Co-funded by the
Erasmus+ Programme
of the European Union

EIROPAS PROFESIONĀLĀS IZGLĪTĪBAS UN APMĀCĪBAS NOZARES KIBERDROŠĪBAS GATAVĪBAS UZLABOŠANA

CYBER.EU.VET

INTELEKTUĀLAIS NODEVUMS IO 3

APMĀCĪBU MATERIĀLS

NGO NEST Berlin
AEII
tandemplus network
Latvian European Community Studies Association
COFAC
EOS
inerciadigital
meath partnership

Ievads

Šo apmācību formātu izstrādāja projekta CYBER.EU.VET partneri, kas sastāv no 6 moduļiem, kun o var izmantot skolotāji un pasniedzēji profesionālās izglītības un apmācību (VET) sektorā. Katrs modulis aptver teorētisko daļu, praktiskos piemērus un uzdevumus darbam grupās. Apmācības formāts ir pieejams lietošanai dažādās Eiropas valstīs, un tas ir jāpielāgo vietējām vajadzībām un apstākļiem, kad vien tas ir nepieciešams. Pielāgošana galvenokārt var būt nepieciešama praktiskajos piemēros un gadījumu izpētē, ko nodrošina apmācības formāts.

PROJEKTA PARTNERI IZSTRĀDĀJUŠI ŠĀDUS MĀCĪBU MODUĻUS:

KIBERUZBRUKUMI

Modulis 1

1. Moduļa pārskats

Mērķa grupa

- Profesionālās izglītības un apmācību (VET) pedagogi un instruktori
- Studenti
- Atbilstošo organizāciju un iniciatīvu pārstāvji (NVO, valsts un reģionālās varas iestādes, izglītības iestādes)

Moduļa apraksts

Ņemot vērā katru gadu pieaugošo kiberuzbrukumu skaitu un mērogu, īpaši jaunāko ekonomisko, politisko un ar labklājību saistīto notikumu gaismā (Covid-19 ierobežojumu sekas, militārais konflikts Ukrainā u.c.), ar vien biežāk ir svarīgi diskutēt par aktuāliem kiberuzbrukumiem. Tāpēc moduļa mērķis ir sniegt pamatizpratni par kiberuzbrukumiem un iemācīties reaģēt/pārvaldīt incidentus.

Modulis sastāvs no šādām tēmā (nodaļām):

- Definīcija un saistītie jautājumi
- Veidi
- Aktuālākie incidenti (praktiskie piemēri)
- Kā aizsargāties no kiberuzbrukumiem un kā reaģēt uz incidentiem

Katras nodaļas noslēgumā paredzēta praktiskā aktivitāte.

Mācību mērķi

- Sniegt pamatizpratni par jautājumiem, kas saistīti ar kiberuzbrukumiem.
- Nodrošināt izpratni par iespējamo kiberuzbrukumu un draudu sekam un ietekmi.
- Atpazīt un klasificēt izplatītākos kiberuzbrukumu veidus.
- Prast reaģēt uz uzbrukumiem – kur ziņot, ja notiek incidents.
- Nodrošināt informācijas un literatūras avotus tālākai un detalizētākai tēmas apguvei, lai sekotu līdzi aktuālajiem kiberuzbrukumiem un padomiem kā no tiem pasargāties.

Ilgums

Makmimāli 1,5h

Šo moduli instruktors/pasniedzējs nolasīs, izmantojot PowerPoint prezentāciju, lai dalītos ar teorētiskajām zināšanām kopā ar vairākiem vizuāliem elementiem, praktiskiem piemēriem un vingrinājumiem (maks. 20 minūtes par katru nodaļu + praktiskā aktivitāte).

Prezentācijas ieteicams sagatavot, izmantojot CYBER.EU.VET prezentācijas pielāgotu veidni, kas pieejama projekta mājas lapā. Ņemot vērā straujo attīstību un progresu kiberdrošības jomā, ieteicams nepārtraukti pārskatīt nodaļu saturu un, ja nepieciešams, pielāgot to atbilstoši aktualitātēm.

Tāpat pasniedzējiem ir ieteicams pielāgot šo moduli savas vietējās profesionālās izglītības iestādes (VET) vajadzībām un iekļaut vietējos aktuālos incidentu piemērus. Šis modulis galvenokārt aptver Latvijas praktiskos piemērus, kā arī dažus starptautiskus piemērus. Ieteicams – lielāku akcentu likt 3.nodaļu, lai analizētu un apspriestu praktiskus incidentu piemērus kopā ar attēliem un video.

1.nodaļa – Kiberuzbrukumi

Ko tas nozīmē? Ievads tēmā

Mācību aktivitāte #1 - teorija

Definīcija un nozīme

Kiberuzbrukums (dsk. kiberuzbrukumi) – nelegāls mēģinājums iegūt nesankcionētu piekļuvi lietotāja datoram, tehnoloģiju sistēmām ar mērķi radīt zaudējumus, sabojāt, atspējot, kontrolēt, bloķēt, dzēst, mainīt, viltot, nozagt tehnoloģiju sistēmā glabātos datus (datorā, viedtālrunī, rūterī, u.c.).

Parādoties Covid-19 ierobežojumiem un nepieciešamībai pāriet uz digitālu darba un mācību formātu, ir pieaudzis kiberdraudu un uzbrukumu skaits, bet digitālā aizsardzība kļuva vēl svarīgāka. Termins "kiberuzbrukums" ir cieši saistīti ar tādiem terminiem kā "kiberdraudi" (iespēja, ka var notikt konkrēts uzbrukums) un "kiberrisks".

Visizplatītākie kiberuzbrukumi — ļaunprātīga programmatūra, pikšķerēšana, pārtvērējuzbrukums (man-in-the-middle-attack), paroles uzbrukums, pakalpojuma atteikuma (piekļuves lieguma, DoS) uzbrukums un daudzi citi.

Uzbrucēju saziņas veidi: personīgie kontakti, tālrunis, elektroniskais pasts, ļaunprogrammatūra.

Avots: https://cert.lv/lv/2022/02/kiberuzbrukuma-riskam-paklauts-ikviens-interneta-lietotajs; https://www.investopedia.com/terms/c/cybersecurity.asp

Kas var veikt kiberuzbrukumus?

Kiberuzbrukumi ir ģeogrāfiski nepiesaistīti – veicami no jebkuras vietas pasaulē - virtuāli, tos var organizēt individuālā persona vai grupējums, izmantojot vienu vai vairākas dažādas uzbrukuma stratēģijas, un tie varbūt vērsti pret jebkuru tehnoloģiju sistēmu - pret privātpersonām, valsts vai privātiem uzņēmumiem.

Kāpēc notiek kiberuzbrukumi (motivācija) un ko tie var izraisīt?

Uzbrukumi virtuālajā vidē parasti ir saistīti ar identitātes zādzību, datorresursu iegūšanu, informācijas zādzību un viltošanu, pieeju komercnoslēpumiem, šantāžu, neslavas celšanu. Kiberuzbrukumi galvenokārt tiek organizēti, lai gūtu finansiālu labumu (nozagtu kredītkartes numuru un kodu), traucētu darbību un atriebtos (piemēram, lai kaitētu kādas organizācijas reputācijai).

Piemēram, Covid-19 krīze vai militārā situācija Ukrainā tiek izmantota, lai piesaistītu lietotāju uzmanību krāpnieciskos e-pastos un sociālajo mediju paziņojumos.

DAŽI STATISTIKAS DATI

Attālinātais darba režīms, uz kuru piespiedusi pāriet globālā pandēmija, ir palielinājis kiberdrošības riskus un veicinājis jauna veida incidentus. Vairums no tiem attiecas arī uz izglītības iestādēm un to būtu jāņem vērā pedagogu un jaunatnes turpmākos izglītības un apmācību pasākumos.

Saskaņā ar Deloitte analizēto informāciju 2020. g. aprīlī Šveicē notikuši 350 kiberuzbrukumi, salīdzinot ar normu – 100-150 (pikšķerēšana, krāpnieciskas tīmekļa vietnes, tieši uzbrukumi uzņēmumiem utt.).

Attālinātā darba veida pieaugums prasa pievērst lielāku uzmanību kiberdrošībai, jo kiberrisku esamība ir krietni palielinājusies. Tas izriet, piemēram, no tā, ka 47% indivīdu, strādājot no mājām, iekrīt pikšķerēšanas krāpniecībā.

Latvijā, piemēram, lielākais apdraudēto unikālo IP adrešu skaits Latvijā tika konstatēts 2020. gada februārī-aprīlī, kad sākās Covid-19 pandēmija (vairāk nekā 10 tūkstoši uzbrukumu mēnesī) - saskaņā ar CERT.LV, kas ik mēnesi un ik gadu publicē datus un pārskatu par aktuālākajiem incidentiem – "Kiberlaikapstākļi".

Avots: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

Interaktīvais rīks – **tiešsaistes pasaules kiberdraudu karte**

Mācību aktivitāte #1 - praktiskais uzdevums

Diskusija ar dalībniekiem par viņu pieredzi kiberuzbrukumos (10-15 min):
1) Kādus kiberuzbrukumus Jūs zināt?
2) Vai esat (Jūs vai Jūsu radinieki/draugi) kādreiz piedzīvojuši kiberuzbrukumu/incidentus? Kā tie atrisinājās?

2.nodaļa - Kiberuzbrukumu veidi

Mācību aktivitāte #2 - teorija

Visizplatītākās kiberuzbrukumu metodes (veidi):

Ļaunprogrammatūra/Ļauntūra (malware) – ļaunprātīga programmatūra, kas tiek izmantota, lai bojātu lietotāja ierīces (datorus, tālruņus utt.) vai tīklu. Ļauntūras piemēri: spiegprogrammatūra un trojāni, datortārpi, vīrusi, izspiedējvīrusi, reklāmprogrammatūra, surogātpasts. Atkarībā no ļaunprātīga koda hakeri var izmantot ļaunprātīgu programmatūru, lai nozagtu vai slepeni kopētu sensitīvus datus, dzēstu datus, bloķētu piekļuvi failiem, traucētu sistēmas darbību vai padarītu sistēmas neizmantojamas [DigiCERT]

Ļauntūra galvenokārt tiek izplatīta diviem mērķiem – informācijas iegūšanai (spiegprogrammatūra pārsuta datus no upura ierīces, piem., paroles) vai peļņas gūšanai (šifrējošais izspiedējvīruss, kas uzbrukuma rezultātā nošifrē datus lietotāja ierīcē un datu atgūšanai tika pieprasīta izpirkuma maksa) [CERT Report 2020]

Pikšķerēšana jeb personīgo datu izkrāpšana – metode, kurā uzbrucēji nosūta šķietami likumīgu e-pastu ar lūgumu lietotājiem izpaust konfidenciālu informāciju. Adresāti tiek maldināti lejupielādēt e-pastā iekļauto ļaunprogrammatūru, atverot pievienoto failu vai iegulto saiti. Parasti tās ir tīmekļa vietnes, kas izskatās pēc reālu uzņēmumu vietnēm, lietotājam tajās ir jāievada sava personīgā informācija (bankas konts, kredītkaršu numuri un paroles, tai skaitā autentifikācijas pakalpojumu paroles). Datu izkrāpšana var būt veikta arī telefoniski vai WhatsApp lietotnē [Investopedia]

Pakalpojuma liegums (DoS) – hakeri bombardē organizācijas serverus ar liela apjoma vienlaicīgiem datu pieprasījumiem, līdz upuris nevar atbildēt vai avarē, tādējādi padarot serverus nespējīgus apstrādāt jebkādus likumīgus pieprasījumus. Līdz ar to sistēmas lietotājiem piekļuve pakalpojumam nav iespējama. DoS uzbrukumi var ilgt no dažām stundām līdz vairākiem mēnešiem un var izmaksāt uzņēmumiem laiku un naudu, kamēr to resursi un pakalpojumi nav pieejami [Investopedia]

Pārtvērējuzbrukums (man-in-the- middle-attack) – uzbrucēji slepeni iekļaujas starp divām pusēm, piem., atsevišķa datora lietotāju un tā finanšu iestādi. Atkarībā no faktiskā uzbrukuma detaļām šāda veida uzbrukumu var precīzāk klasificēt kā "uzbrukums briesmoņa vidū" vai "uzbrukums iekārtas vidū" u.tml. Šādā gadījumā uzbrucējs pārtver, dzēš vai modificē datus, kad tie no datora, viedtālruņa vai citas pieslēgtas ierīces tiek pārraidīti tīklā [Investopedia, TechTarget]

Mācību aktivitāte #2 - praktiskais uzdevums

Grupas diskusija – kāda veida īpašības (raksturiezīmes) signalizē par uzbrukumiem/krāpnieciskiem ziņojumiem? (10–15 min)

- Dalībniekiem tiek dotas 10 minūtes, lai pierakstītu īpašības
- Diskusija par rezultātiem

3.nodaļa - Draudu un uzbrukumu piemēri

Kā identificēt draudus?

Mācību aktivitāte #3 - teorija

Kiberuzbrukumu piemēri (Ukrainas kara kontekstā)

- Krāpnieciskas e-pasta vēstules angļu valodā ar aicinājumu atbalstīt kādu no militārā konflikta pusēm – Ukrainu vai Krieviju.
- VIDEO – Kā krāpnieki nolaupa Ukrainas kara savāktos ziedojumus? – BBC News (angliski)
- RAKSTS – 4 Krievijas un Ukrainas kara krāpniecības veidi, kas vērsti uz patērētājiem (angliski)

Piemēri par galvenajiem incidentiem, balstoties uz situāciju Latvijā (2021-2020) un ārvalstīs:

Ļaunprogrammatūra

Covid-19 situācija tika izmantota, lai izplatītu ļaunprogrammatūras mēģinājumus: piemēram, e-pastus Pasaules veselības organizācijas vārdā, norādot, ka pielikumā iekļauta informācija par Covid-19 aktualitātēm; saites uz diagrammām ar Covid-19 izplatību, kuras funkcionalitāte bija vērsta uz lietotāju datu zagšanu; ļaunprātīgas e-pasta vēstules veselības aprūpes iestādēm par Covid-19 aizsardzības līdzekļu piegādi u.c.

Pasaulē bīstamākās ļaunprogrammatūras Emotet izplatības pieaugums gan pasaules, gan Latvijas tīmeklī, paredzēta sensitīvas informācijas nozagšanai. Emotet upura iekārtā parasti nonāca no kādas jau inficētas kontaktpersonas e-pasta. Emotet kalpo kā "durvju atvērējs" uz citiem datoriem, ļaujot nesankcionēti piekļūt citām ļaunprogrammatūras ģimenēm. Latvijā inficējās vairāk nekā 200 uzņēmumu.

Pikšķerēšana jeb personīgo datu izkrāpšana

Vairumā gadījumu pikšķerēšanas kampaņas bija vērstas uz e-pasta un Office 365 piekļuves datu izkrāpšanu, uz banku, starptautisku maksājumu sistēmu, to skaitā Smart-ID piekļuves datu iegūšanu un uz populārāko sociālo tīklu – Facebook, Instagram – piekļuves datu izkrāpšanu. Covid-19 tēma bieži tika izmantota, lai piesaistītu lietotāju uzmanību krāpnieciskos e-pastos un sociālo mediju paziņojumos.

Pandēmijas laikā tika novēroti pastiprināti datu izkrāpšanas mēģinājumi, izmantojot sūtījumu piegādes pakalpojumu sniedzēju zīmolus (Latvijas Pasts, DHL, Omniva, DPD, AliExpress u.c.). Tāpat tika novēroti inovatīvi uzbrukumi – Office 365 piekļuves tiesību izkrāpšana, šo uzbrukums bija grūti identificēt ar tehniskiem līdzekļiem, jo cietušā ierīcē netika veiktas ļaunprātīgas darbības, bet uzbrukumi tika realizēti pašā Office 365 vidē.

VIDEO Pikšķerēšana

Krāpšanas piemēri

Intensīvie krāpšanas mēģinājumi, t.sk. sociālās inženierijas uzbrukumi. Lielākā daļa krāpniecību bija vērstas uz iedzīvotāju maksājumu karšu piekļuves datu izgūšanu, finanšu līdzekļu izkrāpšanu, kā arī e-pasta piekļuves datu iegūšanu. Uzbrucēji sūtīja iedzīvotājiem krāpnieciskas e-pasta vēstules un īsziņas, kā arī veica krāpnieciskas telefonsarunas, visbiežāk uzdodoties par banku vai e-pasta pakalpojumu sniedzēju pārstāvjiem. Vairāki uzņēmumi cieta no iejaukšanās biznesa sarakstē (BEC), kur kopējie zaudējumi sasniedza gandrīz 200 000 EUR.

Preču piegādes jautājums tika izmantots krāpšanas mēģinājumos pret pārdevējiem, kuri reklāmas portālos ievietoja informāciju par preču pārdošanu. Izliekoties par ieinteresētiem pircējiem un izmantojot "WhatsApp" komunikācijas platformu, krāpnieki izteikuši vēlmi iegādāties preci. Izmantojot sūtījumu piegādes pakalpojumu sniedzēju zīmolus, krāpnieki lūguši pārdevējus ievadīt maksājuma kartes detaļas viltotajās "Omniva", DPD un vēlāk arī "Latvijas pasta" mājaslapās, lai atklātu gan CVV kodu, gan kartes anci.

Uzbrucēji izmantoja pielāgotas tīmekļa vietņu adreses (dor nus), kas bija līdzīgas sākotnējām tīmekļa vietņu adresēm, lai maldinātu sabiedrību.

Uzbrucēji centās iegūt arī maksājumu karšu informāciju, nosūtot e-pastus ar lūgumu pieteikties "Bitcoin" bilancei, reģistrējoties krāpnieciskam kriptovalūtas maiņas pakalpojumam.
Aktīvākie mēģinājumi bija izspiešanas kampaņas, kurās uzbrucēji apgalvoja, ka viņiem izdevies uzlauzt lietotāja ierīci un iegūt kompromitējošus materiālus, par kuru neizplatīšanu tika pieprasīta izpirkuma maksa; krāpnieciskas loterijas pazīstamo zīmolu vārdā, piedāvājot laimēt jaunākos viedtālruņu modeļus vai citas vērtīgas balvas.

CITI PIEMĒRI

Maldinošas reklāmas sociālajos tīklos – nesankcionēti izmantojot Latvijā pazīstamu personu vārdus, interneta lietotāji tika aicināti investēt naudu kriptovalūtā. Krāpnieki veica arī telefona zvanus un mēģināja pārliecināt cilvēkus investēt. Atsevišķos gadījumos tika novēroti atkārtoti krāpšanas mēģinājumi, kur jau finanšu krāpniecībā cietušajiem tika piedāvāta palīdzība atgūt zaudētos līdzekļus.

Telefonkrāpnieki – viltojot dažādu kredītiestāžu tālruņu numurus un uzdodoties par bankas pārstāvjiem, krāpnieki, izmantojot sabiedrības vājās zināšanas par papildu autentifikācijas metodēm, izkrāpa finanšu līdzekļus no vairākiem tūkstošiem lietotāju, nodarot Latvijas kredītiestādēm kopējos zaudējumus simtiem tūkstošu vērtībā.

Hakeru pielāgošanās nepieciešamībai uzsākt attālināto darbu: ņemot vērā uzņēmumu nepieciešamību strauji pāriet uz attālinātā darba režīmu un elektronisko dokumentu aprites ieviešanu, hakeri izmantoja situāciju, lai pielāgotu savus uzbrukumus – piem. vairāki uzņēmumu grāmatveži saņēma e-pastus direktora vai cita darbinieka vārdā, lai veiktu steidzamu maksājumu vai mainītu algas kontu.

Latvia and Lithuania detain 108 over multi-million euro call centre scam

Iejaukšanās biznesa sarakstē – kompromitējot uzņēmumu vai to sadarbības partneru e-pastus, uzbrucēji izvēlējās piemērotu brīdi, lai kādai no pusēm nosūtītu rēķinu ar mainītu kontu (2021.gadā zaudējumu apjoms sasniedza 500 000 EUR).

Krāpnieciskas ziņas – uzbrucēji mēģināja pārtvert WhatsApp kontus, lūdzot nosūtīt sešciparu kodu, kas it kā kļūdaini tika nosūtīts uz lietotāja tālruņa numuru. Tā kā šādi ziņojumi nāca no lietotāju esoša kontaktu saraksta (patiesībā uzlauztiem kontiem), daži cilvēki pārsūtīja savus kodus, zaudējot piekļuvi savam WhatsApp kontam. Divfaktoru autentifikācijas izmantošana būtu aizsardzības līdzeklis pret šādu uzbrukumu.

PIEMĒRS Kad lietotājs kopīgo ciparu kodu ar hakeri (skat.ekrānšāviņu un rakstu)
PIEMĒRS SMS no vietējās bankas ar krāpniecības saiti (piemērs ar SMS no SEB bankas).

Krāpnieku e-pasti – krāpnieki uzdodoties par Latvijas Pastu, lūdz samaksāt par it kā aizkavēta sūtījuma piegādi. E-pastā norādītā saite ved uz viltus tīmekļa vietni, kas paredzēta norēķinu kartes datu izkrāpšanai (skat ekrānšāviņus).

Viltus interneta veikali – īpaši liela aktivitāte tika novērota svētku sezonā, pielietojot sociālo mediju reklāmu. To veicināja arī Covid-19 ierobežojumi, kuru dēļ uzņēmumi pārgājuši uz produktu pārdošanu tiešsaistē.

PIEMĒRS Scammers lure AliExpress users to fake online stores (bildes un krāpšanas piemēri); How to Recognize a Scam

Romantiskā krāpšana – krāpnieki izmanto cilvēkus, kuri meklē romantiskus partnerus, bieži vien izmantojot iepazīšanās vietnes, lietotnes vai sociālos medijus, izliekoties par potenciālajiem partneriem. Krāpnieki spiež uz emocionāliem stimuliem, lai no upura iegūtu naudu, dāvanas vai personisku informāciju.

PIEMĒRS Investigation story on Romance Scammer [by North Lab]

Piekļuves lieguma uzbrukumi (DoS un DDoS)

Pandēmijas laikā tika reģistrēti DDoS uzbrukumi valsts un pašvaldību iestādēs (piem., Nacionālajā bibliotēkā, e-klasē, e-veselībā u.c.). Ilgstoši DDoS uzbrukumi traucēja skolu darbībai. Līdzīgi ziņojumi mācību gada sākumā saņemti arī no citām izglītības iestādēm. Ar šādiem izaicinājumiem saskaras arī izglītības iestādes citviet Eiropā.

Gan Eiropā, gan Latvijā kļuva aktuāli naudas izspiešanas mēģinājumi, kas primāri bija vērsti pret finanšu iestādēm vai privātā sektora uzņēmumiem (uzbrucēji draudot apturēt uzņēmuma tīmekļa vietnes vai citu resursu darbību ar uzbrukumu līdz pat 2 Tb/s, ja netiks veikta izpirkuma samaksa, īstenoja testa uzbrukumu sērijas).

CITI TRENDI

Kompromitētas iekārtas un datu noplūdes

Iekārtu kompromitēšanas gadījumi var skart privātpersonas, uzņēmumus, kā arī valsts un pašvaldību iestādes (kompromitēti e-pastu konti, ar kuriem organizāciju darbinieki inficēja savas iekārtas, atverot pielikumus vai saites no šķietami zināmiem kontaktiem – kolēģiem un sadarbības partneriem; kompromitētas tīmekļa vietnes – dēļ novecojuša spraudņa vai neatjauninātas satura vadības sistēmas) .

Piem., 2020.g.-2021.g. vairākas valsts iestādes uz laiku zaudēja piekļuvi saviem sociālo tīklu kontiem, jo uzbrucēji pārņēma kontroli pār kādu no kontu administratoru profiliem. Tika saņemti ziņojumi par ielaušanās gadījumiem Zoom, MS Teams un citās platformās sanāksmju laikā, kas radušies zināšanu trūkuma dēļ par pieejamajiem drošības pasākumiem (*uzgaidāmā telpa, ierobežotas iespējas pievienoties dalībniekiem no ārvalstīm u.c.).

Ielaušanās mēģinājumi (jebkurš uzbrukuma veids, kura mērķis ir apdraudēt organizācijas drošību) - līdz ar organizāciju pāriešanu attālinātā darba režīmā, tika novērota palielināta botu aktivitāte, kas meklē ievainojamas, neatbilstoši konfigurētas un/vai ar vājām parolēm aizsargātas tīmeklī pieslēgtas iekārtas (potenciālie botu mērķi – darba devēja steigā izsniegtas, nepietiekami droši konfigurētas iekārtas vai personīgie datori, kuri pēkšņi tiek izmantoti darbam, kā arī attālinātās piekļuves pakalpojumi (RDP) ar vāju paroli un nepietiekamu papildu aizsardzību).

VIDEO Ielaušanās mēģinājumi (angļu valodā)

Lasiet vairāk - Ielaušanas mēģinājumu atpazīšana (angļu valodā)

AVOTS CERT.LV and “Kiberlaikapstākļi”; Investopedia

PAPILDUS ELEMENTI

Apsveriet arī diskusijas par citām viltus un krāpnieciskas informācijas metodēm, piemēram, deepfake un citām.

Mācību aktivitāte #3 - praktiskais uzdevums

Nodaļas noslēgumā tiek organizēts Kahoot tests, kurā dalībniekiem ir jāatbild, vai sniegtā informācija ir krāpnieciska vai jāatrisina citus līdzīgus jautājumus.

Dalībniekiem: https://kahoot.it/

Lektoram: https://create.kahoot.it/details/aae86dee-754f-45c3-b1f6-bc01ae9ed954

4.nodaļa - Kā rīkoties incidenta gadījumā?

To novēršana un kā sagatavoties

Mācību aktivitāte #4 - teorija

DAŽI PADOMI UN IETEIKUMI AIZSARDZĪBAI

- Vienmēr rūpīgi pārbaudiet savus e-pasta ziņojumus un pievēršat uzmanību – pielikumiem vai iegultai (iekļautai) hipersaitei no nezināmiem/svešiem sūtītājiem; ziņām ar steidzamu lūgumu kaut ko lejupielādēt; piedāvājumiem ar apbalvojuma solījumu, kas izklausās pārāk labs, lai būtu patiess.

VIDEO Spaidonis (ar subtitriem angļu valodā)

- Pievērsiet uzmanību URL adreses pareizrakstībai. Pikšķerēšanas vietnēs bieži tiek izmantotas tīmekļa adreses, kas izskatās līdzīgas pareizajai vietnei, bet satur vienkāršu pareizrakstības kļūdu, piem., "l" tiek aizstāts ar "1". Nepareiza vai dīvaina pareizrakstība ir signāls par iespējamu krāpniecību.
- Izmantojiet sarežģītas un atšķirīgas paroles starp savām ierīcēm, e-pasta un sociālo mediju kontiem. Lai iegūtu vairāk praktisku padomu, skatiet CYBER.EU.VET moduli par parolēm (Modulis 4).

- Kur iespējams, savās ierīcēs izmantojiet daudzfaktoru autentifikācijas iestatījumus (piem., paroli un sejas ID vai pirksta nospiedumu savā tālrunī. Gmail – kad lietotājs pierakstās, izmantojot jaunu ierīci, pēc lietotājvārda un paroles ievadīšanas parādās pieprasījums apstiprināt Jūsu identifikāciju no citas ierīces, parasti mobilā tālruņa).

  Divpakāpju verifikācija WhatsApp lietotnē (Android lietotājiem)
- Neveiciet darījumus ar sensitīvo informāciju, izmantojot atvērto publisko Wi-Fi tīklu, kafejnīcās un citās publiskās vietās.
- Nodrošiniet to, lai vismaz vissvarīgākajiem datiem Jūsu ierīcē būtu rezerves kopija – mākoņkrātuvē vai ārējā ierīcē. Pārliecinieties, ka varat atjaunot nepieciešamos datus no rezerves kopijām, un uzziniet, cik daudz laika tas prasa.
- Programmatūras atjauninājumi – ir svarīgi sekot līdzi programmatūras atjauninājumiem un nekavējoties tos instalēt. Pat vienas dienas kavējums var būt kritisks.
- Izmantojiet VPN. Virtuālie privātie tīkli nodrošina papildu aizsardzības līmeni interneta lietošanai mājās. Paļauties tikai uz vienu VPN nevar, lai novērstu kiberuzbrukumus, taču tas var būt noderīgs šķērslis kiberuzbrukumu novēršanai.
- Regulāri sekojiet līdzi jaunumiem uzbrukumu pasaulē un atceraties, ka ka globālie, nacionālie politiskie un ekonomiskie notikumi, kā arī ar cilvēku ciešanām saistītie notikumi (pandēmijas, militārie konflikti) var tikt izmantoti kā tēma/"piesegs" potenciālajam kiberuzbrukumam.
- Papildus – CERT.LV ieteikumi, saasinoties ģeopolitiskajai situācijai Eiropā un pieaugot kiberdraudiem: https://cert.lv/lv/2022/02/cert-lv-ieteikumi-saasinoties-geopolitiskajai-situacijai-eiropa-un-pieaugot-kiberdraudiem

Kur ziņot par kiberdraudiem vai incidentiem?

- Jūsu darbavietā, izglītības iestādē – nosūtiet ekrānšāviņus, attēlus vai video attiecīgajai personai Jūsu iestādē (piemēram, IT nodaļā). Brīdiniet savus kolēģus un draugus.
- Nacionālo kibertelpu atbalstošās institūcijās:
  1. Nacionālās/reģionālās institūcijas, kas atbalsta iedzīvotājus un MVU kiberrisku vai -uzbrukumu gadījumā (piem., Latvijā – CERT.LV); instrukcija, kā pareizi pārsūtīt krāpnieciskus e-pastus
  2. Valsts policija
  3. Nacionālās/reģionālās organizācijas, kas cīnās pret pārkāpumiem un nelegālu saturu internetā un izglīto bērnus par drošu interneta lietošanu (piem., Latvijas Drošāka interneta centrs) u.c.

INFORMĀCIJAS AVOTI PAR AKTUALITĀTĒM

Lai sekotu līdzi jaunumiem par kiberdrošību un kiberdraudiem, **regulāri lasiet vietējos vai starptautiskos avotus:**

https://portswigger.net/daily-swig/cyber-attacks

https://www.euronews.com/tag/cyber-attack

OUCH! Newsletters - pasaulē vadošie, bezmaksas drošības informācijas biļetens, kas paredzēts ikvienam.

Vietnes ar Latvijas resursiem:

https://www.esidross.lv/

https://cert.lv/lv/ (ieskaitot "Kiberlaikapstākļi", instrukcija kā pārsūtīt kaitīgus e-pastus)

https://drossinternets.lv/

Mācību aktivitāte #4 - praktiskais uzdevums

Diskusija ar dalībniekiem - kursa lietderības novērtējums (5-10 min aktivitāte)

2. Moduļa mācību rezultāti

Zināšanas

- Izglītojamajam būs pamatizpratne par kiberuzbrukumu galvenajiem jautājumiem
- Izglītojamajam būs izpratne par aktuālajiem incidentiem (ņemot vērā globālos notikumus).
- Izglītojamais pārzinās informācijas avotus, kur sekot līdzi brīdinājumiem un aktuālajiem incidentiem.

Prasmes

LIzglītojamais spēs identificēt un klasificēt izplatītākos kiberdraudu veidus un tos izskaidrot.

Kompetences

- Izglītojamais spēs atpazīt potenciālos kiberdraudus un zinās, kur par tiem ziņot.
- Izglītojamais varēs izvēlēties pamatinstrumentus un paņēmienus aizsardzībai pret kiberuzbrukumiem.

3. Bibliogrāfija

CERT.LV (Information Technology Security Incident Response Institution): https://cert.lv/lv

Covid-19 pikšķerēšanas piemēri: https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp

Digicert, What are Malware, Viruses, Spyware, and Cookies? https://www.websecurity.digicert.com/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them

Fichtner, E. (2022), Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks: https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks

Information Technologies Security Incident Response Institutions (2021), CERT.LV Annual Report 2020: https://cert.lv/uploads/parskati/CERTLV-annual-report-2020_ENG.pdf

InInformatīvais ziņojums "Latvijas kiberdrošības stratēģija 2019.–2022.g.": https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf

Latvijas Drošāka interneta centrs, projekts-platforma "Drossinternets.lv": https://drossinternets.lv

LIKTA (Latvijas Informācijas un komunikācijas tehnoloģijas asociācija): https://likta.lv/digitalas-parmainas-izglitiba/

Li, Y., Liu, Q (2021), A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Science Direct, Vol. 7, p. 8176-8186: https://www.sciencedirect.com/science/article/pii/S2352484721007289

Merriam-webster dictionary, cyberattack: https://www.merriam-webster.com/dictionary/cyberattack

Prat, M.K. (2021), Cyber-attack – definition: https://www.techtarget.com/searchsecurity/definition/cyber-attack

Simplilearn, Cyber Security Full Course 2022: https://youtu.be/yr1Psapupsc

CERT.LV (2022), IT drošības seminārs "Esi drošs" martā (in Latvian): https://cert.lv/lv/2022/02/it-drosibas-seminars-esi-dross-marta#Sanita_Vitola

Esi Drošs (2022), Kiberuzbrukuma riskam pakļauts ikviens interneta lietotājs (in Latvian): https://www.esidross.lv/2022/02/10/kiberuzbrukuma-riskam-paklauts-ikviens-interneta-lietotajs/

1. Moduļa pārskats

Mērķa grupa

- VET pedagogi
- Studenti
- Izglītības nozarē strādājošo publisko iestāžu pārstāvji: pašvaldības, reģionālās un valsts varas iestādes

Moduļa apraksts

Mūsdienās cilvēki daudz laika pavada pie ekrāna. Jaunieši aug pasaulē, kurā ir nepieciešamas jaunas tehnoloģijas un galvenais saziņas kanāls starp viņiem ir internets. Piemēram, klātbūtne sociālajos medijos jauniešiem var sniegt daudz priekšrocību, tomēr tajā pastāv arī zināmi riski. Ir daudz cilvēku, kuri kādreiz cietuši no iebiedēšanas vai cieš no tās pašreiz. Vairumā gadījumu cilvēki neapzinājās par to un problēmām, kas var rasties viņu dzīvē. Šī iemesla dēļ mēs vēlētos izmantot šo moduli, lai saprastu, kas ir kibermobings un kā to var novērst.

Mācību mērķi

- Izpratnes veicināšana par kibermobingu
- Zināšanu sniegšana, kā to noteikt
- Izpratnes veicināšana par kibermobinga ietekmi
- Iepazīstināt ar tā galvenajām sekām
- Paņēmienu nodrošināšana, kā to novērst un tikt ar to galā

Ilgums

2 stundas

1. nodaļa - Kā atklāt kibermobingu?

Kādas ir tā sekas?

Šo nodaļu instruktors/pasniedzējs nolasīs, izmantojot PowerPoint prezentāciju, lai dalītos ar teorētiskajām zināšanām kopā ar vairākiem vizuāliem elementiem – īsiem video un reāliem kibermobinga gadījumiem, apkopojot informāciju no PowerPoint slaidiem (maks. 30 minūtes). Prezentācijas ieteicams sagatavot, izmantojot CYBER.EU.VET prezentācijas pielāgotu veidni.

Mācību aktivitāte 1

Ieteicamais saturs, ko pasniedzējs nolasa audzēkņiem (maks. 30 min.):
Kibermobings – lai arī bieži vien ir saistīts ar kiberizsekošanu, pats par sevi ir ļoti nopietna problēma, un tā izplatība pēdējos gados ir pieaugusi.

Kā atklāt kibermobingu?

Kibermobings (cyberbulling) bieži vien ir **grūti atpazīstams**, jo tas notiek "aiz slēgtām durvīm" vai privātā tālrunī/datorā.

Šīs ir visizplatītākās pazīmes, ka kāds ir emocionālās pazemošanas upuris:

- Kļūst neparasti sarūgtināta, ja nevar izmantot datoru/ tālruni vai arī pēc ierīču lietošanas.
- Ātri pārslēdz ekrānus vai aizver programmas, kad kāds paiet garām.
- Izvairās no diskusijām par to, ko viņš/viņa dara datorā.
- Atsakās no ģimenes vai draugiem.
- Nevēlās piedalīties aktivitātēs, kas iepriekš sniedza baudu.
- Atsakās iet uz skolu.
- Arvien biežāk ziņo par saslimšanas simptomiem.
- Parādās depresijas vai skumju pazīmes.

Kibermobinga sekas upuriem var būt postošas. Viņi var piedzīvot dažādas negatīvas emocijas, piemēram, skumjas, dusmas, vilšanās un pazemojumu. Viņi var justies arī izolēti un vientuļi, tā, it kā viņiem nebūtu neviena, pie kā vērsties.

Upuri var ciest arī mācību vidē, jo viņi var būt pārāk apmulsuši, lai ietu skolā vai piedalītos stundās. Dažos gadījumos upuri var pat apsvērt pašnāvību.

Kibermobings var negatīvi ietekmēt arī tos, kuri ir liecinieki tam, ka tas notiek ar kādu citu. Viņi var justies nobijušies, bezpalīdzīgi un skumji. Viņiem var parādīties miega un ēšanas traucējumi, kā arī rasties trauksme un depresija.

Kibermobinga ietekme un sekas:
Kad iebiedēšana notiek tiešsaistē, var justies tā, it kā Jums uzbrūk visur, pat mājās. Var šķist, ka nav glābiņa. Ietekme var būt ilgstošā un izpausties dažādos veidos:

- **Garīgi** – persona jūtas sarūgtināta, samulsusi, dumja, pat sabijusies vai dusmīga
- **Emocionāli** – kauna sajūta vai intereses zudums par iemīļotajām lietām
- **Fiziski** – nogurums (miega zudums) vai tādi simptomi kā vēdersāpes un galvassāpes

Sajūta, ka citi smejas vai uzmācas, var traucēt cilvēkiem runāt vai mēģināt tikt galā ar problēmu. Ekstremālos gadījumos kibermobings pat novest pie tā, ka cilvēki atņem sev dzīvību.

VIDEO Words Hurt | Cyberbully Short Film (angliski)

Ietekme (sekas):

- Slimība
- Depresija
- Izolācija
- Dusmas
- Pazemojums

Mācību aktivitāte 2

Grupas diskusija – jautājumi un atbildes; Novērtēšana un atsauksmes (maks. 10 min).
Tagad, kad zināt visizplatītākās pazīmes, kas liecina par to, ka kāds ir emocionāli pazemots,

- Vai pazīsti kādu, kas ir bijis šādā situācijā?
- Vai Jūs varētu viņam/viņai palīdzēt?

2. nodaļa - Kā novērst/apturēt kibermobingu?

Mācību aktivitāte 1

Ieteicamais saturs, ko pasniedzējs nolasa audzēkņiem (maks. 30 min.):

Kibermobingu izraisa samērā viegla piekļuve digitālo mediju platformām un ierīcēm. Bieži vien tās tiek izmantotas bez jebkādas uzraudzības, kas padara kibermobingu par ļoti grūti risināmu izaicinājumu. Lai novērstu šo praksi, būtu nepieciešams krietns laiks, lai efektīvi uzraudzītu katru tiešsaistes mijiedarbību. Lai gan cilvēkiem bieži vien nav iespējams pilnībā atbrīvoties no digitālajiem rīkiem, ir metodes, ko vecāki, skolēni un pedagogi var izmantot, lai cīnītos pret šo parādību un mazinātu tās kaitīgo ietekmi.

Vecākiem efektīvs veids, kā novērst kibermobingu, ir vienkārši runāt ar bērniem par šo problēmu. Tāpat ir svarīgi diskutēt par drošību internetā, privātumu un paroļu pārvaldību. Uzstādīt vadlīnijas par to, kā skolēniem uzvesties internetā un mudināt jauniešus būt atklātiem ar viņu vecākiem par jebkuru pazemojumu, kuru viņi izjutuši dēļ emocionālās pazemošanas internetā vai reālajā dzīvē.

Jaunieši var palīdzēt paši sev nekļūt par kibermobinga upuri, būdami piesardzīgi attiecībā uz to, ko viņi publicē internetā. Jauniem cilvēkiem vajadzētu izvairīties no savu paroļu kopīgošanas un nodrošināt to, lai tiešsaistes konfidencialitātes iestatījumi viņus pasargā.

Audzēkņiem ir nozīmīga loma kibermobinga novēršanā. Jauniešiem, kuriem ir izpratne par kibermobinga iezīmēm, pamanot, ka pazemošana notiek ar kādu citu, viņi var paziņot par šo faktu uzticamam pieaugušajam. Viņiem vajadzētu būt arī laipniem, dāsniem un atbalstošiem pret bērnu, kuram tiek darīts pāri. Pedagogiem, treneriem un citiem uzticamajiem pieaugušajiem ir jāapvienojas ar vecākiem un jauniešiem, lai cīnītos pret kibermobingu. Bieži vien šīs personas var pamanīt izmaiņas bērna uzvedībā un palīdzēt atrisināt šo problēmu, pirms to spēj izdarīt vecāki.

Tehnoloģijas un internets nav tas, kas izraisa problēmu. Patiesā problēma ir cilvēki, kuri tos izmanto, lai kaitētu citiem. Līdz ar to ir svarīgi iemācīt pusaudžiem, kā droši un atbildīgi izmantot sociālos medijus un kas viņiem jādara, ja viņi tiek iebiedēti internetā.

Kas jādara, ja esi saskaries ar kibermobingu?

- NEATBILDĒT un nekomentēt kibermobinga ziņojumus.
- BLOĶĒT iesaistītās personas.
- IZRAKSTĪTIES no tīmekļa vietnes, kurā notiek iebiedēšana.
- Aizsargāt savas PAROLES un pārbaudīt KONFIDENCIALITĀTES IESTATĪJUMUS.
- SAGLABĀT visus iespējamos pierādījumus. Ekrānšāviņi vai izdrukas.
- ZIŅOT par kibermobingu: gandrīz katrā tīmekļa vietnē ir iespēja ziņot par pārkāpumu.
- Pastāstīt uzticamam PIEAUGUŠAJĀM par notiekošo vai sazinieties ar POLICIJU.

Kā rīkoties, ja ar kādu notiek emocionālā pazemošana?

- Pastāstiet par to saviem vecākiem vai uzticamam pieaugušajam, lūdziet viņu padomu.
- Ziņojiet par situāciju tehnoloģiju, lietotnes vai sociālo mediju pakalpojumu sniedzējam.
- Ja situācija ir saistīta ar klases biedriem, informējiet savus skolotājus.
- Sniedziet savu atbalstu personai, kura tiek iebiedēta, piemēram, nosūtiet mīļu ziņu.

Tiesiskās darbība: gan neslavas celšanas, gan apmelošana ir noziegumi, kuru rezultātā var uzsākt tiesvedības procesu.

Jautā pēc palīdzības:

- tikt galā ar kibermobinga situācijām ir ļoti grūti, ja to risina tikai pats.

VIDEO Emma's Story: Cyberbullied by a Best Friend (angliski)

Kā es varu sevi izglītot?

- Organizācijas: pastāv daudz organizāciju, kas izplata informāciju par kibermobingu. Zemāk ir norādītas tīmekļa vietnes, kas veido un kopīgo noderīgu saturu. Tas var palīdzēt ikvienam, kurš uztraucas par kibermobingu vai to ir piedzīvojis.
- Blogi un podkāsti: sekošana līdzi blogiem un podkāstiem ar fokusu par šo tēmu ir lielisks veids kā būt lietas kursā un saņemt jaunākos padomus vai perspektīvas.
- Grāmatas.
- Lietotnes un programmatūra: ir daudz produktu, kas ļauj vecākiem ierobežot un/vai uzraudzīt savu bērnu interneta aktivitātes. Katram vecākam ir jāizlemj, vai šāda veida uzraudzība ir piemērota, pamatojoties uz bērna vecumu un interneta paradumiem. Daži vecāki pat uzrauga valodu, kas var būt vērsta uz kibermobingu. Ir arī uzņēmumi, kas sadarbojas ar skolām, lai ļautu tām anonīmi ziņot par pazemošanas incidentiem.

Mācību aktivitāte 2

Grupas diskusija – jautājumi un atbildes; Novērtēšana un atsauksmes (maks. 15 min.)

Rakstīšanas vingrinājums:
Aprakstiet situāciju, kurā notiek kiberhuligānisms. Tas var būt reāls vai izdomāts.
Vai Tu vari palīdzēt? Ja jā, kā? Ja ne - kāpēc?
Paskaidrojiet, kā Jums tas liek justies.

2. Moduļa mācību rezultāti

Zināšanas

- Izglītojamais zinās, kā konstatēt kibermobingu un kā upuris jūtas to piedzīvojot.
- Izprotot kibermobinga iezīmes un apzinoties metodes, kā to risināt, jaunieši, pieaugušie un pedagogi var palīdzēt izveidot labāku, empātiskāku digitālo pasauli.

Prasmes

- Izglītojamais izpratīs, kā atpazīt, ja kāds tiek emocionāli pazemots.
- Izglītojamais pratīs orientēties, kāds reakcijas un atbalsta līmenis ir nepieciešams atkarībā no konkrētā scenārija.

Kompetences

- Izglītojamais pratīs atpazīt kibermobinga epizodes un nekavējoties tos risināt, izmantojot atbilstošus rīkus.
- Izglītojamais varēs identificēt, kurš ir vislabākais un atbilstošākais atbalsta veids, kas jāsniedz konkrētajā gadījumā.

3. Bibliogrāfija

https://socialmediavictims.org/cyberbullying/effects/
https://americanspcc.org/impact-of-cyberbullying/
https://www.unicef.org/end-violence/how-to-stop-cyberbullying
https://www.security.org/resources/cyberbullying-resources-books-podcasts/

1. Moduļa pārskats

Mērķa grupa

- VET pedagogi
- Izglītības nozarē strādājošo publisko iestāžu pārstāvji: pašvaldības, reģionālās un valsts varas iestādes

Moduļa apraksts

Šis ir turpinājums modulim "Kibermobings. Kas tas ir? Kā mēs varam to atklāt?" (Modulis 2) un tā mērķis sniegt kompetences, lai veicinātu izpratni par kibermobingu un nodrošinātu preventīvus paņēmienus, lai nekļūtu par kibermobinga upuri.

Mācību mērķi

- Izprast preventīvo pasākumu nozīmi
- Izpratnes veicināšana par kibermobingu
- Palielināt izpratni par kibermobinga novēršanas metodēm

.

Ilgums

1,5 stundas

1.nodaļa - Kāpēc novērst kibermobingu?

Šo nodaļu instruktors nodrošinās kā PowerPoint prezentāciju, kurā būs ietverts teorētiskais materiāls, kā arī vairāki vizuālie elementi, piemēram, īsfilmas un uz reālās dzīves balstīti kibermobinga scenāriji, apkopojot slaidos ietverto informāciju (katrai nodaļai veltot 20-30 min.).
Mēs iesakām sagatavot prezentācijas, izmantojot CYBER.EU.VET pielāgotu veidni, ko var atrast projekta mājas lapā. Pēc prezentācijas ir paredzēta grupas diskusija, kurā ikviens var dalīties viedoklī un sajūtās par apgūto informāciju.

Mācību aktivitāte 1

Ieteicamais saturs, ko pasniedzējs nolasa audzēkņiem (maks. 20 min.):

Novērst vai iejaukties?

Saskaņā ar pētījumiem – personas, kas tiek emocionāli pazemotas, piedzīvo negatīvus iznākumus, t.sk. emocionālus, fiziskus, garīgus, kā arī akadēmiskās grūtības. Turklāt kibermobings ir būtisks jauniešu stresa avots. Kibermobinga rezultātā upuri ir psiholoģiski ievainoti, izjūt kaunu un dažreiz bailes. Viņi ne tikai vaino sevi par piedzīvoto uzmākšanos un ļaunprātīgu rīcību, bet jūtas arī ārkārtīgi satraukti. Pētījumi liecina, ka vairāk nekā 35% indivīdu, pret kuriem tika vērsts kibermobings, pauduši stresa simptomus. Šāda veida emocionālā pazemošana var būt īpaši kaitīga, jo bieži vien tā ir publiska. Parasti daudzi cilvēki var redzēt, kas ir rakstīts vai ievietots internetā. Ir grūti vai pat neiespējami izdzēst visas pēdas par kaut ko, kas reiz tika publicēts tiešsaistē. Tas nozīmē, ka kibermobings var turpināties

Kad cilvēki regulāri piedzīvo uzmākšanos sociālajos medijos, izmantojot īsziņas, tūlītējo tērzēšanu un bloga ierakstus, viņi var sākt justies bezcerīgi. Viņiem var šķist, ka pašnāvība ir vienīgais veids, kā izbeigt viņu ciešanas. Tā kā kibermobinga draudi ir ļoti nopietni, profesionālās izglītības un apmācību (VET) pedagogiem ir svarīgi izglītot savus darbiniekus par šo jautājumu, pirms tas rada reālas sekas. Preventīvu pasākumu nodrošināšana samazina kibermobinga riskus.

Mācību aktivitāte 2

Grupas diskusijas (maks. 10 min)

Jautājiet saviem audzēkņiem:

- Kāpēc kibermobinga preventīvie pasākumi ir svarīgi?
- Vai Jūs kādreiz esat bijis informēts(-a) par kibermobingu?
- Kā Jūs parasti saņemat informāciju par kibermobinga pārkāpumiem?

2.nodaļa - Izpratnes veicināšana

Mācību aktivitāte 1

Ieteiktais prezentācijas saturs, ko pasniedzējs sniedz audzēkņiem (maks.30 min.):

Ir ļoti svarīgi pārrunāt ar audzēkņiem, kā droši un atbildīgi izmantot sociālos medijus, atklājot kibermobinga likumpārkāpējus, un, kā rīkoties, ja viņi tiek emocionāli pazemoti internetā.

VIDEO Cyberbullying - How to Avoid Cyber Abuse (angliski)

DOMĀ PIRMS PUBLICĒ

Studentiem savas ziņas/darba pārlasīšanu pirms publicēšanas jāpadara par pašsaprotamu praksi. Ziņu var ierakstīt sava datora vai viedtālruņa piezīmju sadaļā un vēlāk pēc dažām stundām to izskatīt, lai izlemtu, publicēt vai nepublicēt. Tā kā kiberblēži kaut kādā veidā var izmantot pret Jums to, ko publicējāt, tad Jums būs mazāka vēlme teikt kaut ko tādu, ko vēlāk nožēlosit vai ko varētu izmantot pret jums. Protams, ja kāds vēlēsies rīkoties pret Jums, tad viņš centīsies iegūt pat vismazāk nozīmīgu informāciju, līdz ar to informācijas pārbaude pirms tās publicēšanas/kopīgošanas samazinās kiberuzbrukuma smaguma līmeni. Domāšana pirms publicēšanas var palīdzēt uzturēt veselīgas "attiecības" ar sociālajiem medijiem.

ESI PIESARDZĪGS AR PUBLISKĀM IERĪCĒM

Studentiem jābūt uzmanīgiem, lietojot publiskas ierīces, piemēram, universitātes vai bibliotēkas datorus, jo uzbrucēji var to izmantot savā labā. Pastāv daudzas iespējas caur publiskajām ierīcēm inficēties ar ļaunprātīgām programmām, piemēram, **taustiņspiedienu reģistrētājs** (keyloggers).

Kā apgalvo lielākā daļa avotu, tā ir lietojumprogramma, kas diskrēti reģistrē, kuri tastatūras taustiņi tiek piespiesti. Taustiņspiedienu reģistrētājs var būt izmantots, lai pārtvertu paroles un citu personisko informāciju, kas tiek ievadīta ar tastatūras palīdzību, radot lielus draudus lietotājiem, piem., nodrošinot kibernoziedzniekiem piekļuvi Jūsu sociālo mediju kontiem. Vissvarīgākais, kas jāzina par taustiņspiedienu reģistrētājiem, ir tas, ka antivīrusa programmas tos bieži nevar atklāt, jo tirgū ir ieejami daudzi likumīgi reģistrētāji vecāku kontroles nolūkiem, uzņēmuma drošībai utt.

VIDEO Could a Keylogger Be Spying on You? (angliski)

Papildus specializētajām uzraudzības programmām studentiem ir jāatgādina par izrakstīšanos no saviem kontiem, jo viņi tos nejauši var atstāt atvērtus un pieejamus tiem, kas atradīsies pie blakus esošajiem datoriem.

AIZSARDZĪBA TIEŠSAISTĒ

Kibermobinga un citu krāpniecisku darbību apkarosanai, ir ļoti svarīgi visur izmantot spēcīgas paroles. Spēcīga parole ir tā, kuru nevar viegli uzminēt vai uzlauzt. Spēcīgai parolei ir jābūt garai, un tajā jāiekļauj cipari, īpašās rakstzīmes un mazie/lielie burti, Parolei nekādā gadījumā nedrīkst ietvert acīmredzamu informāciju, piemēram, vārdu, dzimšanas datumu u.tml.

Aizsargājot savus kontus, Jūs nodrošināsiet to, ka neviens tiem nevar piekļūt.

PAR KIBERMOBINGA GADĪJUMIEM IR JĀZIŅO!

Make Pārliecinieties, ka Jūsu studenti saprot, cik svarīgi ir ziņot par kibermobinga gadījumiem. Tas ietver ne tikai kibermobinga identificēšanu, bet arī sociālo mediju platformas, interneta pakalpojumu sniedzēja un citu iesaistīto pušu informēšanu. Lai izbeigtu uzmākšanos, audzēkņiem, iespējams, vajadzētu informēt vietējās tiesību aizsardzības iestādes (valsts policiju).

Kad audzēkņi ir iesnieguši visas sūdzības, veiciet nepieciešamās darbības, lai bloķētu personu kontu, kas iesaistīti kibermobingā. Viņiem arī jāapzinās, ka pat pēc bloķēšanas likumpārkāpēji var izveidot alternatīvus kontus, lai atgrieztos pie upura. Ja emocionālā pazemošana notiek internetā, tad to var ierakstīt, saglabāt vai parādīt kādam, kas var palīdzēt. Ir svarīgi, lai cietušie saglabā šos pierādījumus, ja situācija paliek nekontrolējama.

VIDEO: IGNORE OR REPORT A CYBER BULLY (ANGLISKI)

Mācību aktivitāte 2

Prezentējiet studentiem šādu notikuma scenāriju (Erasmus+ projekts YouProMe)

YouProMe Erasmus+ project – www.youpromeproject.eu

Džesikai ir 18 gadi. Viņa dzīvo kopā ar saviem vecākiem, viņi abi ir profesionāļi un vienmēr ir aizņemti ar darbu. Džesika ir vecākā no visiem trim bērniem. Ģimenē nevienam nav būtisku veselības problēmu. Viņa mācās skolā un ir čakla skolniece. Džesika patīk dzīvnieki un viņa labprāt pavada laiku kopā ar draugiem. Viņai ir puisis. Džesikai ir mobilais tālrunis un viņa regulāri izmanto sociālos tīklus.

Džesika ziņoja: "Pirms dažām nedēļām savam puisim nosūtīju dažus attēlus. Jebkurā gadījumā domāju, ka viņš ir mans puisis, bet tad viņš tos parādīja savam draugam, un viņa draugs tos nosūtīja visiem pārējiem. To uzzināja skolā, un tad policija ir runājusi ar viņu un viņa draugu. Kopš tā laika neesmu gājusi uz skolu, bet sociālajos tīklos tagad visi mani sauc par padauzu. Es nevaru izturēt, kad viņi skatās uz mani, un es jau zinu, ko viņi domā. Pat meitenēm ir līdzīgs viedoklis par mani. Stulbākais ir tas, ka visi tā dara, visi sūta bildes, bet man vienkārši nepaveicās ar puisi, kurš mani nodeva. Es nekad vairs nevienam neuzticēšos. Es jutos tā, it kā viss ir beidzies un atpakaļ ceļa vairs nav."

Tā rezultātā Džesika jau mēnesi nav bijusi skolā un atsakās tajā atgriezties. Viņa ir atteikusies no visām savām skolas sporta aktivitātēm. Viņas māte ir kopā ar sporta jaunatnes darbinieku un ir teikusi, ka ir nobažījusies par dažām "tumšajām" lietām, ko Džesika saka. Džesika vēlas mainīt savu klātbūtni sociālajos tīklos un atgūt sākotnējo pārliecību. Džesika un viņas ģimene nezina, kāds atbalsts ir pieejams un kā vislabāk atbalstīt viņas garīgo veselību, nezina arī, kā jaunatnes darbinieks var būt starpnieks šajā situācijā. Džesika ir sapratusi interneta ļaunprātīgas izmantošanas risku un atzinusi, ka viņai ir nepieciešams atbalsts, lai pārvaldītu savu garīgo veselību, jo tas ir ietekmējis viņas lēmumu pieņemšanu.

Tagad varat uzsākt sarunu, balstoties uz šiem jautājumiem (maks. 30 minūtes):

- Kādi riski šeit pastāv?
- Kādi dienestus šeit būtu jāiesaista?
- Kā Jūs ieteiktu rīkoties Džesikai un viņas mātei?

2. Moduļa mācību rezultāti

Zināšanas

- Izglītojamais izpratīs kibermobinga novēršanas būtību.
- Izglītojamais zinās, kādi preventīvi rīki ir pieejami, lai izvairītos no kibermobinga.

Prasmes

- Izglītojamais pārzinās, kā atpazīt gadījumus, ja kāds tiek emocionāli pazemots.
- Izglītojamais pratīs orientēties, kāds reakcijas un atbalsta līmenis ir nepieciešams atkarībā no konkrētā scenārija.

Kompetences

- Izglītojamais spēs īstenot efektīvus izpratnes veicināšanas pasākumus pret kibermobingu.
- Atkarībā no situācijas, izglītojamais varēs noteikt, kāds palīdzības veids ir nepieciešams.

3. Bibliogrāfija

https://www.verywellfamily.com/how-to-prevent-cyberbullying-5113808
https://anti-bullyingalliance.org.uk/sites/default/files/uploads/attachments/cyberbullying-and-send-module-final%281%29_1.pdf
https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/
https://www.connectsafely.org/tips-to-help-stop-cyberbullying/

AUTENTIFIKĀCIJA UN PAROLES

Modulis 4

1. Moduļa pārskats

Mērķa grupa

- VET pedagogi
- Studenti
- Izglītības nozarē strādājošo publisko iestāžu pārstāvji: pašvaldības, reģionālās un valsts varas iestādes

Moduļa apraksts

Profesionālās izglītības un apmācību (VET) speciālisti un viņu audzēkņi ikdienā saskaras ar dažādiem kiberdrošības apdraudējumiem. Lai gan tiešsaistē ir pieejami dažādi izglītojoši materiāli par kiberdrošību, tie ne visi ir atjaunināti vai arī izglītojamie tos uztver kā pārāk vienkāršus vai pārāk sarežģītus.

Šī moduļa saturs nodrošinās izglītojamos (moduļa dalībniekus) ar prasmēm un zināšanām, lai uzlabotu viņu izpratni par autentifikāciju un parolēm, kā arī pilnveidos prasmes izvairīties no kiberdrošības uzbrukumiem. Labāk aprīkoti VET pedagogi varēs turpināt atbalstīt savus audzēkņus, lai viņi atpazītu ikdienas apdraudējumus un arī mācētu no tiem izvairīties.

Mācību mērķi

- Uzlabot izpratni par autentifikāciju kiberdrošībā
- Uzlabot izpratni par dažādām autentifikācijas metodēm
- Uzlabot izpratni par visbiežāk izmantoto autentifikācijas metožu galvenajām iezīmēm
- Izprast riskus, neizmantojot sarežģītas paroles
- Nodrošināt metodes, lai viegli būtu pārvaldīt sarežģītas paroles

Ilgums

2 stundas

1.nodaļa - Autentifikācija

Šo nodaļu pasniedzējs īstenos kā PowerPoint prezentāciju, kurā dalīsies teorētiskajās zināšanās kopā ar vairākiem vizuāliem elementiem – īsiem video, apkopojot slaidos ietverto informāciju (maks. 20 minūtes).

Prezentāciju ieteicams sagatavot, izmantojot CYBER.EU.VET pielāgotu veidni, ko var atrast projekta mājas lapā. Sakarā ar straujo attīstību un progresu kiberdrošības jomā ieteicams regulāri pārskatīt moduļa informāciju un nepieciešamības gadījumā pielāgot saturu atbilstoši jaunākajiem notikumiem šajā jomā.

Pēc prezentācijas seko 10 minūšu gara grupas diskusija, lai pārdomātu apgūto un novērtētu izglītojamo izpratnes līmeni par tēmu, kā arī radītu vietu turpmākiem jautājumiem un atsauksmēm.

Mācību aktivitāte 1

Pasniedzējs sagatavo prezentāciju ar šādu ieteicamo saturu (maks. 20 minūtes):

Kas ir autentifikācija?

Autentifikācijas process datorsistēmu kontekstā nozīmē lietotāja identitātes nodrošināšanu un apstiprināšanu. Pirms lietotājs mēģina piekļūt informācijai, kas glabājas tīklā, viņam jāpierāda sava identitāte un atļauja piekļūt datiem. Ielogojoties tīklā, lietotājam ir jānorāda unikāla pieteikšanās informācija, tostarp lietotājvārds un parole. Šī prakse tika izstrādāta, lai aizsargātu tīklu pret hakeru iekļūšanas. Autentifikācija pēdējos gados ir manāmi paplašinājusies, pieprasot vēl vairāk personiskās informācijas no lietotāja, piemēram, biometriju, lai nodrošinātu konta un tīkla drošību no tiem, kam ir tehniskās prasmes, lai izmantotu ievainojamības.

VIDEO: WHAT IS AUTHENTICATION? (ANGLISKI)

Kāpēc autentifikācija ir svarīga?

Autentifikācija ir būtisks solis, lai nodrošinātu lietotāju datu drošību, un novērstu un bloķētu jebkādu nesankcionētu piekļuvi tiešsaistes datiem. Ja autentifikācija nav droša, sistēmai var viegli uzbrukt un to uzlauzt, un kibernoziedznieki var piekļūt sistēmā glabātajiem datiem un informācijai.

Ir ļoti svarīgi to novērst un pārliecināties, ka lietotāji pārzina dažādas brīvi lietojamas vai bezmaksas pieejamas autentifikācijas metodes, lai novērstu jebkādu nesankcionētu piekļuvi saviem personas vai profesionālajiem datiem. Organizācijām un uzņēmumiem ir ieteicams ieguldīties augstas kvalitātes autentifikācijas rīkos, lai aizsargātu savus tiešsaistes datus no iespējamiem pārkāpumiem.

VIDEO: WEEKLY CYBERSECURITY TIP - AUTHENTICATION (ANGLISKI)

Izplatītas metodes autentifikācijai ar paroli

Ņemot vērā nemitīgi mainīgo kiberdraudu un uzbrukumu raksturu, pēdējos gados ir izstrādāts plašs dažādu autentifikācijas metožu klāsts.

Dažas no visizplatītākajām autentifikācijas metodēm ir:

1. Standarta autentifikācija ar paroli
2. Divu faktoru (divpakāpju) autentifikācija
3. Autentifikācija ar marķierīci
4. Biometriskā autentifikācija
5. Datora atpazīšanas autentifikācija
6. Cilvēktests jeb CAPTCHA

1. STANDARTA AUTENTIFIKĀCIJA AR PAROLI

- Visvienkāršākais un visbiežāk izmantotais autentifikācijas veids.
- Nepieciešams ievadīt lietotājvārdu kopā ar paroli, kas ļauj piekļūt tīklam, kontam vai lietojumprogrammai.

Lai samazinātu paroles uzlaušanas risku, lietotājiem ir jāizveido spēcīga parole. Drošs paroļu pārvaldnieks vai programmatūra var palīdzēt novērst jebkādu nesankcionētu piekļuvi tiešsaistē glabātajiem datiem.

2. DIVU FAKTORU AUTENTIFIKĀCIJA (2FA)

- Divu faktoru autentifikācija prasa, lai lietotāji autentificētos, izmantojot to, ko "viņi zina"(zināšanas) un to, ko "viņiem ir" (īpašums). Parole vai PIN kods kalpo kā zināšanas, un konkrēts fizisks objekts, piemēram, viedtālrunis, kodu kalkulators – kalpo kā īpašums.
- Divfaktoru autentifikācijai lietotājam parasti ir jāievada savs lietotājvārds, parole un vienreizējs kods, kas tiek nosūtīts uz fizisko ierīci (mobilo tālruni, karšu lasītāja ierīci utt.).

3. AUTENTIFIKĀCIJA AR MARĶIERĪCI (TOKEN)

- Marķierīces sistēmās tiek izmantota speciāli izveidota fiziska ierīce, kas uzrāda pastāvīgi mainīgu identifikatora kodu, lai nodrošinātu divu faktoru autentifikāciju. To ieteicams izmantot, ja nevēlaties paļauties uz mobilajiem tālruņiem.
- Tas varētu būt sargspraudnis, kas tiek ievietots ierīces USB portā, vai viedkarte ar radiofrekvences identifikāciju vai tuva darbības lauka sakaru mikroshēmu (NFC).
- Lai uzturētu marķiera sistēmas drošībā, ir ļoti svarīgi nodrošināt, lai fiziskā autentifikācijas ierīce (t.i., sargspraudnis vai viedkarte) nenonāktu nepareizās rokās.

4. BIOMETRISKĀ AUTENTIFIKĀCIJA

- Biometriskā autentifikācija balstās uz lietotāja fiziskajām īpašībām, lai tos identificētu. Biometriskajā autentifikācijā izmanto pirkstu nospiedumus, acs tīklenes vai varavīksnenes skenēšanu vai sejas un balss atpazīšanu. Šis ir ļoti drošs autentifikācijas veids, jo divām personām nebūs vienādas fiziskās īpašības. Biometriskā autentifikācija ir efektīvs veids, kā precīzi zināt, kurš logojās sistēmā.

5. DATORA ATPAZĪŠANAS AUTENTIFIKĀCIJA

- Datora atpazīšana ir paroles autentifikācijas metode, kas verificē lietotāja leģitimitāti, pārbaudot, vai viņš atrodas noteiktā ierīcē. Šīs sistēmas instalē nelielu programmatūras spraudni (plug-in) lietotāja ierīcē, pirmo reizi veiksmīgi ielogojoties. Šis spraudnis satur kriptogrāfijas ierīces marķieri. Kad lietotājs nākamreiz piesakās, marķieris tiek pārbaudīts, lai pārliecinātos, ka viņš atrodas tajā pašā uzticamajā ierīcē.
- Šī sistēma lietotājam ir neredzama, un tai nav nepieciešamas nekādas papildu autentifikācijas darbības. Vienkārši tiek ievadīts lietotājvārds un parole, un verifikācija notiek automātiski.
- Lai uzturētu augstu drošības līmeni, datorizētām atpazīšanas autentifikācijas sistēmām ir jāiespējo pierakstīšanās no jaunām ierīcēm, izmantojot citus verifikācijas veidus (piemēram, divu faktoru autentifikāciju ar kodu, kas tiek piegādāts ar SMS palīdzību).

6. Cilvēktests jeb CAPTCHAS

- CAPTCHA nav vērsta uz konkrēta lietotāja verifikāciju, kā to dara citas šajā rakstā uzskaitītās metodes. Tā vietā CAPTCHA mērķis ir noteikt, vai lietotājs ir cilvēks, lai novērstu datora vadītus mēģinājumus uzlauzt kontus, piemēram, brutāla spēka uzbrukumus.
- CAPTCHA sistēma parāda “izkropļotu” burtu un ciparu attēlu vai arī attēlus un lūdz lietotājam ierakstīt to, ko viņš redz uz ekrāna. Tā kā datoriem un robotprogrammatūram ir grūti noteikt šos “izkropļojumus”, CAPTCHA palielina drošību, radot papildu barjeru automatizētām uzlaušanas sistēmām.

Mācību aktivitāte 2

Grupas diskusija – jautājumi un atbildes; Novērtēšana un atsauksmes (maks. 10 minūtes)
Ieteicamie jautājumi novērtēšanai:

- Kas ir autentifikācija?
- Kāpēc autentifikācija ir svarīga?
- Kādas pašlaik ir visizplatītākās autentifikācijas metodes un kādas ir to galvenās īpašības?

2.nodaļa - Paroles

Mācību aktivitāte 1

1. LIETAS, KURAS CILVĒKIEM NEVAJADZĒTU DARĪT

Slaidi ar attēliem, kas parāda lietas, kuras cilvēkiem nevajadzētu darīt, paradoties plašākā auditorijā.

GADĪJUMU IZPĒTE

- "Beļģijas policija nopublicēja ierakstu ar WiFi paroli. To rādīja nacionālajā televīzijā" - https://www.reddit.com/r/cybersecurity/comments/cnkhft/the_belgian_police_have_a_post_it_with_the_wifi/
- "Havaju salu neatliekamās palīdzības dienesta parole bija slēpusies publiskajā fotoattēlā, kas bija uzrakstīta uz Post-it līmlapiņas" - https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1
- "Četras apkaunojošas paroles noplūdes televīzijas tiešraidē" - https://www.itgovernance.co.uk/blog/four-embarrassing-password-leaks-on-live-tv

2. STATISTIKA

Dažu statistikas datu prezentācija:

- 81% no visiem ar datiem saistītiem pārkāpumiem notiek sliktas paroles drošības dēļ
- Slikti darbinieku paroles paradumi
- Top 200 populārākās paroles

3. DROŠAS PAROLES NOZĪME

Neuzlaužamas paroles anatomija

4. PAMATNOTEIKUMI

Raksturojiet pamatnoteikumu kopumu, piemēram:

- Neizmantojiet pārlūkprogrammas paroļu pārvaldniekus; "ļaunprātīgā programmatūra" var viegli tiem piekļūt.
- Nekopīgojiet savu paroli.
- Iegaumējiet, nevis ierakstiet paroles uz papīra vai digitāli.
- Regulāri mainiet paroles (vismaz reizi divos mēnešos).
- Ja iespējams, iespējojiet divu faktoru autentifikāciju.
- Katrā vietnē jāizmanto cita parole.
- Iegādājoties jaunu ierīci, nomainiet sākotnējo paroli.
- Nelietojiet parastos vārdus. Viens no biežākajiem uzbrukuma veidiem notiek caur "vārdnīcas" izmantošanu.

Drošas paroles noteikumi:

- Izveidojiet sarežģītas paroles: vismaz 12 rakstzīmes, ar lielajiem un mazajiem burtiem, cipariem un speciālajām rakstzīmēm.
- Neizmantojiet viegli "atklājamus" terminus: ar savu vārdu, dzimšanas pilsētu vai zināmiem terminiem, mājdzīvnieka vārdu, automašīnas reģistrācijas numuru; mobilā tālruņa numuru, ģimenes svētku datumiem, utt.
- Iegaumējiet, nevis pierakstiet.
- Izveidojiet personīgo "atslēgu", kas ir daļa no visām parolēm.
- Izmantojiet teicienu, izplatītus izteicienus vai kaut ko viegli iegaumējamu. Piem., izmantojiet katra vārda pirmos divus burtus.
- Pārslēdzaties starp lielajiem, mazajiem burtiem un simboliem.
- Pievienojiet kaut ko, kas ir saistīts ar vietni/rīku.

Mācību aktivitāte 2

Grupas vingrinājums

Pārbaudiet savas paroles garumu! - https://www.passwordmonster.com

Vai esmu jau uzlauzts? - https://haveibeenpwned.com/Passwords

Diskusija un atsauksmes (maks. 10 min.)

Ieteicamie jautājumi novērtēšanai:

- Cik gadus Jūsu parole izturēs parasto uzlaušanas (crack) algoritmu mašīnu?
- Vai man vajadzētu mainīt savu paroli?

Mācību aktivitāte 3

Pasniedzējs sagatavo prezentāciju ar šādu ieteicamo saturu (maks. 20 minūtes):

Kas ir paroļu pārvaldnieki?

- Digitālie seifi
- Ļauj saglabāt dažādu pakalpojumu pilnvaras un piezīmes
- Bankas rekvizīti arī var būt aizsargāti
- Viena galvenā atslēga

Var būt izmantota biometriskā autentifikācija.

Vietējie paroļu pārvaldnieki

- Saglabājiet datus pašreizējā ierīcē
- Paroles fails ir šifrēts
- Katru paroli ir atļauts saglabāt citā šifrētā failā
- Atļauj izmantot tikai vienā ierīcē

Piemēram, KeypassXC

Tiešsaistes paroļu pārvaldnieki

- Dati tiek glabāti mākonī
- Atļauj piekļūt dažādu pakalpojumu pilnvaras datiem un piezīmēm jebkurā ierīcē
- Nav nepieciešama uzstādīšana
- Viena galvenā atslēga
- Dati tiek šifrēti no ierīces uz serveri

Piemēram, Bitwarden, Latspass, Keeper, 1Password

Fizisko paroļu pārvaldnieki

- Fiziskās ierīces (piemēram, USB pildspalva)
- Sinhronizācija nav nepieciešama
- Katrai autentifikācijai tiek ģenerēta piekļuves atslēga
- Ja mēs pazaudējam ierīci, mēs zaudējam piekļuvi!!!

Piemēram, OnlyKey

Mācību aktivitāte 4

Grupas praktiskā aktivitāte

- Izveidojiet sarežģītu paroli
- Instalējiet paroļu pārvaldnieku portatīvajā datorā vai viedtālrunī
- Aktivizējiet MFA/2FA

Diskusija un atsauksmes (maks. 10 minūtes)

Ieteicamie jautājumi novērtēšanai:

- Cik grūti tas bija?
- Vai izmantosiet kādu no šīm labās prakses piemēriem?

2. Moduļa mācību rezultāti

Zināšanas

- Izpratne par autentifikācijas definīciju, tās nozīmi un dažām izplatītākajām autentifikācijas metodēm
- Izpratne par riskiem, neizmantojot sarežģītas paroles
- Labo prakšu izmantošana, lai pārvaldītu personīgās paroles

Prasmes

- Identificēt un izmantot vispiemērotāko autentifikācijas metodi
- Noteikt un lietot vispiemērotāko paroles sarežģītību

Kompetences

- Saprast autentifikācijas nozīmi
- Izlemt par vispiemērotāko autorizācijas metodi dažādām tiešsaistes darbībām un izmantot tās, lai uzlabotu tiešsaistes drošību
- Izprast sarežģītu paroļu izmantošanas nozīmi
- Strukturēt labāko prakšu metodes personīgo paroļu pārvaldībai

3. Bibliogrāfija

https://www.sangfor.com/blog/cybersecurity/the-basics-of-authentication-in-cyber-security

https://www.passportalmsp.com/blog/which-password-authentication-method-works-best-businesses

1. Moduļa pārskats

Mērķa grupa

- VET pedagogi
- VET studenti
- Publiskās un privātās ieinteresētās puses, kuras vēlās uzlabot zināšanas un izpratni par kiberdrošības apdraudējumiem

Moduļa apraksts

Šajā modulī galvenā uzmanība tiks pievērsta faktisko apdraudējumu izgaismošanai, pieslēdzoties publiskajām Wi-Fi sistēmām, kā tie darbojas un kā tos novērst.

Mācību mērķi

- Izpratnes veicināšana par maldīgiem priekšstatiem par publisko Wi-Fi tīklu izmantošanu
- Sniegt zināšanas par apdraudējumiem, ko rada publisko Wi-Fi tīklu izmantošana

Ilgums

1 stunda

1.nodaļa

Modulis ietver gan video mācību daļas, gan atklātas diskusijas. Proti, sākotnēji tiks rādīts pirmais ievada video. Šis video ar eksperta palīdzību parāda, kā publiskie tīkli ir riskanta vieta, lai pieslēgtos internetam. Tomēr šis pirmais videoklips ir ļoti īss, un tas neļauj aptvert lielu daļu no tālāk esošā procesa. Šī pirmā daļa noslēdzas ar diskusiju starp audzēkņiem.

2.nodaļa

Otrkārt, tiks nodrošināts konkrētāks video. Neskatoties uz tā neformālo veidu, kā risināt šo jautājumu, video noteikti labāk aptver šo jautājumu. Kad video ir noskatīts, instruktors/ pasniedzējs tiek aicināts izvirzīt diskusijas par publisko tīklu riskiem dalībnieku vidū un, ja iespējams, dalīties savā personīgajā pieredzē.

Mācību aktivitāte 1

Viens no aspektiem, kam šis modulis vēlas pievērst uzmanību, ir mehānismi, ar kuriem tiek izvirzīti publiskie Wi-Fi draudi. Nepārtraukta mācību aktivitāte ir mēģinājums pielietot ieteikumus, kas iegūti, izmantojot šī moduļa video saturu, sākot no restorāna/bāra, kur dalībnieki ieturēs maltīti pusdienu pārtraukumā, līdz dzelzceļa/autobusa stacijai, kur dalībnieki apstāsies pirms atgriezties mājās pēc apmācībām.

2. Bibliogrāfija

https://www.youtube.com/watch?v=4YbXXW3DLQM&ab_channel=Techquickie
https://www.youtube.com/watch?v=1OVTmrXGHyU&ab_channel=CBSBoston
https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks
https://goodspeed.io/blog/7-dangers-of-public-wifi.html
https://www.youtube.com/watch?v=NkNgW3TwMy8&ab_channel=TheModernRogue

SOCIĀLO TĪKLU IZMANTOŠANA

Modulis 6

1. Moduļa pārskats

Mērķa grupa

- VET pedagogi
- Studenti
- Izglītības nozarē strādājošo publisko iestāžu pārstāvji: pašvaldības, reģionālās un valsts varas iestādes

Moduļa apraksts

Tiešsaistes sociālie tīkli (Online Social Networks, OSN) ir ieņēmuši vēl nebijušu vietu cilvēku profesionālajā, izglītības un privātajā ikdienas dzīvē, tostarp profesionālās izglītības un apmācību (VET) pedagogu un viņu audzēkņu jomā. Kamēr šādas integrācijas priekšrocības ir bijis vieglāk atpazīt un adaptēt kā formālās un neformālās izglītības neatņemamu sastāvdaļu, ar to saistītajiem riskiem nav pievērsta tāda pati uzmanība, un paši pedagogi tos bieži vien ignorē.

Vienkāršotā pieeja daudzpusīgajam sociālo tīklu drošības jautājumam, kā arī dažu pieejamo mācību materiālu sarežģītība nav pietiekams, lai izveidotu nepieciešamo kapacitāti draudu novēršanai un reaģēšanai, ko rada šo platformu izmantošana.

Šī moduļa mēģinājums ir nodrošināt izglītojamiem pamatzināšanu kopumu un stiprināt viņu apmācību kapacitāti, kā arī uzlabot viņu personīgo pieeju sociālo tīklu drošībai.

Mācību mērķi

- Izpratnes veicināšana par kiberriskiem un apdraudējumiem, kas saistīti ar sociālo mediju un tīklu izmantošanu
- Stiprināt dezinformācijas procesa ietekmi uz lietotāju veidota satura (User-generated content, UGC) platformu drošību
- Veicināt dažādu kiberdrošības draudu veidu identificēšanu
- Stiprināt spēju novērst un reaģēt uz kiberdraudiem sociālajos tīklos
- Nodrošināt metodes, lai vienkāršā veidā pārvaldītu sarežģītas paroles

Ilgums

2 stundas

1.nodaļa - Sociālo tīklu apdraudējumi

Šī nodaļa tiks nodrošināta, izmantojot Power Point prezentāciju. Tajā tiks piedāvāta dažu ziņu virsrakstu lasīšana ar plaši izplatītiem stāstiem par kiberdraudu upuriem, izmantojot sociālos tīklus.
Stāsti un saturs tiks pielāgoti tā, lai tie atbilstu kontekstam, un atjaunināti atbilstoši jaunākajiem datiem, informācijai.
Pēc prezentācijas ir paredzēta 10 minūšu gara grupas diskusija, lai noskaidrotu dalībnieku viedokļus par moduli un novērtētu izglītojamo izpratnes līmeni par tēmu, kā arī radītu vietu turpmākiem jautājumiem un atsauksmēm.

Mācību aktivitāte 1

Ieteiktais prezentācijas saturs, ko pasniedzējs nolasa audzēkņiem (maks.20 min.):

Kas ir tiešsaistes sociālie tīkli?
Tiešsaistes sociālais tīkls (OSN) ir sociāla struktūra, ko veido indivīdi vai organizācijas, kurus sauc par mezgliem (mezglu grupām) un kurus savieno viens vai vairāki specifiski saskares punkti, piemēram, draudzība, kopīgas intereses, apmaiņa ar finansēm, uzskati par attiecībām, zināšanas vai prestižs. Sociālo tīklu vietnes, piemēram, Facebook, Twitter, Instagram utt., ir domātas ne tikai saziņai vai mijiedarbībai ar citiem cilvēkiem visā pasaulē, bet ir arī efektīvs rīks uzņēmējdarbības veicināšanai. Atšķirībā no tradicionālajām tīmekļa un mediju platformām, sociālie tīkli ir paredzēti tikai lietotāju radīta satura (UGC) mitināšanai un izplatīšanai atbilstoši kritērijiem (algoritmiem), kuru pamatā ir pašu lietotāju izteiktās un datos reģistrētās darbības un preferences. Šajā ziņā visi lietotāji aktīvi piedalās sociālo tīklu procesu ilgtspējības veicināšanā.

Kas ir sociālo mediju apdraudējumi?
Sociālo mediju apdraudējumi var būt jebkas, kas apdraud lietotāja konta drošību. Kiberdraudi var būt gan tīši, gan netīši; mērķtiecīgi vai nemērķēti, un tie var nākt no dažādiem avotiem, t.sk. no ārvalstu nācijām, kas iesaistītas spiegošanā un informatīvajā karā, no noziedzniekiem, hakeriem, vīrusu rakstītājiem, neapmierinātiem darbiniekiem un līgumslēdzējiem, kas strādā iekš organizācijas.

SOCIĀLO TĪKLU IZMANTOŠANA

Modulis 6

Kā izskatās sociālo mediju apdraudējumi?

Tā kā sociālajos tīklos ir milzīgs lietotāju skaits un tajos glabājas milzīgs datu apjoms, tie ir dabiski mērķi surogātpasta izplatītājiem, pikšķerēšanai un ļaunprātīgiem uzbrukumiem. Turklāt tiešsaistes sociālie uzbrukumi ietver identitātes zādzību, neslavas celšanu, vajāšanu, personas cieņas aizskaršanu un kibermobingu. Hakeri veido viltus profilus un atdarina personības vai zīmolus, vai arī apmelo pazīstamu personu tās draugu lokā.

Privātums attiecas uz prasību, lai lietotāju profili nekad nepublicētu un neizplatītu informāciju tīmeklī. Dažāda informācija personiskajās mājas lapās var saturēt ļoti sensitīvus datus, piemēram, dzimšanas datumus, mājas adreses, personīgos mobilo tālruņu numurus utt. Šo informāciju var izmantot hakeri, kuri pielieto sociālās inženierijas paņēmienus, lai gūtu labumu no šādas sensitīvas informācijas un zagtu naudu.

Kā sociālo mediju apdraudējumi mainās dažādās platformās?

Sociālo mediju apdraudējumu veids ir atkarīgs no uzbrucēja mērķiem. Facebook nodrošina lietotājiem iespēju turēt savus attēlus un komentārus privātā režīmā, tāpēc uzbrucējs bieži vien var sadraudzēties ar mērķa upura draugiem vai nosūtīt draudzības uzaicinājumu mērķa upurim pa tiešo, lai piekļūtu viņa publicētajai informācijai. LinkedIn ir vēl viena izplatīta platforma sociālo mediju vidē, kas domāta biznesa tīklu veidošanai. Ja uzbrucēja mērķis ir kāds uzņēmums, LinkedIn ir lieliska sociālo mediju vietne, lai apkopotu biznesa e-pastus pikšķerēšanas uzbrukumiem. Daudzas sociālo mediju platformas publiski attēlo lietotāju ziņas, tāpēc uzbrucēji var ievākt nepieciešamo informāciju, par to nezinot lietotājam. Daži uzbrucēji veiks papildu darbības, lai iegūtu piekļuvi lietotāja informācijai, sazinoties ar mērķa upuri vai viņa draugiem.

Kāpēc ir svarīgi runāt par OSN draudiem?

Tiešsaistes interneta vidē ir gandrīz 4 miljardi lietotāju. 2020. gada 30. decembrī no kopējā interneta "iedzīvotāju" skaita 2,7 miljardi sastādīja Facebook ikmēneša dinamiskie lietotāji, 330 miljoni –Twitter aktīvie lietotāji un 320 miljoni – Pinterest vietnes lietotāji.

Sociālo tīklu vietņu izmantošana pieaug eksponenciāli. Ja skatāmies tikai uz Facebook, tad ik sekundi tiek izveidoti septiņi jauni profili, bet ik minūti tiek ievietoti 510 000 komentāru, atjaunināti 298 000 statusu un augšupielādēti 136 000 fotoattēlu. Sakarā ar to, ka nepārtraukti tiek augšupielādēts milzīgs datu apjoms, pastāv liela drošības risku iespējamība. Ikviens var publicēt ļaunprātīgu saturu, kas paslēpts multivides datos vai izmantojot saīsinātus vienotus resursu vietražus (URL) jeb tīmekļa vietņu adreses. Eksistē ~83 miljoni viltus profilu, starp kuriem var būt neleģitīmie lietotāji vai profesionāļi, kas veic testēšanu un izpēti. Katru dienu tiek uzlauztas aptuveni 1000 000 vietņu.

Lai gan dažas sociālo tīklu vietnes, piemēram, Twitter, neļauj lietotājiem izpaust privātu informāciju, tomēr pieredzējuši uzbrucēji var izsecināt konfidenciālu informāciju, analizējot lietotāja ierakstus un citu tiešsaistē ievietoto informāciju. Tiešsaistē kopīgotā personiskā informācija kibernoziedzniekiem var sniegt pietiekami daudz informācijas, lai viņi varētu iegūt mūsu e-pastu un paroles.

Personiskās informācijas vērtība

Sociālie tīkli savus pakalpojumus bieži vien piedāvā bez maksas. Personiskā informācija ir ne tikai sociālo tīklu valūta, bet arī galvenais kiberdraudu mērķis tajos.

Kiberuzbrukumu var būt viegli uzsākt, jo parasti daudzi cilvēki savu personisko informāciju sniedz sociālo mediju platformām. Uzbrucēji var viegli savākt šos datus un izmantot tos savā labā.

Informācijas vākšana datu zagšanai nav vienīgais iemesls, lai sociālos medijus izmantotu izlūkošanai. Sociālajos medijos ievietotā informācija varētu tikt izmantota, lai iegūtu paroles vai uzdotos par biznesa lietotājiem.

Izmantojot sarakstu ar mērķa grupu, uzbrucējs pārskata/izpēta sociālo mediju kontus, lai iegūtu personisko informāciju. Personiskā informācija var palīdzēt uzbrucējam iegūt mērķa uzticību sociālās inženierijas uzbrukumā. To var arī izmantot, lai uzminētu atbildes uz drošības jautājumiem konta pārņemšanai vai pietuvinātos lietotājam ar augstākām privilēģijām. Mājdzīvnieku vārdi, iecienītākās sporta komandas un izglītības vēsture ir iespējamās norādes uz paroli vai atbildes uz jautājumiem, ko izmanto, lai pārbaudītu lietotāja identitāti paroles atiestatīšanai.

Kāpēc svarīgi mācīties par OSN draudiem?

Iespējams lietotājam draudzīgās saskarnes (interface) un procesi, ko OSN platformas piedāvā, liecināja cilvēkiem, ka iepriekšējas zināšanas nav nepieciešamas, lai piekļūtu viņu pakalpojumiem un saturam.

Izglītība ir nozīmīga, lai apturētu tiešsaistes sociālo tīklu draudus.

Pirmais solis ir izglītot lietotājus par draudiem, kas saistīti ar pārāk daudz informācijas izpaušanu interneta vidē. Pat sociālo mediju konti, kas iestatīti privātajā režīmā, var tikt izmantoti uzbrukumā, ja uzbrucējs iegūtu piekļuvi privātajām ziņu plūsmām. Lietotāji nekad nedrīkst savos sociālo mediju kontos publicēt privātu korporatīvo informāciju vai informāciju, ko varētu izmantot konta pārņemšanai.

Otrais solis ir lietotāju izglītošana par to, kā tiek radīts un izplatīts digitālais saturs un kā lietotāju darbības var būt virzītas uz konkrētiem mērķiem, kuriem saturs ir izveidots. Visu sociālo mediju saturu veido un izmanto lietotāji atbilstoši viņu dažādajiem personīgajiem un/vai kolektīvajiem mērķiem. Šo iemeslu dēļ daļa no šī satura ne vienmēr var būt ērta, patiesa vai ētiski pareiza.

Visbeidzot, lietotājiem jābūt izglītotiem par to ierīču drošu lietošanu un uzturēšanu, ar kuru palīdzību viņi var piekļūt tiešsaistes sociālo tīklu pakalpojumiem, jo parasti tie ir riska un ielaušanās pārnēsātāji. Daži izglītojošie aspekti šajā sakarā jau ir ilustrēti citos apmācību moduļos, un tie nozīme:

- izvairīties no klikšķināšanas uz reklāmām, jo īpaši uznirstošajiem logiem, kas lietotājiem liek lejupielādēt programmatūru, lai skatītu saturu
- nekopīgot paroles
- izvairīties no ziņojumiem vai ierakstiem sociālajos tīklos, kas mudina uz ātru rīcību (kā sociālās inženierijas paņēmiens)
- nepieņemt draudzības uzaicinājumus no nezināmiem cilvēkiem, pat ja lietotājam ir vairāki kopīgi draugi
- izvairīties no sociālo tīklu lietošanas publiskajos Wi-Fi tīklājos (izplatīta vieta, kur uzbrucēji var “slaucīt” datus, izmantojot pārtvērējuzbrukums (man-in-the-middle attack))
- regulāri mainīt piekļuves kodus un paroles

Mācību aktivitāte 2

Lūdziet izglītojamajiem sociālo tīklu meklētājā vai Google atrast savus vārdus, lai analizētu kādu privāto informāciju par viņiem var ievākt pēc tā, kas tika atrast internetā (dzimšanas vieta un datums, ģimenes locekļi, adrese, tālruņa numurs, mājdzīvnieki, sentimentāli partneri, vaļasprieks un vēlmes). Aicināt izglītojamos pārdomāt par veidiem, kā šī informācija var būt izmantota pret viņiem.

2.nodaļa - OSN apdraudējumu veidi

Mācību aktivitāte 1

Lūdziet dalībniekus uzskaitīt visus drošības apdraudējumus, ar kuriem, viņi varētu saskarties sociālajos medijos, un lūdziet viņiem paskaidrot, vai, pēc viņu domām, draudi varētu pastāvēt pirms OSN pastāvēšanas.

DAŽĀDI DRAUDI TIEŠSAISTES SOCIĀLAJOS TĪKLOS UN MEDIJOS

Mēs varam iedalīt OSN draudus trīs kategorijās:

1. Vispārpieņemtie draudi – tādi, ar kuriem lietotāji ir saskarušies jau kopš sociālo tīklu pirmsākumiem.
2. Mūsdienu (moderni) draudi – uzbrukumi, kuros tiek izmantoti uzlabotas metodes, lai kompromitētu lietotāju kontus
3. Mērķtiecīgi uzbrukumi – tādi, kas ir vērsti pret kādu konkrētu lietotāju.

VISPĀRPIEŅEMTIE DRAUDI

Surogātpasts

Surogātpasts ir termins, ko lieto nevēlamiem lielapjoma elektroniskajiem ziņojumiem. Lai gan e-pasts ir ierastais surogātpasta izplatības veids, sociālo tīklu platforma vēl veiksmīgāk izplata surogātpastu. Likumīgo lietotāju saziņas datus var viegli iegūt uzņēmuma tīmekļa vietnēs, blogos un diskusiju grupās. Nav grūti pārliecināt mērķklientu izlasīt surogātpasta ziņojumus un uzticēties to drošībai. Lielākā daļa surogātpastu ir komerciālās reklāmas, taču tie var būt izmantoti, lai apkopotu sensitīvu informāciju no lietotājiem vai arī tie var saturēt vīrusus, ļaunprogrammatūras vai krāpniecību.

Ļaunprātīgas programmatūras uzbrukums

Ļaunprogrammatūra ir kaitīga programmatūra, kas ir izstrādāta tam, lai inficētu datorsistēmu vai piekļūtu tai, parasti bez lietotāja zināšanās. Ļaunprātīga programmatūra var izmantot sociālo tīklu struktūru, lai izplatītos, izmantojot koplietotus vietrāžus URL vai OSN apakšlietojumprogrammas, piemēram, e-spēles vai spraudņus.

Pikšķerēšana

Pikšķerēšanas uzbrukums ir sava veida sociālās inženierijas uzbrukums, kurā agresors var iegūt sensitīvu un konfidenciālu informāciju, piemēram, upura lietotājvārdu, paroli un kredītkartes datus, izmantojot viltotas vietnes un e-pastus, kas izskatās pēc patiesām.

IOSN gadījumā uzbrucējam ir jāpiesaista klients viltus lapai, kur viņš var realizēt pikšķerēšanas uzbrukumu. Lai to paveiktu, uzbrucējs izmanto dažādas sociālās inženierijas metodes. Piemēram, viņš var nosūtīt lietotājam ziņojumu, kurā teikts: "Jūsu personiskie attēli tiek kopīgoti šajā vietnē, lūdzu, pārbaudiet!". Noklikšķinot uz šī URL, lietotājs tiek novirzīts uz viltotu tīmekļa vietni, kas izskatās pēc kādas likumīgas sociālā tīkla vietnes.

MŪSDIENU DRAUDI

Starpvietņu skriptošanas uzbrukums (XXS)

Starpvietņu skriptēšana ir ļoti izplatīts uzbrukuma vektors. Tā ir ļaunprātīga mājaslapas koda izmaiņu veikšana, lai piekļūtu lietotāja sensitīvajai informācijai. Būtībā uzbrukumā tiek izpildīts ļaunprātīgs JavaScript upura pārlūkprogrammā, izmantojot dažādas metodes. Pārlūkprogrammu var nolaupīt tikai ar vienu pogas klikšķi, kas var nosūtīt serverim ļaunprātīgu skriptu. Šis skripts "atlido" atpakaļ pie upura un tiek izpildīts pārlūkprogrammā. Pievilcīgas saites un pogas populārās sociālo tīklu vietnēs, piemēram, Twitter un Facebook, var maldināt lietotājus sekot URL, vīrusu uznirstošajiem brīdinājumiem un daudzsološām reklāmām vai multivides saturam, kuru atbloķēšanai nepieciešams apmeklēt saiti vai noklikšķināt uz pogas. Dažiem lietotājiem var tikt piedāvāts kopēt un ielīmēt JavaScript, kas satur saiti uz pārlūkprogrammas adrešu joslu. Šie uzbrukumi var vai nu nozagt informāciju, vai darboties kā spiegprogrammatūra. Šādi uzbrukumi var arī nolaupīt datorus, lai uzsāktu uzbrukumus lietotājiem, kur par to nenojauš, kamēr patiesais uzbrukuma izraisītājs ir paslēpts aiz apdraudētās iekārtas.

Profila klonēšanas uzbrukums

Šajā uzbrukumā tiek klonēts lietotāja profils, pateicoties iepriekšējām zināšanām vai tiešsaistē savāktajai informācijai. Uzbrucējs var izmantot šo klonēto profilu tajā pašā vai citā sociālo tīklu platformā, lai izveidotu uzticamas attiecības ar lietotāja (potenciālā upura) draugiem. Kad kontakts ir izveidots, uzbrucējs apkrāpj upura draugus, lai tie uzķertos viltus profilam, pieņemot to par īsto, un tādā veidā veiksmīgi izgūst konfidenciālu informāciju, kas neparādās viņu publiskajos profilos. Šo uzbrukumu var izmantot arī cita veida kibernoziegumu veikšanai, piemēram, kibermobingam, kibervajāšanai un šantažēšanai.

Nolaupīšana (hijacking)

Nolaupīšanas gadījumā pretinieks apdraud lietotāja kontu vai pārņem to kontroli, lai paveiktu kādu krāpšanu internetā. Vietnes bez daudzfaktoru autentifikācijas un konti ar vājām parolēm ir mazāk aizsargātas pret nolaupīšanu, jo paroles var iegūt ar pikšķerēšanas palīdzību. Kad konts ir uzlauzts, uzbrucējs var sūtīt ziņojumus, kopīgot ļaunprātīgo saiti un mainīt konta informāciju, un tas viss apdraud lietotāja kontroli pār savu kontu, kā arī viņa reputāciju.

Secinājumu uzbrukums

Šādā uzbrukumā tiek izsecināta apstrādātas personas konfidenciālā informācija, kuru lietotājs, iespējams, nevēlas izpaust. Izdarītie secinājumi balstās uz statistiku, ko lietotājs atspoguļo kādos OSN. Tajā tiek izmantotas datu ieguves metodes par publiski redzamajiem datiem, kā piemēram, lietotāja draugu saraksts un tīklu tipoloģija. Izmantojot šo paņēmienu, uzbrucējs var atrast organizācijas slepeno informāciju vai lietotāja ģeogrāfisko un izglītības informāciju.

Sibilas uzbrukums/botu tīkls (robottīkls)

Sibilas uzbrukumā mezgls (dators) pieprasa vairākas identitātes tīklā. Tas var kaitēt sociālo tīklu platformām, jo tajās ir milzīgs lietotāju skaits, kas savienoti ar vienādranga tīklu (2P2, peer-to-peer network). Vienādrangi ir savstarpēji saistītas datoru sistēmas, izmantojot internetu, un tās var dalīties ar ierakstiem bez centrālā servera izmantošanas. Šo mašīnu tīklu var saukt arī par botu tīklu (Botnet). Vienkāršiem vārdiem, botu tīkli ir „zombēti" datori, kas dara to, ko liek „saimnieks" jeb uzbrucējs. Viena tiešsaistes vienība var izveidot vairākas viltotas identitātes un izmantot tās, lai izplatītu nevēlamu informāciju, ļaunprogrammatūru vai pat ietekmētu organizācijas reputāciju un popularitāti. Piemēram, ar tiešsaistes aptauju var manipulēt, izmantojot dažādas interneta protokola (IP) piegādes, lai iesniegtu milzīgu balsu skaitu, un agresors var pārspēt patiesu (neviltotu) klientu. Līdzīga armija, piemēram, var vairākas reizes kopīgot vienu ziņojumu un inficēt tā saturu ar vīrusu.

Klikšķu laupīšana (clickjacking)

Tā ir ļaunprātīga metode, kurā iebrucējs maldina lietotāju noklikšķināt uz lapas, kas atšķiras no tās, uz kuras viņš plānoja noklikšķināt. Lai veiktu šo uzbrukumu, uzbrucējs izmanto pārlūkprogrammu ievainojamību. Lapai, kurai lietotājs vēlās piekļūt, pa virsu tiek ielādēta cita lapa kā caurspīdīgs slānis. Divas zināmās klikšķu laupīšanas variācijas – "patīk" pogas laupīšana (likejacking) un kursora laupīšana (cursorjacking). Priekšējais slānis parāda "substanci", ar kuru klients var būt ievainots. Brīdī, kad klients uzspiež uz šo viltotu saturu, viņš faktiski uzspiež uz pogas "Patīk". Jo vairāk lietotājiem patīk ieraksts, jo vairāk tas izplatās un ir redzams. Veicot kursora laupīšanu, uzbrucējs aizstāj faktisko kursoru ar pielāgotu kursora attēlu. Kursors tiek nobīdīts no tā faktiskās peles pozīcijas. Šādā veidā uzbrucējs var mānīt lietotāju, lai viņš noklikšķinātu uz ļaunprātīgās vietnes, gudri pozicionējot lapas elementus.

Deanonimizācijas uzbrukums

Diezgan daudzās sociālo tīklu vietnēs, piemēram, Twitter un Facebook, lietotāji var paslēpt vai aizsargāt savu patieso identitāti pirms jebkādu datu izpaušanas, izmantojot aizstājvārdu vai izdomātu nosaukumu. Bet, ja trešā puse vēlas noskaidrot lietotāja patieso identitāti, to var izdarīt, izsekojot sīkfailus, tīkla topoloģijas un lietotāju grupu reģistrāciju, lai atklātu klienta īsto identitāti. Tā ir sava veida informācijas ieguves metode, kurā noslēpumaina informācija tiek savstarpēji saistīta ar citiem informācijas avotiem, lai atkārtoti atpazītu nezināmo informāciju. Uzbrucējs var ievākt informāciju par lietotāja dalību grupā, nozogot pārlūkprogrammas vēsturi un apvienojot šo vēsturi ar savāktajiem datiem. Tādējādi uzbrucējs var deanonimizēt lietotāju, kurš apmeklē uzbrucēja vietni.

MĒRĶTIECĪGI UZBRUKUMI

Kibermobings

Kibermobings ir elektronisko plašsaziņas līdzekļu, piemēram, e-pasta ziņojumu, tērzēšanas, tālruņa sarunu un tiešsaistes sociālo tīklu izmantošana, lai iebiedētu vai uzmāktos personai. Atšķirībā no tradicionālās iebiedēšanas, kibermobings ir nepārtraukts process, jo tas tiek pastāvīgi uzturēts, izmantojot sociālos medijus. Uzbrucējs atkārtoti sūta iebiedējošus ziņojumus, seksuālas piezīmes, izplata baumas un dažreiz publicē apkaunojošus attēlus vai videoklipus, lai uzmāktos cilvēkam. Viņš var publicēt arī personisku vai privātu informāciju par upuri, kas izraisa apmulsumu vai pazemojumu. Kibertiranizēšana var notikt arī nejauši, lai gan šādu e-pasta ziņojumu, īsziņu un tiešsaistes ierakstu atkārtojumi reti kad ir nejauši.

Kiber-iedraudzināšana (Cyber grooming)

Kiber-iedraudzināšana ir intīmu un emocionālu attiecību nodibināšana ar upuri (parasti bērniem un pusaudžiem) ar nolūku veikt piespiedu seksuālu vai garīgu vardarbību. Tās galvenais mērķis ir iegūt jaunieša uzticību un tad ar tā palīdzību iegūt arī intīmu un individuālu informāciju no bērna. Dati bieži vien ir baudkāres raksturā, izmantojot seksuālas sarunas, attēlus un video, kas dod uzbrucējam priekšrocības draudēt un šantažēt bērnu. Uzbrucēji bieži vēršas pie pusaudžiem vai bērniem caur viltotu identitāti bērniem draudzīgās vietnēs, atstājot viņus neaizsargātus un neinformētus par to, ka īstais nolūks ir – kiberuzmākšanās. Tomēr upuris var arī neapzināti uzsākt tīrīšanas procesu, saņemot atalgojošus piedāvājumus, piemēram, skaidru naudu apmaiņā pret kontaktinformāciju vai personīgām fotogrāfijām. Advancēto mediju anonimitāte un pieejamība ļauj ļaundariem vienlaikus vērsties pie vairākiem jauniešiem, eksponenciāli palielinot kiberkopšanas gadījumu skaitu.

Kiberizsekošana

Kiberizsekošana ir personas novērošana, izmantojot internetu, e-pastu vai cita veida elektronisko saraksti, kas rada bailes no vardarbības un traucē šīs personas garīgo mieru. Tā nozīmē personas privātumu tiesību aizskaršanu. Uzbrucējs izseko upuru personisko vai konfidenciālo informāciju un izmanto to, lai viņus apdraudētu ar nepārtrauktiem un pastāvīgiem ziņojumiem visas dienas garumā. Šāda rīcība liek upurim ārkārtīgi uztraukties par savu drošību un izraisa viņā nepatikšanas, bailes vai satraukumu. Mūsdienās lielākā daļa cilvēku savā sociālā tīkla profilā kopīgo savu personisko informāciju, piem., tālruņa numuru, dzīvesvietu, rajonu un grafiku, kā arī savu reāllaika atrašanas vietu. Uzbrucējs var apkopot šos datus un izmantot tos kiberizsekošanai.

Mācību aktivitāte 2

Dalībnieki strādā pāros. Palūdziet, lai viņi uzdodas par savu partneri, kamēr intervē viņu 10 minūtes. Piedāvājiet viņiem izmēģināt savas atbildes, mēģinot iegūt nepieciešamo informāciju no partnera ģērbšanās veida, līdzi nēsātajām ierīcēm un citām kontekstuālām detaļām, kas varētu šķist noderīgas, lai uzdotos par savu partneri.

Mācību aktivitāte 3

Palūdziet dalībniekiem pārskrullēt sociālo tīklu ierakstus 1 minūtes garumā un saskaitīt visus "aicinājumus uz rīcību", saites un pogas uz kurām viņi ir aicināti noklikšķināt. Lūdziet viņiem dalīties savos novērojumos par to, kā katra no šīm saitēm atspoguļo iespējamos apdraudējumus un kā viņiem jāizlemj par to, kad mijiedarbotos saturu un kad ne.

3.nodaļa - Padomi aizsardzībai sociālajos medijos

Mācību aktivitāte 1

Izdaliet katram izglītojamajam vienu vai vairākas kartītes, kurās piedāvāti (izdomāti) sociālo mediju publikāciju ekrānuzņēmumi no dažādām platformām, un aiciniet viņus noteikt, kādu sensitīvu informāciju viņi var iegūt no viena šāda ieraksta un kādus iespējamos draudus tas var radīt.

KAS IR SOCIĀLO MEDIJU DROŠĪBA

Sociālo mediju drošības vadlīnijas ir paredzētas, lai novērstu nesankcionētu piekļuvi Jūsu sociālo mediju kontiem, aizsargātu Jūsu tiešsaistes identitāti pret viltus uzdošanos vai datu zādzībām, kā arī aizsargātu Jūsu tīklu no ļaunprātīgām identitātēm vai sociālo mediju satura. Tā kā ONS apdraudējumu modelis un mērķi bieži ir atkarīgi no platformas veida, attiecīgi jāņem vērā arī daži specifiski draudu novēršanas paņēmieni.

VISPĀRĒJĀ PRAKSE

Izmantojiet spēcīgu paroli: lai nodrošinātu kontu drošību, lietotājiem jāizvēlas spēcīga parole. Tām nevajadzētu būt pārāk īsam, jo īsās paroles var viegli uzminēt. Tām ir jābūt pietiekami garam, un tajā ir jābūt burtciparu vērtībām ar dažām speciālajām rakstzīmēm. Lietotājiem nevajadzētu izmantot to pašu paroli, ko viņi lieto citiem kontiem – ja uzbrucējs kaut kādā veidā uzzina šo paroli, viņš var apdraudēt pārējos šī lietotāja kontus.

Ierobežojiet lokācijas kopīgošanu: mūsdienās atrašanās vietas kopīgošana ir kļuvusi par trendu. Daudzās sociālo tīklu vietnēs ir ieviesta arī ģeogrāfiskās atzīmes funkcija, kas automātiski atzīmē lietotāja ģeogrāfisko atrašanās vietu, kad lietotājs augšupielādē jebkādu multimediju elementu sociālajos medijos. Lietotājam to ir jāpārslēdz uz manuālo režīmu, lai atrašanas vieta netiek atzīmēta automātiski. Lietotājiem ir ļoti rūpīgi jāveic multimediju satura augšupielādi, jo tas var saturēt sensitīvos metadatus, un ir ieteicams visās mobilajās ierīcēs un kontos pārslēgt ģeogrāfiskās atzīmes manuālajā režīmā.

Esiet izvēlīgs attiecībā uz draudzības uzaicinājumiem: tika novērots, ka daudzi lietotāji apstiprina draudzības uzaicinājumu, neanalizējot visu pieprasītāja profilu. Cilvēki parasti apstiprina uzaicinājumus, pamatojoties uz informāciju par kopīgajiem draugiem. Ja pieprasītājam ir daži kopīgi draugi, viņš/viņa tiek apstiprināta. Dažreiz uzbrucēji apzināti padara savu profilu pievilcīgu vai viņi var personificēt kontu. Tātad, ja persona, kas sūta draudzības uzaicinājumu, nav zināma, šo pieprasījumu labāk ignorēt. Tas varētu būt viltots konts, kas mēģina nozagt sensitīvu informāciju.

Domājiet par to, kādu saturu kopīgojiet: lietotājiem jābūt uzmanīgiem attiecībā uz saviem ierakstiem, jo dažreiz tie var atklāt personisku un cita veida informāciju. Daudzas organizācijas ievēro stingrus noteikumus informācijas un multimediju satura kopīgošanai. Ir diezgan daudz gadījumu, kad cilvēki tiek atlaisti no darba dēļ nelikumīgas informācijas kopīgošanas.

No šādas situācijas var izvairīties, ja darbinieki ir labi informēti par savas organizācijas protokoliem attiecībā uz attēliem, video un ziņojumiem, ko viņi publicē internetā. Nelikumīga informācijas apmaiņa var kaitēt organizācijas reputācijai tirgū, kā arī tās datiem un intelektuālajam īpašumam.

Esiet piesardzīgi attiecībā uz trešo pušu vietnēm un lietotnēm: nelikumīgi lietotāji var piekļūt kādas personas kontam un iegūt sensitīvu informāciju, kopīgojot ļaunprātīgu saiti. Mūsdienās saīsinātie URL kļūst ļoti populāri dažādās sociālo mediju platformās. Šie saīsinātie URL var būt aizsegti ar ļaunprātīgu kodu vai skriptu. Šie skripti mēģina apkopot lietotāja personisko un konfidenciālo informāciju, kas var pārkāpt šī lietotāja privātumu. Turklāt hakeri var izmantot ievainojamības priekšrocības trešās puses lietotnē, kas ir integrēta daudzos populāros sociālajos tīklos. Šādas trešās puses lietotnes piemērs ir spēles, kuras var spēlēt tiešsaistes sociālajos tīklos un kuras pieprasa lietotāja publisko informāciju, lai izmantotu viņu pakalpojumus. Šī savākta informācija var būt nodrošināta nepiederošām personām vai trešo pušu iejaukšanās darbībām. Lai izvairītos no šī riska, lietotājiem jābūt uzmanīgiem, instalējot savā profilā trešās puses lietotnes.

Instalējiet interneta drošības programmatūru: dažus draudus, kuru modelis ir zināms, var viegli noteikt ar pretvīrusu palīdzību. Pateicoties pretvīrusu programmatūrai, zināmā mērā var atklāt tādus draudus kā kiberuzmākšanās un kibermobings

MULTIMEDIJU SATURA KOPLIETOŠANAS VIETŅU LIETOŠANAS PRAKSE

- Nevajadzētu publicēt sensitīvu informāciju savos fotoattēlos un to parakstos. Pārāk daudz privātas informācijas atklāšana profilā var būt bīstama.
- Izvairieties no pašreizējo atrašanās vietu kopīgošanas sociālajos medijos. Ģeogrāfiskās atzīmēšanas funkciju, ko nodrošina dažādas multimediju platformas, ir jāizslēdz manuāli.
- Ja lietotne netiek ilgstoši izmantota, labāk ir deaktivizēt piekļuvi tai. Ir tik daudz trešo pušu lietotņu, kas izmanto sociālo mediju kontus, lai ielogotos. Drošības un privātuma apsvērumu dēļ piekļuve ir jāatļauj tikai uzticamām lietotnēm.
- Uzstādiet divpakāpju autentifikāciju visiem saviem sociālo mediju kontiem, kur vien iespējams. Tas nodrošina kontam papildu drošības līmeni. Ja ļaundaris uzzina lietotāja paroli, viņam joprojām būs nepieciešams otrs faktors, lai autentificētos. Otrais faktors sastāv no unikāla, laika ziņā ierobežota koda, ko lietotāji saņem īsziņas veidā savā mobilajā tālrunī.

DISKUSIJU FORUMU LIETOŠANAS PRAKSE

- Jāpievērš uzmanība uz dažādu avotu sniegtajām saitēm, pirms uz tām klikšķināt. Iespējams, tā ir kāda aizdomīga vietne, kas mēģina iegūt lietotāja piekļuves datus.
- Lietotājiem vienmēr vajadzētu pievērst uzmanību vietņu URL adresēm. Kaitīgas vietnes var izskatīties praktiski neatšķiramās no īstām, tomēr URL vietrādī var būt nelielas neatbilstības, piem., atšķirības pareizrakstībā (piem., "0" burta "o" vietā, kas nav pamanāms, ja lasa ātri) vai alternatīvais domēns.
- Esiet piesardzīgi attiecībā uz informāciju, kurā klientam tiek prasīts rīkoties nekavējoties, tiek piedāvāts kaut kas, kas izklausās nereāls vai tiek pieprasīta personiska informācija.

SOCIĀLO TĪKLU PLATFORMU LIETOŠANAS PRAKSE

- Lietotājiem vajadzētu uzzināt par dažādu sociālo mediju platformu privātuma un drošības iestatījumiem un tos izmantot. Katra platforma nodrošina iestatījumus, konfigurācijas un konfidencialitātes sadaļas, lai ierobežotu to, kurš un kādas grupas var redzēt dažādus lietotāja profila aspektus. Nevajadzētu paļauties tikai uz tiem konfidencialitātes iestatījumiem, ko platforma piedāvā pēc noklusējuma.
- Jo sīkāku informāciju lietotājs sniedz, jo vieglāk uzbrucējam ir izmantot šo informāciju, lai nozagtu identitāti vai veiktu citus kibernoziegumus. Tādējādi informācijas kopīgošanu būtu jāierobežo.
- Pirms draudzības uzaicinājuma apstiprināšanas ir pilnībā jāpārbauda pieprasītāja profils. Var izveidot dažādas grupas, lai koplietotu dažāda veida informāciju, piemēram, dažādas grupas kolēģiem un ģimenei.

PROFESIONĀLO TĪKLU LIETOŠANAS PRAKSE

- Profesionālos tīklus galvenokārt izmanto, lai veidotu kontaktus un palielinātu savu redzamību potenciālajiem personāla atlases uzņēmumiem. Lai nodrošinātu drošu profesionālo tīklu lietošanu, pirms jaunas personas pievienošanas savam kontaktu sarakstam ir jāpārbauda citu lietotāju sniegtā informācija. Parasti ļaundaris nesniedz daudz informācijas par savu karjeru.
- Lietotājs var pārbaudīt, vai profilā nav kādu pareizrakstības vai gramatikas kļūdu, jo, ja persona piesakās darbam, informācijai jābūt ļoti labi uzrakstītai, bez acīmredzamajām kļūdām. Profilam jāietver kvalitatīvu informāciju par šo personu.
- Ja lietotājs vēlas justies drošs profesionālajā tīklā, atbilstības pārbaude personas karjerā var būt laba prakse. Profils, kas pastāvīgi mainās īsā laika posmā, ir iebrucēja visbiežāk izmantotā daļa. Brīdī, kad krāpniekam ir jāvēršas pret viena vai otra veida organizāciju, viņš vienkārši pievieno jaunu pozīciju (amatu), kas varētu būt piemērota viņa mērķiem.

▪ Tāpat ir jāpārbauda profilā sniegto informāciju. Ja persona apgalvo, ka strādā pie noteikta darba devēja, lietotājs var pārbaudīt uzņēmuma direktoriju (kontaktinformāciju) vai arī nekautrēties un pārbaudīt informāciju uzņēmuma cilvēkresursu nodaļā.

Mācību aktivitāte 2

Lūdziet paskaidrot dalībniekus, kam, viņuprāt, ir piekļuve jaunākajiem ierakstiem, ko viņi ir publicējuši savos iecienītākajos OSN. Visbeidzot, palīdziet pārbaudīt viņu privātuma iestatījumus un analizējiet kopā cik daudz no viņu teiktā atbilst patiesībai. Rosiniet grupas diskusiju par viņu novērojumiem un secinājumiem.

Mācību aktivitāte 3

Aiciniet dalībniekus vēlreiz apskatīt kartiņas (kas tika izmantoti **šīs nodaļas 1. mācību aktivitātē**) un pajautājiet, vai viņi var noteikt papildu riskus attēlotajos sociālo mediju ierakstos. Diskutējiet, ko viņi darītu, lai novērstu šos riskus.

2. Moduļa mācību rezultāti

Zināšanas

- Kiberriski un apdraudējumi, kas saistīti ar sociālo mediju un tīklu izmantošanu
- Platformu drošība ar lietotāju veidoto saturu (UGC)

Prasmes

- Dažādu kiberdrošības apdraudējumu veidu identificēšana

Kompetences

- Novēršana un reaģēšana uz kiberdraudiem sociālajos medijos
- Sarežģīto paroļu pārvaldīšana

3. Bibliogrāfija

https://www.proofpoint.com/us/threat-reference/social-media-threats
https://www.digitalshadows.com/blog-and-research/how-cybercriminals-weaponize-social-media/
https://www.researchgate.net/publication/221663523_Cyber_Threats_In_Social_Networking_Websites
https://www.researchgate.net/publication/324860729_Social_Media_Security_Risks_Cyber_Threats_And_Risks_Prevention_And_Mitigation_Techniques

Co-funded by the
Erasmus+ Programme
of the European Union

EIROPAS PROFESIONĀLĀS IZGLĪTĪBAS UN APMĀCĪBAS NOZARES KIBERDROŠĪBAS GATAVĪBAS UZLABOŠANA

CYBER.EU.VET

IO2 KIBERDROŠĪBAS IZPRATNES VEICINĀŠANAS APMĀCĪBU MATERIĀLS VET SEKTORĀ

NGO NEST Berlin
AEII
tandemplus
Latvian European Community Studies Association
COFAC
EOS
inerciadigital
meath partnership

INTRO

No 2021. gada rudens, atzīmējot Eiropas kiberdrošības mēnesi, līdz 2022. gada pavasarim projekta CYBER.VET.EU partneri savās valstīs organizēja spēļu izstrādes pasākumus (Game Jam). Tajā tika iesaistīti jaunieši, sniedzot viņiem iespēju mijiedarboties ar kiberdrošības tēmām un nodrošinot jaunus rīkus.

Šīs intelektuālā nodevuma galvenais mērķis bija vajadzība palielināt izpratni par kiberdrošību. Mēs pievērsāmies spēļošanas ("gamification") procesam, lai iegūtu risinājumu, kas ir viegli pārņemams, ātri ieviešams, mērogojams ar laiku un iekļaujošs. Spēļošanas process, kas definēts kā "spēļu mehānikas pielietošana kontekstos, kas nav saistīti ar spēlēm, lai veicinātu iesaistīšanos un paaugstinātu motivācijas līmeni", ir veids, kā noturēt lietotājus iesaistītus mācību aktivitātēs, sasniedzot lieliskus rezultātus pat īsā laika periodā, pateicoties izklaides elementu izmantošanai, kas motivē dalībniekus vairāk pievērsties vielai un praktizēt to. Tādējādi šīs nodevums kalpos kā vadlīniju, apmācības un praktiskās nodarbības kombinācija. Un tas ir viegli uzlabojams, kad ir nepieciešams pievienot jaunus materiālus.

SPĒĻU IZSTRĀDES PASĀKUMU/AKTIVITĀŠU SASNIEGTIE REZULTĀTI

- Stiprināta izpratne par digitālo drošību
- Stiprināta izpratne par digitālo drošību starp kopienas dalībniekiem (ģimenē, draugiem, kolēģiem)
- Ļaunprogrammatūras “sekmīgo” apdraudējumu līmeņa samazināšana iestādēs
- Datu noplūdes gadījumu skaita samazināšana
- Palielināta interese par kiberdrošības nozari kā nodarbinātības iespēju.

AEII / INERCIA DIGITAL [ES]

AKTIVITĀTES

Svarīgākās aktivitātes, ko īstenoja Spānijas partneri AEII un Inercia Digital:

- Hakatons
- Spēļu izstrādes pasākums (Game Jam)
- Info dienas
- Starptautiskā konference
- Informatīvais pasākums

REZULTĀTI

Spēļu izstrādes pasākums Spānijā nodrošināja vairākus noderīgus rezultātus (skat.zemāk):

https://scratch.mit.edu/projects/611211889/

https://scratch.mit.edu/projects/611201682/

https://www.youtube.com/watch?v=3QFI9iB0iJU&t=124s

AEII / INERCIA DIGITAL [ES]

GAME JAM

Gamejam in Cyber.EU.VET

20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

0 No me gusta Compartir Descargar Guardar ...

Gamejam in Cyber.EU.VET

20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

0 No me gusta Compartir Descargar Guardar ...

AEII / INERCIA DIGITAL [ES]

Hakatons

"Kiberdrošība izglītībā"

2021. g. 20.-22. oktobrī, Spānijas partneri AEII un Inercia Digital piedalījās tiešsaistes hakatonā ar citiem 47 dalībniekiem, no kuriem daudzi bija IT eksperti. https://www.comprometidosporelfuturo.com/proyectos#, atbalsta Boehringer Ingelheim Spānijā.

RISINĀMĀ PROBLĒMA

Kibermobings (jeb emocionālā pazemošana) ir viens no galvenajiem jauniešu interneta riskiem. Bieži vien var atrastas interneta ierakstus ar aizskarošu saturu par kādiem cilvēkiem un tie tiek izmantoti, lai uzmāktos un ņirgātos par upuriem.

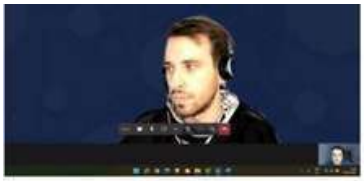
Kibermobings bieži izraisa nopietnus traucējumus upuriem, piemēram, pēctraumatiskā stresa sindromu, depresiju, pašnāvnieciskas domas un uzvedību vai arī trauksmi.

Šīs izaicinājums nozīmē – izpētīt un analizēt, ko jaunieši zina par drošību, kā arī likt viņiem apzināties riskus, ar kuriem viņi saskaras savos izglītības centros un ikdienas dzīvē. Šis izaicinājums, izmantojot spēļošanu, cenšas palielināt studentu un pedagogu izpratni ikdienas dzīvē par jautājumiem, kas saistīti ar drošību jauno tehnoloģiju izmantošanā.

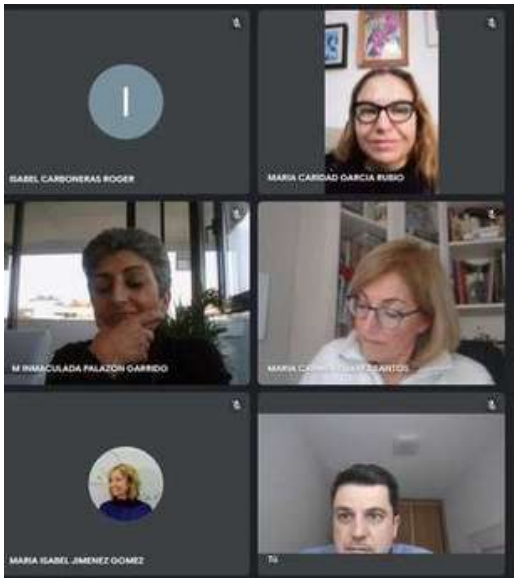
REZULTĀTI

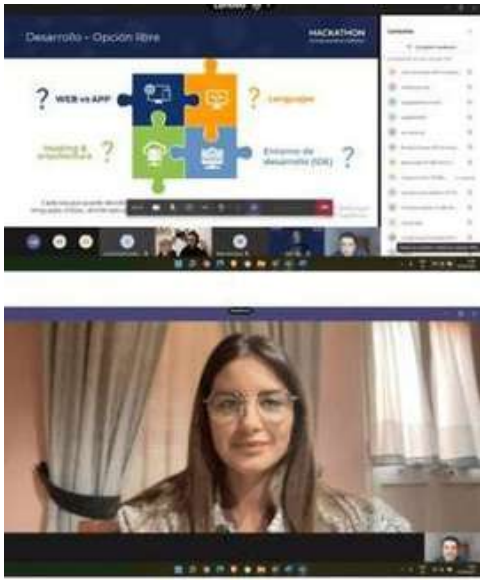
Spēle un animācija saistīta ar kiberdrošību izglītībā

- Valsts pārvaldes, profesionālās izglītības skolu, IT ekspertu, skolotāju, studentu un projekta partnera iesaiste
- Īsu interaktīvu video veidošana



AEII / INERCIA DIGITAL [ES]





Kopumā pēc daudzu aptauju īstenošanas var secināt, ka profesionālās izglītības iestāžu pedagogu un studentu zināšanas par kiberdrošību Spānijā joprojām ir zemas. Līdz ar to šis un citi līdzīgi projekti Spānijā ir ļoti aktuāli.

NVO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

GAME JAM

Partneri – NVO Nest Berlin (Vācija), Extrafondente Open Source - EOS (Itālijā) un IASIS (Grieķija) – 2022. gada februārī organizēja kopīgu spēļu izstrādes sesiju. "Game Jam" sākās sestdien, 12.02., un kopumā ilga 6 dienas. Pasākuma laikā nacionālās komandas izstrādāja un strādāja kopā pie spēles prototipa (tiešsaistes vai galda spēles).

Tika sapulcēta neatkarīga žūrija un tai tika lūgts novērtēt spēles projektu, ievērojot kopējās vadlīnijas un vērtēšanas veidni.

Uzvarētāju komandai tika piešķirts 6 mēnešu mentorings, kā arī tehniskie resursi spēles idejas tālākai attīstībai.

PAR SPĒLI

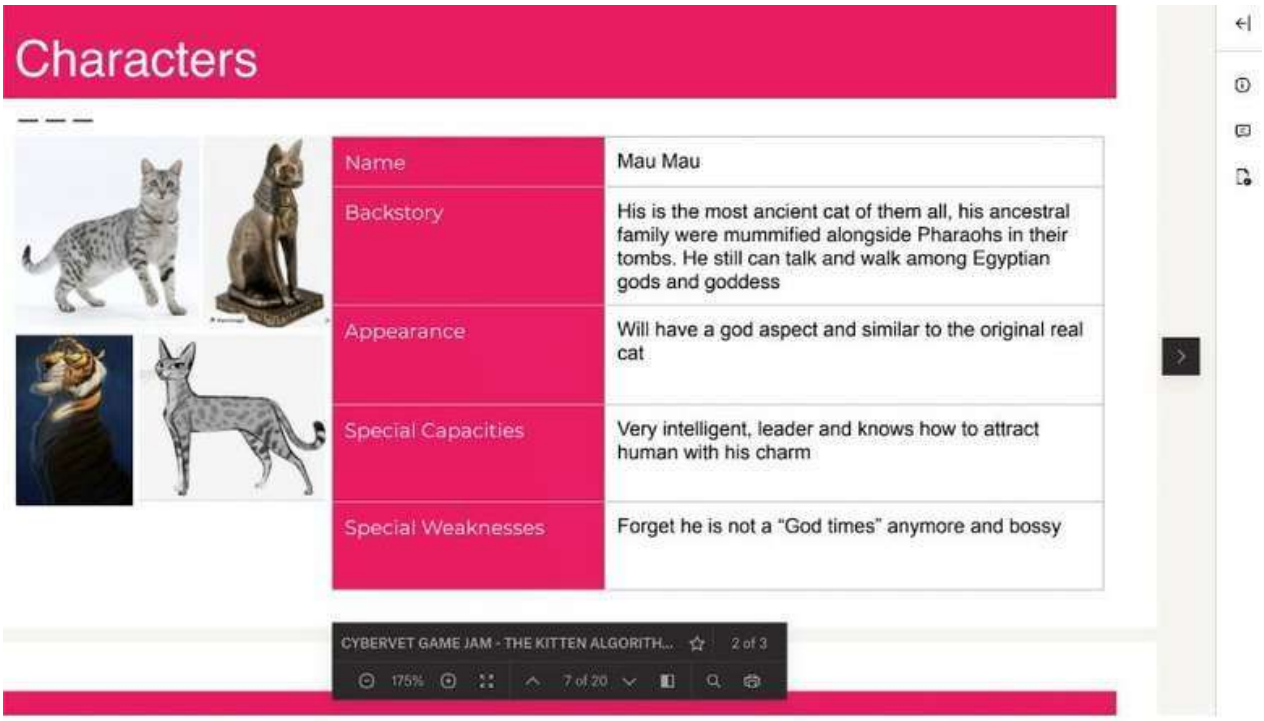
Tā ir stratēģiskā galda spēle, paredzēta 2 līdz 6 spēlētājiem, un tās spēlēšana aizņem ~ 30-60 minūtes. Šajā spēlē jācenšas apmānīt cilvēkus, lai pārliecinātu viņus, ka esi labākais kaķis, un iegūt lielāku prestižu, iegūstot pēc iespējas vairāk cilvēku kaķa kalpu. Esat modri – citi kaķi-priekšnieki aktīvi mēģinās sabotēt Tavu ceļu, lai nokļūtu pie cilvēkiem un iegūtu slavu sev. Neuzticies viņu jaukajām sejām!

Spēle tiek zaudēta, ja Tev nav pietiekami daudz cilvēku, Tavu kalpu, vai arī ir beidzies 10. raunds un nevienam spēlētājam komandā nav vismaz 4 cilvēku.

Grūtības ir tādas, ka ir 6 priekšnieki, kas mēģina apmānīt cilvēkus un kļūt par viņu kalpiem, lai priekšnieki varētu viņus kontrolēt, taču visiem ir viens un tas pats mērķis, un daži var pat palīdzēt cilvēkiem atbrīvoties no kaķa kontroles.

NVO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

Mau Mau



LECSA (LV)

GAME JAM

LECSA, partneris no Latvijas, spēļu izstrādes pasākumu organizēja no 2021. g. 27. septembra līdz 1. oktobrim. Ņemot vērā epidemioloģiskos ierobežojumus un atšķirīgo dalībnieku atrašanās vietu, pasākums tas tika organizēts hibrīda veidā (uz vietas Saldus tehnikumā un Zoom platformā). Pasākuma laikā tika izveidotas 6 komandas (4-5 cilvēki komandā), kas strādāja pie spēles prototipa izveides. Lai sasniegtu taustāmus rezultātus, "Game Jam" koncepcija paredzēja divu veidu spēļu izstrādi – datorspēles un galda spēles.

AKTIVITĀTES

- 2021.g. augusts - septembris tika veltīts pasākuma plānošanai un organizēšanai (kiberdrošības un spēļu izstrādes ekspertu uzrunāšana, informācijas izplatīšana potenciālajiem dalībniekiem, kritēriju definēšana spēļu izstrādei u.c.)
- Info pasākums (Multiplier Event): Aktualitātes kiberuzbrukumos (27.09.2021.) – CYBER.EU.VET projekts un lekcija par kiberuzbrukumu tendencēm ar **CERT.LV kiberdrošības ekspertu Armīnu Palmu**.

Dalībnieku skaits: 26 personas

Vieta: Saldus Tehnikums (Saldus) un ZOOM platforma

- Spēļu izstrādes pasākuma paziņojums (27.09.2021.): kiberdrošības aktuālo izaicinājumu definēšana un apspriešana (vajadzību novērtējums); komandu veidošana, tikšanās ar mentoriem un diskusija par turpmāko darbu (darbnīca par spēles dzinēju Unity), ideju ģenerēšanas sesija par spēles ideju un koncepciju.
- Spēļu izstrādes pasākuma norise (28.09-30.09.2021.): komandu darbs pie spēļu prototipiem, nepieciešamības gadījumā tika nodrošinātas konsultācijas ar mentoriem.
- Pičošana par progresu (30.09.2021.): prezentācijas par spēļu koncepcijām un darba gaitu, lai saņemtu mentoru ieteikumus.
- Lielais fināls (01.10.2021.): četras komandas prezentēja savus rezultātus un mentori sniedza vērtējumu. Viena komanda, strādājot pie datorspēles, ir izstājusies. Pasākuma noslēgums un neformāla diskusija.

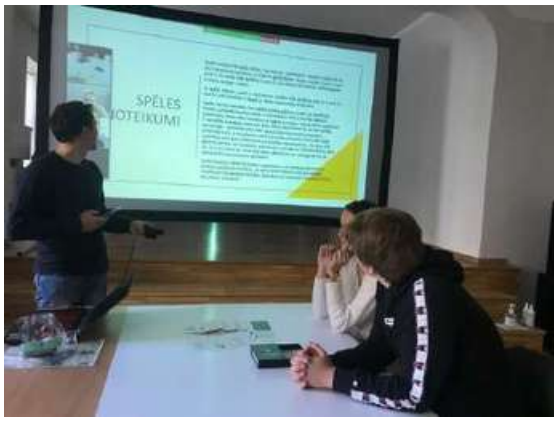
Dalībnieku skaits: 30 personas

Vieta: Saldus Tehnikums (Saldus) un ZOOM platforma

LECSA (LV)

REZULTĀTI

1. Datorspēles prototips – The Virus
2. Galda spēle – Cards about Security
3. Galda spēle – Kiberkarš
4. Konkurētspējīga kāršu spēle – Cyber Mind



PIEMĒRS Cyber Mind - karšu spēle

Šī ir izglītojoša kāršu spēle ar viktorīnas elementiem. Spēles galvenais uzdevums ir iemācīt ikdienas drošības pamatus internetā un to, kam cilvēki sevi pakļauj, tajā darot muļķīgas lietas. Tajā aplūkotas tādas tēmas kā interneta drošība un datu aizsardzība sociālo tīklu lietošanas kontekstā. Spēles rezultātā cilvēkiem (spēlētājiem) jāspēj atpazīt krāpšanas mēģinājumus reālajā dzīvē.

Izstrādāja komanda "Veiksminieki" – Renārs Rikards Hartmanis, Estere Ozoliņa, Sindija Diāna Valtere u.c. (Saldus tehnikuma audzēkņi).

Līmenis: pamata (iesācējiem). Mērķa grupa – skolēni, studenti, skolotāji un vecāki

Spēle satur: 50 kārtis, 2 dzīvību paliktņi (spēlētāju dzīvības skaitīšanai), 2 kauliņi un noteikumu kārts.

PAR SPĒLI

Kiberuzbrukumu mēģinājumu skaits pasaulē pieaug katru dienu, tāpēc tās valdība nāca klajā ar ideju organizēt turnīru, lai identificētu apkārtējos cilvēkus, kas rada kiberriskus, un veikt pretuzbrukumus pret tiem.
Izglītojoša spēle, kas palīdz uzzināt par galvenajiem kiberuzbrukumu veidiem, to novēršanas un likvidēšanas metodēm, aizsargājot sevi vai savu komandu un sniedzot pretuzbrukumu pretiniekam. Spēles mērķis ir atņemt visas pretinieka/-u dzīvības.

KĀ SPĒLĒT SPĒLI/ NOTEIKUMI

Spēlētāju skaits: 2 vai 4 personas (1 pret 1 vai 2 pret 2).
Katram spēlētājam vai komandai (ja 2 vs 2) spēles sākumā ir "100 dzīvības" (veselība = HP). Veselības skaitīšana tiek veikta, izmantojot melnas piezīmju lapiņas vai citas pieejamās piezīmju lapas.
Ja iespējams, nozīmējiet atsevišķu personu, kas sekotu līdzi un rēķinātu spēlētāju enerģijas un veselības patēriņu. Vai arī spēlētāji to dara paši.
Katram spēlētājam tiek izdalītas 5 kārtis. Ja spēle tiek spēlēta 2 pret 2, tad abiem spēlētājiem ir "viena kopīga roka" komandā, t.i. komandai ir 10 kārtis kopā.

Ir trīs veidu kārtis: uzbrukuma kārtis (sarkanas), aizsardzības kārtis (dzeltenas) un dzīvības vai dziedināšanas kārtis (zaļas).

Spēle notiek raundos. Spēlētājs/komanda, kura izmet lielāko skaitli, uzsāk spēli.

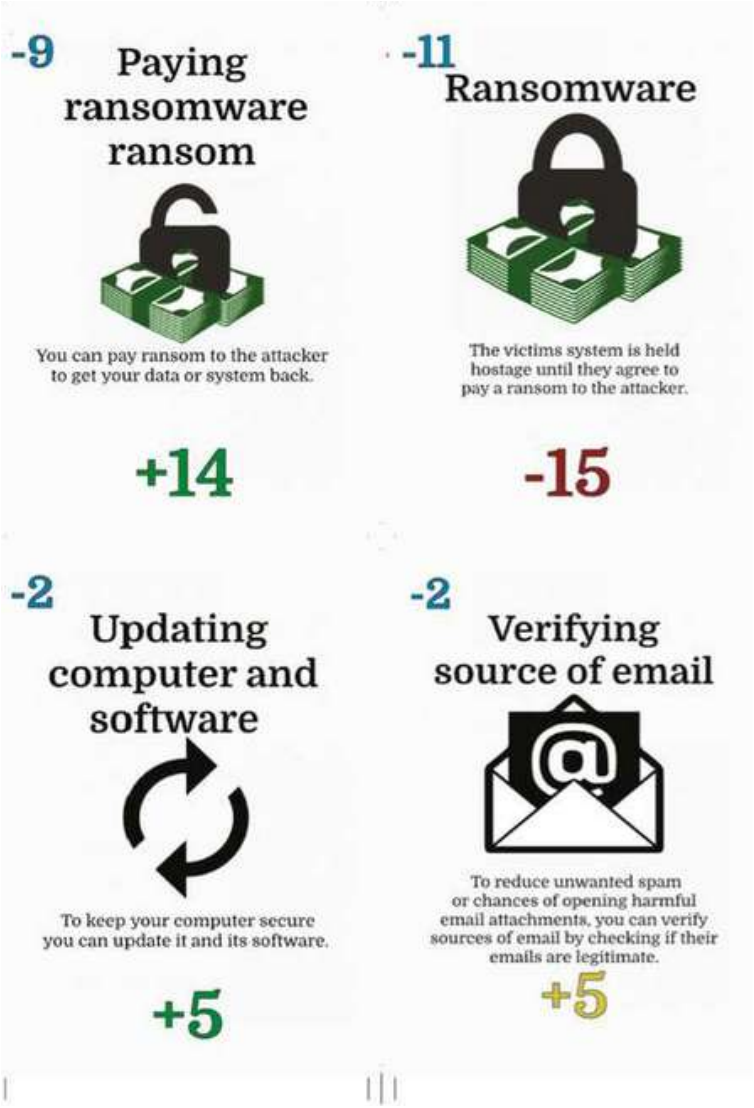
Katra kārts maksā enerģiju. Katra raunda sākumā spēlētājs met 2 kauliņus, lai noteiktu Enerģijas lielumu, kas ir norādīta kārts augšpusē (zilā krāsā). Kārtis ir jāizspēlē tā, lai netiktu pārsniegts uzmestas enerģijas cipars.
Spēlētājs/komanda, kura uzsāk raundu, var uzbrukt (ar uzbrukuma kārtīm), aizsargāties (aizsargkārtis) vai pievienot dzīvību (ārstējošās kārtis), savukārt otrie spēlētāji var

izmantot
tikai uzbrukuma un aizsardzības kārtis, lai samazinātu savas dzīvības ievainojamību.
Ņemiet vērā - max dzīvību skaits vienam spēlētājam/komandai spēles laikā nevar pārsniegt 100 HP (piem., ja dzīvības un enerģijas summa pēc izspēlētā raunda veido 110 HP, jūsu dzīvību skaits tik un tā paliek – 100 HP).
Spēle beidzas, tiklīdz spēlētājam/komandai izbeidzas visas dzīvības (0 dzīvības).
Ja spēles laikā beigušās kārtis, tad ir vēlreiz jāsajauc kārtis no izmestas kaudzes.

LECSA (LV)

Kāršu piemēri

Zilais cipars – enerģija
Sarkanās - uzbrukuma kārtis
Dzeltenās - aizsardzības kārtis
Zaļās - dziedināšanas kārtis



Dzīvību uzskaites piemērs

PIEMĒRS Kiberkarš - galda spēle

Izstrādāja komanda "Exodus" (Saldus Tehnikuma studenti), komandas līderis Valdemārs Šperbergs.

2-6 spēlētāji < – > Piemērota cilvēkiem no 15 gadu vecuma

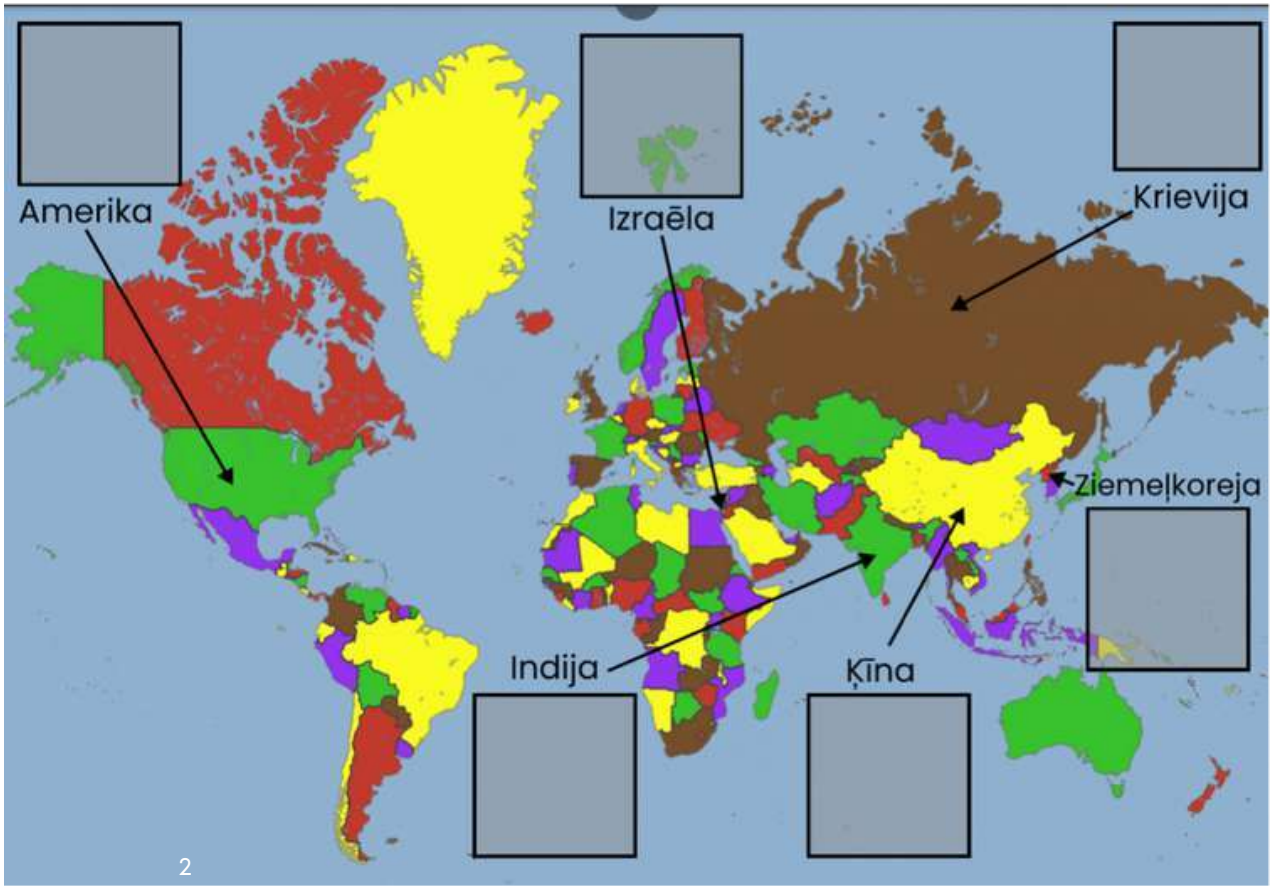
Galda spēle ar lielu uzsvaru uz taktiku un nejaušību.

Līmenis: izglītojoša spēle tiem, kuriem jau ir kāda izpratne par kiberdrošību.

Spēle saturs: pasaules karte, 2 metamie kauliņi, valstu serveri, kārtis ar tādām funkcijām kā “uzbrukums”, “aizsardzība” vai “reakcija”, ievainojumu leģenda, tabula ar iespējamiem gājieniem katram ievainojuma veida.

PAR SPĒLI

Spēles mērķis ir aizsargāt spēlētāja pārstāvēto valsti un uzbrukt citām valstīm, lai uzvarētu kiberkarā. Katram spēlētājam ir jāizvēlas valsts, kuru pārstāvēt. Katram spēlētājam ir viens serveris ar 3 ievainojumiem. Spēlētāja mērķis ir uzlauzt citu valstu serverus, ekspluatējot divus no trim ievainojumiem, vai izlabot divus no trim ievainojumiem savā serverī.



LECSA (LV)

KĀ SPĒLĒT

Spēlētāji izvēlas valsti, ko pārstāvēt, un izvieto serveri norādītajā laukā uz kartes. Katrai valstij ir savi bonusi.

Katrs spēlētājs, neskatoties, izvelk 3 ievainojamības — vienu no katra grūtības līmeņa — un novieto tās ar seju uz leju attiecīgajās vietās (servera laukos). Spēlētājiem ievainojamības nav zināmas.

Ievainojamībām ir 3 grūtības līmeņi. Grūtības līmenis nosaka, cik liels skaitlis ir nepieciešams, lai ekspluatētu ievainojamību (skat. "Uzbrukumi"), kā arī nosaka, cik gājienus būs jāveic, lai salabotu ievainojamību (skat. "Aizsardzība").

Spēle notiek raundos un var veikt šādas darbības – **Skenēšana**, **Uzbrukums** un **Aizsardzība**. Spēlētāji nosaka spēlētāju secību, metot divus kauliņus.

SPĒLES SĀKUMS

- Katra raunda sākumā katrs spēlētājs saņem 4 kārtis. Raunda beigās iespējams – paturēt 2 kārtis vai apmainīt pret esošajām.
- 1. raunds ir skenēšana, kurā nav atļautas Attack vai Défense kartes. Nākamajās kārtās spēlētāji var izvēlēties skenēt vai uzbrukt, vai mēģināt labot savas ievainojamības (skat. Aizsardzība). Spēle turpinās raunds pēc raunda, līdz tiek sasniegt uzvaras nosacījums.

Skenēšana

- Uzbrucējs izvēlas valsti, kurā skenēt (meklēt) ievainojamību (piem., “Es pārbaudu Krievijas 2. līmeņa ievainojamību”).
- Spēlētājs veic skenēšanu – met 2 kauliņus, pieliekot savas valsts bonusu un salīdzina ar ievainojamības grūtību + valsts bonusi.
- Ja uzbrucējs ir uzmetis vienādu vai lielāku skaitli par upura ievainojuma grūtības līmeni, uzbrucējs drīkst paskatīties skenēto ievainojumu.
- Valsts bonusi netiek pieskaitīti skenējot sevi.

Grūtības līmeņi

1.grūtības līmenis - jāuzmet vismaz 4 (neieskaitot valsts bonusus)

2.grūtības līmenis - jāuzmet vismaz 8 (neieskaitot valsts bonusus)

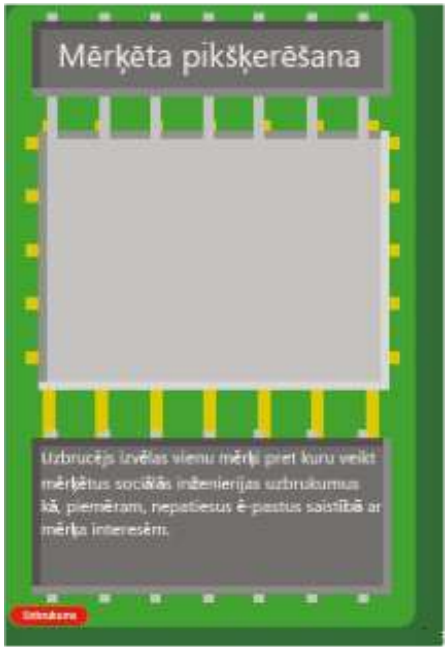
3.grūtības līmenis - jāuzmet vismaz 11 (neieskaitot valsts bonusus).

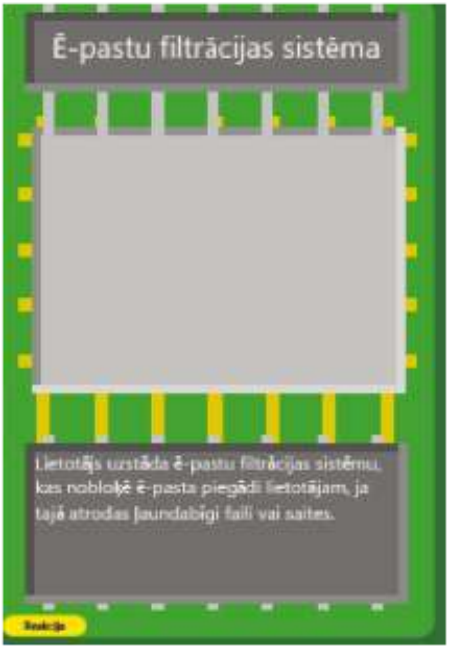
UZBRUKUMS

- Spēlētājam jānosauc uzbrukuma mērķi (piem., "Es uzbrūku Krievijas 2. līmeņa ievainojumam") un tad jāatklāj Uzbrukuma kārti visiem spēlētājiem, novietojot to blakus ievainojumam.
- Spēlētājs met kauliņus, lai redzētu vai uzbrukums strādā, salīdzinot uzmesto ar ievainojuma grūtību + bonusi (ja uzmestā summa + bonusi sakrīt vai pārsniedz grūtības pakāpi, uzbrukums ir veiksmīgs).
- Uzbrukumus var atvairīt, izmantojot Reakcijas kārti, kas paredzēta tam uzbrukumam.
- Katram uzbrukumam ir sava tipa reakcijas, kuras var izspēlēt un arī sava tipa ievainojums, kam tas strādā.
- Ja uzbrukums nav izdevies vai tiek nobloķēts ar Reakcijas kārti, tad abas kārtis paliek uz galda līdz nākošā raunda beigām un liedz citiem spēlētājiem uzbrukt ar tādu pašu uzbrukumu tam pašam ievainojumam. Pēc gājiena abas kārtis atgriežas kaudzē.

Grūtības līmeņi

1.grūtības līmenis - jāuzmet vismaz 4 (neieskaitot valsts bonusus)
2.grūtības līmenis - jāuzmet vismaz 8 (neieskaitot valsts bonusus)
3.grūtības līmenis - jāuzmet vismaz 11 (neieskaitot valsts bonusus).





Aizsardzība

- Tajā tiek izvēlēta pareizā aizsardzības metode pret noteiktu ievainojumu. Reakcijas kārtis atceļ ienākošo uzbrukumu (un pārējos uzbrukumus, kas mērķēti uz šo pašu ievainojumu) uz 1 gājienu.
- Lai atceltu ienākošo uzbrukumu, uz Uzbrukuma kārts jānovieto Reakcijas kārti, kas sakrīt ar uzbrukuma tipu (skat. ievainojumu tabulu), tiklīdz uzbrukums tiek izspēlēts.
- Lai sāktu sava ievainojuma labošanu, jānovieto Aizsardzības kārti blakus labojamam ievainojumam.
- Citi spēlētāji var uzbrukt šim ievainojumam, kamēr tas ir aizsardzībā (pirms aizsardzības gājieni ir beigušies).
- Kad spēlētājs cenšas salabot ievainojumu savā serverī ar Aizsardzības kārti, viņš nedrīkst uzbrukt, bet var censties novērst uzbrukumus pret sevi ar Reakcijas kārtīm. Lai pilnībā salabotu ievainojamību, ir vajadzīgi |grūtības līmenis + 1| gājieni. Skenēšanas darbības ir atļautas labošanas periodā.
- Ja aizsardzības metode nav pareiza, spēlētājs izlaiž 3 gājienus un šajā periodā nevar izmantot Aizsardzības kārtis (reakcijas un skenēšanas darbības ir atļautas).

Valstu bonusi

- ASV: +2 skenēšanai
- Krievija: +2 uzbrukumiem
- Ķīna: +2 aizsardzībai pret uzbrukumiem
- Ziemeļkoreja: +2 aizsardzībai pret skenēšanu
- Indija: + 1 visos uzbrukumos, - 1 pret uzbrukumiem
- Izraēla: +3 visos uzbrukumos, -3 pret uzbrukumiem

Ievainojumi pēc līmeņa

Ievainojums	Uzbrukums	Aizsardzība	Reakcija
1.ievainojuma līmenis			
SSH serveris ar lietotājvārdu	Paroles minēšana	Publiskās atslēgas lietošana	Bloķēšana perioda iestatījumi
Administrācijas panelis ar lietotājvārdu	Paroles minēšana	Ārējo pieprasījumu bloķēšana	Bloķēšana perioda iestatījumi
Neapmācīts darbinieks	Pikšķerēšanas kampaņa	IT drošības treniņi	Ē-pastu filtrācijas sistēma; Ē-pastu SPAM saraksta ieviešana
Ievainojams SMB protokols	EternalBlue ekspluatācija	CVE-2017-0144 Labojums	n/a
XSS ievainojums	Koda injekcija; Koda injekcija izmantojot polyglot	Ievada sintēze	Simbolu melnā saraksta ieviešana
SQL Injekcija	Koda injekcija; Koda injekcija izmantojot polyglot	Ievada sintēze	Simbolu melnā saraksta ieviešana
Rūtera panelis ar noklusējuma lietotājvārdu un paroli	Noklusējuma datu izmantošana	Pilnīga autentifikācijas datu nomaiņa	Vienas sesijas limits

2.ievainojuma līmenis			
Administrācijas panelis	Lietotājvārda minēšana;	Ārējo pieprasījumu bloķēšana	Bloķēšana perioda iestatījumi
XSS ievainojums ar filtru	Koda injekcija izmantojot polyglot	Ievada sintēze	Simbolu melnā saraksta ieviešana
SQL injekcija ar filtru	Koda injekcija izmantojot polyglot	Ievada sintēze	Simbolu melnā saraksta ieviešana
Nepilnīgi nokonfigurēts ugunsmūris	Pakešu fragmentācija	Konfigurācijas labojums	IDS ieviešana
WiFi tīkls ar WEP drošību	Pakešu okšķerēšana	WPA2 standarta izmantošana	RADIUS ieviešana
Aizņemts priekšnieks	Lielo zivju pikšķerēšana	IT drošības treniņi	Ē-pastu filtrācijas sistēma; Ē-pastu SPAM saraksta ieviešana
Administrācijas panelis	Lietotājvārda minēšana;	Ārējo pieprasījumu bloķēšana	Bloķēšana perioda iestatījumi
3.ievainojuma līmenis			
Pakalpojuma atteices kļūda	DDoS	IP adrešu bloķēšana un slodzes limitēšana	Slodzes balansētāji
Ievainojama OpenSSL programma	Heartbleed ekspluatācija	CVE-2014-0160 Labojums	n/a
Ievainojama Print Spooler programma	PrintNightmare ekspluatācija	CVE-2021-36958 Labojums	n/a
Bufera pārpildes ievainojums	Bufera pārpilde	Bufera limitu ieviešana	Bufera palielināšana
Vājš jaucējvērtības algoritms	Jaucējvērtības atšifrēšana	Jaucējvērtību algoritma uzlabošana	Garas paroles izmantošana
Slinks IT speciālists	Mērķēta pikšķerēšana	IT drošības treniņi	Ē-pastu filtrācijas sistēma; Ē-pastu SPAM saraksta ieviešana

LECSA (LV)

SSH serveris

SSH serveris ar lietotājvārdu

Administrācijas panelis

Administrācijas panelis ar lietotājvārdu

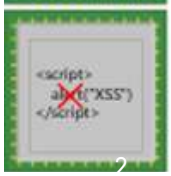
Neapmācīts darbinieks

Ievainojams SMB protokols

XSS ievainojums

SQL injekcija

Rūtera panelis ar noklusējuma lietotājvārdu un paroli



XSS ievainojums ar filtru

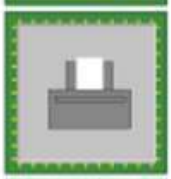
SQL injekcija ar filtru

Nepilnīgi nokonfigurēts ugunsmūris

WiFi tīkls ar WEP drošību

Pakalpojuma atteices kļūda

Ievainojama OpenSSL programma



Ievainojama Print Spooler programma

Bufera pārpildes ievainojums

Vājš jaucējvērtības algoritms

Aizņemts priekšnieks

Slinks IT speciālists

LECSA (LV)

GAME JAM

LECSA (LV)

LATVIJAS SPĒĻU IZSTRĀDES PASĀKUMA PIEREDZE & PRAKTISKIE PADOMI

- 2 dienu pasākuma laikā nav iespējams izveidot datorspēles gala versiju, bet gan pirmo prototipu, pie kā var turpināt strādāt tālāk, pēc pasākuma, atkarībā no dalībnieku motivācijas.
- Balvas vai cita veida ieguvumi var palīdzēt iesaistīt vairāk dalībnieku un nodrošināt labākus (taustāmākus) rezultātus noslēgumā (mūsu gadījumā – pasākuma noslēgumā tika nodrošināta pica un dzērieni, turpmāks mentoru atbalsts, piem., spēļu izvietošanas platforma par brīvu)).
- Spēļu izstrādes un kiberdrošības jautājumu mentoriem ir svarīga loma "Game Jam", konsultējot un palīdzot dalībniekiem.
- Savlaicīga plānošana – šis ir diezgan sarežģīta tipa pasākums un prasa rūpīgu plānošanu.
- Organizatoriem jārēķinās, ka dažas komandas var izstaties no pasākuma (limitēta laika dēļ, lai tiktu pie rezultāta).

FB publikācijas ar pasākuma rezultātiem:
https://www.facebook.com/cybereuvetproject.eu/posts/1381276452112141
https://www.facebook.com/saldustehnikums/posts/1780232175520378

Pasākumu organizēja LECSA sadarbībā ar Latvijas Universitāti | Ekonomikas un kultūras augstskolu | McĀbols | cert.lv | Coldwild Games | Saldus tehnikumu!

MĪTAS PARTNERĪBA (IE)

AKTIVITĀTES

- Vajadzību novērtēšanas informācija – tikšanās ar studentiem (kodēšanas apmācība vietējā Pieaugušo izglītības iestādē)
- 2-dienu spēļu izstrādes pasākums (1.dienā - tiešsaistes informatīvā sesija; 2. diena – veltīta "Game Jam")
- Informatīvais pasākums “Kiberdrošības izpratnes rīts”

APRAKSTS & REZULTĀTI

1) Vajadzību novērtēšanas informācija – tikšanās ar studentiem (kodēšanas apmācība vietējā Pieaugušo izglītības iestādē) Datums: 2021.g. oktobris

APRAKSTS

Lai izplatītu informāciju par projektu un noteiktu "Game Jam" galvenās tēmas, Mītas partnerības (Meath Partnership) komanda organizēja informatīvu sesiju ar vietējās kodēšanas apmācības klases audzēkņiem. Pēc dalīšanās ar informāciju par kiberdrošību un diskusijas par jaunākajiem apdraudējumiem sekoja grupu ideju ģenerēšanas sesija, kurā studenti tika sadalīti divās grupās, lai pārrunātu jautājumus un to rezultātā tika apzinātas interesantākās tēmas turpmākai pētīšanai "Game Jam" laikā. Dalībnieki tika arī sīkāk informēti par "Game Jam" un CYBER.EU.VET projektu.

VAJADZĪBU NOVĒRTĒŠANAS PIEMĒRS


YBER.VET.EU

Co-funded by the Erasmus+ Programme of the European Union

Needs assessment meeting guidelines

1. What do you know about cybersecurity?
2. Why do I need to be worried about it?
3. What are the biggest cybersecurity concerns/threats right now?
4. Do you know how to recognise those threats?
5. What is a cyber attack?
6. Can you give us an example of a cyber attack?
7. Can you give us, at least, 3 possible solutions to it?

MĪTAS PARTNERĪBA (IE)

REZULTĀTI

Šīs aktivitātes rezultātā Mītas partnerības komanda ieguva labāku izpratni par studentu vispārējām zināšanām saistībā ar kiberdrošību un kiberdraudiem, kā arī apkopoja informāciju, kas tālāk tika iekļauta "Game Jam" plānošanas un ieviešanas procesā.

VAJADZĪBU NOVĒRTĒŠANA - STUDENTI DARBĪBĀ

2) 2-dienu spēļu izstrādes pasākums
(1.dienā - tiešsaistes informatīvā sesija; 2. diena – veltīta "Game Jam")

APRAKSTS

1. DIENA tika veltīta dalībnieku uzņemšanai, projekta CYBER.EU.VET prezentācijai un "Game Jam" atklāšanai, kā arī informācijas apmaiņai par 2 tēmām, kas tika identificētas vajadzību novērtējuma tikšanas laikā. Dalībniekiem tika piedāvāta iespēja vai nu strādāt individuāli vai komandā. Tāpat 2.dienā viņam bija iespēja uzdot jautājumus vai saņemt papildu skaidrojumus par procesu, kas saistīts ar spēļu izstrādi.

2. DIENA tika veltīta spēļu izstrādei. Mūsu komandas pārstāvji un IT atbalsta eksperti bija pieejami Zoom platformā, lai atbalstītu dalībniekus visā "Game Jam" laikā, no 9:00 līdz 21:00. Dalībnieki tika aicināti augšupielādēt savas spēles Itchio platformā, izmantojot profilu, kas izveidots šim pasākumam: CYBER.EU.VET : Cybersecurity Game Jam - itch.io

REZULTĀTI

Pēc tam, kad dalībnieki prezentēja savu spēļu projektu, viens dalībnieks nolēma turpināt izstrādi un augšupielādēt spēli tālākai izvērtēšanai. Pārējie dalībnieki nolēma neiesniegt savus projektus, jo tie bija ļoti agrīnā stadijā.

Click or not click

Online interactive cybersecurity game

A short narrative driven game on raising awareness for cyber security threats. The game prompts players to make the right decision and avoid losing your security level.

Link: https://itch.io/jam/cybereuvet-cybersecurity-gamejam

Interaktīvā tiešsaistes kiberdrošības spēle:
https://itch.io/jam/cybereuvet-cybersecurity-gamejam

MĪTAS PARTNERĪBA (IE)

3) Informatīvais pasākums "Kiberdrošības izpratnes rīts"
Datums: 2021.g. novembris

APRAKSTS

Informatīvais pasākums organizēts tiešsaistē Zoom platformā ar mērķi palielināt informētību par projektu un tā aktivitātēm. Informācija par pasākumu tika izplatīta starp visdažādākajām ieinteresētajām personām, kuras interesējas vai ir iesaistītas kiberdrošībā. Pasākums sākās ar prezentāciju un pārskatu par projektu un "Game Jam", kam sekoja prezentācija un diskusija par kiberdrošību un praktiskas informācijas apmaiņa par to, kā palikt drošam tiešsaistē (aktuālie kiberdraudi un iespējamo uzbrukumu novēršana).

REZULTĀTI

Informatīvais pasākums veicināja izpratni par projektu, kā arī nodrošināja iespēju iepazīstināt plašāku auditoriju ar sasniegtajiem rezultātiem kopš projekta sākuma. Šī bija arī lieliska iespēja dalīties ar pasākuma dalībniekiem praktiskajā informācijā un padomos par kiberdrošību.

AKTIVITĀTES

1) 2021. g. okt. – 2022. g. febr.: Kiber un ētiskās uzlaušanas pēc-diploma kurss topošajiem profesionāļiem un skolotājiem tirgū (sadarbībā ar vietējo konsultācijas uzņēmumu Cybersec)
2) 2022. g. janvārī: 2 spēļu izstrādes sesijas profesionālās un apmācību izglītības iestādēs:
Escola de Comércio de Lisboa - https://escolacomerciolisboa.pt
Escola Profissional Almirante Reis - https://www.epar.pt

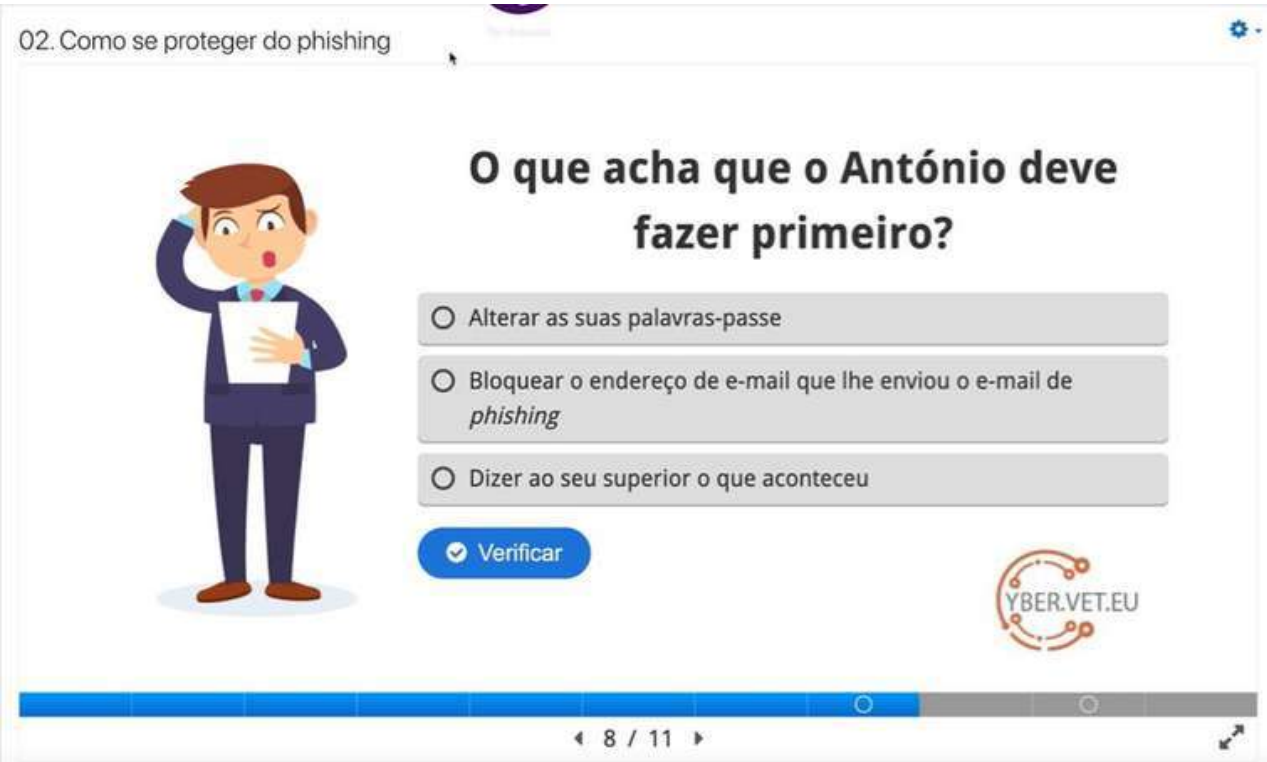
3) 2022. g. martā: kiberapmācības vidusskolēniem Lusofonas Universitātē pasākuma Tecweb ietvaros - https://tecweb.ulusofona.pt

REZULTĀTI

Izplatīšanas (dissemination) apliecinājumu ziņojumā ir iekļauti dažādi testi, kas veikti kalendārā gada laikā (no 2021. g. aprīļa līdz 2022. g. aprīlim). Šajā pārskatā redzami sociālo tīklu publikāciju ekrānšāviņi, dažādu pasākumu plakāti, anketas par kiberdrošības izpratni (pieejams portugāļu valodā https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oeplRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform).

Cyberjam laikā, pamatojoties uz kiberdrošības izpratnes aptaujām, tika izveidots arī mini-lietotājam draudzīgu/interaktīvu spēļu komplekts par vienkāršām situācijām.

COFAC / UDL (PT)



Tāpat partneri organizēja dalībniekiem dažas izpratnes veicināšanas sesijas par izvēlēto tēmu, kā arī rīkoja informatīvo pasākumu, kurā prezentēja visus materiālus un radīto saturu.

Spēļu dizaina rīks (IASIS) - Cyberopolis

Šī ir galda spēle un tā ir paredzēta cilvēkiem, kuri interesējas par kiberdrošību (2-4 spēlētājiem). Spēles galvenie aspekti ir saistīti ar datu konfidencialitāti un datu integritāti... savukārt tēmas, kurām tā pievēršas, ir ļaunprātīga programmatūra, pikšķerēšana, tīmekļa vietņu uzbrukumi, lietojumprogrammu uzbrukumi, surogātpasts, identitātes zādzība, DDoS un pārtvērējuzbrukumi...

Skat. ''Cyberopolis'' attēlu, lai labāk izprastu soļus, kas jāveic spēles laikā un kādi izaicinājumi ir jāatrisina...

Un spēles ekrānšāviņus GameJam sesijas laikā, kur varam redzēt spēles panākumus un dalībnieku lielo interesi.

TANDEM PLUS TĪKLS – PARTNERIS IASIS [GR]

VIDEO - Kibermobinga novēršana

Šis Grieķijas partnera izstrādātais video iepazīstina auditoriju ar dažādiem veidiem, kā novērst un apkarot kibermobingu.

Dizains

NGO Nest Berlin e.V

Berlīne, 2022

Co-funded by the Erasmus+ Programme of the European Union