Kompiuterių virusai. Antivirusinės programos ir kompiuterio apsauga nuo virusų.

Kompiuterių virusas yra programa, kuri savarankiškai trikdo kompiuterio programų darbą bei keičia kompiuteryje esančią informaciją.

Virusas yra kompiuterinio kodo dalis, kuri prisijungia prie programos ar failo, kad galėtų plisti iš kompiuterio į kompiuterį kartu su siunčiama programa ar failu. Virusai gali sugadinti jūsų techninę ar programinę įrangą ar failus.

Virusų atsiradimas

- Pirmieji virusų prototipai buvo žaidimų programos, kurios stengdavosi sudoroti priešininkų programas ir užimti jų vietą atmintinėje.
- Drauge su žaidžiančiomis programomis ėmė rastis programos, kurios nepriklausomai nuo vartotojo noro pakeisdavo jo vykdomų programų veiksmus. Tai virusinės programos – virusai.
- Pirmasis IBM asmeninių kompiuterių virusas buvo užregistruotas 1985 m. Jis buvo pavadintas EGABTR vardu, nes jis buvo skirtas sugriauti kompiuterio, turinčio EGA tipo vaizduoklį, darbą.

Viruso veikimas

- Virusas pradeda veikti, kai paleidžiama kokia nors programa, prie kurios tas virusas buvo „prikibęs“. Bet kuriuo momentu virusas gali perimti valdymą ir, atlikęs kenkėjiškus veiksmus, valdymą grąžina vykdomai programai.
- Yra virusinių programų, kurios pasislepia kitose programose, tačiau nesidaugina, o tik reguliariai atlieka kenkėjiškus veiksmus, pavyzdžiui, nuolatos spausdina įvairius pranešimus, žodžius arba skaičius.
- Kai kurios virusinės programos gali tūnoti kompiuteryje ilgą laiką ir pradėti veikti esant kokioms nors aplinkybėms. Pavyzdžiui, virusas CIH (vadinamas Černobylio) atgyja ir ima veikti balandžio 26 dieną.

Virusų veikimo pasekmės

- Virusuotos programos visiškai nustoja veikti arba blogai veikia;
- Trikdomas vartotojo darbas: spausdinami įvairūs pranešimai, ekrane pasirodo įvairūs ženklai;
- Sulėtėja sistemos darbas;
- Sumažėja vietos kompiuterio pagrindinėje atmintinėje bei diskuose;
- Modifikuojami ar kitaip sugadinami duomenys byloje;
- Sunaikinama informacija diskuose, gali būti net suženklinamas visas diskas prarandant jame buvusią informaciją
- Fiziškai sugadinami kai kurie kompiuterio įrenginiai.

Virusų klasifikacija

- Beveik nekenksmingi, nedarantys įtakos kompiuterio darbui, tačiau krečiantys įvairius pokštus;
- Nelabai kenksmingi, iš esmės netrikdantys kompiuterio darbo, tačiau mažinantys atmintinės talpą;
- Kenksmingi, trikdantys kompiuterio darbą, stabdantys vartotojų programas;
- Labai kenksmingi, naikinantys programas, duomenis, kompiuterio darbui reikalingą informaciją.

Pagal veikimo pobūdį visus virusus galima suskirstyti į 3 dideles grupes:

1. **plintančias kartu su programomis bei bylomis**. (Šie virusai vadinami bylų virusais. Dažniausiai pažeidžia bylas, turinčias pritvardžius: *.bat, *.com, *.exe, *.sys, *.lib, *.obj, *.dot, *.doc. Ypač pavojingi būna vykdomųjų bylų *.exe ir *. Com virusai. Jie įsiterpia į bylą ir pakeičia bylos pradžią taip, kad pirmosios tos bylos komandomis tampa viruso komandos.
2. **užgrobiančius diskelio ar disko pirmąjį – įkelties– sektorių**. Įkelties virusai užkrečia diskelių ar diskų įkelties (angl. boot) sektorius. Virusas jame esančią informaciją perkelia kitur, o ten įrašo savo programą. Kai sisteminė įkelties programa nuskaito įkelties sektoriaus turinį, tai ji perkelia į pagrindinę atmintinę viruso programą ir perduoda jai valdymą. Tada virusas pradeda įvairiai modifikuoti operacinės sistemos darbą.
3. **plintančius kompiuterių tinklais**. (tarptautinės kompiuterių saugumo asociacijos duomenimis apie 80 procentų visų infekcijos atvejų užkrečiama elektroninio virusais. Neretai minimi polimorfiniai virusai., kurie plisdami kaskart patys save pakeičia.

Kirminai

Tai elektroniniu paštu ar bendravimo kanalais plintančios ir labai sparčiai besikopijuojančios programos, kurios bemat užima kompiuterio darbinę atmintinę ir paplinta po visą kompiuterių tinklą. Kirminai dokumentų kompiuteryje neužkrečia, bet rimtai sutrikdo kompiuterio ir tinklų veikimą. Kirminai dažniausiai būna pridėti prie elektroninių laiškų ir paleidžiami atvėrus laiško priedą.

Trojos arkliai

Taip vadinamos kompiuterinės programos, paslėptos kitose esą naudingose programose. Trojos arkliai patys neplinta, tačiau naudojasi interneto vartotojų smalsumu ir patiklumu. Parsisiuntus ir paleidus kokią nors tarsi naudingą programą, pradeda veikti ir joje glūdintis Trojos arklys, kuris dažniausiai kompiuterį padaro prieinamą visiems ar tik konkretiems interneto įsilaužėliams. Tuomet šie įsilaužėliai gali įsibrauti į kompiuterį, gauti jame saugomus duomenis, netgi valdyti kompiuterį ir juo pasinaudoti atakoms prieš kitus kompiuterius.

Apsauga nuo sukčių ir apgavikų

Jei jūs gavote žinutę, kurioje pasiūlymas skamba per daug gerai, kad tai būtų tiesa, tikriausiai taip ir yra. Miesto legendos ir melagingos pagyros gyvuoja ištisus amžius, bet jų populiarumas vis dar toks pat, nes internetu platinti melagingas žinutes yra labai paprasta.
Nusikaltėliai suprato, kad internetu jie galės vogti jūsų tapatybę ir sukčiauti, kartais net labai kūrybingai įtraukiant pokalbių realiuoju laiku elementus, šnipinėjančią programinę įrangą ir atitraukiant jūsų dėmesį. Iki šiol jūs turbūt girdėjote apie duomenų vagystes (phishing arba vishing) ir žinote, kad negerai užkibti ant meškerės. Tai daugiau nei erzinančios nepageidaujamos elektroninės žinutės. Tokiu būdu gauta informacija gali būti panaudota jūsų kredito kortelės numerio, slaptažodžio, sąskaitos informacijos ar kitų asmeninių duomenų vagystei. Kita nauja sukčiavimo programa yra „pharming“ (kai apgavikai sugadina sistemas tam, kad nukreiptų jus į konkrečias svetaines), kuri panaši į „phishing“ , nes ja taip pat siekiama pavogti jūsų tapatybę. Pagrindinis skirtumas tarp jų toks, kad pastaroji renka asmeninę informaciją apie jus per netikrą tinklalapį, kuris atrodo kaip tikras.

Kaip apsaugoti kompiuterį nuo „spyware“ ir „adware“

„Spyware“ - tai gana nauja šnipinėjimo programa, bet gana intensyviai ir atkakliai plintanti. Tiesą sakant, kai kurie tyrimai rodo, kad net 88% kompiuterių užkrėsti nepageidautinomis šiai kategorijai priskirtinomis programomis. Taigi kas yra „spyware“? Tai bendrai vartojamas terminas programinei įrangai apibūdinti, kuri atlieka tam tikrus veiksmus, tokius kaip reklamavimas (žinoma kaip „adware“), renka asmeninę informaciją ar keičia jūsų kompiuterio konfigūraciją be jūsų sutikimo. Kaip ir kirminai bei virusai, šnipinėjimo programinė įranga yra kompiuteriui kenkianti programa („malware“), bet ji nesielgia kaip tipinis virusas ar „kirminas“. Ji dažniausiai nepridaro jokios žalos kompiuteriui, išskyrus tai, kad sugriauna jo darbą, ir nebeplinta naudodamasi jūsų adresų knygute. Jūsų kompiuteryje gali būti šnipinėjimo ar kitos nepageidaujamos programinės įrangos, jei jūs matote iššokantį reklamos langą, nors ir nesate prisijungę prie tinklo, arba jei jūsų nustatytas interneto puslapis pasikeičia be jūsų leidimo, atsiranda naujos įrankių juostos ir jūs negalite jų atsikratyti, jūsų kompiuteris visiškai sulėtėja arba užlūžta.

Venkite nepageidaujamų elektroninio pašto žinučių (spam)

Naujausi tyrimai parodė, kad 80 procentų ar net daugiau visų išsiųstų laiškų sudaro nepageidaujamos elektroninio pašto žinutės. Stulbinantys skaičiai! Vis dėlto jūs matote tik dalelytę šio srauto. Dauguma interneto paslaugų teikėjų ar elektroninio pašto programų turi elektroninių „šiukšlių“ filtrus, kurie tarnauja kaip priešakinė gynybos linija, sauganti nuo nepageidaujamų elektroninio pašto žinučių.
Jūs galite pasinaudoti technologijomis, kurios padėtų susidoroti su nepageidaujamomis žinutėmis, kurios šiuos filtrus apeina. Jūs turite keturis galingus įrankius, kurie gali padėti sulaikyti nepageidaujamų žinučių antplūdį.

Makrovirusai

Šie virusai apkrečia įvairiomis raštinės programomis sukurtus dokumentus, pavyzdžiui, beveik visus Microsoft Office programų dokumentus. Jei atveriant apkrėstą dokumentą programoje būna neuždraustas makrokomandų vykdymas, tada virusas kopijuojamas į kitus atvertus dokumentus bei dokumentų šablonus. Nuo šablonų užkrečiami visi naujai kuriami dokumentai.
Interneto svetainėse gali būti kenkėjiškų *Java*, *JavaScript* bei *ActiveX* programėlių. Pakanka aplankyti tokią svetainę, ir žalinga programa parsiunčiama į kompiuterį bei pradeda jame veikti.
Savotiškais virusais laikomi ir apgaulingi laiškai (angl. *hoax*), kurių autoriai, pavyzdžiui, siunčia "laimingus" laiškus, praneša apie tariamus kompiuterinius virusus, prašo pagalbos ar pan., ir skatina šiuos

laiškus persiųsti visiems pažįstamiems. Tokie laiškai kompiuteriui žalos nedaro, tačiau bereikalingas jų siuntinėjimas apkrauna pašto sistemas. Gavę tokius laiškus, jų nepersiųskite, bet iškart pašalinkite.

Virusai ir elektroninis paštas

Vienas iš dažniausiai pasitaikančių virusų plitimo būdų - jų persiuntimas elektroniniais laiškais.
Virusas, veikiantis užkrėstame kompiuteryje, prideda savo kopiją prie laiškų ir siunčia juos visiems e. pašto programos adresinėje esamiems adresatams.
Laiško priedas gali būti pavadintas tarsi svarbus dokumentas, sąskaita ar net paveikslėlis. O pačiame laiško tekste siūloma jį atvėrus perskaityti.
Atvėrus ir paleidus prie laiško pridėtą užkratą, kompiuteris tikriausiai bus užkrėstas ir panašiai gali pradėti siuntinėti viruso kopijas visiems Jūsų adresinėje esantiems žmonėms.

Ką daryti?

Gavę laišką su pridėtu dokumentu, įvertinkite, ar tikrai verta rizikuoti ir šį priedą pasižiūrėti. Virusų siunčiami laiškai dažniausiai turi tokius požymius:

- nenurodyta laiško tema arba vietoje jos tėra simbolių kratinys;
- tekste pranešama apie laimėjimą loterijoje, kurioje nedalyvavote, informaciją, kurios neprašėte, pateikiamos nuorodos į su Jūsų veikla nesusijusius dalykus;
- laiške pranešama apie banko sąskaitos problemas ar neįvykdytą mokėjimo pavedimą;
- nurodytas laiško siuntėjas nesusijęs su laiško turiniu ar laiškas parašytas neįprasta Jūsų bendravimui kalba (pavyzdžiui, anglų).

Net jei pažįstate laiško siuntėją, tai visai nereiškia, kad laiškas siųstas iš jo kompiuterio. Siuntėjo adresą labai nesunku suklastoti.
Jei nutarėte priedą atverti, pirmiausia jį įrašykite kur nors kompiuterio diske, o tik po to atverkite. Tuomet antivirusinė programa geriau atliks savo darbą - patikrins ar priedas nepavojingas.

Kenksmingas paties laiško kodas
Į laišką galima įterpti tam tikrus kenksmingus intarpus su programų kodu. Šie intarpai gali būti siunčiami kartu su laišku arba įterpiami iš tam tikrų interneto svetainių laiško peržiūros metu. Pirmuosius dažniausiai aptinka antivirusinė kompiuterio programa. Antruosius paprastai blokuoja pati pašto programa.

Antivirusinės programos

Antivirusinių programų paskirtis - aptikti ir nukenksminti žalingą programinę įrangą. Šiuolaikinės antivirusinės programos geba naikinti ne tik tikruosius kompiuterinius virusus, bet ir Trojos arklius ar kirminus. Kai kurios iš jų netgi užkerta kelią duomenų išviliojimui.
Kokia bebūtų gera antivirusinė programa, ji bus veiksminga tik tada, jei reguliariai ją atnaujinsite. Kasdien paplinta vis nauji kompiuteriniai virusai, todėl antivirusinė programa turi juos pažinti. Dauguma tokių programų kasdien (galite nurodyti ir rečiau) automatiškai jungiasi internetu ir parsisiunčia naujausią informaciją apie galimus virusus.

Įsigydami antivirusinę programinę įrangą įvertinkite, kiek laiko ji bus nemokamai naujinama. Daugelis kompiuterių pardavėjų kaip papildomą vertę siūlo kompiuteryje įdiegtas komercines antivirusines programas su pusmečio ar metų naujinių prenumerata. Tačiau, pasibaigus šiam laikui, už prenumeratos pratęsimą turite sumokėti. To nepadarius, antivirusinė kompiuterio apsauga tampa nepakankamai veiksminga. Dar daugiau, kai kurių antivirusinių programų negalima paprastai pašalinti ir įdiegti kitą (vienu metu kompiuteryje gali veikti tik viena tokia programa). Todėl iškart turėtumėte apsispręsti - ar naudosite komercinę programą ir nuolat mokėsite už naujinimus, ar iškart diegsite nemokamą antivirusinę programą.

Laimei, tokių nemokamų antivirusinių programų sukurta nemažai ir jas galima parsisiųsti internetu. Lyginamąjį antivirusinių programų sąrašą rasite Wikipedijoje (anglų k.). Atkreipkite dėmesį į programos licencijos tipą (*Freeware* ir GPL - laisvojo naudojimo).

Namų vartotojui visiškai pakanka, pavyzdžiui, *Avira AntiVir PersonalEdition Classic* (http://www.avira.com), *AVG Anti-Virus Free* (http://www.grisoft.com) ar *ClamWin* (www.clamwin.com). Be abejo, kompiuteryje diegiama tik viena antivirusinė programa. Nemokamo naudojimo programos kompiuterį saugo ne blogiau, nei įvairios mokamos programos, o kartais ir geriau. Manoma, kad minėta *Avira AntiVir* yra viena iš veiksmingiausių antivirusinių programų.

Suabejojus turima antivirusine programa ir norint patikrinti savo kompiuterį, tą galima padaryti pasinaudojus tiesioginio tikrinimo priemonėmis *Microsoft saugos centro,* http://housecall.trendmicro.com ar http://www.pandasecurity.com svetainėse. Paprastai siūloma atsisiųsti *Active*X tipo programą - siųsdamiesi įsitikinkite, kad Jūsų naršyklė jos neblokuoja.

Tam tikrus virusus aptinka ir pašalina nedidelės apimties programa *McAfee Avert Stinger*, kurią galima parsisiųsti iš http://vil.nai.com/vil/stinger ir paleisti savo kompiuteryje. Šios programos kompiuteryje įdiegti ir saugoti nereikia, geriau kiekvienąkart parsisiųsti naujausią jos atmainą.

Microsoft Windows vartotojai, parsisiųsdami naujinius, reguliariai gauna kompiuterį patikrinančią ir pavojingesnius virusus pašalinančią programinę priemonę.

http://anti-virus-software-review.toptenreviews.com - daugiausia komercinių antivirusinių programų galimybių palyginimas (anglų k.). Kai kurios iš jų asmeniniam naudojimui yra nemokamos; http://www.esaugumas.lt - daugiausia asmeniniam naudojimui skirtos nemokamos antivirusinės programos.

Profilaktikos priemonės

- Kiekvieną iš kitur atneštą diskelį tikrinkite antivirusine programa.
- Bylas kompiuteryje laikykite suglaudintas – į tokias bylas virusai neprasiskverbia.
- Nevykdykite neaiškių ar elektroniniu paštu gautų programų. Pradėdami vykdyti naują programą, būtinai patikrinkite ją antivirusine programa.
- Periodiškai atnaujinkite antivirusines programas.
- Turėkite svarbiausių duomenų kopijas.

Kompiuterio apsauga

1. Interneto užkarda

Internetas (pasaulinis kompiuterių tinklas) yra sudarytas iš daugybės mažesnių tinklų. Platieji tinklai (WAN) apima tūkstančius ar milijonus vartotojų mieste ar net visoje šalyje. Juos sudaro sujungti vietiniai (LAN) įstaigų, interneto tiekėjų ir pan. tinklai, turintys nuo kelių iki kelių tūkstančių vartotojų. Kai didelių organizacijų darbuotojai dirba skirtinguose vietovėse, tų pastatų vietiniai tinklai įvairiomis ryšių linijomis sujungiami į virtualius vietinius tinklus (VLAN).

Kompiuteriai į tinklus jungiami pačiais įvairiausiais būdais - specialiais kabeliais, bevieliu ryšiu, telefono ryšiu (pavyzdžiui, pasinaudojant mobiliaisias telefonais).

Vienas iš svarbiausių kompiuterių tinklų privalumų yra tai, kad jų pagalba galima naudotis bendrais ištekliais - spausdintuvais, serveriais, galingų kompiuterių skaičiavimo galimybėmis ir pan.

Prie kiekvieno kompiuterio, kuris įjungtas į kompiuterių tinklą, gali prisijungti kiti žmonės, gauti kompiuteryje esančius duomenis, adresus bei slaptažodžius ar netgi valdyti kompiuterį, matyti, kas rodoma jo ekrane. Tam reikia žinoti prisijungimo duomenis, kompiuteryje turi būti leista jungtis svečiams ir paliktos tam tikros landos kompiuterio apsaugos sistemose.

Interneto programišiai nuolat žvalgo kompiuterių tinklus ir radę neapsaugotą kompiuterį stengiasi įsibrauti, įrašyti jame kenksmingą programinę įrangą, kuri ne tik išsiųstų norimus duomenis, bet ir prireikus perimtų kompiuterio valdymą.

Vienu metu panaudodami tūkstančius tokių kompiuterių "zombių", interneto kenkėjai atakuoja įvairias svetaines, kurios dėl milžiniško kreipinių skaičiaus nustoja veikti. Taip pat šie kompiuteriai gali būti panaudoti įsilaužimui į kitus kompiuterius ar virusų platinimui.

Jei kompiuteris kuriuo nors būdu prijungtas prie interneto, tai jis atakuojamas maždaug porą kartų per minutę, o jei internetą gaunate iš didžiųjų interneto tiekėjų, turinčių tūkstančius vartotojų - net kas kelias sekundes.

Nuo įsibrovėlių kompiuterį gali apsaugoti interneto užkarda (angl. *firewall*). Daugelis operacinių sistemų (pavyzdžiui, *Microsoft Windows XP*, *Vista* ar *7*) turi nuosavą užkardą, kurią tereikia įjungti (apie tai - papildomos medžiagos skyrelyje).

Užkarda tikrina iš interneto ir į jį siunčiamas informacijos užklausas. Nekenksmingos užklausos praleidžiamos, o įtartinos blokuojamos. Tinkamai nustačius užkardą, interneto įsibrovėliai tiesiog negalės aptikti Jūsų kompiuterio. Pačiam kompiuterio vartotojui naršyti internete užkarda praktiškai netrukdo. Tačiau įvairių programų mėginimai be vartotojo žinios išsiųsti kokią nors informaciją į išorę ar kitaip susisiekti su interneto kompiuteriais bemat sustabdomi.

Kai kurie kompiuterinio tinklo prietaisai (pavyzdžiui, maršrutizatoriai) taip pat turi interneto užkardas. Įstaigų vidinis kompiuterių tinklas (intranetas) paprastai apsaugomas centralizuotai - išorės vartotojai negali į jį patekti. Todėl darbo vietų kompiuteriuose pakanka įjungti standartinę operacinės sistemos užkardą.

2. Belaidžio tinklo apsauga

Tokiame tinkle duomenys perduodami radijo signalais, kuriuos tinklo veikimo zonoje gali priimti bet kuris bevielio tinklo įrangą turintis kompiuteris. Neretai įsilaužėliai įsitaiso geras kryptines antenas, kuriomis siunčiamus duomenis priima šimto ir daugiau metrų atstumu. Dar kiti belaidžio ryšio įrangą montuoja automobilyje ir ieško pažeidžiamų tinklų.

Nors nėra visiškai patikimų belaidžio ryšio apsaugos būdų, tačiau verta pasinaudoti bent tomis priemonėmis, kurias turi operacinė sistema ir belaidžio tinklo įranga.

Microsoft Windows XP, Vista bei *7* operacinėse sistemose belaidžio tinklo prieiga reguliuojama valdymo skydelio priemone *Bevielio tinklo nust. vedlys*. Čia būtina pasirinkti duomenų šifravimo raktą, - tuomet ryšys bus gana saugus. Atitinkamus nustatymus reikia nustatyti ir namų ar įstaigos belaidžio tinklo prieigos taške.

3. Virusai ir apsaugos nuo jų priemonės

Įvairios kenkėjiškos kompiuterinės programos, sutrikdančios kompiuterio veikimą ar trukdančios dirbti, vadinamos bendru kompiuterinių virusų vardu. Šiuo metu žinoma labai daug virusų, o kasdien sukuriami vis nauji.

Nuo virusų saugo speciali programinė įranga. Vienos antivirusinės programos žvalgo kompiuterio laikmenas ir ieško užkrėstų dokumentų, o juos suradusios mėgina virusą pašalinti. Kitos antivirusinės programos budi visą naudojimosi kompiuteriu laiką ir stebi paleidžiamas programas, atveriamus ir įrašomus dokumentus.

Kokią antivirusinę programą benaudotumėte, ją reikia kaip galima dažniau atnaujinti, kad toji pažintų pačius naujausius atsiradusius virusus.

Kokia bebūtų gera antivirusinė kompiuterio apsauga, tačiau visada išlieka nedidelė tikimybė, kad koks nors virusas šią apsaugą įveiks ir pažeis kompiuteryje laikomus duomenis. Todėl būtina reguliariai daryti svarbiausios informacijos kopijas į kitas laikmenas, kad prarastus duomenis vėliau iš jų būtų galima atkurti.

4. Apsauga nuo šnipinėjančių programų

Labai panašios į Trojos arklius yra įvairios šnipinėjimo programos (angl. *Spyware*, *Adware*), kurios seka kompiuterio vartotojo elgesį ir šiuos duomenis išsiunčia internetu. Visa tai yra daroma vartotojui nežinant ir be vartotojo sutikimo. Tokie šnipai gali būti įdėti netgi į legalią programą, parduodamą su

licencija. Tikriausiai tokių šnipinėjančių programų yra ir Jūsų kompiuteryje - tyrimai rodo, kad 4 kompiuteriuose iš 5 aptinkama kokia nors sekimo įranga.

Nors įstatymai pripažįsta, kad kiekvienas žmogus turi teisę į privatumą ir asmeninės informacijos apsaugą, šnipinėjanti programinė įranga šiurkščiai pažeidinėja šias teises.

Pagrindinis šnipinėjančių programų darbas yra surinkti ir išsiųsti informaciją apie naršymą internete: kokiuose tinklalapiuose lankosi vartotojai, kiek laiko yra prisijungę ir pan. Taip pat dažniausiai yra renkama informacija ir apie patį kompiuterį: kokia jo operacinė sistema, procesorius, atmintis ir t.t. Yra net sukurti šnipai išsiaiškinti, ar naudojamos programos kompiuteryje yra legalios, ar ne.

Surinkta informacija gali būti panaudota komerciniais tikslais ar statistikai, tačiau vartotojas nežino, kam konkrečiai yra renkama tokia informacija ir kas su ja yra daroma vėliau.

Vienas sekimo sistemos pavyzdžių yra visiems gerai žinomos paieškos sistemos *Google* ir elektroninio pašto *GMail* pora. Nors atskirai veikianti *Google* yra visai nekenksminga, tačiau, tuo pat metu naudojant *GMail*, pastaroji surenka žinias apie ieškotą informaciją bei lankytas svetaines. Kadangi *GMail* turi vartotojo atpažinimo duomenis, jam gali būti siuntinėjamos reklaminės šiukšlės.

Kai kurie darbdaviai naudoja šnipinėjančias programos savo darbuotojams sekti. Paplitęs įsitikinimas, kad darbdavys turi teisę kontroliuoti darbuotojo susirašinėjimą ir naudojimąsi internetu, tačiau Lietuvos Respublikos įstatymai draudžia darbuotojų sekimą, pokalbių pasiklausymą ir kitos asmeninės informacijos rinkimą.

Kaip interneto šnipai patenka į Jūsų kompiuterį? Daugelį šnipinėjančių programų parsisiunčiate ir įdiegiate kompiuteryje patys, susivilioję jų žadamomis galimybėmis. Pavyzdžiui, anksčiau garsi programa *Gator* buvo tarsi naudinga - įsimindavo įvairius svetainių slaptažodžius ir padėdavo užpildyti registracijos formas, tačiau tuo pat metu sekdavo vartotoją ir išsiųsdavo visus duomenis apie jo elgesį. Daugelis interneto naršyklių ir e. pašto programų priedų - šnipų palengvina informacijos paiešką ar papuošia e. laiškus įvairiais paveikslėliais. Todėl nepasitikėkite įvairiose svetainėse siūlomomis esą naudingomis programomis ir jas siųskitės tik iš patikimų šaltinių. Daugiau informacijos apie diegiamą programinę įrangą ir kaip ją vertina saugumo specialistai, nesunkiai rasite pasinaudoję kuria nors interneto paieškos sistema. Jau minėjome *Google* su *GMail*. Dauguma interneto svetainių kompiuteryje įrašo taip vadinamus slapukus (angl. *cookies*), kurie leidžia atpažinti tų svetainių lankytojus ir prisiminti jų veiksmus. Pavyzdžiui, internetinės bankininkystės svetainės po kiekvieno vartotojo veiksmo patikrina įrašytus slapukus ir pakartotinai nebereikalauja įvesti slaptažodžių. Baigus seansą, su juo susiję slapukai pašalinami. Tačiau kai kurių svetainių įbrukti slapukai galioja keliasdešimt metų ir juos gali pasiimti kitos lankomos svetainės.

Daugelis antivirusinių programų neapsaugo nuo šnipų. Tam skirta speciali programinė įranga, kuri peržiūri kompiuterio atmintinę ir laikmenas ieškodama žinomų informacijos rinkimo priemonių, o radusi - pasiūlo jas pašalinti. Kadangi šnipinėjimo priemonių, kaip ir virusų, atsiranda vis naujų, su jomis kovojančias programas taip pat reikia naujinti.

Populiariausios kovos su šnipinėjančia programine įranga programos yra *Lavasoft Ad-Aware Free* (www.lavasoft.de) bei *Spybot - Search & Destroy* (http://www.safer-networking.org). Jos yra nemokamos. Bendrovė *Microsoft* legalių *Microsoft Windows* vartotojams siūlo saugos komplektą *Windows Security Essentials*, kurią galima parsisiųsti iš *Microsoft* svetainės. Ten pat pateiktos įdiegimo, naudojimosi instrukcijos bei patarimai.