

Saugus nuotolinis mokymasis internete

Atmintinė mokytojams

1. Kompiuterinė darbo vieta.

Nuotoliniam mokymuisi rekomenduojama naudoti asmeninius kompiuterius su įdiegta Windows 10 operacine sistema. Jei naudojamos senesnės operacinės sistemos (Windows XP, Windows 7) reikia naudoti Antivirusinę programinę įrangą.(pvz: nemokamos -Avira Free Antivirus, Bitdefender Antivirus Free)

2. Slaptažodžiai.

Jungiantis prie nuotolinio mokymosi platformų, mokymosi sistemų bei socialinių tinklų, naudojami prisijungimo slaptažodžiai. Pasirenkant slaptažodžius rekomenduojama:

- Slaptažodžio ilgis- rekomenduojama ne mažiau 8 simboliai
- Slaptažodyje nenaudokite:
 - lengvai nuspėjamos asmeninės informacijos (pvz.: vardai, pavardės, gimimo datos, augintinių vardai ir tt);
 - Lengvai nuspėjamų simbolių sekų (pvz: 123456, qwerty, slaptazodis, 000000 ir pan)
 - Lietuviškų raidžių (ą,ų,š,č,ę,į,ū,ž)
- Slaptažodyje rekomenduojama naudoti derinius iš skaičių, didžiųjų bei mažųjų raidžių ir specialiųjų simbolių (pvz: „Sg.18@*L”)

3. Prisijungimo duomenys.

Paaiškinkite vaikams, kad negalima siųsti, perduoti jokių prisijungimo prie „virtualios klasės“ nuorodų ar duomenų kitiems asmenims.

4. Mokinių elgesys.

Priminkite mokiniams, kad virtualiose pamokose galioja tokios pačios drausmės ir mandagaus elgesio taisyklės kaip ir mokykloje. Stebėkite, ką „virtualioje klasėje“ veikia, ką kitiems demonstruoja mokiniai ir, pastebėję netinkamą elgesį, atitinkamai reaguokite.

5. Saugumo pažeidimai.

Mokytojas, prieš naudodamasis vaizdo konferencijų aplinka, įsitikina, kad atliko visus reikalingus veiksmus, siekiant sklandaus darbo:

- pakviečia prisijungti tik tuos asmenis, kurie turi dalyvauti veikloje;
- kontroliuoja, kas iš dalyvaujančiųjų gali kalbėti, dalintis savo kompiuterio ekranu arba pateikti informaciją ant Jūsų rodomo ekrano.

Jei atlikus visus šiuos veiksmus, vykstant vaizdo konferencijai, neteisėtai prisijungia pašalinis asmuo, neikvokite savo laiko ir energijos aiškinimuisi, kaip jis gavo prisijungimą, ką jis čia veikia, o stenkitės iš karto užblokuoti jo garsą ir vaizdą ir tęskite savo suplanuotas veiklas.

Apie nepageidaujamų asmenų prisijungimą ar nepageidaujamą elgesį Jūsų virtualioje aplinkoje informuokite savo mokyklos vadovą, pateikdama (-s) tai patvirtinančią informaciją, įskaitant įvykio laiką.

6. Duomenų apsauga.

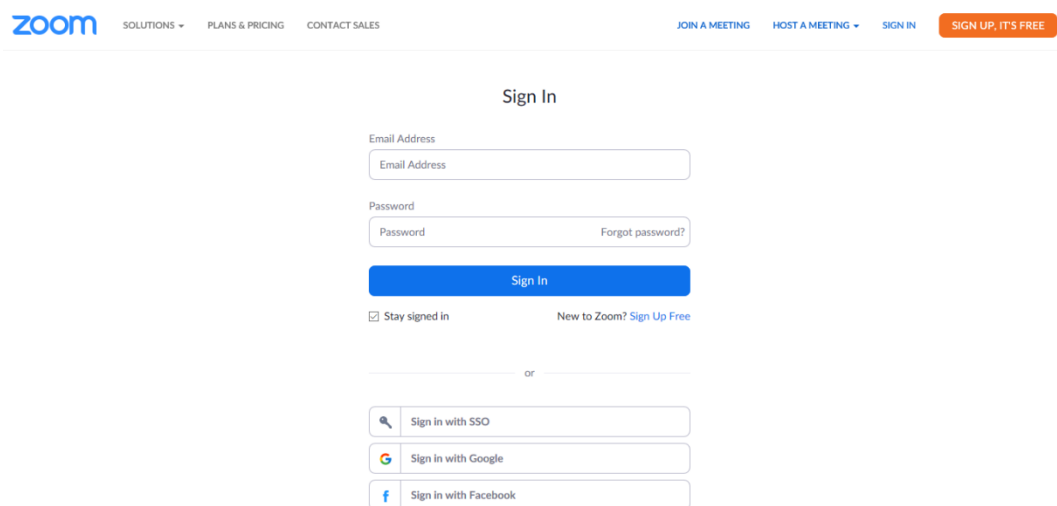
Asmens duomenys – tai bet kokia informacija, kuri padeda identifikuoti asmenį arba jo šeimos narius. Kalbant apie mokyklos duomenis, tai yra mokinio vardas ir pavardė, adresas, kontaktiniai duomenys, drausminės priemonės, pažymiai ir informacija apie pažangą. Šia informacija negalima dalintis per susirašinėjimo ar virtualių mokymų platformas. Jei mokiniai siunčia mokytojui atliktų darbų kopijas, turi būti galimybė panaikinti tokius susirašinėjamus (Pvz.: jei susirašinėjimas vyksta per Facebook Messenger programą, vėliau bus galima ištrinti grupę ir susirašinėjamą).

Saugus naudojimas ZOOM platforma

Saugiam ZOOM platformos naudojimui rekomenduojama atlikti žemiau pateiktus nustatymus, kad tai padaryti reikia:

1. Įjungti ZOOM nustatymų puslapį:

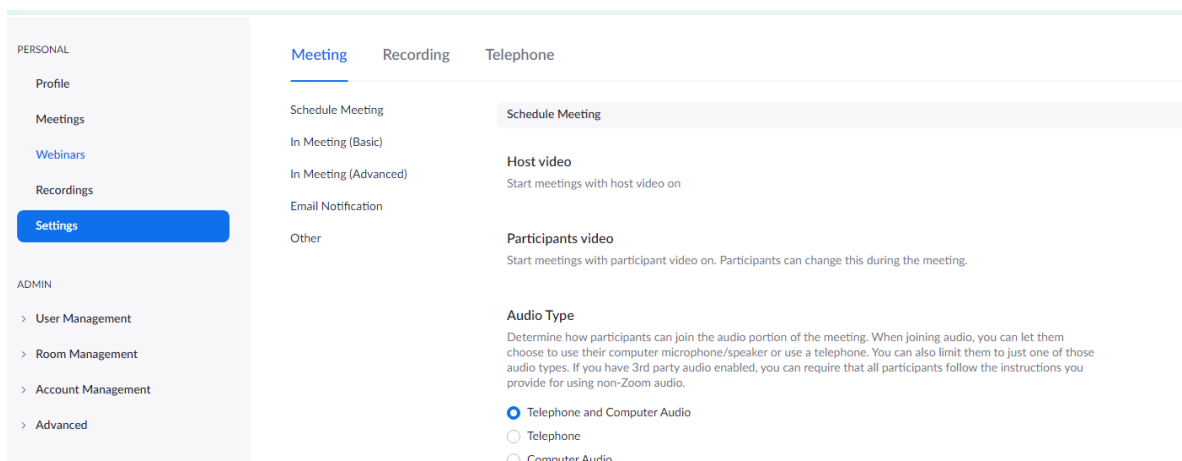
- a. Interneto naršyklės pagalba atverčiame puslapį <https://zoom.us/signin>









- b. Atsidariusiame lange pasirenkame prisijungimo prie savo ZOOM paskyros būdą:

- Jei jungiatės prie paskyros su savo susikurtu slaptažodžiu, įveskite savo email adresą ir slaptažodį, spauskite „Sign In“;
- Jei jungiatės kitais būdais (dažniausiai naudojamas prisijungimas per „Facebook“, spauskite atitinkamą prisijungimą

- c. Prisijungus, renkamės „Settings“



2. Patikriname sekančius nustatymus:

- a. Join before host – turi būti išjungtas. 
Pasirinkimas leidžia/neleidžia mokinių prisijungimą į virtualią klasę kol neprisijungusi mokytoja
- b. Require a password for instant meetings- turi būti įjungtas. 
Su pakvietimu bus siunčiamas ID ir slaptažodis. Jungiantis spaudžiant atsiųstą nuorodą, slaptažodžio nebus prašoma. Slaptažodis būtų reikalingas jungiantis prie virtualios klasės suvedant Meeting ID.
- c. Private chat – turi būti išjungtas. 
Įjungus, virtualios klasės mokiniai galės susirašinėti tarpusavyje. Nustatymas gali būti koreguojamas ir tiesiai iš virtualios pamokos mygtuko  pagalba
- d. File transfer – turi būti išjungtas. 
Įgalina failų persiuntimą tarp virtualios klasės mokinių.
- e. Screen sharing – turi būti įjungtas su sekančiais pasirinkimais:
Nustatoma kas galės demonstruoti savo ekrano vaizdą (Desktop Sharing) Nustatymas gali būti koreguojamas ir tiesiai iš virtualios pamokos mygtuko  pagalba.

Screen sharing

Allow host and participants to share their screen or content during meetings



Who can share?

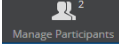


Host Only All Participants

Who can start sharing when someone else is sharing?

Host Only All Participants

Prasidėjus virtualiai pamokai rekomenduojama atlikti:

Paspaudus ekrano apačioje esantį „Security“ mygtuką-

- a. Įjungti opciją „Enable Waiting Room“ (Dažniausiai būna įjungta automatiškai) Į virtualią klasę dalyviai gali patekti tik mokytojai patvirtinus- paspaudus „Manage participants“  mygtuką ir pasirinkus Admit prie laukiančio dalyvio  
- b. Įjungti opciją „Lock meeting“ („užrakinama virtuali klasė) Įjungtama kai visi dalyviai susirinkę. Niekas daugiau nebus prijungtas prie virtualios klasės. Jei reikia kažką prijungti, opcija trumpam išjungtama.
- c. Išjungti opciją „Share Screen“. Išjungtama galimybė pamokos dalyviams demonstruoti savo ekrano vaizdą. Ekrano vaizdą galės rodyti tik mokytoja.
- d. Išjungti opciją „Chat“ . Išjungtama galimybė virtualios pamokos dalyviams susirašinėti tarpusavyje. Žinutes visiems dalyviams galės rašyti tik mokytoja