



Skaitmeninė tapatybė ir saugumas

Atitinkamas pabėgimo kambario scenarijus ir projekto šaltinis	- ER1 Dirbtinio intelekto supratimas - ER11 Išnaudojimas internete ir skaitmeninis saugumas - Savarankiško mokymo darbalapis: Etikos problemos skaitmeniniame versle
Tikslinė grupė ir poreikiai	Amžiaus diapazonas: 15–25 Grupės dydis: 3–6 dalyviai Reikalingos ankstesnės žinios arba patirtis: Pagrindinis kasdienis išmaniųjų telefonų ir socialinių tinklų naudojimas
Trukmė	60–75 minutės
Tikslinės kompetencijos sritys	- Asmens duomenų ir privatumo apsauga - Skaitmeninės tapatybės ir pėdsako supratimas - Etiškas sprendimų priėmimas ir saugus skaitmeninis elgesys
Tikslai	- Nustatykite stiprius ir silpnus slaptažodžių taisykles. - Atpažinkite sukčiavimą ir nesaugų elgesį internete. - Nustatyti skaitmeninio pėdsako reikšmę ir poveikį. - Priimkite etiškus sprendimus realiose skaitmeninėse dilemose. - Taikykite pagrindines privatumo apsaugos strategijas.



Medžiagos ir įranga	• Spausdinti galvosūkių lapai (slaptažodžių logikos tinklėlis, žinučių / įrašų ekrano kopijos, scenarijų kortelės) • Rašikliai ir popierius arba balta lenta užrašams • Laikmatis arba atgalinis laikrodis
Naudingi ištekliai	• Talis - ENISA tapatybės apsaugos ir sukčiavimo atakoms atsparaus daugiafaktorinio autentifikavimo gairės • Europos Komisija - Geresnis internetas vaikams • Nemokamas sukčiavimo simulatoriaus žaidimas - Sukčiauk, jei gali
Aplinkos paruošimas	• Paruoškite 4 iššūkio stotis, pažymėdami jas skaičiais, nurodančiais jų atlikimo tvarką. • Padėkite po vieną dėlionę kiekvienoje stotelėje. • Stalus išdėliokite taip, kad komandos keistųsi tarp stočių.
Žingsnis po žingsnio instrukcijos	1 žingsnis – istorijos pristatymas (5 min.) Dalyviams pranešama, kad jų paskyra socialinės žiniasklaidos programėlėje buvo pažeista, nulaužta ir pakeista. Jie privalo ją apsaugoti ir pašalinti probleminį turinį, kol neatsirado negrįžtamos žalos. 2 veiksmas – 1 stotis: slaptažodžio loginis galvosūkis (15 min.) Dalyviai sprendžia loginę lentelę, kad nustatytų stipriausią slaptažodį, remdamiesi taisyklėmis (ilgis,



	simboliai, unikalumas), ir apsaugo paskyrą, kad galėtų pereiti į kitą etapą. 3 veiksmas – 2 stotis: sukčiavimas apsimitant arba saugus (15 min.) Dalyviai analizuoja žinutes ir įrašus ir nusprendžia, ar jie saugūs, nesaugūs ar susiję su sukčiavimu, kad nustatytų rizikas ir užblokuotų galimas grėsmes prieš tęsdami. 4 veiksmas – 3 stotis: skaitmeninio pėdsako scenarijai (10 min.) Scenarijų kortelėse aprašomi tipiniai veiksmai internete (per didelį dalijimasis informacija, diskusijos, el. laiškų grandinės) ir galimos pasekmės. Dalyviai turi susieti kiekvieną veiksmą su jo ilgalaikiu poveikiu, kad išspręstų kitą galvosūkį. 5 žingsnis – 4 stotelė: Etinės dilemos (10 min.) Dalyviai turi rinktis iš kelių sudėtingų situacijų variantų (dalintis duomenimis, siekiant „padėti“ draugui, pranešti apie kibernetinius patyčias arba jas demaskuoti, skelbti ar cenzūruoti jautrią temą). Kiekvienas pasirinkimas veda prie skirtingų rezultatų, kuriuos žaidėjai turi pagrįsti ir atsakingai spręsti, remdamiesi viskuo, ko išmoko ankstesnėse stotyse. Įrodžius savo supratimą, jie gali prisijungti prie savo sugadintos paskyros ir jaustis saugūs internete.
Aptarimo klausimai	• Koks elgesys internete atrodė „normalus“ ir įprastas, bet iš tikrųjų buvo rizikingas?



	• Kaip maži veiksmai laikui bėgant sukuria skaitmeninį pėdsaką? Ką tai reiškia? • Ar etiniai pasirinkimai visada buvo akivaizdūs? Kodėl taip arba kodėl ne? Kokios būtų jų pasekmės? • Ką pakeistumėte savo internetinio gyvenimo įpročiuose?
Vertinimas ir įvertinimas	• Grupės sprendimų stebėjimas, refleksijos kokybė ir 5-osios stotelės bei aptarimo pagrindimas • Savęs vertinimo kontrolinis sąrašas („Galiu atpažinti sukčiavimą sukčiavimo būdu“, „Žinau, kaip apsaugoti savo duomenis“)
Variacijos ir adaptacija	• Jaunesnės grupės: Mažiau scenarijų, daugiau vaizdinių užuominų, konkrečių ir „juodai baltų“ dilemų • Neuroįvairūs dalyviai: Aiškos piktogramos, sumažintas tekstas, struktūrizuoti pasirinkimai, papildomos užuominos, lankstus laikas • Pažengusiųjų grupės: Daugiau prieštaringų dilemų be tobulo atsakymo skatina diskusijas ir niuansų paiešką
Patarimai	• Venkite moralizuoti; sutelkite dėmesį į pasekmes ir objektyvią riziką, o ne į vertinimą. • Skatinkite diskusiją ir tarpininkavimą, kai dalyviai nesutaria. • Scenarijai turi būti realistiški ir artimi dalyvių kasdieniam skaitmeniniam gyvenimui. • Pabrėžkite, kad saugumas yra bendra atsakomybė.



Nuorodos ir papildoma literatūra

- Europos Sąjungos kibernetinio saugumo agentūra (ENISA). (2023 m.). [*Kibernetinio saugumo pagrindai piliečiams.*](#)
- Europos Komisija. (2025). [*DigComp 3.0: Europos skaitmeninių kompetencijų sistema.*](#)



Bendrai finansuoja
Europos Sąjunga



Finansuojama Europos Sąjungos lėšomis. Tačiau išreiškiamas požiūris ar nuomonė yra tik autoriaus (-ių) ir nebūtinai atspindi Europos Sąjungos ar Europos švietimo ir kultūros vykdomosios įstaigos (EACEA) požiūrį ar nuomonę. Nei Europos Sąjunga, nei EACEA negali būti laikoma už juos atsakinga.

Projekto kodas: 2023-2-LT02-KA220-YOU-000183156