NEPAGEIDAUJAMŲ ELEKTRONINIO PAŠTO PRANEŠIMŲ STUDIJA

NEPAGEIDAUJAMI ELEKTRONINIO PAŠTO PRANEŠIMAI, KAS TAI?

Tiksliai nusakyti *spam* (angl.) sąvoką nėra paprasta, nes sutinkama keletas to paties reiškinio apibūdinimų. Dažniausiai sutinkamas *spam* apibūdinimas – nepageidaujami elektroninio pašto pranešimai (toliau – NEPP), siunčiami dideliais kiekiais be vartotojų sutikimo. Eiliniam vartotojui tai tiesiog pranešimai – el. šiukšlės, kurių nepageidaujama matyti asmeninėje el. pašto dėžutėje. NEPP yra siunčiami naudojant el. paštą, judriojo ryšio (telefonais siunčiama SMS) ar kitus el. komunikacijos būdus bei priemones. Taip pat *spam* gali būti apibrėžta kaip nereikalautų el. pašto žinučių siuntimo praktika, paprastai komercinio pobūdžio, dideliais kiekiais ir dažnai tiems asmenims, su kuriais siuntėjas anksčiau nepalaikė jokių ryšių. 2006 m. tinklų ir informacijos saugumo būklės tyrimo (toliau – tyrimo) duomenimis, 96 proc. interneto paslaugų vartotojų niekada nėra įsigiję tokiu būdu siūlomų prekių ar paslaugų. Tik 1 proc. tiesioginės apklausos dalyvių nurodė, kad dažnai įsigyja prekių ar paslaugų, siūlomų nepageidaujamais komerciniais pranešimais. Taip pat yra pastebima, kad daugėja ir kenkėjiško pobūdžio NEPP, kai su el. pašto pranešimais keliauja ir kompiuteriniai virusai. Interneto vartotojams nepageidauti pranešimai ir virusai sukelia tas pačias problemas, tačiau jų pavojingumas kompiuterinėms sistemoms yra skirtingas.

ASMENS PRIVATUMO APSAUGOS PROBLEMOS

Bet kurio el. pašto vartotojo atžvilgiu NEPP problema turi keletą aspektų. Pirma, el. pašto adresai yra renkami be jų sutikimo ir jiems nežinant. Antra, el. pašto vartotojas gauna didelius nepageidaujamos reklamos kiekius. Trečia, prisijungimo laikas prie el. pašto dėžutės gali el. pašto vartotojui kainuoti. Ketvirta, el. pašto vartotojas gaišta laiką rūšiuodamas ir trindamas gautus pranešimus.

El. pašto adresas yra būtinas, norint pasiųsti arba gauti el. pranešimą. Tačiau jis taip pat yra svarbus informacijos šaltinis, turintis asmeninius vartotojo duomenis. El. pašto adresus galima rinkti keliais būdais:

- Bet kokios programinės įrangos, nuperkamos arba gaunamos nemokamai, gamintojas gali paprašyti užsiregistruoti.
- Yra įmanoma įvesti programinį kodą į kliento programinę įrangą, kuris perduos jo el. pašto adresą programinės įrangos gamintojui apie tai nežinant šios programos vartotojui (nematomas duomenų apdorojimas).
- Kai kurios naršyklės gali būti sukonfigūruotos taip, kad siųstų el. pašto adresą kaip slaptažodį anonimiškai jungiantis prie FTP tarnybinių stočių (tačiau tai dažnai nėra automatiškai nustatomas parametras).
- El. pašto adreso gali būti klausiama įvairiose svetainėse dėl įvairių priežasčių (pvz., komercinėse svetainėse atliekant pirkimo užsakymą, registruojantis prieš patenkant į pokalbių svetainę ir t. t.).
- El. pašto adresas gali būti perimtas siunčiant pranešimą.
- El. pašto adresai gali būti renkami viešose interneto vietose įvairiais kitais būdais.

Kai į reklamuotojo duomenų bazę patenka vartotojo el. pašto adresas, vartotojas gali būti užverstas įvairiais reklaminiais pasiūlymais. Norint išvengti NEPP, derėtų naudoti apsaugos priemones, kurios padėtų apsisaugoti nuo el. pašto adreso platinimo, pavyzdžiui, prieš suteikiant el. pašto adresą svetainei, reikėtų atidžiai perskaityti svetainės pateikiamą sutartį ir privatumo politiką, pokalbių svetainėms pateikti tik pokalbiams skirtus anoniminius pašto adresus.

NEPP PAPLITIMO PRIEŽASTYS IR BŪDAI

El. paštas yra patogi terpė el. šiukšlinimui: pranešimų pristatymas yra sąlyginai nemokamas, paslauga naudojasi itin daug žmonių, daug el. pašto adresų galima surinkti automatiniais būdais.

El. pranešimai siuntėjui galima sakyti nieko nekainuoja, tačiau dideli jų srautai ne tik mažina tinklų pralaidumą, bet ir atima daug gavėjo laiko, kai reikia surūšiuoti korespondenciją. NEPP šiuo metu pasaulyje sudaro didesnę dalį el. pašto srauto. 2004 m. NEPP srautas vidutiniškai sudarė 74 proc. viso pranešimų srauto, o 2005 m. šis skaičius priartėjo prie 83 proc. Duomenys gauti išanalizavus daugiau kaip 900 milijonų el. pašto pranešimų (informacijos šaltinis – saugumo kompanija „Messaglabs“). Priežastys, lemiančios NEPP plitimą:

- NEPP siuntėjai naudoja įvairias kompiuterines technologijas, padedančias automatizuoti NEPP rinkimą bei siuntimą. Norint, kad NEPP pasiektų milijonus žmonių, reikia didelio kiekio el. pašto vartotojų adresų. Surinkti didelį kiekį adresų NEPP siuntėjams padeda specialios kompiuterinės programos. Angliškai šis procesas vadinamas *harvesting*. Tokios programos skenuoja internetiniuose tinklalapiuose, pokalbių svetainėse bei kitose interneto tinklo srityse esančią informaciją, suranda el. pašto adresus ir juos nukopijuoja. Vėliau šie adresai panaudojami NEPP siųsti. Yra pastebėta, kad internete vyksta surinktų el. pašto adresų duomenų bazių prekyba.
- 86 proc. el. pašto adresų, esančių įvairiuose interneto tinklalapiuose visame pasaulyje, yra lengvai prieinami specialioms adresų surinkimo programoms (informacijos šaltinis – JAV Federalinė prekybos komisija).

NEPP ANALIZĖ, PASEKMĖS IR PERSPEKTYVOS

Didėjantys NEPP srautai kelia didžiules problemas elektroninių ryšių tinklų teikėjams. Interneto prieigos paslaugų teikėjų sistemos perkrautos, mažėja bendras srauto pralaidumas, kovai su NEPP reikia papildomų išteklių, patiriama finansinių nuostolių. Kartu su šiais pranešimais didėja plintančių kompiuterinių virusų ir įvairių apgaulės būdų grėsmė. Europos Komisijos 2001 m. tyrimų duomenimis, dėl NEPP buvo patirta 10 mlrd. eurų nuostolių.

2006 m. tyrimo duomenimis, dažniausiai pasitaikantys tinklo ir informacijos saugumo incidentai, su kuriais susiduria Lietuvos įmonės ir interneto paslaugų teikėjai (toliau – IPT), ir toliau išlieka kompiuteriniai virusai bei NEPP. 2005 m. kompiuterinius virusus, kaip didžiausią grėsmę, nurodė 79 proc. įmonių ir net 100 proc. IPT, atitinkamai 76 proc. įmonių ir 100 proc. IPT nurodė susiduriantys su NEPP. 2006 m. kompiuterinius virusus, kaip didžiausią grėsmę, nurodė absoliuti dauguma įmonių (86 proc.) ir IPT (98 proc.). Palyginti su 2005 m. tyrimo rezultatais, įmonėse kompiuterinių virusų sukeliamų incidentų skaičius padidėjo 7 proc., o NEPP – net 18 proc. Remiantis tyrimo duomenimis daugiau kaip 74 proc. Lietuvos apklaustų įmonių ir 85 proc. IPT naudojo įvairias programines priemones kovai su didėjančiu NEPP srautu. IPT šiuo tikslu dažniausiai naudojo filtravimą (68 proc.), juoduosius sąrašus (angl. *black list*) (64 proc.), pilkuosius sąrašus (angl. *grey list)* (28 proc.), siunčiamų pranešimų skaičiaus apribojimo priemones (30 proc.). Palyginti su 2005 m. tyrimo duomenimis, apklaustų įmonių ir IPT, naudojančių NEPP blokavimo priemones, skaičius išaugo, įmonių – 36 proc. ir IPT – 13 proc. 2006 m. didesnis skaičius IPT pradėjo naudoti efektyvesnes kovos su NEPP priemones, pavyzdžiui, pilkąjį sąrašą (išaugo nuo 16 iki 28 proc.).

Europos Parlamento technologijų vertinimo grupės 2006 m. spalio 16 d. ataskaitoje „Informacinės technologijos ir privatumas Europoje“ akcentuojama, kad „NEPP yra ne tik erzinantis, bet ir brangai kainuojantis. NEPP filtrai kainuoja ir atima laiko, nes juos reikia instaliuoti“.

Dažniausiai pasitaikantys tinklų ir informacijos saugumo incidentai, su kuriais 2006 m. susidūrė interneto vartotojai, ir toliau išlieka kompiuteriniai virusai bei NEPP. Susiduriantys su kompiuteriniais virusais nurodė 71,2 proc. apklausos dalyvių, o NEPP gauna 47 proc. Palyginti su 2005 m. rezultatais, vartotojų, susiduriančių su kompiuteriniais virusais, sumažėjo atitinkamai 7 proc. tarp tiesioginės apklausos dalyvių, o tiesioginės apklausos dalyvių, susiduriančių su NEPP, sumažėjo 16 proc.

Iš pirmiau pateiktų rodiklių galima padaryti išvadą, kad vartotojų, susiduriančių su NEPP bei kompiuteriniais virusais, sumažėjimą lėmė ir IPT naujausių filtravimo technologijų naudojimas bei NEPP ribojančių taisyklių taikymas. 2006 m. priemones kovai su NEPP naudojo 23 proc. interneto vartotojų. Palyginti su 2005 m. rezultatais, antivirusinių ir NEPP valdymo programų (angl. *anti-spam*) naudojimas tarp visų vartotojų padidėjo 2–3 proc.

Vartotojų nuomonės tyrimai taip pat rodo, kad NEPP yra viena iš pagrindinių vartotojams aktualių saugumo problemų. Dėl sukeliamų nepatogumų didėja vartotojų nepasitikėjimas el. pašto paslauga ir apskritai internetu. Prognozuojama, kad dėl UMTS (angl. *Universal Mobile Telecommunications Systems*) standarto, kai judriojo ryšio tinklas taps atviras internetui, paplitimo ši problema taps dar opesnė.

KITŲ ŠALIŲ ĮSTATYMŲ, TAIKOMŲ KOVOJE SU NEPP, TRUMPA APŽVALGA

Daugelyje pasaulio šalių NEPP draudžia įstatymai, tačiau tokių įstatymų įgyvendinimas yra sudėtingas. Pagal vadinamąjį „pasirinkimo“ metodą interneto šiukšlėmis laikomi visi el. pašto pranešimai, siunčiami be gavėjo sutikimo. Tačiau Jungtinės Valstijos siūlo reklamuotojams palankesnį „atsisakymo“ mechanizmą. JAV pagal dabar galiojančius įstatymus tokių pranešimų siuntimas nėra draudžiamas, nebent gavėjas nepageidauja jų gauti. Europos Bendrijoje NEPP siuntimą reglamentuoja Direktyvos 2002/58/EB (direktyva dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje) 13 straipsnio 1 dalis, kuri nustato, kad „naudoti automatinio skambinimo sistemas be žmogaus įsiterpimo (skambinimo automatus), faksimilinius aparatus (faksus) ar el. paštą tiesioginės rinkodaros tikslais gali būti leidžiama tik gavus išankstinį abonentų sutikimą“. Trumpai apžvelgsime kai kurių Europos Bendrijos šalių minėtos Direktyvos nuostatų perkėlimą į nacionalinę teisę.

Nyderlandų telekomunikacijų įstatymas aiškiai neapibrėžia, ką reiškia išankstinis sutikimas. Įstatyme nėra minima, kad tiesioginės rinkodaros pardavėjas gali prašyti sutikimo skambindamas. Įstatymas pabrėžia, kad automatinių skambinimo sistemų ir el. pranešimų be žmogaus įsikišimo naudojimas nepageidaujamiems pranešimams siųsti abonentams komerciniais tikslais yra leistinas tik tuomet, jei siuntėjas gali įrodyti, kad abonentas yra davęs tokiai veiklai savo išankstinį sutikimą. Duotą skambučio metu sutikimą yra sunku įrodyti. Toliau Įstatymas skelbia, kad, jei el. kontaktiniai duomenys yra (pirkimo ir pardavimo) sandorio rezultatas, šalys gali naudoti šiuos duomenis tiems patiems tikslams, jei tai yra apie tos pačios rūšies produktus ir abonentas yra davęs savo sutikimą tuo metu, kai kontaktiniai duomenys buvo duoti duomenų valdytojui.

Pagal Portugalijos Duomenų apsaugos įstatymą ir, duomenų apsaugos institucijos nuomone, skambinimas prašyti sutikimo jau yra tiesioginė rinkodara. Pirma, jau vyksta duomenų tvarkymas, antra, negalima iš karto atskirti skambučio tikslo, nes, iš vienos pusės, prašoma sutikimo, iš kitos pusės, reklamuojamas konkretus produktas. Skambučio tikslas – tiesioginė rinkodara. Portugalijos įstatymas nustato, kad el. pranešimams, siunčiamiems be duomenų subjekto (gavėjo) įsikišimo, reikia išankstinio sutikimo. Vadinasi, būtų skambinama nepriklausomai nuo to, ar gavėjas įsikištų. *Opt-out* (angl.) režimas yra leistinas klientams arba tuomet, jei asmuo jau yra davęs savo sutikimą, taip pat juridiniams asmenims. Kad ir kaip ten būtų, jei asmuo nesiskundžia ir duoda savo sutikimą, duomenų valdytojas turi teisę daryti tiesioginę rinkodarą. Tačiau tai, kad išankstinis sutikimas buvo gautas, turi įrodyti duomenų valdytojas.

Danijos duomenų apsaugos institucija informuoja, kad Danijoje nėra leidžiama skambinti tiesioginės rinkodaros tikslais, nes tai būtų nepageidaujami pranešimai. Danijoje tai daryti leistina tik tada, jei tai susiję su žiniasklaida, draudimu ir pan. Iš praktinės pusės yra svarbu gauti abonento sutikimą raštu, kad būtų galima įrodyti, jog abonentas sutiko, jei kiltų teisminių ginčų. Žodinio sutikimo neužtektų.

TECHNINĖS IR ORGANIZACINĖS PRIEMONĖS

El. pašto paslaugų teikėjai sutartyse su klientais ar viešai internete publikuojamose savo taisyklėse numato apribojimus dėl pranešimų platinimo. Pavyzdžiui, „Microsoft“ kompanija, siekdama pažaboti NEPP srautus, „Hotmail“ sistemoje riboja vieno vartotojo išsiunčiamų laiškų skaičių (per parą iki 100 laiškų). Tokią tendenciją galima pastebėti ir Lietuvoje kai kurių el. pašto paslaugų teikėjų taisyklėse.

Europos Bendrijos šalių, pvz., Vokietijos, Prancūzijos, Austrijos, nacionaliniuose įstatymuose yra įgyvendintos Direktyvos 2000/31/EB nuostatos, reikalaujančios *Robinson-List* sukūrimo. *Robinson-List* – registras, į kurį visi fiziniai ir juridiniai asmenys, nenorintys gauti neprašytų reklamos pranešimų, gali įvesti savo el. pašto adresą. Pavyzdžiui, Vokietijoje veikia interneto portalas http://www.erobinson.de, kuriame fiziniai ir juridiniai asmenys, pateikę savo duomenis, gali atsisakyti ne tik el. pašto reklaminių pranešimų, bet ir skambučių, SMS, MMS žinučių, siunčiamų iš mobiliojo ryšio tinklų.

Didžiojoje Britanijoje įmonės, norėdamos tiesioginės rinkodaros tikslais naudotis DMA (angl. *Direct Marketing Association*) duomenų baze, prieš užsisakydamos šias paslaugas turi gauti asociacijos sutikimą. Kompanija, kuri reklaminiams pranešimams siųsti naudojasi DMA duomenų baze, garantuoja DMA bazės el. pašto paslaugų pasirinkimą bei apribojimus. Pirkėjai, kurie pareiškia norą negauti neprašytų žinučių, yra pašalinami pagal susitarimą iš DMA bazės sąrašų.

NEPP gali būti platinami ir iš valstybių, kuriose tiesioginė rinkodara nėra teisiškai reglamentuojama. Tokiais atvejais el. pašto paslaugų teikėjai taiko filtravimo technologijas.

NEPP REGLAMENTAVIMAS LIETUVOJE

Lietuvoje NEPP atžvilgiu yra įtvirtinta vadinamoji išankstinė abonento sutikimo sistema (angl. *opt-in*), kuri reiškia, kad, norint siųsti masinį komercinį el. pranešimą, SMS, MMS ar pan., turi būti gautas išankstinis tokio pranešimo gavėjo sutikimas.

Lietuvos Respublikos elektroninių ryšių įstatymo (Žin., 2004, Nr. 69-2382) (toliau – ERĮ) 68 str. 1 dalyje yra nustatyta, kad „naudoti elektroninių ryšių paslaugas, įskaitant elektroninio pašto pranešimų siuntimą, tiesioginės rinkodaros tikslu leidžiama tik esant išankstiniam abonento sutikimui“. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo (Žin., 2003, Nr. 15-597) 2 str. 12 dalyje nustatyta, kad „tiesioginė rinkodara – veikla, kuri skirta paštu, telefonu arba kitokiu tiesioginiu būdu siūlyti asmenims prekes ar paslaugas ir (ar) teirautis jų nuomonės dėl siūlomų prekių ar paslaugų“.

ERĮ 68 straipsnio 2 dalis numato, kad asmuo, kuris teikdamas paslaugas ar parduodamas prekes Asmens duomenų teisinės apsaugos įstatymo nustatyta tvarka ir sąlygomis gauna iš savo klientų el. pašto kontaktinius duomenis, gali naudoti šiuos kontaktinius duomenis savo paties panašių prekių ar paslaugų rinkodarai, jei klientams yra suteikiama aiški, nemokama ir lengvai įgyvendinama galimybė nesutikti arba atsisakyti tokio kontaktinių duomenų naudojimo pirmiau nurodytais tikslais, kai šie duomenys yra renkami ir, jei klientas iš pradžių neprieštaravo tokiam duomenų naudojimui, siunčiant kiekvieną pranešimą. ERĮ 68 straipsnio 3 dalyje nurodyta, kad draudžiama tiesioginės rinkodaros tikslu siųsti el. pašto pranešimus slepiant siuntėjo, kurio vardu informacija siunčiama, tapatybę arba nenurodant galiojančio adreso, kuriuo gavėjas galėtų

pareikalauti nutraukti tokios informacijos siuntimą. Šių nuostatų priežiūra yra pavesta Valstybinei duomenų apsaugos inspekcijai.

Elektroninių ryšių įstatyme numatyto asmens duomenų tvarkymo ir privatumo apsaugos pažeidimas pagal Administracinių teisės pažeidimų kodekso 214^{23} straipsnį „Neteisėtas asmens duomenų tvarkymas ir privatumo apsaugos pažeidimas elektroninių ryšių srityje“ užtraukia baudą nuo penkių šimtų iki vieno tūkstančio litų. Tokie pat veiksmai, padaryti asmens, bausto administracine nuobauda už šio straipsnio pirmojoje dalyje numatytus pažeidimus, užtraukia baudą nuo vieno tūkstančio iki dviejų tūkstančių litų.

INSPEKCIJOS VEIKLA

ERĮ yra įtvirtinta, kad Valstybinė duomenų apsaugos inspekcija:

1) prižiūri, kaip vykdomos šio ERĮ devintojo skirsnio, išskyrus šio Įstatymo 63 straipsnio 5 dalies, 65 straipsnio 4 dalies ir 70 straipsnio 7 dalies, nuostatos, Viešojo administravimo įstatymo nustatyta tvarka nagrinėja skundus dėl asmens duomenų tvarkymo ir privatumo apsaugos bei surašo administracinių teisės pažeidimų protokolus;

2) bendradarbiauja su Ryšių reguliavimo tarnyba asmens duomenų ir privatumo apsaugos srityje.

Minėtojo įstatymo devintojo skirsnio nuostatos taip pat iš dalies susijusios su vieno tinklų ir informacijos saugumo aspekto – privatumo apsaugos – užtikrinimu. Abonentus būtina apsaugoti nuo privatumo pažeidimų per gaunamus neužsakytus pranešimus tiesioginės rinkodaros tikslais, ypač siunčiamus skambinimo automatais, telefaksais ir el. paštu, įskaitant ir SMS pranešimus.

Daugeliu atvejų Inspekcija gauna pagrįstus skundus dėl tiesioginės rinkodaros pažeidimų, išskyrus nedidelį kiekį skundų, kurie persiunčiami kitoms institucijoms ar grąžinami kaip nepagrįsti.

Rekomenduojamą skundo dėl duomenų subjekto teisių pažeidimo formą galima rasti Inspekcijos tinklalapyje adresu www.ada.lt. Taip pat Inspekcija rekomenduoja kartu su skundu pateikti ir NEPP aprašo kopiją. Kaip padaryti NEPP aprašo kopiją, galima rasti studijos priede.

Lietuvos el. pašto vartotojai, gaunantys NEPP iš JAV (tai galima nustatyti iš siuntėjo adreso, pranešime siūlomų prekių ar paslaugų ir pan.), gali apie tai pranešti JAV Federalinei prekybos komisijai el. paštu adresu uce@ftc.gov ir taip prisidėti prie globalinės kovos su NEPP (http://www.microsoft.com/lietuva/security/home/spam/spamoptions.mspx).

Masiškai plintant NEPP, vien tik galimybės nubausti NEPP siuntėją nepakanka. Lietuvos Respublikos Vyriausybės 2006 m. gruodžio 6 d. nutarimu Nr. 1211 priimtoje Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijoje akcentuojama, „kad būtų užkirstas kelias šiam neigiamam reiškiniui, įstatymais turėtų būti reglamentuojamas techninių ir organizacinių priemonių, skirtų jo prevencijai ir nepageidaujamų elektroninio pašto pranešimų sklaidos užkardymui, nustatymas bei panaudojimas“.

IŠVADOS

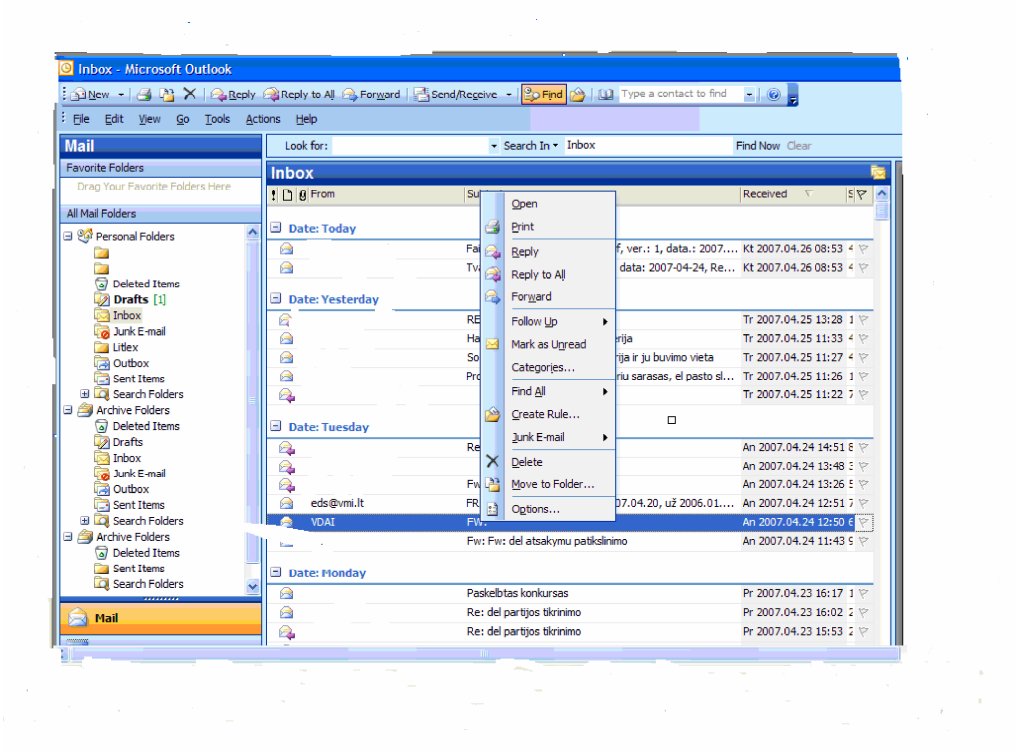
El. pašto vartotojai turėtų atsargiai elgtis su savo asmeniniais el. pašto adresais, kurie yra paklausi prekė internete. Norint išvengti NEPP, el. pašto adresą derėtų tinkamai saugoti kaip asmens kodą.

Parengė
Informacijos ir technologijų skyriaus
vyr. specialistas
Zigmantas Medutis
2007-07-06

NEPP studijos priedas

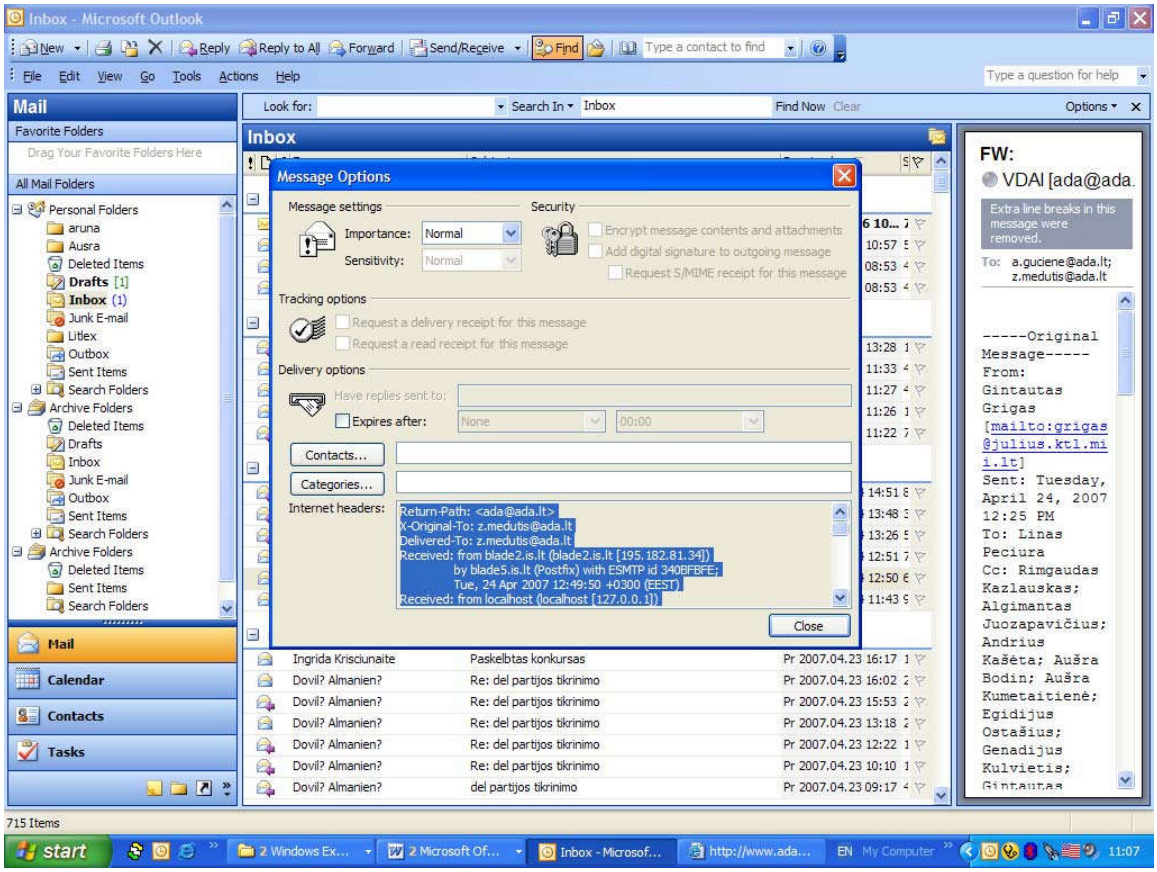
Kaip padaryti NEPP aprašo kopiją

Jei el. pašto vartotojas naudojasi „Microsoft Office Outlook“ pašto programa, tai jis turėtų atlikti programoje šiuos veiksmus:
1. Pelės kairiuoju klavišu pažymėti NEPP.
2. Spragtelėti pelės dešinį klavišą.
3. Atsidariusioje meniu juostoje kairiuoju pelės klavišu spragtelėti mygtuką „Options“ (1 pav.).



1 pav.

4. Atsidariusiame lange „Message Options“ dešiniu pelės klavišu pažymėti visą tekstą, esantį langelyje „Internet headers“.



2 pav.

5. Pažymėtą tekstą nukopijuoti į turimą tekstinio redaktoriaus programą (Word, NotePad ir t. t.) (3 pav).:

Return-Path: <yyy@xxxx.lt>
X-Original-To: xxxx@xxxx.lt
Delivered-To: xxxx@xxxx.lt
Received: from blade2.is.lt (blade2.is.lt [195.182.81.34])
by blade5.is.lt (Postfix) with ESMTP id 340BFBFE;
Tue, 24 Apr 2007 12:49:50 +0300 (EEST)
Received: from localhost (localhost [127.0.0.1])
by blade2.is.lt (Postfix) with ESMTP id 277982B6D;
Tue, 24 Apr 2007 12:49:50 +0300 (EEST)
X-Virus-Scanned: Contact the antivirus@is.lt for more information
Received: from blade2.is.lt ([127.0.0.1])
by localhost (blade2.is.lt [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id dTeyj+d0t4ZY; Tue, 24 Apr 2007 12:49:50 +0300 (EEST)
Received: from DAI (unknown [195.182.66.110])
by blade2.is.lt (Postfix) with ESMTP id C853A2B5E;
Tue, 24 Apr 2007 12:49:49 +0300 (EEST)
From: "VVVV" <yyy@xxxx.lt>
To:
<xxxx@xxxx.lt>
Subject: FW:
Date: Tue, 24 Apr 2007 12:51:31 +0300
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-4"
Content-Transfer-Encoding: quoted-printable
X-Mailer: Microsoft Office Outlook, Build 11.0.5510
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3028
thread-index: AceGUnavm+3sszofQEOnp3rK67B/RQAA6QRA
Message-Id: <20070424094949.C853A2B5E@blade2.is.lt>

3. pav. El. pranešimo aprašas