

# Aizsardzība pret pikšķerēšanu 4. industriālās revolūcijas laikmetā (CyberPhish)



## CyberPhish saīsinātā 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

<b>Saturs</b> .....	<b>2</b>
<b>Ievads</b> .....	<b>3</b>
<b>1. Mācību programmas (e-apmācības moduļa) struktūra</b> .....	<b>3</b>
1.1 Ievads .....	3
1.2 Detalizēta e-apmācības moduļa struktūra .....	4
1.2.1 Ievads kiberdrošībā .....	4
1.2.2 Kiberdrošība Eiropas Savienībā (ES).....	6
1.2.3 Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana .....	7
1.2.4 Kiberuzbrukumu izpratne un rīcība kiberuzbrukuma gadījumā.....	9

## IEVADS

Cyberphish saīsinātā mācību programma detalizēti apraksta mācību programmas struktūru, un tās mērķis ir sniegt kodolīgus, bet tālejošus moduljus kiberdrošības jomā, īpašu uzsvaru liekot uz pikšķerēšanas uzbrukumiem. To izmanto ieviešanai augstākās izglītības iestāžu studiju moduļos un izplatīšanas nolūkos, lai piesaistītu dalībniekus kursiem.

Šo īso versiju veido trīs līmeņu tēmas: galvenās tēmas, apakštēmas un apakštēmu punkti, kuru galvenā mērķauditorija ir studenti, citi kursu dalībnieki un pasniedzēji. Tie var izmantot šo mācību programmu, lai izprastu šī kursa galvenos mērķus un uzdevumus.

Svarīgi atzīmēt, ka, lai gan mācību programmas īstenošanā ir paredzēta jaukta mācību pieeja, veids, kā tā ir strukturēta, ļauj elastīgi to īstenot.

Mācību programma nodarbojas ar kiberdrošības ieviešanu, īpašu uzmanību pievēršot pikšķerēšanai. Tā ir paredzēta gan uzņēmumiem, gan privātpersonām kopumā, un tās mērķis ir sagatavot abas puses 4. industriālās revolūcijas laikam un potenciālajām drošības problēmām, ko tā rada.

Mācību programmas ietvaros izglītojamie apgūst prasmes, kā atpazīt un novērst kiberuzbrukumus un kā aizsargāt ierīces un datus pret brutāliem uzbrukumiem.

## MĀCĪBU PROGRAMMAS (E-APMĀCĪBAS MODUĻA) STRUKTŪRA

### 1.1 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.

<b><i>Mācību programmas modulis</i></b>	<b><i>Moduļa mērķis</i></b>
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 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 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 izpētes analīzi.</p>
3.0 Kiberuzbrukumi - sociālā inženierija un pikšķerēšana	<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>
4.0 Kiberuzbrukumu izpratne un rīcība kiberuzbrukuma gadījumā	<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>

## 1.2 Detalizēta e-apmācības moduļa struktūra

### 1.2.1 Ievads kiberdrošībā

<b>Moduļa nosaukums</b>	1.0 Ievads kiberdrošībā
<b>Kopējais ilgums</b> (Stundas / slaidi)	3 stundas 46 - 60 slaidi
<b>Pasniegšanas metodes</b>	Klātienē Tiešsaistē Jaukta pasniegšanas metode
<b>Novērtējums</b>	Klātienē / tiešsaistes tests



<b>Mācību rezultāti</b>	<ul style="list-style-type: none"> <li>• Vispārēja izpratne par kiberdrošību</li> <li>• Izpratne par kiberdrošības izaicinājumiem</li> <li>• Izpratne par to, kā kiberuzbrukumi ir mainījušies laika gaitā, kā rezultātā pastiprinājušies kiberuzbrukumu darbības un tādējādi arī pretpasākumi</li> <li>• Izpratne par to, kādēļ ir svarīgi sekot līdzi kiberdrošības jaunumiem un kādēļ ir nepieciešams pastāvīgi atjaunināt zināšanas par kiberdrošību</li> <li>• Izpratne par dažādām ar kiberdrošību saistītām definīcijām</li> </ul>		
<b>Prasības</b>	Sākotnējās zināšanas nav nepieciešamas		
<b>Moduļa apraksts</b>	<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>		
<b>MODUĻA APAKŠTĒMAS</b>			
<b>1.1 Vispārīga informācija - 4. industriālās revolūcijas izaicinājumi</b>	<ul style="list-style-type: none"> <li>• Ievads kiberdrošībā</li> <li>• Īsa kibernetikas attīstības vēsture un tās straujās izaugsmes iemesli, kā arī vēsturiskie posmi un pašreizējā situācija</li> <li>• Vispārīga informācija par problēmu, iezīmējot kiberuzbrukumu radītos izaicinājumus, ar ko saskaras uzņēmumi</li> <li>• Izaicinājumi, ar ko saskaras uzņēmumi: <ul style="list-style-type: none"> <li>- Nav robežu;</li> <li>- Tehnoloģijas: Plaša tehnoloģiju (mobilo tehnoloģiju) izmantošana;</li> <li>- Mākoņdatošana;</li> <li>- Lielo datu izaicinājumi;</li> <li>- Trešo personu riski;</li> <li>- Lietu internets;</li> </ul> </li> <li>• Pieaugošo draudu izaicinājums;</li> <li>• Valstu apdraudējumi</li> </ul>		
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	1,5	23	30



<b>1.2 Kiberdrošības vēsture</b>	<ul style="list-style-type: none"> <li>• Īss izklāsts par to, kā kiberuzbrukumi ir mainījušies laika gaitā, kā rezultātā pastiprinājušies kiberuzbrukumu darbības un tādējādi arī pretpasākumi.</li> <li>• Šajā sadaļā var tikt iekļauti vietējie / Eiropas / starptautiskie gadījumu pētījumi</li> </ul>		
	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	1,0	15	20
<b>1.3 Kiberdrošības definīcijas</b>	<ul style="list-style-type: none"> <li>• Sadaļa par kiberdrošības žargonu / terminiem un statistiku / avotiem</li> </ul>		
	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	0,5	8	10

### 1.2.2 Kiberdrošība Eiropas Savienībā (ES)

<b>Moduļa nosaukums</b>	2.0 Kiberdrošība ES
<b>Kopējais ilgums</b> <i>(Stundas / slaidi)</i>	3 stundas 48 - 67 slaidi
<b>Pasniegšanas metode</b>	Klātienē Tiešsaistē Jaukta pasniegšanas metode Diskusijas
<b>Novērtējums</b>	Klātienes / tiešsaistes tests
<b>Mācību rezultāti</b>	<ul style="list-style-type: none"> <li>• Kiberdrošības juridisko aspektu izpratne</li> <li>• Izpratne par pašreizējo ES politiku saistībā ar kiberdrošību</li> <li>• Izpratne par ES tiesību aktiem, kas saistīti ar kiberdrošību</li> <li>• Kiberdrošības vietējo likumu saistīšana un salīdzināšana ar ES tiesību aktiem</li> </ul>
<b>Prasības</b>	IT un biznesa pamatzināšanas varētu būt noderīgas, lai labāk izprastu moduli
<b>Moduļa apraksts</b>	<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>
<b>MODUĻA APAKŠTĒMAS</b>	



<b>2.1 Kiberdrošības veicināšana Eiropas Savienībā</b>	<ul style="list-style-type: none"> <li>• Īss ievads par ES politiku un iniciatīvām, kuru mērķis ir veicināt kiberdrošības jēdzienu</li> </ul>			
	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	
	1,0	20	30	
<b>2.2 Kiberdrošības juridiskie aspekti</b>	<ul style="list-style-type: none"> <li>• Kiberdrošības juridiskie aspekti visā pasaulē (vispārīgi) un jo īpaši ES, tostarp neatbilstības sekas</li> <li>• Kiberdrošības vietējo likumu saistība, salīdzinājums un kontrasts ar ES likumiem</li> </ul>			
	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	
	0,5	5	7	
<b>2.3 Pārskats par kiberdrošības tendencēm</b>	<ul style="list-style-type: none"> <li>• Reālo dzīves scenāriju un gadījumu izpēte, ieskaitot statistiku, tendences, attiecīgos draudus, riskus (juridiskos, reputācijas, finanšu)</li> <li>• Ieskats nesenantos kiberuzbrukumos un diskusijas par kvalifikācijas celšanas nozīmi, ņemot vērā iespējamus kiberuzbrukumu riskus.</li> </ul> <p><i>Piezīme: Diskusija var noritēt tiešsaistē vai klātienē. Treneris vada diskusiju un sniedz norādes par to, kas sagaidāms no diskusijas.</i></p>			
	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	
	1,5	23	30	

### 1.2.3 Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana

<b>Moduļa nosaukums</b>	3.0 Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana
<b>Kopējais ilgums</b> <i>(Stundas / slaidi)</i>	10 stundas 150 - 200 slaidi
<b>Pasniegšanas metode</b>	Klātienē Tiešsaistē Jaukta pasniegšanas metode Interaktīvu rīku (piemēram, tiešsaistes scenāriju rīku) izmantošana Diskusijas
<b>Novērtējums</b>	Klātienē / tiešsaistes tests
<b>Mācību rezultāti</b>	<ul style="list-style-type: none"> <li>• Izprot kiberuzbrukumu jēdzienu</li> <li>• Spēj definēt sociālo inženieriju un apgriezto sociālo inženieriju</li> <li>• Izprot sociālās inženierijas modalitāti un tās saistību ar kiberuzbrukumiem</li> <li>• Izprot visbiežāk sastopamos kiberdrošības draudus</li> <li>• Izprot galvenās kiberuzbrukumu kategorijas un paņēmienus</li> </ul>



<b>Prasības</b>	IT un biznesa pamatzināšanas varētu būt noderīgas, lai labāk izprastu moduli		
<b>Moduļa apraksts</b>	<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>		
<b>MODUĻA APAKŠTĒMAS</b>			
<b>3.1 Ievadinformācija par kiberuzbrukumiem</b>	<ul style="list-style-type: none"> <li>Īsa ievadinformācija par kiberuzbrukumiem, jo īpaši pikšķerēšanas uzbrukumiem</li> </ul>		
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	0,5	8	10
<b>3.2 Sociālās inženierijas moduļi un manipulācijas</b>	<ul style="list-style-type: none"> <li>Sociālo inženierijas modeļu pārskats, īpašu uzmanību pievēršot šādiem aspektiem: <ul style="list-style-type: none"> <li>a) "Ietekmes ieroči" - R. Cialdini<sup>1</sup> <ul style="list-style-type: none"> <li>- Atbildes darbība</li> <li>- Aņņemšanās un konsekvence</li> <li>- Sociālie pierādījumi</li> <li>- Patika</li> <li>- Autoritāte</li> <li>- Trūkums</li> </ul> </li> <li>b) Sociālās inženierijas psiholoģiskie aspekti</li> <li>c) Pārskats par reverso sociālo inženieriju</li> </ul> </li> </ul>		
	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	4	60	80
<b>3.3 Dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni</b>	<ul style="list-style-type: none"> <li>Šajā sadaļā tiek definēti dažādi kiberuzbrukumu veidi (jo īpaši, pikšķerēšana) un tas, kā tos atpazīt (nākamā nodaļa), tostarp, bet ne tikai: <p><b>Kategorijas</b></p> <ul style="list-style-type: none"> <li>- Ar VDAR saistīti uzbrukumi</li> <li>- E-pasti;</li> <li>- Tūlītējā ziņojumapmaiņa;</li> <li>- Sociālie tīkli;</li> <li>- Tīmekļa vietnes;</li> <li>- Izkrāpšana ar loterijas palīdzību;</li> <li>- SMS;</li> </ul> </li> </ul>		

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



	<ul style="list-style-type: none"> <li>- Tālruņa zvani;</li> <li>- Klātienē;</li> <li>- “Sērfošana uz citu pleciem”;</li> </ul> <p><b>Dažādu tehniku apvienojums</b></p> <ul style="list-style-type: none"> <li>- “Spray and Pray” jeb masveida pikšķerēšana</li> <li>- “Spear phishing” jeb mērķtiecīga pikšķerēšana</li> <li>- “Whaling” jeb vaļu medības</li> <li>- “Vishing” jeb balss pikšķerēšana</li> <li>- “Smishing” jeb SMS pikšķerēšana</li> <li>- “Angler Phishing” jeb klientu apkalpošanas pikšķerēšana</li> <li>- “Clone phishing” jeb klona pikšķerēšana</li> <li>- “Malvertising” jeb ļaunprātīgas reklāmas</li> </ul>		
	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	4	60	80
<b>3.4 Gadījumu izpēte</b>	<ul style="list-style-type: none"> <li>• Vairāku dažādu partnerorganizāciju veiktu gadījumu pētījumu prezentācija</li> <li>• 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 datums, informācija par upuri, uzbrukuma modalitāte, sekas, gūtās mācības un tā tālāk. Pēc tam izglītojamais no katras grupas iepazīstina pārējos ar analīzes rezultātiem. Treneris un kolēģi sniedz konstruktīvas atsauksmes.</i></li> </ul>		
	<i>leteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>
	1,5	22	30

#### 1.2.4 Kiberuzbrukumu izpratne un rīcība kiberuzbrukuma gadījumā

<b>Moduļa nosaukums</b>	4.0 Kiberuzbrukumu izpratne un rīcība kiberuzbrukuma gadījumā
<b>Kopējais ilgums</b> <i>(Stundas / slaidi)</i>	14 stundas 210 - 255 slaidi
<b>Pasniegšanas metode</b>	Klātienē Tiešsaistē Jaukta pasniegšanas metode
<b>Novērtējums</b>	Klātienē / tiešsaistes tests
<b>Mācību rezultāti</b>	<ul style="list-style-type: none"> <li>• Apgūt pamatzināšanas par e-drošību un drošību</li> <li>• Izprot dažādu informācijas saturu</li> <li>• Izprot identitāti un nošķirt dažādus uzbrukumus, kas saistīti ar identitāti</li> <li>• Izprot kiberuzbrukumu radītās sekas indivīdiem un/vai organizācijām</li> </ul>



	<ul style="list-style-type: none"> <li>• Definē un izprot kiberhigiēnas kā proaktīvas darbības pret kiberuzbrukumiem nozīmi</li> <li>• Izprot un izmanto dažādas aizsardzības metodes pret kiberuzbrukumiem</li> <li>• Izstrādā un ievieš rīcības plānu reaģēšanai uz kiberuzbrukumu</li> </ul>					
<b>Prasības</b>	Iepriekšējie moduļi					
<b>Moduļa apraksts</b>	<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>					
<b>MODUĻA APAKŠTĒMAS</b>						
<b>4.1 Pamatzināšanas par e-drošību</b>	<ul style="list-style-type: none"> <li>• Informācijas satura atšķirības (atklāta, privāta, biznesa u.t.t.); Intelektuālais īpašums; Autortiesības;</li> <li>• 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.</li> <li>• Zina par identitātes un personas datu zādzību cēloņiem un sekām darbavietā un internetā (krāpnieciska informācijas izmantošana, informācijas zuduma draudi, sabotāža).</li> <li>• Zina par draudiem, kas saistīti ar personas datu izpaušanu.</li> <li>• Īss ievads par kiberuzbrukumu sekām gan individuālam, gan organizācijai. Papildu informācija jāizpēta 4.4. sadaļā.</li> </ul>					
	<table border="1"> <thead> <tr> <th><i>Ieteicamais ilgums stundās</i></th> <th><i>Minimālais slaidu skaits</i></th> <th><i>Maksimālais slaidu skaits</i></th> </tr> </thead> <tbody> <tr> <td>0,5</td> <td>8</td> <td>10</td> </tr> </tbody> </table>	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	0,5	8
<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>				
0,5	8	10				
<b>4.2 Proaktīvas darbības</b>	<ul style="list-style-type: none"> <li>• Kiberhigiēna internetā (līdz minimumam samaziniet informāciju par personām, tostarp informāciju personīgajos kontos sociālajos medijos, ko uzbrucēji varētu izmantot)</li> <li>• Kiberhigiēna darba vietā</li> <li>• Tehniskie rīki un pasākumi (pikšķerēšanas e-pastu filtrēšana un bloķēšana)</li> </ul>					
	<table border="1"> <thead> <tr> <th><i>Ieteicamais ilgums stundās</i></th> <th><i>Minimālais slaidu skaits</i></th> <th><i>Maksimālais slaidu skaits</i></th> </tr> </thead> <tbody> <tr> <td>2</td> <td>30</td> <td>35</td> </tr> </tbody> </table>	<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>	2	30
<i>Ieteicamais ilgums stundās</i>	<i>Minimālais slaidu skaits</i>	<i>Maksimālais slaidu skaits</i>				
2	30	35				



<b>4.3. Pikšķerēšanas uzbrukumu atpazīšana</b>	<ul style="list-style-type: none"> <li>Gadījumu izpētes analīze, izmantojot 3.3. sadaļā - <i>Dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni</i> minētos paņēmienus</li> <li>Sadaļa kiberuzbrukumu atpazīšanai (atsaucoties uz iepriekšējās nodaļas punktiem), tostarp, bet ne tikai: <ul style="list-style-type: none"> <li>Kritiskā domāšana</li> <li>Saišu pārbaude</li> <li>Izpratne par URL</li> <li>Ziņojumu analīze</li> <li>Sarkano karogu atpazīšana</li> </ul> </li> </ul>		
	<i>leteicamais ilgums stundās</i> 5	<i>Minimālais slaidu skaits</i> 75	<i>Maksimālais slaidu skaits</i> 90
<b>4.4 Rīcība kiberuzbrukumu gadījumā</b>	<ul style="list-style-type: none"> <li>Informācija par kiberdrošību, tostarp informācija par kaitējumu, ko kiberuzbrukumi nodada indivīdiem un organizācijām, un to, kā rīkoties kiberuzbrukuma gadījumā, balstoties uz iepriekšējā nodaļā apgūto.</li> </ul> <p>Cita starpā, jāiekļauj šādi aspekti:</p> <ul style="list-style-type: none"> <li>Droša navigācija</li> <li>Spēcīgu parolu izveide</li> <li>Izvairīšanās no uzbrukumiem</li> <li>Droša iepirkšanās tiešsaistē</li> <li>Pretkiberuzbrukumu programmatūras instalēšana</li> <li>Sīkdatnes</li> <li>Atbilstošu dublējumu izveide</li> <li>Failu šifrēšana</li> <li>Divu faktoru autentifikācija</li> <li>Ļaunprogrammatūra</li> <li>Droša pārlūkošana</li> </ul> <ul style="list-style-type: none"> <li>Šajā sadaļā tiek iekļauti arī vietējie / Eiropas / starptautiskie gadījumu pētījumu piemēri, kas minēti iepriekšējos moduļos.</li> <li>Kur tas nepieciešams, šajā sadaļā ietver vienkāršas soli pa solim instrukcijas un attālus.</li> <li>Šajā sadaļā iekļauta informācija par darbībām, kas jāveic, reaģējot uz kiberuzbrukumu, tostarp atkopšanas procedūras, ja organizācija un/vai lietotājs kļūst par kiberuzbrukuma upuriem.</li> </ul>		
	<i>leteicamais ilgums stundās</i> 5	<i>Minimālais slaidu skaits</i> 75	<i>Maksimālais slaidu skaits</i> 90
<b>4.5 Kaitējuma mazināšana, reaģējot uz incidentiem</b>	<ul style="list-style-type: none"> <li>Incidentu reaģēšanas plānu izstrāde, attīstīšana un īstenošana, norādot rekomendētās darbības un labāko praksi, ko nepieciešams īstenot datu aizsardzības pārkāpuma gadījumā.</li> </ul> <p><i>Piezīme: Šīs sadaļas elementus var pielāgot konkrēto valstu vajadzībām.</i></p>		
	<i>leteicamais ilgums stundās</i> 1,5	<i>Minimālais slaidu skaits</i> 22	<i>Maksimālais slaidu skaits</i> 30

