

REKOMENDACIJOS „SAUGUS DARBAS INTERNETE“

ĮVADAS

Įgyvendindama Mokyklų tobulinimo programą (Lietuvos Respublikos Vyriausybės 2002 m. gegužės 28 d. nutarimas Nr. 759) ir siekdami, kad mokyklų tobulinimo programos dalyviai išmoktų saugotis internete tykojančių pavojų, apsaugotų savo kompiuterį, savo informaciją nuo nesankcionuoto priėjimo, galėtų saugiai naudoti internetą bei intraneto technologijas, A komponento „Mokymo ir mokymosi sąlygų gerinimas“ 2 dalinio komponento „Virtuali mokymosi aplinka“ ekspertų darbo grupė parengė rekomendacijas „Saugus darbas internete“. Informacinių technologijų ekspertų komisija 2005 m. gegužės 31 d. posėdyje pritarė rekomendacijų „Saugus darbas internete“ naudojimui mokyklose. Šios rekomendacijos supažindina su grėsmėmis, kylančiomis iš interneto, bei apsaugos būdais. Rekomendacijos skiriamos interneto vartotojams, dirbantiems su asmeniniu kompiuteriu, pajungtu į internetą mokykloje arba namuose.

Kiekviena kompiuterizuota mokyklos darbo vieta, naudojama dirbti intranete arba virtualioje mokymosi aplinkoje, bus pajungta į vietinį kompiuterių tinklą ir turės interneto prieigą. Iš interneto vartotojai gaus ne tik naudingą informaciją ir informacines paslaugas, jiems taip pat grės visi internete slypintys pavojai. Tarp tokių grėsmių gali būti:

- Kompiuterinių virusų bei interneto kirminų pavojus. Tai yra piktavališkos programos, turinčios savęs platinimo mechanizmą. Dažnai virusai bei kirminai atlieka žalingus veiksmus: sunaikina informaciją, atlieka kompiuterines atakas kitų kompiuterių atžvilgiu, perkrauna kompiuterių bei tinklo išteklius ir pan.

- Pavojus prarasti informaciją. Įsilaužėliai, gavę nesankcionuotą priėjimą prie kompiuterio, gali sunaikinti arba pavogti (perimti) privačią svarbią informaciją. Dažnai įsilaužėlių tikslas – perimti vartotojų slaptažodžius, banko (mokėjimo kortelių) informaciją, el. pašto adresus ir kt.

- Įsilaužėliai aukos kompiuterį gali panaudoti kitokiems savo piktavališkiems tikslams, pavyzdžiui, kompiuteris gali būti paverstas naujų atakų poligonu ar piratinės programinės įrangos saugykla. Pažeistas kompiuteris bus perkraunamas, programinė įranga sugadinama, dėl padarytų nuostolių kompiuterio savininkas gali susilaukti sankcijų iš interneto paslaugų teikėjo ar iš teisėsaugos institucijų. Norint atkurti kompiuterio normalų veikimą, visada prarandama daug laiko ir lėšų.

Galima išvardyti tokias priežastis, dėl kurių pažeidžiami kompiuteriai:

- Vartotojams dažnai trūksta žinių apie interneto pavojus.
- Parduodami nauji kompiuteriai dažnai nėra pakankamai apsaugoti nuo interneto grėsmių.
- Vartotojai nesinaudoja (dėl žinių, laiko ar noro trūkumo) techninėmis priemonėmis (kurios dažnai yra pigios arba nemokamos), skirtomis padidinti kompiuterio saugumą.
- Dažnai saugumo problemoms neskiriama pakankamai dėmesio – įsigyjant naują kompiuterinę įrangą neskiriama lėšų kompiuteriui apsaugoti.

KOMPIUTERIO APSAUGA

Pagrindiniai kompiuterio apsaugojimo principai yra šie:

1. Neleisti prie kompiuterio prisijungti iš išorės (panaudojant užkardas).
2. Nuolat atnaujinti operacinės sistemos komponentus bei kitą naudojamą programinę įrangą.
3. Naudoti antivirusines priemones.

Taip pat svarbu yra prisiminti saugaus darbo internete principus (slaptažodžių naudojimas, atsargus elgesys su rinkmenomis iš interneto)

UŽKARDA

Užkarda – tai įranga (aparatinė arba programinė), sukurianti apsauginę sieną tarp jūsų kompiuterio ir interneto. Ji gali apsaugoti kompiuterį nuo daugelio įsilaužėlių bei kompiuterinių virusų ir kirminų.

Ką gali ir ko negali užkarda?

Gali:

- apsaugoti nuo interneto virusų, kirminų, bandančių įsiskverbti į jūsų kompiuterį iš interneto;
- apsaugoti nuo įsilaužėlių, atakuojančių jūsų kompiuterį;
- neleisti nepageidautinoms programoms jūsų kompiuteryje išsiųsti informacijos iš jūsų kompiuterio.

Negali

- apsaugoti nuo kompiuterių, kuriuos jūs laikote patikimais (pvz., kaimyninis vietinio tinklo kompiuteris);
- apsaugoti nuo interneto virusų, kirminų, kuriuos gaunate elektroniniu paštu, naudodamiesi naršykle ar kita programa.

Dėmesio: nerekomenduojama kompiuterį jungti į tinklą (internetą), prieš tai neapsaugojus jo aparatine ar programine užkarda.

APARATINĖ UŽKARDA

Vietinį tinklą rekomenduojama apsaugoti specialiu įrenginiu – aparatine užkarda. Toks įrenginys turėtų uždrausti bet kokius prisijungimus iš interneto prie darbo kompiuterių. Tokią funkciją gali atlikti:

- specializuotas įrenginys, atliekantis tik užkardos funkcijas;
- tinklo maršrutizatorius ar bevielės prieigos taškas (wireless access point) su galimybe filtruoti tinklo srautus;
- įrenginys (serveris), atliekantis vidinio tinklo adresų transliavimo funkcijas (NAT).

PROGRAMINĖ UŽKARDA

Net jei jūsų vietinis tinklas apsaugotas aparatine užkarda, nereikia pamiršti pavojų, kylančių iš to paties vietinio tinklo. Tai gali būti tiek priešiška nusiteikęs kaimynas, kolega, tiek kompiuterinis virusas. Nuo tokių problemų gali apsaugoti programinė užkarda, įdiegta į jūsų kompiuterį. Čia išvardytos kelios tokios programinės sistemos, turinčios taip pat ir nemokamas versijas (gali būti apribotos naudojimo galimybės):

- Operacinė sistema MS Windows XP turi savo vidinę užkardą MS Windows XP „Internet Connection Firewall“. Įjungimo instrukcijas galima rasti čia: http://cert.litnet.lt/dokumentai/winxp_fw/. Ankstesnėms MS Windows versijoms galima naudoti toliau išvardytas programines užkardas;
- ZoneAlarm (nemokama versija namų vartotojams bei nepelno organizacijoms, išskyrus valstybines bei mokslo organizacijas);
- Kerio Personal Firewall (nemokamas namų vartotojams);
- Oupost Firewall 1.0 (nemokamas);
- Sygate Personal Firewall (nemokamas asmeniniam naudojimui).

PROGRAMINĖS ĮRANGOS ATNAUJINIMAS

Apsaugojus kompiuterį su aparatine ar programine užkarda, galima jį pajungti į tinklą. Pirmas žingsnis, kurį reikia padaryti – atnaujinti kompiuterio programinę įrangą. Operacinę sistemą galima atnaujinti:

- prisijungus prie <http://windowsupdate.microsoft.com>;
- pasirinkus Start->All Programs ->Windows Update.

Būtina įdiegti visus siūlomus svarbiausius atnaujinimus (Critical Updates and Service Packs).

AUTOMATINIS PROGRAMINĖS ĮRANGOS ATNAUJINIMAS

Būtina užtikrinti, kad naudojama programinė įranga būtų atnaujinama laiku, vos tik gamintojas išleidžia svarbias pataisas. Tam reikalinga įjungti automatinį operacinės sistemos komponentų atnaujinimą.

MS Windows XP instrukcijos:

- pasirinkite Start->Control Panel;
- dukart spragtelėkite System;
- pasirinkite kortelę „Automatic updates“;
- pažymėkite langelį prie „Keep my computer up to date“.

ANTIVIRUSINĖ PROGRAMINĖ ĮRANGA

Internetu keliauja daugybė įvairių piktybinių programų – internetinių virusų bei kirminų. Jų galima sulaukti tiek elektroniniu paštu, tiek interneto pokalbių kanaluose, tiek per kitas elektroninio bendravimo priemones. Užkardos neapsaugo nuo virusų, atkeliaujančių elektroniniu paštu ar gaunamų naršant internetą. Viena geriausių priemonių tam – antivirusinė programinė įranga su nuolat atnaujinama virusų duomenų baze. Toliau išvardytos kelios tokios sistemos:

- Dr.Web. Nemokamas Lietuvos valstybinėms mokymo įstaigoms. Plačiau apie tai svetainėje <http://aldona.mii.lt/pms/lok/drweb/> ;
- Avast! antivirus. Avast! 4home – nemokama versija namų vartotojams;
- AVG Anti-Virus;
- Lavasoft Ad-aware, skirta aptikti ir išnaikinti piktybines reklamines, šnipinėjimo ir panašias programas. Ad-aware Standard Edition – nemokama nekomerciniam naudojimui;
- McAfee VirusScan;
- Kaspersky Anti-Virus Personal;
- BitDefender;
- Norton Antivirus.

PAVOJŲ KELIANTI INFORMACIJA

Kita didelė problema yra pačių interneto vartotojų pernelyg didelis patiklumas. Internetas nėra saugi vieta, nes kartu su jums reikalinga informacija čia galite gauti ir piktybinių programų bei virusų. Siekdami piktavališkų tikslų, įsilaužėliai bei virusai specialiai suformuoja žinutes, kurios įtikina nieko neįtarantį vartotoją pažiūrėti prisegtus laiško priedus, įvykdyti atsiųstą programą. Dažnai tokių atakų aukos patiki suklastotu atgaliniu adresu (laiško laukas „Nuo:“), žinutės tema, specialiai parinktu žinutės tekstu (pvz., pasiūlymas įdiegti atsiųstas saugumo pataisas) ar kitais žinutės požymiais. Toks puolimo metodas vadinamas socialine inžinerija.

Štai keletas patarimų tiems, kuriems tenka peržiūrėti el. paštu gautas rinkmenas:

- Niekada neperžiūrėkite prikabintų rinkmenų, gautų iš nepažįstamų asmenų tiek elektroniniu paštu, tiek pokalbių kanalais, tiek kitais būdais.
- Jei priedo nelaukėte – laikykite jį įtartinu, netgi jei jį siuntė gerai pažįstami asmenys. Netgi Word dokumentas gali turėti įterptą žalingą programos kodą. Prieš atidarydami gautą

Microsoft Office dokumentą, programoje Microsoft Word (Excel, Powerpoint ar pan.) pasirinkite Tools->Options, Security, Macro Security->Security Level, pažymėkite High.

- Net jei siuntėjas jums žinomas, tačiau tokio laiško priedo iš jo nelaukėte, įsitikinkite, ar jis iš tikro siuntė šį laišką (paskambinkite jam arba paklauskite elektroniniu laišku), naudodami antivirusinę programą patikrinkite gautą rinkmeną dėl virusų.

- Atkreipkite dėmesį, ar žinutės tekstas logiškas – ar siuntėjas galėjo atsiųsti tokio turinio laišką bei prisegti rinkmeną?

SLAPTAŽODŽIAI

Pagrindinė slaptažodžių paskirtis yra apsaugoti informaciją bei kitus kompiuterinius išteklius: elektroninius laiškus, jūsų kompiuterio bylas, įrenginius ir panašiai. Slaptažodžius galima sulygtinti su raktais nuo jūsų kambario durų – užrakinę duris jūs apsaugote kambarį nuo vagių, vandalų ar nuo nekviestų svečių. Įprasta, kad durų raktas yra unikalus, ir mažai tikėtina, kad kas nors suras kitą raktą, galintį atrakinti jūsų duris. Kuo rakto forma sudėtingesnė, tuo bus sunkiau atrasti kitą tinkamą raktą. Tą patį galima pasakyti apie slaptažodį. Kuo slaptažodį lengviau atspėti, tuo jūsų informacija bus silpniau apsaugota. Slaptažodžius galima atspėti žinant tam tikrus faktus apie asmenį (gimimo data, telefono ar automobilio numeriai, šeimos narių vardai ir pan.) arba tiesiog naudojant įprastus žodžius iš žodyno.

Taip pat prastų, silpnų slaptažodžių pavyzdžiai – tai pasikartojančių simbolių sekos (pvz., abab1212), simbolių sekos, atitinkančios klaviatūros išdėstymą (pvz., qwerty).

Gerą slaptažodį turi sudaryti raidės (didžiosios ir mažosios), skaitmenys bei specialieji simboliai. Norėdami sudaryti gerą ir lengvai įsimenamą slaptažodį, galite panaudoti žinomą frazę. Iš tokios frazės paėmę pirmąsias raides arba priebalses (antrąsias, paskutines raides), atlikę raidžių pakeitimus į specialius simbolius arba skaičius (pagal bet kokias asociacijas), gausite slaptažodį, kurį sunku atspėti, bet nesunku įsiminti.

Pavyzdys:

- paimekime frazę: **Tėtė kala, Mama mala;**
- surinkime priebalsius bei simbolį „,“: **Ttkl,Mmml;**
- atlikime pakeitimus **Tt = 2T; Mmm = 3m;**
- gausime slaptažodį **2Tkl,3ml.**

Dėmesio: niekada nenaudokite šiame pavyzdyje sudaryto slaptažodžio.

Siūlymai kitiems galimiems simbolių pakeitimams:

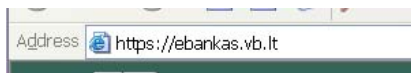
- žodelis „ir“ = &
- è = \$ (lietuviška raidė „ė“ lietuviškoje klaviatūroje yra ties simboliu \$)
- A = 4, E = 3, S = 5, O = 0 ir panašiai.

SAUGIŲ TECHNOLOGIJŲ NAUDOJIMAS

Dirbant internete reikia atminti, kad siunčiama informacija keliauja nesaugiais tinklais, t.y. siunčiamą informaciją pakeliui galima perimti (pavogti), siunčiama informacija gali nukeliauti ne ten, kur jūs manote siunčiąs. Nuo tokio informacijos praradimo galima apsisaugoti šifruojant informaciją. Viena populiariausių šifravimą naudojančių technologijų yra SSL.

Siūsdami privačią informaciją:

- Rinkitės saugius siuntimo metodus, paremtus SSL technologijomis, pvz. https, pop3s, imaps. Šie metodai siunčiamą informaciją šifruoja, taip ji apsaugojama nuo pašalinių akių. Šitaip jungdamiesi prie tinklalapio, naršyklėje interneto adresą prasidės ne http:// o https://, pavyzdžiui:



Naršyklės apačioje apie saugų prisijungimą primena užrakintos spynos piktograma:



Pašto skaitymo programai taip pat galima nurodyti naudoti saugius siuntimo metodus, pažymėjus varnelę prie „SSL“ (tik jei paslaugos teikėjas tokią paslaugą siūlo).



Niekada nesiųskite slaptažodžių ar kitos svarbios informacijos pokalbių kanalais (chat) – paprastai pokalbiai siunčiami nešifruoti, be to, dažnai neįmanoma įsitikinti pašnekovo tapatybe.

SAUGUS NARŠYMAS

Benaršant internete galima užklysti į piktavališkai sudarytas interneto svetaines, kuriose naršyklė, vartotojui nežinant, parsisiunčia piktybines programas ir, esant prastiems saugumo nustatymams, tokias programas įvykdo. Dėl to kompiuteryje gali atsirasti šnipinėjimo programos, piktybines programos, nuolat iškviečiančios reklamas, iš kompiuterio gali būti pavogta slapta privati informacija. Toliau pateiktos instrukcijos MS Internet Explorer programos saugumui padidinti:

1. pasirinkite Tools->Internet Options. Pasirinkite skiltį Security;
2. pasirinkę Internet zoną spragtelėkite Custom Level ir atsidariusiame Security Settings lange:

- 2.1. Scripting skiltyje, prie „Allow paste operations via script“, pasirinkite „Prompt“;
- 2.2. Skiltyje „ActiveX controls and plug-ins“ prie „Download signed ActiveX Controls“ pasirinkite „Prompt“; prie „Download unsigned ActiveX Controls“ pasirinkite „Disabled“; prie „Initialize and script ActiveX Controls not marked as safe“ pasirinkite „Disabled“;
- 2.3. „Microsoft VM“ srityje, prie „Java permissions“, pasirinkite „High safety“;
- 2.4. „Miscellaneous“ srityje, prie „Access to data sources across domains“, pasirinkite „Disabled“ ir spragtelkite OK.

Local intranet ir Trusted sites zonos paprastai turi ne tokius griežtus saugumo nustatymus, todėl neįtraukite į šias zonas nepatikimų serverių adresų. Patikrinti galite pasirinkę atitinkamą zoną ir spragtelėję „Sites...“.

Dėl Internet Explorer saugumo spragų piktybines programas gali įvykdyti netgi naršyklės su pačiais griežčiausiais saugumo nustatymais. Dėl šios priežasties yra rekomenduojama naudoti kitokias naršyklės nei Internet Explorer bei kitas pašto skaitymo programas nei Outlook ar Outlook Express. Populiarios yra šios nemokamos interneto naršymo bei el. pašto skaitymo programos:

- Mozilla
- Firefox ir Thunderbird
- Netscape
- Opera

SAUGUS EL. PAŠTO SKAITYMAS

Pašto skaitymo programa Microsoft Outlook Express yra pridedama prie operacinės sistemos MS Windows ir yra viena populiariausių pašto skaitymo programų. Deja, dažnai skaitydami laiškus vartotojai apkrečia savo kompiuterį virusais. Čia išvardyti keli patarimai, kaip padidinti elektroninių laiškų skaitymo proceso saugumą.

- Sugriežtinkite saugumo nuostatas: Tools->Options->Security. Pasirinkite Zone: „Restricted sites“ arba „Restricted sites zone (More secure)“ – Outlook Express programai.

- Spragtelėkite Zone Settings, „Security level for this zone“ skiltyje nustatykite reikšmę High. Spragtelėkite OK, OK. Pastarasis nustatymas uždraudžia vykdyti su laišku atėjusias ActiveX, Java, JavaScript bei panašias programas.
- Įjunkite rinkmenos plėtinio parodymą. Nemažai virusų plinta sudarydami dvigubus plėtinius (pvz., jpg.exe). Jei Windows sistema neparodo plėtinių, gautos rinkmenos pavadinimą jūs matysite nekorektiškai (pvz., Photo.jpg vietoj Photo.jpg.exe).
- Instrukcijos MS Windows XP sistemai:
 - atverkite My Computer;
 - pasirinkite Tools->Folder Options;
 - pasirinkite View kortelę, panaikinkite pažymėjimą prie punkto „Hide file extensions for known file types“, spragtelėkite OK.

Neperžiūrėkite el. laiškų HTML pavidalu. Instrukcijos:

- Mozilla ir Netscape: View->Message Body As->Plain Text arba View->Message Body As->Simple HTML.
- Outlook Express 6 (SP1): Tools->Options... , pasirinkite Read, padėkite varnelę prie „Read all messages in plain text“.
- Outlook2003: Tools->Options... : Preferences kortelėje pasirinkite „E-mail Options...“, padėkite varnelę prie „Read all standard mail in plain text; Security kortelėje spragtelėkite „Change Automatic Download Settings...“, padėkite varnelę prie „Don't download pictures or other content automatically in HTML e-mail“.
- Outlook 2002 instrukcijos: <http://support.microsoft.com/?kbid=307594>. **Dėmesio:** šiai sistemai reikalingi registro pakeitimai. Nerekomenduojame to atlikti vartotojams, neturintiems darbo su registrais patirties.

SPAM

Kas yra SPAM? SPAM – tai šiukšlės, gaunamos elektroniniu paštu. Paprastai tai būna reklaminio pobūdžio elektroninės žinutės, kurios neprašytos pasiekia vartotojo el. pašto dėžutę. SPAM laiškai surija kompiuterių tinklo, pačių kompiuterių išteklius, už kuriuos moka patys SPAM gavėjai. Taip pat SPAM surija ir laiką, reikalingą tokiems laiškams peržiūrėti, atskirti nuo reikalingų laiškų, juos šalinti.

Kaip SPAM siuntėjai sužino jūsų el. pašto adresą? SPAM platinimas – tai savotiškas, dažnai pasipiktinimą keliantis verslas, atnešantis platintojams tam tikrų pajamų. Kuo daugiau platintojas išsiųs laiškų, tuo didesnės pajamos jo laukia. Taigi tokiems interneto šiukšlintojams reikalingos tonos el. pašto adresų, kur jie galėtų išsiųsti nepageidaujamas reklamas. Šie el. adresų klodai paprastai randami internete – viešai prieinamuose tinklalapiuose, el. pašto konferencijose. Piktavaliai netgi naudoja robotus – specialias programas, naršančias internetą, renkančias iš tinklalapių pašto adresus. Jūsų el. pašto adresas taip gali patekti į archyvus, kuriuos vėliau nupirks interneto šiukšlintojas ir naudos reklamai platinti. Kitas adresų surinkimo būdas – naudoti interneto virusus, surenkančius pašto adresus iš el. pašto adresų knygelės užkrėstame kompiuteryje. Aptikti adresai kaipmat perduodami SPAM platintojams.

Kaip elgtis su SPAM laiškais? Visiškai išvengti SPAM laiškų yra sunku – ne visiems priimtina slėpti savo el. pašto adresą neskelbiant jo internete. Taip pat negalite būti garantuotas, kad virusas jo nepavogs iš kolegos ar draugo kompiuterio. Tačiau kovai su SPAM laiškais galite naudoti tam tikras priemones bei turite atminti kelis patarimus, padėsiančius išvengti tokių laiškų antplūdžio:

- Niekada neatsakinėkite į nelauktus reklaminius laiškus. Bet koks atsakas į tokį laišką (net jei tai bus prašymas daugiau šiukšlių nesiuntinėti) tik patvirtins SPAM platintojui, kad jo

reklama buvo peržiūrėta ir jog tokiam „pavyzdingam“ skaitytojui galima pateikti dar šūsni reklamos.

- Neretai SPAM laiškai būna taip suformuoti, jog užtenka vien tik neatsargiai peržiūrėti tokią žinutę, ir jūsų el. pašto adresą užregistruojamas SPAM platintojų bazėse, kaip potencialaus reklamos skaitytojo. Tai paskatins juos siųsti dar daugiau internetinio šlamšto. Tam, kad to išvengtumėte, naudokite el. pašto skaitymo programą, nerodančią HTML formatuotų laiškų. Tokią funkciją turi Mozilla bei Netscape el. pašto skaitymo programos. Įjungti tokią funkciją galima taip: View->Message Body As->Plain Text arba View->Message Body As->Simple HTML. Outlook2003 taip pat turi panašią galimybę, kurią galima aktyvuoti taip: Tools->Options..., pasirinkite Security, spragtelėkite „Change Automatic Download Settings...“, panaikinkite varnelę prie „Don't download pictures or other content automatically in HTML e-mail“.

- Kai kurios programos atlieka gautų el. laiškų analizę ir gali atlikti SPAM laiškų filtravimą (pvz., tokius laiškus šalinti arba perkelti į specialų katalogą vėlesnei peržiūrai). Tarp tokių programų yra:

- Netscape (įjungiamas Tools->Junk Mail Controls..., pažymėti „Enable junk mail controls“).

- Mozilla. Pastaba: Mozilla ir Netscape programas visų pirma reikia pamokyti pažinti SPAM laiškus. Tam tikrą laiką turėsite tikrinti, ar programa nedaro klaidingų sprendimų, ir rankiniu būdu žymėti nepažintas SPAM žinutes, bei naikinti SPAM žymes nuo klaidingai pažymėtų laiškų.

- Outlook 2003 (tvarkomas Tools->Options, pasirinkti Junk E-mail...).

ŠALTINIAI

1. <http://www.cert.org>
2. <http://www.securityfocus.com>
3. <http://cert.litnet.lt>
4. <http://www.sans.org>
5. <http://www.microsoft.com>

Parengė Mokyklų tobulinimo programos A komponento „Mokymo ir mokymosi sąlygų gerinimas“ 2 dalinio komponento „Virtuali mokymosi aplinka“ ekspertai: Giedrius Balbieris, Nijolė Kriščiūnienė, Dainora Muraškienė, Marius Urkis, Gintaras Vaskela, Arvydas Verseckas, Vytautas Verseckas, Edita Sederevičiūtė