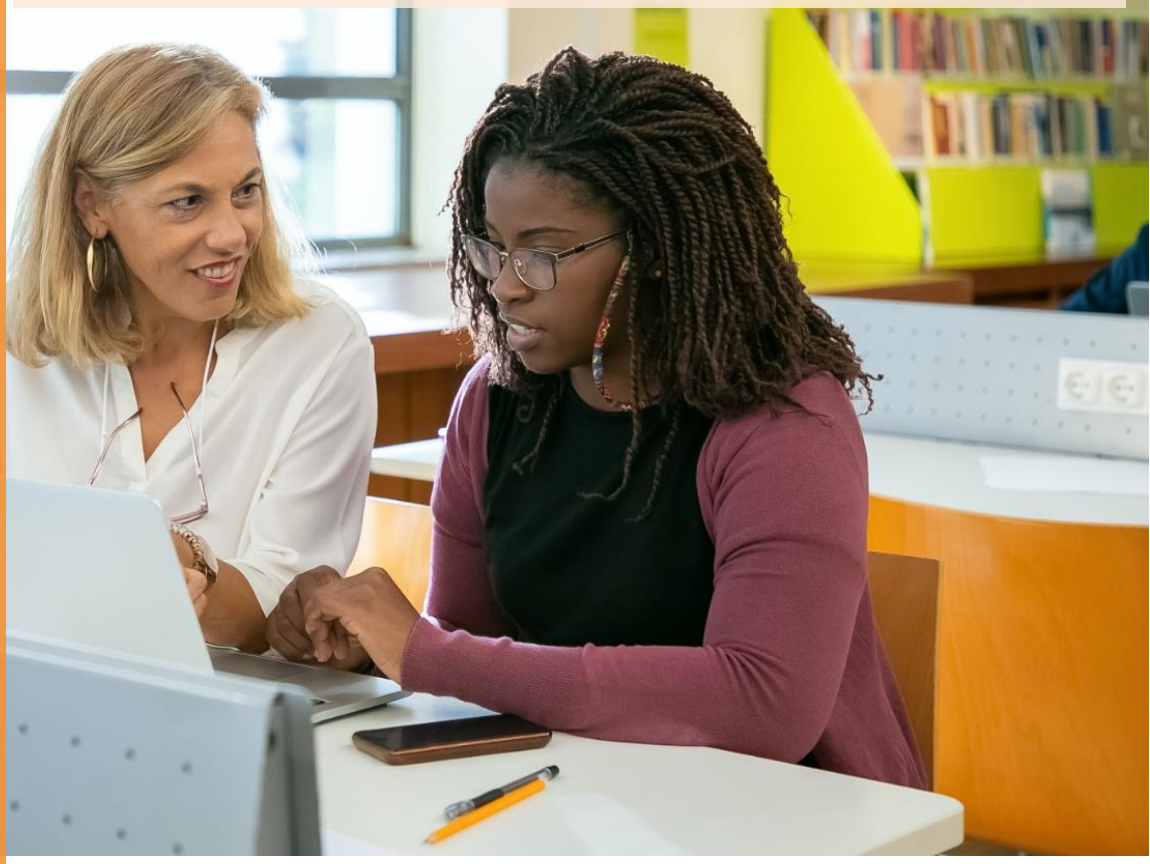
Projektas APRICOT:
Mokomės būti ir (su)gyventi besikeičiančiame laike: dėmesingos tėvystės ugdymo programa

# Medijų raštingumo programa ir medžiaga suaugusiųjų švietėjams

## 6 priedas. Saugus naudojimasis socialiniais tinklais



Bendrai finansuojama pagal Europos Sąjungos programą „Erasmus+“

Europos Komisijos parama šio leidinio rengimui nereiškia pritarimo jo turiniui, kuriame pateikiama autorių nuomonė, todėl Europos Komisija negali būti laikoma atsakinga už informaciją panaudotą šiame leidinyje.

Šį intelektinį produktą sumanė ir parengė strateginių partnerysčių projekto APRICOT komanda.
**Projekto koordinatorius** – VšĮ *Šiuolaikinių didaktikų centras* (Lietuva)
**Projekto partneriai**:
Apricot Training Management Ltd. (Jungtinė Karalystė)
ItF Institut Kassel e.V. – Frauencomputerschule (Vokietija)
Planeta Ciencias (Ispanija)

**Redakcijos koordinatorė**: Daiva Penkauskienė
**Rengėjai:** Hilary Hale, Beate Hedrich, Betül Sahin, Alejandra Goded, Anca Dudau, Daiva Penkauskienė
**Redakcinė kolegija**: Sophy Hale, Seda Gürcan, Konrad Schmidt, Cihan Sahin, Josafat Gonzalez Rodriguez, Roc Marti Valls, Virgita Valiūnaitė



**Metai, mėnuo:** 2021 lapkritis

Bendrai finansuojama pagal Europos Sąjungos programą „Erasmus+“

# Turinys



Bendrai finansuojama pagal Europos Sąjungos programą „Erasmus+“

# 6 priedas. Saugus naudojimasis socialiniais tinklais

## Skirtingi el. pašto adresai ir saugūs slaptažodžiai

Jei įmanoma, skirtingų socialinių tinklų paskyroms reiktų naudoti skirtingus el. pašto adresus. Taip, iš atitinkamuose puslapiuose pateikiamos informacijos, sunkiau sudaryti išsamų profilį. Skirtingiems el. pašto adresams susikurti, gali būti naudojamos nemokamos el. pašto paskyros. Šios paskyros turėtų būti retkarčiais panaudojamos, kad liktų suaktyvintos. Renkantis teikėją, reikia pasirūpinti, kad teikėjas negalėtų baigti el. pašto galiojimo ir nepriskirtų jo naujam vartotojui. Priešingu atveju, yra rizika, kad kitas vartotojas perims el. pašto adresą ir taip gaus prieigą prie susietos socialinio tinklo paskyros.

Taip pat rekomenduojama naudoti skirtingus ir saugius slaptažodžius atskiroms paslaugoms, pvz., „Facebook“ ar „Twitter“. Svarbi taisyklė slaptažodžiui: kuo ilgesnis, tuo geriau. Jį turėtų sudaryti mažiausiai aštuoni simboliai, slaptažodis neturėtų būti vientisas žodis, jį turėtų sudaryti didžiosios ir mažosios raidės bei specialieji simboliai ir skaičiai. Slaptažodžių tvarkyklė, pvz., *keepass.info*, gali palengvinti įvairių slaptažodžių tvarkymą. Niekada negalima duoti savo slaptažodžio tretiesiems asmenims.

## Dviejų komponentų (two-factors) autentifikavimas

Naudojant *dviejų komponentų* autentifikavimą, saugumas dar labiau padidėja. Šį saugumo būdą sudaro: pirmasis komponentas (kategorijos žinios) – stiprus slaptažodis ir antrasis komponentas (kategorijos valdymas) – techninis įrenginys, pvz., raktas, išmanioji kortelė ar speciali USB atmintinė, naudojamas papildomam autentifikavimui. Gali būti naudojama ir teikėjo atsiunčiama SMS žinutė. *Dviejų komponentų autentifikavimas* suteikia daug geresnę vartotojo paskyros apsaugą. Kad neteisėta prieiga būtų prieinama trečiosioms šalims, reikalingi abu komponentai – reikia žinoti slaptažodį ir turėti įrenginį.

## Atsargumas diegiant programėles, priedus ar papildinius

Daugelis socialinių tinklų leidžia įdiegti trečiųjų šalių programas, pvz., žaidimus. Tačiau internetiniai sukčiai taip pat sukuria tokias programas ir išnaudoja jas, kad gautų prieigą prie profilio. Prieš kažką diegiant, būtina patikrinti teikėjo ir šaltinių patikimumą.

## Ypatingas atsargumas naudojant mobilųjį telefoną

Socialiniai tinklai dažnai naudojami per mobiliuosius įrenginius, tokius kaip išmanieji telefonai ar planšetiniai kompiuteriai. Operatoriai ar trečiųjų šalių teikėjai tam kuria programėles. Šios programėlės dažnai naudoja „jautrius“ duomenis, esančius mobiliajame įrenginyje, pvz., adresų knygelę, nuotraukas, vaizdo įrašus ar vietos informaciją. Be to, mobilusis įrenginys paprastai automatiškai užregistruojamas socialiniame tinkle. Jei prietaisas pametamas, duomenis gali panaudoti jį radęs ar pavogęs asmuo, klaidinančiai prisistatydamas kaip savininkas. Dėl šios priežasties, reiktų nesaugoti slaptažodžių mobiliuosiuose įrenginiuose ir, vietoj jungimosi per programėlę, jungtis bei atsijungti tiesiai iš socialinio tinklo svetainės.

Bendrai finansuojama pagal Europos Sąjungos programą „Erasmus+“

## Prašymas susisiekti

Tapatybės vagystė yra viena iš skaitmeninio amžiaus rizikų. Prašymai susisiekti turi būti priimami atsargiai. Jei iš pažįstamų gaunami abejotini prašymai, reikia visada patikrinti šių žinučių patikimumą. Svarbu į savo draugų ar kontaktų sąrašą įtraukti tik žmones, žinomus „iš realaus pasaulio“. Nežinomi asmenys gali turėti piktų ketinimų. „Virtualūs draugai“ gali būti asmenys tariamų ar netikrų paskyrų pagalba prisiėmę svetimą tapatybę ir galimai panaudoti jas nusikalstamoms veikoms ar neteisėtam verslui internete.

## Kiekvienas nuorodų ar mygtukų paspaudimas pasveriamas iš anksto

Internetiniai nusikaltėliai naudojasi socialiniais tinklais, kad pokalbiuose pritrauktų vartotojus įrašais ar nuorodomis į paruoštas svetaines. Tokios svetainės naudojamos prieigai prie duomenų arba įrenginių užkrėtimui kenkėjiška programa. Nekaltai atrodantis paspaudimas gali aktyvuoti kenkėjiškų programų įdiegimą įrenginyje. Kenkėjiška programa gali, pavyzdžiui, nepastebimai įjungti įrenginio kamerą, per mikrofoną įrašyti pokalbius arba užklausti vietos. Įrenginyje saugoma adresų knygelė, nuotraukos ar vaizdo įrašai gali patekti į neteisėtas rankas.

## Privatumo apsauga

Kiekvienas socialinis tinklas siūlo eilę privatumo nustatymų. Šiuos nustatymus galima naudoti, pvz., norint rodyti savo profilį tik draugams ir leisti skelbti įrašus. Reiktų apsvarstyti glaudžią socialinių tinklų operatorių integraciją su kitomis interneto paslaugomis. Ši integracija leidžia sudaryti labai išsamų vartotojo profilį. Retkarčiais reiktų atlikti internetinę savo ar šeimos narių paiešką, kad būtų galima sužinoti, kokią informaciją apie jus galima rasti. Taip pat reiktų reguliariai tikrinti naudojamų socialinės žiniasklaidos paskyrų saugos nustatymus ir atkreipti dėmesį į nuorodas, vedančias į kitas paskyras. Socialinės žiniasklaidos paslaugų teikėjai gali pakeisti šiuos nustatymus savo iniciatyva.

Nereiktų teikti asmeninės informacijos tinkle. Kai informacija yra paskelbiama internete, ją labai sunku arba net neįmanoma ištrinti.

## Pranešimas apie kibernetinį persekiojimą ir neapykantos komentarus

- Svarbu pranešti apie asmenis, kurie priekabiauja ar įžeidinėja kitus, socialinio tinklo operatoriui. Operatoriai gali ištirti ir ištrinti abejotinas paskyras.
- Akivaizdžių ar įtariamų nusikaltimų atveju svarbu kreiptis patarimo į policiją.
- Reikia informuoti asmenis, kurių atžvilgiu nukreiptas netinkamas elgesys ir, jei reikia, paduoti skundą.

## Paskyros ištrynimas

Jei paskyra nebenaudojama, galima sukurti atsarginę duomenų kopiją, o paskyrą ištrinti. **Perskaitykite duomenų apsaugos taisykles ir bendrąsias sąlygas.**

Bendrai finansuojama pagal Europos Sąjungos programą „Erasmus+“

## Teisės ir pareigos

Socialinius tinklus valdo pelno siekiančios kompanijos, kurios dažniausiai finansuojamos iš reklamos. Taisyklėse ir sąlygose pateikiama informacija apie tai, kaip paslaugų teikėjas tvarko asmens duomenis ir kaip šie duomenys perduodami reklamos industrijai. Prieš kuriant profilį, būtina atidžiai perskaityti bendrąsias taisykles ir sąlygas bei duomenų apsaugos nuostatas.

Kai kurie socialiniai tinklai numato sau teisę į vartotojų leidinius. Tai reiškia, kad, pavyzdžiui, nuotraukų ir vaizdo įrašų naudojimo teisės perduodamos socialinio tinklo operatoriui. Be to, gana įprasta, kad suteiktos naudojimo teisės išlieka, net jei vartotojas palieką tinklą ir ištrina profilį. Taigi, prieš kažką paskelbiant, reikia labai gerai pagalvoti. Taip pat reikėtų pasirūpinti, kad skelbiant paveikslėlius, tekstus ar vaizdo įrašus nebūtų pažeistos trečiųjų šalių teisės.

Socialiniuose tinkluose taip pat yra elgesio taisyklės – internetinis etiketas (*netiquette*), kurio privalu laikytis.

Internetinis etiketas reiškia taisykles, kurias dauguma žmonių laiko savaime suprantamomis. Beveik kiekvienas forumas ir kiekviena svetainė, pokalbių kambarys ir t.t. turi savo internetinį etiketą. Tačiau, iš esmės, gairės yra tos pačios:

- Pirmiausia perskaitykite, tada pagalvokite, tada skelbkite.
- Tekstas turi būti trumpas.
- Laikykitės teisinių nuostatų.
- Būkite mandagūs ir tolerantiški.
- Nenaudokite per daug didžiųjų raidžių ar skyrybos ženklų, tokių kaip šauktukai.
- Jokių žodinių atakų.
- Taisyklinga rašyba.
- Naudokite skyrybos ženklus.
- Pasakyti „ačiū“ niekada nepakenks.
- Jokio šlamšto ir ilgų tekstų.
- Nenaudokite per daug šypsenėlių.
- Jokios diskriminacijos, seksistinių ar rasistinių šūkių.
- Neskelbkite asmeninių duomenų, telefono numerių ar reklamos.

Prieš užduodant klausimą pirmiausia naudojama paieškos funkcija, ieškoma DUK‘e (skiltyje *Dažniausiai užduodami klausimai*). Daugeliu atvejų tai užkerta kelią vėl ir vėl užduoti klausimą, kuris jau buvo užduotas.

Priklausomai nuo portalo, tinklaraščio ir t.t. taisyklių sąrašas gali skirtis. „Internetinis etiketas“ naudojamas „Facebook“, el. laiškuose ir kitose vietose, kur galima rašyti savo tekstus ir komentarus internete.

## Asmeninės atakos ir elektroninės patyčios

Socialinė žiniasklaida, „Messenger“ paslaugos ir kitos programėlės įgalina arba palengvina patyčias internete ir kibernetinį persekiojimą, nes dažnai siūlo ne tik platformas, kuriose patyčios ar persekiojimai vyksta, bet ir viešai skelbia privačią naudotojų informaciją.

Bendrai finansuojama pagal Europos Sąjungos programą „Erasmus+“

## Elektroninės patyčios

Patyčios elektroninėje erdvėje – tai tyčinis, tam tikrą laiką tunkantis kitų asmenų įžeidinėjimas, gąsdinimas, „jautrios“ informacijos viešinimas ar priekabiavimas internete. Agresorius (patyčių iniciatorius) ieško aukos, kuri negali arba turi sunkumų apsiginti nuo išpuolių ir naudoja šį jėgų disbalansą, stumdamas auką į socialinę izoliaciją.

Elektroninės patyčios vyksta socialiniuose tinkluose, vaizdo portaluose ir išmaniųjų telefonų žinučių programėlėse, pvz., „WhatsApp“, erzinančių telefono skambučių pagalba ir pan. Patyčių iniciatorius dažniausiai elgiasi anonimiškai, todėl auka nežino, iš kur kyla išpuoliai, priešingai nei realių patyčių atveju, kai paaugliai dažniausiai pažįsta vienas kitą iš savo tikros asmeninės aplinkos. Todėl aukos beveik visada įtaria, kas slepiasi už išpuolių.

### Skirtumas tarp elektroninių patyčių ir patyčių

Patyčios elektroninėje erdvėje kai kuriais aspektais skiriasi nuo patyčių realiame pasaulyje.

- **Elektroninės patyčios nesibaigia su mokykla ar darbu**. Kadangi elektroniniai priekabiautojai gali pulti internetu 24 valandas per parą, jie gali persekioti ir namuose.
- Patyčių elektroninėje erdvėje mastas yra didesnis nei realiame gyvenime, nes:
  - auditorija yra nevaldomai didelė;
  - turinys plinta itin greitai;
  - turinys, kuris buvo seniai užmirštas, gali bet kada išplaukti į viešumą.
- **Patyčių iniciatoriai gali veikti anonimiškai**: agresorius tiesiogiai nepasirodo savo aukai. Nežinojimas, kas yra agresoriai, gali dal labiau gąsdinti ir neraminti auką.
- **Poveikis aukai nematomas**: nusikaltėlis nemato aukos reakcijos į įžeidžiantį pareiškimą ar žeminantį vaizdą, todėl gali nepilnai suvokti savo išpuolių poveikio.

### Patyčių tipai

Elektroninės patyčios, kaip ir patyčios realiame gyvenime, būna skirtingų tipų:

- **Priekabiavimas**: pakartotinai siunčiamos įžeidžiančio ir skaudinančio pobūdžio žinutės el. paštu, trumposiomis / momentinėmis žinutėmis ar pokalbiuose (*chats*).
- **Šmeižtas / gandai**: gandų skleidimas internetu ir mobiliojo telefono paslaugų pagalba didesnei žmonių grupei.
- **„Jautrios“ informacijos atskleidimas**: informacijos, konfidencialiai suteikto konkrečiam asmeniui, siuntimas kitiems, siekiant sukompromituoti auką.
- **Atskirtis / ignoravimas**: sąmoningas atskyrimas nuo socialinės veiklos, grupių, pokalbių ir kt.

### Interneto kultūros veiksnių įtaka elektroninėms patyčioms

Internetas lemia didžiulius žmonių bendravimo būdų pokyčius. Viena vertus, tai teigiamas pokytis, kurio dėka žmogus visada lengvai pasiekiamas, galima greitai patikrinti, ką parašė draugas ar kokia nuotrauka buvo ką tik paskelbta. Kita vertus, galima pastebėti ir neigiamų tendencijų, kurias atneša ši nauja „internetinio bendravimo kultūra“.

Bendrai finansuojama pagal Europos Sąjungos programą „Erasmus+“

## Greitas gyvenimo tempas

Interneto greitis vis didesnis, mobilusis internetas taip pat nuolat gerina savo galimybes. Informacija vartotoją pasiekia vis greičiau, vis per trumpesnį laiką. Vartotojai taip pat prie to prisitaiko. Bendravimas tampa greitesnis ir neramesnis. Viena diena neprisijungus reiškia – kitą dieną kompiuteryje ar išmaniajame telefone yra daugybė draugų, pažįstamų ar kolegų žinučių.

Tačiau šis greitis lemia ir tai, kad įrašai, nuotraukos ar vaizdo įrašai bendrinami ir siunčiami spontaniškai. Ne tik teigiami, bet ir žmogui nepalankūs momentiniai vaizdai ar menkinantys komentarai. Ši informacija per įvairias paslaugas labai greitai pasklinda nevaldomai didelei žmonių grupei.

## Anonimiškumas ir atstumas

Anonimiškumas palankus nevaržomam internetiniam bendravimui. Kiekvienas, kuris anonimiškai naršo internete, sunkiai gali sulaukti neigiamų savo veiksmų pasekmių. Dar daugiau, bendraujant internetu negalima matyti tiesioginės kitos pusės reakcijos, išskyrus vaizdo pokalbius. Todėl vartotojas dažnai negali įvertinti, kaip kiti priima jo pareiškimus, nes nemato, kaip kitas žmogus reaguoja, kokios jo veido išraiškos ir gestai. Kadangi taip bendraujantys žmonės nesusitinka akis į akį, internete lengva įskaudinti kitų žmonių jausmus.

## Perteklinis asmeninės informacijos bendrinimas

Socialiniai tinklai ir daugelis paslaugų, tokių kaip „WhatsApp“, „Twitter“, „Ask.fm“ ir kt., priklauso nuo to fakto, kad vartotojai dalijasi vieni su kitais daugeliu dalykų. Vaikai ir paaugliai lengvai susigundo daug atskleisti apie save, nes nori išbandyti, kaip pasiekti savo bendraamžius. Tačiau kitų atsiliepimai apie paskelbtas nuotraukas, vaizdo įrašus ir kitus pateiktus duomenis ne visada teigiami, o vartotojas diskredituojamas ir užgauliojamas dėl atsiskleidimo kitiems.

## Draugai ar pažįstami

Naudojant socialinius tinklus ir momentinio susirašinėjimo platformas, galima greitai ir lengvai užmegzti naujas pažintis. Tokie pažįstami iš karto pridedami į „Facebook“, „WhatsApp“ ir kitur. Laikui bėgant kaupiasi vis daugiau kontaktų, atsiradusių įvairiomis aplinkybėmis. Darosi vis sunkiau aprėpti bendrą vaizdą. Tačiau svarbu suprasti, kas gali skaityti įrašus, matyti nuotraukas, nes ne viskas tinka visiems kontaktams.

Daugelis socialinių tinklų siūlo vartotojams galimybę rūšiuoti savo kontaktus į skirtingas grupes. Įrašus, kuriuos įkelia vartotojas, galima bendrinti specialiai konkrečioms grupėms (draugams, pažįstamiems ir pan.). Tokiu būdu galima išvengti nemalonių nepažįstamų žmonių reakcijų į asmeninį indėlį.

## Patarimai tėvams

Kaip tėvams suprasti, kad jų vaikas patiria patyčias?

Bendrai finansuojama pagal Europos Sąjungos programą „Erasmus+“

Elektronines patyčias galima aptikti ir su jomis kovoti ankstyvosiose stadijose. Jei pastebėjote, kad vaiko elgesys staiga pasikeitė, reikalinga pagalba. Požymiai, rodantys, kad vaikas galimai patiria elektronines patyčias:

- vaikas tampa uždaras;
- praranda norą bendrauti;
- smarkiai pasikeitė vaiko naudojimosi internetu įpročiai;
- izoliuojasi nuo išorinio pasaulio;
- reaguoja agresyviai;
- turi daug pasiteisinimų ar nepaaiškinamų fizinių nusiskundimų;
- savo išvaizda ima mėgdžioti sektinus pavyzdžius ir grožio idealus;
- sumenkina savo padėtį.

Atsiradus šiems simptomams, tėvai, norėdami išvengti galimos didelės elektroninių patyčių žalos, turėtų nedelsdami pasikalbėti su vaiku užkirsdami joms kelią. Jei vaikas patiria patyčias platesniu mastu, visada patartina pasikonsultuoti su specialistu. Pagalbą internete galima rasti „Büendnis gegen Cybermobbing e.V. – Mobbing Internet / Netz“ ((https://www.buendnis-gegen-cybermobbing.de) ir „Klicksafe“ (https://www.klicksafe.de/themen/kommunizieren/cyber-mobbing).

## Kaip tėvai gali padėti savo vaikams?

Svarbu pro aktyviai kalbėti su patyčių aukomis apie jų problemas ir suteikti pirminę emocinę paramą. Tačiau tėvai turėtų klausti ir eksperto patarimo bei nuomonės, kaip antai pasinaudojant nemokama konsultacine telefono linija. Ši karštoji linija gali būti pasiekiama anonimiškai 24 valandas per parą ir turi tinkamai apmokytus kontaktinius asmenis. Taip pat svarbu nevengti vaiko problemų, neapsimesti, kad nieko nevyksta, bet veikti atvirai.

## Kaip apsisaugoti nuo patyčių internete?

Nėra jokios garantijos, kad netapsite elektroninių patyčių auka. Siekiant sumažinti pavojų, gali būti naudojami paprasti, bet veiksmingi metodai. Kaip bendrai elgesiui internete, taip ir apsisaugojimo nuo patyčių atveju, galioja tie patys principai:

- niekada per daug neatskleiskite internete savo privataus gyvenimo;
- atidžiai valdykite privatumo nustatymus ir atsakingai pasirinkite draugus;
- galvokite, ką ir kieno atžvilgiu darote internete;
- būkite labai atsargūs viešai kalbėdami apie rūpesčius ir problemas internete.

**Nepamirškite, žinios yra jėga!**

Tėvai turėtų atkreipti vaikų dėmesį į tai, kaip elgtis elektroninių patyčių atveju, atvirai kalbėdami apie patyčias ir nagrinėdami įvairius variantus. Labai svarbus dalykas, kad tėvai aiškiai pasakytų, jog apie tai yra bet kada yra pasirengę pasikalbėti.

Bendrai finansuojama pagal Europos Sąjungos programą „Erasmus+“