Rokasgrāmata profesionālās izglītības un apmācības sniedzējiem

BDA

mathemagenesis

MUĞLA SITKI KOÇMAN ÜNİVERSİTESİ

eLearning software

EduVibes

WITTENBORG University of Applied Sciences

2024

Co-funded by the European Union

GOOD START

Good Digital Hygiene for Startups

Projekta Nr: 2022-1-LV01-KA220-VET-000086725 | Project title: Good Digital Hygiene for Startups

Saturs

1. Modulis – Digitālā higiēna PIA profesionāļiem

1.daļa – Digitālās higiēnas nozīme PIA izglītībā

Digitālā higiēna un kiberdrošība

Digitālā higiēna ir iemaņas un paradumi, ko indivīdi piemēro, lai nodrošinātu savu privātumu, drošību un kopējo labklājību tiešsaistē. Tā ir plašs proaktīvu rīcību un pasākumu kopums ar mērķi aizsargāt personisko informāciju, novērst tiešsaistes draudus un mazināt ar digitālajām aktivitātēm saistītos draudus. Digitālās higiēnas praktiskie piemēri ir spēcīgu paroļu lietošana, divu faktoru autentifikācijas izmantošana, programmatūras regulāra atjaunināšana, uzmanīga dalīšanās ar personisko informāciju tiešsaistē un digitālās pēdas uzraudzība. Digitālā higiēna ir cieši saistīta ar citu jēdzienu,- kiberdrošība. Bieži digitālo higiēnu uzskata par indivīda pārziņā esošu kiberdrošības proaktīvu elementu.

Kiberdrošība ir specializēta joma, kas rūpējas par datorsistēmu, tīklu un datu aizsardzību no neautorizētas piekļuves, kiberuzbrukumu un citu drošības pārkāpumu novēršanu. Tā iekļauj tehnisku paņēmienu, drošības protokolu un aizsardzības stratēģiju ieviešanu, lai padarītu drošākus digitālos aktīvus un mazinātu kiberdraudu izraisītos potenciālos riskus. Cilvēki, kas strādā kiberdrošības jomā, bieži identificē sistēmu vājās vietas, izstrādā drošības risinājumus, uzrauga aizdomīgas aktivitātes un reaģē un drošības incidentiem, lai nodrošinātu informācijas un resursus integritāti, konfidencialitāti un pieejamību. Tādēļ kiberdrošības aktivitātes bieži veic profesionāļi, bet digitālā higiēna ir katra indivīda atbildība.

Digitālā higiēna PIA organizācijās

Dažādas organizācijas sagaida, ka viņu darbinieku sekos dažādiem pamatnoteikumiem, kas nodrošina digitālās higiēnas noteikumu un labās prakses ievērošanu. Profesionālās izglītības un apmācību (PIA, *angliski VET*) organizācijas piemēro vispārējus noteikumus, kas ir spēkā visām organizācijām, kas strādā ar cilvēkiem un viņu personas informāciju un ar pakalpojumiem un produktiem, kas ir viņu īpašums un kurus izstrādā, glabā un izplata digitālajā vidē. Taču šīm organizācija ir arī īpaši izaicinājumi, kas saistīti ar piedāvātā pakalpojuma veidu un mērķa klienta īpašo dabu. Izglītotāji bieži nonāk situācijā, kur viņiem ir jāsniedz papildu palīdzība saviem klientiem. Tas nozīmē, ka viņiem jākļūst par digitālās higiēnas aģentiem veicot apmācības jeb sniedzot iecerēto pamata pakalpojumu.

Ir vairāki iemesli, kāpēc digitālā higiēna ir ļoti nozīmīga tieši PIA organizācijām:

- **Sensitīvas informācija aizsardzība**

Darot savu darbu PIA organizācijas bieži apstrādā sensitīvu informāciju, ieskaitot datus par studentiem, informāciju par mācību progresu un finanšu datus. Šī informācija var būt kritiski svarīga organizācijai, lai veiktu mācību analītiku vai novērtētu klientam sniegto pakalpojumu kvalitāti. Laba digitālās higiēnas prakse palīdz nodrošināt šo informāciju no neautorizētas piekļuves, datu pārkāpumiem, kiberdraudiem un stiprina sensitīvu datu konfidencialitāti un integritāti.

- **Organizācijas reputācijas noturēšana**

Neuzmanīgi apstrādājot tām uzticētos datus, PIA organizācijas var neatgriezeniski sabojāt klientu un partneru uzskatus par tām. Datu pārkāpumi vai drošības incidenti var nozīmīgi bojāt PIA organizācijas reputāciju. Uzliekot augstu prioritāti digitālās higiēnas ieradumiem, organizācijas demonstrē drošības, uzticamības un profesionālisma saistību uzņemšanos, palielinot savu reputāciju ieinteresēto pušu, to skaitā studentu, vecāku, darba devēju un regulējošo institūciju acīs.

- **Atbilstība regulējumiem**

Atkarībā no darba specifikas un veidā, tās sazinās ar klientiem, PIA organizācijām ir jāievēro dažādi noteikumi un jānodrošina atbilstības prasības, kas saistītas ar datu aizsardzību, privātumu un kiberdrošību. Digitālās higiēnas labās prakses ievērošana palīdz nodrošināt atbilstību likumiem un noteikumiem un ļauj samazināt riskus, kas saistīti ar soda naudu izmaksām un juridiskās atbildības uzņemšanos neatbilstību gadījumos.

- **Atbalsts mācībām un mācīšanai**

Digitālās tehnoloģijas spēlē nozīmīgu lomu mūsdienu izglītībā, atbalstot tiešsaistes mācības, sadarbības projektus un digitālo vērtēšanu. Šīs tehnoloģijas izmanto, lai izstrādātu, pārvaldību un izplatītu mācību materiālus, organizāciju mācību vides, pārvaldību mācību dalībnieku iesaisti tajās vai analizētu datus par mācību procesu. Uzturot drošu un uzticamu digitālo infrastruktūru, PIA organizācijas var nodrošināt viengabala mācību pieredzi studentiem un mācībspēkiem, veicinot inovācijas, radošumu un iesaisti mācīšanas un mācīšanās aktivitātēs.

- **Kiberdrošības risku mazināšana**

Izglītības sektors var kļūt par mērķi kibernoziedzniekiem, kuri vēlas izmantot digitālo sistēmu un tīklu vājās vietas vai studentu un treneru, kuri nav pieraduši mācībām digitālajā vidē, zināšanu un prasmju trūkumu. Digitālās higiēnas prakses ieviešana samazina kiberdrošības riskus, ieskaitot inficēšanos ar ļaunprogrammatūru, pikšķerēšanas uzbrukumus, izspiedējvīrusu draudus, neautorizētu piekļuvi izglītības resursiem, tādējādi nodrošinot izglītības pakalpojumu un darbību turpināšanu.

- **Atbildīgas digitālās pilsonības veicināšana**

Dažiem procesa dalībniekiem šī var būt pirmā iespēja piedalīties mācībās, kas tiek nodrošinātas digitālajā vidē vai izmanto digitālo vidi, lai izstrādātu, pārvaldītu un izplatītu mācību materiālus, vadītu zināšanu pārnesi un

veidotu komunikāciju ar citiem dalībniekiem, izmantojot digitālos rīkus, vai veiktu administratīvas darbības mācību laikā. PIA organizāciju pienākums ir izglītot studentus un darbiniekus, kas iesaistīti mācībās, par drošu un atbildīgu digitālo praksi. Integrējot digitālās higiēnas mācības PIA mācību programmās, organizācijas stiprina mācību dalībnieku zināšanas, prasmes un attieksmi, kas vajadzīgas, lai orientētos digitālajā pasaulē, pasargātu savu tiešsaistes identitāti un sniegtu ieguldījumu digitālajā sabiedrībā.

- **Sagatavošana nākotnes karjerai**

Mūsdienu digitālajā laikmetā digitālā pratība un kiberdrošības izpratne ir svarīgas prasmes indivīdiem, kas uzsāk darba attiecības. Pat, ja apgūt prasmes, kas saistītas ar digitālo higiēnu, nav studenta pamata mērķis, dalība mācībās var sniegt iespējas uzlabot šīs prasmes, kas noderēs nākotnē. Treneriem un mācību organizatoriem jāapzinās, ka iespējams būs jāvelta daļa no mācību laika un resursiem tieši šim mērķim. Veicinot digitālās higiēnas iemaņas, PIA organizācijas nodrošina studentus ar pamata zināšanās un prasmēm, kas vajadzīgas, lai orientētos digitālajos izaicinājumus viņu nākotnes karjerā neatkarīgi no tā, vai tās būs tradicionālajās vai digitālajās nozarēs. Tas pats attiecas uz treneriem, kas piedaloties mācībās, izmantojot digitālo vidi un rīkus droši un atbildīgi, padara savas mācību metodes modernas un iespējams saskatīs jaunas iespējas savā karjerā.

Kopumā digitālā higiēna ir svarīga PIA organizācijām gan visas organizācijas, gan individuāla darbinieka, gan klienta līmenī, lai aizsargātu sensitīvu informāciju, uzturētu organizācijas reputāciju, nodrošinātu atbilstību likumiem, atbalstītu mācīšanos un mācīšanu, mazinātu kiberdrošības riskus, veicinātu atbildīgu digitālo pilsonību un sagatavotu studentus un zināmā mērā arī viņu trenerus un citus organizācijas darbiniekus veiksmīgai pastāvēšanai digitālajā pasaulē. Uzliekot augstu prioritāti digitālajai higiēnai, PIA organizācijas veido drošu un veicinošu mācību vidi un iespējo mācību dalībnieku izaugsmi digitālajā laikmetā.

2.daļa – Prasmes un prasības PIA treneriem un mācībspēkiem

Lomas un atbildības PIA organizācijās

Sāksim ar to, kādas lomas var būt iesaistītas PIA mācībās, kurām būtu jāapzinās digitālās higiēnas problēmas un jāpiemīt atbilstošām prasmēm. Atkarībā no situācijas vadot un piedaloties mācībās, kas norisinās digitālā vidē un izmanto digitālos rīkus, PIA treneriem un mācībspēkiem var iznākt saskarties ar dažādu pienākumu sadalījumu, kurus veic procesa dalībnieki. Tādēļ ieviešos un pārvaldot digitālo higiēnu PIA organizācijā var būt nepieciešama dažādu pušu lomu un pienākumu koordinācija un sadarbība to izpildē. Treneri var būt situācijā, kur viņus atbalsta pilnvērtīga IT komanda, kas rūpējas par mācību tehniskajiem aspektiem, bet tik pat labi viņiem var nākties paļauties uz pašu prasmēm un zināšanām. Šī iemesla dēļ prasmes un prasības pret PIA treneriem un mācībspēkiem var atšķirties atkarībā no organizācijas, kuras sastāvā tie ir.

Ir vairākas tipiskas lomas un atbildības indivīdiem, kas ir iesaistītas mācību procesā mūsdienu digitālajā vidē, un katram no tiem ir savi pienākumi un vēlamās prasmes:

- **Galvenais informācijas direktors (***angliski Chief Information Officer (CIO)***) vai Galvenais tehnoloģiju direktors (***angliski Chief Technology Officer (CTO)***)**

Organizācijas atbildīgais par informāciju vai tehnoloģijām pārsvarā atbild par organizācijas digitālās higiēnas stratēģiju, politiku un procedūrām. Viņi uzstāda organizācijas mērķus, paturot prātā digitālās higiēnas un kiberdrošības jautājumus. Viņu pienākumos ietilpst nodrošināt digitālās higiēnas pūliņu saskaņošanu ar organizācijas kopējiem IT un drošības mērķiem, piešķirt resursus un budžetu digitālās higiēnas iniciatīvām un kiberdrošības pasākumiem un nodrošināt vadība un atbalstu IT un drošības komandām, kas ievieš digitālās higiēnas praksi.

- **IT drošības menedžeris vai kiberdrošības menedžeris**

Dažās organizācijās var būt īpaša pozīcija IT drošības menedžerim vai kiberdrošības menedžerim vai kādam, kas nodrošina šo lomu kā daļu no darba pienākumiem. Šāda loma izstrādātu un ieviestu kiberdrošības kontroli, drošības pasākumus un risku vadības pasākumus, lai aizsargātu PIA sistēmas, tīklus un datus. Viņi arī veiktu regulārus drošības izvērtējumus, auditus un ievainojamības pārbaudes, lai identificētu un mazinātu potenciālos draudus un ievainojamības, uzraudzītu drošības incidentus un reaģētu uz kiberdrošības incidentiem un koordinētu incidentu atbildes aktivitātes. Dažreiz šī loma izstrādā un nodrošina kiberdrošības mācības un izglītības programmas darbiniekiem, kas liek tiem uzņemties PIA trenera lomu. Dažreiz viņus kā ekspertus var arī aicināt mācīt studentus ārpus pašu organizācijas, lai veicinātu digitālas higiēnas labo praksi.

- **IT administrators vai sistēmu administrators**

IT administratori ir atbildīgi par IT infrastruktūras pārvaldību organizācijā un var veikt daļu no uzdevumiem, lai atbalstītu PIA trenerus, dažreiz fonā un nemanot. Viņu pienākumos ietilpst PIA sistēmu, serveru un tīklu infrastruktūras uzturēšana un administrēšana, ievērojot digitālās higiēnas standartus un labo praksi; lietotāju kontu un pieejas tiesību pārvaldība, lai nodrošinātu drošu pieeju PIA resursiem un datiem; drošības programmatūras instalēšana, konfigurēšana un atjaunināšana, lai izvairītos no ievainojamības riskiem, ar kuriem var sastapties izmantojot digitālos rīkus un veicot mācību darbības, piemēram, daloties ar mācību materiāliem vai komunicējot ar mācību dalībniekiem. Viņi arī ir atbildīgi par sistēmas žurnālu, aizdomīgu aktivitāšu trauksmes signālu, neautorizētas piekļuves mēģinājumu un drošības pārkāpumu uzraudzību.

- **Datu aizsardzības oficieris vai privātuma oficieris**

Datu aizsardzības oficieri spēlē nozīmīgu lomu PIA, jo eksistē noteikumi un regulas nacionālā un starptautiskā līmenī, kas pieprasa uzmanību no PIA organizāciju puses, lai pārvaldītu mācību dalībnieku sensitīvos datus. Šī loma nodrošina atbilstību datu aizsardzības regulām un privātuma līkumiem, kas nosaka personas datu ievākšanu, lietošanu un uzglabāšanu PIA vidē; izstrādā un uztur datu aizsardzības politiku, procedūras un dokumentāciju, tajā skaitā datu aizsardzības ietekmes novērtējumus un privātuma paziņojumus; apstrādā datu subjektu pieprasījumus, privātuma sūdzības un pieprasījumu, kas saistīti ar datu aizsardzību un privātuma praksi; sadarbojas ar IT un juridiskajām komandām, lai risinātu datu drošības incidentus, pārkāpumus un privātuma pārkāpumus.

- **Izglītības tehnologs vai mācību dizainers**

Ja iepriekš minētās lomas var sastapt jebkurā organizācijā, tad izglītības tehnologa vai mācību dizaina speciālista lomas ir tieši saistītas ar mācībām un izglītību, kas tiek veikta organizācijā. Viņu pienākumos ietilpst digitālās higiēnas principu un prakses integrēšana ar PIA mācību programmām, instrukcijām un mācību aktivitātēm; apmācības un atbalsta sniegšana treneriem un izglītotājiem par digitālās higiēnas mācību iekļaušanu mācību praksē, tādu mācību tehnoloģiju rīku un resursu izvērtēšana un ieteikšana, kas piešķir augstāku prioritāti PIA studentu drošības, privātuma un piekļuves jautājumu risināšanai.

- **Gala lietotāji (darbinieki un studenti)**

Pēdējo lomu bieži sadala divās grupās, kurām ir līdzīga atbildība par digitālo higiēnu. No gala lietotājiem sagaida, ka viņi sekos digitālās higiēnas politikai, vadlīnijām un labai praksei, lietojot PIA sistēmas, ierīces un tiešsaistes resursus. Organizācijas mācībspēkiem var būt organizācijas uzstādīts pienākums piedalīties mācībās par administratīvajām aktivitātēm, kas jāveic noteiktā veidā saskaņā ar organizācijas noteikumiem un politiku. Cita starpā viņu pienākums var būt piedalīties kiberdrošības apmācībās un izglītības pasākumos, lai uzlabotu savu izpratni par digitālajiem riskiem un pienākumiem ziņot par drošības incidentiem, aizdomīgām aktivitātēm un bažām par kiberdrošību atbilstošajam IT vai drošības speciālistam, lai tas veiktu

izmeklēšanu un rastu risinājumu. Bet PIA treneriem ir jāapzinās arī sava loma kā padomdevējiem studentiem, kuriem var būt nepieciešama palīdzība lietojot digitālo vidi, kas viņiem nav pazīstama, mācību laikā.

Katrs cilvēks PIA organizācijā vienlaicīgi var pildīt vairākas lomas mācību laikā vai arī viņš var koncentrēties tikai uz dažiem pienākumiem. Tomēr, skaidri definējot lomas un atbildības indivīdiem, kas ir iesaistīti digitālās higiēnas ieviešanā un pārvaldībā PIA organizācijās, institūcijas var efektīvi sadarboties, lai iedzīvinātu kiberdrošības apziņas kultūru, veicināt digitālās higiēnas praksi un aizsargāt PIA resursu un datu konfidencionalitāti, integritāti un pieejamību. Taču organizācijām būs vajadzīgs, lai šiem indivīdiem piemistu noteiktas prasmes un zināšanas, lai iesaistītos iepriekš minētajā praksē.

Digitālo prasmju ietvari

Ir izveidoti gatavi digitālo prasmju ietvari, kas apraksta prasmju kopu, kurai jāpiemīt tiem cilvēkiem, kas iesaistīti dažādās aktivitātēs digitālajā vidē. Daži no tiem iekļauj vispārējas digitālās prasmes, bet citi ir vairāk specifiski kiberdrošības un digitālās higiēnas problēmu risināšanai. Turpmāk aprakstīti noderīgi ietvari, kas ļauj identificēt vēlamās digitālās higiēnas prasmes PIA treneriem un mācībspēkiem un iespējamās mācību vajadzības mācību dalībniekiem, kas piedalās izglītībā digitālajā vidē.

- **Digitālo kompetenču ietvars pilsoņiem (***angliski Digital Competence Framework for Citizens (DigComp))* **[1]**

DigComp 2.2 ietvars, ko izstrādājusi Eiropas Komisija, ir jaunākā Digitālo kompetenču ietvara pilsoņiem versija. Tas definē galvenos elementus digitālajām kompetencēm piecās jomās: informācijas un datu pratība, komunikācija un sadarbība, digitālā satura radīšana, drošība un problēmu risināšana. Katra joma ir sīkāk sadalīta specifiskās kompetencēs, kas apraksta prasmes un zināšanas, kas vajadzīgas, lai būtu pratīgs digitālajā vidē.

Šis ietvars kalpo kā vadlīnijas indivīdiem, lai novērtētu un uzlabotu viņu digitālās prasmes, un mācību nodrošinātājiem un politikas izstrādātājiem, lai izstrādātu mācību plānus un politiku, kas atbalsta digitālo izglītību un apmācību. DigComp 2.2 arī ievieš prasmju līmeņus un to lietošanas piemērus, padarot to praktiski noderīgu dažādās izglītības un profesionālajās situācijās. Ietvars uzsver efektīvas un kritiskas darbības nozīmi digitālajā sabiedrībā.

- **Eiropas e-kompetenču ietvars** *(angliski European e-Competence Framework (E-CF))* **[2]**

Eiropas e-kompetenču ietvars (e-CF) ir standartizēts ietvars, kas apraksta kompetences, prasmes un prasmju līmeņus informāciju un komunikāciju tehnoloģiju (IKT) profesionāļiem, kas izstrādāts, lai atbalstītu IKT profesionāļu izaugsmi un mobilitāti. Ietvars sastāv no piecām kompetenču jomām, kas saistītas ar IKT, piemēram, plānošana, izstrāde, norise, iespējošana un vadīšana. Tas iekļauj kopā 41 kompetenci un arī

prasmju līmeņus, kas apraksta zināšanas, prasmes un autonomijas pakāpi katram līmenim, sākot no pamata līdz pat ekspertam. Tas iekļauj arī zināšanu un prasmju, kas saistītas ar kompetencēm, piemērus.

E-CF ir domāts, lai palīdzētu organizācijām cilvēkresursu vadības menedžeriem, treneriem un izglītotājiem izstrādāt darba lomas un karjeras ceļus IKT profesionāļiem, uzlabotu darbaspēka pārvaldību un veicinātu IKT sektora profesionālo attīstību. Tas arī kalpo kā rīks politikas izstrādē, izglītības un apmācību saskaņošana Eiropas digitālajā tirgū.

- **Eiropas kiberdrošības prasmju ietvars** *(angliski European Cybersecurity Skills Framework* **(ECSF) [3]**

Eiropas kiberdrošības prasmju ietvars (ECSF) ir izstrādāts, lai harmonizētu un standartizētu kiberdrošības prasmes, lomas un kompetences Eiropā. Tas kalpo kā pamatstruktūra kiberdrošības prasmju attīstībā un novērtēšanā ar mērķi pievērst uzmanību kiberdrošības prasmju trūkumam un uzlabot kiberdrošības situāciju organizācijās un nācijās. ECSF iedala kiberdrošības prasmes vairākās jomās, detalizējot īpašās lomas un kompetences, kas nepieciešamas kiberdrošības laukā. Tas uzskaite pamata kiberdrošības lomas, kas tipiski nepieciešamas organizācijām, specifiskas prasmes un spējas, kas vajadzīgas, lai efektīvi pildītu šīs lomas, un prasmju jeb ekspertīzes līmeņus no iesācēja līdz ekspertam, kas vajadzīgas katrai kompetencei.

Ietvars ir noderīgs dažādiem interesentiem, ieskaitot izglītības iestādes, uzņēmumus un politikas veidotājus, lai izstrādātu mācību plānus, apmācību programmas un karjeras ceļus kiberdrošībā. Tas atbalsta skaidri karjeras struktūru izveidi kiberdrošībā, padarot prasmju iztrūkuma identificēšanu un efektīvu novēršanu vieglāku.

- **Digitālo kompetenču ietvars izglītotājiem** *(angliski Digital Competence Framework for Educators (DigCompEdu)* **[4]**

DigCompEdu ietvars apraksta digitālo kompetenču attīstības prasības izglītības speciālistiem. Tas ir specifiski pielāgots pedagogiem visos izglītības līmeņos, no bērnības līdz augstākajai un pieaugušos izglītībai, un fokusējas uz digitālo prasmju, kas nepieciešamas efektīvas mācīšanas pilnveidošanai arvien intensīvākā digitālajā mācību vidē. Ietvars ir strukturēts ap sešām kompetenču jomām: profesionālai iesaistei (digitālo tehnoloģiju lietošana komunikācijai, sadarbības un profesionālajai izaugsmei), digitālo resursu lietošanai (digitālo resursu izstrādei un mainīšanai un efektīvai pārvaldībai), mācīšanai un mācībām (digitālo tehnoloģiju izmantošana mācīšanas un mācību procesa sagatavošanai, ieviešanai un pārvaldībai), novērtēšanai (digitālo tehnoloģiju izmantošana vērtēšanai mācību rezultātiem un procesam), mācību dalībnieku iespējošanai (digitālo rīku lietošana, lai iesaistītu mācību dalībniekus un personalizētu viņu mācību pieredzi), mācību dalībnieku digitālo kompetenču attīstības atvieglošanai (stratēģiska mācību dalībnieku digitālo prasmju veicināšana un droša un atbildīga digitālo rīku lietošana). Papildus tam DigCompEdu ietvars identificē 22 atsevišķas kompetences un to līmeņus no "Iesācēja" līdz "Pionierim", piedāvājot pedagogiem ceļu, kā uzlabot viņu digitālo praksi.

Ietvars kalpo kā vadlīnijas pedagogiem, lai novērtētu un uzlabotu viņu digitālās kompetences, un atbalsta izglītības iestādes, izstrādājot mācību programmas un politiku, kas saskaņota ar modernām izglītības vajadzībām.

Minētie ietvari, lai arī vispārēji identificē prasības tiem indivīdiem un organizācijām, kas iesaistās jebkādās darbībās digitālajā vidē, sniedz strukturētu ieskatu prasmju kopumā, kas nepieciešamas PIA treneriem un mācībspēkiem.

PIA treneru un mācībspēku prasmes

Zināmā mērā PIA treneri un mācībspēki neatšķiras no citiem dalībniekiem digitālajā vidē. Šī iemesla dēļ prasmēm, kas vajadzīgas labas digitālās higiēnas praksei, būtu jāpiemīt visiem. Šīs prasmes iekļauj veselu rindu tehnisku, uzvedības un kognitīvo spēju. Tās ir arī prasmju apakšgrupa, kuras mēdz dēvēt par modernajām jeb nākotnes prasmēm, un, balstoties uz nesenajām digitālās vides attīstības tendencēm, šīs ir tās pašas prasmes, kuras izceļ kā izšķirošas organizācijām tuvākajā nākotnē, lietojot mākoņtehnoloģijas, analizē lielus datu apjomus un lietojot mākslīgā intelekta rīkus, lai palielinātu darba produktivitāti un efektivitāti [5,6].

Tomēr PIA treneru un mācībspēku darba specifika pieprasa pievērst īpašu uzmanību tam, kā viņi apstrādā datus un sazinās ar citiem mācību procesā Turpmāk seko dažas svarīgas prasmes, kas nepieciešamas PIA treneriem un mācībspēkiem, kas saistītas ar labu digitālo higiēnu:

- **Vispārēja apjausma par kiberdrošību**

Šī prasme iekļauj izpratni par tipiskiem tiešsaistes draudiem, piemēram, ļaunatūru, pikšķerēšanu, sociālās inženierijas uzbrukumiem, un zināšanas par to, kā tādus atpazīt un kā uz tiem reaģēt; zināšanas par drošu interneta izmantošanu, ieskaitot izvairīšanos no aizdomīgām mājaslapām, drošu interneta pieslēgumu lietošanu (HTTPS), un uzmanīšanos lejuplādēt datnes un klikšķināt uz saitēm.

- **Datu aizsardzība un privātums**

Šīs prasmes ietver spēju šifrēt jutīgus datus gan pārsūtīšanas laikā, gan uzglabājot tos, kā arī zināšanas par to, kā droši dzēst vai iznīcināt datus, kad tas ir nepieciešams; un izpratni par to, kā konfigurēt privātuma iestatījumus dažādās tiešsaistes platformās un ierīcēs, lai kontrolētu personiskās informācijas koplietošanu.

- **Ierīču drošība un pārvaldība**

Šīs prasmes ietver programmatūras, operētājsistēmu un lietojumprogrammu regulāru atjaunināšanu, lai novērstu drošības ievainojamības un aizsargātu pret zināmiem uzbrukumiem; spēju izveidot stipras un unikālas paroles dažādiem kontiem un efektīvi izmantot paroļu pārvaldības rīkus, lai droši uzglabātu un

pārvaldītu paroles; kā arī vairāku faktoru autentifikācijas iespējošanu un pārvaldību, kur tas ir iespējams, lai pievienotu papildu drošības slāni tiešsaistes kontiem.

- **Droša digitālā komunikācija**

Šī prasme ietver drošas komunikācijas praksi, piemēram, šifrētu e-pasta pakalpojumu izmantošanu vai drošu ziņojumapmaiņas lietotņu izvēli un izmantošanu, daloties ar konfidenciālu informāciju vai sazinoties ar studentiem, biedriem, kolēģiem vai partneriem ārpus PIA organizācijas; ievērot vadlīnijas, lai identificētu un izvairītos no pikšķerēšanas e-pastiem, krāpšanām un citām sociālās inženierijas taktikām, kas varētu apdraudēt PIA sistēmas vai izraisīt datu pārkāpumus.

- **Digitālās pēdas pārvaldība**

Šī prasme ietver izpratni par savas digitālās pēdas sekām un soļu veikšanu, lai samazinātu personiskās informācijas izplatīšanu tiešsaistē; un apmācību dalībnieku konsultēšanu darīt to pašu.

- **Kritiskā domāšana**

Šī prasme ietver kritiskās domāšanas prasmju attīstīšanu un piemērošanu, lai novērtētu tiešsaistes avotu uzticamību, identificētu dezinformāciju un krāpšanu, kā arī pieņemtu pamatotus lēmumus par tiešsaistes aktivitātēm, veicot vai sagatavojot mācības.

- **Nepārtraukta mācīšanās**

Šī prasme ietver iesaistīšanos vispārējā savu prasmju uzlabošanā; jaunu rīku un pieeju apgūšanu apmācībai digitālā vidē vai mūsdienīgu digitālo rīku izmantošanu; un sekošanu jaunākajiem kiberdrošības draudiem, privātuma jautājumiem un labākajai praksei, nepārtraukti mācoties un attīstoties.

- **Digitālā pilsonība un ētika**

Šī prasme ietver atbildīgas digitālās pilsonības praksi, nodrošinot PIA apmācību, ievērojot noteikumus un respektējot citu indivīdu un organizāciju tiesības; veicinot atbildīgu digitālo pilsonību starp studentiem, mācot ētisku uzvedību, cieņpilnu komunikāciju un digitālo etiķeti tiešsaistes vidē; veidojot analītiskās domāšanas prasmes, lai palīdzētu studentiem novērtēt tiešsaistes informācijas uzticamību, atpazīt digitālos riskus un pieņemt pamatotus lēmumus par savām tiešsaistes aktivitātēm; aizsargājot apmācībā iesaistīto indivīdu un organizāciju digitālo reputāciju.

Nosauktās prasmes var salīdzināt ar iepriekš aprakstīto DigCompEdu ietvaru, taču tās var precīzi neatbilst individuālajām kompetencēm, kas iekļautas šajā ietvarā. Drīzāk kompetenču jomu aprakstos ietvarā ir elementi, kas atbilst PIA treneriem un pedagogiem noderīgajām prasmēm.

Tabula 1.Saite starp PIA treneriem ieteicamajām prasmēm un DigCompEdu kompetenču jomām.

PIA trenera prasme	DigCompEdu kompetenču joma
Vispārēja apjausma par kiberdrošību	• Mācību dalībnieku iespējošana • Mācību dalībnieka digitālās kompetences attīstība
Datu aizsardzība un privātums	• Digitālie resursi • Mācību dalībnieka digitālās kompetences attīstība
Ierīču drošība un pārvaldība	• Mācīšana un mācīšanās • Mācību dalībnieka digitālās kompetences attīstība
Droša digitālā komunikācija	• Profesionālā iesaiste • Novērtēšana
Digitālās pēdas pārvaldība	• Digitālie resursi • Mācību dalībnieka digitālās kompetences attīstība
Kritiskā domāšana	• Mācīšana un mācīšanās • Mācību dalībnieka digitālās kompetences attīstība
Nepārtraukta mācīšanās	• Profesionālā iesaiste • Mācību dalībnieka digitālās kompetences attīstība
Digitālā pilsonība un ētika	• Mācību dalībnieku iespējošana • Mācību dalībnieka digitālās kompetences attīstība

Šīs prasmes nodrošina VET treneriem un pedagogiem iespējas piedalīties izglītības aktivitātēs, ievērojot labākās prakses digitālās higiēnas jomā. Praktiska norāde uz dažām labākajām praksēm ir pieejama Digitālās higiēnas ceļvedī [7]. Tas apraksta 12 drošas digitālās dzīves principus, kuriem visiem nepieciešamas zināšanas par digitālo pasauli, un tie ietver:

- darba programmatūras, antivīrusu, ugunsmūra u.c. atjaunināšanu,
- drošu paroļu lietošanu, to drošu pārvaldību un vairāku faktoru autentifikācijas izmantošanu,
- uzmanību, lejupielādējot programmatūru,
- izpratni par pikšķerēšanu un citām aizdomīgām metodēm apdraudēt jūsu resursus,
- digitālās un sociālās pēdas ierobežošanu,
- vispārēja "drošība vispirms" domāšanas principa pieņemšana, strādājot ar informāciju digitālajā vidē.

PIA apmācībā un izglītībā digitālās higiēnas prasmju apgūšana un praktizēšana ir svarīga, lai nodrošinātu drošu vidi informācijas apmaiņai.

3. daļa – Digitālās higiēnas adaptācija PIA mācību programmā un mācībās

Digitālās higiēnas tēmas būtu jāiekļauj ikdienas PIA apmācībā. PIA treneriem un pedagogiem jāievēro digitālās higiēnas vadlīnijas, plānojot un vadot apmācības, kurās tiek izmantoti digitālie rīki apmācības vides nodrošināšanai; mācību materiālu izstrādei un izplatīšanai; komunikācijas organizēšanai starp līdzbiedriem un starp treneriem un studentiem; apmācības rezultātu analīzei; un administratīvo procedūru veikšanai un apmācības procesa uzlabošanas plānošanai.

Turklāt PIA treneriem jāapzinās, ka, pat ja apmācības tēma nav saistīta ar digitālo pasauli, daļa šīs informācijas var būt nepieciešama, lai palielinātu apmācības efektivitāti. Treneriem jāņem vērā savu studentu iespējamā pieredze un jāpielāgo apmācības grafiks, rezervējot laiku un pieliekot pūles, lai skaidrotu un demonstrētu dažas apmācības prakses, kas uzlabos studentu digitālo higiēnu.

Protams, dažkārt digitālā higiēna un citas saistītās tēmas var būt mācību galvenā tēma. Šādos gadījumos PIA treneri un pedagogi var vadīt studentus, lai viņi iegūtu jaunas zināšanas un prasmes, kas saistītas ar digitālo higiēnu.

No PIA treneru viedokļa digitālo higiēnu var uztvert kā praksi, kas nodrošina drošas un produktīvas digitālās aktivitātes mācību laikā neatkarīgi no apmācības tēmas. Vairāki profesionālās izglītības un apmācības aspekti var prasīt digitālās vides izmantošanu, lai uzlabotu apmācības rezultātus un palielinātu studentu apmierinātību. Treneriem jāzina, kā digitālo rīku izmantošana ietekmē apmācības procesu, un jācenšas integrēt dažus digitālās higiēnas aspektus pašā apmācībā. Šeit ir daži ieteikumi, kā uzlabot apmācības procesu:

- **Tēmas un kursu moduļi par digitālo drošību**

Piedāvājot mācību saturu, sākot specifisku apmācības aktivitāti vai prasot studentiem veikt ar apmācību saistītu administratīvo darbību, ieviesiet padomus mazāku apmācības tēmu vai plašāku moduļu veidā, kas māca studentiem par kiberdrošības pamatiem, piemēram, paroļu pārvaldību, pikšķerēšanas mēģinājumu atpazīšanu un personisko un darba vietas datu aizsardzību. Kad iespējams, pielāgojiet šīs tēmas specifiskām nozarēm, darba situācijām, darba lomām vai aktivitātēm, kas saistītas ar studentu faktisko darba jomu vai nākotnes darba pozīciju, uz kuru viņi gatavojas, padarot informāciju atbilstošu un piemērojamu.

- **Praktiskās darbnīcas, individuāls un grupu darbs**

Veicot praktiskos uzdevumus mācību laikā, piemēram, praktiskās darbnīcas vai individuālus vai grupu darba uzdevumus, organizējiet darbnīcas, kurās studenti var praktizēt drošu tīklu izveidi, VPN izmantošanu, drošības programmatūras uzstādīšanu un pārvaldību, kā arī regulāru drošības pārbaužu veikšanu; vai ļaujiet viņiem pieredzēt, kā dažas kļūdas, kuras viņi, iespējams, neapzinās, var novest pie problēmām drošā mācību

vidē. Praktiska pieeja un iespējas izmēģināt un kļūdīties palīdz nostiprināt teorētiskās zināšanas, praktiski tās pielietojot.

- **Ētika un atbilstība**

Apmācības laikā iekļaujiet diskusijas un sniedziet vadlīnijas par ētisku uzvedību tiešsaistē un digitālo darbību juridiskajām sekām, ja teorētiskie apmācības temati vai praktiskie uzdevumi ietver dažādu rīcību ietekmi. Tas var aptvert tādas tēmas kā datu privātuma likumi, kas attiecas uz apmācības tēmu vai studentu lomām un profesionālo uzvedību, ētisko hakošanu un profesionālas tiešsaistes klātbūtnes uzturēšanas nozīmi.

- **Digitālās pēdas pārvaldība**

Izglītojiet studentus par viņu digitālās pēdas pārvaldību, uzsverot ilgtermiņa ietekmi uz personisko un profesionālo reputāciju tiešsaistē. Apmācība var ietvert sociālo mediju efektīvu izmantošanu, digitālā satura pārvaldību un tiešsaistes ierakstu seku izpratni. Izglītojiet studentus par to, kā darba rīki var radīt digitālo pēdu un kā viņiem vajadzētu pārvaldīt savus darba rezultātus un citu rezultātus, kas iegūti sadarbības laikā.

- **Nepārtraukta mācīšanās**

Apzinieties, ka mūsdienu digitālā vide mainās nepārtraukti. Atkarībā no viņu lomas un darba jomas, no kuras viņi nāk vai kurā vēlas iesaistīties, studentiem var būt nepieciešamas jaunas zināšanas par jaunu digitālo rīku izmantošanu. Ir svarīgi būt informētiem par jaunākajām tehnoloģijām un zināt jaunākos draudus, kas var ietekmēt studentus, kuri apgūst apmācības tēmu. Jaunu iespēju apzināšana digitālajā vidē un jaunu rīku ieviešana studentiem var palielināt apmācības kvalitāti un uzlabot studentu zināšanas un prasmes. Iespēju meklēšana nepārtrauktai mācīšanai un sertifikācijai digitālās drošības praksēs var kļūt par integrālu mācību plāna sastāvdaļu neatkarīgi no pamata mācību tematiem.

- **Novērtēšana un sertifikācija**

Novērtējumi ir daļa no apmācības. Atkarībā no apmācības temata un mērķiem novērtējumi var būt vairāk vai mazāk formāli un var ietvert digitālo rīku izmantošanu novērtējumu veikšanai un rezultātu apkopošanai un analīzei. Labā prakse ir pārliecināties, ka studenti zina, kā pareizi izmantot novērtēšanas rīkus. Novērtējumu saturs var ietvert zināšanu un prasmju pārbaudi, kas iegūtas konkrēti digitālās higiēnas jomā, vai par vispārējām zināšanām. Novērtējumi un sertifikācija var tikt izmantoti, lai motivētu studentus, un rezultātu atspoguļojums var pieprasīt papildu digitālās vides izpēti. Studentiem var būt nepieciešama palīdzība, iegūstot un apstrādājot jauno sertifikācijas informāciju vai izmantojot jaunās kvalifikācijas, lai palielinātu viņu nodarbinātības iespējas.

Var manīt, ka dažas no iespējām PIA apmācības uzlabošanai attiecībā uz digitālo higiēnu atbilst iepriekš identificētajām prasmēm. Visus šos elementus var iekļaut PIA programmās un skatīt no diviem dažādiem skatupunktiem: kādas digitālās higiēnas prasmes būtu jāizmanto kā daļa no mācībām un prasa papildu uzmanību mācību laikā; un kādas ir papildu iespējas uzlabot digitālās higiēnas zināšanas un prasmes mācību

laikā papildus galvenajām tēmām. Šo elementu ievērošana var uzlabot mācību kvalitāti un sniegt studentiem papildu priekšrocības viņu darba vidē, kas lielā mērā paļaujas uz digitālās pasaules iespējām.

No praktiskā viedokļa tas nozīmē, ka PIA treneriem un pedagogiem būtu jāievieš droša mācību vide un rīki, kas īpaši paredzēti apmācībai, jāizveido vadlīnijas mācību materiālu apstrādei, jāizmanto saziņas rīki un jāveic komunikācija, domājot par personiskās informācijas un īpašumtiesību informācijas aizsardzību, jāpārvalda dati par mācību procesu un rezultātiem, kas bieži ietver jutīgu informāciju, un jāievēro un jāsniedz vispārēji padomi, kas veicina labas digitālās higiēnas prakses ievērošanu.

4. daļa – Labās prakses piemērs – digitālā higiēna PIA organizācijā

Apskatīsim labas prakses piemēru, kā digitālo higiēnu var ieviest PIA organizācijā, lai nodrošinātu organizācijas drošību un PIA treneru un apmācībā iesaistīto studentu drošību.

Situācijas apraksts

Profesionālās izglītības un apmācības uzņēmums vēlas nodrošināt tiešsaistes apmācību saviem studentiem, lai izvairītos no dārgiem un laikietilpīgiem ceļojumiem un nodrošinātu studentiem iespēju piedalīties apmācībā no drošas fiziskas vides. VET uzņēmumā ir iekšējo un ārējo treneru personāls, kuriem ir dažāda iepriekšējā pieredze ar tiešsaistes apmācību nodrošināšanu un kuriem var būt atšķirīgas zināšanas un prasmes saistībā ar šādu apmācību veikšanu. Uzņēmumam ir arī iekšējie darbinieki, kuri veic ar mācībām saistītās administratīvās darbības un apstrādā informāciju, kas dažkārt ir jutīga un jāievēro atbilstības noteikumi un vadlīnijas. Parasti treneriem būs jāizmanto Microsoft Teams vide apmācības veikšanai, mācību materiālu koplietošanai un saziņai ar studentiem, kamēr iekšējais atbalsta personāls izmantos Microsoft Teams un e-pastu, lai pārvaldītu studentus pirms, mācību laikā un pēc apmācības, kā arī kādu no dokumentu glabāšanas sistēmām mācību materiālu pārvaldībai un koplietošanai.

Lietas, par kurām VET uzņēmums ir noraizējies, ir:

- nepareiza personiskās informācijas apstrāde no jebkura apmācības dalībnieka puses,
- uzņēmuma un ārējo partneru īpašumtiesību informācijas rūpīga izmantošana,
- piekļuves ierobežošana apmācībai tikai paredzētajai auditorijai,
- bagātīgas pieredzes nodrošināšana studentiem,
- noteikta reputācijas līmeņa uzturēšana kā labam apmācību pakalpojumu sniedzējam tirgū.

Apskatīsim, kā digitālās higiēnas jautājumus var risināt šajā situācijā.

Risinājums

Šāda veida situācija ir sarežģīta un prasa pievērst uzmanību vairākiem digitālās higiēnas aspektiem:

- Microsoft Teams vides iestatīšanas organizēšana un lietotāju pārvaldība apmācības laikā,
- to treneru, kuri vada mācības, apmācība,
- faktisko apmācību sesiju vadīšana ar studentu un treneru iesaistīšanos,
- apmācības materiālu apstrāde, kas tiek izmantoti apmācības laikā,
- komunikācijas organizēšana starp treneri un studentiem un starp pašiem studentiem,
- apmācību izvērtējumu veikšana un atsauksmju vākšana.

Detalizētāks labas prakses apraksts katram no šiem aspektiem seko tālāk.

Uzstādīšana un lietotāju pārvaldība

Teams for Education: Tika izveidota Teams vide, kas ir atsevišķa no ikdienas saziņai un zināšanu apmaiņai izmantotās Teams vides PIA organizācijas darbiniekiem. Microsoft Teams for Education ir pieejams tām PIA organizācijām, kas atbilst oficiālo izglītības organizāciju prasībām, un tas piedāvā papildu funkcijas, kas ir noderīgas apmācību veikšanai.

Single Sign-On (SSO): Tika ieviesta vienotā pierakstīšanās (SSO) izmantošana, izmantojot kopīgu autentifikācijas platformu (piemēram, Active Directory), lai vienkāršotu piekļuvi Microsoft Teams, lietotnēm, kas tiek izmantotas Microsoft Teams vidē, un citiem rīkiem, ko apmācību laikā centrāli izmanto un apstiprina PIA organizācija.

Lomu bāzēta piekļuves kontrole: Tika piešķirtas lomas un atļaujas Teams vidē, balstoties uz lietotāja pozīciju. Konkrēti tika piešķirtas 4 lomas, katrai ar savām privilēģijām Teams vidē: sistēmu administrators, apmācību administrators (persona, kas organizē apmācību sesijas pirms apmācības un analizē apmācību rezultātus pēc tās), treneris (persona, kas vada apmācību un praktiskos uzdevumus un apstrādā apmācību materiālus apmācības laikā) un students, nodrošinot atbilstošu piekļuvi funkcijām un informācijai.

Drošas autentifikācijas prakse: Kur nepieciešams, lietotājiem, kuriem tika piešķirtas lielākas privilēģijas piekļūstot jutīgai informācijai, tika sniegta apmācība par vairāku faktoru autentifikācijas (MFA) un stipru paroļu izmantošanu, lai uzlabotu drošību.

Treneru apmācība

Microsoft Teams apmācību darbnīcas: Tika plānotas un vadītas īpašas darbnīcas treneriem par efektīvu Microsoft Teams izmantošanu, un iekšējie un ārējie treneri tika aicināti piedalīties, lai saņemtu vadlīnijas par drošu darbu Teams vidē. Apmācība ietvēra komandu un kanālu izveidi un pārvaldību, sapulču plānošanu un sadarbības funkciju, piemēram, kopīgoto failu un tērzēšanas, izmantošanu.

Paplašināto funkciju apmācība: Treneriem tika nodrošināta papildu apmācība par paplašinātām funkcijām, piemēram, grupu istabām, tiešraides pasākumiem un trešo pušu lietotņu integrēšanu, kas var uzlabot apmācības pieredzi, un tika piedāvāta iespēja praktizēt šīs funkcijas praktisko uzdevumu laikā apmācībā.

Nepārtraukts atbalsts: Tiem treneriem, kuriem bija nepieciešamas pilnībā aprīkotas fiziskās apmācību telpas, tika piedāvātas telpas ar drošu interneta pieslēgumu. Tiem treneriem, kuri plānoja izmantot savas telpas, tika nodrošinātas vadlīnijas par drošu apmācību vadīšanu. Tika nodrošināta īpaši nozīmēta IT atbalsta personāla kontaktinformācija, lai palīdzētu treneriem tehnisko problēmu gadījumā.

Mācību sesiju vadīšana

Sesiju plānošana: Iekšējie apmācību administratori un treneri tika apmācīti izmantot kalendāru sesiju plānošanai, atgādinājumu iestatīšanai un darba kārtības nodrošināšanai uzaicinājumā uz sapulci. Automātiskie uzaicinājumi tika izveidoti studentiem, lai samazinātu risku pievienoties nepareizām apmācību sesijām.

Interaktīvās funkcijas: Visiem treneriem tika ieteikts izmantot papildu Teams funkcijas, piemēram, aptaujas, viktorīnas un tāfeles sesiju laikā, lai iesaistītu studentus un uzlabotu mācīšanos, kad vien iespējams. Papildu rīku un funkciju izmantošana tika atļauta, taču treneriem tika ieteikts instruēt studentus, tos izmantojot papildu informācijas vai praktisko uzdevumu veikšanai.

Sesiju ierakstīšana: Apmācību sesiju ierakstīšana bija stingri ierobežota GDPR dēļ un tika veikta tikai pēc visu studentu skaidras piekrišanas. Kad ieraksti tika izveidoti, tie tika droši uzglabāti un pieejami tikai tiem, kas piedalījās apmācību sesijās, un tikai uz ierobežotu laiku. Lai gan ieraksti vispārīgi tiek uzskatīti par noderīgiem studentiem apmācību satura pārskatīšanai vēlāk, PIA organizācijai jāapzinās ar tiem saistītie riski.

Grupu telpas: Grupu aktivitātēm vai diskusijām ar mācību administratora palīdzību tika izveidotas grupu telpas, tām piešķirtas piekļuves tiesības, un tika veikta atbilstoša apmācība treneriem, ļaujot treneriem pārvietoties starp telpām, lai vadītu un uzraudzītu apmācību progresu.

Mācību materiālu pārvaldība

Failu un resursu koplietošana: Visi apmācību materiāli, kas tika izmantoti apmācību laikā, tika glabāti drošos serveros. Elektroniskās atslēgas uz apmācību materiāliem vai faktiskās apmācību materiālu kopijas pārvaldīja īpašs apmācību administrators. Mazāk sensitīviem materiāliem tika izmantota Teams vide.

Kopīga rediģēšana: Kad praktisko uzdevumu laikā notika sadarbība ar dokumentiem vai prezentācijām reāllaikā, treneriem un studentiem tika ieteikts izmantot oficiālu programmatūru, piemēram, Office 365 integrāciju, un būt uzmanīgiem, lai nepārspīlētu ar informācijas izplatīšanu.

Versiju kontrole: PIA organizācijā tika ieviesta iekšējo dokumentu, kas bija daļa no apmācību materiāliem, versiju kontrole. Visiem treneriem tika ieteikts uzņemties ekspertu lomu attiecībā uz ārējiem apmācību materiāliem un viņi tika mudināti konsultēties ar iekšējiem apmācību administratoriem par apmācību materiālu, studentu ceļvežu un praktisko testu versijām, kur tas bija piemērojams, lai mazinātu kaitējumu PIA organizācijas reputācijai, nodrošinot neaktuālas apmācību materiālu versijas.

Komunikācija starp studentiem un treneriem

Regulāri atjauninājumi: Teams tērzēšana tika izmantota paziņojumu veikšanai, atjauninājumu koplietošanai un atsauksmju sniegšanai par apmācību sesijām.

Speciālie kanāli: Tika izveidoti kanāli specifiskām apmācību sesijām un atsevišķām studentu grupām, veicinot mērķtiecīgas diskusijas un resursu koplietošanu.

Privātā tērzēšana: Papildu privātās tērzēšanas starp treneri un studentiem tika ierobežotas tikai uz situācijām, kad abas puses piekrita papildu komunikācijai, un kontaktinformācijas apmaiņa tika organizēta centrāli.

Novērtējums un atgriezeniskā saite

Atsauksmju formas: Lai apkopotu atsauksmes par apmācību sesijām, tika izmantotas Microsoft Forms vai iekšēji PIA organizācijas izstrādāta programmatūra. Saites uz atsauksmju programmatūru tika izplatītas caur Teams vidi, nodrošinot, ka tikai paredzētā auditorija var piedalīties atsauksmju sniegšanā. Piekļuve informācijai, kas sniegta atsauksmju formās, bija ierobežota tikai VET organizācijas iekšējiem apmācību administratoriem.

Mācību progresa izsekošana: Tika izmantotas uzdevumu funkcijas Teams, lai piešķirtu uzdevumus, savāktu pabeigtos darbus un sniegtu vērtējuma rezultātu.

Šāda gan tehniskās vides, gan procesu un lomu izveide nodrošina visaptverošu, drošu un interaktīvu apmācību vidi, izmantojot Microsoft Teams, apmierinot gan treneru, gan studentu vajadzības, un vienlaikus uzturot augstu digitālās higiēnas un efektivitātes standartu.

Avoti

1. Vuorikari, R., Kluzer, S. and Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.
2. European e-Competence Framework, https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf, [accessed April 15, 2024].
3. European Union Agency for Cybersecurity (ENISA). European Cybersecurity Skills Framework Role Profiles, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles [accessed April 15, 2024].
4. Punie, Y., editor(s), Redecker, C., European Framework for the Digital Competence of Educators: DigCompEdu, EUR 28775 EN, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73718-3 (print),978-92-79-73494-6 (pdf), doi:10.2760/178382 (print),10.2760/159770 (online), JRC107466.
5. World Economic Forum, “Future of Jobs Report 2023”, https://www.weforum.org/publications/the-future-of-jobs-report-2023/
6. Chui, M., Issler, M., Roberts, R., Yee, L. “McKinsey Technology Trends Outlook 2023”, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#new-and-notable
7. Digital Hygiene Cheat Sheet. https://digitalhygiene.net/ [accessed April 15, 2024].

2. Modulis – Digitālās higiēnas pielāgotā programma PIA vajadzībām

Ievads

Digitālās higiēnas lomas mūsu ikdienas dzīvē ir pieaugusi un kļuvusi nozīmīgāka. Strauji pieaugot digitalizācijai un tai ieejot cilvēka darbības sfērās ir radusies steidzama nepieciešamība padarīt mūsu digitālo vidi drošu. Viens no galvenajiem un fundamentālajiem aizsardzības pasākumiem šajā sakarā ir nodrošināt pareizu digitālo higiēnu. Tas ir īpaši svarīgi, ņemot vērā pieaugošos kiberapdraudējumus, ar kuriem saskaras organizācijas. Digitālā higiēna galvenokārt koncentrējas uz veselīgas un drošas digitālās klātbūtnes uzturēšanu, un tas ir kļuvis arvien aktuālāk, jo vairāk organizāciju pāriet uz darbībām tiešsaistē. Šis modulis ir izveidots, lai nodrošinātu spēcīgu mācību programmu, kas var apmācīt studentus profesionālajā līmenī attīstīt, novērtēt un uzturēt labas digitālās higiēnas prakses.

Šī programmas apgūšana ļaus studentam iegūt nepieciešamās pamatprasmes analītiskajā un praktiskajā jomā, lai efektīvi novērtētu, uzturētu un, ja nepieciešams, iejauktos, lai nodrošinātu digitālo higiēnu organizācijas ietvaros. Šī ir patiešām aktuāla programma, ņemot vērā augsto pieprasījumu pēc profesionāļiem ar prasmēm šajā jomā. Šī attīstības programma ir izstrādāta, balstoties uz labākajām praksēm šajā jomā. Programmas uzmanības centrā ir jaunuzņēmumu un MVU profesionāļi, kam svarīgi šie mācību moduļi un struktūra. Mērķis ir izveidot kompetenci šajā līmenī, kas nozīmē, ka programma ir izstrādāta un strukturēta tā, lai tā būtu pieejama tiem, kas vēlas to apgūt nepilna vai pilna laika režīmā. Programma ir arī izstrādāta, lai būtu praktiska un orientēta uz praktisko pielietojumu un ātri apgūstama. Tomēr tā ir arī izstrādāta tā, lai studenti to varētu apgūt savā ātrumā.

1. daļa – Programmas apskats

Šī rokasgrāmata ir izstrādāta, lai sniegtu studentiem, kuri uzsāk vai gatavojas uzsākt Profesionālās izglītības un apmācības (PIA) digitālās higiēnas programmā, kā arī instruktoriem, atbilstošai informācijai par programmas mērķi, plānošanu, struktūru un novērtēšanu. Atzīstot, ka ne visas organizācijas ir vienādas un neprasa vienādu digitālās higiēnas prasmju līmeni, šis modulis un tā dažādās daļas ir modulāras struktūras. Tas ļauj indivīdiem, kuri ir kompetenti noteiktās jomās, koncentrēties uz vai pāriet uz citiem moduļiem, attīstoties viņu vajadzībām. Programmas galvenais mērķis ir izveidot spēcīgu digitālās higiēnas pamatu, dodot iespēju gan studentiem, gan instruktoriem efektīvi pārvaldīt un mazināt kiberdraudus. Šī mācību programma

ir arī izstrādāta, lai aptvertu būtiskas bāzes līmeņa profesionālās kiberdrošības sertifikāciju daļas, piemēram, GIAC Security Essentials (GSEC) un CompTIA Security+. Tādējādi tā nodrošina papildu vērtību un palielina motivāciju studentiem piedalīties šajā programmā.

Programmas mērķis un moduļu mērķi

Digitālās higiēnas moduļa galvenie mērķi ir veidoti, lai uzlabotu organizāciju kiberdrošības stāvokli, nodrošinot dalībniekiem iespēju:

- Novērtēt organizāciju piedzīvotos kiberdrošības draudus.
- Novērtēt un ieviest pamata tīkla drošību.
- Zināt, kā ieviest un uzturēt pamata šifrēšanas protokolus.
- Novērtēt un ieviest datu pārvaldības un drošības protokolus.
- Novērtēt un pielietot pamata aparatūras un programmatūras drošības protokolus.
- Pārvaldīt drošību mobilajā vidē.

Mācību metodoloģija

Programma apvieno teorētisko apmācību un praktisko zināšanu pielietojumu. Tiek izmantoti gadījumu izpētes, praktisko darbu laboratoriju sesijas un interaktīvas darbnīcas, lai nodrošinātu, ka mācību dalībnieki var pielietot apgūtos konceptus reālās dzīves situācijās. Šī pieeja ne tikai uzlabo izpratni, bet arī nodrošina, ka absolventi ir gatavi darbam un spēj nekavējoties ieviest visaptverošas digitālās higiēnas prakses pēc programmas pabeigšanas.

Novērtēšana un nepārtraukta uzlabošana

Digitālās higiēnas programmas novērtēšana ir gan stingra, gan nepārtraukta, izmantojot dažādas metodes dalībnieku zināšanu un prasmju novērtēšanai. Šīs metodes ietver viktorīnas, praktiskos eksāmenus, projektos balstītus novērtējumus un noslēguma projektu, kas ietver visu dalībnieku apgūto materiālu. Atgriezeniskās saites mehānismi ir integrēti mācību programmā, nodrošinot dalībniekiem savlaicīgus ieskatus par viņu progresu un jomām, kur nepieciešams uzlabojums. Turklāt pati mācību programma tiek regulāri atjaunināta, lai atbilstu jaunākajiem kiberapdraudu izlūkošanas datiem un tehnoloģiskajiem sasniegumiem, nodrošinot atbilstību un efektivitāti mūsdienu kiberdrošības izaicinājumu risināšanā.

Secinājumi

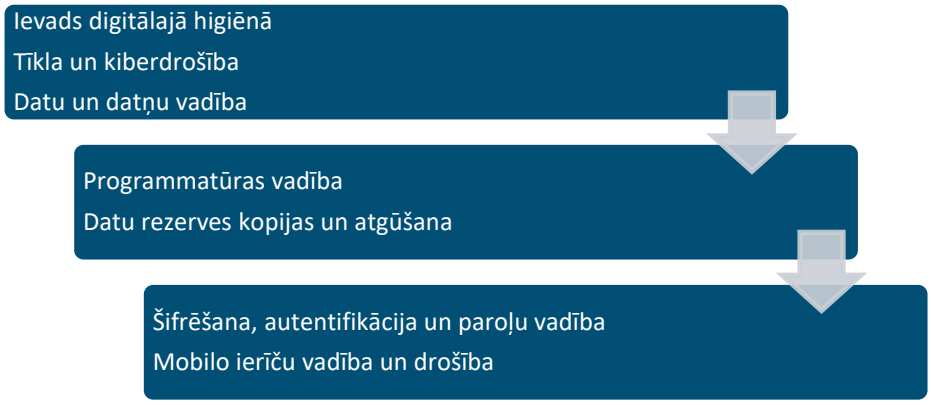
Digitālās higiēnas programma PIA institūcijā ir izstrādāta ne tikai, lai sniegtu būtiskas kiberdrošības zināšanas un prasmes, bet arī lai ieaudzinātu dalībniekos proaktīvu un informētu kiberdrošības kultūru. Programmas beigās dalībnieki nebūs tikai absolventi; viņi būs pilnvaroti digitāli pilsoņi, kas spēs būtiski veicināt savas

organizācijas kiberdrošības aizsardzību. Šī visaptverošā programma ir stūrakmens nākamās paaudzes kiberdrošības profesionāļu sagatavošanā, kas ir gatavi risināt digitālā laikmeta dinamiskos izaicinājumus.

2. daļa – Galvenās mācību jomas

Mācību programmas apskats

Kods	Mācību joma/tēma
D21	Ievads digitālajā higiēnā
D22	Tīkla un kiberdrošība
D23	Datu un datņu vadība
D24	Programmatūras vadība
D25	Datu rezerves kopijas un atgūšana
D26	Šifrēšana, autentifikācija un paroļu vadība
D27	Mobilo ierīču vadība un drošība



Ievads digitālajā higiēnā

Šis priekšmets ir izstrādāts, lai sniegtu studentiem visaptverošu pārskatu par digitālo higiēnu. Šis pārskats nodrošinās gan konceptuālu satura pārskatu, gan dažus praktiskos aspektus, apskatot programmu no integrētas perspektīvas. Galvenā uzmanība tiks pievērsta dažādām digitālās higiēnas jomām un to savstarpējai saistībai. Tas sniegs sākotnēju pārskatu par digitālās higiēnas pamatprincipiem un praksi un to, kā atsevišķās daļas sader kopā. Šī tēma nodrošina pamatzināšanas un izpratni, kuras vēlāk papildinās citas tēmas.

Galvenās tēmas šajā priekšmetā

- Digitālās higiēnas izpratne: Izpēte par to, kas veido digitālo higiēnu un kāpēc tā ir kritiska mūsdienu digitālajā laikmetā.

- Digitālās higiēnas pamatelementi: Pamatprakse un protokoli, kas nodrošina datu un sistēmu integritāti un drošību.
- Drošības ietekme uz digitālo higiēnu: Detalizēts pārskats par to, kā efektīva digitālā higiēna var mazināt dažādus kiberapdraudējumus.
- Digitālās higiēnas ieviešanas pamati: Praktiski soļi digitālās higiēnas pasākumu ieviešanai personīgā un organizācijas kontekstā.
- Kiberdrošības atbilstība: Pārskats par pamatprincipiem un ES un nacionālajām politikām, noteikumiem un atbilstības prasībām kiberdrošības jomā.

Priekšmeta mācību rezultāti

Līdz šī priekšmeta beigām studenti spēs:

- Definēt digitālo higiēnu un saprast tās kritiskos komponentus.
- Identificēt potenciālos kiberapdraudējumus un saprast digitālās higiēnas lomu aizsardzībā pret šiem apdraudējumiem.
- Ieviest pamata digitālās higiēnas prakses dažādās platformās un ierīcēs.
- Komunicēt digitālās higiēnas nozīmi līdzbiedriem un vadītājiem, veicinot labāko prakšu ieviešanu savās organizācijās.
- Saprast pamata kiberdrošības atbilstības prasības.

Mācību metodes

Tiks izmantota lekciju, interaktīvu darbnīcu un gadījumu izpētes kombinācija, lai nodrošinātu studentiem spēcīgu mācību pieredzi. Katra sesija mērķē līdzsvarot teorētiskās zināšanas ar praktisko pielietojumu, nodrošinot, ka studenti var pārvērst apgūto par praktiskām stratēģijām savās darbavietās.

Ieteicamā literatūra

- Brooks, C.J., Grow, C., Craig, P., Short, D., (2018), Cybersecurity Essentials.
    - Grāmata nodrošina kārtīgu ievadu kiberdrošības jomā un faktiski ir noderība iesācēja līmeņa kiberdrošības sertifikācijām.
- Paula, D., Cruz, M., (2023), Cybersecurity Essentials Made Easy: A No-Nonsense Guide to Cyber Security for Beginners.
    - Grāmata ir svarīgs avots, lai saprastu kiberdrošības izaicinājumus un kā tos mazināt. Tā ir īpaši atbilstoša jaunuzņēmumu īpašniekiem un studentiem, kas vēlas saprast drošību tiešsaistē.
- Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
    - Šis avots nodrošina pieejamu kopsavilkumu par kiberdrošības atslēgas jēdzieniem un izaicinājumiem, padarot to par izcilu resursu studentiem, kas uzsāk savu ceļu kiberdrošības risku un aizsardzības mehānismu izpratnē.
- Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
    - Brūsa Šneiera grāmata ir svarīga, lai saprastu datu privātuma un drošības situāciju, ļaujot ieskatīties kā personas dati tiek ievākti un lietoti, un cik svarīga ir robusta datu pārvaldības prakse.

Šie resursi ir atlasīti, lai sniegtu teorētiskas zināšanas un prasmes tīklu un kiberdrošībā, atbalstot mācību programmu un uzlabojot digitālās higiēnas mācību pieredzi PIA studentiem.

Tīkla un kiberdrošība

Šis priekšmets ir vērsts uz studentu nodrošināšanu ar nepieciešamajām prasmēm, lai identificētu, novērtētu un neitralizētu tīkla draudus. Viens no galvenajiem izaicinājumiem, ar kuriem organizācijas saskaras pašreizējā darbības vidē, ir tīkla drošības nodrošināšana. Tā kā lielākā daļa tīklu ir savienoti ar internetu, tie bieži tiek pakļauti ļaunprātīgiem indivīdiem, kuri var mēģināt izmantot tīkla ievainojamības, lai neautorizēti piekļūtu tīklam. Lai to sasniegtu, studenti tiks apmācīti par galvenajiem tīkla jēdzieniem, bieži lietotiem protokoliem, portiem, LAN, WAN un mākoņsistēmām.

Galvenās tēmas šajā priekšmetā

- Ievads kiberdrošībā
- Ievainojamību analīze
- Draudu un risku novērtēšana
- Tīkla drošības protokoli – Ugunsmūri, antivīrusi
- Biežākie kiberdrošības uzbrukumi
- Biežākie kiberdrošības rīki
- Ētika kiberdrošībā

Priekšmeta mācību rezultāti

- Identificēt galvenos tīkla konceptus: Studenti spēs aprakstīt tīklu pamata aspektus, tostarp LAN, WAN un mākoņsistēmas, un saprast to lomu organizācijas infrastruktūrā.
- Novērtēt tīkla ievainojamības: Studenti apgūs prasmes veikt ievainojamību analīzi dažādās tīkla sistēmās, lai identificētu iespējamās drošības vājās vietas.
- Ieviest drošības pasākumus: Studenti būs prasmīgi iestatīt un pārvaldīt tīkla drošības protokolus, piemēram, ugunsmūrus un antivīrusu sistēmas, lai aizsargātos pret kiberdraudiem.
- Veikt draudu un risku novērtējumus: Studenti spēs novērtēt un prioritizēt riskus, kas saistīti ar kiberdrošības draudiem tīkla sistēmām.
- Saprast ētiskās sekas: Studenti izpētīs ētiskos apsvērumus kiberdrošībā, saprotot atbildību par datu un sistēmu aizsardzību no neautorizētas piekļuves.

Mācību metodes

- Interaktīvās lekcijas: Fokusējas uz fundamentālo un progresīvo tīkla konceptu, drošības protokolu un ētisko jautājumu ieviešanu kiberdrošībā.

- Praktiskās laboratorijas: Praktiskās sesijas datorlaboratorijās, kur studenti var izmantot reālas un simulētas tīkla vides, lai pielietotu drošības pasākumus un rīkus.
- Gadījumu analīze: Reālu kiberdrošības incidentu apspriešana un analīze, lai saprastu draudu mehānismus un efektīvus pretpasākumus.
- Grupu projekti: Studentu komandas novērtēs hipotētisku tīkla uzstādījumu ievainojamības un piedāvās visaptverošu drošības stratēģiju.
- Vieslektoru sesijas: Kiberdrošības profesionāļi ir aicināti dalīties ar atziņām un pieredzi, uzsverot pašreizējos izaicinājumus un jaunās tehnoloģijas.

Ieteicamā literatūra

- Stewart, J. M., Chapple, M., & Gibson, D. (2020). *CompTIA Security+ Guide to Network Security Fundamentals* (7th ed.). Cengage Learning.
    - Šī pamācība iekļauj plašu spektru pamata tēmu par tīklu drošību un ir piemērota studentiem, kas uzsāk savu ceļu kiberdrošībā.
- Marsh, N., (2023), Cybersecurity: A Fat-Free Guide to Network Security Best Practices (Fat-Free Technology Guides). This book provides a comprehensive insight into cyber threats and critical network security issues.
- Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.
    - Visaptverošs resurss, kas nodrošina padziļinātu ieskatu informācijas drošības principos, ieskaitot detalizētu izklāstu par ievainojamības analīzi, draudu un risku novērtējumu.
- Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.
    - Stallinga teksts nodrošina pilnvērtīgu pārskatu par tīkla drošības protokoliem un standartiem, ir ideāls studentiem, kuriem nepieciešama detalizēta izpratne par tīklu drošības tehniskajiem aspektiem.
- Computer & Internet Security: A Hands-on Approach 3rd ed. Edition by Wenliang Du

Šie akadēmiskie resursi atbalstīt mācību programmu, nodrošinot teorētisku ietvaru un praktisku ieskatu tīkla vides pārvaldībā un nodrošināšanā, saistoties ar uzskaitītajiem mācību rezultātiem un mācību metodēm.

Datu un datņu vadība

Dati, kā jau minēts iepriekš, ir viens no vērtīgākajiem aktīviem, kas pieder organizācijām. Līdz ar to šī aktīva pārvaldība ir kļuvusi par arvien svarīgāku lomu organizācijā. Tas ir īpaši svarīgi, ņemot vērā pieaugošās drošības bažas kibervidē. Pareiza datu pārvaldība ir kļuvusi par būtisku efektīvai kiberdrošībai, īpaši jutīgas informācijas iegūšanā, organizēšanā un izplatīšanā. Datu pārvaldība attiecas uz principiem un praksēm, kas tiek piemērotas datu pārvaldībai un aizsardzībai. Kiberdrošības kontekstā datu pārvaldība ir arī saistīta ar datu aizsardzību no neautorizētas piekļuves, modifikācijas un pārsūtīšanas. Pašreizējā vidē, kurā tiek vākti, analizēti un izplatīti lieli datu apjomi, drošības pārvaldības aspekti ir ieguvuši ievērību. Tāpēc ir palielinājusies nepieciešamība pēc profesionāļiem, kuri ir prasmīgi datu pārvaldībā.

Galvenās tēmas šajā priekšmetā

- Datu pārvaldība
- Datu klasifikācija
- Šifrēšana datu pārvaldībā

- Datu uzraudzība un audits
- Datu rezerves kopijas un atjaunošana
- Datu integritāte un privātums
- Piekļuves kontrole un autentifikācija

Priekšmeta mācību rezultāti

- Saprast datu pārvaldību: Studenti izpratīs datu pārvaldības pamatkoncepcijas un tās lomu organizācijas kontekstā.
- Klasificēt datus: Studenti spēs klasificēt datus pēc to jutīguma un nozīmīguma, piemērojot atbilstošus drošības pasākumus dažādiem datu veidiem.
- Ieviest datu šifrēšanu: Studenti sapratīs un pielietos šifrēšanas paņēmienus, lai aizsargātu datu integritāti un konfidencialitāti glabāšanas un pārsūtīšanas laikā.
- Veikt datu auditus: Nodrošināt studentus ar prasmēm veikt regulāru datu uzraudzību un auditus, lai nodrošinātu atbilstību drošības politikām un noteikumiem.
- Pārvaldīt datu atjaunošanu: Studenti apgūs stratēģijas datu rezerves kopiju veidošanai un atjaunošanai, lai nodrošinātu datu pieejamību un nepārtrauktību datu zuduma vai sistēmu kļūmju gadījumā.
- Nodrošināt datu integritāti un privātumu: Studenti sapratīs metodes, kā uzturēt datu integritāti un pārvaldīt privātuma iestatījumus, lai aizsargātu lietotāju datus no neautorizētas piekļuves.
- Pielietot piekļuves kontroli: Studenti būs spējīgi ieviest spēcīgas piekļuves kontroles un autentifikācijas metodes, lai aizsargātu datu piekļuvi.

Ieteicamā literatūra

- Ladley J., (2019)., Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program 2nd Edition. This book provides a comprehensive view of data governance and security.
- Talabis, M., & Martin, J. (2015). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis. Syngress.
    - Šī grāmata nodrošina praktiskus rīkus un tehnikas, lai novērtētu informācijas drošības riskus, ieskaitot tos, kas saistīti ar datu pārvaldību.
- Bertino, E., & Sandhu, R. (2017). Data Privacy and Security. Springer.
    - Visaptverošs pārskats par datu privātuma un drošības tehnikām, šis teksts ir nozīmīgs, lai saprastu sarežģījumu jutīgu datu aizsardzībai dažādās vidēs.
- Swanson, M., & Guttman, B. (2016). Generally Accepted Principles and Practices for Securing Information Technology Systems. National Institute of Standards and Technology.
    - Šī vadības publikācija piedāvā vadlīnijas un labo praksi, lai nodrošinātu IT sistēmas, ieskaitot detalizētas nodaļas par datu pārvaldību un drošības kontroli.

Šie akadēmiskie resursi pastiprinās mācību ietvaru, nodrošinot teorētiskās zināšanas un praktiskus pielietojuma piemērus, ļaujot studentiem kļūt spējīgiem efektīvi vadot un nodrošinot organizācijas datus.

Programmatūras vadība

Programmatūras pārvaldība ir būtisks kiberdrošības elements. Programmatūras pārvaldība ietver sistemātisku procesu, kas saistīts ar plānošanu, izvietošanu, uzraudzību un uzturēšanu visā tās dzīves ciklā. Tas ietver tādus uzdevumus kā versiju kontrole, jauninājumu pārvaldība, licencēšana un drošības atjauninājumi. Efektīva programmatūras pārvaldība nodrošina optimālu veiktspēju, drošību un atbilstību, vienlaikus samazinot riskus un ievainojamības. Mūsdienu organizācijas saskaras ar dažādiem programmatūras drošības izaicinājumiem, piemēram, vājām parolēm, nedrošiem API, neatjauninātām ievainojamībām, pikšķerēšanu un datu noplūdēm, lai nosauktu dažus. Tāpēc ir svarīgi, lai viņiem būtu apmācīti darbinieki, kas efektīvi pārvaldītu organizācijas programmatūru un novērstu programmatūras drošības pārkāpumus. Šis modulis nodrošinās studentus ar praktiskām pamatzināšanām par to, kā efektīvi pārvaldīt organizācijas programmatūru un samazināt drošības pārkāpumu risku.

Galvenās tēmas šajā priekšmetā

- Lietojumprogrammu drošība
- Programmatūras testēšana un auditi
- Lietotāju piekļuves un privilēģiju pārvaldība
- Regulāru atjaunināšanas protokolu ieviešana
- Gala ierīču drošības pasākumi

Priekšmeta mācību rezultāti

- Apgūt lietojumprogrammu drošību: Studenti sapratīs lietojumprogrammu aizsardzības pamatus no projektēšanas līdz ieviešanai, tostarp kopējās ievainojamības un to novēršanas stratēģijas.
- Veikt programmatūras testēšanu un auditus: Studenti iegūs prasmes dažādās programmatūras testēšanas un audita metodēs, lai identificētu un novērstu drošības problēmas.
- Pārvaldīt lietotāju piekļuvi: Studenti iemācīsies efektīvi pārvaldīt lietotāju piekļuvi un privilēģijas, lai nodrošinātu, ka tikai autorizēti lietotāji piekļūst kritiskiem programmatūras resursiem.
- Ieviest atjaunināšanas protokolus: Nodrošināt studentus ar zināšanām, lai izveidotu un uzturētu regulārus programmatūras atjaunināšanas protokolus, lai mazinātu ievainojamības.
- Uzlabot gala ierīču drošību: Studenti sapratīs gala ierīču drošības pasākumus, lai aizsargātu organizācijas infrastruktūru no tādiem draudiem kā ļaunprātīga programmatūra un izspiedējprogrammatūra.

Ieteicamā literatūra

- Du, W., (2022), Computer Security: A hands-on approach, 3rd edition.
  - Grāmata izpēta programmatūras pārvaldību, ievainojamības un to novēršanas aktivitātes.
- Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). Software Security Engineering: A Guide for Project Managers. Addison-Wesley Professional.

    - Šī grāmata sniedz visaptverošu pamācību drošības prakses integrēšanā programmatūras izstrādē, padarot to par būtisku avotu, lai saprastu aplikāciju drošību un dzīvescikla vadību.
- Anton, A. I., & Earp, J. B. (2004). A Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. Academy of Management Review.
    - Grāmata nodrošina ieskatu lietotāju pieejas tiesību un privilēģiju pārvaldībā, identificējot svarīgākos interesentu un viņu vajadzības, kas ir būtiski programmatūras izstrādē.
- Lindqvist, U., & Neumann, P. G. (2017). The Future of Cybersecurity: Challenges and Opportunities. IEEE Security & Privacy.
    - Šis raksts apspriež nākotnes izaicinājumus un iespējas kiberdrošībā, ieskaitot programmatūras nepārtrauktus uzlabojumus un galapunktu drošības mērus.

Šie resursi atbalstīs mācību programmu, sniedzot teorētisko pamatu un praktisko ieskatu programmatūras izstrādē, nodrošinot, ka studenti ir sagatavoti risināt programmatūras drošības izaicinājumus modernā organizācijas vidē.

Datu rezerves kopijas un atgūšana

Šis modulis ir izstrādāts, lai sniegtu studentiem visaptverošu izpratni par datu rezerves kopiju veidošanas un datu atgūšanas procesu un kā to var īstenot. Visām mūsdienu organizācijām ir jābūt atbilstošām datu rezerves kopiju un atgūšanas politikām, protokoliem un sistēmām. Lielākā daļa pašreizējo organizāciju ir datos balstītas un piešķir lielu nozīmi savu datu un informācijas resursu pārvaldībai. Principā lielākā daļa organizāciju, īpaši mazie un vidējie uzņēmumi (MVU), glabā savus datus centralizētā vietējā vai mākoņa datubāzē. Mākoņbāzētās sistēmas ir kļuvušas arvien modernākas un drošākas ar ļoti sarežģītiem pārvaldības kontroles mehānismiem, padarot tās mazāk jutīgas pret tradicionālajām fizisko glabāšanas sistēmu iznīcināšanas problēmām. Tomēr tās joprojām ir pakļautas cilvēka kļūdām, nepareizai konfigurācijai un datu pārkāpumiem, tāpēc ir svarīgi, lai IT personāls, kas pārrauga šādas sistēmas, būtu zinošs atbilstošajās tehnoloģijās, protokolos un procesos. Šis modulis ir paredzēts, lai sniegtu studentam šādas zināšanas.

Galvenās tēmas šajā priekšmetā

- Datņu pārvaldība
- Rezerves kopiju un atjaunošanas protokoli
- Rezerves kopiju veidi
- Rezerves kopiju pakalpojumi un ierīces

Priekšmeta mācību rezultāti

- Saprast datņu pārvaldību: Studenti apgūs efektīvus datņu pārvaldības principus, kas ir būtiski datu organizēšanai rezerves kopiju veidošanas nolūkos.
- Apgūt rezerves kopiju un atjaunošanas protokolus: Studenti sapratīs dažādus rezerves kopiju un atjaunošanas protokolus un to, kā tos efektīvi pielietot dažādās situācijās.

- Identificēt rezerves kopiju veidus: Studenti spēs atšķirt dažādus rezerves kopiju veidus (pilnas, inkrementālas, diferenciālas) un izlemt, kurš ir vispiemērotākais konkrētām situācijām.
- Izmantot rezerves kopiju pakalpojumus un ierīces: Sniegt studentiem zināšanas par dažādiem rezerves kopiju pakalpojumiem un ierīcēm, tostarp mākoņbāzētiem un lokāliem risinājumiem, un kā tos droši īstenot.
- Samazināt datu zuduma riskus: Studenti sapratīs, kā plānot un īstenot datu atjaunošanas stratēģiju, lai samazinātu dīkstāves laiku un datu zudumus datu pārkāpumu vai katastrofu gadījumā.

Ieteicamā literatūra

- Preston, W., (2021), Modern Data Protection: Ensuring Recoverability of All Modern Workloads.
    - Šī grāmata ir par modernu datu aizsardzību un kā tā tiek integrēta vispārēja datorsistēmu un programmatūras drošībā.
- Data Backup And Recovery A Complete Guide - 2023 Edition
- Toigo, J. W. (2009). Disaster Recovery Planning: Preparing for the Unthinkable (3rd ed.). Prentice Hall.
    - Sniedz visaptverošu ieskatu avārijas seku novēršanas plānošanā, ieskaitot detalizētu diskusiju par rezerves kopiju stratēģijām kā kritisku avārijas seku novēršanas sastāvdaļu.
- Duffy, D. (2014). Cloud Computing: Strategies for Cloud Computing Adoption. Faithful Pen Publishing.
    - Analizē mākoņdatošanas pieņemšanu, koncentrējoties uz mākoņa bāzētiem rezerves kopiju pakalpojumiem un ar tiem saistītiem drošības apsvērumiem.

Šie akadēmiskie resursi pastiprinās mācību programmu sniedzot studentiem pamata izpratni un praktiskas prasmes datu rezerves kopiju un atgūšanas stratēģijām, kas ir būtiskas, lai samazinātu potenciālo datu zudumu modernā organizācijas vidē.

Šifrēšana, autentifikācija un paroļu vadība

Dati un informācija ir kļuvuši par vienu no svarīgākajiem organizācijas aktīviem, un daudzos gadījumos tie ir galvenais uzņēmuma vērtības noteicējs. Šādu aktīvu būtiskā nozīme liek pret tiem izturēties ar vislielāko rūpību. Viens no galvenajiem rīkiem datu un informācijas aktīvu aizsardzībai ir šifrēšana jeb kriptogrāfija. Šifrēšana ir svarīga kiberdrošībai, jo tā ir būtiska jutīgu datu un informācijas aizsardzībai un drošai saziņai. Tā nodrošina spēcīgus autentifikācijas protokolus un paroļu pārvaldību. Šifrēšana ļauj nodrošināt atbilstošu autentifikācijas sistēmu ieviešanu, kas nodrošina organizācijas datu un informācijas konfidencialitāti, integritāti un pieejamību atbilstošajiem darbiniekiem.

Galvenās tēmas šajā priekšmetā

- Kriptogrāfijas pamati
- Šifrēšana no gala līdz galam
- Šifrēšanas standarti
- Daudzfaktoru autentifikācija
- Atslēgu pārvaldība
- Labāko standartu izvēle jūsu uzņēmumam

- Labākā prakse šifrēšanas tehnoloģiju ieviešanā

Priekšmeta mācību rezultāti

- Saprast kriptogrāfijas pamatus: Studenti apgūs kriptogrāfijas pamatprincipus, tostarp tās vēsturi, mērķi un galvenos mehānismus.
- Ieviest šifrēšanu no gala līdz galam: Apmācāmie iegūs prasmes iestatīt un pārvaldīt šifrēšanu no gala līdz galam, lai nodrošinātu drošu saziņu.
- Pielietot šifrēšanas standartus: Studenti iepazīsies ar dažādiem šifrēšanas standartiem un apgūs to pielietošanu atbilstoši organizācijas vajadzībām.
- Izmantot daudzfaktoru autentifikāciju: Studenti apgūs spējas ieviest un pārvaldīt daudzfaktoru autentifikācijas sistēmas, lai uzlabotu drošību.
- Pārvaldīt kriptogrāfiskās atslēgas: Studenti sapratīs atslēgu pārvaldības procesus un labāko praksi, lai nodrošinātu kriptogrāfisko atslēgu drošību un integritāti.
- Izvēlēties un ieviest šifrēšanas tehnoloģijas: Studenti apgūs, kā izvēlēties piemērotas šifrēšanas tehnoloģijas savam uzņēmumam un labāko praksi to ieviešanā, lai efektīvi aizsargātu datus.

Ieteicamā literatūra

- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
    - Šī grāmata sniedz visaptverošu ievadu kriptogrāfijas laukāThis textbook provide un tīkla drošībā, ieskaitot detalizētu šifrēšanas tehnoloģiju un atuentifikācijas protokolu apskatu.
- Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography (2nd ed.). CRC Press.
    - Piedāvā padziļinātu moderno kriptogrāfijas tehniku izpēti, koncentrējoties uz pastiprinātiem drošības apsvērumiem un praktiskajiem pielietojumiem.
- Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley.
    - Šī grāmatu runā par kriptogrāfijas sistēmu dizainu un ieviešanu, uzsverot pareizu ieviešanu, lai novērstu ievainojamības.

Šie resursi ir izvēlēti, lai sniegtu teorētisko pamatojumu un praktiskas prasmes šifrēšanā, autentifikācijā un paroļu pārvaldībā, atbalstot mācību programmas mērķus sniegt studentiem vajadzīgās zināšanas, lai nodrošinātu efektīvu organizācijas datu aizsardzību.

Mobilo ierīču vadība un drošība

Organizācijas arvien vairāk izvieto mobilās ierīces kā galveno darba platformu un saziņas līdzekli. Tas īpaši attiecas uz jaunizveidotajiem uzņēmumiem un MVU, kur elastība un sasniedzamība jebkurā laikā ir kļuvusi par galveno kritēriju panākumiem. Lai gan mobilā tehnoloģija ir attīstījusies tiktāl, ka lielākā daļa modernāko viedtālruņu ir tikpat jaudīgi un daudzpusīgi kā klēpjdatori un galddatori, šo ierīču bezvadu raksturs padara tās uzņēmīgas pret ļaunprātīgiem indivīdiem, kas cenšas iegūt nesankcionētu piekļuvi. Šis modulis ir izstrādāts, lai sniegtu ieskatu par šo ierīču un to platformu ievainojamībām un kā šādus riskus var mazināt.

Galvenās tēmas šajā priekšmetā

- Izpratne par draudiem mobilajām ierīcēm
- Risku novērtēšana mobilajām lietotnēm
- Starp-procesu komunikācijas ugunsmūri
- Mobilās drošības tehnoloģijas
- Mobilās datu piekļuves kontroles un riska pārvaldība

Priekšmeta mācību rezultāti

- Identificēt draudus mobilajām ierīcēm: Studenti apgūs spēju atpazīt dažādus draudus, kas mērķē uz mobilajām platformām, un sapratīs to iespējamo ietekmi.
- Novērtēt riskus mobilajām lietotnēm: Studenti iegūs prasmes novērtēt ar mobilajām lietotnēm saistītos riskus, pievēršot uzmanību drošības ievainojamībām.
- Ieviest mobilās drošības tehnoloģijas: Studenti spēs ieviest un pārvaldīt drošības tehnoloģijas, kas ir īpaši paredzētas mobilajām ierīcēm.
- Pārvaldīt starp-procesu komunikācijas ugunsmūrus: Studenti iegūs zināšanas par ugunsmūru konfigurēšanu un pārvaldību, kas kontrolē starp-procesu komunikāciju mobilajās ierīcēs.
- Piemērot mobilās datu piekļuves kontroles: Studenti apgūs, kā izveidot un īstenot datu piekļuves kontroles, lai nodrošinātu sensitīvas informācijas drošību mobilajās ierīcēs.

Ieteicamā literatūra

- Doherty, J., (2021), Wireless and Mobile Device Security 2nd Edition.
    - Šī grāmata apskata ātrās mobilo ierīču integrācijas organizācijas komunikāciju vidē ietekmi, saistītajiem drošības apsvērumiem un tā tos mazināt.
- Russell, B., Van Duren, Drew., (2018), Practical Internet of Things Security - Second Edition: Design a security framework for Internet-connected Ecosystem
- Zdziarski, J. A. (2015). Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It. O'Reilly Media, Inc.
    - Šī grāmata sniedz padziļinātu ieskatu iOS drošības arhitektūrā, apspriež biežākās ievainojamības un piedāvā stratēģijas iOS aplikāciju nodrošināšanai.
- Fried, S. (2011). Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World. CyberAge Books.
    - Šī pamācība ir nozīmīga studentiem un praktiķiem, kuriem jāsaprot īpašie drošības izaicinājumi, kurus rada mobilās ierīces, kuras arvien biežāk izmanto personiskajā un profesionālajā kontekstā.

Šie resursi atbalstīs mācību programmu, nodrošinot pamata zināšanas un specifiskas prasmes, kas nepieciešamas, lai efektīvi pārvaldītu un nodrošinātu mobilās ierīces, nodrošinot, ka studenti ir labi sagatavot reaģēt uz mobilās drošības izaicinājumiem modernā organizācijas kontekstā.

3. daļa – Digitālās higiēnas novērtējums un atgriezeniskās saites mehānismi PIA organizācijām

Ievads

Novērtēšana un atgriezeniskā saite ir būtiskas izglītības procesa sastāvdaļas, nodrošinot gan pasniedzējiem, gan studentiem svarīgas atziņas par mācīšanas un mācīšanās efektivitāti. Digitālās higiēnas mācību programmā spēcīgi novērtēšanas un atgriezeniskās saites mehānismi ir īpaši svarīgi. Tie nodrošina, ka apgūtās zināšanas un prasmes ne tikai tiek saprastas un saglabātas, bet arī tiek pielietotas reālās situācijās, kur digitālās drošības riski ir izplatīti.

Šī vienība ir izstrādāta, lai izklāstītu stratēģijas un metodoloģijas studentu snieguma novērtēšanai un konstruktīvas atgriezeniskās saites nodrošināšanai visas digitālās higiēnas mācību programmas laikā. Tā ietver teorētisko zināšanu novērtējumu un praktiskos novērtējumus.

Novērtēšanas stratēģijas

Formatīvie novērtējumi

- **Viktorīnas un īsie testi**: Bieži viktorīnas un īsie testi tiks veikti katra moduļa laikā, lai novērtētu galveno jēdzienu izpratni un sniegtu tūlītēju atgriezenisko saiti. Tas palīdz stiprināt mācīšanos un identificēt jomas, kur studentiem var būt nepieciešams papildu atbalsts.
- **Praktiskie uzdevumi**: Studentiem tiks doti uzdevumi, kas prasa teorētisko zināšanu pielietošanu praktiskās situācijās, piemēram, ugunsmūra konfigurēšana, datu atjaunošanas plāna izstrāde vai šifrēšanas protokolu ieviešana.
- **Savu biedru novērtējumi**: Tas ietver studentu savstarpējo uzdevumu vai projektu novērtēšanu. Savu biedru novērtējumi var palīdzēt attīstīt kritiskās domāšanas un analītiskās prasmes, jo studenti mācās kritizēt kiberdrošības risinājumus, balstoties uz labāko praksi.

Summatīvie novērtējumi

- **Gala eksāmeni**: Visaptveroši eksāmeni katra moduļa beigās pārbaudīs studentus par plašu tēmu loku, kas aptvertas kursa laikā. Šie eksāmeni ietvers gan daudzizvēļu jautājumus, gan esejas veida jautājumus, lai novērtētu studentu teorētisko un praktisko izpratni.
- **Noslēguma projekti**: Programmas beigās studenti veiks noslēguma projektu, kas ietver visaptverošu digitālās higiēnas stratēģiju izveidi vai pārvaldīšanu hipotētiskām organizācijām. Šis projekts tiks vērtēts pēc dažādiem kritērijiem, tostarp inovācijas, piemērojamības un atbilstības kiberdrošības principiem.

Nepārtrauktie novērtējumi

- **Portfolio pārskati**: Studenti uzturēs portfeli (portfolio) ar savu darbu un sasniegumiem visas mācību programmas laikā. Šie portfeļus pasniedzēji periodiski pārskatīs, lai novērtētu progresu un sniegtu personalizētu atgriezenisko saiti.
- **Pašnovērtējumi**: Mudinot studentus iesaistīties pašnovērtējumā, var veicināt lielāku atbildību par viņu pašu mācīšanās procesu. Tiks nodrošināti pašnovērtējuma rīki un kontrolsaraksti, lai palīdzētu studentiem novērtēt savu izpratni un prasmes.

Atgriezeniskās saites mehānismi

- **Pasniedzēja atsauksmes**: Atsauksmes tiks sniegtas sistemātiski par visiem novērtējumiem, koncentrējoties uz studentu darba stiprajām un vājajām pusēm. Šīs atsauksmes būs savlaicīgas, specifiskas un konstruktīvas, lai mudinātu studentus pārdomāt savu mācīšanos un identificēt uzlabojumu jomas.
- **Savu biedru atsauksmes**: Grupas projektos un savstarpējos novērtējumos studenti tiks mudināti sniegt atsauksmes viens otram. Šī atsauksmju sniegšana būs strukturēta, lai nodrošinātu konstruktivitāti un koncentrēšanos uz konkrētiem kritērijiem.
- **Automatizētas atsauksmes**: Noteiktiem novērtējumu veidiem, īpaši viktorīnām un dažiem praktiskiem vingrinājumiem, tiks izmantotas automatizētas atsauksmju sistēmas. Šīs sistēmas var sniegt tūlītējus rezultātus un atziņas, ļaujot ātri novērst nepilnības.
- **Atsauksmju cilpas**: Veidojot atsauksmju cilpas mācību programmā, kur studenti var pārdomāt atsauksmes, pārskatīt savu darbu un iesniegt to atkārtotai pārbaudei, veicina uz izaugsmi orientētu domāšanu un nodrošina nepārtrauktu uzlabošanos.

Atgriezeniskās saites ieviešana mācību programmas izstrādē

Saņemtās atsauksmes no šiem dažādajiem mehānismiem nav tikai studentu labā. Tām ir arī būtiska loma mācību programmas izstrādē:

- **Mācību programmas pielāgojumi**: Regulāras studentu snieguma datu un atsauksmju pārbaudes palīdzēs identificēt mācību programmas jomas, kurām var būt nepieciešami pielāgojumi vai uzlabojumi.
- **Pasniedzēju attīstība**: Atsauksmes no studentiem var arī norādīt uz profesionālās attīstības vajadzībām pasniedzējiem, norādot jomas, kurās viņiem var būt nepieciešams lielāks atbalsts vai apmācība.

Noslēgums

Digitālās higiēnas mācību programmas novērtēšanas un atgriezeniskās saites mehānismi profesionālās izglītības un apmācības (PIA) iestādēs ir būtiski, lai nodrošinātu, ka izglītības mērķi tiek sasniegti. Izmantojot dažādas novērtēšanas stratēģijas un daudzkanālu atsauksmju sistēmas, mācību programma ne tikai efektīvi novērtē studentu mācīšanos, bet arī nepārtraukti uzlabo mācīšanas metodes un mācību programmas dizainu. Šī dinamiskā pieeja nodrošina, ka mācību programma paliek aktuāla un efektīva, sagatavojot studentus risināt reālās pasaules digitālās higiēnas izaicinājumus.

4. daļa – Labā prakse PIA organizācijās

Ievads

Dinamiskajā digitālās higiēnas jomā teorētiskās zināšanas kopā ar praktisko pielietojumu rada visefektīvāko mācību vidi. Šī sadaļa apskata labās prakses piemērus, ko pieņēmušas profesionālās izglītības un apmācības (PIA) iestādes, kas veiksmīgi integrējušas digitālās higiēnas principus savās mācību programmās. Šie gadījumu pētījumi kalpo kā piemēri digitālās higiēnas programmu izstrādei un pilnveidei, sniedzot ieskatu veiksmīgās stratēģijās un metodoloģijās, kuras var atkārtot vai pielāgot citas iestādes.

Gadījums 1: CyberVET Academy

Pārskats:

CyberVET Academy ir pazīstama ar savu spēcīgo digitālās higiēnas mācību programmu, kas apvieno stingru akadēmisko izglītību ar reālās pasaules pielietojumu. Šī iestāde ir kļuvusi par paraugu, kā nemanāmi integrēt jaunās tehnoloģijas un kiberdrošības labāko praksi profesionālajā apmācībā.

Pamata stratēģijas

- Nozares partnerības: CyberVET ir izveidojusi partnerības ar vadošajiem tehnoloģiju uzņēmumiem, lai nodrošinātu, ka viņu mācību programma atbilst pašreizējiem nozares standartiem un praksei. Šīs partnerības arī veicina vieslekcijas, prakses iespējas un piekļuvi modernākajām tehnoloģijām.
- Simulētas mācību vides: CyberVET Academy ir ieguldījusi līdzekļus modernu simulētu kiberdrošības laboratoriju izveidē, kur studenti var droši izpētīt un novērst reāllaika kiberdraudus. Šī praktiskā pieredze ir neatsverama.

Iznākumi:

- Ievērojams studentu nodarbinātības pieaugums, 90% absolventu iegūstot darbu kiberdrošības jomā sešu mēnešu laikā pēc izlaiduma.
- Uzlabota studentu iesaistīšanās un apmierinātība, ko veicina praktiskā mācību pieeja un tieša nozares iesaiste.

Gadījums 2: TechBridge VET

Pārskats:

TechBridge VET izceļas ar savu fokusu uz mobilo ierīču pārvaldību un drošību, kas ir arvien aktuālāki jautājumi digitālās higiēnas jomā.

Pamata stratēģijas:

- Modulāras mācību programmas izveide: TechBridge mācību programma ir ļoti modulāra, ļaujot studentiem pielāgot savus mācību ceļus atbilstoši viņu karjeras mērķiem un tehnoloģiskajiem sasniegumiem.
- Kopienas projekti: Studenti piedalās kopienas iesaistes programmās, kurās viņi izmanto savas zināšanas, lai palīdzētu vietējiem mazajiem uzņēmumiem uzlabot to digitālās drošības pasākumus.

Iznākumi:

- Kopienas projekti ne tikai palielinājuši studentu praktiskās prasmes, bet arī veicinājuši kiberdrošības izpratni vietējo mazo uzņēmumu īpašnieku vidū.
- Modulārā pieeja nodrošinājusi augstu izglītības elastību, pielāgojoties straujām tehnoloģiju izmaiņām un studentu vajadzībām.

Gadījums 3: SecurePath Institute

Pārskats:

SecurePath Institute ir integrējis digitālo higiēnu visās savās profesionālajās programmās, parādot, kā kiberdrošība ir būtiska dažādām tehniskajām disciplīnām.

Pamata stratēģijas:

- Starpdisciplināra pieeja: Integrējot digitālās higiēnas nodarbības tādās programmās kā veselības aprūpe, automobiļu tehnoloģija un biznesa vadība, SecurePath nodrošina, ka visi studenti apzinās kiberdrošības nozīmi savās attiecīgajās jomās.
- Nepārtraukta mācību programmas novērtēšana: Institūts izmanto ar mākslīgo intelektu darbinātu analītikas sistēmu, lai nepārtraukti novērtētu un atjauninātu savu mācību programmu, balstoties uz jaunākajiem kiberapdraudējumu izlūkdatiem un nozares tendencēm.

Iznākumi:

- Studenti no netehniskām programmām absolvē ar spēcīgu digitālās higiēnas izpratni, padarot viņus daudzpusīgākus un pievilcīgākus darba devējiem.
- Nepārtrauktā mācību programmas novērtēšana ir ļāvusi SecurePath noturēties digitālās higiēnas izglītības priekšgalā, ātri pielāgojoties jaunajiem draudiem.

Labās prakses sekas

Šo institūciju panākumi ilustrē vairākas labākās prakses, kuras var pieņemt vai pielāgot citas profesionālās izglītības un apmācības (PIA) iestādes:

- Nozares sadarbība: Spēcīgas saites ar nozari ne tikai uztur mācību programmu aktuālu, bet arī uzlabo studentu darba izredzes pēc absolvēšanas.
- Praktiska pielietošana: Praktiska mācīšanās, izmantojot laboratorijas, simulācijas vai kopienas projektus, ir būtiska, lai efektīvi izprastu un pielietotu digitālās higiēnas principus.
- Elastība un starpdisciplinaritāte: Elastīga un starpdisciplināra pieeja nodrošina, ka digitālās higiēnas izglītība var ātri pielāgoties izmaiņām un aptvert plašu profesionālo jomu spektru.
- Atsauksmes un nepārtraukta pilnveide: Nepārtraukta mācību programmas novērtēšana un pārskatīšana, balstoties uz atsauksmēm no dažādām ieinteresētajām pusēm, tostarp studentiem, pasniedzējiem un nozares partneriem, nodrošina programmas efektivitāti un aktualitāti.

Gadījums 4: DigitalDefenders College

Pārskats:

DigitalDefenders College ir pazīstama ar savu specializēto pieeju kiberdrošības mācīšanā, īpašu uzsvaru liekot uz ētisko hakošanu un digitālās tiesu ekspertīzes tehnikām. Šī profesionālās izglītības iestāde ir apņēmusies sagatavot prasmīgus profesionāļus, kas gatavi risināt kiberapdraudējumu sarežģītību mūsdienu digitālajā vidē.

Pamata stratēģijas:

- Ētiskās hakošanas moduļi: Iekļaujot plašus moduļus par ētisko hakošanu, koledža nodrošina studentiem prasmes identificēt un izmantot sistēmu ievainojamības, visu to darot kontrolētā, ētiskā un likumīgā ietvarā. • Reālas pasaules kiber tiesu ekspertīze: Studenti piedalās praktiskos kiber tiesu ekspertīzes vingrinājumos, kas imitē reālus datu pārkāpumu scenārijus, palīdzot viņiem saprast, kā izsekot, analizēt un efektīvi mazināt pārkāpumus.

Iznākumi:

- Absolventi ir pazīstami ar savu proaktīvo pieeju kiberdrošībai, un daudzi iegūst amatus augstas likmes sektoros, piemēram, finanšu un valdības nozarēs.

- Praktiskā pieredze ētiskajā hakošanā un kiber tiesu ekspertīzē ir radījusi augstu studentu iesaistīšanās līmeni, veicinot dziļu izpratni par kiberapdraudējumu praktiskajām sekām.

Gadījums 5: InnovateTech Institute

Pārskats:

InnovateTech Institute ir izcēlies, integrējot savā digitālās higiēnas mācību programmā progresīvas tehnoloģiju tendences, piemēram, mākslīgo intelektu (MI vai angliski AI) un mašīnmācīšanos (MM vai angliski ML). Šī pieeja sagatavo studentus arvien vairāk MI virzītajai kiberdrošības ainavai.

Pamata stratēģijas:

- MI virzīti drošības risinājumi: Mācot studentiem izmantot MI un MM, lai izstrādātu sarežģītus kiberdrošības pasākumus, tādējādi priekšlaicīgi apsteidzot kibernoziedzniekus, kuri arī izmanto progresīvās tehnoloģijas.
- Sadarbības projekti ar tehnoloģiju uzņēmumiem: Studenti strādā pie projektiem sadarbībā ar tehnoloģiju uzņēmumiem, izveidojot uz MI balstītus drošības risinājumus, kas sniedz viņiem reāllaika ieskatu nozares izaicinājumos un prasībās.

Iznākumi:

- Studenti ir izstrādājuši vairākus uz MI balstītus drošības rīkus, kurus ir pieņēmuši sadarbības partneri, tādējādi demonstrējot savu tiešo ietekmi uz pašreizējiem kiberdrošības risinājumiem.
- MI un MM integrēšana digitālās higiēnas izglītībā ne tikai padarījusi mācību programmu spēcīgāku, bet arī ievērojami palielinājusi studentu nodarbinātības iespējas tehnoloģiju virzītajās nozarēs.

Kopsavilkums gadījumu izpētei

Šie papildu gadījumu pētījumi no DigitalDefenders College un InnovateTech Insitute vēl vairāk nostiprina veiksmīgas digitālās higiēnas mācību programmas būtiskos aspektus profesionālās izglītības iestādēs:

- Specializācija un uzlabota apmācība: Programmas, kas piedāvā specializētu apmācību kiberdrošības augsti pieprasītās jomās, piemēram, ētiskajā hakošanā un mākslīgajā intelektā, var ievērojami uzlabot mācību programmas atbilstību un pievilcību.
- Reāla pielietojuma prasmes: Praktisks, reāla pielietojuma mācību prasmes, neatkarīgi no tā, vai tās ir kiber tiesu ekspertīzes vai sadarbības projekti ar nozari, nodrošina, ka studenti ne tikai ir pazīstami ar teorētiskajiem jēdzieniem, bet arī prasmīgi tos pielieto reālās situācijās.

- Inovatīva un nākotnei gatava mācību programma: Saglabājot mācību programmas atbilstību jaunākajiem tehnoloģiskajiem sasniegumiem, studenti tiek sagatavoti jaunām draudu un iespēju situācijām, padarot viņus par vērtīgiem resursiem jebkurā kiberdrošības lomā, ko viņi uzņemsies pēc absolvēšanas.
- Šie piemēri demonstrē daudzveidīgas stratēģijas, kuras var ieviest, lai efektīvi uzlabotu digitālās higiēnas izglītību, katra unikāli veicinot galveno mērķi – veicināt prasmīgu profesionāļu izaugsmi, kas ir gatavi aizsargāt digitālos aktīvus arvien sarežģītākā kibervidē.

Noslēgums

Pieci gadījumu pētījumi, ko veikušas CyberVET Academy, TechBridge VET, SecurePath Institute, DigitalDefenders College un InnovateTech Institute, sniedz bagātīgu veiksmīgu stratēģiju un pieeju kopumu, integrējot digitālo higiēnu profesionālās izglītības un apmācības (PIA) mācību programmās. Katra iestāde ar savu unikālo fokusu un metodoloģiju uzsver praktiskās, ar nozari saskaņotās un inovatīvās izglītības izšķirošo lomu, sagatavojot studentus adaptēties kiberdrošības sarežģītībā mūsdienu digitālajā pasaulē.

Galvenās atziņas un labās prakses

- Nozares sadarbība un saskaņošana: Kopīga tēma visos gadījumu pētījumos ir stipru saišu uzturēšanas ar nozares līderiem un uzņēmumiem svarīgums. Šīs partnerības ne tikai uztur mācību programmas aktuālas ar jaunākajām tehnoloģijām un praksēm, bet arī uzlabo studentu nodarbinātību, piedāvājot prakses iespējas, reālus projektus un saskari ar nozares standartiem.
- Praktiska un reāla pieredze: Katra iestāde uzsver nepieciešamību praktiski pielietot apgūtos jēdzienus. Neatkarīgi no tā, vai tas notiek kiberdrošības laboratorijās, simulētās vidēs vai reālās tiesu izmeklēšanās, praktiskā pieredze ir būtiska. Tā ne tikai nostiprina teorētiskās zināšanas, bet arī sagatavo studentus reālās pasaules izaicinājumiem, ar kuriem viņi saskarsies savā karjerā.
- Specializēti moduļi un uzlabota apmācība: Tādas iestādes kā DigitalDefenders College izceļ specializētas apmācības priekšrocības tādās jomās kā ētiskā hakošana un kibertiesu ekspertīze. Tāpat InnovateTech Institute fokuss uz MI vadītiem drošības risinājumiem ilustrē priekšrocības, ko sniedz jaunāko tehnoloģiju integrācija mācību programmā, sagatavojot studentus nākotnes tendencēm un inovācijām kiberdrošībā.
- Starpdisciplināras un elastīgas mācību pieejas: SecurePath Institute digitālās higiēnas integrācija dažādās profesionālajās programmās parāda starpdisciplināras pieejas vērtību, kas paplašina kiberdrošības izglītības piemērojamību un aktualitāti. Turklāt TechBridge VET modulārā mācību

programmas izstrāde nodrošina lielāku elastību, pielāgojoties straujām tehnoloģiju izmaiņām un daudzveidīgām studentu interesēm.

- Nepārtraukta uzlabošana un pielāgošanās: SecurePath Institute izmantotā MI vadītā analītikas sistēma nepārtrauktai mācību programmas novērtēšanai un InnovateTech Institute dinamiskās atjaunināšanas protokoli uzsver pastāvīgas novērtēšanas un pielāgošanās nozīmi. Mācību programmas saglabāšana atsaucīga uz mainīgo kiberapdraudējumu ainavu nodrošina, ka izglītības programmas paliek aktuālas un efektīvas.

Ieskatu apkopojums no šīm dažādajām PIA iestādēm atklāj, ka digitālās higiēnas mācību programmas efektivitāte ir atkarīga no tās spējas apvienot teorētiskās zināšanas ar praktiskām prasmēm, pielāgoties tehnoloģiskajiem sasniegumiem un veicināt stipras nozares saites. Šie elementi ir būtiski, lai sagatavotu studentus ne tikai atbilstībai pašreizējām kiberdrošības jomas prasībām, bet arī spēt radīt inovācijas un vadīt citus nākotnes izaicinājumos. Šī holistiskā pieeja ne tikai uzlabo mācīšanās pieredzi, bet arī ievērojami palielina absolventu nodarbinātību un gatavību aizsargāt digitālos aktīvus globāli savienotā pasaulē. PIA iestādēm turpinot attīstīt un pilnveidot savas programmas, atziņas no šiem gadījumu pētījumiem sniedz vērtīgas vadlīnijas, lai izstrādātu spēcīgas, visaptverošas digitālās higiēnas mācību programmas, kas ir gatavas risināt rītdienas kiberdrošības ainavas izaicinājumus.

Avoti:

1. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.
2. Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.
3. Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography* (2nd ed.). CRC Press.
4. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.
5. Chapple, M., Seidl, D., & Stewart, J. M. (2018). *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide* (8th ed.). Sybex.
6. Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley Professional.
7. Conklin, W. A., White, G., Cothren, C., Williams, D., & Davis, R. (2016). *Principles of Computer Security: CompTIA Security+ and Beyond* (5th ed.). McGraw-Hill Education.
8. Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* (5th ed.). Prentice Hall.
9. Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press.
10. Zdziarski, J. A. (2015). *Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It*. O'Reilly Media.
11. Tipton, H. F., & Nozaki, M. K. (2013). *Official (ISC)2 Guide to the CISSP CBK* (4th ed.). CRC Press.
12. Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach Publications.
13. Kim, D., & Solomon, M. G. (2016). *Fundamentals of Information Systems Security* (3rd ed.). Jones & Bartlett Learning.
14. Caloyannides, M. A. (2010). *Privacy Protection and Computer Forensics* (2nd ed.). Artech House.
15. Toigo, J. W. (2009). *Disaster Recovery Planning: Preparing for the Unthinkable* (3rd ed.). Prentice Hall.
16. Ross, R. S. (2013). *Managing Information Security Risks: The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Approach*. Addison-Wesley.
17. Bodmer, C., Kilger, M., Carpenter, G., & Jones, J. (2012). *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. McGraw-Hill Osborne Media.
18. Enck, W. (2011). *Understanding Android Security*. IEEE Security & Privacy Magazine.
19. Anton, A. I., & Earp, J. B. (2004). *A Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts*. Academy of Management Review.
20. Liska, A., & Gallo, T. (2016). *Rethinking the Security of the Internet of Things*. Elsevier.
21. Clarke, N. L., & Furnell, S. M. (2016). *Cybersecurity Education: Strategies and Best Practices*. Springer.
22. Bishop, M. (2018). *Computer Security: Art and Science*. Addison-Wesley.

23. Eckert, J. W. (2017). *CompTIA Linux+ Guide to Linux Certification*. Cengage Learning.
24. Skoudis, E., & Zeltser, L. (2019). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall.
25. Easttom, C. (2019). *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. McGraw-Hill Education.
26. Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson.
27. Andress, J., & Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress.
28. Goodrich, M. T., & Tamassia, R. (2019). *Introduction to Computer Security*. Pearson.
29. Dafoulas, G. A., & Maia, C. (2015). *Global Security, Safety, and Sustainability: Tomorrow's Challenges of Cyber Security*. Springer.

Tiešsaistes resursi un mājaslapas:

- Cybersecurity & Infrastructure Security Agency (CISA)
    - Mājaslapa: https://www.cisa.gov/
    - CISA nodrošina bagātīgus resursus par kiberdrošības labo praksi un draudiem, piedāvājot vadlīnijas, rīkus un brīdinājumus, kas ir nozīmīgi izglītībai un izpratnei.
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
    - Mājaslapa: https://www.nist.gov/cyberframework
    - NIST’s ietvars ir plaši pielietots standarts kiberdrošības risku pārvaldībai un tas nodrošina strukturētas vadlīnijas, kuras var iekļaut izglītojošās mācību programmās.
- Open Web Application Security Project (OWASP)
    - Mājaslapa: https://owasp.org/
    - OWASP ir tiešsaistes kopiena, ka piedāvā brīvi pieejamus resursus tīkla aplikāciju drošībai, ieskaitot rīkus, standartus un labo praksi.
- SANS Institute
    - Mājaslapa: https://www.sans.org/
    - Atzīts līderis kiberdrošības mācībās, SANS Institute piedāvā plašu spektru pētniecības publikāciju, mācību materiālu un drošības vadlīniju.
- Krebs on Security
    - Mājaslapa: https://krebsonsecurity.com/
    - Žurnālista Briana Krebsa vadīts blogs, kas sniedz padziļinātu ieskatu par drošības jaunumiem un izpēti, kas koncentrējas uz jaunākajiem draudiem un pārkāpumiem.
- Infosec Institute
    - Mājaslapa: https://resources.infosecinstitute.com/

- Infosec Institute nodrošina resursus un mācības par informācijas drošību, un piedāvājot ieskatu sniedzošas publikācijas un nozares jaunumus.

- The Hacker News
  - Mājaslapa: https://thehackernews.com/
  - Tiešsaistes kiberdrošības jaunumu žurnāls The Hacker News piedāvā jaunāko informāciju par kiberdrošības riskiem un inovācijām

- Bruce Schneier's Blog
  - Mājaslapa: https://www.schneier.com/
  - Brūss Šneiers ir pazīstams drošības tehnologs, kura blogs sniedz ieskatu digitālās pasaules drošības un privātuma problēmās.

3. Modulis: Ieviešana un uzturēšana

1. daļa – Digitālās higiēnas kultūras izveide jaunuzņēmumos un PIA organizācijās

Kas ir digitālās higiēnas kultūra?

Kā mēs esam atklājuši iepriekšējos moduļos, digitālās higiēnas termins pirmo reizi parādījās 2000. gadu sākumā, lai izskaidrotu drošu, organizētu un ētisku digitālo prakšu principus, kuru mērķis ir efektīvi aizsargāt sistēmas datus, privātumu un integritāti [1]. Šajā modulī mēs izpētīsim šo principu sistēmisko pielietojumu plašākā mērogā, pielāgotu PIA sniedzējiem visā Eiropā, un piedāvāsim ieteikumus, kā veidot labāku digitālās higiēnas kultūru, kas iedvesmos inovācijas un entuziasmu organizācijās.

Tātad, kas tieši ir digitālās higiēnas kultūra? Līdzīgi daudzām citām tīkla kultūrām, kas cenšas nodrošināt veiksmīgu organizāciju, vai tā būtu orientēta uz struktūru vai izpēti [2], digitālās higiēnas kultūra koncentrējas uz kopīgu domāšanas veidu. Šajā domāšanas veidā katrs dalībnieks tic organizācijas misijai un veido stratēģijas, kas balstītas uz kolektīvo atbildību un drošu digitālo prakšu integrāciju.

Izpētīsim, kā digitālās higiēnas kultūru var paplašināt no vadības līmeņa līdz darba grupām un līdz katram indivīdam.

Digitālās higiēnas kultūras attīstība vadības līmenī

Pēc Covid laikmetā, kad attālināts darbs ir kļuvis par jauno normu un ievainojamības digitālajā pasaulē var būt gan emocionālas, gan tehniskas [3] (piemēram, sociālās inženierijas uzbrukumi, kas var izpausties kā emocionāls stāsts, kas ir pikšķerēšanas mēģinājums), situācija prasa ne tikai vadītāju, bet līderi, kurš spēj efektīvi orientēties digitālās pasaules sarežģītībā, demonstrējot digitālās higiēnas prakses kā neatņemamu organizācijas vērtību daļu. Zemāk ir minēti daži svarīgi punkti, kuros līderis var veicināt drošu un atbalstošu digitālās higiēnas kultūru:

- **Veicināt organizatorisko elastību [4]:**

Līderiem jānodrošina, ka viņu organizācijas ir pielāgojamas digitālajiem uzlabojumiem, kā arī izaicinājumiem, kas var rasties digitālo prakšu dēļ. Lai vadītu savu komandu cauri šīm pārmaiņām, visiem līderiem vispirms jāizprot sava pozīcija, lēmumi un emocijas [5] dažādos apstākļos, pirms viņi motivē citus kopēja mērķa sasniegšanai.

- **Risināt vadības izaicinājumus [5]:**

Līderiem jebkurā organizācijā jāatpazīst potenciālie vadības izaicinājumi, kas var rasties digitalizācijas rezultātā, piemēram, kiberdrošības draudi, privātuma jautājumi, prasmju trūkums vai problēmas, ko rada attālināts darbs. Viņiem jābūt gataviem novērtēt savu komandu spējas uzturēt digitālo higiēnu. Tas prasa zināmu tehnisko kompetenci; tādēļ līderiem ieteicams saprast un efektīvi skaidrot tehniskos jautājumus savai komandai.

- **Attiecību veidošana un sadarbības procesi [6]:**

Līderiem jebkurā organizācijā vajadzētu veidot attiecības ar plašu ieinteresēto pušu loku gan iekšējā, gan ārējā līmenī. Tas prasa augstu koordinācijas un atbildības līmeni, kā arī uzņemties atbildību veicināt spēcīgu sadarbības sajūtu starp darbiniekiem un citām ieinteresētajām pusēm.

- **Ieguldījumi izglītībā un apmācībā [5]:**

Līderiem jebkurā organizācijā būtu jāiegulda nepārtrauktā sevis un savu darbinieku izglītošanā un apmācībā, lai sekotu jaunākajām digitālās higiēnas praksēm un tehnoloģijām. Dažas kiberdrošības kompānijas [7], kā arī dažas valdības iestādes Eiropā, piemēram, Eiropas Savienības Kiberdrošības aģentūra (ENISA), piedāvā dažādus tiešsaistes un klātienes kursus par kiberdrošības izpratni un krīzes vadību [8].

Digitālās higiēnas kultūras attīstība grupas līmenī

Pēc digitālās higiēnas stratēģijas ceļveža izstrādes, kiberdrošības jautājumi jebkurā organizācijā jāapspriež arī grupas līmenī. Darba grupas, tostarp departamenti, programmas, studenti vai projektu vadītāji, var būtiski veicināt digitālās higiēnas kultūras veidošanu savās iestādēs ar atbilstošo Datoru ārkārtas reaģēšanas komandu (CERT) atbalstu un sadarbību.

Zemāk ir minēti daži svarīgi punkti, kurus katra darba grupa var izmantot, lai veidotu digitālās higiēnas kultūru:

- **Efektīvas komunikācijas nodrošināšana grupās:**

Viens efektīvs komunikācijas veids grupām ir sākt sanāksmes vai kursus ar diskusijām par kiberdrošību. Katra grupa var atvēlēt piecas minūtes sanāksmes sākumā dalībnieku jautājumiem. Šo sanāksmju laikā var izstrādāt noteikumus un vadlīnijas par to, kā ierīces jāizmanto nodaļās vai klasēs, lai stiprinātu digitālās higiēnas kultūru [9].

Vēl viena noderīga metode grupām var būt prasība par elektroniskajiem parakstiem vai QR kodiem koplietotiem dokumentiem, kas var noteikt, vai e-pastu vai digitālu darījumu veic grupas dalībnieks [10]. Vēl viens faktors, kam jāpievērš uzmanība, ir drošāku informācijas glabāšanas iespēju izvēle, piemēram, mākoņkrātuve, nevis USB zibatmiņas [10].

- **Efektīvu dokumentēšanas metožu izveide digitālajiem uzbrukumiem:**

Digitālo uzbrukumu dokumentēšana ir kritisks aspekts kiberdrošības uzturēšanā. Visām organizācijām skaidri jāizskaidro vadlīnijas dokumentēšanai. Daži no procedūru posmiem digitālo uzbrukumu dokumentēšanai var būt šādi [11]:

Solis 1: Uzturēt organizētu žurnālu: Incidenta gadījumā mudiniet katru komandas dalībnieku iekļaut datus, piemēram, datumu, laiku, e-pasta adresi, svarīgās saites, lietotāju kontu vārdus un metadatus.

Solis 2: Ieviest strukturētas veidnes: Izmantojiet gatavas veidnes datu pārkāpumu incidentu dokumentēšanai. Piemēram, varat izmantot incidentu žurnāla veidni no Access Now, starptautiskas NVO, kas cenšas aizsargāt cilvēku digitālās pilsoņu tiesības visā pasaulē.

Solis 3: Izmantot dažādus dokumentēšanas formātus: Mudiniet komandas dalībniekus izmantot dažādus formātus savu problēmu dokumentēšanai. Viņi var izmantot Internet Archive's Wayback Machine, lai saglabātu tīmekļa lapu, vai izmantot video ierakstīšanas rīkus, lai ierakstītu video kā pierādījumu savām problēmām.

Solis 4: Droši glabāt informāciju: Izveidojiet rezerves kopijas savās ierīcēs, uzticamās glabāšanas vietās un, ja iespējams, aizsargājiet savus failus ar šifrēšanu.

- **Regulāru digitālās higiēnas novērtējumu izveide:**

Regulāru auditu un riska novērtējumu veikšana var palīdzēt identificēt ievainojamības un nodrošināt, ka digitālās higiēnas prakses tiek ievērotas [11]. Daži veidi, kā veidot regulārus digitālās higiēnas novērtējumus, ir šādi:

  - Izstrādāt kiberdrošības ieradumu rutīnu, piemēram, vīrusu skenēšanu, paroļu maiņu, programmatūras atjaunināšanu un cieto disku tīrīšanu [12].
  - Izmantot pareizos rīkus, piemēram, tīkla ugunsmūri, pretvīrusu programmatūru, šifrēšanu vai rezerves risinājumus [13].
  - Meklēt palīdzību no uzticamiem pakalpojumiem, kas nodrošina ievainojamību skenēšanu, tīmekļa lietojumprogrammu skenēšanu un pikšķerēšanas novērtējumus [14].

Digitālās higiēnas kultūras attīstība individuālā līmenī

Cilvēciskie faktori ir viena no vājākajām kiberdrošības sastāvdaļām. Daži cilvēku kļūdu piemēri digitālo prakšu kontekstā var ietvert sliktu paroļu pārvaldību, nejaušu datu dzēšanu vai kļūšanu par pikšķerēšanas vai citu sociālās inženierijas krāpšanas upuri. Tomēr vienmēr ir iespējams samazināt riskus, pievēršot uzmanību un ievērojot digitālās higiēnas prakses.

Šeit ir daži galvenie punkti, kur katrs indivīds var veicināt higiēnas kultūras veidošanu organizācijā:

- **Esi uzmanīgs ar savu digitālo pēdu [15]:**

Orientēšanās tiešsaistes vietnēs var būt sarežģīta, un cilvēkiem vajadzētu būt uzmanīgiem ar savu digitālo pēdu. Tīmekļa pārlūkprogrammu, e-pasta pakalpojumu sniedzēju, mobilo lietotņu, meklētājprogrammu un sociālo mediju platformu izsekošanas mehānismi var apdraudēt personisko privātumu. Lai uzlabotu drošību ikdienas tīmekļa pārlūkošanas aktivitātēs, apsveriet šos soļus:

Solis 1: Esi uzmanīgs ar informāciju, ko dalies sociālajās platformās, un izraksties no saviem sociālo mediju kontiem, jo sociālo mediju vietnes var veikt analītiku ar taviem kontiem pat tad, ja tu tos neizmanto [16].

Solis 2: Izmanto privātumu ievērojošus pārlūkus, piemēram, duckduckgo.com un startpage.com, kas prioritizē privātumu un nodrošina lietotājiem meklēšanas rezultātus bez personalizētas izsekošanas.

Solis 3: Esi informēts par savu sociālo loku tiešsaistes aktivitātēm [16]: Saproti, ka draugu un ģimenes tiešsaistes klātbūtne var ietekmēt tavu digitālo drošību. Sniedz viņiem padomus par drošām tiešsaistes praksēm.

Solis 4: Esi uzmanīgs ar sava viedtālruņa iestatījumiem: Līdzīgi kā ar portatīvajiem datoriem, arī tavi viedtālruņi ir svarīga tavu tiešsaistes aktivitāšu sastāvdaļa. Prioritizē drošību, regulāri izrakstoties no lietotnēm, kurās ir sensitīva informācija. Izrakstīšanās arī veicinās tavu darba produktivitāti. Pētījumā par viedtālruņu lietošanas monitorēšanu tika konstatēts, ka, izrakstoties un atsakoties no izsekošanas sīkfailiem, dalībnieki katrā sesijā pavadīja mazāk laika [17].

- **Pievērs uzmanību programmatūras atjauninājumiem:**

Bieži programmatūras atjauninājumi ir būtiski labas digitālās higiēnas uzturēšanai, jo nespēja atjaunināt programmatūru vai tīmekļa pārlūkus var radīt nopietnas ievainojamības.

Pavisam nesens piemērs, kas parāda programmatūras atjauninājumu nozīmi, radās 2021. gadā, kad Adobe paziņoja, ka pārtrauc Flash izmantošanu, lielā mērā drošības ievainojamību dēļ [18]. Apskatāmo drošības ievainojamību vidū bija iespēja efektīvi apiet tīmekļa pārlūka drošības pasākumus. Datoru ārkārtas reaģēšanas komandas (CERT) bija spiestas risināt šīs problēmas. Šis piemērs parāda, ka uzmanības pievēršana atjauninājumiem ir svarīga, lai aizsargātu savu programmatūru un lietotnes no ievainojamībām.

- **Izmanto stipras paroles [19]:**

Vājas paroles, kuras ir viegli uzminēt, var pakļaut indivīdus un organizācijas datu drošības riskam. Tādēļ neizmantojiet savu vārdu vai dzimšanas dienu kā paroli. Spēcīgākās paroles ir tās, kuras būs viegli atcerēties, bet grūti uzlauzt. Šeit ir daži padomi, kā izveidot stipras paroles un kā tās atcerēties [19]:

Solis 1: Konstruē teikumu ar dažādiem simboliem, kas ietver lielos un mazos burtus. Piemēram, teikumu "I Like Apples but I Hate Oranges" var pārvērst par "IL@bIH0".

Solis 2: Izmanto divfaktoru autentifikāciju: Papildus spēcīgu paroļu izveidei uzlabo savu drošību ar divfaktoru autentifikāciju (2FA). Autentifikācija pievieno papildu drošības slāni, pieprasot otro verifikācijas soli, piemēram, kodu, kas tiek nosūtīts uz tavu mobilo ierīci, tādējādi samazinot nesankcionētas piekļuves risku.

Solis 3: Paturi savas paroles konfidenciālas un, ja nepieciešams, glabā tās droši, izmantojot paroļu pārvaldnieku vai autentifikācijas lietotni, piemēram, Dashlane vai 1Password. (Tomēr atceries, ka šo pārvaldnieku drošība ir tikai tik stipra, cik vājākais posms!)

Solis 4: Nodrošini savu paroļu drošību, regulāri tās atjauninot.

- **Klikšķini apdomīgi [14]:**

Esi uzmanīgs pret pikšķerēšanu: Pikšķerēšanas mērķis ir apmānīt cilvēkus, lai viņi nodotu savu sensitīvo informāciju, uzdodoties par uzticamu avotu. Pikšķerēšana ir nopietns noziegums. Ja krāpniekiem izdodas apmānīt cilvēkus, lai tie nodotu personisko informāciju, viņi var piekļūt viņu e-pastiem, bankas kontiem vai sociālo mediju kontiem. Tādēļ, ja kaut kas šķiet mazliet neparasts, vai e-pasts lūdz tevi verificēt personisko informāciju, īpaši ar pielikumu vai saiti, kuru mudina klikšķināt, vispirms uzticies savam instinktam un padomā pirms klikšķināšanas.

2. daļa - Digitālās higiēnas prakses uzraudzība, revīzija un nepārtraukta uzlabošana

Domājiet par savu digitālo klātbūtni kā par vērtīgu aktīvu, piemēram, savu māju vai automašīnu. Tāpat kā jums būtu nepieciešamas regulāras apkopes sesijas, lai uzturētu savu automašīnu vai māju drošu un funkcionālu, tāpat arī digitālās higiēnas prakšu pārbaude ir svarīga, lai nepārtraukti uzturētu jūsu sistēmas drošas un funkcionālas. Šajā sadaļā mēs apskatīsim prakses, kuras jūs varat īstenot gan organizācijas, gan individuālā līmenī, lai uzturētu jūsu kompetences svaigas attīstoties tehnoloģijām.

Organizācijas līmeņa prakses

Šeit ir daži rīki un metodes, kas var būt noderīgi, lai uzraudzītu, novērtētu un uzlabotu jūsu digitālo higiēnu organizācijas līmenī.

- **Atrodiet jaunākos ES noteikumus:**

Jaunāko noteikumu izpratne un ieviešana palīdz institūcijām identificēt visaktuālākās problēmas un attiecīgi rīkoties, lai mazinātu draudus un izmantotu priekšrocības.

Viens no nopietnākajiem izaicinājumiem, kas satrauca politikas veidotājus, ir MI. 2023. gada 9. decembrī Eiropas Savienība ieviesa jaunu likumu, ko sauc par "MI aktu", kura mērķis ir "izmantot tehnoloģiju potenciālās priekšrocības, vienlaikus cenšoties aizsargāt pret iespējamiem riskiem, piemēram, darba vietu automatizāciju" [20]. Palikt informētam par jaunākajiem Eiropas Savienības noteikumiem par MI ir būtiski atbildīgas un autorizētas digitālās prakses ietvaros. Jūs varat pārskatīt atjauninātos noteikumus, piemēram, MI aktu, tiešsaistē no Eiropas Savienības likumdošanas lapas, lai nodrošinātu atbilstību vadlīnijām un izvairītos no iespējamiem juridiskiem sarežģījumiem.

- **Drošības pārbaudes:**

Visaptveroša drošības iestatījumu pārskatīšana ir būtiska, lai uzraudzītu jūsu digitālās higiēnas vadlīniju efektivitāti. Jūs varat izmantot Google un Facebook regulārās drošības pārbaudes, kas palīdz jums iziet cauri privātuma pasākumiem, atļaujām un kontrolei pār jūsu jaunākajām aktivitātēm. Jūs varat arī izmantot tiešsaistes resursus, kas ļauj jums meklēt dažādus datu pārkāpumus, piemēram, haveibeenpwnd.com, lai apzinātos riskus un datu pārkāpumu biežumu.

- **SVID analīze:**

SVID ir akronīms no Stiprās puses, Vājās puses, Iespējas un Draudi, un tā ir stratēģiska analīzes metode, kas izveido ceļvedi, lai noteiktu jebkuras organizācijas pozīciju un stratēģijas turpmākai attīstībai. Šeit ir daži padomi, kas jāņem vērā, veicot SVID analīzi jūsu organizācijā, saskaņā ar pētījumu par uzņēmumu e-gatavību [21]:

1. **Sagatavošanās SVID analīzei:**
    a. SĀKT AR MĒRĶI: Apsveriet mērķi un ilgtermiņa sekas, piemērojot SVID analīzi.
    b. DEFINĒJIET ANALIZĒJAMĀS JOMAS: Identificējiet konkrētas jomas, kas saistītas ar digitālās higiēnas kultūru, piemēram, darbinieku informētību, drošības protokolu ievērošanu, infrastruktūru utt.
    c. NOZĪMĒJIET KOMANDAS DEFINĒTAJĀS JOMĀS: Izveidojiet komandas, kas ir eksperti analizējamajās jomās, un nodrošiniet, lai visas dažādās komandas būtu darbotos saskaņoti ar analīzes veikšanas metodoloģiju.
2. **Stiprās un vājās puses analīze:**
    a. IDENTIFICĒJIET SAVAS STIPRĀS UN VĀJĀS PUSES: Organizācijas stiprās un vājās puses ir iekšējo faktoru rādītāji, kas parāda šīs organizācijas efektivitāti un neefektivitāti. Ir svarīgi iekļaut pamatojumus par lēmumiem, lai konkrēts faktors tiktu uzskatīts par vājumu. (Piemēram, novecojušas lietojumprogrammas var tikt uzskatītas par vājumu, jo tās padara sistēmas viegli ievainojamas uzbrukumiem).
    b. NOSKAIDROJIET IDENTIFICĒTO JAUTĀJUMU RELEVANCI: Noteikt, kas ir vājums un kas ir stiprā puse, var būt sarežģīti. Pētnieki iesaka [21] izmantot "100 punktu metodi", lai novērtētu un prioritizētu tos. Katrs komandas dalībnieks var piešķirt 100 punktus stiprajai vai vājajai pusei, un jo vairāk punktu piešķirts, jo nozīmīgāka tā ir. Pēc tam, kad visi ir piešķīruši savus punktus, komanda nosaka vidējo vērtību, lai noteiktu to kopējo svaru.
3. **Iespēju un draudu analīze:**
    a. Novērtējiet draudu relevanci un iespējamību, mēģinot tos organizēt šādās kategorijās: ekonomiskie, sociālie, politiskie, tehnoloģiskie un vides draudi.
    b. Novērtējiet iespējas, kas saistītas ar attīstības virzieniem. Tās varētu būt finanšu resursi, pieaugoša sabiedrības interese vai starptautiskās iespējas.
4. **SVID matricas izveide:** Izvēlieties stiprās puses, vājās puses, iespējas un draudus un grupējiet tos atbilstoši vislielākajai svaram jūsu organizācijas digitālās higiēnas kultūrai. Izstrādājiet rīcības plānus, pamatojoties uz identificētajām stratēģijām, kas varētu: (1) koncentrēties uz vājumu novēršanas izmanojot iespējas, (2) koncentrēties uz stiprās puses izmantošanu, lai gūtu labumu no iespējām, (3) koncentrēties uz vājuma mazināšanu, lai izvairītos no draudiem, vai (4) koncentrēties uz stipro pušu izmantošanu, lai novērstu draudus.
5. **Pārskatiet rezultātus:** Regulāri pārskatiet īstenoto stratēģiju progresu un periodiski atkārtojiet SVID analīzi, lai pielāgotos jaunajiem attīstības virzieniem digitālajā vidē.

- **Regulāras rezerves kopijas:**

Rezerves kopijas ir būtiskas, kad nepieciešams atjaunot sensitīvu informāciju, piemēram, paroles zuduma, tehnisku incidentu utt. gadījumā. Dažreiz sistēmas avārijas cēloņu uzraudzīšana ir iespējama arī, pārskatot sistēmas drošības ievainojamības vai kļūdas. Atvērtā pirmkoda rezerves kopiju sistēmu, piemēram, UrBackUp izmantošana, kas ļauj jums glabāt savu dokumentu kopijas, var būt vērtīgs rīks, lai uzraudzītu un pārskatītu jūsu digitālās higiēnas prakses ārkārtas situācijās.

Indivīda līmeņa prakses

Katrs indivīds spēlē nozīmīgu lomu digitālās higiēnas prakses attīstīšanā, un ir iespējami daudzi soļi, lai pārskatītu, uzraudzītu un attīstītu esošās prakses. Šeit ir daži veidi, kā uzlabot savu digitālo higiēnu individuālā līmenī.

- **Zināšanas un izglītība:**

Digitālās pratības apguve nenozīmē tikai zināt rīkus un metodes, bet arī izprast pastāvīgi mainīgo tehnoloģisko ainavu. Iepazīt tiešsaistes draudus un sekot līdzi jaunumiem, var piedaloties nepārtrauktās mācību iespējās, piemēram, Microsoft Digital Literacy kursi, kuros dalībnieki var apgūt digitālās pratības pamatus, piemēram, darbu ar datoru, kā arī augstāka līmeņa prasmes, piemēram, satura radīšanu tiešsaistē. Tāpat pētnieki [22] norāda uz mediju pratības un drošas un atbildīgas interneta lietošanas mācīšanas nozīmi, kas būtu jāatspoguļo indivīdu reālās dzīves pieredzēs un interesēs.

- **Atbildīga uzvedība tiešsaistē:**

Mūsu uzvedībai tiešsaistē ir reālas sekas. Kā uzsvērts akadēmiskajos pētījumos [23], ir svarīgi tiešsaistē iesaistīties ētiski un būt digitāli prasmīgam. Atbildīga uzvedība tiešsaistē nozīmē piedalīties diskusijās ar cieņu un jūtīgumu. Turklāt digitālo politiku izpratne veicina drošāku un cieņpilnākas tiešsaistes kopienas veidošanos. Ja neesat pārliecināts, vai jūsu digitālās darbības ietver labas prakses, varat izmantot Mičiganas Universitātes "Labā digitālā pilsoņa" ceļvedi.

- **Pārskatīšana un pielāgošanās:**

Līdzīgi kā jebkurš digitālās pasaules aspekts, tehnoloģiskā ainava ir dinamiska un prasa no mums nepārtraukti pielāgot savas prakses. Tādēļ, digitālo darbību pārskatīšana, pielāgošanās krāpniecības mēģinājumiem, pikšķerēšanas mēģinājumu atpazīšana un uzmanīšanās kādu informāciju lejuplādē, ir būtiski aspekti, lai uzturētu drošību tiešsaistē. Rīks, kas var palīdzēt jums pārskatīt prakses un regulāri tās atjaunināt, ir Digitālās kompetences ietvars (DigComp). Tas ir atsauces rīks institūcijām, indivīdiem un izglītotājiem, ko izstrādājusi ES un kas tiek regulāri atjaunināts (šīs rokasgrāmatas publicēšanas datumā pēdējā versija ir 2.2). DigComp ir pieejams ES publikāciju vietnē.

Regulāri DigComp atjauninājumi nodrošina, ka ietvars paliek aktuāls un atspoguļo pašreizējo digitālo vidi. Tāpat kā DigComp, jūs varat pārskatīt un atjaunināt savas digitālās higiēnas prakses, lai nodrošinātu, ka tās atbilst pašreizējām jūsu organizācijas vajadzībām, un apsvērt prasmes, kas saistītas ar jaunajām tehnoloģijām.

3. daļa - Digitālās higiēnas nākotnes: izaicinājumi un iespējas

Ieejot nākotnē, mēs varam sagaidīt jaunus izaicinājumus un iespējas tehnoloģisko attīstību jomā. Digitālo tehnoloģiju mainīgā ainava, īpaši mākslīgais intelekts, iegūstot jaunas spējas un prasmes (MI), rada jaunus sarežģījumus. Šo sarežģītību un iespēju izpratne ir būtiska, lai nodrošinātu drošu un inovatīvu pieredzi visiem. Šajā vienībā mēs aplūkosim dažus no visaktuālākajiem jautājumiem par digitālās higiēnas nākotni, īpaši koncentrējoties uz jaunajām tehnoloģijām un to, ko tās varētu piedāvāt inovāciju jomā.

A-Jaunās tehnoloģijas

Vairākas jaunās tehnoloģijas, piemēram, blokķēdes, robotika, lietu internets (IoT), papildinātā realitāte (AR) un virtuālā realitāte (VR) ir paredzētas, lai veidotu nākotni. Starp šīm tehnoloģijām, ģeneratīvie MI čatboti, piemēram, ChatGPT, ir izpelnījušies vislielāko uzmanību kopš to izveides 2022. gadā. MI pieaugums piešķir jaunas dimensijas digitālajai higiēnai un kiberdrošībai. MI tehnoloģijas jau var "atbildēt uz jautājumiem, rakstīt dzeju, ģenerēt datora kodu un sarunāties" [24]. Daži eksperti uzskata, ka MI apdraudēs daudzu darbinieku darba vietas, jo darbi tiks automatizēti [25], savukārt daudzas kompānijas jau izmanto ģeneratīvo MI savās praksēs [26]. Tātad, kā profesionālās izglītības iestādes, piemēram, PIA organizācijas, varētu gūt labumu no MI iespējām?

- **Mācību pieredzes uzlabošana:**

Profesionālās izglītības un apmācības jomā ģeneratīvajam MI varētu būt liels potenciāls revolucionizēt mācību pieredzi. Pētnieki liecina, ka MI var radīt reālistiskus scenārijus, simulācijas vai novērtējumus, kas atbilst studentu vajadzībām, interesēm un spējām [27]. Reālistiski scenāriji var piedāvāt praktisku, visaptverošu pieredzi, kas var būt izšķiroša tādās jomās kā veselības aprūpe. Papildus tam, veselības aprūpes izglītība var ievērojami gūt labumu no rutīnas uzdevumu optimizēšanas, diagnožu veidošanas vai personalizētas medicīnas piedāvāšanas, kas pieprasa diskusiju par privātuma un stipras pārvaldības nodrošināšanu [28].

- **Mācīšanas un novērtēšanas uzlabošana:**

Pielāgojoties nozares tendencēm un integrējot MI PIA mācīšanā un novērtēšanā, tas var palīdzēt pasniedzējiem optimizēt viņu darba plūsmu. NVO un starptautiskās organizācijas jau pēta iespējas uzlabot studentu darba precizitāti, pilnvērtību un vispārējo kvalitāti, kas var arī nodrošināt tūlītēju atgriezenisko saiti [29]. Tāpat kā veselības aprūpes izglītībā, MI spēja novērtēt studentu darbu noteikti izraisīs diskusijas par MI ētiku, kas ir svarīgs diskusijas punkts, kuru skolotājiem un vecākiem vajadzētu ņemt vērā.

- **Pielāgojamas mācību pārvaldības sistēmas:**

Mācību pārvaldības sistēmas (angliski Learning Management Systems (LMS)) jau ir paplašinājušas PIA skolotāju iespējas, piedāvājot mācību un mācīšanas materiālus vienā vietā, kā arī izsekojot studentu progresam un sniegumam [30]. Ar MI LMS ir palielinājusi iespēju revolucionizēt LMS [31]. Ar MI darbinātās LMS var veidot uzlabotus uzdevumus, kas pārsniedz automatizāciju, piemēram, prognozējot studentu sniegumu, tādējādi ļaujot skolotājiem izveidot stratēģijas studentu snieguma uzlabošanai [32].

B-Regulatīvie izaicinājumi

Iepriekšējās nodaļās mēs jau esam izpētījuši, kā jauni tehnoloģiskie sasniegumi kļūst par pārmaiņu veicinātājiem dažādās nozarēs un izglītības sistēmās. Šie sasniegumi prasa, lai visi iesaistītie būtu atbildīgi un veicinātu drošāku jaunās tehnoloģijas izmantošanu. Problēmas, piemēram, datu privātums, algoritmu neobjektivitāte, ētiska izmantošana un atbildība, prasa visaptverošus regulējošos ietvarus.

- **Datu privātums izglītībā**

Izglītības kontekstā, īpaši tiešsaistes izglītībā, kur tiek apstrādāti lieli datu apjomi, pastāv bažas par privātumu un drošību [33]. Neatļauta piekļuve mākonim vai sensitīvas informācijas ļaunprātīga izmantošana rada ievērojamus riskus izglītības iestādēm, un kopš 2018. gada Eiropas Savienības Vispārīgā datu aizsardzības regula (GDPR) prasa, lai visas iestādes ES un ārpus tās ievērotu tās prasības personisko datu aizsardzībai un pārvietošanai [34]. Tādēļ katrai PIA iestādei ir ieteicams uzraudzīt savu atbilstību GDPR un piemērot nepieciešamos pasākumus, attīstoties regulai.

- **Algoritmu neobjektivitāte**

Ar MI darbināta LMS var pārmantot neobjektivitāti no datiem, ar kuriem tā ir apmācīta. Nodarbinātības kontekstā, MI darbināti nodarbinātības procesi var būt īpaši kaitīgi dažām grupām, kā atklājās Amazon darbā pieņemšanas procesā, kur prognozēšanas sistēma tika apmācīta ar lielāko daļu vīriešu kandidātu CV. Tas radīja neobjektivitāti, kurā vīriešu kandidāti guva priekšroku pār sieviešu kandidātēm [35]. Arī skolotājiem būtu jāapzinās šis MI sistēmu aspekts un jāpārbauda savas iespējams neobjektīvā uzvedība attiecībā uz studentiem. Arvien svarīgāk ir, lai politikas veidotāji veicinātu auditējamu un caurspīdīgu algoritmu izstrādi [36].

- **Jauno tehnoloģiju ētika**

Līdzīgi kā bažas par algoritmu neobjektivitāti, jaunās tehnoloģijas, piemēram, MI, integrēšana izglītībā rada būtiskus jautājumus. Kāda būtu jauno tehnoloģiju loma izglītībā lēmumu pieņemšanā? Vai pastāv būtiskas atšķirības starp dažādām studentu grupām attiecībā uz to, kā jaunās tehnoloģijas ietekmē viņu mācīšanos?

MI kontekstā pētnieki uzskata privātumu, neobjektivitāti, uzraudzību un autonomiju par galvenajām jomām, kas norāda uz ētiskiem izaicinājumiem šo sistēmu izmantošanā izglītībā [37]. Šīs jomas, kā arī iepriekš minētie jautājumi prasa vairāk profesionālās attīstības iespēju skolotājiem, lai izglītotu nākamās paaudzes par MI

ētisku izmantošanu un izstrādi. Šajā kontekstā tādas iniciatīvas kā ES Digitālās kompetences ietvars (DigComp) var kalpot kā vērtīgs ceļvedis. Atzīstot ētiskā MI izmantošanas veicināšanas nozīmi, izpildvaras lēmumu pieņēmēji, piemēram, Eiropas Padome, jau ir procesā, lai definētu ētikas vadlīnijas un veicinātu caurspīdību, kas nodrošinās tehnoloģiju uzņēmumu atbildības uzņemšanos. Papildus iepriekš minētajam MI aktam, Eiropas Savienība arī izstrādā politikas, lai atbalstītu un veicinātu jauno tehnoloģiju, piemēram, VR, robotikas un biotehnoloģijas izmantošanu, kas, kā paredzams, būtiski ietekmēs pilsoņu dzīvi [38].

C-Iespējas inovācijām

Saskaņā ar 2021. gada OECD ziņojumu, virtuālā realitāte, papildinātā realitāte, robotika un mākslīgais intelekts kļuva arvien izplatītāki PIA dažādās nozarēs, piemēram, loģistikā, lauksaimniecībā, viesmīlībā, enerģētikā un informācijas tehnoloģijās, un tuvākajos gados tie kļūs vēl izplatītāki [39]. Šajā sadaļā mēs aplūkosim, kā dažādas nozares jau izmanto šīs tehnoloģijas un kādas iespējas tās piedāvā nākotnē.

- **Informācijas tehnoloģijas (IT)**

Jaunās tehnoloģijas, piemēram, virtuālās realitātes mākoņa laboratorijas, var nodrošināt IT studentiem praktisku pieredzi dažādās jomās, piemēram, tīkla konfigurācijā vai kiberdrošībā [40]. Kiberdrošības laboratorijas simulē kiberdraudus un uzbrukumus, piedāvājot PIA studentiem praktisku vidi, lai izprastu digitālo sistēmu ievainojamības, nepakļaujot sevi reālās pasaules riskiem. Sistēmas, piemēram, augstas veiktspējas skaitļošana, kā arī blokķēde, piedāvā jaunus apmācību veidus kiberdrošības jomā [41].

- **Loģistika un transports**

Komercprodukti, piemēram, simulācijas spēles, var palīdzēt studentiem risināt reālās pasaules izaicinājumus, un loģistikas gadījumā komerciāli pieejama spēle Truck & Logistics Simulator to nodrošina, kur studenti var veikt loģistikas uzdevumus no sākuma līdz beigām [39]. Tā kā tehnoloģija spēlē izšķirošu lomu sarežģītu uzdevumu plānošanā, PIA nodrošinātājiem, skolotājiem un studentiem ir jāievēro laba digitālā higiēna un jāsaglabā informācijas integritāte loģistikas tīklos, daloties ar komercializētiem produktiem.

- **Lauksaimniecība**

No droniem līdz MI, jaunajām tehnoloģijām ir potenciāls palielināt lauksaimniecības un lauksaimniecības prakses produktivitāti, samazināt ietekmi uz vidi un nodrošināt augstāku ienākumu līmeni. Augstas izšķirtspējas dronu apsekojuma modeļi var radīt efektīvāku apūdeņošanas plānošanu un precīzāku kultūraugu un lopu uzraudzību [42]. Tāpat AR var tikt izmantota, lai veicinātu viedās lauksaimniecības attīstību [43], kas mērķē uz riska mazināšanu, ražas palielināšanu un stresa mazināšanu agro biznesā [44]. Tomēr nevar aizmirst par riskiem, kas saistīti ar šo tehnoloģiju izmantošanu [45]. Uzturot labu kiberdrošību un iekļaujot atbildīgu MI praksi, var mazināt MI, AR un citu jauno tehnoloģiju izmantošanas riskus.

- **Viesmīlība**

Viesmīlība ir viena no nozīmīgākajām nozarēm daudzās Eiropas valstīs, kas veicina ekonomiku, nodrošinot miljoniem darba vietu. Jaunās tehnoloģijas var piedāvāt ieskaujošas mācību pieredzes viesmīlības un tūrisma studentiem. Viesnīcu vadības simulācijas un klientu apkalpošanas scenāriji, ko nodrošina lietu internets (IoT), kas ļauj kontrolēt telpu temperatūru, apgaismojumu un citas funkcijas, var radīt labāku pieredzi viesiem [46]. VR mācību modeļi, kurus izmanto ar īpašu aprīkojumu, jau tiek izmantoti nozares vadošajiem viesmīlības līderiem [47]. Simulētās pasaules pieredze var palīdzēt cilvēkiem mācīties ātrāk, saglabāt zināšanas ilgāk un būt vairāk iesaistītiem apmācībā [48]. Lai gan šie attīstības uzlabojumi uzlabo lietotāju pieredzi, tie var arī būt traucējoši un dezorientējoši dažiem lietotājiem. Tāpēc ir svarīgi apsvērt lietotāja interfeisu un lietotāja pieredzi, ieviešot izmaiņas [49].

- **Atjaunojamā enerģija**

Jaunās tehnoloģijas, piemēram, MI darbinātas prognozēšanas uzturēšanas sistēmas, savienotie sensori un papildinātā realitāte var paātrināt atjaunojamās enerģijas izmantošanu [50], vienlaikus simulējot saules paneļu, vēja turbīnu vai hidroelektrostaciju darbību un uzturēšanu, ļaujot studentiem iegūt praktiskas prasmes kontrolētā vidē [51]. Tāpat kā lauksaimniecības sektorā, jauno tehnoloģiju izmantošana rada ievērojamus riskus, kas padara digitālās higiēnas prakses par svarīgu elementu sistēmu aizsardzībā [52].

Inovatīvo tehnoloģiju, piemēram, robotu, virtuālās realitātes (VR), papildinātās realitātes (AR) un simulatoru izmantošana ļauj skolotājiem attīstīt studentu profesionālās prasmes, vienlaikus veicinot viņu digitālās un personiskās prasmes. Šīs tehnoloģijas, visticamāk, kļūs izplatītākas PIA organizācijās tuvākajos gados, jo tām ir priekšrocības attiecībā uz elastību, izmaksām un drošību [39]. Labas digitālās higiēnas mācīšana ir būtiska, lai drošā, veselīgā, atbildīgā un cieņpilnā veidā integrētu digitālās tehnoloģijas mūsu dzīvē [9].

4. daļa – Digitālās higiēnas kultūras labās prakses gadījumi

Iepriekšējās sadaļās mēs aplūkojām svarīgos aspektus, kā veidot spēcīgu digitālās higiēnas kultūru gan jaunizveidotajos uzņēmumos, gan PIA organizācijās. Mēs izpētījām uzraudzības, pārskatīšanas un nepārtrauktas digitālās higiēnas prakšu uzlabošanas nozīmi, lai nodrošinātu drošu un efektīvu digitālo vidi. Šajās diskusijās tika uzsvērta labas digitālās higiēnas kultūras veidošanas nozīme. Tagad, kad mēs pārejam uz pēdējo 3. moduļa daļu, 4. daļā, mēs iedziļināsimies reālas pasaules pielietojumos ar piemēriem, kas parāda digitālās higiēnas principu praktiskos lietošanas gadījumus.

Pasaules digitālās higiēnas labās prakses gadījumi

- **Specializēta rīkkopa digitālās higiēnas prakses veicināšanai (Serbija)**

Viens ievērojams piemērs labas digitālās higiēnas prakses pielietošanā ir Belgradā bāzēta fonda Share Cert sagatavotais ceļvedis, kas uzsver stratēģiskus kiberdrošības pasākumus [53]. Sistematizēti kategorizējot visizplatītākos draudus un drošības pasākumus, šis ceļvedis tiek atbalstīts ar atvērtu platformu, kur indivīdi un organizācijas var iegūt informāciju par aktuālākajiem jautājumiem digitālajā vidē un saņemt vispārīgus padomus par digitālās higiēnas kultūru.

- **Sabiedrības informētības kampaņas digitālo tiesību aizsardzībai (Grieķija)**

Vēl viena svarīga iniciatīva digitālo tiesību aizsardzības jomā ir bāzēta Grieķijā un tā ir nevalstiska organizācija (NVO) Homo Digitalis, kas koncentrējas uz privātuma tiesībām, personas datu aizsardzību, diskriminācijas aizliegumu digitālajā telpā un informācijas brīvību. Ar vairāk nekā 100 biedriem viņi aktīvi piedalās pētījumos un veic izmeklēšanas sabiedrības labā, kas savukārt var palīdzēt likumdevējiem labāk izprast jautājumus, kas saistīti ar digitālajām tiesībām [54].

- **Ātrās reaģēšanas komplekts arvien digitalizētākai pilsoniskajai sabiedrībai (globāls)**

Starptautiskie Datoru ārkārtas reaģēšanas komandu (CERT) un Ātrās reaģēšanas tīkla (RaReNet) tīkli ir sadarbojušies, lai palīdzētu ātrās reaģēšanas speciālistiem, digitālās drošības treneriem un tehnoloģiski prasmīgiem aktīvistiem labāk pasargāt sevi no visbiežāk sastopamajiem digitālajiem ārkārtas gadījumiem ar tā saucamo Digitālo pirmās palīdzības komplektu, kas sniedz vadlīnijas dažādu problēmu risināšanai [55]. Pieejams 13 valodās un pastāvīgi attīstās ar ārēju ieguldījumu, Digitālais pirmās palīdzības komplekts ir vērtīgs resurss atbildīgas un drošas interneta lietošanas veicināšanai.

- **Noturīgu rīku izveide, lai sekotu digitālās higiēnas praksēm pilsoniskajā sabiedrībā (globāls)**

Digitālās noturības centrs ir bezpeļņas organizācija, kas darbojas vairāk nekā 20 valstīs, lai izveidotu noturīgas digitālās sistēmas, nodrošinot pilsoniskās sabiedrības drošību [56]. Viņu projekti ietver pakalpojumu un rīku nodrošināšanu, piemēram, kopfinansēšanas rīku nepatiesas informācijas identificēšanai un ziņošanai, digitālo platformu drošības jautājumu ziņošanai, vizualizācijas rīku draudu un uzbrukumu digitālajām sistēmām monitorēšanai un kopienas rīku, lai izveidotu spēcīgu dalības tīklu CiviCERT ietvaros.

- **Tīkli, kas atvieglo reaģēšanas komandu apmaiņu globāli, lai sekotu digitālās higiēnas praksēm pilsoniskajā sabiedrībā (globāls)**

CiviCERT ir tīkls, kas apvieno CERT, neatkarīgos interneta satura un pakalpojumu sniedzējus, kā arī NVO un indivīdus [57]. Tīkla dalībnieki veic, koordinē un atbalsta digitālās drošības incidentu, kas viņiem tiek ziņoti, apstrādi sadarbības mehānismā, kur nepieciešams citu partneru viedoklis. Pats CiviCERT ievēro labas digitālās higiēnas prakses, kur locekļi sazinās, izmantojot šifrētas platformas, piemēram, šifrēto e-pasta sarakstu un ļaunprogrammatūras informācijas apmaiņas platformu, lai dalītos ar informāciju par jauniem draudiem pilsoniskajai sabiedrībai un veidnēm, lai nodrošinātu uzticamas un standartizētas procedūras ārkārtas situāciju risināšanai.

- **Digitālo cilvēktiesību veicināšana attīstības valstīs (Rietumāzija un Ziemeļāfrika)**

SMEX ir NVO, kas aizstāv cilvēktiesības digitālajā vidē Rietumāzijā un Ziemeļāfrikā [58]. Digitālās higiēnas prakšu kontekstā viņi piedāvā atbalstu interneta lietotājiem, aktīvistiem un cilvēktiesību organizācijām viņu kiberdrošības problēmu risināšanai un izveido programmas, lai informētu sabiedrību par regulām un interneta tiesībām. SMEX arī aktīvi sadarbojas ar vietējiem un starptautiskiem partneriem, lai veicinātu izpratni un īstenotu digitālās higiēnas prakses, veicinot drošāku tiešsaistes vidi indivīdiem un organizācijām, kas aizstāv cilvēktiesības digitālajā telpā Rietumāzijā un Ziemeļāfrikā.

- **Digitālo prasmju mācību programma K-12 skolēniem (Ziemeļamerika)**

Digitālās higiēnas jēdziens kļūst arvien nozīmīgāks izglītības sistēmās visā pasaulē. Viena no organizācijām, kas specializējas digitālās pratības materiālu sagatavošanā K-12 skolēniem, ir Common Sense Media, neatkarīga organizācija, kas atrodas Ziemeļamerikā un kuras mērķis ir palīdzēt skolēniem, vecākiem un skolotājiem ar datos balstītiem ieskatiem par mediju un digitālās vides ietekmi uz bērnu fiziskajām, emocionālajām, sociālajām un mentālajām vajadzībām [59]. Viņu pētījumos balstītā Digitālā pilsonība mācību programma risina svarīgus mediju un tehnoloģiju jautājumus skolās, piemēram: Kā aizsargāties pret iebiedēšanu? Kā aizsargāt mūsu privātumu? Kā orientēties dezinformācijā?

- **Izglītojoši materiāli labākai digitālajai pratībai (Ziemeļamerika)**

Digitālās pratības centrs ir Amerikas bezpeļņas organizācija, kuras mērķis ir veicināt pētījumus un atvērtā koda materiālu radīšanu [60], kā arī mācību programmu dizaina rīkus, nodarbības, aktivitātes un novērtējumus, kurus var izmantot un pielāgot dažādiem izglītības kontekstiem [61]. Mediju pratība ir svarīga digitālās higiēnas prakses sastāvdaļa, un uzsvars uz mediju pratību ne tikai uzlabo digitālo higiēnu, bet arī veicina informētāku un apdomīgāku sabiedrību, kas labāk sagatavota iesaistīties digitālās pasaules sarežģījumos.

- **Eiropas kiberdrošības mēnesis (Eiropa)**

Katru gadu oktobris tiek atzīmēts kā Eiropas kiberdrošības mēnesis (angliski The European Cyber Security Month (ECSM)), svarīgs ikgadējs pasākums, ko organizē Eiropas Savienības Kiberdrošības aģentūra (ENISA) un Eiropas Komisija [62]. Veltīts kiberdrošības informētības stiprināšanai starp ES pilsoņiem un organizācijām, ECSM ir viena no daudzajām ES daudzdimensionālajām pieejām, lai veicinātu labas digitālās higiēnas prakses. Visu oktobri konferences, semināri un tīmekļa semināri veido plašu kampaņu, kas ne tikai palielina izpratni par kiberdrošību, bet arī aktīvi dalās ar atjauninātu informāciju un ekspertu padomiem. Aicinot veicināt drošāku interneta lietošanu, ECSM sniedz digitālās higiēnas padomus un izceļas kā visaptveroša un sadarbības iniciatīva, līdzīga globāliem tīkliem, piemēram, CiviCERT, un reģionālām NVO, piemēram, SMEX, spēlējot būtisku lomu labas digitālās higiēnas prakšu veicināšanā un uzturēšanā visā Eiropas Savienībā.

- **Kiberdrošības spēle pirmsskolas vecuma bērniem (globāls)**

Interland [63] ir interaktīva spēle, ko piedāvā Google, un tā ir daļa no programmas "Be Internet Awesome" [64], kas veicina digitālās higiēnas prakses bērnu un jauniešu mācībās. Kā dinamiska un interaktīva spēle, Interland iesaista skolēnus ar savu spēli, piedāvājot praktisku pieeju labas digitālās higiēnas prakses galveno aspektu mācīšanai, izmantojot spēļošanu [65]. Sarežģīti jautājumi, piemēram, privātums, pikšķerēšana, uzlaušana un kibermobings, tiek tulkoti jaunākiem skolēniem krāsainās animācijās, kas ir piemērotas viņu kompetences līmenim [66]. Kopumā Interland ir ievērojams piemērs labas digitālās higiēnas prakses ieaudzināšanai no jauna vecuma, izmantojot tehnoloģijas.

Šajā modulī mēs apspriedām labas digitālās higiēnas prakšu ieviešanu un nozīmi. Mēs aplūkojām tādus tematus kā digitālās higiēnas kultūras veidošana jūsu organizācijā dažādos vadības līmeņos, prakšu nepārtraukta uzlabošana, informētība par nākotnes iespējām un izaicinājumiem, un izpētījām gadījumus no visas pasaules. Apskatiet šīs rokasgrāmatas citus moduļus, lai iegūtu papildu padomus un stratēģijas par labām digitālās higiēnas praksēm, un apmeklējiet tīmekļa vietni "Good Digital Hygiene for Startups".

Avoti

1. daļa – Digitālās higiēnas kultūras izveide jaunuzņēmumos un PIA organizācijās

[1] Boulet, C. (2006). Digital Hygiene: Clean Living on a Dirty Network. *Interface: The Journal of Education, Community, and Values 6(3).* Retrieved from: Digital Hygiene: Clean Living on a Dirty Network (core.ac.uk) [Access Date 05.12.2023]

[2] Groysberg, B., Lee, J., Price, J., & Cheng, J. Y.-J. (2018, January-February). The leader's guide to corporate culture. *Harvard Business Review.* Retrieved from: The Leader's Guide to Corporate Culture (hbr.org) [Access Date 05.12.2023]

[3] Trevors, M. (2017). Cyber hygiene: 11 essential practices. Software Engineering Institute Blog. Retrieved from https://insights.sei.cmu.edu/blog/cyber-hygiene-11-essential-practices/ [Access Date 05.12.2023]

[4] Ly, B. The Interplay of Digital Transformational Leadership, Organizational Agility, and Digital Transformation. J Knowl Econ (2023). https://doi.org/10.1007/s13132-023-01377-8

[5] Harvard Business School Online. (n.d.). *How to Become a More Effective Leader.* Harvard Business School Publishing. Retrieved from https://info.email.online.hbs.edu/leadership-ebook

[6] Cortellazzo, L., Bruni, E., & Zampieri, R. (2019). The role of leadership in a digitalized world: A review. *Frontiers in Psychology,* 10, 1938. https://doi.org/10.3389/fpsyg.2019.01938

[7] Cisco. (n.d.) Cisco Learning Network Store. Retrieved from https://learningnetworkstore.cisco.com/

[Access Date 06.12.2023]

[8] European Union Agency for Cybersecurity (ENISA). (n.d.). Online training material for cybersecurity specialists: Technical and operational. ENISA. Retrieved from https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#identification_handling [Access Date 06.12.2023]

[9] Sklar, A. (2017). Sound, smart, and safe: A plea for teaching good digital hygiene. *LEARNing Landscapes Journal*, 10(2). https://doi.org/10.36510/learnland.v10i2.799 [Access Date 06.12.2023]

[10] Glazer, K. (2017, March 22). A quick guide to good digital hygiene. *Literacy Now*. Retrieved from https://www.literacyworldwide.org/blog/literacy-now/2017/03/22/a-quick-guide-to-good-digital-hygiene

[Access Date 06.12.2023]

[11] Documenting Digital Attacks (n.d). Digital First Aid. Retrieved from https://digitalfirstaid.org/documentation/

[12] Saraf, A. (2021, May 14). Three steps to healthy digital hygiene. *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/05/14/three-steps-to-healthy-digital-hygiene/

[Access Date 11.12.2023]

[13] Kaspersky. (n.d.). Cyber hygiene habits: 11 ways to improve your security. Retrieved from https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

[14] Cybersecurity and Infrastructure Security Agency (CISA). (2022). 4 things you can do to keep yourself cyber safe. Retrieved from https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe [Access Date 11.12.2023]

[15] CHAYN. (2018). *Do it Yourself Online Safety.* Retrieved from https://chayn.gitbook.io/diy-online-safety/english [Access Date 07.12.2023]

[16] Torbet, G. (2019, February 3). Social media sites can predict your behavior even if you don't use them. *Digital Trends.* Retrieved from https://www.digitaltrends.com/social-media/social-media-privacy-friends-prediction/

[17] Toth.R., & Trifonova, T. (2021). Somebody's Watching Me: Smartphone Use Tracking and Reactivity. *Computers in Human Behavior Reports, 4*, *100142*, https://doi.org/10.1016/j.chbr.2021.100142

[Access Date 07.12.2023]

[18] Brooks, T. (2021, July 29). Why You Should Update Your Web Browser. *How-To Geek.* Retrieved from https://www.howtogeek.com/725165/why-you-should-update-your-web-browser/ [Access Date 08.12.2023]

[19] Barrons, M. (2016, September 12). How to Create Secure Passwords You Won't Forget. *InfoWare Group Blog.* Retrieved from https://infowaregroup.com/blog/how-to-create-secure-passwords-you-won't-forget [Access Date 08.12.2023]

2. daļa – Digitālās higiēnas prakses uzraudzība, revīzija un nepārtraukta uzlabošana

[20] Scott, M. (2023, December 8). Europe's plan to tame Big Tech: A new legal framework. *The New York Times*. Retrieved from E.U. Agrees on AI Act, Landmark Regulation for Artificial Intelligence - The New York Times (nytimes.com)

[21] Rehak, D., & Grasseova, M., (2011). The Ways of Assessing the Security of Organization Information Systems through SWOT Analysis. In M. Alshawi & M. Arif (Eds.), *Cases on E-Readiness and Information*

Systems Management in Organizations: Tools for Maximizing Strategic Alignment (1st ed., pp. 162-184). IGI Global. https://doi.org/10.4018/978-1-61350-311-9

[22] Gleason, Benjamin & von Gillern, Sam. (2018). Digital citizenship with social media: Participatory practices of teaching and learning in secondary education. Educational Technology and Society. 21. 200-212. https://www.researchgate.net/publication/322733013_Digital_citizenship_with_social_media_Participatory_practices_of_teaching_and_learning_in_secondary_education [Access Date 20.12.2023]

[23] Lewin, C., Niederhauser, D., Johnson, Q., Saito, T., Sakamoto, A., & Sherman, R. (2021). Safe and Responsible Internet Use in a Connected World: Promoting Cyber-Wellness. *Canadian Journal of Learning and Technology, 47*(4), Special Issue.

3. daļa – Digitālās higiēnas nākotnes: izaicinājumi un iespējas

[24] Metz, C. (2023). What's the Future of AI? *The New York Times.* Retrieved from https://www.nytimes.com/2023/03/31/technology/ai-chatbots-benefits-dangers.html?searchResultPosition=1

[25] Gleason, Benjamin & von Gillern, Sam. (2023). Tinkering With ChatGPT, Workers Wonder: Will This Take My Job? *The New York Times.* Retrieved from https://www.nytimes.com/2023/03/28/business/economy/jobs-ai-artificial-intelligence-chatgpt.html

[26] Banholzer, M., Fletcher, B., LaBerge, L., & McClain, J. (2023, August 31). Companies with Innovative Cultures Have a Big Edge with Generative AI. *McKinsey & Company.* Retrieved from https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/companies-with-innovative-cultures-have-a-big-edge-with-generative-ai [Access Date 21.12.2023]

[27] Chng, E., Tan, A.L. & Tan, S.C. Examining the Use of Emerging Technologies in Schools: a Review of Artificial Intelligence and Immersive Technologies in STEM Education. Journal for STEM Educ Res 6, 385–407 (2023). https://doi.org/10.1007/s41979-023-00092-y [Access Date 21.12.2023]

[28] Spatharou, A., Hieronimus, S., & Jenkins, J. (2020, March 10). Transforming healthcare with AI: The impact on the workforce and organizations. *McKinsey & Company.* Retrieved from https://www.mckinsey.com/industries/healthcare/our-insights/transforming-healthcare-with-ai

[29] Kopp, W., & Thomsen, B. S. (2023, May 1). How AI can accelerate students' holistic development and make teaching more fulfilling. *World Economic Forum.* Retrieved from

https://www.weforum.org/agenda/2023/05/ai-accelerate-students-holistic-development-teaching-fulfilling/

[30] Pappas, C., (2016, January 7). The Top 8 Benefits Of Using Learning Management Systems. *Elearning Industry.* Retrieved from https://elearningindustry.com/top-8-benefits-of-using-learning-management-systems

[31] Seo, K., Tang, J., Roll, I. *et al.* The impact of artificial intelligence on learner–instructor interaction in online learning. *International Journal of Educational Technology in Higher Education* 18, 54 (2021). https://doi.org/10.1186/s41239-021-00292-9

[32] Yadav, N. R., & Deshmukh, S. S. (2023). Proceedings of the International Conference on Applications of Machine Intelligence and Data Analytics. In *Proceedings of the International Conference on Applications of Machine Intelligence and Data Analytics (ICAMIDA 2022)* Retrieved from https://www.atlantis-press.com/article/125986295.pdf

[33] Duball, J. (2020). Shift to Online Learning Ignites Student Privacy Concerns. *International Association of Privacy Professionals (IAPP).* Retrieved from https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/

[34] United States International Trade Administration. (n.d.). European Union - Data Privacy and Protection. Retrieved from https://www.trade.gov/european-union-data-privacy-and-protection

[35] Gonzalez, G. (2018, October 10). Amazon Abandons AI Recruiting Tool That Showed Bias Against Women. *Inc.* Retrieved from https://www.inc.com/guadalupe-gonzalez/amazon-artificial-intelligence-ai-hiring-tool-hr.html

[36] Gatzemeier, S. (2021, June 18). AI Bias: Where Does It Come From and What Can We Do About It? *UC Berkeley School of Information Blog.* Retrieved from https://blogs.ischool.berkeley.edu/w231/2021/06/18/ai-bias-where-does-it-come-from-and-what-can-we-do-about-it/

[37] Akgun, S., Greenhow, C. Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI Ethics* 2, 431–440 (2022). Retrieved from https://doi.org/10.1007/s43681-021-00096-7

[38] Polluveer, K. (2023). Innovation Policy. *European Parliament Fact Sheet.* Retrieved from https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/en/FTU_2.4.6.pdf

[39] OECD (2021), Teachers and Leaders in Vocational Education and Training, OECD Reviews of Vocational Education and Training, OECD Publishing, Paris, https://doi.org/10.1787/59d4fbb1-en

4. Promoting innovative pedagogical approaches in vocational education and training | Teachers and Leaders in Vocational Education and Training | OECD iLibrary (OECD-ilibrary.org)

[40] eduLAB Pty Ltd. (2020, August 12). eduLAB Introduction Video. *Vimeo.* Retrieved from https://vimeo.com/447337687

[41] N.d. (2022, March 27). 7 Technology Innovations That Will Impact Cybersecurity in 2022 and Beyond. *Cloud Security Alliance Blog.* Retrieved from 7 Technology Innovations That Will Impact Cybersecurity in 2022 | CSA (cloudsecurityalliance.org)

[42] World Economic Forum. (2021, March). Artificial Intelligence for Agricultural Innovation. *Community Paper.* Retrieved from WEF_Artificial_Intelligence_for_Agriculture_Innovation_2021.pdf (weforum.org)

[43] BIS Research. (2021, October 7). The Increasing Adoption of Augmented Reality (AR) in Agriculture. Retrieved from https://blog.marketresearch.com/the-increasing-adoption-of-augmented-reality-ar-in-agriculture

[44] BIS Research. (2021, October 7). The Increasing Adoption of Augmented Reality (AR) in Agriculture. Retrieved from https://eos.com/blog/smart-farming/

[45] Tzachor, A., Devare, M., King, B., et al. (2022). Responsible artificial intelligence in agriculture requires a systemic understanding of risks and externalities. *Nature Machine Intelligence, 4*, 104–109. https://doi.org/10.1038/s42256-022-00440-4

[46] Bettencourt, J. (2023, November 16). How the hospitality industry is using AR, and VR for the guest experience. *Hotel Management.* Retrieved from https://www.hotelmanagement.net/tech/how-hospitality-industry-using-ar-vr-guest-experience

[47] Kover, A. (2020, March 10). A new perspective on hospitality: How Hilton uses VR to teach empathy. *Facebook Reality Labs Tech Blog.* Retrieved from https://tech.facebook.com/reality-labs/2020/3/a-new-perspective-on-hospitality-how-hilton-uses-vr-to-teach-empathy/

[48] Guenther, D. (2021, September 9). Virtual Reality training prepares hospitality workers for the next era of travel. *Medium.* Retrieved from https://medium.com/@DanielGuenther/virtual-reality-training-prepares-hospitality-workers-for-the-next-era-of-travel-7a8d5d3b8be5

[49] Pencarelli, T. The digital revolution in the travel and tourism industry. *Inf Technol Tourism* 22, 455–476 (2020). Retrieved from https://doi.org/10.1007/s40558-019-00160-3

[50] Amon, C., Slaughter, A., & Motyka, M. (2018, September). Global renewable energy trends. *Deloitte.* Retrieved from https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/global-renewable-energy-trends.html

[51] Travelers. (n.d.). Predictive Maintenance at Solar and Wind Installations. Retrieved from https://www.travelers.com/resources/business-industries/energy/predictive-maintenance-at-solar-and-wind-installations

[52] Victor, D. G. (2019, January 10). How artificial intelligence will affect the future of energy and climate. *Brookings Institution.* Retrieved from https://www.brookings.edu/articles/how-artificial-intelligence-will-affect-the-future-of-energy-and-climate/

[9] Sklar, A. (2017). Sound, smart, and safe: A plea for teaching good digital hygiene. *LEARNing Landscapes Journal*, 10(2). https://doi.org/10.36510/learnland.v10i2.799 [Access Date 06.12.2023]

4. daļa – Digitālās higiēnas kultūras labās prakses gadījumi

[53] ShareCert Toolkit. (n.d.). Retrieved from Cybersecurity Toolkit

[54] Homo Digitalis. (2022, July 13). A big success for Homo Digitalis: The Hellenic DPA fines CLEARVIEW AI with €20 million. Retrieved from https://homodigitalis.gr/en/posts/12155/

[55] Digital First Aid. (n.d.). Retrieved from Digital First Aid Kit

[56] Digiresilience. (n.d.). Retrieved from Center for Digital Resilience

[57] CivicERT. (n.d.). Retrieved from CiviCERT

[58] SMEX. (n.d.). Retrieved from SMEX

[59] Common Sense Media. (n.d.). Digital Literacy and Citizenship. Retrieved from https://www.commonsensemedia.org/what-we-stand-for/digital-literacy-and-citizenship

[60] Center for Media Literacy. (2005). Five Key Questions of Media Literacy. Retrieved from https://www.medialit.org/sites/default/files/14B_CCKQPoster+5essays.pdf

[61] Center for Media Literacy. (n.d.). Retrieved from https://www.medialit.org/https://www.medialit.org/

[62] European Cyber Security Month. (n.d.). Retrieved from https://cybersecuritymonth.eu/

[63] Google. (2023). Be Internet Awesome: Interland. Retrieved from https://beinternetawesome.withgoogle.com/en_us/interland/

[64] Google. (2023). Be Internet Awesome: Interland. Retrieved from https://beinternetawesome.withgoogle.com/en_us

[65] Bogardus Cortez, M. (2018, April 17). The Digital Citizenship Curriculum: Digital Literacy, Cyber Hygiene and More. *EdTech Magazine.* Retrieved from How to Design Your Digital Citizenship Curriculum - EdTech (edtechmagazine.com)

[66] Bogardus Cortez, M. (2014, July 24). Digital Citizenship Game by Google & ITSE Aims to Educate. *EdTech Magazine.* Retrieved from Digital Citizenship Game by Google & ITSE Aims to Educate | EdTech Magazine