

Projekto numeris: 2023-2-LT01-KA210-ADU-000173746

POZITYVI SKAITMENINĖ TĖVYSTĖ



Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.



IVADAS ✱



JTVTK pozityvią tėvystę apibrėžia kaip tėvų elgesį, kuriuo atsižvelgiama į vaikų interesus ir jų teises. Visame pasaulyje šeimose pradėjus naudoti internetą, naujas skaitmenines technologijas ir socialinę žiniasklaidą, esminis tėvų vaidmuo ir auklėjimo tikslai išlieka nepakitę: tėvai vis dar privalo auklėti, saugoti, aprūpinti, mylėti, bendrauti su vaikais ir jiems vadovauti. Taip pat galioja, kad auklėjimo praktika tiek anksčiau, tiek šiandien yra veiksmingiausia, kai ji grindžiama pozityviosios tėvystės vertybėmis ir principais, skatinančiais atvirą bendravimą ir pasitikėjimą. Šiuos modelius ir vertybes reikia taikyti ir interneto pasaulyje, kad būtų ne tik užmegztas ryšys tarp tradicinių vertybių ir interneto pasaulio, bet ir apribota su juo susijusi rizika vaikams. Skaitmeninė aplinka vaikams teikia didžiulę naudą, atverdamą naujus švietimo, kūrybiškumo ir socialinės sąveikos kanalus. Tačiau ji taip pat gali kelti rimtų pavojų, įskaitant elektronines patyčias, pavojų privatumui, kitų veiklų apleidimą, sėslų elgesį, priklausomybę nuo interneto ir kt.

ĮVADAS ✨



"Erasmus+" projekto POZITYVI SKAITMENINĖ TĖVYSTĖ tikslas - suteikti tėvams žiniasklaidos priemonių naudojimo raštingumo žinių ir priemonių, kad jie galėtų ugdyti savo vaikų kritinio mąstymo įgūdžius bendraujant su skaitmenine žiniasklaida: analizuoti interneto turinį, atpažinti šališkumą, dezinformaciją ir priimti pagrįstus sprendimus skaitmeninėje aplinkoje. Derindami kritinį mąstymą su žiniasklaidos priemonių naudojimo raštingumu, tėvai gali geriau parengti savo vaikus atsakingai ir įžvalgiai naršyti skaitmeniniame pasaulyje.

Ši mokymosi programa bus įvadinis mokymas tėvams, nes jie yra pagrindiniai globėjai ir auklėtojai šeimoje. Šiuo metodu siekiama išmokyti tėvus suprasti su mokymusi internete ir dinamiškų internetinių priemonių naudojimu susijusius klausimus, kad jie galėtų integruotis į savo vaikų skaitmeninį gyvenimą ir padėti tėvams bei vyresnio amžiaus suaugusiems šeimoje mokytis apie interneto pavojus ir spąstus. Ši mokomoji medžiaga skatina saugą internete ir sprendžia skaitmeninės atskirties, egzistuojančios tarp skirtingų šeimos kartų, problemą.



Co-funded by
the European Union

PARTNERIAI



ASOCIACIJA IVAIGO

- Projektų rengimas per socialinius tyrimus, sutelkiant dėmesį į pagrindines problemas, su kuriomis šiuo metu susiduria visuomenė: ~~kok~~ialinė įtarka, aplinkosaugos problemos, bet diskriminacija, skaitmeninė transformacija, fizinės ir psichinės sveikatos priežiūra, moterų įgalinimas, nedarbas, verslumas ir kt.
- Žinių įgijimas ir kūrybiškumo, vaizduotės bei kritinio mąstymo skatinimas pasitelkiant visų rūšių meną ir sportą.
- Tvarus dalyvių profesinių ir asmeninių įgūdžių tobulinimas daugiakultūriniame kontekste.
- Atstovavimas jaunų žmonių, ypač mažumų ir socialinių grupių, interesams.
- Formalaus ir neformalaus jaunimo švietimo skatinimas per vietos veiklą ir tarptautinius projektus. IVAIGO kuria įtraukią aplinką, skatinančią teisingumą ir lygybę.



PARTNERIAI



INCIRLIOVA GENCLIK KULTUR SANAT VE GELISIM DERNEGI

- İ.ova Gençlik Kültür, Sanat ve Gelişim Derneği -IOVA yra ne pelno siekianti organizacija, kurios nariais yra daugiau nei šimtas (100) asmenų, kūrybingų piliečių, žmonių, kurie dalijasi vertybėmis, idėjomis, mintimis, apmąstymais ir vizija. IOVA yra jauna ir dinamiška organizacija, kuri buvo sukurta kaip atsakas į poreikį sukurti gyvybingą, bendruomenės pagrindu veikiančią darinį, kuris gebėtų atpažinti galimybes ir reaguoti į iššūkius, susijusius su vietos bendruomenės ir jos narių unikalumu. IOVA daugiausia dėmesio skiria: Skatinti pilietinį dalyvavimą ir aktyvų įsitraukimą per neformalųjį švietimą;
- įgyvendinti naujas socialines praktikas žiniasklaidos saugumo, netikrų naujienų, smurto socialiniuose tinkluose, žiniasklaidos technologijų konvergencijos ir kt. srityse; IRT strategijų, kaip skaitmeninės atskirties mažinimo priemonės ir kaip galingos ekonominės ir socialinės plėtros visoje ES priemonės, vertė; Skaitmeninio švietimo teikimas su jaunimu dirbantiems asmenims, suaugusiųjų instruktoriams ir mokytojams



PARTNERIAI



EESTI PEOPLE TO PEOPLE

Eesti People to People yra 1997 m. Estijoje įregistruota pelno nesiekianti organizacija, veikianti nuo 1993 m. kaip tarptautinės nevyriausybinės organizacijos "People to People" skyrius. Organizacijos "People to People" tikslas - stiprinti tarptautinį supratimą ir draugystę vykdant švietimo, kultūros ir humanitarinę veiklą, kurios metu įvairių šalių ir skirtingų kultūrų žmonės tiesiogiai keičiasi idėjomis ir patirtimi. Eesti PTP siekia stiprinti tarpkultūrinį bendravimą kiekvienoje bendruomenėje ir tarp bendruomenių bei tautų. Pagrindinės temos yra tolerancija ir tarpusavio supratimas.



Co-funded by
the European Union

Turinys

01

SAUGUMO INTERNETE
SVARBA
SKAITMENINIS PĖDSAKAS

02

PRIVATUMAS INTERNETE
DUOMENŲ PRIVATUMAS
GRĖSMĖS IR PAVOJAI INTERNETE

03

INTERNETINIAI PAVOJAI
PAVOJŲ INTERNETE TĖPAI
KIBERNETINĖS PATYČIOS
KIBERNETINIAI GROBUONYS

04

PRIVAČIOS INFORMACIJOS
SKELBIMAS
FIŠINGAS (SUKČIAVIMAS)

05

PASIKLIOVIMAS SUKČIAIS
ATSITIKTINIS KENKĖJIŠKŲ PROGRAMŲ
ATSISIUNTIMAS
PAGRINDINIAI GEBĖJIMAI UŽTIKRINTI
SAUGUMĄ INTERNETE

06

AKTYVIOS INTERNETO SAUGOS
PRIEMONĖS IR GAIRĖS

07

TĖVŲ KONTROLĖS PRIEMONĖS

08

PAGRINDINĖS PRIEŽIŪROS REKOMENDACIJOS
TĖVAMS

09

TĖVŲ PRIEŽIŪROS PATARIMAI

10

SAUGOS INTERNETE PATIKRA
NUORODOS



Co-funded by
the European Union

Naudojimasis internetu yra giliai įsišaknijęs į šiuolaikinės šeimos gyvenimą: vaikai ir jaunimas aktyviai įsitraukia į veiklą internete, o senjorai pamažu perpranta skaitmeninį kraštovaizdį. Kadangi tėvai vis dažniau imasi skaitmeninių paslaugų teikėjų vaidmens, jiems labai svarbu nepamiršti su naudojimusi internetu susijusios rizikos.

Nors internetas teikia daugybę privalumų, įskaitant prieigą prie informacijos ir bendravimo platformų, jis taip pat kelia naudotojams įvairių pavojų, pavyzdžiui, netinkamo turinio, saugumo pažeidimų, dezinformacijos ir kibernetinių patyčių. Tėvai turi aktyviai saugoti savo šeimos narius, gerbdami jų privatumą.

Svarbu, kad tėvai neužimtų atgrasios pozicijos skaitmeninių technologijų atžvilgiu, bet priimtų iššūkį užtikrinti, kad vaikai, jaunimas ir senjorai galėtų saugiai naudotis interneto teikiamais privalumais. Tam reikia suteikti jiems įgūdžių ir žinių, kad jie galėtų atpažinti ir sumažinti internete kylančius pavojus ir grėsmes.

Todėl visiems šeimos nariams, įskaitant vaikus, paauglius, jaunus suaugusiuosius, tėvus ir senjorus, būtinas visapusiškas mokymas apie saugą internete. Tėvai, kaip šeimos pagrindas, turi išskirtinę galimybę teikti paramą, pagalbą ir patarimus pažeidžiamiausiems šeimos nariams.

Erasmus+ projekto POZITYVI SKAITMENINĖ TĖVYSTĖ projekto A2 saugaus naudojimosi internetu gairėmis siekiama supažindinti tėvus su internete tykančiais pavojais, kad jie galėtų laikytis prevencinio ir informuoto požiūrio ir maksimaliai padidinti naudojimosi internetu naudą, kartu užtikrindami savo šeimos narių saugumą.



Co-funded by
the European Union



SAUGUMO INTERNETE SVARBA

Saugumas internete, arba interneto sauga, yra labai svarbus aspektas, padedantis atsakingai naršyti skaitmeniniame pasaulyje. Jis apima įvairią praktiką ir elgesį, kuriais siekiama apsaugoti save ir kitus nuo grėsmių ir pavojų internete. Tai apima asmeninės informacijos apsaugą, saugių bendravimo kanalų užtikrinimą ir teigiamo skaitmeninio pilietiškumo skatinimą.

Šiuolaikiniame tarpusavyje susijusiame pasaulyje, kuriame išmanieji telefonai, planšetės ir kompiuteriai yra visur, būti saugiam internete yra kaip niekada svarbu. Asmenys turi žinoti su veikla internete susijusią riziką, pavyzdžiui, kibernetinės patyčias, sukčiavimą ir netinkamo turinio poveikį. Būdami informuoti ir taikydami saugią praktiką, asmenys gali sumažinti šią riziką ir saugiau naudotis internetu.

Tėvams ir globėjams svarbiausia užtikrinti vaikų saugumą internete. Tam reikia stebėti jų veiklą internete, nustatyti amžių atitinkančius apribojimus ir mokyti juos saugaus elgesio internete. Be to, skatindami atvirą bendravimą apie patirtį internete, galite padėti vaikams jaustis patogiau, jei jie norės aptarti bet kokius rūpesčius ar problemas, su kuriomis gali susidurti internete.

Galiausiai, saugumas internete - tai asmenų įgalinimas priimti pagrįstus sprendimus ir užtikrintai naršyti skaitmeniniame pasaulyje. Būdami budrūs ir laikydamiesi tinkamos kibernetinės higienos, visi galime prisidėti prie saugesnės ir patikimesnės interneto aplinkos visiems.



Co-funded by
the European Union

SKAITMENINIS PĖDSAKAS

Skaitmeninio pėdsako sąvoka yra panaši į „elektroninių duonos trupinių“ pėdsaką naršant internete. Šį pėdsaką sudaro įvairūs veiksmai ir sąveikos, pavyzdžiui, lankomos svetainės, įkeliamos nuotraukos ir bendravimas socialiniuose tinkluose. Panašiai kaip pėdsakai paplūdimyje, jūsų skaitmeninis pėdsakas gali daug ką atskleisti apie jus ir jūsų veiklą internete.

Tačiau kitaip nei paplūdimio pėdsakai, kurie laikui bėgant gali išnykti, jūsų skaitmeninis pėdsakas gali išlikti neribotą laiką. Tai reiškia, kad viskas, ką darote ar rašote internete, gali likti visam laikui, net jei vėliau tai ištrinsite. Šis išliekamumas pabrėžia, kad svarbu nepamiršti, kuo dalijatės internete, ir galimas savo skaitmeninių veiksmų pasekmes.

Jūsų skaitmeniniame pėdsake esanti informacija gali būti naudojama išsamiam jūsų profiliui, įskaitant jūsų interesus, įpročius ir elgseną, sukurti. Labai svarbu apsvarstyti, kas gali gauti prieigą prie šios informacijos, ir suprasti, kad net ir nustačius griežtus privatumo nustatymus visada yra galimybė, kad turinys bus nukopijuotas ir juo bus dalijamasi ne tik jūsų numatytoje auditorijoje.

Iš esmės, skaitmeninio pėdsako valdymas reiškia, kad reikia žinoti, kokį pėdsaką paliekate internete, ir imtis priemonių, kad jis tiksliai atspindėtų jūsų ketinimus ir vertybes. Tai reiškia, kad reikia atkreipti dėmesį į turinį, kuriuo dalijatės, išmanyti privatumo nustatymus ir atsargiai vertinti galimas ilgalaikes savo veiksmų internete pasekmes.



Co-funded by
the European Union



SKAITMENINIS PĖDSAKAS

Šiuolaikiniame skaitmeniniame amžiuje labai svarbu valdyti savo skaitmeninį pėdsaką, nes veikla internete gali turėti ilgalaikį poveikį jūsų asmeniniam ir profesiniam gyvenimui. Pateikiame keletą patarimų, kurie padės veiksmingai valdyti skaitmeninį pėdsaką:

1. Būkite atidūs tam, kuo dalijatės: Pagalvokite prieš skelbdami informaciją. Apsvarstykite galimas dalijimosi asmenine informacija, nuotraukomis ar nuomonėmis internete pasekmes. Atminkite, kad kartą ką nors paskelbus, gali būti sunku tai visiškai pašalinti.

2. Naudokitės privatumo nustatymais: Susipažinkite su privatumo nustatymais socialinės žiniasklaidos platformose ir kitose internetinėse paslaugose. Sureguliuokite šiuos nustatymus, kad galėtumėte kontroliuoti, kas gali matyti jūsų įrašus ir informaciją.

3. Reguliariai peržiūrėkite savo buvimą internete: Periodiškai peržiūrėkite savo socialinės žiniasklaidos profilius ir internetines paskyras. Pašalinkite arba atnaujinkite bet kokią pasenusią ar nereikšmingą informaciją.

4. Apribokite asmeninę informaciją: Venkite internete dalytis slapta asmenine informacija, pavyzdžiui, savo adresu, telefono numeriu ar finansine informacija.

5. Naudokite stiprius slaptažodžius: Naudokite stiprius, unikalius savo internetinių paskyrų slaptažodžius, kad išvengtumėte neteisėtos prieigos. Apsvarstykite galimybę naudoti slaptažodžių tvarkyklę, kad galėtumėte saugiai sekti slaptažodžius.

6. Būkite atsargūs, ką spaudžiate: Saugokitės sukčiavimo apgaulės ir kenkėjiškų nuorodų. Venkite spausiti nuorodas ar atsisiųsti priedus iš nežinomų ar įtartinų šaltinių.

7. Stebėkite savo reputaciją internete: Naudokitės paieškos sistemomis ir reguliariai tikrinkite, kokia informacija apie jus prieinama internete. Radę netikslios ar žalingos informacijos, imkitės priemonių jai pašalinti.

8. Švieskite save ir kitus: Būkite informuoti apie geriausią interneto saugumo ir privatumo užtikrinimo praktiką. Švieskite savo draugus ir šeimos narius apie tai, kaip svarbu valdyti savo skaitmeninį pėdsaką.

Laikydami šiuos patarimus galite veiksmingai valdyti savo skaitmeninį pėdsaką ir apsaugoti savo reputaciją internete. Atminkite, kad jūsų buvimas internete atspindi jus pačius, todėl labai svarbu kontroliuoti, kuo dalijatės ir kaip save pristatote internete.



Co-funded by
the European Union

PRIVATUMAS INTERNETE

Interneto privatumas, dar vadinamas interneto privatumu arba skaitmeniniu privatumu, yra tai, kiek asmeninė, finansinė ir naršymo informacija išlieka konfidenciali, kai asmuo yra internete. Didėjant asmeninių duomenų, kuriais dalijamasi ir kurie saugomi internete, kiekiui, susirūpinimas dėl privatumo internete labai išaugo.

Interneto privatumo apsauga yra labai svarbi dėl kelių priežasčių. Pirma, asmenys turi teisę saugoti savo asmeninio gyvenimo duomenis ir nesidalyti jais su nepažįstamais asmenimis. Be to, gali būti sudėtinga žinoti, kokią asmeninę informaciją renka ir kas ją renka, nes vienos įmonės surinkti duomenys gali būti perduoti kitoms įmonėms be jūsų žinios ar sutikimo.

Duomenų privatumas internete turėtų būti vertinamas taip pat svarbiai, kaip ir privatumas fiziniame pasaulyje. Lygiai taip pat, kaip konfidencialų pokalbį vestumėte už uždarytų durų arba finansiniais duomenimis dalytumėtės tik su banku, turėtumėte imtis priemonių, kad apsaugotumėte savo privatumą internete. Tai apima stiprių, unikalių slaptažodžių naudojimą, atsargumą dėl informacijos, kuria dalijatės internete, ir reguliarią privatumo nustatymų peržiūrą socialinėje žiniasklaidoje ir kitose interneto platformose.

Vertindami ir saugodami savo privatumą internete, galite sumažinti riziką, kad jūsų asmeninė informacija bus netinkamai panaudota arba ja bus dalijamasi be jūsų sutikimo.



Co-funded by
the European Union

DUOMENŲ PRIVATUMAS

Duomenų privatumas yra pagrindinė teisė, kuriai skiriama daug dėmesio, ypač Europos Sąjungoje įgyvendinus Bendrąjį duomenų apsaugos reglamentą (BDAR). 2018 m. įsigaliojęs BDAR buvo sukurtas siekiant apsaugoti kiekvieno ES piliečio privatumą ir duomenis, nustatant griežtas asmens duomenų rinkimo, tvarkymo ir saugojimo taisykles.

BDAR sudaro 99 straipsniai, kuriuose išdėstyti įvairūs duomenų apsaugos aspektai. Kai kurios pagrindinės nuostatos yra šios:

1. Teisė susipažinti su duomenimis: asmenys turi teisę žinoti, kokius duomenis apie juos įmonė saugo ir kaip jie naudojami.
2. Teisė į duomenų ištrynimą, dar vadinama "teise būti pamirštam": tam tikromis aplinkybėmis asmenys gali prašyti ištrinti savo asmens duomenis.
3. Sutikimas: prieš rinkdamos arba tvarkydamos asmens duomenis, įmonės turi gauti aiškų asmenų sutikimą. Tai apima aiškų ir nedviprasmišką sutikimą dėl slapukų ir naršymo istorijos.
4. Duomenų kiekio mažinimas: įmonės turėtų rinkti ir tvarkyti tik tuos duomenis, kurie yra būtini tam tikslui, kuriam jie buvo surinkti.
5. Duomenų perkeliamumas: asmenys turi teisę gauti savo asmens duomenis iš bendrovės įprastai naudojamu ir kompiuterio skaitomu formatu.
6. Duomenų apsaugos pareigūnai: kai kurios organizacijos privalo paskirti duomenų apsaugos pareigūną, kuris prižiūrėtų, kaip laikomasi BDAR.

BDAR padarė didelę įtaką tam, kaip įmonės tvarko asmens duomenis, reikalaujamas, kad jos įgyvendintų griežtesnes duomenų apsaugos priemones ir užtikrintų didesnę duomenų tvarkymo praktikos skaidrumą. Bendrasis duomenų apsaugos reglamentas padėjo sustiprinti teises į duomenų privatumą ir suteikti asmenims daugiau galimybių kontroliuoti savo asmeninę informaciją.



Co-funded by
the European Union

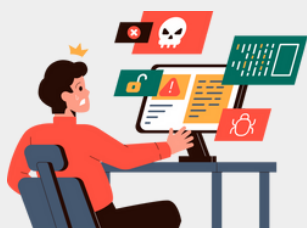
GRĖSMĖS IR PAVOJAI INTERNETE

Kibernetinės grėsmės - tai kenkėjiška veikla, kuria siekiama sugadinti duomenis, pavogti informaciją arba sutrikdyti skaitmenines operacijas. Šios grėsmės apima platų veiksmų spektrą, įskaitant kibernetines atakas, nukreiptas prieš informacinių technologijų turtą, kompiuterių tinklus, intelektinę nuosavybę ir neskelbtinus duomenis. Kibernetinės grėsmės gali kilti tiek iš vidaus, tiek iš išorės šaltinių.

Vidinės grėsmės gali kilti dėl patikimų organizacijos naudotojų, kurie piktnaudžiauja savo privilegijomis arba prieiga prie neskelbtinos informacijos. Kita vertus, išorinės grėsmės kyla iš nutolusių vietovių ir jas dažnai sukelia nežinomos šalys, siekiančios pasinaudoti skaitmeninių sistemų pažeidžiamumu.

Kibernetinių grėsmių pavyzdžiai - kenkėjiškos programos, išpirkos reikalaujanti programinė įranga, sukčiavimo atakos ir atsisakymo aptarnauti (DoS) atakos. Šios grėsmės gali turėti rimtų pasekmių, įskaitant finansinius nuostolius, duomenų saugumo pažeidimus ir žalą organizacijos reputacijai.

Norėdamos apsisaugoti nuo kibernetinių grėsmių, organizacijos ir pavieniai asmenys turi įgyvendinti patikimas kibernetinio saugumo priemones. Tai apima reguliary programinės įrangos atnaujinimą, stiprių slaptažodžių naudojimą, neskelbtinų duomenų šifravimą ir naudotojų švietimą apie galimas grėsmes ir kaip jų išvengti. Be to, daugiafaktorinio autentiškumo patvirtinimo įdiegimas ir reguliarius atsarginių duomenų kopijų darymas gali padėti sumažinti kibernetinės atakos poveikį.



Co-funded by
the European Union

GRĖSMĖS IR PAVOJAI INTERNETE

Interneto pavojus galima apibrėžti kaip viską, kas gali pakenkti interneto naudotojui. Ši žala gali būti įvairių formų (pvz., fizinė, emocinė, psichologinė, finansinė, socialinė ir reputacijos). Toliau pateikiama daug įvairių interneto pavojų rūšių:

Pavojų internete rūšys: Šiandien internete galima rasti beveik viską - nuo pramogų, kredito ir finansinių paslaugų iki produktų iš visų pasaulio kampelių. Nors internetas suteikia tam tikrą anonimiškumo lygį, vis dažniau atsiranda būdų, kuriais gali kilti pavojus naudotojo asmeninei informacijai.

1. Kibernetinės patyčios - tai patyčios, kurios vyksta naudojant skaitmenines technologijas, pavyzdžiui, socialinę žiniasklaidą, žinučių siuntimo platformas, žaidimų platformas ir mobiliuosius telefonus. Jos apima pasikartojantį elgesį, kuriuo siekiama įbauginti, supykdyti ar sugėdinti asmenį, prieš kurį nukreiptos patyčios. Kibernetinių patyčių pavyzdžiai: melo ar gandų apie žmogų skleidimas socialinėje žiniasklaidoje, skaudžių žinučių ar grasinimų siuntimas žinučių programėlėmis, apsimetinėjimas žmogumi, siekiant siųsti piktas žinutes.

Vienas iš pagrindinių skirtumų tarp tiesioginių patyčių ir elektroninių patyčių yra tas, kad elektroninės patyčios palieka skaitmeninį pėdsaką. Tai reiškia, kad egzistuoja patyčių elgesio įrašas, kuris gali būti naudingas kaip įrodymas, padedantis sustabdyti patyčias. Svarbu, kad asmenys žinotų apie savo skaitmeninį pėdsaką ir suprastų, kad jų veiksmai internete gali turėti realių pasekmių.

Siekiant kovoti su elektroninėmis patyčiomis, asmenims būtina pranešti apie bet kokius elektroninių patyčių atvejus atitinkamai platformai arba institucijai. Taip pat svarbu šviesti jaunimą apie atsakingą elgesį internete ir kibernetinių patyčių poveikį. Dirbdami kartu galime sukurti saugesnę internetinę aplinką visiems.



Co-funded by
the European Union

GRĖSMĖS IR PAVOJAI INTERNETE

2. **Kibernetiniai grobuonys** - tai asmuo, paprastai suaugęs, kuris naudojami internetu, kad išnaudotų vaikus ir paauglius įvairioms prievartos formoms, įskaitant seksualinę, emocinę, psichologinę ar finansinę žalą. Šie grobuonys taikosi į pažeidžiamus asmenis įvairiose interneto platformose, pavyzdžiui, pokalbių kambariuose, tiesioginių žinučių siuntimo svetainėse, socialiniuose tinkluose ir vaizdo žaidimuose.

Viena iš įprastų kibernetinių grobuonių naudojamų taktikų - susikurti netikrą tapatybę, apsimetant pačiu vaiku ar paaugliu. Naudodamiesi šia netikra tapatybe, jie užmezga santykius su aukomis, palaipsniui įgyja jų pasitikėjimą ir manipuliuoja, kad jos įsitrauktų į žalingą veiklą.

Įkalbinėjimo procesas yra pagrindinė kibernetinių grobuonių naudojama strategija, kai jie laikui bėgant pamažu manipuliuoja savo aukomis, dažnai pasinaudodami jų pažeidžiamumu ir nesaugumu. Šis procesas gali apimti iš pažiūros nuoširdžios draugystės ar santykių su auka užmezgimą ir tik tada išnaudojimą savo naudai.

Labai svarbu, kad tėvai, globėjai ir pedagogai šviestų vaikus ir paauglius apie saugumą internete ir kibernetinių grobuonių keliamus pavojus. Skatinimas atvirai bendrauti apie bendravimą internete ir ribų nustatymas gali padėti apsaugoti jaunuolius nuo tapimo šių plėšrūnų aukomis. Be to, stebint veiklą internete ir žinant įspėjamuosius požymius galima atpažinti galimą piktnaudžiavimą ir užkirsti jam kelią.



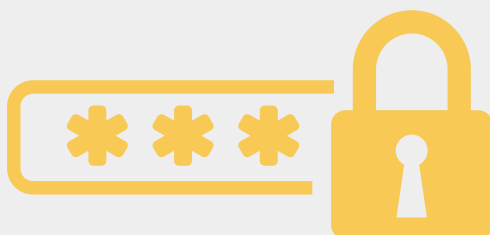
Co-funded by
the European Union

GRĖSMĖS IR PAVOJAI INTERNETE

3. Privačios informacijos skelbimas Vengti dalytis asmenine informacija labai svarbu norint apsaugoti duomenis, išvengti tapatybės vagystės ir išlikti saugiams internete. Tai svarbu ne tik naršant internete, bet ir naudojantis bei dalijantis informacija socialinės žiniasklaidos platformose.

Asmeninės informacijos, kurią reikėtų saugoti, pavyzdžiai: 1. Vardai : vardas, pavardė ir tėvų vardai. 2. Asmens tapatybės numeriai: socialinio draudimo numeris, vairuotojo pažymėjimo numeris, paso numeris, paciento identifikacinis numeris, mokesčių mokėtojo identifikacinis numeris, kredito sąskaitos numeris arba finansinės sąskaitos numeris. 3. Adresai: gatvės adresas ir el. pašto adresas. 4. Biometriniai duomenys: tinklainės skenavimas, pirštų atspaudai, veido geometrija arba balso parašai. 5. Transporto priemonės identifikavimo arba nuosavybės numeriai. 6. Telefono numeriai. 7. Informacija apie technologinį turtą: žiniasklaidos prieigos kontrolės (MAC) arba interneto protokolo (IP) adresai, susiję su tam tikru asmeniu.

Naudojantis socialine žiniasklaida svarbu nepamiršti, kokia informacija dalijatės. Venkite viešai skelbti asmeninę informaciją, pavyzdžiui, savo vardą, pavardę, adresą ar telefono numerį. Naudokite privatumo nustatymus, kad galėtumėte kontroliuoti, kas gali matyti jūsų įrašus ir informaciją, ir būkite atsargūs priimdami draugų prašymus ar žinutes iš nepažįstamų asmenų. Budriai saugodami savo asmeninę informaciją galite sumažinti tapatybės vagystės ir kitų internetinių grėsmių riziką.



Co-funded by
the European Union

GRĖSMĖS IR PAVOJAI INTERNETE

4. **Fišingas** (sukčiavimo atakos) - tai kibernetinių nusikaltėlių naudojama apgaulinga taktika, kuria siekiama apgaule priversti asmenis pateikti jautrią informaciją, pvz., kredito kortelių numerius ar prisijungimo duomenis. Šios atakos paprastai susijusios su suklastotais pranešimais, pavyzdžiui, el. laiškais ar žinutėmis, kurie atrodo kaip iš teisėtų šaltinių. Sukčiavimo atakų tikslas - pavogti asmeninę informaciją arba įdiegti kenkėjišką programinę įrangą į aukos įrenginį.

Fišingo atakos gali būti įvairių formų, įskaitant el. laiškus, kurie atrodo kaip banko ar populiarios interneto paslaugos. Šiuose el. laiškuose dažnai būna nuorodų, kurias spustelėjus patenkama į suklastotas svetaines, imituojančias teisėtos svetainės išvaizdą. Patekus į suklastotą svetainę, aukų prašoma įvesti savo asmeninę informaciją, kurią vėliau perima kibernetiniai nusikaltėliai.

Nors sukčiavimo atakos tradiciškai siejamos su el. laiškais, dabar kibernetiniai nusikaltėliai taikosi į aukas ir kitais būdais. Tai - tekstinės žinutės, telefono skambučiai, suklastotos programėlės ir socialinės žiniasklaidos viktorinos. Šia taktika siekiama įkalbėti asmenis pateikti savo asmeninę informaciją arba spustelėti kenkėjiškas nuorodas.

Norint apsisaugoti nuo sukčiavimo atakų, svarbu būti atsargiems atidarant elektroninius laiškus ar žinutes iš nežinomų siuntėjų. Patikrinkite el. laiškų autentiškumą tikrindami siuntėjo el. pašto adresą ir venkite spausti nuorodas ar atsisiųsti priedus iš įtartinų šaltinių. Be to, naudokite saugumo programinę įrangą ir nuolat ją atnaujinkite, kad galėtumėte aptikti sukčiavimo atakas ir užkirsti joms kelią.



Co-funded by
the European Union

GRĖSMĖS IR PAVOJAI INTERNETE

5. **Patekimas į sukčių rankas** - internetiniai sukčiai tai kibernetinių nusikaltėlių internete vykdomos sukčiavimo schemos. Šios apgavystės gali būti įvairių formų ir skirtos apgauti asmenis, kad šie pateiktų konfidencialią informaciją arba pinigus. Internetinės apgaulės gali būti vykdomos įvairiais kanalais, įskaitant apgaulingus el. laiškus, socialinę žiniasklaidą, SMS žinutes, netikrus techninės pagalbos skambučius ir gąsdinančias programas. Pagrindinis internetinių sukčių tikslas dažniausiai yra pavogti asmeninę informaciją, pavyzdžiui, kredito kortelės duomenis ar prisijungimo duomenis, arba apgaule priversti asmenis siųsti pinigus sukčiui. Kai kurie dažniausiai pasitaikantys interneto sukčiavimo būdai yra šie:

1. Sukčiavimo el. laiškais: iš tikrųjų, tai yra bandymas apgaule išvilioti asmenis, kad jie pateiktų asmeninę informaciją arba paspaustų kenkėjiškas nuorodas.

2. Sukčiavimai socialinėje žiniasklaidoje: sukčiavimai, vykstantys socialinės žiniasklaidos platformose, pavyzdžiui, suklastoti profiliai arba skelbimai, kurie veda į sukčiavimo svetaines arba kenkėjiškų programų atsisiuntimus.

3. SMS sukčiavimai: sukčiavimai, siunčiami SMS žinutėmis, kuriose dažnai pateikiamos nuorodos į netikras svetaines arba prašoma pateikti asmeninę informaciją.

4. Suklastoti techninės pagalbos skambučiai: sukčiai, prisistatantys techninės pagalbos atstovais, kurie bando įtikinti asmenis, kad jų kompiuteryje yra problema, ir prašo sumokėti arba suteikti prieigą prie kompiuterio, kad galėtų "išspręsti" problemą.

5. Scareware - tai suklastota programinė įranga arba iššokantys pranešimai, kuriuose teigiama, kad kompiuteris užkrėstas virusu, ir vartotojas raginamas įsigyti nereikalingą programinę įrangą ar paslaugas.

Norint apsisaugoti nuo internetinių sukčių, svarbu būti atsargiems, kai gaunate nepageidaujamas žinutes ar prašymus pateikti asmeninę informaciją. Prieš pateikdami bet kokią informaciją ar spustelėdami nuorodas, patikrinkite siuntėjo ar organizacijos teisėtumą. Be to, naudokite atnaujintą saugumo programinę įrangą, kuri padės aptikti sukčiavimo atvejus ir užkirsti jiems kelią.



Co-funded by
the European Union

GRĖSMĖS IR PAVOJAI INTERNETE

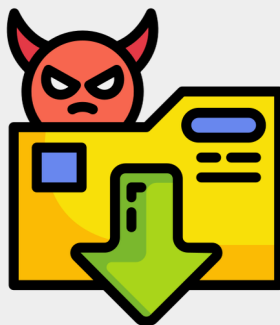
6. **Atsitiktinis kenkėjiškų programų atsisiuntimas** - netyčinis kenkėjiškos programinės įrangos atsisiuntimas yra dažna kompiuterių saugumo grėsmė, galinti turėti rimtų pasekmių. Kenkėjiška programinė įranga apima virusus, Trojos arklius ir kitas kenksmingas programas, skirtas kompiuterio sistemai sugadinti arba sutrikdyti jos veikimą.

Kompiuterinis virusas - tai kenkėjiškos programinės įrangos rūšis, galinti save dauginti ir plisti į kitus kompiuterius. Ji gali pakeisti jūsų kompiuterio veikimą, dažnai be jūsų žinios ar leidimo, ir gali sukelti įvairių problemų - nuo nedidelių nemalonumų iki rimtos žalos.

Norint išvengti atsitiktinio kenkėjiškų programų atsisiuntimo, svarbu būti atsargiems atsisiunčiant programinę įrangą iš interneto. Atidžiai įvertinkite nemokamą programinę įrangą ir venkite atsisiuntimo iš tarpusavio dalijimosi failais svetainių, nes tai dažni kenkėjiškų programų šaltiniai. Be to, būkite atsargūs dėl laiškų iš nežinomų siuntėjų, nes juose gali būti kenkėjiškų priedų arba nuorodų.

Daugumoje dabartinių interneto naršyklių yra integruotų saugumo nustatymų, kurie gali padėti apsaugoti nuo internetinių grėsmių. Svarbu nuolat atnaujinti šiuos nustatymus ir įjungti papildomas saugumo funkcijas, pavyzdžiui, iššokančiųjų langų blokatorius ir kovos su kenkėjiška veikla priemonės.

Tačiau veiksmingiausias būdas apsaugoti nuo virusų ir kitų kenkėjiškų programų - naudoti atnaujintą patikimo tiekėjo antivirusinę programinę įrangą. Antivirusinė programinė įranga gali padėti aptikti ir pašalinti kenkėjiškas programas iš kompiuterio, taip pat realiuoju laiku apsaugoti nuo naujų grėsmių. Reguliariai atnaujindami antivirusinę programinę įrangą ir atlikdami kompiuterio skenavimą, galite apsaugoti savo sistemą nuo kenkėjiškų programų užkrėtimo.



Co-funded by
the European Union

PAGRINDINIAI GEBĖJIMAI UŽTIKRINTI SAUGUMĄ INTERNETE

Saugumas internete - tai bendras žodis, kuriuo siekiama užtikrinti vaikų, jaunuolių ir pažeidžiamų šeimos narių saugumą naudojantis bet koku prie interneto prijungtu įrenginiu. Interneto pasaulis gali įvairiais būdais praturtinti vaikų ir paauglių gyvenimą tiek asmeniniu, tiek edukaciniu požiūriu. Svarbu apibendrinti pagrindinius gebėjimus besimokantiems saugiai elgtis internete:

a) Atpažinti riziką: norint išlikti saugiam internete, labai svarbu atpažinti veiklos internete riziką. Nustatydami galimas grėsmes ir pavojus, asmenys gali imtis aktyvių veiksmų, kad sumažintų poveikį internete ir apsisaugotų nuo žalos.

Pirmiausia, svarbu laikytis prevencinio požiūrio į saugumą internete. Tai reiškia, kad reikia žinoti apie galimus pavojus ir imtis veiksmų jiems sumažinti, kol jie dar netapo problema. Būdami informuoti apie dažniausiai pasitaikančias interneto grėsmes, pavyzdžiui, sukčiavimą, kenkėjiškas programas ir tapatybės vagystes, asmenys gali geriau apsisaugoti nuo šių pavojų.

Kitas svarbus saugaus buvimo internete aspektas - poveikio internete mažinimas. Tai gali būti asmeninės informacijos, kuria dalijamasi socialiniuose tinkluose ir kitose svetainėse, ribojimas, privatumo nustatymų naudojimas, siekiant kontroliuoti, kas gali matyti jūsų informaciją, ir atsargumas spaudžiant nuorodas ar atsisieniūčiant priedus iš nežinomų šaltinių.

Norint išlikti saugiam skaitmeniniame pasaulyje, labai svarbu suvokti veiklos internete riziką ir imtis aktyvių veiksmų jai sumažinti. Būdami informuoti ir iniciatyvūs, asmenys gali apsisaugoti nuo internetinių grėsmių ir saugiau naudotis internetu.



Co-funded by
the European Union

PAGRINDINIAI GEBĖJIMAI UŽTIKRINTI SAUGUMĄ INTERNETE

b) Asmeninės informacijos saugojimas:

Siekiant užtikrinti saugų buvimą internete, labai svarbu saugoti asmeninę informaciją. Kad apsaugotumėte savo tapatybę ir užtikrintumėte saugų skaitmeninį gyvenimą sau ir savo šeimai, svarbu laikytis tam tikrų gairių:

1. Naudokite stiprius, unikalius slaptažodžius: Slaptažodžiai yra raktai į jūsų skaitmeninius namus. Labai svarbu kiekvienai savo paskyrai naudoti stiprius, unikalius slaptažodžius ir vengti lengvai atspėjamų slaptažodžių. Apsvarstykite galimybę naudoti patikimą slaptažodžių tvarkyklę, kad galėtumėte saugiai kurti ir saugoti sudėtingus slaptažodžius.
2. Niekada su niekuo nesidalykite slaptažodžiais, net su patikimais asmenimis. Dalijimasis slaptažodžiais gali pakenkti jūsų paskyrų ir asmeninės informacijos saugumui.
3. Reguliariai darykite atsargines svarbių duomenų kopijas, kad apsaugotumėte juos nuo praradimo ar vagystės. Tai galima padaryti naudojant išorinius kietuosius diskus, debesijos saugojimo paslaugas ar kitus atsarginių kopijų kūrimo sprendimus. Atsarginių kopijų duomenys turėtų būti užšifruoti ir saugiai laikomi.
4. Užtikrinkite, kad visa jūsų įrenginiuose esanti programinė įranga, įskaitant operacines sistemas, naršykles ir taikomąsias programas, būtų reguliariai atnaujinama naudojant naujausias saugumo pataisas ir atnaujinimus. Tai padeda apsisaugoti nuo pažeidžiamumų, kuriais gali pasinaudoti kibernetiniai nusikaltėliai.
5. Naudokite saugumo programinę įrangą. Įdiekite ir reguliariai atnaujinkite patikimą antivirusinę ir antivirusinę programinę įrangą savo įrenginiuose, kad apsisaugotumėte nuo virusų, kenkėjiškų programų ir kitų internetinių grėsmių.
6. Įjunkite dviejų veiksmų autentifikavimą (2FA): jei įmanoma, savo paskyrose įjunkite 2FA, kad užtikrintumėte papildomą saugumo lygį. Tam reikia ne tik slaptažodžio, bet ir antros patvirtinimo formos, pavyzdžiui, į telefoną atsiųsto kodo.

Laikydamiesi šių rekomendacijų, galite apsaugoti savo asmeninę informaciją ir užtikrinti saugesnį savo ir savo šeimos narių naudojimąsi internetu.



Co-funded by
the European Union

PAGRINDINIAI GEBĖJIMAI UŽTIKRINTI SAUGUMĄ INTERNETE

c) Neatsisiųskite nežinomų failų: Atsisiunčiant nežinomus failus, jūsų kompiuteriui ir asmeninei informacijai gali kilti įvairių pavojų, įskaitant kenkėjiškas programas, virusus ir kitą kenkėjišką programinę įrangą. Norint apsaugoti save ir savo įrenginius, svarbu laikytis šių rekomendacijų:

1. Būkite atsargūs su el. laiškų priedais. Neatsisiųskite priedų iš nežinomų ar įtartinių el. laiškų. Šiuose prieduose gali būti kenkėjiškų programų, kurios gali pakenkti jūsų kompiuteriui arba pavogti jūsų asmeninę informaciją.

2. Prieš atsisiunčiant bet kokį failą, patikrinkite šaltinį, kad įsitikintumėte, jog jis yra teisėtas. Atsisiųskite failus tik iš patikimų svetainių ir šaltinių.

3. Įdiekite ir reguliariai atnaujinkite antivirusinę programinę įrangą savo kompiuteryje. Ši programinė įranga gali padėti aptikti ir pašalinti kenkėjišką programinę įrangą iš atsisiųstų failų.

4. Įgalinkite failų plėtinių naudojimą: operacinėje sistemoje įjunkite failų plėtinius, kad galėtumėte matyti visą failo pavadinimą. Tai gali padėti nustatyti galimai kenkėjiškus failus.

5. Venkite P2P (peer-to-peer) dalijimosi failais. Būkite atsargūs naudodamiesi P2P dalijimosi failais paslaugomis, nes dėl jų galite susidurti su kenkėjiškomis programomis ir kitais pavojais. Atsisiųskite failus tik iš patikimų šaltinių.

6. Prieš atidarydami atsisiųstus failus, naudokite antivirusinę programinę įrangą. Tai gali padėti aptikti bet kokią faile esančią kenkėjišką programinę įrangą ar virusus.

Laikydami šias rekomendacijas galite sumažinti nežinomų failų atsisiuntimo riziką ir apsaugoti savo kompiuterį bei asmeninę informaciją nuo internetinių grėsmių.



Co-funded by
the European Union



PAGRINDINIAI GEBĖJIMAI UŽTIKRINTI SAUGUMĄ INTERNETE

d) Naudoti kritinio mąstymo įgūdžius analizuojant ir vertinant informaciją internete; Norint apsisaugoti nuo sukčių, sukčiavimo ir dezinformacijos, labai svarbu naudotis kritinio mąstymo įgūdžiais analizuojant ir vertinant informaciją internete. Štai keletas rekomendacijų, padėsiančių jums išlikti saugiams:

1. Būkite skeptiški, kvestionuokite informacijos, su kuria susiduriate internete, šaltinį ir pagrįstumą. Jei kas nors atrodo pernelyg gerai, kad būtų tiesa, arba atrodo ne visai teisinga, prieš imdamiesi kokių nors veiksmų, geriau pasidomėkite išsamiau.

2. Tikrinkite, ar nėra rašybos klaidų ir įtartinų el. pašto adresų. Būkite atsargūs dėl el. laiškų, žinučių ar svetainių, kuriose yra rašybos klaidų arba naudojami neteisėti el. pašto adresai. Tai gali būti bandymų sukčiauti arba sukčiavimo požymiai.

3. Prieš spustelėdami bet kokias nuorodas ar atsisiųsdami priedus, patikrinkite informacijos šaltinį. Ieškokite oficialių svetainių arba patikimų šaltinių, kad įsitikintumėte, jog informacija yra teisėta.

4. Pagalvokite prieš paspausdami. Venkite spausti nuorodas ar priedus, esančius elektroniniuose laiškuose ar pranešimuose iš nežinomų ar įtartinų šaltinių. Prieš spustelėdami užveskite pelės žymeklį ant nuorodų, kad pamatytumėte tikrąjį URL adresą.

5. Būkite atsargūs dėl netikėtų pranešimų: jei iš draugo ar pažįstamo gaunate pranešimą, kuris atrodo neįprastas ar netikėtas, prieš imdamiesi bet kokių veiksmų patikrinkite šaltinį. Gali būti, kad į jį paskyrą buvo įsilaužta.

6. Naudokitės saugumo programine įranga. Įdiekite ir reguliariai atnaujinkite antivirusinę programinę įrangą savo įrenginiuose. Tai gali padėti aptikti kenkėjišką programinę įrangą ir neleisti jai užkrėsti jūsų įrenginio.

Naudodami kritinio mąstymo įgūdžius ir laikydamiesi šių rekomendacijų, galite apsisaugoti nuo internetinių grėsmių ir dezinformacijos.



Co-funded by
the European Union

PAGRINDINIAI GEBĖJIMAI UŽTIKRINTI SAUGUMĄ INTERNETE

e) Patikrinkite, ar svetainė, kurioje esate, yra saugi: Norint apsisaugoti nuo internetinių grėsmių, ypač kai įvedate slapta informaciją, pavyzdžiui, mokėjimo duomenis, labai svarbu patikrinti, ar svetainė yra saugi. Štai keli žingsniai, kaip patikrinti svetainės saugumą:

1. Patikrinkite interneto svetainės URL. Peržiūrėkite svetainės URL ir įsitikinkite, kad jis prasideda "https://", o ne tik "http://". "s" reiškia "secure" (saugus) ir rodo, kad svetainė turi SSL sertifikatą, kuriuo šifruojami tarp jūsų naršyklės ir svetainės perduodami duomenys.

2. Ieškokite pakabinamos spynos piktogramos: patikrinkite, ar adreso juostoje šalia URL adreso yra pakabinamos spynos piktograma. Tai rodo, kad svetainė yra saugi ir naudoja HTTPS šifravimą.

3. Patikrinkite svetainės teisėtumą: prieš įvesdami bet kokią asmeninę ar mokėjimo informaciją, patikrinkite svetainės teisėtumą. Ieškokite kontaktinės informacijos, pavyzdžiui, fizinio adreso ir telefono numerio, ir patikrinkite kitų naudotojų atsiliepimus ar vertinimus.

4. Naudokite saugų mokėjimo būdą: pirkdami internetu, naudokite saugų mokėjimo būdą, pavyzdžiui, "PayPal" arba kredito kortelę, kuris užtikrina pirkėjo apsaugą. Venkite naudoti debetines korteles ar banko pavedimus, nes jie mažiau apsaugo nuo sukčiavimo.

5. Naudokite aukšto saugumo lygio naršyklę: apsvarstykite galimybę naudoti naršyklę, kuri siūlo papildomas saugumo funkcijas, pavyzdžiui, integruotą apsaugą nuo sukčiavimo ir kenkėjiškų programų. Kai kurios naršyklės taip pat rodo žalią adreso juostą arba kitus rodiklius, rodančius, kad svetainė yra saugi.

6. Atnaujinkite naršyklę ir saugumo programinę įrangą, kad apsisaugotumėte nuo naujausių grėsmių ir pažeidžiamumų.

Laikydami šias rekomendacijas galite padėti užtikrinti, kad jūsų lankomos svetainės būtų saugios, ir apsisaugoti nuo internetinių grėsmių apsipirkdami ar naršydami internete.

f) Žinokite apie savo skaitmeninį pėdsaką. Kartą prisijungę, visada prisijungę: viskas, kas paskelbta internete, yra visiems matoma, todėl būtina atsargiai elgtis su socialinio tinklo profiliuose naudojama identifikuojama informacija ir svetainėmis, kuriose lankomasi, registruojamasi ar kuriose saugoma bet kokio tipo naudotojo asmeninė informacija.



Co-funded by
the European Union



AKTYVIOS INTERNETO SAUGOS PRIEMONĖS IR GAIRĖS

Norint išlikti saugiam internete, labai svarbu laikytis saugesnio mąstymo, nes tai padeda atpažinti galimą riziką ir imtis aktyvių apsaugos priemonių. Štai keletas svarbiausių dalykų, kuriuos reikėtų įsidėmėti:

1. Saugokitės klaidingo saugumo jausmo: nors kompiuteriai gali atrodyti saugūs, jie gali būti pažeidžiami įvairių internetinių grėsmių. Svarbu prisiminti, kad kibernetiniai nusikaltėliai internetu gali padaryti realios žalos, pavyzdžiui, pavogti tapatybę, pridaryti finansinių nuostolių ir sugadinti jūsų įrenginius.

2. Būkite informuoti: domėkitės apie naujausias interneto grėsmes ir geriausią saugumo praktiką. Tai gali padėti atpažinti galimus pavojus ir imtis tinkamų veiksmų, kad apsisaugotumėte.

3. Laikykitės saugumo priemonių: naudokitės pirmiau aptartomis saugos priemonėmis, pavyzdžiui, naudokite stiprius, unikalius slaptažodžius, nuolat atnaujinkite programinę įrangą ir nespauskite įtartinų nuorodų ar priedų.

4. Vadovaukitės sveiku protu: jei bendraujant internete kas nors atrodo per daug gerai, kad būtų tiesa, arba atrodo ne taip, kaip turėtų būti, geriausia būti atsargesniems ir to vengti.

5. Reguliariai darykite atsargines duomenų kopijas, naudokite saugumo programinę įrangą ir atsargiai vertinkite informaciją, kuria dalijatės internete.

6. Būkite budrūs ir stebėkite aplinką internete. Būkite atsargūs dėl neprašytų el. laiškų, žinučių ar prašymų pateikti asmeninę informaciją ir prieš imdamiesi bet kokių veiksmų patikrinkite šaltinį.



Co-funded by
the European Union

AKTYVIOS INTERNETO SAUGOS PRIEMONĖS IR GAIRĖS

Pasitelkiant saugų mąstymą ir laikydamiesi šių rekomendacijų galite apsisaugoti nuo internetinių grėsmių ir saugiau naudotis internetu.

- Sukurkite tvirtesnius slaptažodžius.

Stiprus slaptažodis yra vienas geriausių būdų apsaugoti savo paskyras ir asmeninę informaciją nuo įsilaužėlių.

- Naršyklės saugumo funkcijos:

Naršydami internete kompiuteriai susiduria su įvairiomis grėsmėmis, įskaitant virusus, kenkėjiškas ir šnipinėjimo programas. Gera žinia ta, kad jūsų interneto naršyklėje yra daug integruotų saugumo funkcijų, padedančių apsaugoti kompiuterį.

- Venkite nepageidaujamų laiškų ir fišingo

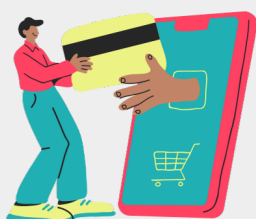
Norint apsisaugoti nuo el. pašto sukčių, kenkėjiškos programinės įrangos ir tapatybės vagysčių, būtina suprasti, kaip atpažinti potencialiai pavojingą turinį ir jo vengti.

- Venkite kenkėjiškos programinės įrangos naudodami antivirusinę programą.

Kenkėjiška programinė įranga yra vienas dažniausių pavojų jūsų kompiuteriui, kai esate prisijungę, tačiau jos lengva išvengti, pagrindai - apsaugoti kompiuterį ir išmokti atpažinti ir vengti įtartinų nuorodų.

- Saugus apsipirkimas internetu

Apsipirkimas internetu yra patogus būdas pirkti patogiai įsitačius namuose. Ir nors yra daug privalumų, yra ir tam tikros rizikos. Yra būdų, kaip apsisaugoti ir užtikrinti savo finansinių duomenų saugumą, pavyzdžiui, patikrinti svetainės saugumą ir tikrumą.



Co-funded by
the European Union

TĖVŲ KONTROLĖS PRIEMONĖS

Tėvų kontrolės priemonės yra esminė priemonė jūsų vaiko saugumui internete užtikrinti. Štai keletas svarbiausių dalykų, į kuriuos reikėtų atkreipti dėmesį:

1. Turinio filtravimas: tėvų kontrolės priemonės leidžia filtruoti turinį, kurį jūsų vaikas gali pasiekti internete, blokuojant netinkamas svetaines ir medžiagą.
2. Laiko apribojimai: nustatykite laiko apribojimus vaiko veiklai internete, kad užtikrintumėte, jog jis ten nepraleidžia per daug laiko.
3. Programėlių ir žaidimų kontrolė: kontroliuokite, kokias programėles ir žaidimus jūsų vaikas gali atsisiųsti ir pasiekti, užtikrindami, kad jie būtų tinkami jo amžiui.
4. Privatumo nustatymai: užtikrinkite, kad vaiko privatumo nustatymai būtų tinkamai sukonfigūruoti ir apsaugotų jo asmeninę informaciją.
5. Stebėjimas ir sekimas: kai kurios tėvų kontrolės priemonės leidžia stebėti vaiko veiklą internete ir sekti jo buvimo vietą.
6. Švietimas ir bendravimas: svarbu šviesti vaiką apie saugumą internete ir atsakingo naudojimosi internetu svarbą. Skatinkite atvirą bendravimą, kad jie jaustųsi patogiai aptardami bet kokius rūpesčius ar problemas, su kuriomis gali susidurti internete.
7. Reguliariai peržiūrėkite ir atnaujinkite tėvų kontrolės nustatymus, kad įsitikintumėte, jog jie vis dar atitinka jūsų vaiko amžių ir brandos lygį.

Atminkite, kad nors tėvų kontrolės priemonės yra vertinga priemonė, ji nėra pilnai patikima. Labai svarbu taip pat mokyti vaiką kritinio mąstymo įgūdžių ir atsparumo, kad jis galėtų saugiai ir užtikrintai naršyti interneto pasaulyje.



Co-funded by
the European Union

SKIRTINGŲ TIPŲ TĖVŲ KONTROLĖS PRIEMONIŲ SUSKIRSTYMAS

Tėvų kontrolės priemonės siūlo įvairias funkcijas, padedančias tėvams valdyti vaikų veiklą internete. Toliau pateikiame įvairių tipų tėvų kontrolės priemonių funkcijų skirstymą:

1. Filtravimas ir blokavimas: šios funkcijos apriboja prieigą prie tam tikrų svetainių, žodžių ar vaizdų, kurie, tėvų nuomone, yra netinkami. Jos gali padėti apsaugoti vaikus nuo prieigos prie žalingo turinio internete.
2. Išsėtinčio turinio blokavimas: ši funkcija neleidžia vaikams dalytis asmenine informacija internete ir el. paštu, taip padėdama apsaugoti jų privatumą ir saugumą.
3. Laiko ribojimas: tėvai gali nustatyti laiko apribojimus, kiek laiko vaikams leidžiama būti internete ir koku paros metu jie gali naudotis internetu. Tai gali padėti valdyti laiką, praleidžiamą prie ekrano, ir užtikrinti, kad vaikai nesilankytų internete netinkamu laiku.
4. Stebėsenos priemonės: šios priemonės įspėja tėvus apie vaikų veiklą internete neužblokuojant prieigos. Jos gali fiksuoti, kuriose svetainėse vaikas lankėsi, ir rodyti įspėjamuosius pranešimus, kai vaikas lankosi tam tikrose svetainėse. Tai leidžia tėvams būti informuotiems apie savo vaikų elgesį internete.

Svarbu pažymėti, kad nors tėvų kontrolės priemonės gali padėti apsaugoti vaikus internete, jos nepakeičia švietimo, atsakomybės ir suaugusiųjų priežiūros. Tėvai turėtų šviesti savo vaikus apie galimą interneto riziką ir nustatyti taisykles dėl tinkamų ir netinkamų svetainių. Atviri ir nuoširdūs pokalbiai su vaikais yra labai svarbūs kuriant saugią interneto aplinką, kurioje jie jaustųsi patogiai ir galėtų aptarti visus rūpimus klausimus ar problemas, su kuriomis gali susidurti internete.



Co-funded by
the European Union

PAGRINDINĖS PRIEŽIŪROS REKOMENDACIJOS TĖVAMS

Tėvų priežiūra yra labai svarbi siekiant užtikrinti vaikų saugumą internete. Štai keletas pagrindinių veiksmingos tėvų priežiūros gairių:

1. Praleiskite laiką internete kartu: mokykite vaikus tinkamo elgesio internete praleisdami su jais laiką internete. Taip galėsite stebėti jų veiklą ir aptarti bet kokią galimą riziką.
2. Kompiuterį padėkite bendroje namų vietoje, pavyzdžiui, svetainėje, kur galėsite lengvai stebėti, kaip juo naudojasi. Venkite statyti kompiuterius atskiruose miegamuosiuose ir stebėkite laiką, praleidžiamą naudojantis išmaniaisiais telefonais ar planšetiniais kompiuteriais.
3. Pažymėkite vaikų mėgstamas svetaines: vaikų mėgstamų svetainių žymėjimas, kad jas būtų galima lengvai pasiekti, padeda jiems saugiai naršyti internete ir sumažina riziką pasiekti netinkamą turinį.
4. Reguliariai tikrinkite finansines sąskaitas, kortelių išrašus ir telefono sąskaitas, ar jose nėra nepažįstamų mokesčių, kurie gali reikšti neleistinus pirkinius internete.
5. Pasiteiraukite apie apsaugą internete: sužinokite, kokios apsaugos internete priemonės taikomos jūsų vaiko mokykloje, popamokinio ugdymo centre, draugų namuose ar bet kurioje kitoje vietoje, kur vaikai gali naudotis kompiuteriu be priežiūros.
6. Rimtai žiūrėkite į pranešimus: jei jūsų vaikas praneša apie nemalonius internetinius mainus ar incidentą, žiūrėkite į tai rimtai ir nedelsdami ištyrkite problemą. Skatinkite atvirą bendravimą, kad jūsų vaikas jaustųsi patogiai aptardamas bet kokius jam rūpimus klausimus.



Co-funded by
the European Union

PAGRINDINĖS PRIEŽIŪROS REKOMENDACIJOS TĖVAMS

Jungtinės Karalystės saugesnio interneto centro direktorius Willas Gardneris pateikė naudingos informacijos tėvams ar globėjams, kurie nori valdyti savo vaikų ir šeimos santykius su internetu. Paimta iš: <https://inews.co.uk/news/technology/tips-and-guidance-for-children-and-parents-for-staying-safe-online-254485>.

- Pasiteiraukite savo šeimos narių (ypač vaikų), kaip internetas juos verčia jaustis:

"Reguliariai kalbėkitės su vaiku apie tai, kaip jis naudoja technologijas, ir išsiaiškinkite, koks yra jo skaitmeninis gyvenimas, įskaitant tai, kokios yra jo mėgstamiausios svetainės ir paslaugos, taip pat kaip jis jaučiasi būdamas internete. Išlausę savo vaiką, galėsite geriausiai suprasti, kaip galite jam padėti."

- Užversti vaikus apribojimais nepadedą:

"Natūralu, kad kaip tėvai jaučiate nerimą dėl rizikos, kurią kelia jūsų vaiko buvimas internete, tačiau jauniems žmonėms interneto pasaulis yra įdomus ir smagus, nes jis suteikia jiems daugybę galimybių." "Atminkite, kad jūsų vaikas technologijas ir internetą naudos skirtingai, atsižvelgiant į tai, kad jis auga pasaulyje, panirusiame į visus skaitmeninius dalykus. Stenkitės įvertinti tiek teigiamus, tiek neigiamus buvimo internete aspektus ir suteikite savo vaikui galimybę pasirinkti saugius sprendimus, o ne priblokškite jį apribojimais."

- Susipažinkite su jų naudojamomis programėlėmis ir paslaugomis:

"Galite imtis veiksmų, kad padėtumėte savo vaikui internete, naudodamiesi tokiomis funkcijomis kaip privatumo nustatymai socialinėje žiniasklaidoje ir suprasdami, kaip pateikti pranešimą apie įvairias programėles, žaidimus ir paslaugas."

- Naudokitės turimomis pagalbos priemonėmis:

"Yra daug įrankių, padedančių valdyti jūsų šeimos naudojamus įrenginius. Pavyzdžiui, žinojimas, kaip įjungti ir naudoti tėvų kontrolės priemones, gali padėti apsaugoti vaiką nuo netinkamo turinio internete."



Co-funded by
the European Union

SAUGOS INTERNETE PATIKRA

"Norton Security Centre" teigimu, saugus elgesys internete gali padėti jums ir jūsų šeimai išvengti nepageidaujamos informacijos, medžiagos ar pavojų internete, kurie gali pakenkti jūsų įrenginiams, asmeninei informacijai ar šeimai. Protinga specialiai vaikus mokyti kompiuterinio saugumo, kad jie netaptų kai kurių anksčiau minėtų įprastų pavojų aukomis.

Pateikiame interneto saugos kontrolinį sąrašą, sudarytą remiantis "Norton Security Centre" patarimais:

1. Naudokite stiprius, unikalius slaptažodžius: Užtikrinkite, kad visos paskyros turėtų stiprius, unikalius slaptažodžius, kad būtų apsaugotos nuo neteisėtos prieigos.
2. Nuolat atnaujinkite programinę įrangą: Reguliariai atnaujinkite operacines sistemas, naršykles ir saugumo programinę įrangą, kad apsisaugotumėte nuo pažeidžiamumų.
3. Naudokite saugumo programinę įrangą: Įdiekite patikimą antivirusinę ir kenkėjiškų programų programinę įrangą, kad apsisaugotumėte nuo virusų ir kitų grėsmių.
4. Būkite atsargūs dėl sukčiavimo apgaulės būdu: Saugokitės el. laiškų, žinučių ar interneto svetainių, kuriose prašoma pateikti asmeninę informaciją arba kuriose yra įtartinių nuorodų.
5. Įjunkite dviejų veiksmų autentifikavimą: Įjunkite dviejų veiksmų autentifikavimą paskyrose, kuriose jis siūlomas, kad užtikrintumėte papildomą saugumo lygį.
6. Naudokitės saugiais tinklais: Venkite naudotis viešuoju "Wi-Fi", kai reikia atlikti neskelbtinus veiksmus, ir prireikus naudokitės virtualiuoju privačiu tinklu (VPN).
7. Stebėkite vaikų veiklą internete: Stebėkite vaikų veiklą internete ir švieskite juos apie saugų elgesį internete.
8. Kurkite atsargines svarbių duomenų kopijas: Reguliariai kurkite svarbių duomenų atsargines kopijas, kad apsisaugotumėte nuo duomenų praradimo dėl kenkėjiškos programinės įrangos ar aparatinės įrangos gedimo.
9. Apribokite dalijimąsi asmenine informacija: Būkite atsargūs dalydamiesi asmenine informacija internete ir tai darykite tik saugiose, patikimose svetainėse.
10. Švieskite save ir savo šeimą: Būkite informuoti apie naujausias interneto grėsmes ir mokykite savo šeimą saugaus elgesio internete.



Co-funded by
the European Union

NUORODOS



Internet safety tips and checklist to help families stay safer online. Norton Security Center. Retrieved from: <https://us.norton.com/internetsecurity-kids-safety-stop-stressing-10-internet-safety-rules-to-help-keep-your-family-safe-online.html>

How to protect your privacy online. Norton Security Center (2021) <https://us.norton.com/internetsecurity-privacy-protecting-your-privacy-online.html>

Internet Safety: Avoiding Spam and Phishing. GCFGlobal (2021) Retrieved from: <https://edu.gcfglobal.org/en/internetsafety/avoiding-spam-and-phishing/1/>

Parental controls. Internet matters (2021) <https://www.internetmatters.org/parental-controls/>

The 5 cyber safety tips every parent should know. Norton Security Center. Retrieved from: <https://us.norton.com/internetsecurity-kids-safety-5-cybersafety-tips-every-parent-should-know.html>

What are web threats? Kaspersky (2021) Retrieved from: <https://thebossmagazine.com/internet-safety-tips/>

What is a digital footprint? netsafe (2021) <https://www.netsafe.org.nz/digital-footprint/>

What is Online Safety? National Online Safety (2021) Retrieved from: <https://nationalonlinesafety.com/wakeupwednesday/what-is-online-safety>

The dangers of sharing personal information on social media.

Patel, D., May 2020, PennToday. Retrieved from: <https://penntoday.upenn.edu/news/dangers-sharing-personal-information-social-media>

STEGNER, Ben. (2017) The complete guide to parental controls. MUO: Technology explained. Retrieved from: <https://www.makeuseof.com/tag/guide-parental-controls/>

Staying safe online: guidelines for parents and teens

<https://inews.co.uk/news/technology/tips-and-guidance-for-children-and-parents-for-staying-safe-online-254485>

How to protect your private information online. UK Norton Security Centre <https://uk.norton.com/internetsecurity-how-to-8-ways-to-protect-your-private-information-online.html>