Veselības informācijas sistēmu apmācību un sertifikācijas ieviešana augstākajā izglītībā

Programmas apraksts

Rezultāts Nr. 2 (O2)
Pēdējo reizi atjaunots: 30.08.2017
Autori:

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.

HIS4HE programmas apraksts

Šī mācību programma sniedz informāciju par noteikumiem un procedūru principiem, personas datu aizsardzību, konfidencialitāti un informācijas drošību darbavietās, kur tiek izmantotas veselības informācijas sistēmas.

Kam šis mācību programma ir paredzēta?
Šī mācību programma ir adresēta pašreizējiem un nākamajiem veselības nozares speciālistiem, kuri vēlas pilnveidot un apliecināt savu kvalifikāciju Veselības informācijas sistēmu lietošanā. Nozares skatījumā mērķa grupa ir medicīnas studenti un pasniedzēji.
Darba tirgus skatījumā ECDL Veselības moduļa ieviešana paaugstinās jauno speciālistu profesionālo kvalifikāciju, un palīdzēs sasniegt veselības nozares prasības.

HIS4HE projekta pieeja
Projekts nodrošina jaukta tipa mācību kursu, kas sastāv no divām daļām – 1. modulis: Pārskats par veselības informācijas sistēmām, to galvenajām iezīmēm, 2. modulis: Darba vietas IT drošība.

Programmas mērķi

Veiksmīgi apgūstot mācību saturu, mācību kursa dalībnieki gūs izpratni par:

- galvenajām veselības informācijas sistēmas (VeIS) iezīmēm;
- ētiskiem jautājumiem un noteikumiem, kas attiecas uz VeIS lietošanu;
- konfidencialitātes, drošības un piekļuves kontroles jautājumiem, izmantojot VeIS;
- elektroniski saglabāto datu analīzes un interpretācijas principiem ;
- vispārīgām zināšanām par IT drošības jautājumiem;
- darba vietas drošības jautājumiem;
- drošu datora lietošanu un darbību digitālajā vidē

HIS4HE projekta apraksts

Viens no projekta *HIS4HE* mērķiem ir atbalstīt veselības aprūpes studentus un jau esošos speciālistus elektronisko veselības sistēmu izmantošanā. Projektā ir izveidots jaukta tipa mācību kurss, kuru sekmīgi pabeidzot, dalībnieki būs sagatavoti darbam ar VeIS , kā arī atbilstoša ECDL sertifikācijas eksāmena kārtošanai. Šo projektu īsteno piecas partneru organizācijas no Lietuvas, Latvijas un Vācijas.

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.

1. modulis

	KATEGORIJA	TĒMA	Nr.	UZDEVUMU APRAKSTS
	1. Jēdzieni	*1.1. Veselības aprūpes informācijas sistēmas*	1.1.1	Definējiet vienotās veselības nozares elektroniskās informācijas sistēmu (turpmāk – veselības aprūpes informācijas sistēma) kā ar pacientu saistītas informācijas uzskaites, glabāšanas un atjaunināšanas platformu, kā klīniskās diagnostikas vajadzībām, tā arī administratīvajām procedūrām.
			1.1.2	Izprotiet, ka veselības aprūpes informācijas sistēma var ietvert pacientu personas datus vai iedzīvotāju veselības stāvokļa ierakstus.
			1.1.3	Izprotiet, ka Elektroniskas veselības kartes informācijas sistēma (turpmāk – EVK IS) ietver pacientu slimības vēsturi, diagnozi, izmeklējumu rezultātus un ārstēšanas plānu, preventīvos pasākumus, iespējams iegūt arī statistiskos datus par iedzīvotāju veselības stāvokli.
			1.1.4	Izprotiet saikni starp datiem par iedzīvotāju veselības stāvokli un pacientu slimības vēsturi.
			1.1.5	Novērtējiet veselības aprūpes pakalpojumu ieguvumus, izmantojot veselības aprūpes informācijas sistēmu, piemēram, saņemot uzticamāku un aktuālāku informāciju, kas uzlabo pacientu aprūpes kvalitāti.

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.

	KATEGORIJA	TĒMA	Nr.	UZDEVUMU APRAKSTS
		1.2. VIS veidi	1.2.1	Izprotiet, ka veselības aprūpes informācijas sistēma sastāv no divām daļām - publiskās daļas un daļas, kurai var piekļūt tikai autorizēti lietotāji. Publiskajā daļā ir pieejama informācija par veselības nozares jaunumiem, veselīgu dzīvesveidu un cita aktuāla informācija. Autorizētajā daļā var pieslēgties kā iedzīvotājs vai kā veselības aprūpes speciālists. Pacienti var apskatīt savus veselības stāvokļa datus, noteikt piekļuvi ārstiem saviem veselības datiem, apskatīt sev izrakstītās medikamentu e-receptes, apskatīt savas e-darbnespējas lapas. Medicīniskais personāls var apskatīt savu pacientu veselības stāvokļa datus, izrakstīt parastās un īpašās e-receptes, izrakstīt e-darbnespējas lapas. Farmaceiti var atzīmēt medikamenta izsniegšanu aptiekā (parastās un īpašās e-receptes).
			1.2.2	Aprakstiet veselības aprūpes informācijas sistēmas galvenās īpašības, piemēram, pieejama, uzticama, ātra piekļuve datiem, iespējams koplietošanas skats, atjaunināta, precīza, nodrošina aprūpes nepārtrauktību, efektīva un tajā ir iekļautas svarīgas drošības funkcijas.
			1.2.3	Izprotiet par veselības aprūpes informācijas sistēmas funkcijām vai rīkiem, piemēram, tikšanās laika rezervēšana un plānošana, rezultātu nosūtīšana, pacientu datu atjaunināšana, recepšu izsniegšana, veselības aprūpe mājās, izmantojot internetu.
			1.2.4	Novērtējiet potenciālos trūkumus, izmantojot veselības aprūpes informācijas sistēmu, piemēram: pārmaiņas medicīniskā personāla/pacientu attiecībās, pacientu veselības stāvokļa datu konteksta zaudēšana u.c.
			1.2.5	Izprotiet, ka veselības aprūpes informācijas sistēma atbalsta, bet neaizstāj klīnisko spriedumu.
			1.2.6	Izprotiet veselības aprūpes informācijas sistēmu veidus, piemēram: biroja vai nodaļas, lokālās, reģionālās, nacionālās vai starptautiskās.

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.

	KATEGORIJA	TĒMA	Nr.	UZDEVUMU APRAKSTS
			1.2.7	Saprast starpību starp pieslēgšanos pie VeIS sistēmas no ierīces/datora, kas atrodas aizsargātā tīklā, vai no ierīces, kas nav aizsargātā tīklā.
			1.2.8	Izprast atšķirību starp dažāda veida HIS, piemēram: mantota sistēma, datorizētas sistēmas, reģistri.
	2. Piesardzības pasākumi	*2.1. Konfidencialitāte*	2.1.1	Aprakstīt veselības aprūpes darbinieka pienākumus attiecībā uz pacienta datu konfidencialitāti VeIS ietvaros: piekļūt pacienta informācijai tikai tad, ja nepieciešams; piekļuve tikai tām sadaļām, par kurām nepieciešams uzzināt; piekļuve tikai tai informācijai, kuru ir atļauts uzzināt; izpratne par personīgās atbildības jēdzienu.
			2.1.2	Izprast pacienta tiesības ievērot datu sensitivitāti (netieši vai skaidri izteiktu) attiecībā uz pacienta, ģimenes locekļu un citu personu datiem. Cienīt pacienta tiesības neatklāt/nezināt informāciju.
			2.1.3	Saprast, ka vietējā likumdošana dod pacientam tiesības pārskatīt un slēpt savus ierakstus.[1]
			2.1.4	Saprast atšķirību starp vispārēju pieeju sistēmai un tiesībām apskatīt un izmantot konkrētu informāciju.
			2.1.5	Saprast valsts prasības attiecībā uz informācijas ziņošanu par pacientu specifiskiem datiem, kā arī noteikumus un ierobežojumus, kas saistīti ar informācijas par sabiedrības veselību un saslimšanām pārvaldīšanu.
			2.1.6	Izprotiet, ka ar veselības aprūpes informācijas sistēmu ir saistīti zināmi konfidencialitātes riski, piemēram, ar pacientu saistīto datu izpaušana trešajām personām.

[1] Data Protection Act, Freedom of Information Act.

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.

	KATEGORIJA	TĒMA	Nr.	UZDEVUMU APRAKSTS
			2.1.7	Izprotiet, ka veselības aprūpes informācijas sistēmas piekļuves noteikumi ir, lai aizsargātu pacientu personas datus, un piekļuve informācijas sistēmai bieži ir balstīta uz veselības aprūpes darbinieku lomām, pienākumiem un atbildību.
		2.2. Drošība	2.2.1	Aprakstiet galvenos veselības aprūpes informācijas sistēmas drošības principus, piemēram, informētība par sistēmas ievainojamību, oficiāla vienošanās par organizatorisko drošības politiku.
			2.2.2	Izprotiet, ka organizatoriskās drošības politikai ir personīga, profesionāla un organizatoriska ietekme.
			2.2.3	Aprakstiet galvenos veselības aprūpes informācijas sistēmas draudus, piemēram, neatļauta vai nesankcionēta piekļuve, datu zudumi, ļaunprātīgi bojājumi vai to pārsūtīšana trešajām personām u.c.
			2.2.4	Aprakstiet aizsardzības pasākumus veselības aprūpes informācijas sistēmas drošībai.
			2.2.5	Izprotiet pienākumu ziņot par drošības pārkāpumiem un draudiem, piemēram, uzdošanos par citu lietotāju, ļaunprātīgu uzbrukumu, vīrusiem vai tārpiem u.c.
			2.2.6	Izprotiet, kāpēc ir svarīga datu uzglabāšana un rezerves kopiju veidošana?
	3. Lietošanas prasmes	*3.1. Navigācija*	3.1.1	Izprotiet, ka veselības aprūpes informācijas sistēma var uzglabāt pacientu datus, kā arī medicīnisko statistiku.
			3.1.2	Atpazīt, ja viens un tas pats indivīds sistēmā ir ierakstīts divas reizes, un saprast pilnvaras, lai vienādus ierakstus apvienotu.
			3.1.3	Uzziniet par informācijas pieejamību veselības aprūpes informācijas sistēmā https://eveseliba.gov.lv.

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.

	KATEGORIJA	TĒMA	Nr.	UZDEVUMU APRAKSTS
			3.1.4	Izprotiet, ka ir iespējams izvēlēties un skatīt pacientu ierakstu kopu, pamatojoties uz dažiem kopīgiem kritērijiem.
			3.1.5	Precīzi ierakstīt pacienta informāciju.
			3.1.6	Atpazīt dažādus datu ievades režīmus (automatizētus).
			3.1.7	Atpazīt dažādus datu ievades režīmus (automatizētus).
		3.2. Lēmumu pieņemšanas atbalsts	3.2.1.	Izprast pieejamo informāciju lēmumu pieņemšanas atbalstam: brīdinājums, atgādinājums, apstiprinājuma pārbaudes u.c.
			3.2.2.	Saprast personīgo atbildību un pilnvaru ignorēt sistēmas pārbaudes ziņojumus.
		3.3. Rezultātu pārskati	3.3.1.	Prast izveidot pārskatus: pacientu sarakstus, aprūpes vienību skaitīšana, pacientu pieraksti/vizītes.
			3.3.2.	Izveidot ikdienas pārskatu, balstoties uz konkrētu vaicājumu, piemēram, pacientu rezultātiem.
			3.3.3.	Izvēlēties pārskata veidu no iepriekš pastāvoša pārskata veida/veidnes.
			3.3.4.	Izvēlēties un apskatīt noteikta veida informāciju, piemēram, rentgenu, EKG, CT-scan, asins analīžu rezultātus.
			3.3.5.	Prast izdrukāt pārskatus, ievērojot drošības principus.
			3.3.6.	Prast pārsūtīt VeIS datus un pārskatus, ievērojot drošības principus.
	4. Noteikumi un procedūras	*4.1. Principi*	4.1.1.	Izprast, ka pacienta ieraksts ir juridisks dokuments, un informāciju nedrīkst dzēst.

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.

	KATEGORIJA	TĒMA	Nr.	UZDEVUMU APRAKSTS
			4.1.2.	Saprast, ka informāciju var pievienot un precizēt, bet ne mainīt.
			4.1.3	Saprast, kam ir tiesības izveidot jaunus ierakstus, piemēram, dzimšanas/ārkārtas/pagaidu ierakstus.
			4.1.4	Saprast VIS audita liecības un to nozīmi.

2. modulis

	KATEGORIJA	TĒMA	Nr.	UZDEVUMU APRAKSTS
	5. Vispārēji IT drošības jēdzieni		5.1.1.	Uzziniet par informācijas tehnoloģiju un interneta priekšrocībām un trūkumiem (riskiem).
			5.1.2.	Uzziniet par kibernoziegumiem, finanšu krāpšanu, nelikumīgām darbībām, datorvīrusiem, urķis, avatāriem, spiegprogrammatūru, tastatūras spiegu, Trojas zirgu, viltus ziņām un slēptu reklāmu.
			5.1.3.	Izprotiet terminu "sociālā inženierija" un ar to saistītās sekas, piemēram: neatļauta piekļuve datoram un ierīcēm, neatļauta informācijas vākšana un krāpšana. Nosakiet sociālās inženierijas metodes, piemēram, tālruņa zvanus, pikšķerēšana, skatīšanās pāri plecam, simulēšana un spiegprogrammatūra.
			5.1.4.	Izprotiet terminus identitāte un identitātes zādzība. Nosakiet identitātes zādzības metodes, piemēram, informāciju atgūšana, datsmelšana un identitātes viltošana. Zināt dažādus veidus, kā ļaunprogrammatūra varētu iekļūt ierīcē.
			5.1.5.	Uzziniet par identitātes un personas datu zādzību iemesliem un sekām darba vietā un internetā (krāpnieciskas informācija izmantošana, informācijas zaudēšanas draudi, kaitniecība). Uzziniet par draudiem, kas saistīti ar personas datu izpaušanu.
			5.1.6.	Uzziniet dažādus veidus, kā varētu tikt nozagta personas identitāte, piemēram, telefona sarunu

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.

	KATEGORIJA	TĒMA	Nr.	UZDEVUMU APRAKSTS
				noklausīšanās, tiešsaistes metodes (e-pasts, sociālie tīkli, tūlītējā ziņojumapmaiņa), datsmelšana, skatīšanās pāri plecam, informācijas atgūšana, dzēstas informācijas atjaunošana).
			5.1.7.	Esiet informēts par privātuma aizsardzības tiesību aktiem.
			5.1.8.	Zināt par organizatoriskajiem datu pārvaldības noteikumiem, datu privātuma principiem, konfidencialitāti.
			5.1.9.	Zināt, ar ko ir jāsazinās, ja atklājat nepiedienīga rakstura informāciju par sevi vai jūsu organizāciju tīmekļa lapās vai sociālajā tīklā. Zināt, ar ko jāsazinās, ja saņemat pikšķerēšanas e-pasta ziņojumus.
			5.1.10.	Izprotiet personīgo atbildību par savām darbībām internetā: nepublicējiet informāciju bez atļaujas, komentārus rakstiet atbildīgi, nelegāli nelejupielādējiet mūziku, filmas utt.).
			5.1.11.	Uzziniet par tīkla etiķeti un un citiem pamata rīcības kodeksiem kibertelpā.
	6. Darba vietas drošības politika uzņēmumā		6.1.1.	Iepazīstieties ar uzņēmuma drošības politikas vadlīnijām: ierīču lietošana darba vietā (uzziniet par iespējām izmantot darba vietas ierīces personīgām vajadzībām). Uzziniet par uzņēmuma politiku attiecībā uz ierīču nešanu uz mājām.
			6.1.2.	Uzziniet par drukāto dokumentu aizsardzību, glabāšanu un pārvaldīšanu. Uzziniet, ka svarīgus drukātos dokumentus ar konfidenciāliem datiem nevar atstāt bez uzraudzības vai aizmirst izņemt no printera. Uzziniet par sekām, ja šos dokumentus izlasītu vai nozagtu nepilnvarotas personas
			6.1.3.	Uzziniet par uzņēmuma drošības politiku par personīgo ierīču izmantošanai darba vietā (piemēram, viedtālruņu, planšetdatoru un USB zibatmiņu), kā arī par šo ierīču savienošanu ar internetu un iespējamām sekām.

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.

6.1.4. Uzziniet par drošības politiku lietotņu instalēšanai uzņēmuma datoros, viedtālruņos un planšetdatoros (izprotiet terminu lietojumprogrammu atļaujas un ziniet par sekām, instalējot lietotnes no nezināmiem avotiem) un ierīču savienošanai ar publiskiem interneta tīkliem. Uzziniet par iespējamiem draudiem un sekām, ja kāds uzlauž uzņēmuma ierīci vai tā tiek inficēta ar vīrusu (personas datu zādzība, neatļautas informācijas glabāšana bez apstiprinājuma, slēptās maksas vai atrašanās vietas izsekošana).

6.1.5. Izprotiet lietotāja autorizācijas mērķi un nozīmi, pieslēdzoties kādai ierīcei vai informācijas sistēmai.

6.1.6. Nosakiet pasākumus, lai novērstu neatļautu piekļuvi tādiem datiem kā: lietotājvārds un parole, PIN kods, mikroshēmas karte, daudzfaktoru autentifikācija, vienreizējā parole un biometrijas dati.

Izprotiet, ka tīkla kontam vajadzētu piekļūt, izmantojot lietotājvārdu un paroli, un tas ir bloķēts vai atslēgts, kad netiek lietots.

6.1.7. Atpazīstiet veidus, kā nodrošināt drošu fizisko vidi un aizsargāt datoru un citas ierīces no datu zādzības, piemēram: neatstāt bez uzraudzības, reģistrēt iekārtu atrašanās vietu un informāciju, izmantot kabeļu slēdzenes, piekļuves kontrole u.c.

6.1.8. Nodrošināt, lai nepiederošām personām nebūtu iespējams redzēt darbinieku ekrānus (katram lietotājam vajadzētu aizsargāt savu ekrānu no novērošanas ar mērķi izgūt informāciju).

6.1.9. Atpazīstiet drošas paroles veidošanas principus, piemēram: atbilstošs garums, dažādi burti, cipari un īpašās rakstzīmes, dažādas paroles dažādiem pakalopjumiem, nedalieties ar citiem un regulāri tāsmainīt.

Izprotiet paroļu pārvaldnieka funkcijas un ierobežojumus.

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.

6.1.10. Izprotiet, ka lietotāja autorizācija ierīcēs, programmās un informācijas sistēmās tiek izmantota konkrētas personas identificēšanai, un piekļuves datus nedrīkst atklāt kolēģiem vai citām personām. Uzziniet par sekām, ja nepilnvarota persona autorizējas, izmantojot svešus piekļuves datus.

6.1.11. Izprotiet, ka jebkuras programmatūras instalēšana uzņēmuma ierīcēs ir atļauta tikai atbildīgajai personai (piemēram, IT administratoram) vai trešās puses uzņēmumam, ar kuru ir vienošanās par IT pārraudzību.

6.1.12. Zināt par nepieciešamību veikt regulāru ierīču pārbaudi un personas, kurām jāveic šī pārbaude. Saprast sekas, ja nepiederoša persona pieslēdzas vai piekļūst uzņēmumu ierīcēm.

6.1.13. Uzziniet, kad un kā ļaunprātīga programmatūra var iekļūt datorsistēmā. Izprotiet par ļaunprātīgo datu izplatīšanos draudiem ārējos datu nesējos.

6.1.14. Zināt par ētiku darba vietā: atšķirt personas datus no uzņēmējdarbības vai uzņēmuma datiem. Zināt, kādus datus var glabāt uzņēmumu ierīcē, un par neatbilstīgu datu saglabāšanas sekām. Saprast, ka uzņēmumu un klientu dati nevar tikt nodoti trešajām personām.

6.1.15. Uzziniet par tiešsaistes sadarbības iespējām, piemēram, dokumentu, printeru un darbvirsmu koplietošanu ar kolēģiem. Uzziniet par datu kontroli, iespējamiem draudiem zaudēt privātumu un, kā dokumentus koplietot droši. Izprotiet, kāda veida dati var tikt kopīgoti ar citiem lietotājiem, neatklājot konfidenciālu informāciju.

6.1.16. Izprotiet, ar kādu mērķi pastāvīgi no atmiņas diskiem tiek dzēsti dati un, kāpēc neizmantotie diski un drukātie dokumenti tiek iznīcināti. Izprotiet atšķirību starp datu dzēšanu un pastāvīgu dzēšanu no ierīcēm. Uzziniet, ka dzēstie dati var tikt atjaunoti no atmiņas diskiem. Uzziniet, ka neizmantoti, kā arī bojāti atmiņas diski vai ierīces ar atmiņas diskiem, piemēram, viedtālruņi, ir jāiznīcina.

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.

7. Datora drošība	7.1.1.	Izprotiet, cik svarīgi ir regulāri atjaunināt programmatūru, piemēram, pretvīrusu, tīmekļa pārlūkprogrammas, spraudņus, lietojumprogrammas, operētājsistēmu.
	7.1.2.	Izprotiet, kā darbojas pretvīrusu programmatūra un tās ierobežojumus. Pretvīrusu programmatūra ir jāinstalē visos datoros un ierīcēs, un uzziniet, ka nevienā gadījumā nav atļauts pretvīrusu programmatūru atspējot.
	7.1.3.	Zināt, kā iestatīt paroles dokumentiem un failu arhīviem.
	7.1.4.	Prast atpazīt galvenās pazīmes, ja ierīce ir inficēta ar vīrusu. Zināt, kas jādara un kādā secībā, ja Jums ir aizdomas, ka datorsistēma ir inficēta.
	7.1.5.	Izprotiet datu rezerves kopiju veidošanas mērķi un priekšrocības, kā arī to, cik nozīmi gadījumos, kad dati no datoriem un citām ierīcēm tiek zaudēti.
8. Drošība internetā	8.1.1.	Zināt, kā droši pārlūkot internetu. Spēt izveidot drošu savienojumu ar e-pakalpojumiem un drošu vidi. Zināt, kā atgūt zaudētās paroles.
	8.1.2.	Uzziniet par sīkdatnēm, paroļu saglabāšanu datorā vai pārlūkprogrammā.
	8.1.3.	Nosakiet vispārpieņemtas pikšķerēšanas iezīmes, piemēram, izmantot likumīgu organizāciju nosaukumus un citu personu vārdus, logotipus, zīmolus, kā arī nepatiesas saites uz tīmekļa vietnēm, veicinot personas datu izpaušanu. Uzziniet, ar ko sazināties, ja saņemat e-pasta ziņojumu no kādas personas, kas veic pikšķerēšanu. Uzziniet par iespējamiem draudiem, atverot šādu ziņojumu pielikumus, kas var saturēt makro vai izpildāmo failu.
	8.1.4.	Spējat identificēt viltotas vietnes, kuras varētu atvērt, noklikšķinot uz saites e-pastā, sociālajos plašsaziņas līdzekļos utt. Uzziniet par sekām, atklājot konfidenciālus datus par sevi vai uzņēmumu. Uzziniet, ar ko sazināties, ja pamanāt viltotu vietni.

Šis projekts tiek finansēts ar Eiropas Komisijas atbalstu.
Šī publikācija [ziņojums] atspoguļo tikai tās autoru viedokli, un Eiropas Komisija nekādā veidā neuzņemas atbildību par šeit ietvertās informācijas tālāku izmantošanu.