

Metodinė rekomendacija mokytojui – Skaitmeninis pėdsakas ir privatumas internete

Pamokos tema: Skaitmeninis pėdsakas – aktyvus ir pasyvus

Trukmė: 45 min.

Tikslinė grupė: 8–12 klasių mokiniai

Pamokos tikslas:

- Suprasti, kas yra aktyvus ir pasyvus skaitmeninis pėdsakas.
- Atpažinti rizikas, kurios kyla iš socialinių tinklų ir pasyvių duomenų rinkimo.
- Išmokti taikyti praktinius būdus, kaip sumažinti rizikas.

Pamokos eiga (45 min.)

1. Įžanga (5 min.)

Priemonės: projektorius / interaktyvi lenta, įvadinis klausimas ekrane.

Veikla: mokytojas pradeda klausimu: „Ar kada pagalvojote, kiek daug internete galima sužinoti apie jus, net jeigu nieko nesakote?“

Parodoma trumpa vizualizacija (pvz., Canva skaidrė). Mokiniai supažindinami su sąvoka „skaitmeninis pėdsakas“.

2. Teorinis pristatymas (10 min.)

Priemonės: PPT skaidrės.

Turinys: aktyvus ir pasyvus pėdsakas, istorinis kontekstas, „patinka ekonomika“.

Mokytojas užduoda klausimus klasei, kad išlaikytų įtrauktį.

3. Grupinė veikla „Mano pėdsakas“ (10 min.)

Priemonės: mokinių telefonai arba kompiuteriai.

Veikla: mokiniai įveda savo vardą „Google“, pažiūri, ką galima apie juos rasti.

Jei nenori naudoti savo duomenų – galima rinktis viešas figūras.

Refleksija: kas nustebino, kokia informacija buvo netikėta.

4. Praktinė užduotis „Privatumo nustatymų patikrinimas“ (10 min.)

Priemonės: mokinių telefonai, mokytojo skaidrės.

Veikla: mokytojas veda „gyvą turą“, kaip pakeisti Instagram, TikTok ar Facebook nustatymus.

Mokiniai realiai pakeičia 1–2 nustatymus savo telefone.

5. Diskusija „Ar mano pėdsakas mane apibūdina?“ (5 min.)

Veikla: klausimas poroms – „Kokį įspūdį sudarytų jūsų pėdsakas darbdaviui?“

Savanoriai pasidalina mintimis visai klasei.

6. Apibendrinimas (5 min.)

Mokytojas pakartoja pagrindines mintis: aktyvus/pasyvus pėdsakas, „patinka ekonomika“, rizikos.

Provokacinis klausimas pabaigai: „Ar šiandien žinote daugiau apie tai, kiek kiti gali matyti apie jus?“

Metodiniai patarimai mokytojui

- Įtraukimas: duokite mokiniams realiai naudotis savo įrenginiais.
- Pritaikomumas: parodykite, kad įgūdžiai naudingi tiek mokykloje, tiek ateityje.
- Etika: neprašykite viešinti asmeninių duomenų, naudokite pavyzdinius profilus.
- Adaptacija: jei telefonai neprieinami – parodykite pavyzdžius ekrane.

Papildomi įrankiai

- Kahoot testas apie privatumo rizikas
- Canva mini infografikas „Mano skaitmeninis pėdsakas“
- Padlet lenta refleksijai (jei dirbama grupėje)

Taikymas / pavyzdžiai

Šioje dalyje pateikiami realūs atvejai, kurie padeda suprasti skaitmeninio pėdsako poveikį kasdienėje veikloje. Kiekvienas pavyzdys struktūruotas taip: Aprašymas → Rizika → Diskusijos klausimai → Praktinis sprendimas.

- Mokykloje – klasės nuotrauka su žyma

Mokinys įkelia klasės nuotrauką ir pažymi draugus. Automatiškai rodoma vieta.

Rizika - Paviešinama, kur ir kada mokiniai būna.

Diskusijos klausimai:

- Ar žinai, kad gali pašalinti žymą?
- Kas gali matyti tavo buvimo vietą?

****Praktinis sprendimas:** Naudoti nustatymą „patvirtinti žymas prieš paskelbiant“.

- Darbe – darbdavio patikra „Google“ paieškoje

Studentas kandidatuoja į darbą, darbdavys suranda senas nuotraukas iš vakarėlio.

Rizika - Reputacijos žala, sumažėjusios įsidarbinimo galimybės.

Diskusijos klausimai:

- Kaip manai, ar darbdaviai turi teisę tikrinti socialinius tinklus?
- Ar tu pats prieš pokalbį patikrintum, ką apie tave galima rasti internete?

****Praktinis sprendimas:** Prieš darbo paiešką patikrinti savo skaitmeninį pėdsaką („egosurfing“).

- Namuose – programėlės leidimai

Žaidimas prašo prieigos prie mikrofono ir nuotraukų.

Rizika - Galimas duomenų rinkimas be reikalo.

Diskusijos klausimai:

- Ar žinai, kur nustatymuose gali pamatyti, kokius leidimus suteikei?
- Ar būtina suteikti prieigą prie mikrofono žaidimui, kuriame nėra garso funkcijų?

****Praktinis sprendimas:** Nustatymuose išjungti nereikalingus leidimus.

- **Viešose erdvėse – geolokacija iš „Snapchat“**

Jaunuolis palieka įjungtą „Snap Map“ funkciją, ir draugai gali realiu laiku matyti jo buvimo vietą.

Rizika - Asmens judėjimas tampa lengvai stebimas, gali būti naudojamas persekiojimui ar net vagystėms.

Diskusijos klausimai:

- Ar būtina dalintis savo buvimo vieta visada?
- Kam galėtų būti naudinga ši informacija?

****Praktinis sprendimas:** Nustatyti „Ghost Mode“ arba apriboti vietos dalinimąsi tik artimiausiems draugams.

- **Socialiniuose tinkluose – netikras profilis**

Sukurtas netikras profilis naudojant mokinio nuotrauką, rastą viešame albume.

Rizika - Tapatybės vagystė, reputacijos žala, galimi patyčių ar sukčiavimo atvejai.

Diskusijos klausimai:

- Ar lengva sukurti netikrą profilį naudojant viešai matomas nuotraukas?
- Kaip jaustumeisi, jei tai nutiktų tau?

****Praktinis sprendimas:** Riboti, kas gali matyti tavo nuotraukas; pranešti platformai apie netikrą paskyrą.

- **Kibernetinės grėsmės – sukčiavimo el. laiškas**

Mokinys gauna laišką su pažadu laimėti prizą spustelėjus nuorodą.

Rizika - Paspaudus nuorodą gali būti pavogti slaptažodžiai ar užkrėstas įrenginys.

Diskusijos klausimai:

- Kaip atpažinti sukčiavimo laišką?
- Ar visada galima pasitikėti nuoroda iš draugo?

****Praktinis sprendimas:** Nespustelėti nuorodų iš nepažįstamų siuntėjų, naudoti „Report phishing“.

- **Šeimoje – vaikų nuotraukos socialiniuose tinkluose**

Tėvai įkelia vaikų nuotraukas į Facebook, pridėdami ir vietos duomenys.

Rizika - Vaikų privatumo pažeidimas, galimybė nepažįstamiems žmonėms kaupti informaciją.

Diskusijos klausimai:

- Ar vaikai turėtų turėti teisę pasirinkti, ar jų nuotraukos viešinamos?
- Kas gali pasinaudoti tokia informacija?

****Praktinis sprendimas:** Dalintis tik privačiai; išjungti lokacijos rodymą; sukurti atskiras ribotas grupes šeimai.

- **Universitete – grupinio pokalbio ekranvaizdis**

Studentas pasidalina „Messenger“ pokalbio ekrano nuotrauka viešame forume.

Rizika - Kitų žmonių duomenys paviešinami be jų sutikimo.

Diskusijos klausimai:

- Ar galima dalintis pokalbio nuotrauka be kitų sutikimo?
- Kaip jaustumėtės, jei jūsų žinutė būtų paviešinta?

****Praktinis sprendimas:** Prieš dalinantis uždengti kitų žmonių vardus ir nuotraukas; gauti leidimą iš pokalbio dalyvių.

- **Psichologinė rizika – „Patinka“ ekonomika**

Jaunuolis įkelia nuotrauką ir nerimauja, jei nesurenka daug „patinka“.

Rizika - Savivertės mažėjimas, priklausomybė nuo socialinių tinklų dėmesio.

Diskusijos klausimai:

- Kodėl „patinka“ mums taip svarbūs?
- Ar galima būti aktyviu socialiniuose tinkluose nesiekiant patikti kitiems?

****Praktinis sprendimas: Riboti laiką socialiniuose tinkluose; nustatyti ekrano laiko limitus; suprasti, kad reakcijos $\neq$ žmogaus vertė.**