošana)</p> <p>- Uzstāšanās aspekti (piemēram, ķermeņa valoda, balsis tonalitāte, ķermeņa valoda)</p> <p>- Īsu prezentāciju sniegšana (klātienē vai tiešsaistē) ar kolēģu atsauksmēm un diskusiju</p> <ul style="list-style-type: none"> • Veicināšanas prasmes <p>- Grupas diskusijas veicināšana (piemēram, uzvedinoši jautājumi, novirzīšana un pārformulēšana)</p> <p>- Sadarbības veicināšana (piemēram, ideju vētra, domu kartēšana, sešas domāšanas cepures),</p> <ul style="list-style-type: none"> • Digitālo rīku izmantošana sociālo prasmju veicināšanai 	2 stundas





	<ul style="list-style-type: none"> - <i>Digitālo rīku izmantošana, lai atvieglotu prezentācijas un diskusijas</i> - <i>Iepazīšanās ar digitālajiem / tiešsaistes rīkiem, tostarp MS Teams, Zoom, Skype, Google Meet, Mentimeter, Kazoom un tā tālāk.</i> 	
D2-03	Tīklošanās pauze	30 minūtes
D2-04	<p>Pamata sociālās prasmes apmācību organizēšanai (2. daļa)</p> <ul style="list-style-type: none"> • Klases pārvaldība <ul style="list-style-type: none"> - <i>Dalīšanās ar labāko praksi - kā kontrolēt, aizraut un iesaistīt izglītojamos gan klātienē, gan tiešsaistē</i> • Efektīvu un konstruktīvu atsauksmju sniegšana <ul style="list-style-type: none"> - <i>Īsas debates grupā (klātienē vai tiešsaistes seminārs), analizējot efektīvas un konstruktīvas atgriezeniskās saites sniegšanas tehnikas</i> 	2 stundas
D2-05	2. diena - Secinājumi un kopsavilkums	30 minūtes
3. diena	Sīkāk par mācību programmu	
<i>Temata Nr.</i>	<i>Temats</i>	<i>Ieteicamais ilgums</i>
D3-01	<p>Ievads mācību satura struktūrā un mācību modalitātēs</p> <p><i>Īsa klātienē vai tiešsaistes sesija, kuras laikā trenerus iepazīstina ar mācību satura struktūru, tostarp mācību rezultātu nozīmi kopā ar mācīšanas modalitātēm.</i></p>	1 stunda
D3-02	<p>Mācību programmu tēmu detalizēta analīze (1. daļa)</p> <p><i>Skaidrojoša sesija par pirmajiem diviem mācību programmas moduļiem</i></p>	1 stunda
D3-03	Tīklošanās pauze	30 minūtes
D3-04	<p>Mācību programmu tēmu detalizēta analīze (2. daļa)</p> <p><i>Skaidrojoša sesija par pēdējiem diviem mācību programmas moduļiem</i></p>	3 stundas
D3-05	3. diena - Secinājumi un kopsavilkums	30 minūtes
4. diena	Noslēguma seminārs - Būtisko sociālo prasmju novērtējums, izmantojot mācību programmu	
<i>Temata Nr.</i>	<i>Temats</i>	<i>Ieteicamais ilgums</i>
D4-01	<p>Semināra ievads</p> <p><i>Pēdējā dienā paredzēts seminārs, kura ietvaros visiem dalībniekiem jāpārdomā 1. dienā iegūtā pieredze, jāpraktizē 2. dienā apgūtās iemaņas un jāizmanto 3. dienā izskaidrotais programmas saturs.</i></p> <p><i>Novērtējumu veido citu dalībnieku - treneru sniegtā atgriezeniskā saite.</i></p> <p><i>Semināra ilgums ir atkarīgs no dalībnieku skaita.</i></p>	30 minūtes
D4-02	<p>Prezentācijas prasmju novērtēšana</p> <p><i>Treneriem tiek lūgts sagatavot un uzstāties 10 minūšu garā prezentācijā, izvēloties jebkuru tēmu no piedāvātās mācību programmas. Katrai prezentācijai seko kolēģu novērtējums un atsauksmes par prezentāciju, tostarp izmantotajām novatoriskajām tehnikām.</i></p> <p><i>Pēc trenera ieskatiem var izmantot citas novērtēšanas metodes</i></p>	15 minūtes katram dalībniekam (maks. 3 stundas)
D4-03	Tīklošanās pauze	30 minūtes
D4-04	Veicināšanas prasmju novērtēšana	15 minūtes katram



	<i>Treneriem tiek lūgts novadīt 10 minūšu garu sesiju, izvēloties jebkuru tēmu no piedāvātā mācību satura. Katrai sesijai seko kolēģu novērtējums un atgriezeniskā saite par veicināšanas prasmēm un klases vadību.</i> Pēc trenera ieskatiem var izmantot citas novērtēšanas metodes	dalībniekam (maks. 3 stundas)
D4-05	4. diena - Kopsavilkums un secinājumi par treneru apmācības kursu	30 minūtes

2. KLĀTIENES / TIEŠSAISTES APMĀCĪBA

Lai integrētu izglītojamās mācību pieredzē, tiek izmantota **četrpakāpju pieeja**. Īsumā:

TIEŠSAISTES ORIENTĒŠANĀS SESIJA	STUDENTU SAGAIĀŠANAS PASĀKUMS	MODUĻU PASNIEGŠANA	INTEGRĀCIJAS SEMINĀRS	MODUĻU PASNIEGŠANA	KURSA PABEIGŠANA	NOSLĒGUMA TĪKĻŠANĀS SESIJA
Informācija par mācību iestādi - Mērķi - Politikas - Procedūras -	Ievads - informācija par treneri Mācību iestāžu vadības informācijas sistēma (MIS) - Informācija par sistēmu - ID/ parole - Resursi - Lietošanas politika - BUJ/ Traucējumu novēršana Oficiālā kursa programma Novērtēšanas metodika Saziņas veidi	Moduļa pasniegšana atkarībā no dienā piešķirto stundu skaita. Pirmā daļa (15 stundas)	Tiešsaistes atsauksmju veidlapa par pašreizējo labo praksi un citu praksi, kam jāpievērš uzmanība Diskusija ar izglītojamajiem	Moduļa pasniegšana atkarībā no dienā piešķirto stundu skaita. Otrā daļa (15 stundas)	Datu apkopošana - No trenera: novērtējumi - No studentiem: digitālās apmācības novērtēšanas veidlapa	Fokusa sesija - Diskusija par rezultātiem - Secinājumi - Turpmākā darbība
 NEPĀRTRAUKTS PASNIEDZĒJU ATBALSTS						
 NEPĀRTRAUKTS SISTĒMAS ATBALSTS						

i. Pašu vadīta virtuālās orientēšanās sesija

Pirmais orientēšanās pieredzes solis ir apmeklēt **tiešsaistes orientēšanās sesiju**. Šī sesija ir pašmācības pieredze, kas ļauj izglītojamajam savā tempā iegūt informāciju par organizāciju, kas nodrošina apmācību (mācību iestādi).

Topošajiem izglītojamajiem, cita starpā, būs iespēja iepazīties ar informāciju, kas ir saistīta ar mācību iestādi kā tādu un konkrēto attiecīgo departamentu. Tiek izcelti departamenta mērķi, politika un procedūras, kā arī mācību iestādes gaidas. Lai nodrošinātu pieejamību izglītojamajiem ar redzes un dzirdes traucējumiem, visiem orientācijas materiāliem un prezentācijām jābūt ar subtitriem un pieejamiem ekrāna lasītājiem.

ii. Sagaidīšanas pasākums

Jaunā studentu grupa tiek laipni gaidīta **studentu sagaidīšanas pasākumā**. Šo notikumu var organizēt klātienē vai tiešsaistē. Šī tikšanās studentiem sniedz lielisku iespēju satikt treneri un kursabiedrus, uzdot jautājumus un iepazīties ar kursa loģistiku.

Trenerim tiks piešķirta atļauja izmantot mācību iestādes informācijas sistēmu un viņš sniegs īsu ievadu par instalēto sistēmu. Izglītojamajiem tiks izsniegti lietotāja ID un viņi saņems palīdzību paroli iestatīšanai. Tāpat tiks sniegtas norādes



par piekļuvi resursiem, ko izglītojamiem ir atļauts izmantot. Izglītojamie izlasa un paraksta "Lietošanas politiku". Tā kā tas nozīmē lielu tehniskās informācijas apjomu, turpmākai izmantošanai būs pieejams "BUJ un traucējumu novēršanas" dokuments.

Treneris var noslēgt sesiju, sniedzot precīzu priekšstatu par oficiālo kursa programmu, vērtēšanas metodiku un pieejamiem saziņas veidiem.

iii. Pastāvīgs atbalsts izglītojamajiem

Mācību iestāde ne tikai nodrošina ar kiberdrošības apmācību kursu saistītu zināšanu, prasmju un uzvedību apgūšanu, bet arī atzīst to, cik svarīgi ir identificēt mainīgās izglītojamo vajadzības un reaģēt uz tām. Pirmkārt, studentiem regulāri būs pieejami treneri pozitīvai mijiedarbībai ar izglītojamiem.

Oficiālā līmenī - pēc noteikta skaita mācību sesiju pabeigšanas tiks organizēts **Integrācijas seminārs**. Tiks apkopotas un apspriestas izglītojamo atsauksmes, lai noteiktu, cik lielā mērā kursa virzība atbilst studentu cerībām un mācību iestādes standartiem.

Pirms integrācijas semināra var izmantot dažādus apmācības novērtēšanas rīkus, kas palīdzētu apkopot datus. Šajā ziņā panākumu rādītāji, cita starpā, ir tas, ka izglītojamais apgūst jaunas prasmes un zināšanas, izjūt pozitīvu attieksmi pret mācīšanās pieredzi un apmācības ietekmē izglītojamā efektivitāti.

Savukārt šī informācija tiek izmantota, lai nodrošinātu kursa programmas kvalitātes uzlabošanu.

iv. Kursa secinājumi

Kursa pabeigšana pati par sevi ir nozīmīgu sasniegumu atzīšanas brīdis.

Tiek organizēta **Noslēguma tīklošanās sesija** ar diviem mērķiem. Ļoti svarīgi ir tas, ka izglītojamajiem tiek dota iespēja pāris stundas dalīties kopīgā priekā. Taču arī mācību iestāde vienlaikus gūst iespēju novērtēt apmācības programmas panākumus. Šim nolūkam tiks izmantots *Kirkpatricka četru līmeņu apmācības novērtēšanas modelis*¹.

Pirms tīklošanās sesijas mācību iestāde apkopo informāciju:

- *no trenera - par novērtējumiem*
Tas kalpos kā mērs tam, cik lielā mērā ir mainījušās izglītojamo zināšanas un prasmes kopš studiju programmas uzsākšanas.
- *no izglītojamajiem.*
Digitāla apmācību novērtēšanas forma, aicinot sniegt komentārus par vispārējo apmierinātību ar mācīšanās pieredzi un mācību rezultātu piemērojamību (vai nē) darba vietā.

Ņemot vērā šos datus, tīklošanās pasākuma laikā notiks **fokusa sesija**, kuras ietvaros mācību iestāde, izmantojot strukturētu paneļdiskusiju, var kvalitatīvi novērtēt tādu rezultātus kā produktivitāte, kvalitāte un efektivitātes vērtējums.

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



3. MĀCĪBU PROGRAMMAS (E-APMĀCĪBAS MODUĻA) STRUKTŪRA

3.1 Ievads

Mācību programma ir paredzēta gan uzņēmumiem, gan indivīdiem, kuri saskarsies ar neizbēgamo pozitīvo un negatīvo ietekmi, ko rada 4. industriālā revolūcija, un kuri vēlas iemācīties un būt vairāk gatavi šīs revolūcijas radīto drošības izaicinājumu pārvarēšanai.

Mācību programmu veido četras atšķirīgas daļas un tā sākas ar ievadu kiberdrošībā un saistītajiem izaicinājumiem, ko rada 4. industriālās revolūcijas iestāšanās. Programmas ietvaros tiek sīkāk aplūkota kiberdrošība un tās juridiskie aspekti Eiropas līmenī, kā arī tas, kā kiberdrošība tiek veicināta Eiropas Savienībā.

Ņemot vērā sociālās inženierijas nozīmi un ietekmi, kā arī tās saistību ar kiberuzbrukumiem, mācību programmā ir izklāstīta kiberuzbrukumu atpazīšana un atbilstoša rīcība, lai izvairītos no postošām un neatgriezeniskām sekām.

Papildus īsam dažādu moduļu aprakstam, mācību programmas struktūra ietver katra moduļa mācību mērķus un ieteicamo ilgumu un mācīšanas modalitātes. Ir svarīgi atzīmēt, ka lai gan mācību programmā norādīts noteikts stundu skaits katrā modulī, šīs stundas jāuzskata par kontaktstundām. Pilna mācību programma kopā prasa 30 stundas, kas atbilst 1 ECTS. Tiek rekomendēts paredzēt tādu pašu stundu skaitu katrā modulī pašmācībai un novērtēšanai.

Mācību programmas modulis	Moduļa mērķis
1.0 Ievads kiberdrošībā	<p>Šī moduļa mērķis ir iepazīstināt gan trenerus, gan studentus ar kiberdrošības kursu un tā tēmām. Tas sākas ar īsu kibernetikas attīstības vēsturi un tās straujās izaugsmes iemesliem, kā arī vēsturiskajiem posmiem un pašreizējo situāciju.</p> <p>Tajā izklāstīti arī kiberuzbrukuma radītie izaicinājumi, ar ko saskaras indivīdi un uzņēmumi līdz ar 4. industriālās revolūcijas atnākšanu, tostarp, bet ne tikai globālo robežu mazināšanos, izplatītu mobilo tehnoloģiju lietošanu, mākoņdatošanu, lietu internetu un lielajiem datiem. Citi izaicinājumi ir saistīti ar trešo pušu riskiem un pieaugošajiem draudiem, tostarp valstu drošības apdraudējumiem.</p> <p>Treneri varēs atrast nepieciešamo materiālu, lai iepazīstinātu izglītojamos ar kiberdrošības koncepciju, kā arī izaicinājumiem, ar kuriem parasti saskaras uzņēmumi, kur tas iespējams, aplūkojot reālus scenārijus.</p> <p>Modulī sīkāk aplūkotas vairākas definīcijas un žargons, kas tiek izmantots kiberdrošības nozarē.</p>
2.0 Pārskats par kiberdrošību ES	<p>Šis modulis iepazīstina izglītojamo ar pašreizējām ES politikām un iniciatīvām, kuru mērķis ir veicināt kiberdrošības jēdzienu. Tajā aplūkoti arī kiberdrošības juridiskie aspekti gan ES, gan visā pasaulē, ļaujot izglītojamajiem iepazīties ar daudziem reālās dzīves scenārijiem un gadījumu izpēti šajā jomā.</p> <p>Modulis ietver pārskatu par kiberdrošības tendencēm, tostarp, bet ne tikai statistiku, attīstības tendencēm, būtiskajiem apdraudējumiem, juridiskajiem, reputācijas un finanšu riskiem un gadījumu izpēti analīzi.</p>



<p>3.0 Kiberuzbrukumi - sociālā inženierija un pikšķerēšana</p>	<p>Šis modulis iepazīstina izglītojamo ar kiberuzbrukumiem, īpašu uzmanību pievēršot pikšķerēšanai. Tajā arī detalizēti aplūkoti sociālās inženierijas un reversās sociālās inženierijas jēdzieni, kā arī sociālās inženierijas ciešā saikne ar kiberuzbrukumiem.</p> <p>Moduļa ietvaros tiek aplūkoti arī dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni, kā arī vairāki reāli gadījumu izpētes piemēri no projekta partnervalstīm.</p>
<p>4.0 Kiberuzbrukumu izpratne un rīcība kiberuzbrukuma gadījumā</p>	<p>Šis modulis iepazīstina izglītojamo ar e-drošības jēdzienu un par proaktīvas pieejas kiberdraudiem nozīmi, izmantojot kiberhigiēnas koncepciju.</p> <p>Modulī arī sīkāk aplūkota pieeja kiberuzbrukumu atpazīšanai un novēršanai.</p> <p>Modulis iepazīstina ar incidentu reaģēšanas plānu izstrādi un ieviešanu, lai mazinātu kiberuzbrukumu sekas.</p>

3.2 Detalizēta e-apmācības moduļa struktūra

3.2.1 Ievads kiberdrošībā

Moduļa nosaukums	1.0 Ievads kiberdrošībā
Kopējais ilgums <i>(Stundas / slaidi)</i>	3 stundas 46 - 60 slaidi
Pasniegšanas metodes	Klātienē Tiešsaistē Jaukta pasniegšanas metode
Novērtējums	Klātienē / tiešsaistes tests
Mācību rezultāti	<ul style="list-style-type: none"> • Vispārēja izpratne par kiberdrošību • Izpratne par kiberdrošības izaicinājumiem • Izpratne par to, kā kiberuzbrukumi ir mainījušies laika gaitā, kā rezultātā pastiprinājušies kiberuzbrukumu darbības un tādējādi arī pretpasākumi • Izpratne par to, kādēļ ir svarīgi sekot līdzi kiberdrošības jaunumiem un kādēļ ir nepieciešams pastāvīgi atjaunināt zināšanas par kiberdrošību • Izpratne par dažādām ar kiberdrošību saistītām definīcijām
Prasības	Sākotnējās zināšanas nav nepieciešamas
Moduļa apraksts	<p>Šī moduļa mērķis ir iepazīstināt gan trenerus, gan studentus ar kiberdrošības kursu un tā tēmām. Tas sākas ar īsu kibernetikas attīstības vēsturi un tās straujās izaugsmes iemesliem, kā arī vēsturiskajiem posmiem un pašreizējo situāciju.</p> <p>Tajā izklāstīti arī kiberuzbrukuma radītie izaicinājumi, ar ko saskaras indivīdi un uzņēmumi līdz ar 4. industriālās revolūcijas atnākšanu, tostarp, bet ne tikai globālo robežu mazināšanos, izplatītu mobilo tehnoloģiju lietošanu, mākoņdatošanu, lietu</p>



	<p>internetu un lielajiem datiem. Citi izaicinājumi ir saistīti ar trešo pušu riskiem un pieaugošajiem draudiem, tostarp valstu drošības apdraudējumiem.</p> <p>Treneri varēs atrast nepieciešamo materiālu, lai iepazīstinātu izglītojamos ar kibernetikas koncepciju, kā arī izaicinājumiem, ar kuriem parasti saskaras uzņēmumi, kur tas iespējams, aplūkojot reālus scenārijus.</p> <p>Modulī sīkāk aplūkotas vairākas definīcijas un žargons, kas tiek izmantots kibernetikas nozarē.</p>					
MODUĻA APAKŠTĒMAS						
1.1 Vispārīga informācija - 4. industriālās revolūcijas izaicinājumi	<ul style="list-style-type: none"> • Ievads kibernetikā • Īsa kibernetikas attīstības vēsture un tās straujās izaugsmes iemesli, kā arī vēsturiskie posmi un pašreizējā situācija • Vispārīga informācija par problēmu, iezīmējot kibernetikas radītos izaicinājumus, ar ko saskaras uzņēmumi • Izaicinājumi, ar ko saskaras uzņēmumi: <ul style="list-style-type: none"> - Nav robežu; - Tehnoloģijas: Plaša tehnoloģiju (mobilo tehnoloģiju) izmantošana; - Mākoņdatošana; - Lielo datu izaicinājumi; - Trešo personu riski; - Lietu internets; • Pieaugošo draudu izaicinājums; • Valstu apdraudējumi 					
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;"><i>leteicamais ilgums stundās</i></th> <th style="text-align: center;"><i>Minimālais slaidu skaits</i></th> <th style="text-align: center;"><i>Maksimālais slaidu skaits</i></th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1,5</td> <td style="text-align: center;">23</td> <td style="text-align: center;">30</td> </tr> </tbody> </table>	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	1,5	23
<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>				
1,5	23	30				
1.2 Kibernetikas vēsture	<ul style="list-style-type: none"> • Īss izklāsts par to, kā kibernetikas ir mainījušies laika gaitā, kā rezultātā pastiprinājušies kibernetikas darbības un tādējādi arī pretpasākumi. • Šajā sadaļā var tikt iekļauti vietējie / Eiropas / starptautiskie gadījumu pētījumi 					
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;"><i>leteicamais ilgums stundās</i></th> <th style="text-align: center;"><i>Minimālais slaidu skaits</i></th> <th style="text-align: center;"><i>Maksimālais slaidu skaits</i></th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1,0</td> <td style="text-align: center;">15</td> <td style="text-align: center;">20</td> </tr> </tbody> </table>	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	1,0	15
<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>				
1,0	15	20				
1.3 Kibernetikas definīcijas	<ul style="list-style-type: none"> • Sadaļa par kibernetikas žargonu / terminiem un statistiku / avotiem 					
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;"><i>leteicamais ilgums stundās</i></th> <th style="text-align: center;"><i>Minimālais slaidu skaits</i></th> <th style="text-align: center;"><i>Maksimālais slaidu skaits</i></th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">0,5</td> <td style="text-align: center;">8</td> <td style="text-align: center;">10</td> </tr> </tbody> </table>	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	0,5	8
<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>				
0,5	8	10				

3.2.2 Kibernetika Eiropas Savienībā (ES)

Moduļa nosaukums	2.0 Kibernetika ES
-------------------------	--------------------



Kopējais ilgums (Stundas / slaidi)	3 stundas 48 - 67 slaidi		
Pasniedzšanas metode	Klātienē Tiešsaistē Jaukta pasniedzšanas metode Diskusijas		
Novērtējums	Klātienes / tiešsaistes tests		
Mācību rezultāti	<ul style="list-style-type: none"> • Kiberdrošības juridisko aspektu izpratne • Izpratne par pašreizējo ES politiku saistībā ar kiberdrošību • Izpratne par ES tiesību aktiem, kas saistīti ar kiberdrošību • Kiberdrošības vietējo likumu saistīšana un salīdzināšana ar ES tiesību aktiem 		
Prasības	IT un biznesa pamatzināšanas varētu būt noderīgas, lai labāk izprastu moduli		
Moduļa apraksts	<p>Šis modulis iepazīstina izglītojamo ar pašreizējām ES politikām un iniciatīvām, kuru mērķis ir veicināt kiberdrošības jēdzienu. Tajā aplūkoti arī kiberdrošības juridiskie aspekti gan ES, gan visā pasaulē, ļaujot izglītojamajiem iepazīties ar daudziem reālās dzīves scenārijiem un gadījumu izpēti šajā jomā.</p> <p>Modulis ietver pārskatu par kiberdrošības tendencēm, tostarp, bet ne tikai statistiku, attīstības tendencēm, būtiskajiem apdraudējumiem, juridiskajiem, reputācijas un finanšu riskiem un gadījumu izpēti analīzi.</p>		
MODUĻA APAKŠTĒMAS			
2.1 Kiberdrošības veicināšana Eiropas Savienībā	<ul style="list-style-type: none"> • Īss ievads par ES politiku un iniciatīvām, kuru mērķis ir veicināt kiberdrošības jēdzienu 		
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	1,0	20	30
2.2 Kiberdrošības juridiskie aspekti	<ul style="list-style-type: none"> • Kiberdrošības juridiskie aspekti visā pasaulē (vispārīgi) un jo īpaši ES, tostarp neatbilstības sekas • Kiberdrošības vietējo likumu saistība, salīdzinājums un kontrasts ar ES likumiem 		
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	0,5	5	7
2.3 Pārskats par kiberdrošības tendencēm	<ul style="list-style-type: none"> • Reālo dzīves scenāriju un gadījumu izpēte, ieskaitot statistiku, tendences, attiecīgos draudus, riskus (juridiskos, reputācijas, finanšu) • Ieskaits neseno kiberuzbrukumos un diskusijas par kvalifikācijas celšanas nozīmi, ņemot vērā iespējamus kiberuzbrukumu riskus. 		



	<i>Piezīme: Diskusija var noritēt tiešsaistē vai klātienē. Treneris vada diskusiju un sniedz norādes par to, kas sagaidāms no diskusijas.</i>		
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	1,5	23	30

3.2.3 Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana

Moduļa nosaukums	3.0 Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana		
Kopējais ilgums <i>(Stundas / slaidi)</i>	10 stundas 150 - 200 slaidi		
Pasniegšanas metode	Klātienē Tiešsaistē Jaukta pasniegšanas metode Interaktīvu rīku (piemēram, tiešsaistes scenāriju rīku) izmantošana Diskusijas		
Novērtējums	Klātienēs / tiešsaistes tests		
Mācību rezultāti	<ul style="list-style-type: none"> • Izprot kiberuzbrukumu jēdzienu • Spēj definēt sociālo inženieriju un apgriezto sociālo inženieriju • Izprot sociālās inženierijas modalitāti un tās saistību ar kiberuzbrukumiem • Izprot visbiežāk sastopamos kiberdrošības draudus • Izprot galvenās kiberuzbrukumu kategorijas un paņēmienus 		
Prasības	IT un biznesa pamatzināšanas varētu būt noderīgas, lai labāk izprastu moduli		
Moduļa apraksts	<p>Šis modulis iepazīstina izglītojamo ar kiberuzbrukumiem, īpašu uzmanību pievēršot pikšķerēšanai. Tajā arī detalizēti aplūkoti sociālās inženierijas un reversās sociālās inženierijas jēdzieni, kā arī sociālās inženierijas ciešā saikne ar kiberuzbrukumiem.</p> <p>Moduļa ietvaros tiek aplūkoti arī dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni, kā arī vairāki reāli gadījumu izpētes piemēri no projekta partnervalstīm.</p>		
MODUĻA APAKŠTĒMAS			
3.1 Ievadinformācija par kiberuzbrukumiem	<ul style="list-style-type: none"> • Īsa ievadinformācija par kiberuzbrukumiem, jo īpaši pikšķerēšanas uzbrukumiem 		
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>



	0,5	8	10
3.2 Sociālās inženierijas moduļi un manipulācijas	<ul style="list-style-type: none"> Sociālo inženierijas modeļu pārskats, īpašu uzmanību pievēršot šādiem aspektiem: <ul style="list-style-type: none"> a) "Ietekmes ieroči" - R. Cialdini² <ul style="list-style-type: none"> - Atbildes darbība - Aņņemšanās un konsekvence - Sociālie pierādījumi - Patika - Autoritāte - Trūkums b) Sociālās inženierijas psiholoģiskie aspekti c) Pārskats par reverso sociālo inženieriju 		
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	4	60	80
3.3 Dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni	<ul style="list-style-type: none"> Šajā sadaļā tiek definēti dažādi kiberuzbrukumu veidi (jo īpaši, pikšķerēšana) un tas, kā tos atpazīt (nākamā nodaļa), tostarp, bet ne tikai: <p>Kategorijas</p> <ul style="list-style-type: none"> - Ar VDAR saistīti uzbrukumi - E-pasti; - Tūlītējā ziņojumapmaiņa; - Sociālie tīkli; - Tīmekļa vietnes; - Izkrāpšana ar loterijas palīdzību; - SMS; - Tālruņa zvani; - Klātienē; - "Sērfošana uz citu pleciem"; <p>Dažādu tehniku apvienojums</p> <ul style="list-style-type: none"> - "Spray and Pray" jeb masveida pikšķerēšana - "Spear phishing" jeb mērķtiecīga pikšķerēšana - "Whaling" jeb vaļu medības - "Vishing" jeb balss pikšķerēšana - "Smishing" jeb SMS pikšķerēšana - "Angler Phishing" jeb klientu apkalpošanas pikšķerēšana - "Clone phishing" jeb klona pikšķerēšana - "Malvertising" jeb ļaunprātīgas reklāmas 		
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	4	60	80

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



3.4 Gadījumu izpēte	<ul style="list-style-type: none"> Vairāku dažādu partnerorganizāciju veiktu gadījumu pētījumu prezentācija Tiešsaistes vai klātienē diskusija mazās grupās (5-6 studenti) <i>Piezīme: Diskusija notiek kā vingrinājums, katrai grupai atrodot un analizējot nesenu pikšķerēšanas uzbrukumu, iekļaujot tādu informāciju kā uzbrukuma datumu, informācija par upuri, uzbrukuma modalitāti, sekas, gūtās mācības un tā tālāk. Pēc tam izglītojamais no katras grupas iepazīstina pārējos ar analīzes rezultātiem. Treneris un kolēģi sniedz konstruktīvas atsauksmes.</i> 		
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	1,5	22	30

3.2.4 Kiberuzbrukumu izpratne un rīcība kiberuzbrukuma gadījumā

Moduļa nosaukums	4.0 Kiberuzbrukumu izpratne un rīcība kiberuzbrukuma gadījumā
Kopējais ilgums <i>(Stundas / slaidi)</i>	14 stundas 210 - 255 slaidi
Pasniegšanas metode	Klātienē Tiešsaistē Jaukta pasniegšanas metode
Novērtējums	Klātienē / tiešsaistes tests
Mācību rezultāti	<ul style="list-style-type: none"> Apgūt pamatzināšanas par e-drošību un drošību Izprot dažādu informācijas saturu Izprot identitāti un nošķirt dažādus uzbrukumus, kas saistīti ar identitāti Izprot kiberuzbrukumu radītās sekas indivīdiem un/vai organizācijām Definē un izprot kiberhigiēnas kā proaktīvas darbības pret kiberuzbrukumiem nozīmi Izprot un izmanto dažādas aizsardzības metodes pret kiberuzbrukumiem Izstrādā un ievieš rīcības plānu reaģēšanai uz kiberuzbrukumu
Prasības	Iepriekšējie moduļi
Moduļa apraksts	Šis modulis iepazīstina izglītojamo ar e-drošības jēdzienu un par proaktīvas pieejas kiberdraudiem nozīmi, izmantojot kiberhigiēnas koncepciju. Modulī arī sīkāk aplūkota pieeja kiberuzbrukumu atpazīšanai un novēršanai. Modulis iepazīstina ar incidentu reaģēšanas plānu izstrādi un ieviešanu, lai mazinātu kiberuzbrukumu sekas.
MODUĻA APAKŠTĒMAS	



4.1 Pamatzināšanas par e-drošību	<ul style="list-style-type: none"> • Informācijas satura atšķirības (atklāta, privāta, biznesa u.t.t.); Intelektuālais īpašums; Autortiesības; • Izpratne par identitātes terminu; zināšanas par identitātes zādzībām un zādzības metodēm. Informācija par spieģrogrammatūru, tastatūras spiegiem, krāpniecisku reklāmu, Trojas zirgiem. Zina dažādus veidus, kā ļaunprātīga programmatūra var iekļūt ierīcē. • Zina par identitātes un personas datu zādzību cēloņiem un sekām darbavietā un internetā (krāpnieciska informācijas izmantošana, informācijas zuduma draudi, sabotāža). • Zina par draudiem, kas saistīti ar personas datu izpaušanu. • Īss ievads par kiberuzbrukumu sekām gan indivīdam, gan organizācijai. Papildu informācija jāizpēta 4.4. sadaļā. 			
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	
	0,5	8	10	
4.2 Proaktīvas darbības	<ul style="list-style-type: none"> • Kiberhigiēna internetā (līdz minimumam samaziniet informāciju par personām, tostarp informāciju personīgajos kontos sociālajos medijos, ko uzbrucēji varētu izmantot) • Kiberhigiēna darba vietā • Tehnoloģiskie rīki un pasākumi (pikšķerēšanas e-pastu filtrēšana un bloķēšana) 			
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	
	2	30	35	
4.3. Pikšķerēšanas uzbrukumu atpazīšana	<ul style="list-style-type: none"> • Gadījumu izpētes analīze, izmantojot 3.3. sadaļā - <i>Dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni</i> minētos paņēmienus • Sadaļa kiberuzbrukumu atpazīšanai (atsaucoties uz iepriekšējās nodaļas punktiem), tostarp, bet ne tikai: <ul style="list-style-type: none"> - Kritiskā domāšana - Saišu pārbaude - Izpratne par URL - Ziņojumu analīze - Sarkano karogu atpazīšana 			
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	
	5	75	90	
4.4 Rīcība kiberuzbrukumu gadījumā	<ul style="list-style-type: none"> • Informācija par kiberdrošību, tostarp informācija par kaitējumu, ko kiberuzbrukumi nodada indivīdiem un organizācijām, un to, kā rīkoties kiberuzbrukuma gadījumā, balstoties uz iepriekšējā nodaļā apgūto. <p>Cita starpā, jāiekļauj šādi aspekti:</p> <ul style="list-style-type: none"> - Droša navigācija - Spēcīgu paroli izveide - Izvairīšanās no uzbrukumiem 			
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	



	<ul style="list-style-type: none"> - Droša iepirkšanās tiešsaistē - Pretkiberuzbrukumu programmatūras instalēšana - Sīkdatnes - Atbilstošu dublējumu izveide - Failu šifrēšana - Divu faktoru autentifikācija - Ļaunprogrammatūra - Droša pārlūkošana <ul style="list-style-type: none"> • Šajā sadaļā tiek iekļauti arī vietējie / Eiropas / starptautiskie gadījumu pētījumu piemēri, kas minēti iepriekšējos modulos. • Kur tas nepieciešams, šajā sadaļā ietver vienkāršas soli pa solim instrukcijas un attālus. • Šajā sadaļā iekļauta informācija par darbībām, kas jāveic, reaģējot uz kiberuzbrukumu, tostarp atkopšanas procedūras, ja organizācija un/vai lietotājs kļūst par kiberuzbrukuma upuriem. 						
	<table border="1"> <thead> <tr> <th data-bbox="496 846 853 920"><i>leteicamais ilgums stundās</i></th> <th data-bbox="853 846 1141 920"><i>Minimālais slaidu skaits</i></th> <th data-bbox="1141 846 1396 920"><i>Maksimālais slaidu skaits</i></th> </tr> </thead> <tbody> <tr> <td data-bbox="496 920 853 965">5</td> <td data-bbox="853 920 1141 965">75</td> <td data-bbox="1141 920 1396 965">90</td> </tr> </tbody> </table>	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	5	75	90
<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>					
5	75	90					
<p>4.5 Kaitējuma mazināšana, reaģējot uz incidentiem</p>	<ul style="list-style-type: none"> • Incidentu reaģēšanas plānu izstrāde, attīstīšana un īstenošana, norādot rekomendētās darbības un labāko praksi, ko nepieciešams īstenot datu aizsardzības pārkāpuma gadījumā. <p><i>Piezīme: Šīs sadaļas elementus var pielāgot konkrēto valstu vajadzībām.</i></p> <table border="1"> <thead> <tr> <th data-bbox="496 1144 853 1218"><i>leteicamais ilgums stundās</i></th> <th data-bbox="853 1144 1141 1218"><i>Minimālais slaidu skaits</i></th> <th data-bbox="1141 1144 1396 1218"><i>Maksimālais slaidu skaits</i></th> </tr> </thead> <tbody> <tr> <td data-bbox="496 1218 853 1261">1,5</td> <td data-bbox="853 1218 1141 1261">22</td> <td data-bbox="1141 1218 1396 1261">30</td> </tr> </tbody> </table>	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	1,5	22	30
<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>					
1,5	22	30					