Interneto grėsmės vaikams

Patarimai tėvams ir mokytojams

Turinys

Šis projektas finansuojamas remiant Europos Komisijai.

Šis leidinys atspindi tik autoriaus požiūrį, todėl Europos Komisija negali būti laikoma atsakinga už bet kokį jame pateikiamos informacijos naudojimą.

Sudarytoja
Laima PAULAUSKIENĖ

Redakcinė kolegija
Alvita ARMANAVIČIENĖ, Rytis RAINYS (Lietuva), Nikolov BOGOMIL (Bulgarija)
Gražina ROKICKA (Lenkija), Božena STAŠENKOVA (Slovakija)

Išleido LĮ „KRIVENTA“
Tel./faks. +370 5 265 06 29, el. p. kriventa@takas.lt

Įvadas

Paskutiniaisiais metais vis daugiau naudojamasi internetu. Sparčiausiai augančią interneto vartotojų grupę sudaro vaikai ir paaugliai. Milžiniškas informacijos kiekis, pasiekiamas internetu, jaunajai kartai yra neįkainojama vertybė. Ši jaunų žmonių karta vienu pelės spragtelėjimu suranda visus reikalingus atsakymus į juos dominančius klausimus. Kita vertus, jau galime pastebėti, kaip penkiametis vaikas nagrinėja interneto svetainių turinį, ir tai tampa kasdienybe. Jaunieji interneto vartotojai dažniausiai dar nepasirengę priimti didelę informacijos įvairovę virtualioje erdvėje – nuo filmų, vaizdajuosčių iki vaikų pornografijos ir pedofilijos.

Internetinė grėsmė kyla vaikų ir jaunimo saugumui. Šios grėsmės šalinimas – pagrindinė problema kuriant informacinę visuomenę. Ypač svarbu tai, kad tėvai ir atsakingi valdžios žmonės, vykdantys įstatymų priežiūrą, laiku išaiškintų skriaudikus ir juos aptarnaujančius informacijos tiekėjus, žinotų maksimalų internetinės grėsmės laipsnį vaikams ir paaugliams, ir atsakingai veikdami galėtų apsaugoti vaikus nuo internetinės grėsmės ir persekiojimo.

Jeigu norime tinkamai apsaugoti vaikus nuo internetinės grėsmės, turime kurti mokomąsias programas tėvams. Internetinės prieigos turi būti saugios ir patikimos.

Iš Baltijos šalių Lietuvoje yra mažiausia interneto vartotojų. Apie 2002 m. vidurį internetu naudojosi tik 21 proc. gyventojų. Per paskutiniuosius trejus metus bendras namų interneto vartotojų skaičius kiekvienais metais padvigubėdavo. Paskutiniuoju metu Lietuvoje yra daugiau kaip 986 tūkst. interneto vartotojų.

Statistikos departamento duomenimis, Lietuvoje 2006 m. 32 proc. namų ūkių turėjo kompiuterius, o reguliariai internetu besinaudojančių žmonių skaičius iki 2006 m. spalio mėnesio pasiekė 1,4 mln. Lyginant su ankstesniais statistiniais duomenimis, kasmet internetu besinaudojančių asmenų skaičius šalyje padidėja apytikriai du kartus. Šis rodiklis šiuo metu yra vienas aukščiausių Europoje.

Deja, kartu su socialiniais visuomenės santykiais į elektroninę erdvę persikėlė ir nusikalstamos veiklos. Tyrimai rodo, kad vis dažniau elektroninių ryšių naudotojai susiduria su konfidencialių duomenų vagystėmis internete (angl. *phishing*), įsilaužimais į informacines sistemas, kompiuteriniais virusais, nepageidaujamo elektroninio pašto (angl. *spam*) srauto didėjimu, atsisakymo aptarnauti atakomis (angl. *Denial of Service, DoS*) bei kitomis tinklų ir informacijos saugumo problemomis.

Lietuvos Respublikos ryšių reguliavimo tarnyba (RRT) nuo 2005 m. atlieka išsamius tinklų ir informacijos saugumo padėties Lietuvoje tyrimus. Šiais tyrimais siekiama išsiaiškinti, kokių saugumo incidentų dažniausiai kyla ir kokiu mastu tai vyksta. Tyrimas parodė, kad didžioji dalis visų naudotojų susiduria su kompiuteriniais virusais ir *spam*.

Įvertinus tai, kad per 20 kompiuterinių virusų gyvavimo metų jų buvo sukurta apie 150 tūkst., ir tai, kad *spam* šiuo metu užima apie 60 proc. viso elektroninio pašto srauto, tokie rezultatai nėra netikėti. Tačiau, lyginant su 2005 m. duomenimis, šiemet daugiau įmonių nuolat susiduria su šiuo reiškiniu, o 43 proc. informacinių paslaugų tiekėjų (IPT) tenka kovoti su DoS atakomis prieš tarnybines stotis ir kompiuterius. Šios atakos potencialiai turi didesnį destrukcinį poveikį negu kiti incidentai, nes dažnai įvykdomos naudojant *botnet* tinklus.

Tyrimai parodė, kad tėvai žino apie interneto keliamą pavojų ir supranta šios problemos svarbą.

Vyriausybė parengė keletą programų, skatinančių ryšių technologijų plėtrą ir kompiuterinį gyventojų raštingumą. 2000 m. gegužę Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos parengė Lietuvos informacinės visuomenės plėtros strategiją, kurioje buvo numatyti uždaviniai keleriems metams į priekį.

Lietuvoje, panašiai kaip ir kitose pasaulio šalyse, daug daugiau mobiliųjų telefonų su internetu vartotojų. Labai svarbu, kad Lietuvai tapus visateise Europos Sąjungos nare pasirūpinta gyventojų ir ypač vaikų apsauga nuo žalingo interneto turinio. Nepaisant to, kad buvo priimti kai kurie įstatymų papildymai, Lietuvoje ir toliau turi būti įgyvendinamos efektyvios apsaugos priemonės. 2003–2004 m. policija gavo tik vieną nusiskundimą dėl nesaugaus interneto. Pedagogikos ir psichologijos centras prie Lietuvos Respublikos švietimo ir mokslo ministerijos ir *Bitė GSM*, antrasis pagal dydį mobilusis operatorius, vykdo plačią ir tikslinę veiklą. Ja siekiama, kad informacinės ir skaitmeninės technologijos šalyje būtų kuo saugesnės. Jau kuris laikas Lietuvoje veikia interneto tinklalapis **www.draugiskasinternetas.lt.** Tai trijų partnerių – Lietuvos Respublikos švietimo ir mokslo ministerijos, Pedagogikos ir psichologijos centro ir *Bitės GSM* – bendros veiklos rezultatas, kuris sulaukė didelio valstybinių institucijų ir nevyriausybinių organizacijų palaikymo bei aktyvaus jų bendradarbiavimo šioje srityje.

Siekiant suteikti visuomenei kuo platesnės ir aktualesnės informacijos daugeliu tinklų ir informacijos saugumo klausimų, 2005 m. vasario 7 d. pradėjo veikti interneto tinklalapis **www.esaugumas.lt**, kuriame skirtingoms vartotojų grupės (namų vartotojams, įmonėms ir valstybės institucijoms) nuolat pateikiama svarbios informacijos apie grėsmes tinklų ir informacijos saugumui.

Kaip paaiškinsite vaikams apie riziką internete, jeigu patys niekada juo nesinaudojate

Jūs nebūtinai turite būti kompiuterių ekspertas, kad išaiškintumėte saugumo taisykles savo vaikams. Tereikia tik paprastas taisykles, kurias sužinojote iš savo tėvų, pritaikyti interneto naudojimui ir priminti vaikams tai kiekvieną dieną. Tačiau kai kuriuos kasdienio bendravimo ir veiklos reikalavimus turėtumėte ypač pabrėžti, tai:

- nesikalbėti su nepažįstamais ir neimti iš jų dovanų;
- iš mokyklos eiti tiesiai į namus;
- tėvai turi žinoti savo vaiko draugus;
- niekam neteikti informacijos apie savo šeimą ir draugus;
- išlikti mandagiu ir taktiškai bendrauti su visais žmonėmis;
- neimti nieko, kas svetima.

Dabar pabandykime visa tai pritaikyti interneto naudotojui.

✕ **NESIKALBĖTI SU NEPAŽĮSTAMAIS IR NEIMTI IŠ JŲ DOVANŲ.** Vaikams reikia aiškinti, kad kiekvienas asmuo, kontaktuojantis su juo internete, yra nepažįstamasis, nepaisant to, kaip ilgai tęsiasi internetinis bendravimas ar internetinė draugystė, kaip seniai jie plepa ir kokį artumą jaučia su tuo žmogumi – vis tiek jis yra nepažįstamas ir nežinomas asmuo. Net ir pačios įdomiausios žinutės ar pokalbiai vaikams ir paaugliams gali būti labai pavojingi, jeigu jiems neaiškinsite, kad **KIEKVIENAS, SU KURIUO JIE NESUSITIKO REALIAME GYVENIME, YRA NEPAŽĮSTAMAS ASMUO**, todėl su juo negalima kalbėtis apie viską, kaip su geru draugu. Kartais vaikams tai labai sunku suprasti, nes bendraudami internetu, ypač namuose, dalyvaujant ir tėvams, jie jaučiasi visiškai saugūs ir nelieka įtarumo ar baimės, patiriamos gatvėje ar kieme.

Praėjusiais metais internetas tapo pagrindine ir viena mėgstamiausių seksualinių maniakų lankymosi vietų, nes virtualioje erdvėje galima veikti anonimiškai, kartu sudaromas klaidingas įspūdis apie tikruosius artimos pažinties tikslus. Jie stengiasi įtikinti vaikus, kad čia, internete, negalioja įprastinės bendravimo taisyklės, čia viskas paprasčiau, greičiau ir saugiau. Įsitikinkite, kad jūsų vaikai žino, jog tai netiesa. Paaiškinkite, kad nenormalu priimti dovanas iš svetimo asmens, nepaisant to, ar jas perduos pats žmogus, ar atsiųs į namus paštu, nes tai gali būti pasala, apgaulė, norint sužinoti tikslų namų adresą.

✕ **IŠ MOKYKLOS EITI TIESIAI Į NAMUS.** Tai viena pagrindinių taisyklių, kurią paveldėjome iš tėvų ir dabar ją perduodame savo vaikams. Ji tinka ir interneto vartotojams. Jeigu leidžiate savo vaikams betiksliai klaidžioti internete, tai gali sukelti nemalonumų. Betikslis naršymas internete prilygsta betiksliam bastymuisi miesto gatvėmis po pamokų, kur taip pat galima sutikti nedorų žmonių arba tiesiog atsirasti netinkamu laiku ir nepageidautinoje vietoje. Jeigu norite apsaugoti savo vaikus, nustatydami naršymui

internete skirto laiko limitą, jie gali tai panaudoti žalingos informacijos paieškai. Kiekvieną dieną baigę namų darbams ar kitoms užduotims atlikti reikiamos informacijos paiešką internete, vaikai gali dar valandą naudotis internetu – paplepėti pokalbių kambariuose ar užsiimti kita mėgstama veikla tik tėvų prižiūrimi. Kaip jūs nurodote, kad po pamokų eitų tiesiai į namus, taip turite reikalauti, kad pasinaudoję internetu tikslinės informacijos paieškai (namų darbams atlikti ir pan.) nutrauktų betikslį naršymą.

✕ **TĖVAI TURI ŽINOTI SAVO VAIKO DRAUGUS.** Tai žodžiai, kuriuos mes sakome savo vaikams kiekvieną dieną, kai jie susiranda naujų draugų realiame gyvenime. O kodėl jų nepritaikius ir interneto draugams? Juk jūs neleidžiate vaikams draugauti ir bendrauti su nepažįstamais žmonėmis. Tos pačios taisyklės galioja ir internetiniams draugams bei naujoms pažintims. Jūs turite žinoti, su kuo vaikai bendrauja internetu, ir įsitikinti, kad jų draugystė yra tikra, o žmogus iš tiesų yra tas, kuriuo jis prisistato, ir bendravimui su juo jūs neprieštaraujate. Neįmanoma pažinti visų žmonių, nes jūsų vaikas kasdien naudojasi internetu, tačiau vis tiek turite žinoti, su kokiais žmonėmis jūsų vaikas palaiko ryšius ir kurie turi jam įtakos. Kai jūsų vaikas susipažįsta mokykloje ar gatvėje su naujais žmonėmis, jis jaučiasi pažeidžiamas, nesaugus, o bendraudamas interneto pokalbių kambariuose, būdamas savo namuose, visiškai nematydamas pašnekovo, jis jaučiasi saugus ir pamiršta apie atsargumą ir grėsmę. Ir dar vienas svarbus dalykas. Kai vaikas mato savo pašnekovą, jis gali atitinkamai reaguoti ir bendrauti su suaugusiais ir savo bendraamžiais, tačiau to negalima padaryti bendraujant internetu. Daugelis pedofilų, kurie ieško savo aukų pokalbių kambariuose, dažniausiai prisistato pasirinktos aukos bendraamžiu, kad išvengtų įtarimų. Kartais jums lengviau nustatyti pašnekovo amžių.

✕ **NIEKAM NETEIKTI INFORMACIJOS APIE SAVO ŠEIMĄ IR DRAUGUS.** Nuolat priminkite savo vaikams, kad jie tikrai nežino, su kuo bendrauja pokalbių kambariuose netgi tada, kai mano, jog gali pasitikėti savo pašnekovais, – tai gali būti visiškai kiti žmonės nei tie, kuriais jie prisistato. Dalytis asmenine informacija interneto pokalbių kambariuose yra tas pats, kas gatvėje garsiai skaityti savo dienoraštį. Jeigu vaikas teikia asmeninę informaciją internete, tai gali pakenkti ir jam, ir jo šeimai. Svarbu reikalauti, kad vaikas laikytųsi tam tikrų taisyklių ir suprastų, jog jūs juo pasitikėjote ir patikėjote jam asmeninę informaciją. Susitarkite su vaikais dėl abipusio pasitikėjimo ir reikalaukite laikytis susitarimo sąlygų. Priešingu atveju jie gali sukelti didelį pavojų jums, jūsų neliečiamumui, kaip ir jūsų sąskaitoms banke. Dažnai vaikai pasimeta ir negali suprasti, kodėl vienu atveju jiems liepiame būti mandagiems ir taktiškai bendrauti su žmonėmis, kartu sakome nekalbėti su nepažįstamais. Suprantamai paaiškinkite vaikams, kad jie neprivalo atsakyti į visus pateikiamus klausimus ir turi išmokti mandagiai pasakyti, kad į tokius klausimus jie negali ir nenori atsakinėti. Prisiminkite specialistų patarimus, jog bendravimas pokalbių kambariuose prilygsta pokalbiui telefonu. Bendraujant internete galioja tos pačios supratimo taisyklės.

✕ **IŠLIKTI MANDAGIU IR TAKTIŠKAI BENDRAUTI SU VISAIS ŽMONĖMIS.** Vaikai yra... vaikai, ir jie dažnai įžeidžia vienas kitą, nepagalvodami apie pasekmes. Iš tiesų, tai kartojasi dažnai, kad žodiniai įžeidimai ir priešiškumas taip įkyri aplinkiniams žmonėms, jog jie sugalvojo net specialų pavadinimą – „pielavojasi“. Tai gali peraugti į ilgą ir nemalonią kovą už viską, kuo domimasi. Jeigu įtariate, kad jūsų vaikas kažką puola žodžiais, įžeidinėja bendraudamas internetu, paaiškinkite, jog žodiniai įžeidimai kalbantis prilygsta padarytai moralinei žalai realiame gyvenime. Jeigu sužinote, kad jūsų vaikas su

kažkuo „kovoja žodžiais“ pokalbių kambariuose, imkitės padėties kontrolės. Praneškite interneto tiekėjui ir atsakingiems svetainės, kurioje vyksta „kova“, asmenims.

NEIMTI NIEKO, KAS SVETIMA. Šiandien vis dažniau vaikai naudojasi internetu – namų darbams atlikti, asmeninei svetainei sukurti ir tvarkyti, muzikos įrašams, programinei medžiagai ir filmams parsisiųsti. Visais minėtais atvejais jie dažniausiai pažeidžia įstatymus. Tuo metu, kai įrašinėja tekstus, muziką, filmus ar programas, jie ima daiktus, kurie jiems nepriklauso. Daugelis tėvų mano, kad viskas gerai, jeigu nurodomas šaltinis. Tai netiesa. Jūsų pareiga išaiškinti savo vaikams, kad muzikos vagystė internete – tai tas pats blogis, kaip vogti muzikos įrašus parduotuvėje, nes imama kažkieno kito nuosavybė. Šiomis dienomis vis dažniau žmonės persekiojami už intelektinės nuosavybės pasisavinimą virtualioje erdvėje.

Priemonės, padedančios aptikti vaikams žalingą internetą

Net jeigu savo vaikams išaiškinote visas saugaus naudojimosi internetu taisykles, vis tiek jie nėra saugūs, ypač kai lankosi interneto pokalbių kambariuose. Iš kai kurių atpažinimo ženklų, pakitusio elgesio galėsite suprasti, kada jūsų vaikai veikiami internetinių pažinčių. Atkreipkite dėmesį, jeigu vaikas staigiai išjungia kompiuterį jums įėjus į kambarį arba ištisomis naktimis plepa pokalbių kambariuose, dažnai skambina telefonu. Dar atsargesni turėtumėte būti, jeigu sulaukiate dovanų namų adresu, o jūsų vaikai nenori paaiškinti, nuo ko tos dovanos ir kokie ryšiai juos sieja. Tuomet pats laikas pradėti kontroliuoti vaikų internetinių ryšių adresus pasinaudojant patarimais, išdėstytais žemiau. Psichologai, padėdami tėvams, kuria tipinį seksualinių prievartautojų aukos portretą. Daugelis tokių aukų yra 12–15 metų vaikai. Jie paprastai bando ištrūkti iš tėvų globos, nori būti nepriklausomi, atsikalbinėja. Seksualinių prievartautojų aukomis dažniausiai tampa vienišiai, kurie realiame gyvenime turi labai mažai draugų, gyvena su vienu iš tėvų ar nedarniose šeimose, todėl ieško meilės, dėmesio, supratimo ir įvertinimo. Kurį laiką vaikai nesupranta, kad jie bendrauja su suaugusiais. Kai pedofilas psichologiškai paveikia ir įtikina vaiką, ypač mergaites, jos jau būna prisirišusios ir mano, kad įsimylėjo tą žmogų. Visa tai išsiaiškinę berniukai jaučiasi apgauti, tačiau kartais jie nori tik pabandyti bendrauti su homoseksualais.

Toliau aptarkime atpažinimo požymius, ryškėjančius stebint vaikus.

- Jeigu jūsų vaikui trūksta draugų pripažinimo ir įvertinimo realiame gyvenime, vadinasi, jis šį trūkumą bandys užpildyti internetinėmis pažintimis. Dažnai šitaip elgiasi nepasitikintys, prastai save vertinantys vaikai. Bendraudami internetu vaikai „neturi veido“ (nesimato jų veidų), todėl jie gali prisistatyti ir pasijusti tuo, kuo iš tiesų norėtų būti.
- Jūsų vaikui 12–15 metų. Šio amžiaus vaikai labiausiai pažeidžiami ir lengviausiai pasiduoda interneto pokalbių kambarių „grobuonims“. 16 m. vaiką tokiems grobuonims sunkiau įvilioti į savo spąstus, nes jie jau pradeda kritiškiau mąstyti, elgiasi panašiai, kaip ir suaugę, darosi įtaresni, atsargesni ir todėl mažiau domina pedofilus.

- Jūsų vaikas praleidžia 1–2 valandomis daugiau laiko internete tiesiog pramogaudamas. Psichologai tvirtina, kad vaiko praleistas laikas internete, proporcingas jo norams, kelia didelę riziką jo internetiniam bendravimui. Turėtumėte būti ypač atsargūs, jeigu leidžiate savo vaikui kai kur nueiti vienam, be suaugusiųjų.
- Jūsų vaikai labai apsaugoti ir pasitikintys arba, atvirkščiai, linkę rizikuoti, keldami jums papildomų rūpesčių. Pedofilų aukomis dažniausiai tampa dviejų kategorijų vaikai: 1) lengvai įgyjantys suaugusiųjų pasitikėjimą už meilę ir draugystę ir 2) nepaklusnūs, norintys kuo greičiau tapti suaugusiais.
- Vaikai slepia nuo jūsų savo internetines paieškas ir lankomus tinklalapius. Tuo galite lengvai įsitikinti. Jeigu dažnai išjungiamas kompiuteris ar monitorius jums įėjus į kambarį, jeigu vaikas nepasakoja apie savo internetinius draugus arba sulaukia keistų telefono skambučių iš jums nepažįstamų žmonių, gauna dovanas iš nepažįstamo žmogaus, vadinasi, jūsų vaikui iškilo grėsmė. Paprašykite jį pateikti savo draugų sąrašą ir lankomų svetainių adresus. Įsitikinkite, kad vaikas juos visus iš tiesų pažįsta. Jeigu jūsų vaikas turi susikūręs savo svetainę ar anketą internete – patikrinkite, ar ten pateikiama teisinga ir leistina informacija, ar nėra nereikalingos asmeninės informacijos, kuri galėtų kelti grėsmę jūsų šeimos saugumui.
  Naudokite interneto tinklalapių turinio filtravimo priemones, blokuojančias prieėjimą prie žalingų tinklalapių. Pasiskaityti ir atsisiųsti pačią programą galima iš tinklalapio www.esaugumas.lt.
- Jūsų vaikas neseniai išsiskyrė su senu draugu, pasikeitė jo elgesys, nuotaika, susirado naujų draugų, apie kuriuos jūs nieko nežinote. Tai gali būti grėsmės požymis. Net jeigu tai ne pokalbių kambarių pedofilų grėsmė, vis tiek reikia pasirūpinti ir skirti jam daugiau dėmesio, nes tai gali turėti rimtų pasekmių.

Mokymo planas

Interneto technologijų įvadinės žinios

Pasauliniai tinklai

Per raktinį žodį *keyword*, valdomą internetinių tyrimų *Internet research*, naudojant paieškos sistemas *search engines*, panašias į *Google*, milijonams žmonių visame pasaulyje lengvai ir greitai prieinama įvairi bendravimo informacija. Pasauliniai internetiniai tinklai neįtikėtinai greitai decentralizavo visą informaciją ir duomenų bazes, tai tiesiog nepalyginama su enciklopedijomis *encyclopedias* ir tradicinėmis bibliotekomis *libraries*. Daugelis individų ir kompanijų arba jų grupių priėmė sprendimą dėl informacijos vartotojų ir serverių registracijos arba *blogs*, kurie dažniausiai naudojami kaip lengvai prieinami ir nefiksuojantys datos dienoraščiai. Kai kurios verslo organizacijos skatina jų pildymą patarimais, liečiančiais jų organizacijų specializaciją, tikėdamos, kad sudomins lankytojus naudingomis žiniomis, laisva informacija ir tuo pačiu susidomės

ir jų korporacija. Vienas šios praktikos pavyzdžių – *Microsoft* darbuotojai, kurie leidžia *blogs* produktus tikėdamiesi sudominti kuo daugiau vartotojų.

Norėdami daugiau sužinoti apie skirtumus tarp pasaulinių tinklų ir paprastojo kasdienio vartojimo interneto, žiūrėkite juodąjį internetą *developers*, kur visa tai aptariama gerokai plačiau.

Nuotolinis valdymas

Internetu kompiuterių vartotojas lengvai ir greitai gali susijungti su kito kompiuterio vartotojo duomenų bazėmis, nesvarbu, kurioje pasaulio šalyje jie būtų. Tai galima atlikti su ar be vartotojo apsaugos, duomenų patikimumo iššifravimo technologijomis pagal poreikį. Šitaip skatinamas naujas būdas dirbti namuose, bendradarbiavimas ir dalijimasis informacija daugelyje pramonės šakų. Buhalteris *Dark Internet*, būdamas namuose, gali revizuoti *accountant* knygų kompanijas, esančias įvairiose šalyse, serveryje *audit* įvairiose šalyse aptarnauja tie patys specialistai. Šiuos skaičiavimus, naudodamiesi elektroniniu paštu pasiųsta informacija iš viso pasaulio, gali atlikti namų darbininkai, buhalteriai, kurie gyvena toli nuo pagrindinės įmonės. Kai kuriuos iš šių dalykų buvo galima atlikti ir anksčiau, negu įsisavintas platus interneto vartojimas, be individualių, išnuomotų *server* linijų, daugelio iš jų praktiškai neapčiuopiamų. Toli nuo darbo kabineto, galbūt kitoje pasaulio šalyje, išvykus atostogų ar į komandiruotę galima sukurti nutolusią darbo vietą *leased lines*, naudojantis virtualiu saugiu asmeniniu tinklu per internetą.

Remote desktop Virtual Private Network teikia galimybę pasinaudoti visais duomenimis, elektroniniu paštu ir bylomis net ir tuo atveju, kai vartotojas labai toli. Ši sąvoka kai kurių žmonių vartojama kaip iš tiesų virtualus asmeninis namų košmaras, nes tai išplečia galimybes bei saugius korporacijos parametrus ir darbuotojo namuose. Pasitaikė tik keli saugos pažeidimo atvejai.

Bylų (dokumentų paketų) rūšiavimas

Kompiuterinė byla *Computer_file* gali būti siunčiama elektroniniu paštu *e-mailed* klientams, kolegoms ir draugams, kaip priedas *attachment*. Tai gali būti įrašoma į serverį *Web site* arba *FTP* lengvų įrašymų serverį visiems. Taip pat gali būti pateikiama specialiojoje vietoje arba serverio byloje *file server* trumpalaikiam naudojimui. Daugkartiniam naudojimui daugeliui vartotojų gali būti palengvintas, sumažintos apimties, *mirror* serverio pagalba, arba sujungiant vienodus tinklų mazgus *peer-to-peer* tinklų tipo BitTorrent. Kiekvienu iš šių atvejų priėjimą prie dokumentų paketo galima valdyti originaliais vartotojų įrengimais *authentication*. Bylos (dokumentų paketo) kelionę internetu gali trukdyti šifruotė, *encryption*, ir pasikeisti įkainiai prieš ar po to, kai sulauksite dokumentų paketo. Paslaugą galima apmokėti nuotoliniu būdu iš kreditinės kortelės *credit card* arba *digital signatures* arba kitokiu pranešimo būdu.

Šie paprasti *MD5* interneto ypatumai tarptautiniu požiūriu sudaro gamybos, prekybos ir kitokio platinimo visko, kas gali būti sumažinta ir išreikšta kompiuterine byla (dokumentų paketu), pagrindą. Tai apima visą biuro dokumentaciją, informaciją, leidinius, programinio aprūpinimo produktus, muziką *music*, fotografiją, vaizdajuostes, multiplikacijas, grafiką ir kitas meno sritis. Šitaip iš esmės keičiama visa nusistovėjusi pramoninė transportavimo sistema RIAA ir MPAA. JAV visa tai valdė gamybą ir jos produktų paskirstymą šalyje.

Ryšių tinklai

Daugelis šiuolaikinių žurnalistų „maitina“ internetą gyvu garso ir vaizdo perteikimu, pavyzdžiui, BBC. Jie taip pat gali leisti reguliuoti garso ir vaizdo kokybę, tarsi filmuotos medžiagos peržiūrą (klasikinių klipų), ir toliau klausytis ir stebėti. Prie šių paslaugų prisijungė „švaraus interneto diapazonas“ – žurnalistai, kurie anksčiau niekada neturėjo radijo ryšio licencijos. Vadinasi, internetinis ryšys, kaip kompiuteris ar kas nors originalesnio, gali būti panaudojamas pokalbiams beveik taip pat, kaip anksčiau tebuvo galima pasiekti tik per televiziją *TV* arba radijo imtuvais *Radio*. Medžiagos diapazonas gerokai platesnis, nuo pornografijos *Pornography* iki aukštos techninės tinklų perjungimo specializacijos. Eilučių perjungimas. *Podcasting* – šioje temoje, kur paprastai garsinė medžiaga iš pradžių įrašoma ir tik tada gali būti panaudojama kompiuteryje arba perjungiama skaitmeniniam garso įrašymui ir tuo pačiu klausymui *Digital audio player*. Šis metodas, panaudojant nesudėtingą įrangą, sudaro galimybę įveikiant nedidelę cenzūrą ar licencijavimo kontrolę garsinę ir vaizdo medžiagą perduoti viso pasaulio vartotojams. Ryšių mazgas *Webcam* gali būti naudojamas kaip pigesnė tinklo plėtros priemonė. Kai kurie ryšio tinklai gali teikti aukščiausios kokybės įprastą vaizdą arba jį sumažinti ar sulėtinti. Interneto vartotojai gali stebėti gyvūniją prie Afrikos vandens telkinių arba laivus Panamos sąsiauryje *Panama Canal*, judėjimą akiratyje arba jų patalpose gyvai ir realiu laiku. Taip pat populiarūs vaizdo pokalbių kambariai, *Chat rooms*, ryšio ir vaizdo konferencijos tarp nutolusių vietovių.

Video conferencing. Galima rasti daugybę įvairių abipusio ir vienpusio garso ryšio būdų.

VoIP

VoIP perteikia balsą, kur IP *Internet Protocol* perduoda internetui nurodymus, kurie yra viso interneto pagrindas. Šis reiškinys prasidėjo apie 2000 m. internetinėse sistemose kaip papildomas abipusis balso pratęsimas nuo žinutės pradžios *Instant Messaging*. Paskutiniaisiais metais šios stotelės tapo labai patogios, jas pradėta naudoti kaip telefoną. Privalumas yra tai, kad internetas perduoda judantį balsą, VoIP gali būti laisvas ir kainuoti gerokai mažiau negu telefono skambutis, be to, perduodamas ypač dideliais atstumais ir tiems asmenims, kurie naudojasi ADSL paslaugomis arba skaitmenine abonentine interneto linija *Digital Subscriber Line*.

Taigi VoIP tampa įprastinio telefono alternatyva. Šitaip paprasčiau bendrauti su įvairiais tiekėjais, skambinant ar gaunant žinutes iš paprasto telefono. Paprasti ir nebrangūs modemai dabar lengvai prieinami ir mažina PC poreikį. Balso kokybė gali keistis nuo kviečiamojo skambučio, tačiau dabar dažnai balso kokybė lenkia tradicinius šaukinius. Dar vis egzistuojanti VoIP problema – telefono numerių prijungimas *Emergency telephonenumber*, numerio rinkimas ir patikimumas. Paskutiniaisiais metais keletas VoIP tiekėjų aprūpina apie 911 numerių šaukinių, bet tai ne universalus priėjimas. Tradicinis telefonas turi turėti liniją ir veikia tol, kol sugenda, VoIP veikia be rezervinio elektroninio ryšio tiekėjo.

Uninterruptible power supply. Daugelis VoIP tiekėjų siūlo neribotą nacionalinių šaukinių skaičių, nes pagrindinis jų tikslas – globalus sujungimas be laiko apribojimų ir už mažą mėnesinį mokestį. VoIP vis populiaresnis pasaulinių žaidimų srityje, kaip žaidėjų ryšio forma. Populiariausių žaidimų klientai įsijungia *Ventrilo*, *Teamspeak*, nors prieinami ir kiti būdai.

Internetas tapo pagrindiniu laisvalaikio leidimo būdu anksčiau, negu sukurtas pasaulinis tinklas su įdomiais socialiniais eksperimentais. MUDs ir MOO ateityje universitetų serveriams pateiks didžiausius informacijos srautus. Šiandien daugelis interneto forumų *Internet forum* skirta žaidimams ir pramogoms bei animaciniams ir trumpametražiniams filmukams *Flash movie*.

Taip pat labai populiarūs pornografijai *Pornography* ir pasipelnymui *Gambling* skirti tinklalapiai. Kai kurios pramonės šakos pasipelnydamos prisiėmė viršenybę prieš pasaulinio interneto tikslus, ir dažnai aprūpina egzistuojantį informacijos šaltinį, skirtą reklamai, kitų serverių naudojimui. Daugelis valstybių bandė riboti abiejų interneto verslo šakų naudojimą, tačiau neįmanoma sustabdyti jų plačiai paskleisto populiarumo.

Viena pagrindinių laisvalaikio leidimo internete sričių – žaidimai *Multiplayer gaming*. Ši laisvalaikio forma sukuria tam tikras bendruomenes pagal amžių ir kilmę tam, kad žaidėjai galėtų mėgautis greitai besikeičiančiu žaidimo ir žaidėjų pasauliu. Jie naudojasi MMORPG pirmo žmogaus nuorodomis *First-person shooter* nuo žaidimo pasirinktų vaidmenų *Computer role-playing game* iki azartinių žaidimo diskusijų *Online gambling*. Tai patobulintas būdas, kuriuo naudojasi daugelis žmonių bendraudami ir leisdami savo laisvalaikį internete. Šitaip buvo apie 1970 m., o šiuolaikiniai diskusiniai žaidimai prasidėjo nuo *Game Spy Arcade* ir *MPlayer.com*, kur žaidėjai pasirašo tipinę registracijos sutartį. Neregistruotų žaidėjų apribojamos galimybės ir net priėjimai prie kai kurių žaidimų.

Daugelis vartotojų internetą naudoja muzikos įrašams, kino filmams parsisiųsti ir kitiems savo malonumo ir atsipalaidavimo darbams. Kaip anksčiau aptarėme, visa tai yra mokama, tik centrinės duomenų bazės jungiasi nemokamai naudodamos vienareikšmių ryšio mazgų sujungimo technologijas. Svarbu pažymėti, kad kai kurie pirminiai duomenų bazių vartotojai imasi atsakomybės apsaugoti autorines kūrėjų teises.

Kita dalis vartotojų naudojasi pasauliniais interneto tinklais ieškodami naujausios sporto varžybų informacijos, planuodami atostogas ir užsakydami keliones, siekdami sumažinti jų kainas ir gauti išankstines nuolaidas.

Žmonės naudojasi pokalbių kambariais *Internet Relay Chat*, žinučių siuntimu *Instant-messaging* ir elektroniniu paštu, norėdami palaikyti ryšį visame pasaulyje su naujais ir buvusiais draugais. Socialinės organizacijos sukūrė specialius serverius, panašius į *Friends Reunited*, ir palaiko jų kontaktą tiesiog savo malonumui.

Informacija apie rizikingą internetą

Internetas kelia keleriopą grėsmę mūsų vaikams, nes jame yra labai daug informacijos, tačiau ne visa atitinka jų reikalavimus. Dalį tos informacijos sudaro pornografija, mokami serveriai. Taip pat yra daug serverių, kuriuose parduodami tabako, alkoholio produktai arba net narkotikai. Jeigu jūsų vaikas gali pasinaudoti kreditine kortele, kas žino, ką jis gali sugalvoti. Patys to nežinodami, vaikai gali išplatinti svarbią asmeninę ar finansinę informaciją nepageidaujamiems žmonėms ar kompanijoms. Vaikai linkę dalyvauti pokalbių varžybose (žaidimuose) arba kontrolinėse prizų apklausose. Jeigu dažnai registruojatės internete ir pildote registracijos formas, kur reikia įrašyti ir asmeninių duomenų, vėliau šia informacija gali pasinaudoti pašaliniai asmenys, visiškai nesusiję su minimos

registracijos tikslais. Ši technika naudojama daugelio nedorų žmonių nedoriems kėslams, siekiama sužinoti jūsų pašto dėžutės duomenis, reikalingus įsilaužimams ir informacijos panaudojimui. Jūsų vaikai gali būti atakuojami kitų vaikų elektroniniais laiškais, forumuose, pokalbių kambariuose ar specialiai sukurtose svetainėse.

Internete vaikai gali pakliūti į melagingus tinklalapius, užmaskuotus kaip el. parduotuvės, bankų svetainės arba svetainės, siūlančios viliojančiai lengvus pinigus. Kai tik jūs įrašote banko identifikacijos duomenis, jie, žinoma, be jūsų žinios perduodami tinklalapio savininkui, kuris gautą informaciją panaudoja savo nedoriems kėslams.

Vienas pavojingiausių dalykų yra tai, kad jūsų vaikas gali tapti grobuonies, kuris stengsis užmegzti su juo virtualius, o vėliau ir realius santykius, auka.

Kol dar visiškai nesupanikavote ir neuždraudėte vaikams visam laikui naudotis internetu, įvertinkite kitu požiūriu šią problemą, antraip jums pasirodys, kad visos internetinės programos yra žalingos vaikui. Jeigu vaikai gali kritiškai ir atsakingai pažvelgti į jūsų finansinę ir asmeninę informaciją, grėsmė gerokai sumažėja. Jūs tik negalite sutrukdyti savo vaikui „užšokti" ant internetinių grobuonių, bet net ir tada jie gali išvengti grėsmės, jeigu nepiktnaudžiaus susitarimo taisyklėmis ir nepažįstamiems neteiks informacijos, kuri gali padėti grobuoniui susirasti vaiką realiame gyvenime.

Interneto rizika konkrečioms amžiaus grupėms

Šiame skyriuje apžvelgsime bendrąsias internetines grėsmes jūsų vaikui pagal amžiaus grupes.

IKI 7 METŲ

Šiuo metu galima pastebėti, kad jau 4–5 metų vaikai naršo internete. Jie dar nemoka skaityti ir rašyti, tačiau net ir jie to nežinodami gali „užklysti" į netinkamo turinio tinklalapius. Nors jiems ir nepavojingi pokalbių kambarių grobuonys, kadangi dar negali parašyti ar perskaityti, vadinasi, negali dalyvauti pokalbiuose ir perduoti jūsų asmeninės ar finansinės informacijos, tačiau nepalikite atviro internetinio tinklo ir neleiskite net ir nemokantiems skaityti ir rašyti vaikams naršyti jame, nes jie labai pažeidžiami ir nesugeba apsiginti. Net jeigu jūs ir išaiškinote vaikams apie gresiančius pavojus ir saugojimosi taisykles, jie, žiūrėdami į paveikslėlius, dar negali atskirti žalingo turinio nuo tinkamos informacijos.

7–10 METŲ

Tokio amžiaus vaikai jau moka skaityti ir rašyti, ir jie tai puikiai išnaudoja. Šis gebėjimas ir yra pagrindinė priežastis, kelianti jiems dar didesnę grėsmę, kad naršydami internete užtiks netinkamo turinio informacijos, kurios dar negali tinkamai įvertinti, tačiau jau gali perskaityti ir parašyti. Naudodamiesi paieškos sistemomis, pvz., *google* arba *yahoo*, darydami rašybos klaidų, jie gali aptikti visiškai ne tuos internetinius tinklalapius, kurių ieško. Taip pat gali nutikti net ir teisingai rašant ieškomo tinklalapio adresą. Internete labai daug panašių adresų ir tinklalapių pavadinimų, tačiau labai skirtingo informacijos turinio.

Šios amžiaus grupės vaikams ypatingą grėsmę kelia internetas, kadangi jie jau moka skaityti ir rašyti, gali dalyvauti pokalbių kambariuose ir dalytis informacija, pildyti įvairias registracijos formas. Pokalbių kambariuose jiems padidėja pedofilų grėsmė, nes jie žino, kad šie vaikai jau turi daugiau laisvės, vieni lanko draugus ir būna kitose vietose be suaugusiųjų.

11–15 METŲ

Remiantis ekspertų išvadomis, tokio amžiaus vaikai pokalbių kambariuose labiausiai medžiojami pedofilų. Paprastai jie medžioja dviejų tipų vaikus: pirmas – per daug pasitikinčius savimi, naivius, tikinčius kiekvienu tokio grobuonies žodžiu, ir antras – visiška priešingybė pirmajam tipui. Jie agresyvūs ir mėgsta rizikuoti laužydami paauglystės amžiaus laisvės apribojimus. Pedofilai labiausiai vertina šią amžiaus grupę, nes tokie vaikai dar nemąsto kaip suaugę, tačiau jie jau gali laisvai susitikinėti su draugais jų namuose, lankytis įvairiuose renginiuose be suaugusiųjų palydos. Šie vaikai dar nėra visiškai subrendę, jie linkę dalytis asmenine informacija, ypač jei mano, kad kažkas kitame internetiniame tinkle yra jų amžiaus ir su jais noriai ir maloniai bendrauja, juos įvertina ar pagiria.

16–18 METŲ

Tai brendimo periodas ir ši grupė savo mąstymu labiau panaši į suaugusius. Vien todėl jiems jau kyla mažesnė interneto grėsmė, tačiau tokio amžiaus vaikai nori būti nepriklausomi, dalytis asmenine ir bankų informacija, nes jie jau sugeba ja naudotis. Jeigu jūsų vaikas būtent tokio amžiaus, turite labai atsargiai naudotis bankine informacija. Vaikai gali pasinaudoti jūsų kreditine kortele ir užsisakyti brangių gaminių arba įkliūti į interneto sukčių, kurių tinklalapiai labai panašūs į bankų ar el. parduotuvių, pinkles ir pateikti jūsų bankinę informaciją.

Kita svarbi rizikos grupė – tai įvairūs duomenys: literatūra apie anoreksiją, rasistinė, teroristinė literatūra, informacija, kaip pasigaminti sprogmenų ir pan.

Žalingo interneto išaiškinimas ir patarimai, kaip tokiu atveju elgtis

PEDOFILIJA (POKALBIŲ KAMBARIAI, KONTAKTŲ UŽMEZGIMAS, DISKUSIJOS, FORUMAI IR T. T.)

Pirmiausia išsiaiškinkime, kokie iš viso yra pokalbių (diskusijų) kambariai. Viename amerikiečių žodyne aiškinama, jog tai – iš tiesų virtuali vieta, kur interneto vartotojai gali užmegzti ryšį realiu laiku naudodamiesi kompiuterio klaviatūra, o šiuo metu ir mikrofonu bei ausinėmis ir vaizdo kameromis.

Žmonėms, kurie niekada nesilankė panašiose į pokalbių kambarius vietose, gali pasirodyti, jog jokios grėsmės čia nebėra, tačiau, kaip ir realiame gyvenime, bendraujant su nepažįstamais yra šiek tiek rizikos. Jūs turėtumėte žinoti, kad kalbėdamasis su kitais šių kambarių lankytojais jūsų vaikas gali susidurti su nedorais suaugusiais. Iš tiesų, virtualioje interneto erdvėje daug anonimiškumo, todėl suaugę (ypač pedofilai) puikiausiai gali prisistatyti vaiko bendraamžiu. Šitaip dažnai elgiasi pedofilai, siekdami kuo greičiau įgyti vaikų pasitikėjimą. Kai tik pavyksta užmegzti kontaktą, grobuonis stengiasi kuo greičiau dalytis su vaiku jo rūpesčiais, apsimeta, kad supranta jo problemas. Pedofilai stebi internete pasyvius pokalbių kambarių lankytojus, kurie daugiau yra stebėtojai arba dar neseniai įsitraukė į pokalbius ir dar neturi draugų, tiksliau, ieško sau pašnekovų, o galbūt ir draugų. Realiame gyvenime, kaip ir virtualioje erdvėje, šie berniukai dažniausiai ignoruojami savo bendraamžių ir beveik neturi draugų, stokoja dėmesio. Kurį laiką jų bendravimas

vyksta tik virtualioje erdvėje, pokalbių kambariuose, vėliau pradeda susirašinėti el. paštu, SMS ir netgi skambinti telefonu. Šitaip grobuonis įgyja daugiau pasitikėjimo, kartu įrodydamas, kad jis taip pat pasitiki vaiku ir jiems abiems naudinga ši draugystė.

Toliau vaikas pamažu ruošiamas tiesos atskleidimui, kadangi naujasis jo internetinis draugas yra gerokai vyresnis, negu paminėjo pažinties pradžioje. Dažniausiai visa tai prasideda klausimais, pvz., ką tu manai apie vyresnį brolį? Ar norėtum turėti vyresnį geradarį, kuris galėtų tau padėti? Šitaip stengiamasi gauti naudos, nukreipti vaiko dėmesį nuo įtarimų, kurie gali jam kilti. Jeigu auka (vaikas) išsigąsta, viskas tuo ir baigiasi. Tačiau to negalima pasakyti apie pedofilus, nes jie tuo pačiu metu bendrauja su keletu vaikų, kad būtų didesnė realaus susitikimo galimybė. Jeigu auka neišsigąsta sužinojusi, kad naujasis jo pašnekovas yra suaugęs, jie pasikeičia adresais arba tariasi dėl susitikimo. Kai susitinka, vaiko visada prašoma, kad jis nepasakotų tėvams ar draugams apie jų pažintį, aiškinama, kad jie to nesupras ir neleis vaikui turėti suaugusių draugų.

Šitaip dažniausiai atsitinka tiems vaikams, kurie turi asmeninių problemų (šeimos ar draugų bendravimo stoka, nesupratimas, jo norų ir nuomonės ignoravimas), apie kurias pedofilas jau žino. Kartais grobuonis netgi pamoko vaiką, kaip ištrinti elektroninius laiškus ar pokalbių kambarių adresus, kad neaptiktų tėvai. Todėl tėvams tiesiog neįmanoma kontroliuoti vaiko internetinių ryšių, išsiaiškinti naujas pažintis ir draugus. Labiausiai pedofilų pažeidžiami šio tipo paaugliai, nes jie, pirma, maištautojai, linkę ieškoti iššūkių, nuošalių vietų ir rizikuoti, įrodyti, kad yra nepriklausomi nuo tėvų. Antra, jie gali laisvai susitikti su bet kuo ir jų niekas nekontroliuoja, tėvai tuo nesidomi arba per daug pasitiki.

Žinomas ir kitas būdas, kai pedofilas nesistengia susitikti su pasirinkta auka (vaiku), bet siekia gauti vaiko nuotrauką, siųsdamas jam pornografinio seksualinio turinio nuotraukas, arba bando tiesiog įtraukti į virtualų seksą. Kalbant apie internetinių pokalbių kambarių pavojų vaikams ir būtent apie pedofiliją, reikia paminėti, kad skriaudikai dažniausiai yra vyrai. Tačiau pasaulyje jau yra užregistruota atvejų, kai skriaudikės buvo moterys – jos įtraukė paaugles į prostituciją ar tvirkino jaunimą. Nepaisant prievartautojo (nusikaltėlio) lyties, rezultatas vis vien nepageidaujamas. Prieš leisdami vaikui naudotis internetu, pirmiausia pagalvokite apie jo saugumą.

Jūs turite įsitikinti, kad padarėte viską, jog apsaugotumėte vaiką nuo gresiančių pavojų. Paaiškinkite ir įtikinkite vaiką, kad ir bendraujant internetu gresia pavojus lygiai taip pat, kaip ir realiame gyvenime susitinkant su nepažįstamais. Reikia suprantamai išaiškinti, kad ne visi daiktai, kuriuos mato internete, yra tokie, kaip atrodo, ir kad ne visi žmonės, su kuriais jis bendrauja internete, yra tie asmenys, kuriais jie prisistato. Svarbu, kad vaikai suprastų ir patikėtų, jog negalima teikti informacijos, adresų, nuotraukų, kreditinių kortelių duomenų ar kitos asmeninės informacijos, nepasitarus su tėvais, be jų žinios, nepaisant to, kaip ilgai tęsiasi internetinė draugystė. Be to, turite nustatyti vaikui aiškias bendrąsias interneto ir lankymosi pokalbių kambariuose taisykles. Naudinga surašyti interneto naudojimosi grafiką, tikslias datas ir realų laiką. Geriausia parinkti tokias dienas ir valandas, kai būnate namuose, kad galėtumėte prižiūrėti vaiką tuo metu, kai jis plepa. Būkite atsargūs, bet neįkyrūs, kad neprarastumėte vaiko pasitikėjimo. Jeigu jūs labai dažnai tikrinsite savo vaikus, jie pradės viską slėpti nuo jūsų. Geriausia būti kažkur netoli, bet ne per arti. Jeigu taip elgsitės, vaikas pasitikės jumis ir praneš, kai tik jam kas nors nutiks neįprasto, pasidalins savo įtarimais ir nerimu. Jeigu jūs nenorite, kad vaikas viską, kas blogo nutinka, slėptų, turite jam išaiškinti, kad jeigu kas ir nutiks blogo, tai nebūtinai dėl to jis kaltas. Kad ir kas nutiktų, nerodykite pykčio, nuraminkite vaiką ir išsiaiškinkite kilusią problemą.

Jeigu kažkas įžeidinėja jūsų vaiką ar siunčia netinkamo turinio informaciją, tiesiog blokuokite tokį pašnekovą, pasinaudodami pokalbių kambarių teikiama pagalba, arba praneškite apie tokį vartotoją pokalbių kambario administracijai. Ir prisiminkite, negalima pykti ir barti vaiko. Jeigu nubausite arba išbarsite vaiką už tai, dėl ko jis nekaltas, patikėkite, jis kitą kartą nesikreips į jus, kai jam kils pavojus, baimė ar grėsmė. Jūs taip pat galite apsilankyti pokalbių kambariuose, kuriuos lanko jūsų vaikas. Nors negalėsite nustatyti, ar tikrai jie yra pavojingi, tai bent jau įsitikinsite, kad jie skirti vaikams.

Ir paskutinis patarimas. Jeigu norite, kad jūsų vaikas rimtai vertintų susitarimą, turite numatyti pasekmes, jei sutartis bus pažeista. Geriausia pasirašyti susitarimą su vaiku, kur jo parašas taip pat svarbus. Susitarime turi būti numatytos teisės ir įsipareigojimai abiejų šalių – jūsų ir vaiko, taip pat ir pasekmės, jeigu sutarties nesilaikoma. Internete galite rasti paruoštą interneto naudojimo sutartį, tačiau galite ir savo paruošti, visas sutarties sąlygas aptardami su vaiku.

VIRUSAI, ĮSILAUŽIMAI IR ŠIUKŠLĖS

Kompiuterinis virusas

Kompiuterio savininkas, turintis interneto prieigą, ne tik gauna naudingos informacijos, bet dažnai susiduria su elektroniniais tinklais plintančiais virusais.

Kompiuteriniai virusai – tai kompiuterinės programos. Nuo įprastų programų jos skiriasi tuo, kad yra piktavališkos ir geba pačios plisti, dažnai įgaudamos epidemijos mastus. Šia savybe kompiuteriniai virusai yra labai panašūs į biologinius virusus. Kompiuteriniai virusai sukelia žalingų padarinių, pavyzdžiui, sunaikina ar sugadina kompiuteryje esančią informaciją, taip pat gali atlikti kompiuterines atakas prieš kitus kompiuterius, lemti kompiuterių ir tinklų perkrovas arba perimti kompiuterio valdymą.

Dažniausiai kompiuteriniai virusai plinta elektroniniu paštu, būna prisegti prie įvairių programų, kurias įjungus aktyvuojamas virusas.

Egzistuoja šimtai tūkstančių kompiuterinių virusų, tačiau daugelį jų galima suklasifikuoti pagal veikimo požymius.

Kirminai. Tai virusų, kurie patys geba daugintis, atmaina. Didžiausias jų keliamas pavojus yra gebėjimas sparčiai daugintis. Įprastas virusas turi įsiskverbti į kitas bylas, o kirminas gali daugintis nesustodamas tol, kol išnaudos kompiuterio duomenų talpą arba išplis po visą tinklą ir sutrikdys jo darbą. Daugiausia kirminai plinta elektroniniu paštu ir aktyvuojami atidarius bylą, prisegamą prie laiško.

Trojanai (dar kitaip vadinami Trojos arkliais) – tai kompiuterinės programos, besislepiančios kitose programose ir išoriškai atrodančios kaip naudingos, tačiau realiai sukeliančios kenksmingų padarinių. Skirtingai nuo kirminų, trojanai negamina savo kopijų, bet aktyvavus programą, už kurios jie slepiasi, kartu aktyvuojamas ir virusas. Veikiantis trojanas ypač pavojingas, nes sudaro virtualų koridorių, per kurį užkrėstasis kompiuteris ir jo ištekliai tampa prieinami iš išorės.

Makrovirusai – tai virusų rūšis, pažeidžianti dokumentus, sukurtus su taikomosiomis programomis, turinčiomis priemones makrokomandoms vykdyti. Dokumentas užkrečiamas, jį atidarant programos lange, jei neuždraustas makrokomandų vykdymas. Jis prilimpa prie *Microsoft Word* ar *Exel* programų šablonų taip, kad visi naujai sukurti

dokumentai jau turėtų viruso kodą, ir virusas, startavęs kitame kompiuteryje, atidarant dokumentą galėtų toliau užkrėsti. Apsisaugoti galima tik *Microsoft Word* ar *Excel* programoje uždraudus automatinį makrokomandų vykdymą.

Boot virusai – vieni pirmųjų kompiuterinių virusų. Tokie virusai plito naudojantis diskeliais ir veikdavo per kompiuterio DOS (angl. *Disk Operating System*) sistemą. Tokių virusų plitimo mastai nebuvo dideli, ir šiuo metu praktiškai jų beveik nepasitaiko.

SPAM

Taip pat aiškiai pastebimas ir kenkėjiško pobūdžio *spam* daugėjimas, kai su el. pašto žinutėmis keliauja ir kompiuteriniai virusai, vadinamieji interneto kirminai bei trojanai. Dažnai tai būna kompiuterinės programos, skenuojančios viruso pažeisto kompiuterio atmintį ir ieškančios el. pašto adresų, kuriais būtų galima persiųsti virusą kitai potencialiai aukai. Taip pat sparčiai plinta laiškai, kurie siunčiami sukčių siekiant sužinoti vertingą informaciją (angl. *phishing*). *Spam* siunčiantys asmenys nori sužinoti slaptažodžius ar kredito kortelių duomenis. Kad atrodytų tikroviškiau, dažnai tokie laiškai melagingai pasirašomi „banko darbuotojų".

Kodėl siunčiamas *spam*?

Kad būtų galima pradėti kovoti su *spam* reiškiniu, visų pirma reikėtų išsiaiškinti priežastį, kodėl kai kurie asmenys siunčia *spam*. Pagrindinė priežastis yra pinigai, t. y. nauda, kurią gauna *spam* siuntėjai.

- Nedidelis pradinis kapitalas. Tereikia įsigyti kompiuterį ir prisijungti prie nebrangaus interneto paslaugų teikėjo bei turėti el. pašto adresų duomenų bazę ir jau galima tapti visaverčiu žaidėju šiame versle. Pastebėta, kad tokią duomenų bazę galima įsigyti internete: 20 mln. adresų kainuoja apytikriai 400 Lt. Papildomai už 110 Lt galima įsigyti programinę įrangą automatizuotam *spam* siuntimui. Tokios programos gali išsiųsti iki 100 žinučių per minutę.
- Atskiros el. pašto žinutės išsiuntimo kaina taip pat nedidelė. Apskaičiuota, kad vidutiniškai vienai žinutei išsiųsti tereikia kelių centų. Tokiame versle pradinės investicijos gali atsipirkti jau po penkių dienų, užtenka, jog į 100 tūkst. *spam* žinučių atsilieptų bent vienas vartotojas.
- El. pašto architektūra, pagrįsta SMTP (*Simple Mail Transfer Protocol*) protokolu, yra nesaugi. Siuntėjo adresas (t. y. laukelis „From") gali būti nesunkiai pakeistas kitu, dėl to *spam* siuntėjai gali veikti anonimiškai ir išvengti įstatymų numatytų sankcijų.
- Ir pagaliau daug ką nulemia tas faktas, kad atsiranda žmonių (sudaro apie 3 proc. *spam* gavėjų), kurie atsiliepia į *spam* laiškus ir užsisako reklamuojamas prekes ar paslaugas.

Faktai apie *spam*

Pastaruoju metu su *spam* susiduria praktiškai kiekvienas el. pašto sistemos vartotojas, nes didžiąją el. pašto srauto dalį sudaro *spam* laiškai. Tai atima daug laiko namie ir darbe bereikalingai tikrinant ir trinant šiuos nepageidaujamus laiškus, be to, smarkiai apkraunama el. pašto sistema. Dėl to patiriami nuostoliai skaičiuojami milijonais. Plačiau apie spam statistiką – www.esaugumas.lt

Spam reglamentavimas Lietuvoje

Nors vartotojai ir interneto paslaugų teikėjai gana dažnai kritiškai atsiliepia apie *spam* reglamentuojančią teisinę bazę, Lietuvoje *spam* reiškinys yra ganėtinai aiškiai reglamentuotas. Lietuvos Respublikos elektroninių ryšių įstatymo 68 straipsnio 1 dalis nustato, kad naudoti elektroninių ryšių paslaugas tiesioginės rinkodaros tikslais leidžiama tik esant išankstiniam abonento sutikimui. Panašų reglamentavimą dėl *spam* numato Asmens duomenų teisinės apsaugos bei Reklamos įstatymai. Lietuvos Respublikos administracinių teisių pažeidimų kodekso 214-23 str. numatyta administracinė nuobauda – bauda nuo 500 iki 1000 Lt, o esant pakartotiniam pažeidimui – nuo 1000 iki 2000 Lt. Plačiau apie *spam* reglamentavimą Lietuvoje – www.esaugumas.lt

Rekomenduojama

Visiškai išvengti *spam* laiškų yra sunku – ne visiems priimtina slėpti savo el. pašto adresą, neskelbiant jo internete. Taip pat negalite būti įsitikinęs, kad virusas jo nesužinos iš kolegos ar draugo užkrėsto kompiuterio. Tačiau kovai su *spam* galite naudoti tam tikras priemones ir pasinaudoti šiais patarimais, padėsiančiais išvengti ar bent jau sumažinti tokių laiškų antplūdį.

- Naudodamiesi el. pašto paslaugomis, taikykite ***spam* filtravimo ir blokavimo (*anti-spam*) priemones**, kurios yra įdiegtos bei konfigūruojamos pagal jūsų poreikius (laiškų nuo atitinkamų adresatų blokavimas, filtravimas pagal nuorodas ir pan.). Su *spam* filtrais susipažinti ir juos įdiegti galite pasinaudoję nuorodomis: *Spam Assassin, SpamBouncer, Frontgate MX, Abuse.Net, K9.*
- Jeigu iš vieno konkretaus adreso gaunate labai daug *spam*, tai **galite pasinaudodami savo pašto programos filtru** juos blokuoti ir siųsti tiesiai į šiukšlių dėžę ar į atskirą katalogą. Kai kurios programos (pvz., *Microsoft Outlook*) atlieka gautų el. laiškų analizę ir gali atlikti *spam* laiškų filtravimą, pvz., tokius laiškus šalinti arba perkelti į specialų katalogą vėlesnei peržiūrai.
- Neretai *spam* laiškai būna suformuoti taip, jog užtenka vien tik neatsargiai peržiūrėti tokią žinutę ir jūsų el. pašto adresas užregistruojamas *spam* platintojų duomenų bazėse kaip potencialaus reklamos skaitytojo adresas. Tai paskatins juos siųsti dar daugiau *spam* į jūsų pašto dėžutę. Kad to išvengtumėte, **išjunkite HTML formatuotų laiškų peržiūros galimybę**. Procedūros atlikimo nuoroda – http://cert.litnet.lt/dokumentai/saugusdarbas.html
- **Niekuomet neatidarinėkite bylų**, kurios buvo gautos el. paštu (t. y. laiško priedai, dažnai turintys priesagas .exe ar pan.) prieš tai neįsitikinę, kad jos neužkrėstos virusais. Pavyzdžiui, virusas „Sobig.F“ plinta, kai atidaromas el. laiško priedas pavadinimu „Thank You“ ar „Re Details“. Virusu užkrėstas kompiuteris po to automatiškai siunčia užkrėstus laiškus visais aptiktais adresais iš elektroninės adresų knygutės.
- **Jei el. paštas tikrinamas iš** bibliotekų, mokymo įstaigų ar kitų **viešųjų vietų, užbaigę darbą uždarykite naršyklę**. Jei yra galimybė, papildomai reikėtų ištrinti slapukus (*cookies*), nes pagal slapukus neprašytų žinučių siuntėjai sprendžia apie vartotojų pomėgius (automobiliai, elektroninės prekės, nekilnojamasis turtas ir pan.) ir prieš siųsdami vartotojams neprašytas žinutes jas atitinkamai klasifikuoja.
- **Būkite atidūs, registruodamiesi tinklalapiuose**. Jeigu interneto svetainėje prašoma užsiregistruoti, būtina įdėmiai perskaityti sąlygas ir įsitikinti, jog žinote, kur

registruojatės ir kodėl reikalinga ši informacija. Jeigu rašote komentarus į kažkokį puslapį viešai prieinamuose tinklalapiuose ar el. pašto konferencijose, naudokitės kitu (alternatyviu) elektroniniu adresu arba savo elektroninį adresą užrašykite su „ETA“ (raidėmis) vietoj simbolio @. Tokiu atveju mažėja tikimybė, kad jūsų adresas bus „pavogtas“ (angl. *Harvesting*) pasitelkus atitinkamas programas.

- **Neatsakinėkite į *spam***. Bet koks atsakas į tokį laišką, net jei jame bus nurodyta, kad jūs daugiau nepageidaujate gauti *spam*, nuorodos spustelėjimas ar atsakymas siuntėjui, „Subject“ lauke nurodant „Unsubscribe“ tik patvirtins *spam* platintojui, jog jo laiškas buvo gautas ir peržiūrėtas ir kad šis adresas yra naudojamas, todėl juo toliau galima siųsti *spam*.
- **Siunčiant laiškus keliems adresatams vienu metu** ir rašant visus adresus „To“ ar „Cc“ adresų grupėje, kiekvieno gavusio laišką pašto programoje bus matomi visų kitų laiško gavėjų adresai. Tokio laiško gavėjų kompiuteryje esantys ar vėliau atsiradę virusai ar šnipinėjimo programos visus rastus elektroninio pašto adresus gali išnaudoti tolesniam viruso platinimui ar SPAM laiškų siuntimui. Jei nėra būtinybės, kad gavėjai matytų, kam siųstas laiškas, rekomenduojama siunčiant laiškus keliems gavėjams vienu metu jų adresus rašyti į „Bcc“ adresų grupę. „Bcc“ grupėje esantys adresai nebus matomi nei kitiems laiško gavėjams, nei jų kompiuteriuose esančioms programoms.

PHISHING

Duomenų vagystė *phishing* (angl. terminas *phishing* kilęs nuo žodžių *password fishing* – slaptažodžių žvejyba) – tai tokia sukčiavimo forma prieš organizacijas ar privačius asmenis, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis *spam* ar falsifikuotais interneto tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis.

Dažniausiai tokio pobūdžio atakos būna nukreiptos prieš bankų klientus, siekiant sužinoti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis.

Vėliau tokiu būdu gauta informacija gali būti panaudota pasipelnymo tikslais vykdant nusikalstamas veikas: neteisėtai jungiantis prie informacinių sistemų, vagiant pinigus iš sąskaitų ar elektroninėje erdvėje atsiskaitant už prekes svetimomis kortelėmis.

✕ Kaip tai veikia?

Išsiaiškinkime, kas yra duomenų vagystė internete. Pateikiame tradicinę veikimo schemą.

- Paprastai ataka pradedama nuo elektroninio pašto laiškų, atrodančių taip, lyg jie būtų siunčiami banko ar kitos rimtos organizacijos (*Phishing* laiško pavyzdys – www.esaugumas.lt). Laiško siuntėjo laukelyje esantis adresas dažniausiai būna netikras (falsifikuotas).
- Laiške gali būti pranešama, kad, pavyzdžiui, sustabdytas vartotojo sąskaitos galiojimas, ir, kol jis neužpildys tam tikrų duomenų anketoje, jo sąskaitos galiojimas nebus atnaujintas. Arba neva keičiantis aptarnavimo sistemai ar jos konfigūracijai reikia atnaujinti prisijungimo duomenis, todėl prašoma juos pateikti ir t. t.

- Dažniausiai tokiuose laiškuose būna nuoroda į realiai egzistuojančios finansinės institucijos suklastotą interneto svetainę, kurios adresas kartais būna beveik identiškas tikrajam tos organizacijos svetainės adresui (skiriasi viena kita raidė ar simbolis). Kadangi dažniausiai klonuojami bankų tinklalapiai, paprastai prašoma atsiųsti banko sąskaitos duomenis, prisijungimo slaptažodžius ar kitus konfidencialius duomenis (*Phishing* tinklalapio pavyzdys – www.esaugumas.lt).
- Laiškas, be teksto ir nuorodų, gali turėti priedų su kompiuteriniais virusais, t. y. žalingomis kompiuterinėmis programomis, kurias atidarius, pasinaudojant operacinių sistemų pažeidžiamumais, gali vykti automatinis konfidencialios informacijos, rastos kompiuteryje, persiuntimas piktavaliams.

Atminkite, kad gauti elektroninio pašto laiškai, kurie atitinka aukščiau aprašytus požymius, ir bus *phishing* atakų, skirtų duomenims vogti, pradžia. Iš esmės sukčiai šioje neteisėtoje veikloje išradingai naudojasi socialine inžinerija, stengdamiesi išgauti konfidencialią informaciją. Patiklūs žmonės kartais patiki išvedžiojimais elektroninio pašto laiškuose ir pateikia prašomus duomenis, dėl to vėliau gali nukentėti. Kadangi tokie laiškai siunčiami masiškai (t. y. milijonais per dieną), užtenka nedidelės dalies „užkibusių" žmonių, kad pasinaudojus jų pateikiama informacija galima būtų pasipelnyti.

✕ Kokie paplitimo mastai?

Dar 2003 m. JAV Federalinio tyrimų biuro (FBI) atstovai *phishing* pavadino „naujausia ir labiausiai susirūpinimą keliančia grėsme internete". Nuo to laiko duomenų vagystės plinta internete labai sparčiai ir, kaip pastebi tarptautinė *Anti-phishing* darbo grupė (APWG), *phishing* atvejų daugėja. Pagal statistiką, duomenų vagysčių aukomis tampa 3–5 proc. laiškų gavėjų ir tai yra daug. Plačiau apie *phishing* statistiką – www.esaugumas.lt

✕ Kaip neužkibti?

Tam, kad žmonės nepakliūtų į duomenų vagystės pinkles ir saugiai naudotųsi elektroninėmis paslaugomis, reikalingas didelis vartotojų atsargumas ir žinojimas, kaip apsaugoti savo duomenis. Todėl būtinas bent minimalus pagrindinių savisaugos elementų išmanymas.

- Visų pirma, labai **atsargiai įvertinkite laiškus, kuriuose prašoma pateikti konfidencialią informaciją**.
- Žinokite, kad patikimos kompanijos, o ypač **bankai, niekada neprašo tokios informacijos pateikti elektroninio pašto laiškais**.
- Neatsakinėkite į aukščiau aprašytus požymius atitinkančius *phishing* laiškus ir **nesinaudokite pateikiamomis nuorodomis į interneto tinklalapius**, kadangi tai gali būti užmaskuoti *phishing* tinklalapiai arba kompiuteriniai virusai, skirti duomenims slapta rinkti jūsų kompiuteryje.
- Jei būtinai reikia pasinaudoti nuoroda laiške, **įrašykite adresą tiesiai į savo interneto naršyklę**.
- Nerašykite svarbios informacijos į iššokančius (angl. *pop-up*) langus.
- Taip pat verta naudotis žemiau pateiktomis papildomomis saugumo priemonėmis, kurios mažina *phishing* atakų galimybes.

- Turėkite įdiegtas antivirusines programas ir laiku jas atnaujinkite. Tokios programos aptinka kompiuterinius virusus, nuolat skenuodamos kietąjį kompiuterio diską ir paleidžiamas programas, todėl geba aptiktus virusus sunaikinti jiems nespėjus padaryti žalos (žemiau pateikiamos internetinės nuorodos, kur galima rasti tokias programas).
- Naudokite *spam* filtravimo programinę įrangą, kadangi daugelis *phishing* atakų prasideda nuo *spam* laiškų. Tokios programos geba atpažinti *spam* laiškus ir juos sunaikinti, kol jie dar nepasiekė jūsų pašto dėžutės, arba gali juos nukreipti į specialų katalogą vėlesnei peržiūrai (žemiau pateikiamos internetinės nuorodos, kur galima rasti tokias programas).
- Naudokite *Anti-Spyware* programinę įrangą, kuri saugo jūsų kompiuterį nuo šnipinėjimą vykdančių programų arba įspėja apie jau esančias kompiuteryje tokio pobūdžio programas, todėl gali užkirsti kelią ir *phishing* programoms. *Spyware* yra tokia programa, kuri dažniausiai būna įdiegiama kartu su kitomis programomis ir, veikdama jūsų kompiuteryje, jums nematant, renka duomenis apie lankomas sritis internete, registruoja klaviatūros klavišų paspaudimus ir pan. (žemiau pateikiamos internetinės nuorodos, kur galima rasti *Anti-Spyware* programas).
- Įsitikinkite, kad svetainė, kurioje rašote konfidencialią informaciją, naudoja šifruotą duomenų perdavimo protokolą – https. Tokio puslapio adresas turi prasidėti ne http://, o https://, be to, naršyklės dešiniajame apatiniame kampe (dažniausiai tai priklauso nuo naršyklės tipo) atsiranda specialus ženklelis, kurį paspaudus galima patikrinti šifravimui naudojamą SSL sertifikatą.
- Reguliariai atnaujinkite operacinę kompiuterio sistemą, kadangi dažni atnaujinimai ištaiso esančias saugumo spragas (pavyzdžiui, *Microsoft Baseline Security Analyzer* (MBSA) patikrinimui, įdiegti naujausi atnaujinimai *Windows* operacinėje sistemoje).
- Domėkitės, kas vyksta elektroninėje erdvėje, kad galėtumėte suprasti jos procesus ir saugoti savo privatumą.

Kur kreiptis pagalbos?

- Gavę *phishing* laišką, turėtumėte apie tai pranešti bankui, kurio darbuotoju sukčius bando apsimesti. Bankas yra suinteresuotas gauti informaciją apie *phishing* atvejus.
- Jeigu supratote, kad įrašėte savo slaptažodžius ar mokėjimo kortelės duomenis į netikrą banko tinklalapį, turite nedelsdamas kreiptis į banką ir užblokuoti prieigą prie sąskaitų.
- Jeigu įtariate, kad jūsų pinigai buvo neteisėtai pasisavinti, kreipkitės į Nusikaltimų elektroninėje erdvėje tyrimo skyrių, tel. (8 5) 272 53 72, el. paštas cyberpolice@policija.lt

SPYWARE

Anglų kalbos terminu *Spyware* vadinama programinė šnipinėjimo įranga. Tai tokios programos, kurios, dažniausiai jums nežinant, renka informaciją apie lankomus tinklalapius, vartotojo vardą, elektroninio pašto adresus, programas ar bylas, esančias kompiuteryje, arba registruoja vartotojo atliekamus veiksmus internete (pvz., naudojantis banko sąskaitomis) ir siunčia šiuos duomenis tretiesiems asmenims (programų gamintojams ar kitiems suinteresuotiems asmenims) be vartotojo leidimo ir netgi be jo žinios.

Kodėl mus šnipinėja?

Pagrindinis šnipinėjimo programų tikslas yra surinkti ir išsiųsti duomenis apie vartotoją, informaciją apie jo pomėgius, lankomas svetaines internete ir kitą informaciją. Vėliau ši informacija *Spyware* kūrėjų gali būti panaudojama komerciniais, moksliniais ar nusikalstamais tikslais. Pavyzdžiui, surinkta informacija apie vartotojo pomėgius gali būti panaudota siunčiant reklamines žinutes pagal konkrečius vartotojo pomėgius, mėgiamas prekes ir pan. *Spyware* analogas *Adware* tampa reklaminiu įrankiu, pavyzdžiui, jis gali keisti pradinį internetinės naršyklės puslapį, atidarinėti iššokančius reklaminio turinio langus ir pan. Taip pat naudojantis *Adware* yra renkama informacija ir apie patį kompiuterį: apie operacinę sistemą, procesorių, atmintį, naudojamas programas kompiuteryje ir jų teisėtumą. Ypač pavojinga šnipinėjimo programų rūšis – **klavišų paspaudimus registruojančios programos** (angl. *Key Logging)*. Tai dar vienas informacijos vogimo būdų. Tokia programa stebi klavišų paspaudimus, juos registruoja, šią informaciją surenka į tam skirtą laikmeną ir ją perduoda į internetą. Pavojinga yra tai, kad, registruojant klavišų paspaudimus, gali būti surinkta konfidenciali informacija, pavyzdžiui, prisijungimų prie informacinių sistemų slaptažodžiai. Dar vienas šnipinėjimo programų pavyzdys – vadinamieji rinkikliai (angl. *dialer*), kurie automatiškai kuria skambinimo sujungimą ir jungiasi prie mokamų serverių per komutuojamas linijas, bet dabar vis mažiau vartotojų naudojasi šiuo ryšiu.

Kaip gauname šnipinėjimo programas?

Šnipinėjimo programos dažniausiai įdiegiamos šiais būdais:

- Kartu su „nemokama“ programine įranga, kurioje būna šnipinėjimo programos. Tokiu atveju vartotojas dažniausiai turi sutikti su gamintojo siūlomu, įmantriai parašytu teisėtumo išsižadėjimu arba EULA (angl. *End User License Agreement*). Pavyzdžiui, įdiegiant *Kazaa.*
- Su *ActiveX*, lankantis nepatikimose interneto svetainėse. Tokiu atveju dažnai naršyklė įspėja apie galimus saugumo pažeidimus, tačiau kai kurie vartotojai, nekreipdami į juos dėmesio, spaudžia *YES*.
- Įdiegiant naršyklės „pagalbinį priedą“, pavyzdžiui, papildomą įrankių juostą. Šis *Spyware* tipas vadinamas angliškuu terminu *Browser Hijacker.*
- Diegiant „nulaužtas“ programas arba naudojant „įsilaužimo“ programėles (angl. *crack*), kuriose gali būti *Spyware* programos.
- Kai kurie virusai gali įdiegti šnipinėjimo programas. Gerai žinomas pavyzdys *Trojan-Downloader*, kuris, be kitokių kenkėjiškų veiksmų, įdiegia šnipinėjimo programas.

Šnipinėjimo programinės įrangos kiekis sparčiai auga (pagal CA duomenis). Webroot duomenimis, 2005 m. I ketv. 87 proc. įmonių ir 88 proc. namų interneto vartotojų kompiuterių buvo apkrėsti *Spyware*. Pagal Webroot, šnipinėjimo programų kūrėjai per metus gauna 2 mlrd. JAV dolerių pelno. Pagal *Internet Advertising Bureau* duomenis, su *Spyware* generuojama beveik ketvirtis visos internetinės reklamos.

Kokius pavojus kelia *Spyware* programos?

- Surenkama privati informacija apie asmenį.
- Pavagiama konfidenciali informacija, pvz., slaptažodžiai, banko sąskaitų numeriai, verslo informacija, kreditinių kortelių duomenys ir panašiai.
- Iššokantys reklaminiai langai, paieškos rezultatų pakeitimas, vartotojo užklausų nukreipimas į kitas svetaines (angl. *DNS cache poisoning*).

- Apkraunamas kompiuteris ir interneto ryšio kanalas, sumažėja internetinės naršyklės ir bendras sistemos stabilumas bei našumas.
- Gali būti sudaryta galimybė apkrėsti sistemą.

Rekomenduojamos apsaugos priemonės

- **Reikia vengti *Spyware* programų**. Deja, dabartiniu metu daugelis interneto vartotojų neturi gilių informatikos srities žinių, diegia daug programų, atsiųstų iš interneto, naršo įvairiose svetainėse, jau nekalbant apie tai, kad didelę dalį interneto vartotojų sudaro vaikai.
- **Naudoti asmeniniams kompiuteriams skirtas programines kovos su *Spyware* priemones.** *Spyware Doctor* (pagal 2-spyware.com, suranda 91 proc., mokama), diegimo ir naudojimo instrukcija – www.2-spyware.com.
- *Spy Sweeper* (pagal 2-spyware.com, suranda 89 proc., mokama), diegimo ir naudojimo instrukcija – www.2-spyware.com.
- *Microsoft Defender* (pagal *2-spyware.com*, suranda 75 proc., laikinai nemokama). *Spybot Search and Destroy* (pagal *2-spyware.com*, suranda 82 proc., nemokama). *Ad-Aware SE* (pagal *2-spyware.com*, suranda 82 proc., *Professional* versija mokama, *Personal* nemokama, bet neturi apsaugos realiu laiku).
- Naudoti antivirusines programas.

Patarimai interneto prieigos (angl. *gateway*) lygmeniu

- Blokavimas pagal žymes (angl. *signature*) iš IDS ar IPS.
- URL (angl. *Uniform Resource Locator*) blokavimas iš tinklo užkardos (angl. *firewall*). *Spyware* protokolų blokavimas iš tinklo užkardos.

ELEKTRONINIO PAŠTO VIRUSAI

Elektroninio pašto virusai naudojasi pašto pranešimais, kaip transportavimo priemone, ir, automatiškai daugindamiesi, keliauja visais adresų knygelėje esančiais adresais.

Kompiuteriniai virusai persiduoda iš vieno kompiuterio į kitą, panašiai kaip ir realiame gyvenime biologiniai virusai nuo vieno žmogaus prie kito. Pavyzdžiui, ekspertų nuomone, kirminas *Mydoom* per vieną 2004 m. vasario dieną apkrėtė ketvirtį milijono kompiuterių. 1999 m. kovą virusas *Melissa* taip greitai plito, kad privertė *Microsoft* ir kitas stambias kompanijas visai išjungti elektroninį paštą, kol jis buvo likviduotas. 2000 m. virusas *Iloveyou* sukėlė tiesiog siaubingą efektą.

ŠNIPINĖJIMO PRIEMONĖS IR PROGRAMOS

Piktybiniai tinklalapiai stengiasi įtaisyti šnipinėjimo priemones į lankytojų kompiuterius. Šis *Screenshot Spam blog* paskatino apsaugos modernizavimo šuolį. Savo veikloje *Computing* skiria didelį dėmesį kovai su piktybiškomis šnipinėjimo programomis *spyware,* siekdamos jas visiškai sunaikinti arba bent jau pristabdyti plitimą. *Malware*. Kai programos išbandymui skirtas terminas eina į pabaigą, pasiūlo naują programą, kuri slapta kontroliuoja vartotoją. Tai kur kas daugiau, negu vien tik aprūpinimas programomis, tai

kompiuterio veiksmų perdavimas trečiųjų asmenų naudai. Labai paprastomis sąlygomis *spyware* tipo programa *Program* gali sekti kompiuterio vartotojo veiksmus ir persiųsti internetu *Internet* visą nukopijuotą informaciją. *Spyware* programa gali sukaupti daug ir įvairios informacijos apie vartotoją. Paprastesnės programos gali susekti, kokius tinklalapius vartotojas lanko, ir šią informaciją perduoti reklamos agentūrai. Sudėtingesnės versijos gali būti naudojamos piktybiniais tikslais ir įrašinėti viską, ką vartotojas parašo *Keystroke logging*, bandyti perimti slaptažodžius ir kreditinių kortelių duomenis. Visos kitos versijos skirtos reklaminiams skelbimams spausdinti ir persiųsti *Pop-up ad*.

ADWARE, ARBA REKLAMAVIMO PALAIKYMO PROGRAMA

Bet kuri programinė įranga *Computer software*, kuri automatiškai pradeda veikti, rodo arba įrašo reklaminę medžiagą į kompiuterį, kai tik ši programa įdiegiama arba kai ja bandoma pasinaudoti.

Adware – savarankiška programa arba veikia sujungta su kita vartojama programa. Tai paprastai naudoja programuotojai *Programmer*, kaip būdą susigrąžinti programavimo plėtrai skirtas išlaidas. Todėl kai kuriais atvejais ji gali būti teikiama vartotojui nemokamai arba už mažesnę kainą. Reklaminis priėjimas gali programuotojui suteikti galimybę ir skatinti jį rašyti, tobulinti ir aptarnauti programavimo paslaugą.

Kai kurios *Adware*, kaip ir *Shareware*, tariamai nemokamos arba bandomajam laikotarpiui skirtos programos *Shareware* tam, kad galima būtų tobulinti ir diferencijuoti. Norint atskirti *Adware* nuo kitos *Shareware*, visų pirma, reikia atminti, kad ši programa skirta reklamavimui. Vartotojams suteikiama teisė pasirinkti – užmokėjus registruoti arba licencijuoti programą ir baigti reklaminių skelbimų priėmimą.

Sukčiavimai kreditinėmis kortelėmis (Trojos arkliai, melagingi interneto tinklalapiai)

Phishing yra skirta rinkti interneto vartotojo asmeninę informaciją, pvz., kreditinės kortelės duomenis, slaptažodžius, tai tarsi maskuotė, suteikianti pasitikėjimą žmogumi. Žmonės, užsiimantys tokio pobūdžio apgavystėmis, sukčiavimais, vadinami *phisher***.** Jie siunčia savo potencialioms aukoms pranešimus, reikalaudami tikrinti savo bankų sąskaitas, nurodydami tinklalapį, labai panašų į banko. Faktiškai jie naudoja šią informaciją pasipelnymo tikslais. Kitas *phishing* panaudojimo būdas – gauti asmeninę informaciją, sukuriant į bankų svetaines panašius tinklalapius, ir nepatyrę žmonės lengvai suklysta. Lenkijoje vaikai, vyresni negu 13 metų, jau patys gali atlikti bankinius pavedimus – apmokėti paprasčiausias buitinių paslaugų sąskaitas, pavaduodami tėvus ar mokytojus bei auklėtojus. Tokiu būdu paauglys gali vienas valdyti sąskaitas, sudarinėti sandorius, reguliuoti savo asmenines išlaidas telefonu ar mobiliuoju telefonu. Tuo pat metu jaunimas tampa potencialiomis *phishing* aukomis, kai perduoda asmeninius duomenis ar asmens kodą fiktyviam bankui.

Prisiminkite: *phishing* naudoja *phishers* kaip pasipelnymo šaltinį. Jūs prarandate – jis uždirba.

Kaip išvengti

- Niekada nerašykite paštu prašomo slaptažodžio arba asmeninių duomenų.
- Niekada nespauskite www.link arba priedo prie jūsų elektroninio pašto pranešimo.
- Niekada neatidarinėkite nežinomų programų, rastų virtualioje erdvėje arba gautų iš kitų šaltinių. Naudokitės *anti-phishing* programa, kaip apsauginiu skydu *hardware* arba programine įranga *software*, kuri funkcionuoja virtualioje erdvėje *Computer network*, kad išvengtumėte kai kurių apsaugos draudžiamų komunikacijų. *Computer security* analoginė funkcija kaip ir *Firewall*, daugiau skirta *phishing* turiniui atpažinti internetiniame tinkle.

Website tinklalapyje ir elektroniniame pašte kovojanti su *spyware* uždaro daugelį piktybinių programų kategorijų. *Malware* sukurta tam, kad būtų galima perimti arba iš dalies kontroliuoti kompiuterio veiksmus, neinformuojant *Computer Informed consent* to mechanizmo savininko arba vartotojo. *Malware* tipo programos sukurtos siekiant perimti kompiuterio valdymo sistemą arba pakenkti vartotojui, jam nežinant. Programinio aprūpinimo sistema niekada nesiunčia elektroniniu paštu asmeninės informacijos, kreditinių kortelių duomenų, slaptažodžių. Visada rašo Jūsų www. banko adresą ir net protokolą https aiškindami, jog tikrina Jūsų banko balansą. Netikėkite tuo.

TROJOS ARKLIAI

Programinės įrangos *Computer software* kontekste Trojos arkliai – piktybinė programa, kuri užslėpta arba pridedama kaip priedas prie teisėtos programos. Pavadinimas paimtas iš klasikinio siužeto apie Trojos arklį (*Trojan Horse*). Ši programa gali pasirodyti naudinga arba įdomi, arba blogiausiu atveju nepavojinga neįtariam vartotojui, tačiau kenksminga dirbant. Dažnai trumpinamas pavadinimas iki *Trojinis* vien todėl, kad iš buvusio paverčiamas į esamą. Yra du tipai Trojos arklių. Vienas, skirtingai nuo kitų, atrodo patrauklus ir naudingas. *Software cracking* įsijungia piktybiškas programos rinkinys, kai tik pradeda veikti visa programa. Įjungus bet kokią programą, kartu įsijungia ir ši kenkianti programa. Antras tipas – autonominė programa, kažkas panašaus į žaidimą arba atskirą rinkmeną (dokumentų rinkinį) su tam tikrais vaizdais vartotojui apgauti. Tada programa pradeda vykdyti jai priskirtas užduotis.

Trojos arklių programos negali veikti pačios savarankiškai, skirtingai nuo kitų *Malware* virusinių *Computer virus*. Kaip graikų trojėnai įtempė arklį į tvirtovės teritoriją tam, kad įvykdytų sumanymą, taip Trojos arklių kompiuterinės programos priklauso nuo pasirinktos aukos veiksmų. Kadangi trojėnai kopijuoja ir perduoda informaciją, kiekviena nauja auka taip pat turi valdyti šią programą. Todėl skirtinga jų kenksmingumo išraiška, priklausanti nuo sėkmingo programos koncepcijos išpildymo, o ne nuo kompiuterio apsaugos sistemų ar konfigūracijos trūkumų *Social engineering*.

ĮSILAUŽIMAI

Tai piktybiškas nepageidaujamos informacijos siuntimas dideliais kiekiais bet kokiomis elektroninės komunikacijos priemonėmis. Pati paprasčiausia forma įtaisyta elektroninio pašto *Electronic mail*, kaip komercinės reklamos paštas.

Įsilaužimo tipai

- Ta pati informacija siunčiama daugybei adresų be jokios užklausos, žinant, kad siuntėjo pelnas padidės nepalyginamai su gavėjo pelnu;
- Komercinė uždrausta ES direktyva 2000/31/ES, neprašytas elektroninis paštas (ISE) ir nekomercinis elektroninis paštas (informacija).

Kaip kovoti su įsilaužimais

Vienkartinius įsilaužimus galima tiesiog ignoruoti. Apie nuolatinius įsilaužimus iš to paties adresato reikia pranešti jūsų interneto administracijai. Taip pat yra autonominė kompiuterinė programa, kurią galite įdiegti į asmeninį kompiuterį. Ji filtruoja ir saugo nuo nepageidaujamų elektroninio pašto laiškų. Tačiau turėtumėte žinoti, jog šios programos nėra tobulos, jos gali atmesti ir jūsų laukiamą laišką.

Būdai, kaip saugoti kompiuterį nuo trojėnų:

- pažeista *JavaScript* ir HTML jūsų pašto programa,
- pažeista automatinė pašto peržiūra,
- nuolatinis pašto sistemos modernizavimas,
- naudojate nenormatyvines pašto programas, dažniausiai kuriamas, tam, kad būtų apeitos ir moderniausios apsaugos sistemos,
- įdiegdami antivirusinę programą *anti-spyware*, nenurodykite savo pašto adreso.

Priemonių rinkinys (kompiuterinės programos)

Priemonių rinkinys, arba *dialer*, – kompiuterinė programa, kuri sudaro jungtį su internetu *Computer program* arba prie kitų kompiuterinių tinklų *Computer network*, analogišku telefonu *Telephone*. Paprastai priemonių rinkinys (programa) dirba be vartotojo pastangų, jam nežinant. Priemonių rinkinys (kompiuterinė programa), kuris pasirodo dažniausiai pornografiniuose puslapiuose, kenksmingas tik to tinklo vartotojams. Priemonių rinkinį (kompiuterinę programą) būtina sujungti su internetu, bent jau su paprasčiausiais tinklais *Broadband Internet access*, tačiau kai kurie iš jų skirti tik plačiajuosčiams interneto tinklams. Tokių priemonių rinkinių tiekėjai dažnai ieško vartotojo kompiuteryje apsaugos defektų *Software security vulnerability* ir panaudoja juos tam, kad vartotojas keistų kompiuterį, nes nuo parduotų kompiuterių skaičiaus didėja jų pelnas.

Kai kurie priemonių rinkiniai (kompiuterinė programa) praneša vartotojui, kad jie atlieka tik specialaus turinio informacijos siuntimą ir tik išrinktiesiems vartotojams. Tokio turinio pavyzdžiai gali būti programinė įranga kompiuterio perkrovimams MP3s MP3 (paprastai reikalavimų pažeidėjai), pornografija ir labai retai slapta informacija, naikinanti panašiai kaip virusai.

Pastaruoju metu tariami „programuotojai“ kreipiasi į programų kūrėjus, kurie prisijungia be vartotojo žinios prie jų kompiuterinių sistemų, kad padėtų atlikti sukčiavimus *Fraud*.

Piktybiškas kompiuterines programas (virusai, įsilaužimai, pornografija ir kt.) galima identifikuoti tokiais būdais:

- kompiuterio perkrovimas *Uploading and downloading* ir tuomet suveikia *Pop-up ad*, ji įsijungia, kai tik bandote įsijungti internetą;
- tinklalapyje yra nežymus priminimas apie kainą;
- tinklalapis pradeda krautis, net jeigu jūs bandote jo atsisakyti, paspaudėte „Atšaukti“;
- kompiuterinė programa jungiasi kaip nemokama, be jokio paaiškinimo;
- kompiuterinė programa atlieka nepageidaujamą susijungimą be vartotojo nuorodos;
- kompiuterinė programa be jokios pirkimo kainos, tik prijungimo numeris;
- labai sunkiai pašalinama ir ištrinama kompiuterinė programa.

Ypatingi gąsdinimai

Viena populiariausių gąsdinimo priemonių *cyber kiber,* kuriai naudojami internetiniai ryšiai, elektroninis paštas, mobilieji telefonai, tekstinės žinutės, diskredituojantys tinklalapiai. Ja siekiama pasityčioti arba nuolat terorizuoti individą ar grupę, naudojami asmeniniai antpuoliai arba kitos kompiuterinio nusikaltimo priemonės. Ypatingi gąsdinimai, vienkartiniai ir pasikartojantys, teikia žalą elektroninio teksto būdu. Žinoma keletas *cyber* gąsdinimo būdų, tačiau visi jie turi keletą bendrų savybių.

Cyber bulling gali prasidėti internete ir baigtis realiame gyvenime. Šiuo atveju chuliganas ir auka paprastai nesusitinka realiame gyvenime ir nepažįsta vienas kito. Šis įžeidimų tipas gali prasidėti nuo „ugnelės“ arba nekaltų diskusijų pokalbių kambariuose. „Ugnelė“ – įžeidžiantis arba provokuojantis kreipinys, išsiųstas paštu arba paskelbtas interneto forumuose, paprastai pareikšta nuomonė, kuri sukelia neigiamą reakciją. Žmogus, išsiuntęs paštu užgauliojimą, laukia, kol jam atsakys, o nesulaukęs – pakartoja tą patį. Chuliganas *cyber* (žmogus, kuris vykdo internetinį persekiojimą) pradeda siuntinėti elektroniniu paštu užgauliojančius pranešimus, norėdamas įžeisti ir padaryti moralinę žalą pasirinktai aukai arba reiškiniui. Šis persekiojimo tipas paprastai tęsiasi neilgai, nes chuliganas nepažįsta aukos, kaip žmogaus, ir jeigu auka nebereaguoja į tokius išpuolius, chuliganui pabosta visa tai ir jis pasirenka kitą auką arba užgauliojimo būdą.

Kitas ***cyber bulling*** tipas pavojingesnis ir žalingesnis, kai chuliganas ir auka yra pažįstami arba buvo susitikę. Tokiu atveju išpuoliai tampa labiau asmeniški ir skaudesni aukai. Gąsdinimai *cyber* gali būti ilgalaikiai, pereinantys į realų gyvenimą, arba atvirkščiai. Kartais chuliganai sukuria specialius internetinius tinklalapius, skirtus aukoms, kur jie pateikia įžeidžiančių pranešimų, ne tik aukos, bet ir jos šeimos ar draugų asmeninę informaciją ir nuotraukų. Žinomi faktai, kad tokie tinklalapiai egzistavo ištisus mėnesius ar net metus, kol apie tai sužino auka. Yra atvejų, kai interneto tinklalapiuose chuliganai ieško bendraminčių, rengia kampanijas prieš pasirinktą auką (vaiką) arba sudaro „pralaimėjusių“ sąrašus. Suaugusiam *cyber bulling* nelabai pavojingas, kadangi nėra fizinių veiksmų ar žalos. Tačiau vaikui, kurio protinis išsivystymas labai trapus, tokia patirtis gali sukelti depresiją, nepasitikėjimą, paskatinti atsiskyrimą nuo bendraamžių ir draugų. Tai gali turėti neigiamos įtakos vaiko ateičiai. Reikalai pakrypsta dar blogesne linkme, jeigu vaikas „auka“ ir chuliganas mokosi toje pačioje mokykloje arba yra iš vieno kiemo, dažnai susitinka realiame gyvenime. Tada įžeidinėjimai ir grasinimai tampa kasdieniu reiškiniu. Tokiu atveju auka negali jaustis saugi nei kieme, nei mokykloje, nei namuose. Chuliganas pažeidžia aukos asmeniškumo ribas ir menkina jo saugumo jausmą net ir namuose.

Norėdami apsaugoti vaikus nuo internetinio persekiojimo *cyber bulling*, turite išaiškinti apie visus galimus pavojus, su kuriais vaikai gali susidurti virtualioje erdvėje. Vaikas turi suvokti, kad geras ir kultūringas elgesys svarbus ne tik realiame gyvenime, bet ir virtualioje erdvėje. Tokiu būdu jūs apsaugosite vaiką ir jis netaps atsitiktinio chuligano auka, mokės atsispirti iššūkiams, bendraudamas su potencialiu chuliganu.

Be to, asmeniniame namų kompiuteryje patariame įdiegti filtravimo programą. Naudodamiesi šia programa, galėsite lengvai blokuoti asmenį, bandantį įžeidinėti jūsų vaiką, ir nutraukti internetinį persekiojimą. Jeigu chuliganas užsispyręs ir toliau erzina ir persekioja jūsų vaiką, siuntinėja užgauliojimus iš įvairių pašto adresų, neleidžia jūsų atviram vaikiškam paštui būti nežinomam, pasirinkite elektroninio pašto programą, kuri filtruoja ir leidžia gauti laiškus tik iš sąraše nurodytų klientų. Nors ir ne kokia idėja, tačiau galite paprašyti vaiko leidimo skaityti užgauliojančius chuligano laiškus. Iš jų jūs galite sužinoti chuligano gyvenamąją vietą, kitą informaciją ir išsaugoti juos, kaip vėlesnių veiksmų ir teisminio ieškinio pagrindą, jeigu elektroninis grasinimas pereina į rimtą grėsmę. Jeigu ir jums rimtai grasinama, galite kreiptis į policiją.

Ypač svarbu žinoti, ar jūsų vaikas realiai buvo susitikęs su chuliganu ir kaip gerai jie vienas kitą pažįsta. Tai pagrindas jūsų tolesniems veiksmams. Jeigu jūsų vaikas nebuvo susitikęs su chuliganu realiame gyvenime ir vienas kito nepažįsta, labai svarbu to išvengti. Jūs turite išaiškinti savo vaikui, kad jokiu būdu nepasakytų namų adreso, telefono numerio, mokyklos ar kitų duomenų, kurie padėtų chuliganui susirasti jūsų vaiką ne internete. Nors ir retai, tačiau pasitaiko, kai chuliganai būna labai pikti ir kerštingi ir visais įmanomais būdais stengiasi surasti savo auką, toliau tyčiotis ir persekioti realiame gyvenime.

Jeigu jūsų vaikas pažįstamas su chuliganu, paprašykite parodyti, supažindinti su persekiotoju. Kai žinosite, kas jis, galite užmegzti kontaktą su jo tėvais. Kartais tėvai nežino, ką veikia jų vaikas internete. Kai jūs pranešite chuligano tėvams apie jų vaiko elgesį, tikėtina, kad jie padės jums išspręsti šią problemą ir imsis visų priemonių, kad sustabdytų netinkamą vaiko elgesį. Paprastai šito pakanka, tačiau kartais tėvai negali patikėti, kad jų vaikas šitaip elgiasi, todėl turite juos įtikinti ir visa tai įrodyti. Čia jums padės visa išsaugota informacija: elektroniniai laiškai iš jo pašto dėžutės, telefoniniai skambučiai, žinutės ir visa kita informacija, kuri identifikuos jį, kaip chuliganą.

Būna atvejų, kai chuliganas internete sukuria tinklalapį, kuriame talpina nuotraukas, komentarus, aukos ir jo šeimos įžeidinėjimus. Kartais aukos netgi nežino apie tokius tinklalapius. Blogiausia tai, kad šie tinklalapiai internete gali būti ilgus metus ir visiems prieinami. Šiuo atveju neįmanoma ištaisyti klaidos patiems, reikia kartu su chuliganu ir jo tėvais kreiptis į serverio administraciją, kuriame yra sukurtas tinklalapis, ir prašyti pagalbos. Paprastai kompanijos pasirašo geros praktikos sutartis, todėl susitarti dėl tinklalapio likvidavimo turėtų būti nesunku.

Taip pat turėtumėte žinoti, kad ne visada vaikas noriai kalbasi su tėvais apie savo nemalonumus ir problemas. Iš jūsų vaiko galbūt ištisus mėnesius ar metus tyčiojosi ir jį įžeidinėjo, kol jūs apie tai sužinojote. Norėdami išvengti tokių situacijų, turite stebėti savo vaiko elgesį, nes kiekvienas pasikeitimas (uždarumas, draugų vengimas, irzlumas) gali būti užgauliojimų ir persekiojimų rezultatas. Reikia gerai pažinti savo vaikus, palaikyti gerus draugiškus santykius, žinoti, kur, kada ir su kokiais draugais jie bendrauja.

Kitos interneto grėsmės

Keletas internetinių problemų, nepanašių į seksualines ar ekonomines. Viena iš jų – „tekstų rinkiniai“. Kai kurie tinklalapiai, klubai daro tam tikros ligos ar elgesio kultą, ir visa tai pateikia kaip rimtą medicininę išvadą. Toks turinys gali išgąsdinti nekaltai užklydusį vaiką. Dar viena problema – tai neofašizmas. Pasaulyje keletas labai stiprių organizacijų platina tokio pobūdžio informaciją daugelyje interneto tinklalapių ir pokalbių kambarių. Tinklalapiai, kuriuose pateikiama kryptingo turinio informacija, tačiau negali būti priskirti prie rasizmą ar nacizmą propaguojančių tekstų, laisvai egzistuoja toliau. Blogybė ta, kad tekstuose ir istorijose pateikiama iškreipta ir tikrovės neatitinkanti informacija apie etnines problemas ir organizacijas. Ypač vaikus reikia saugoti nuo vadinamo *scarification,* arba tinklalapių, kuriuose pateikiama kūno ar organų modifikacijos pavyzdžiai. Tokių tinklalapių autoriai lankytojams ir svečiams prisistato kaip labai protingi ir išsilavinę žmonės. Deja, jie siūlo vaikams labai pavojingas, žalingas ir netgi mirtį skatinančias žinias. Keletas pavyzdžių iš panašaus turinio tinklalapių, kai vadovybės nuotraukos paverčiamos lavonais, kūnais be odos, atskiros kūno dalys derinamos prie turimų nuotraukų. Šie tinklalapiai paskutiniuoju metu labai plačiai pasklidę virtualioje erdvėje. Keletas tinklalapių siūlo nemokamai kompaktinius diskus arba filmus su tokio turinio informacija ir nuotraukomis.

Vėliausias nepageidautinas interneto tinklalapių pavyzdys – masinė terorizmo psichozė. Milžiniški tinklalapiai sujungti į vieningus mazgus LVS, yra ir individualūs serveriai, kurie siūlo tokią informaciją, mokymus, kaip tapti teroristu, kaip namų sąlygomis pasigaminti sprogmenų, arba pateikia filmuotą žmogžudysčių medžiagą, sulėtinant žiauriausius momentus.

Filtravimo programos

Parengtas priemonių paketas, kuriuo naudodamiesi tėvai, pedagogai, bibliotekininkai ir kiti pasirinktų vaikų poreikius atitinkantį turinį, identifikuotų ir filtruotų informaciją.

Pastaruoju metu prieinamos technologijos, kurios atlieka šešių tipų veiksmus, grindžiamus teksto turiniu: pasiūlykite filtravimo paiešką, praneškite, kontroliuokite, įspėkite ir blokas.

⚠ ***PASIŪLYTI***

REKOMENDUOKITE PRITAIKYTI VAIKAMS SKIRTĄ INFORMACIJĄ

Didelė vaikiško turinio tinklalapių, knygų ir brošiūrų įvairovė. Papildomai kai kurios filtravimo programos pateikia vaikiškų tinklalapių sąrašą, kuriais galima naudotis. Pasiūlymų pavyzdžiai: *Yahooligans*!, Amerikos bibliotekų asociacija, didieji tinklų serveriai *Bonus.com*, mikroschemų maršrutai 6–16 ir *CyberYES* sąrašas, geltonųjų puslapių tinklas.

⚠ ***SĄRAŠO FILTRAVIMAS***

PARINKITE VAIKAMS TINKAMĄ INFORMACIJĄ, APIMANČIĄ JIEMS AKTUALIUS KLAUSIMUS

Daug paieškos sistemų filtruoja suaugusių teminio turinio informaciją. Tai pripažįstama kaip pranašesnė filtravimo programa jų kompanijose. Patraukli sutartinė kaina ir marketingo strategija, kurios tikslas – pritraukti kuo daugiau tėvų ir jų vaikų ir išjudinti visą sistemą. Informaciją blokuoja *Google.com*, *Altavista.com*.

⚠ ***PRANEŠTI***

NURODYKITE INFORMACIJOS TURINĮ

Filmų pavadinimai, pristatymai ir kiti turinio aprašymai padės tėvams ir kitiems vaikų priežiūros darbuotojams kontroliuoti interneto turinį. Tačiau ši informacija bus naudinga tik tuo atveju, jei bus lengvai prieinama. Kai kurios programos sukurtos tam, kad pateiktų informaciją apie turinį, kai tik vartotojas bando prie jo prieiti. Ši informacija gali būti pateikta grafiškai, tinklalapyje, kaip baneris ar kita programine išraiška. Pavyzdžiui, *TRUSTe* rodo *trustmark,* kurie tinklalapiuose turi pripažintus slaptumo tipus. *EvaluWeb* rodo banerio tinkamumą atitinkamai amžiaus grupei ir net puslapių dalis tinklalapiuose. Internetinių tinklų apžvalgą atlieka *Alexa*, kartu pateikiama ir papildoma antraeilė informacija apie tinklalapį.

⚠ ***KONTROLIUOTI***

VĖLESNĖ VARTOTOJO TURINIO SĄRAŠO APŽVALGA

Daugelis filtravimo mechanizmų taip pat įjungia kontrolės funkciją. Pavyzdžiui, ieškiklis *Cyber* kontroliuoja visą veiklą internete tuo metu, kai vaikas juo naudojasi. Suaugęs „administratorius“ gali peržiūrėti, kokia informacija vaikas naudojosi, kokiuose tinklalapiuose ir pokalbių kambariuose lankėsi, kokius el. laiškus išsiuntė. Kita programa filtruoja, savavališkai registruoja visus mėginimus pažeisti „administratoriaus“ nurodymus.

⚠ ***ĮSPĖTI***

PATEIKITE TURINIO INFORMACIJĄ IR REKOMENDUOKITE

BLOKUOTI NETINKAMĄ TURINĮ

Įspėjamosios programos prieš atverčiant tinklalapį praneša, kad netinkamas turinys. Šios priemonės gali būti naudingos, kai netikėtai atsiverčia netinkamo turinio tinklalapis. Daugelis suaugusiųjų tinklalapių įjungia vaizdinį įspėjimą apie pagrindinį tinklalapį, kuris įveda į kitus šalutinius tinklalapius, netinkamus vaikams iki 18 metų. *Microsoft* kompiuterinė programa, kuri atlieka interneto apžvalgą ir skirta netinkamo turinio informacijai blokuoti, taip pat gali atlikti ir įspėjimo funkciją įrašant slaptažodį. Tėvai gali pasakyti vaikui slaptažodį, kurį įrašę jie galės naudotis internetu ir filtruota informacija. Tokiu būdu vaikai bus įspėjami, kad turinys netinkamas, tačiau gali naudotis, jeigu jie taip nori. Svarbiausia yra tėvų ir vaikų santykių problema sprendžiant internetinį saugumą, kadangi jaunimas labiau išprusęs ir tėvai gali pasirodyti kaip neraštingi kalbant apie kompiuterinius reikalus.

PADĖTIS

Aukščiau pateiktos programinės įrangos gali būti išdėstytos įvairiose asmeninės kompiuterinės sistemos vietose arba su įgaliojimu prieinamose interneto vietose ar tinklalapiuose.

ASMENINIS KOMPIUTERIS

Programų išdėstymas asmeniniame kompiuteryje gali palengvinti jo konfigūraciją administratoriui ar mokytojui. Patys vaikai, be tėvų žinios, gali perkonfigūruoti programas, esančias kompiuteryje. Kai kurių PC gaminių paskirtis – išvengti trukdymų. Daugelį PC programų reikia modernizuoti, tačiau įsijungus internetinį tinklą modernizavimas vyksta automatiškai. Programinės įrangos, kurios gali judėti kompiuteryje, įjungia *Cyber* paiešką ir apsaugą.

VIETINIŲ TINKLŲ UGNIASIENĖ ARBA VIETINĖ APSAUGA

Programinės įrangos išdėstymas LAN arba įgyvendinant vietinio serverio pasitikėjimą gali būti naudingas sprendimas mokyklų ir bibliotekų PC internetiniuose tinkluose. Centralizuota konfigūracija naudingesnė ir lengviau pritaikoma administravimo sistemoje negu individualiems įsibrovėliams. Kompiuterinės programos, kurias galima valdyti LAN arba vietiniams įgaliotiems serveriams įjungia kontrolės programas: *CyberPatrol*, *Bess*, *Cyber Snoop*, *I-Gear*, *NetNanny*, *SafeSurf Internet Filtering Solution*, *SmartFilter*, *SurfControl*.

INTERNETO TEIKIMAS IR APTARNAVIMAS

Interneto paslaugų teikėjai faktiškai nepajėgia kontroliuoti organizacijų ir individualių vartotojų naudojamos milžiniško kiekio informacijos. Kai kurie ISP paslaugų paketai specialiai paruošti vaikams. ISP gali kontroliuoti ir filtruoti internetą arba riboti prisijungimą prie pokalbių kambarių, telekonferencijų ar panašių paslaugų. ISP programų, kurios valdo AME įrenginius, pavyzdžiai: *netFilter*, *SurfControl*.

PAIEŠKŲ SISTEMOS

Kai kurios paieškos sistemos skirtos vaikams ir jaunimui. Pavyzdžiui, *Google* arba *AltaVista* sukurti taip, kad nerodytų suaugusiems skirto turinio informacijos.

TINKLALAPIAI

Tinklalapių įvairumas į turinių sąrašą įtraukia ir vaikams skirtus tinklalapius. Kai kurie tinklalapiai turi etiketes (logotipus), grafiką ir kitus turinio aprašus, padedančius tėvams parinkti tinkamo turinio informaciją. Internetinius tinklalapius vertina asociacija ICRA – tarptautinė nekomercinė interneto lyderių organizacija, dirbanti saugaus interneto plėtros srityje. Operatyvios informacijos tiekėjai išsiaiškina, kokie anketinės apklausos elementai (temos) yra pateikiami jų tinklalapiuose. Tuomet sukuriamas mažas failas (informacijos paketas), turintis etiketę (pavadinimą), kuris atitinka informacijos turinį vienoje ar keliose srityse. Tokiu būdu vartotojai, ypač mažų vaikų tėvai, gali pasinaudoti filtravimo programa tam, kad leistų arba uždraustų prisijungti prie tinklalapių su atitinkamos informacijos etikete. Svarbiausia tai, kad asociacija interneto turiniui vertinti nesinaudoja informacijos tiekėjo turinio vertinimu (grupavimu), o tai atlieka ICRA rūšiavimo (atrankos, filtravimo) sistema. ICRA žodynas sudarytas iš kelių temų kategorijų, pavyzdžiui:

- ar yra nuogumų,
- ar yra seksualinio turinio teksto,
- prievartos aprašymų,
- vartojama kalba,
- ar yra vartotojo nurodyto turinio,
- kito žalingo turinio tekstų, azartinių žaidimų, narkotikų ar alkoholio aprašymų.

Atitikimas užsakovo reikalavimams

Interneto filtravimo priemones sudaro platus reguliavimo variantų diapazonas, įskaitant ir reguliavimo mechanizmus, leidžiančius ar blokuojančius sąrašus pagal raktinį žodį ar frazę tam, kad būtų nustatyta turinio kategorija ir išaiškėtų, ar reikia turinio neatitikimo blokavimo, įspėjamojo pranešimo, ar jungtis prie registracijos, ar atlikti kitą veiksmą. Į aukštos kokybės ir atsakingai parinktas programas tuo pat metu gali kreiptis daugybė įvairių poreikių turinčių klientų.

Klasifikacija

Nepriklausomai nuo to, kokie pasirinkti mechanizmų veiksmai, būtini turinio atrankai arba identifikavimui, vis tiek jie yra specifinio pobūdžio. Bet kuriai turinio klasifikavimo sistemai svarbu žinoti, kas atlieka klasifikaciją ir kokius kriterijus naudoja šiems tikslams.

KAS IR KAIP

Klasifikacija atlikta šiais būdais.

✕ **Operatyvinės informacijos tiekėjų** ICRA ir *SafeSurf* sistemų pavyzdžiai, skirti operatyvinės informacijos tiekėjų filmų atrankai.

✕ **Nepriklausomi ekspertai.** Daugelis filtravimo kompanijų naudoja informacinių specialistų (tėvų ir mokytojų) klasifikacijos turinio komandas. Tai AME, *Becc*, *Bonus.com*, *Cyber*, *SurfControl*.

✕ **Vietiniai administratoriai.** Tėvai, mokytojai ar kiti suinteresuoti asmenys turi asmeniškai nuspręsti, kokio turinio informacija gali būti prieinama jų prižiūrimiems vaikams. *Cyber* paieškos sistema ir ieško, ir peržiūri ieškomus vietinių administratorių pavyzdžius. Žinoma, gali pasitaikyti tikrinimo mechanizmo klaidų, kurias pastebi dispečeris.

✕ **Tinklalapių specialistai ir tiekėjai. Bendradarbiavimas.** Viena iš atviros informacinės visuomenės privilegijų yra ta, kad galima išsakyti savo nuomonę dėl informacijos turinio ir ja pasidalyti su kitais, kurie taip pat turi teisę vertinti jūsų informaciją ar nuomonę. Tai tinka ne tik teisėto turinio informacijai, bet ir kitos kategorijos nepageidaujamai informacijai. Turime prisiminti, kad ne visa nepageidaujamo turinio informacija yra neteisėta. Žinoma, etika, kultūros stoka, interneto saugumas – globalios problemos, tačiau pagrindinės moralinės vertybės yra nuolatinės ir privalomos.

✕ **Apžvalga arba nuomonė.** Vienas kūrinių (produkto) klasifikacijos būdų – apžvalga arba nuomonės. Šis būdas naudojamas kelių organizacijų restoranų ir filmų klasifikacijai. Neseniai šį būdą pradėjo naudoti *Ned Šeferd* pasaulinė nuomonių tyrimų tarnyba. *Ned Šeferd* sukūrė „vertintojų bendruomenę“ – žmonių grupę, kurie vertina ir klasifikuoja informacijos turinį, o gaunami rezultatai verti apdovanojimų.

✕ **Automatizuotos programos.** Automatizuotos programos padeda klasifikuoti pokalbių turinį. Kai kurios iš šių programų, pvz., *evaluWeb,* nuolat naudojamos veiksmingai klasifikacijai, kadangi vartotojas to reikalauja. Kitų tipų programos naudojamos tam, kad padėtų žmoniškiesiems klasifikatoriams aptiktus įtartinus tinklalapius blokuoti. Naudojama ir kita turinio klasifikavimo programinė įranga *netFilter*.

Klasifikacijos schema

Klasifikacijos schemos gali būti skirtos vaikams „tinkamo“ arba „netinkamo“, arba ir tokio, ir tokio turinio informacijai identifikuoti. Turinys gali būti klasifikuojamas pagal jo tinkamumą tam tikrai amžiaus grupei, pasirinkto tipo pagrindu arba tam tikrais turinio elementais, arba pagal tai, kas kūrė turinį, t. y. valstybinis ar nevalstybinis informacijos šaltinis.

Kas gali Jums padėti

Valstybinės organizacijos

Vaiko teisių apsaugos kontrolierius. Vaiko, jo teisių ir teisėtų interesų apsauga – vienas svarbiausių valstybės ir visuomenės uždavinių. Nors per pastarąjį šimtmetį požiūris į vaikus, kaip į labiausiai pažeidžiamus visuomenės narius, labai pasikeitė, taip pat buvo nemažai nuveikta vaiko teisų apsaugos srityse, tinkama vaiko teisių ir jo teisėtų interesų apsauga ir gynimas vis dar yra pagrindinis valstybės uždavinys. **http://vaikams.lrs.lt/informaciniai/apie%20nauja%20istatyma.htm**

Pagal Lietuvos Respublikos Konstituciją Seimas ir Prezidento institucija nustato valstybės politiką vaiko teisių apsaugos srityje, o Vyriausybė užtikrina šios politikos įgyvendinimą. Kiekvienas ministras atsako už jam pavestą valstybės valdymo sritį. Socialinės apsaugos ir darbo ministerijai Lietuvos Respublikos Vyriausybės 2003 m. vasario 6 d. nutarimu Nr. 194 priskirta vaiko teisių apsaugos valdymo sritis ir nustatyta kitų ministerijų kompetencija. **http://www.socmin.lt/index.php?796824077**

Vidaus reikalų ministerija. Siekiant stiprinti visuomenės saugumą ir teritorinių policijos įstaigų bendradarbiavimą, vykdant nepilnamečių elgesio kontrolę ir teikiant jiems socialinę pagalbą, 2005 m. rugsėjo 12–23 d. Lietuvos Respublikos teritorijoje vykdyta prevencinė priemonė „Nepilnametis“.

Socialinė pagalba. Valstybinę šeimų ir vaikų rėmimo sistemą sudaro dvi pagrindinės dalys: nepriklausomai nuo šeimos turto ir pajamų mokamos pašalpos bei mažas pajamas turinčioms šeimoms teikiama parama įvertinus jų pajamas. **http://www.socmin.lt/index.php?1216440096**. Kiekvienoje savivaldybėje ir mokykloje dirba socialiniai darbuotojai, kurie sprendžia socialines vaikų problemas.

Nevalstybinės organizacijos

http://www.sos-kaimas.lt/

SOS vaikų kaimo šeimos koncepcija paremta keturiais principais: kiekvienam vaikui reikia motinos, jis auga natūraliai kartu su savo broliais ir seserimis, savo namuose, palankioje kaimo aplinkoje.

http://www.ppc.lt/ http://www.globa.lt/
„Vaikai internete“

http://vaikams.lrs.lt/

Vaiko, jo teisių ir teisėtų interesų apsauga – vienas svarbiausių valstybei ir visuomenei keliamų uždavinių. Nors per pastarąjį šimtmetį požiūris į vaikus, kaip labiausiai pažeidžiamus visuomenės narius, labai pasikeitė ir nemažai nuveikta vaiko teisių apsaugos srityse, tinkama vaiko teisių ir jo teisėtų interesų apsauga ir gynimas vis dar yra pagrindinis valstybės uždavinys.

http://www.policija.lt/viesoji/index.php?page_id=134

Siekiant stiprinti visuomenės saugumą, nepilnamečių, esančių Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos (toliau – Kalėjimų departamentas) regionų pataisos inspekcijų ir joms pavaldžių teritorinių pataisos inspekcijų (toliau – pataisos inspekcijos) įskaitoje, recidyvinio nusikalstamumo prevencijos, aktyvesnio pataisos inspekcijų ir teritorinių policijos įstaigų bendradarbiavimo, vykdant nepilnamečių, kuriems

teismo nustatyti draudimai ar paskirti įpareigojimai, elgesio kontrolę, bei teikiant jiems socialinę pagalbą, 2005 m. rugsėjo 12–23 d. Lietuvos Respublikos teritorijoje bendru Kalėjimų departamento direktoriaus ir Lietuvos policijos generalinio komisaro 2005 m. rugsėjo 6 d. įsakymu Nr. 4/07-171/5-V-530 buvo vykdoma prevencinė priemonė „Nepilnametis“.

http://www.lijot.lt/index.php?language=lt&page=19

Lietuvos jaunimo organizacijų taryba (LiJOT) – didžiausia nevyriausybinė jaunimo organizacija Lietuvoje, vienijanti nacionalines jaunimo organizacijas ir regionines jaunimo organizacijų sąjungas.

http://www.smm.lt/visi_projektai.htm, http://www.draugiskamokykla.lt/lt.php, http://www.drasinkimeateiti.lt, http://www.mtp.smm.lt/, http://www.pvc.lt/, http://www.draugiskasinternetas.lt/lt – vaikams skirtų interneto tinklalapių adresai.

Užtikrinti Lietuvos vaikų dvasinę gerovę, teikiant psichologinę paramą, atsižvelgiant į kiekvieno vaiko ir šeimos unikalumą; įtraukiant ir mokant savanorius, vykdant švietimo, sveikatos apsaugos, teisėtvarkos, socialinio darbo specialistų švietimą ir bendradarbiaujant su kitomis pagalbą vaikams teikiančiomis institucijomis.

http://www.saugus-vaikas.lt/

Rizikos grupės vaikų sveikos gyvensenos įgūdžių ugdymo ir psichikos sveikatos stiprinimo programa, finansuojama Kauno m. savivaldybės, kviečia pasinaudoti nemokama specialistų pagalba – patyrusiems smurtą, išgyvenantiems krizę, netekusiems tėvų globos vaikams Saugaus vaiko centre teikiama individuali psichologinė pagalba, rengiami grupiniai užsiėmimai.

http://paramoscentras.w3.lt/

Šios programos tikslas – teikti informaciją ir techninę pagalbą neįgaliems vaikams, jų tėvams ir pedagogams. Vaikai su fizine negalia turi ribotas galimybes judėti, bendrauti ir gauti reikalingą informaciją. Internetas ir kompiuterinė technika padėtų spręsti šias problemas ir prisidėtų prie neįgalių vaikų integracijos į visuomenę bei švietimo. Šiuo metu kuriama programos dalyvių el. konferencija, skatinamas jų bendravimas su kitais naujosiomis technologijomis besinaudojančiais vaikais, kompiuterinis raštingumas, kuris vėliau praverstų neįgaliems asmenims ieškant darbo.

http://www.indigo.home.lt/

Indigo – tai tokie **vaikai**, kurių auros yra krištolinės spalvos. Masiškai Indigo **vaikai** ėmė gimti maždaug apie 2000 metus.

http://www.jieznovaikai.lt/lt.php

„Jiezno vaikai“ rūpinasi beveik šimtu našlaičių ir vaikų iš asocialių šeimų, gyvenančių Jiezno vaikų globos namuose. Tai 3–18 metų mažai kam reikalingi ir daug skausmo patyrę vaikai. Fondas nori paskatinti juos mokytis ir tobulėti, domėtis savo ateitimi ir tapti visavertėmis asmenybėmis. Fondo prioritetas – vaikų švietimas ir visokeriopas jų lavinimas.

http://www.sos-vaikai.lt/main.php?id=1&lang=lt

Į SOS **VAIKAI** globą patenkančių vaikų gyvenimo istorijos yra labai įvairios.

http://mintys.lt/tevai_ir_vaikai.php

Meilės alimentai. Aš vėl noriu būti šešių. Tiems, kas mano, kad tėvai jiems skolingi. Erma Bombek „Tėtis po lova“. Tai, ką girdėjome, kai buvome **vaikai.**

http://www.pastoge.lt/vaikai

Čia patenka **vaikai**, kuriems nesaugu savo šeimoje. Į „Pastogės“ centrą patenkantys **vaikai** dažniausiai yra patyrę smurtą, apleisti.

Metodinė medžiaga ugdytojams apie interneto saugumą

Įvadas

Ši metodinė medžiaga parengta projekto „Initial application of an educational strategy measures on children internet safety“, finansuoto Europos Komisijos *Socrates* programos lėšomis, įgyvendinimo metu.

Projekto tikslai:

- paskatinti suaugusiųjų švietimą apie efektyvią vaikų apsaugą nuo galimo neigiamo interneto poveikio;
- bendros ugdymo metodikos kūrimas (mokymai, metodinė medžiaga);
- partnerių – organizacijų darbuotųjų bendrųjų kompetencijų, šviečiant visuomenę (mokytojus, tėvus ir t. t.), kėlimas;
- nemokamos prieigos prie metodinės medžiagos, aktualios informacijos interneto saugumo tema, užtikrinimas (visą informaciją galima rasti interneto svetainėje www.onechildprotection.org).

Projektą koordinuoja Bulgarijos nacionalinė vartotojų organizacija. Projekte dalyvaujančios organizacijos partnerės – Lietuvos nacionalinė vartotojų konfederacija, Lenkijos vartotojų asociacija, Slovakijos vartotojų organizacijų asociacija ir Čekijos vartotojų gynimo asociacija.

Metodinės medžiagos paskirtis – prisidėti keliant ugdytojų kompetenciją saugaus interneto srityje. Tai priemonė, apibendrinanti partnerių patirtį, sukauptą įgyvendinant projektą. Medžiaga gali būti naudojama organizuojant mokymus tėvams, mokytojams, psichologams arba kitiems suinteresuotiems asmenims. Tokie mokymai gali būti organizuojami nevyriausybinių organizacijų, vietos valdžios atstovų, bendruomeninių centrų ir / arba mokyklų. Galima parsisiųsti ir elektroninį medžiagos variantą savišvietai.

1 TEMA.

Kaip suprasti, kad vaikas gali tapti žalingo interneto poveikio auka

KLAUSIMAI

1. Kuris iš išvardintų požymių rodo, kad vaikui gali išsivystyti priklausomybė nuo interneto:
   A) vaikas skundžiasi, kad jam dirgina akis,
   B) vaikas naršo internete 1–1,5 val.,
   C) nugaros skausmai.

2. Kurios amžiaus grupės vaikams kyla didesnė rizika tapti seksualinio išnaudojimo auka:
   A) 12–15 metų,
   B) 8–10 metų,
   C) 16–18 metų.

3. Kurios grupės vaikai turi mažiausiai šansų būti neigiamai paveikti interneto:
   A) vaikai, rūpestingai prižiūrimi tėvų,
   B) vaikai, linkę į agresiją, provokuojančiai besielgiantys,
   C) ramaus būdo vaikai.

4. Kuri iš išvardintų komunikacijos priemonių dažniausiai naudojama interneto pažeidėjų:
   A) el. paštas,
   B) pažinčių svetainės,
   C) bendravimo kambariai.

UŽDUOTIS DISKUSIJAI

Aptarkite mokytojo, psichologo ir tėvų funkcijas bei vaidmenis ribojant laiką, kurį vaikas naršo internete.

UŽDUOTYS

Išdėstykite pagal didėjančią rizikos grėsmę šiuos požymius:

- vaikas neturi draugų,
- vaikas internete naršo daugiau negu 1,5 valandos,
- vaikas slepia, kuo jis užsiima internete,
- vaikas vis labiau tolsta nuo savo senų draugų.

Paaiškinkite savo pasirinkimą.

ATVEJIS

Kaip reaguotumėte į namus gavę siuntinį, kurio siuntėjo vaikas nenorėtų nurodyti.

2 TEMA.
Kompiuteris ir interneto technologijos

KLAUSIMAI

1. Ką reiškia terminas „*multimedia*“ *informacija:*
   A) tekstas, pateiktas kartu su nuotraukomis,
   B) tekstas, pateiktas kartu su nuotraukomis, vaizdo ir garso klipais, animacija,
   C) „multimedia“ – tai interneto svetainė.

2. Kuo tinklalapis skiriasi nuo naršyklės:
   A) tinklalapiai įjungiami naudojantis naršykle,
   B) nėra jokio skirtumo,
   C) naršyklėse galima rasti nuorodų į tinklalapius.

3. Ką bendro turi ICR, ICQ, MSN *Messenger*, *Skype* ir *Yahoo Messenger:*
   A) jomis naudodamiesi žmonės iš viso pasaulio, prisijungę prie interneto, gali bendrauti realiuoju laiku,
   B) el. pašto dėžutės,
   C) serveriai.

4. Kokie yra pagrindiniai VOIP (skambučiai internetu) privalumai:
   A) galima naudoti dideliu atstumu,
   B) nemokama paslauga,
   C) kaina priklauso nuo nustatyto mokesčio už interneto paslaugą.

UŽDUOTIS DISKUSIJAI

Jūsų manymu, ar etiška skaityti vaiko el. laiškus, siekiant užtikrinti jo saugumą. Ar šiuo atveju vaiku verta pasitikėti?

UŽDUOTYS

- Prisijunkite prie interneto 20 minučių ir sudarykite paieškos sistemų sąrašą.
- Naudodamiesi paieškos sistemomis, sudarykite sąrašą tinklalapių, skirtų interneto saugumui užtikrinti.

ATVEJIS

Jūsų vaikas skundžiasi, jog nepažįstamas žmogus atsiuntė jam nuorodą į tinklalapį, tačiau paspaudus ją antivirusinė programa blokuoja prieigą prie to tinklalapio. Ką Jūs darysite?

3 TEMA.
Galimos grėsmės, naudojantis internetu

KLAUSIMAI

1. Informacija internete:
   A) labai gausiai pateikiama ir nevisa tinka Jūsų vaikui,
   B) kelia pavojų vaiko saugumui, todėl vaikui turi būti uždrausta naudotis internetu,
   C) visiškai nenaudinga vaikui, neatitinka jo poreikių.

2. Ar vaiko asmeninės informacijos viešinimas internete gali kelti pavojų:
   A) taip, nes niekas nežino, kokiais tikslais ta informacija yra renkama,
   B) taip, nes vaikas gali neatskirti, kokia informacija gali būti skirta viešinimui, o kokia – ne,
   C) ne.

3. Kas yra el. agresija:
   A) bandymas perkelti virtualųjį bendravimą į realybę,
   B) pašto dėžutės blokavimas siunčiant *spam,*
   C) agresijos proveržiai, emocinė prievarta el. pokalbių kambariuose.

4. Rizikos, kurią kelia internetas:
   A) galima išvengti, jeigu vaikas naudosis internetu prižiūrimas tėvų,
   B) galima išvengti, jeigu ugdoma vaiko atsakomybė už savo veiksmus ir sąmoningumas,
   C) yra per daug, geriausia apsaugos priemonė – uždrausti vaikui naudotis internetu.

UŽDUOTIS DISKUSIJAI

Papasakokite atvejų, kai buvo kilusi reali grėsmė internete.

UŽDUOTIS

Sudarykite grėsmių, kylančių naudojantis internetu, sąrašą, išdėstykite didėjančia eilės tvarka ir pagrįskite savo pasirinkimą.

ATVEJIS

Jūsų vaikas gavo el. pranešimą, jog laimėjo loterijoje 1 mln. litų. Norint gauti pinigus reikia pateikti asmeninę informaciją ir banko sąskaitos duomenis, iš kurios bus išskaičiuotas administracinis 200 litų mokestis. Vaikas suteikė prašomą informaciją ir papasakojo apie tai Jums. Grupėse aptarkite šį atvejį.

4 TEMA.
Rizikos specifika, atsižvelgiant į amžiaus grupes

KLAUSIMAI

1. Vaikas iki 7 metų:
   A) priklauso amžiaus grupei, kuriai kyla mažiausia rizika patekti į seksualinių išnaudotojų internetu akiratį,
   B) yra per mažas, nesidomi internetu,
   C) turi būti prižiūrimas suaugusiųjų, kai naudojasi internetu, nes negali atskirti, kuri informacija jam tinkama, o kuri – ne.

2. Rizika 7–10 metų vaikui būti seksualiai išnaudotam internetu nėra didelė, nes:
   A) tokio amžiaus vaikai internetu naudojasi prižiūrimi tėvų, ir tai žino psichikos sutrikimų turintys žmonės (pedofilai),
   B) tokio amžiaus vaikai dar neturi rašymo ir skaitymo įgūdžių,
   C) tokio amžiaus vaikai nesidomi internetu.

3. Pedofilų akiratyje atsiranda:
   A) naivūs vaikai, tikintys viskuo, kas jiems yra sakoma,
   B) vaikai, turintys polinkį rizikuoti, išbandyti kažką naujo, smalsūs,
   C) vaikai, norintys būti nepriklausomi, subrendę, todėl sąmoningai ieškantys iššūkių.

4. Vaikai, patenkantys į 16–18 metų grupę:
   A) yra pakankamai subrendę ir nebelieka rizikos, kad jie teiks asmeninę informaciją nepažįstamiesiems,
   B) labiausiai linkę dalytis asmenine informacija (ypač susijusia su finansais) bei gali būti paveikti informacijos, propaguojančios rasizmą, neapykantą, valgymo sutrikimus ir pan.,
   C) priklauso didesnės rizikos grupei negu 11–15 metų vaikai.

UŽDUOTIS DISKUSIJAI

Aptarkite tėvų ir mokytojų darbo su vaiku specifiką pagal skirtingas amžiaus grupes, siekiant užkirsti kelia pavojams.

UŽDUOTIS

Aprašykite, kuo internetas gali būti naudingas įvairioms amžiaus grupėms.

ATVEJIS

Įsivaizduokite, kad turite 5 ir 17 metų vaikus. Ar leistumėte vyresniajam vaikui prižiūrėti jaunėlį, kai pastarasis naudojasi internetu.

5 TEMA.
Pedofilija

KLAUSIMAI

1. Pedofilija – tai:
   A) psichikos sutrikimas,
   B) prisirišimas prie vaiko,
   C) mada, propaguojama interneto.

2. Kuri vaikų grupė gali būti labiausiai veikiama išorinių veiksnių:
   A) vaikai, kurių puikūs mokymosi rezultatai, sportuojantys, prižiūrimi rūpestingų tėvų,
   B) uždaro būdo vaikai, iš probleminių šeimų, nestabilios psichikos,
   C) vaikai, turinys daug draugų, praleidžiantys daug laiko gatvėse, rūkantys.

3. Koks pedofilų tikslas:
   A) padėti vaikui mokytis,
   B) užmegzti kontaktą su vaiko tėvais,
   C) užmegzti kontaktą su vaiku.

4. Kaip elgtis, jei turite įtarimų, jog pedofilas užmezgė kontaktą su Jūsų vaiku:
   A) reikia rimtai pakalbėti su vaiku ir paaiškinti galimas grėsmes,
   B) reikia uždrausti vaikui naudotis internetu,
   C) reikia nubausti vaiką.

UŽDUOTIS DISKUSIJAI

Pagal ką galima atpažinti pedofilą:

- kalbą,
- elgesį, išsiskiriantį iš kitų pokalbių kambaryje esančių žmonių,
- intencijas, užuominas,
- bandymą sužinoti kuo daugiau asmeninės vaiko informacijos.

UŽDUOTIS

Sudarykite sąrašą situacijų, kada kyla rizika vaikui sutikti pedofilą internete.

ATVEJIS

Vaikas skundžiasi, jog internetu bendrauja su gana agresyviai nusiteikusiu nepažįstamu pašnekovu, kurio elgesys ganėtinai keistas. Jums aišku, kad vaiko pašnekovas – pedofilas. Kokie tolesni Jūsų veiksmai?

6 TEMA.
Virusai, *Spyware, Adware*

KLAUSIMAI

1. Kompiuterinį virusą galima parsisiųsti:
   A) per el. laiškus, parsiųstas rinkmenas, infekuotas bylas,
   B) per *Spyware,*
   C) kraunant interneto puslapius.

2. *Spyware* naudojimas gali kelti grėsmę, nes:
   A) atidaro langus ir nuorodas, kurių Jūs net nebandėte arba nenorėjote atidaryti,
   B) nutraukia normalų kompiuterio darbą,
   C) „stebi“, ką Jūs spausdinate, ir siunčia duomenis iš Jūsų kredito kortelės.

3. Ar *Adware* gali sukelti tokią pat grėsmę, kaip ir virusas:
   A) ne, *Adware* nekenkia sistemai kaip virusas,
   B) taip, ir virusas, ir *Adware* kenkia vienodai, bet *Adware* pasekmės rimtesnės,
   C) taip, ir virusas, ir *Adware* kenkia vienodai.

4. Geriausia antivirusinė programa yra:
   A) ta, kuri brangiausiai kainuoja,
   B) kurios teisiškai pripažintas statusas,
   C) kurią galima labai dažnai atnaujinti.

UŽDUOTIS DISKUSIJAI

Prašome išvardyti ir aptarti grėsmes kompiuteriui, kurias gali kelti virusas.

UŽDUOTIS

Paieškokite internete antivirusinių, *antispyware* programų.

ATVEJIS

Kai išjungiate kompiuterį, pasirodo pranešimas, teigiantis, kad Jūsų kompiuteris užkrėstas viruso. Jūs neturite programos, kuri tokiu būdu praneštų apie užkrėtimą. Kai paspaudžiate ant pranešimo, atsidaro nežinomas tinklalapis. Ar galite paaiškinti, kas atsitiko.

7 TEMA.
Atsiskaitymo banko kortele grėsmės

KLAUSIMAI

1. Kuris naudojimosi kreditine kortele būdas gali kelti pavojų:
   A) kai kompiuteryje išsaugoma informacija apie banko kortelę ir sąskaitą,
   B) kai bankas neseniai pakeitė kortelę,
   C) kai internetu perkami brangūs daiktai.

2. Nemalonumai, kurių gali pridaryti vaikas, turėdamas informacijos apie banko kortelę:
   A) gali išleisti didelę sumą nereikalingiems daiktams,
   B) gali būti pavogta tapatybė,
   C) bankas gali skirti sankcijas.

3. Pareiškimas, jog „atsiskaitymas kreditine kortele yra vienintelis įmanomas būdas perkant internetu“, yra:
   A) klaidingas,
   B) teisingas.

4. CVC kodas yra:
   A) 3 ženklų kodas, būtinas darant pavedimus internetu,
   B) asmeninis pirkėjo slaptažodis, atsiskaitant kortele,
   C) banko, išdavusio kortelę, kodas.

UŽDUOTIS DISKUSIJAI

- Aptarkite naudojimosi atsiskaitymo kreditine kortele internetu privalumus ir trūkumus.
- Kai Jūs duodate kortelę savo vaikui, ką Jūs jam aiškinate?

UŽDUOTIS

Sudarykite sąrašą asmenų, kuriems leistumėte naudotis savo banko kortele. Paaiškinkite savo pasirinkimą.

ATVEJIS

Jūsų kortele buvo pasinaudota be Jūsų žinios. Sužinote, kad Jūsų vaikas, pasinaudojęs ja, išleido nemažą pinigų sumą linksmybėms su draugais. Tolesni Jūsų veiksmai.

8 TEMA.
Phishing, Trojos arklio virusas, *spam*

KLAUSIMAI

1. *Phishing* – tai galima grėsmė, kuri įgyvendinama per:
   A) informaciją tinklalapiuose, išoriškai panašiuose į bankų tinklalapius,
   B) siuntinėjant virusais užkrėstus el. laiškus,
   C) tai informacijos, susijusios su Jūsų banko kortelės duomenimis, išaiškinimas, naudojantis specialia programine įranga.

2. Kai gaunate el. laišką su prisegtu priedu nuo nepažįstamo siuntėjo, Jūs:
   A) parsisiunčiate priedą ir atidarote jį,
   B) niekada neparsisiunčiate .zip arba .rar failų, jeigu jų siuntėjas arba priedo turinys Jums nežinomas,
   C) Jūs naudojate antivirusines, *antiphishing* programas, todėl jaučiatės apsaugoti nuo galimos grėsmės.

3. Kuris iš išvardytų teiginių apie Trojos arklio virusą yra teisingas:
   A) šiuolaikinė antivirusinė programa gali be problemų atpažinti šį virusą ir apsaugoti nuo jo,
   B) šiuolaikinė antivirusinė programa gali be problemų panaikinti Trojos arklio viruso pasekmes kompiuterio sistemai,
   C) egzistuoja Trojos arklio viruso rūšių, kurių gali neatpažinti antivirusinės programos.

4. Kas yra *spam*?
   A) reklaminio pobūdžio laiškai, nuolat siuntinėjami į Jūsų pašto dėžutę,
   B) būdas blokuoti nepageidaujamus adresatus,
   C) reklaminio pobūdžio laiškų blokavimas.

UŽDUOTIS DISKUSIJAI

Sugalvokite ir aptarkite būdus, kaip apsisaugoti nuo *spam*.

UŽDUOTYS

- Išvardinkite būdus, kaip galima apsisaugoti nuo *spam*.
- Išvardinkite požymius, pagal kuriuos galima nuspręsti, kad Jūsų kompiuteris užkrėstas Trojos arklio virusu.

ATVEJIS

Jums paskambina iš mokyklos ir praneša, kad kompiuteris, kuriuo naudojasi Jūsų vaikas, užkrėstas Trojos arklio virusu. Kokie Jūsų veiksmai?

9 TEMA.
„Dialeriai“

KLAUSIMAI

1. Kas yra „dialeriai“ (angl. *dial* – skambinti):
   A) programinė įranga, pvz., ICR, ICQ, MSN *Messenger* arba *Skype*, kuria naudojantis galima bendrauti su visu pasauliu,
   B) programinė įranga, kuria nusikaltėlis gali be vartotojo žinios prisijungti prie laidinio telefono,
   C) programinė įranga, kuri leidžia naudotis ypatingo turinio tinklalapiais (pvz., nemokamomis mp3 bylomis).

2. Kuris iš išvardintų prisijungimo prie interneto būdų kelia didžiausią riziką tapti „dialerių“ auka:
   A) ADSL,
   B) Broadband,
   C) telefono linija / modemas.

3. Kam kyla didžiausia rizika tapti „dialerių“ auka:
   A) tėvams,
   B) vaikams,
   C) ir tėvams, ir vaikams.

4. „Dialerio“ per mėnesį sukelta žala gali siekti:
   A) daugiau negu 700 Lt,
   B) iki 350 Lt,
   C) iki 700 Lt.

UŽDUOTIS DISKUSIJAI

Aptarkite, kokios valstybinės institucijos ir tarnybos gali padėti apsisaugoti nuo „dialerių“.

UŽDUOTYS

- Išvardinkite būdus, kaip nusikaltėlis gali užkrėsti Jūsų kompiuterį „dialerio“ programine įranga.
- Išvardinkite programas, kurios gali apsaugoti nuo „dialerių“.

ATVEJIS

Jūs gaunate telefono sąskaitos išklotinę, kurioje matyti telefono skambučiai į Filipinus ir Panamą. Kokie Jūsų veiksmai?

10 TEMA.
El. agresija, pirkiniai internetu

KLAUSIMAI

1. Kas yra „flame“ (angl. *flame* – žara):
   A) provokatorius, ieškantis el. agresijos (*bullying*) aukos,
   B) pokalbių kambariai, kur praktikuojama el. agresija,
   C) provokuojantys pranešimai, kurių tikslas – sukelti neigiamą pokalbių kambarių dalyvių atsaką.

2. El. agresija (*bullying*):
   A) nekelia pavojaus, nes agresorius asmeniškai nepažįsta savo aukos,
   B) gali kelti pavojų, nes agresorius ir auka gali susitikti realiame gyvenime,
   C) pastovus *spam* siuntinėjimas į Jūsų pašto dėžutę.

3. Kas yra „mail client“:
   A) programinė įranga, kuriai veikiant gaunate laiškus tik iš žmonių, įtrauktų į kontaktų sąrašą,
   B) programinė įranga, kuria naudodamiesi nusikaltėliai gali siųsti laiškus iš skirtingų adresų,
   C) pokalbių kambarys, kur galima sutikti daug agresorių.

4. Kai vaikas parodo Jums provokacinį el. laišką, Jūs:
   A) iš karto jį ištrinate,
   B) išsaugote kaip įkaltį, kad galėtumėte panaudoti vėliau,
   C) draudžiate vaikui naudotis internetu.

UŽDUOTIS DISKUSIJAI

Išvardinkite būdus, kuriais gali pasinaudoti el. agresoriai.

UŽDUOTIS

Aptarkite, ką reikia daryti, siekiant apsaugoti vaiką nuo el. agresijos.

ATVEJIS

Gaunate šokiruojančio turinio pranešimą apie save, kai esate el. pokalbių kambaryje. Pranešimą perskaito ir kiti pokalbių kambario dalyviai. Jūsų veiksmai?

II TEMA.
Mąstymo formavimo grėsmės – anoreksija, neonacizmas, kūno modifikacijos

KLAUSIMAI

1. Anoreksija – tai:
   A) apetito nebuvimas,
   B) psichologinis sutrikimas,
   C) emocinis išsekimas.

2. Kokiais metodais naudojasi neonacistai, kad paveiktų savo ideologija vaikus:
   A) įdomūs paveikslėliai,
   B) politinių teorijų išaiškinimas paprasta kalba,
   C) klaidingų faktų pateikimas, siekiant iškreipti realybę.

3. Kuo gali būti pavojingas internetas, kai kalbama apie kūno modifikacijas (plastines operacijas, auskarų vėrimą, tatuiruotes ir t. t.):
   A) informacija, kaip tai galima atlikti namų sąlygomis,
   B) bendraujama su asocialiais asmenimis,
   C) informacija apie kūno modifikacijas.

4. Kas nėra kūno modifikacijos:
   A) auskarų vėrimas,
   B) kūno atletika,
   C) vegetarizmas.

UŽDUOTIS DISKUSIJAI

Ar anoreksija gali būti paveldima? Kokie veiksniai gali sukelti anoreksiją? Aptarkite.

UŽDUOTIS

Išvardinkite pavojingiausius kūno modifikavimo būdus, apie kuriuos informacijos vaikas gali rasti internete.

ATVEJIS

Vaikas praneša Jums, kad nori implantuoti magnetą po pirštu oda. Jūsų reakcija.

12 TEMA.
Filtrai

KLAUSIMAI

1. Kokios yra filtrų (kaip programinės įrangos) funkcijos:
   A) mažina riziką užsikrėsti virusu,
   B) saugo vaikus nuo naudojimosi nepadoraus turinio tinklalapiais,
   C) atlieka tas pačias funkcijas, kaip ir paieškos sistemos.

2. *google.com* ir *altavista.com* yra:
   A) tinklalapiai vaikams,
   B) paieškos sistemos, kurios turi filtrą, kad apsaugotų vaikus nuo naudojimosi nepadoraus turinio tinklalapiais,
   C) nepadoraus turinio tinklalapiai.

3. *Alexa* – tai:
   A) paieškos sistema, kuri atsirenka nepadoraus turinio paieškos rezultatus,
   B) paieškos sistema, kuri turi filtrą, saugantį vaikus nuo naudojimosi nepadoraus turinio tinklalapiais,
   C) tinklalapiai su papildoma vaizdine informacija.

4. Programos *Cyber Snoop*, *Bess* ir *CYBERsitter* skirtos:
   A) kurti aplankytų tinklalapių archyvą, siekiant išsiaiškinti jų turinį,
   B) programos, kurios siunčia įspėjimus, jeigu tinklalapis yra nerekomenduojamas vaikams,
   C) programos, kurios blokuoja priėjimą prie tam tikrų tinklalapių.

UŽDUOTYS DISKUSIJAI

- Kas, Jūsų nuomone, yra „padorumo kriterijus“ kalbant apie informaciją internete?
- Ar, Jūsų nuomone, yra normalu, kai vaikas turi kompiuterį su interneto prieiga savo kambaryje?

UŽDUOTIS

Per *google.com* paieškos sistemą (anglų kalba) įrašykite žodį „sex“, pasirinkite funkciją rodyti paveikslėlius („images“). Ar, Jūsų nuomone, tokie vaizdai tinkami vaikams? Pasirinkite funkciją „ModerateSafeSearch is on“ -> „Safe Search filtering“, pažymėkite „Do not filter my search results“, paspauskite „Safe preferences“. Pažiūrėkite į paveiksliukus ir aptarkite, ar tokie vaizdai tinka vaikams žiūrėti.

ATVEJIS

Jums įėjus į kambarį vaikas staiga užverčia tinklalapio langą. Jūsų reakcija?

13 TEMA.
Institucijos

KLAUSIMAI

1. Į kurią instituciją kreiptumėtės pajutę grėsmę savo ir vaiko gyvybei ir sveikatai:
   A) Vidaus reikalų ministeriją,
   B) Vaiko teisių apsaugos tarnybą,
   C) Vaikų liniją.

2. Kokiu būdu geriausia pateikti prašymą vaiko teisių apsaugos institucijai:
   A) raštu,
   B) žodžiu (susitikus),
   C) telefonu.

3. Kokios institucijos daugiausia dėmesio skiria vaikų apsaugai nuo žalingo interneto poveikio:
   A) nevyriausybinės organizacijos,
   B) mokykla,
   C) valstybinės institucijos.

4. Interneto kavinėse, klubuose turi būti uždraustas prisijungimas prie nepadoraus turinio tinklalapių:
   A) taip,
   B) teisė apsispręsti turi būti suteikta kavinėms ir klubams,
   C) ne.

UŽDUOTIS DISKUSIJAI

Kaip turėtų dirbti valstybinės vaikų teisių apsaugos institucijos, kad būtų skirta daugiau dėmesio vaikų apsaugai nuo žalingo interneto poveikio?

UŽDUOTIS

Išvardinkite institucijas ir organizacijas, kurios galėtų prisidėti kovojant su žalingu interneto poveikiu vaikui.

ATVEJIS

Jūsų vaikas bendrauja su ES piliečiu, kuris, pasirodo, yra pedofilas. Kaip spręsite šią problemą? Atsižvelkite į ES teisinę sistemą, skirtumus tarp atsakingų institucijų ir organizacijų struktūros.

Teisingi atsakymai

1 tema. Atsakymai:	**1 – B**	**2 – A**	**3 – C**	**4 – A**
2 tema. Atsakymai:	**1 – B**	**2 – A**	**3 – A**	**4 – B**
3 tema. Atsakymai:	**1 – A**	**2 – A**	**3 – C**	**4 – B**
4 tema. Atsakymai:	**1 – C**	**2 – A**	**3 – C**	**4 – B**
5 tema. Atsakymai:	**1 – A**	**2 – B**	**3 – C**	**4 – A**
6 tema. Atsakymai:	**1 – A**	**2 – C**	**3 – A**	**4 – C**
7 tema. Atsakymai:	**1 – A**	**2 – B**	**3 – B**	**4 – A**
8 tema. Atsakymai:	**1 – A**	**2 – B**	**3 – C**	**4 – A**
9 tema. Atsakymai:	**1 – B**	**2 – C**	**3 – C**	**4 – A**
10 tema. Atsakymai:	**1 – C**	**2 – B**	**3 – A**	**4 – B**
11 tema. Atsakymai:	**1 – B**	**2 – C**	**3 – A**	**4 – C**
12 tema. Atsakymai:	**1 – B**	**2 – B**	**3 – C**	**4 – A**
13 tema. Atsakymai:	**1 – A**	**2 – A**	**3 – B**	**4 – A**