UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo

VARNOST ELEKTRONSKEGA DAVČNEGA POSLOVANJA V SLOVENIJI

Urška Škarlin

Ljubljana, april 2011

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

DIPLOMSKO DELO

VARNOST ELEKTRONSKEGA DAVČNEGA POSLOVANJA V SLOVENIJI

Kandidatka: Urška Škarlin
Vpisna številka: 33094
Študijski program: visokošolski študijski program Javna uprava prva stopnja

Mentor: viš. pred. dr. Mitja Dečman

Ljubljana, april 2011

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Urška Škarlin, študentka javne uprave, z vpisno številko 04033094, sem avtorica diplomskega dela z naslovom Varnost elektronskega davčnega poslovanja v Sloveniji.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega lastnega raziskovalnega dela;
- sem poskrbela, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;
- sem poskrbela, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena na seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;
- sem pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo, in sem to tudi jasno zapisala v predloženem delu;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata, bodisi v obliki skoraj dobesednega parafraziranja, bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorski in sorodnih pravicah, Ur. l. RS, št. 21/1995), kršitev pa se sankcionira tudi z ukrepi po pravilih Univerze v Ljubljani in Fakultete za upravo;
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za upravo;
- je elektronska oblika identična s tiskano obliko diplomskega dela, in da soglašam z objavo dela v zbirki Dela FU.

Diplomsko delo je lektorirala mag. Suzana Jakoša.

Ljubljana, 11. 2. 2011

Podpis avtorice:

POVZETEK

V spletu se pojavlja vedno več spletnega kriminala, saj sta razširjenost interneta in njegova uporaba čedalje večja, kar pomeni, da smo veliko bolj izpostavljeni nevarnostim. Te zajemajo različne finančne prevare, prevare pri pridobivanju osebnih podatkov, različne vdore v računalniške zbirke podatkov ter uničenje računalniških zbirk podatkov zaradi okužbe z virusi, s trojanskimi konji in črvi. Za svojo varnost lahko največ naredimo sami z zavestnim ravnanjem, kar pomeni, da posodabljamo računalniški sistem in računalnik pred spletnimi nevarnostmi zaščitimo z ustrezno protivirusno programsko opremo. Tega se zaveda čedalje več uporabnikov interneta, še posebej mlajši uporabniki, medtem ko imajo starejši v zvezi s tem še nekaj težav. Cilja spletnih kriminalcev sta pridobitev in zloraba osebnih podatkov internetnih uporabnikov. Ko že mislimo, da smo v spletu zaščiteni zaradi posodabljanja ter namestitve protivirusnih programov, se kmalu pojavijo nove vrste okužbe računalnikov ali prevare pri pridobivanju različnih podatkov, s katerimi so oškodovani potencialni uporabniki interneta. Elektronsko poslovanje omogoča čedalje širšo paleto storitev in postaja vedno bolj priljubljeno med ljudmi. Glede na to dejstvo tudi javna uprava v tehnološkem napredku ne zaostaja in ponuja napredne spletne storitve. Ena izmed teh je tudi tema diplomskega dela, in sicer aplikacija elektronskega davčnega poslovanja oziroma e-davki. Gre za nekakšno spletno vložišče dokumentov, ki jih davčni zavezanci posredujemo Davčni upravi Republike Slovenije po internetu.

V diplomskem delu obravnavam varnost elektronskega davčnega poslovanja v Sloveniji, kar zajema tudi opis nastanka interneta ter njegovega delovanja, povezavo e-uprave z internetnimi nevarnostmi, ki prežijo na nas, rešitve in opisa aplikacije e-davki, elektronsko davčno poslovanje nekaterih drugih držav ter pravno ureditev e-poslovanja v Sloveniji.

Ključne besede: splet, e-davki, prevare, spletni kriminal, internet, zaščita, e-uprava

SUMMARY

SECURITY OF ELECTRONIC TAXES IN SLOVENIA

Cyber-criminal rises from year to year because the prevalence and use of internet rises and that makes us a bit more exposed to the risk. The risk is including various intrusions in data base, financial frauds, personal data theft an destroying computer data bases with viruses, trojan horses and worms. We can all do the most for our own safety and protection. That means that we have to update our computer regulary and we have to use anti-virus software protection. From year to year are users of internet awared of his danger, especially the younger generation, older generation have a little bit more problems with that. The objective of cyber criminals is the aquisition and misuse of personal data of internet users. When we allready think that we are protected with our software security programs there comes a new types of computer infections or deception to obtain various data and make damage to potential users of the internet. Electronic commerce provides us with, even wider range of services and his popularity among the people grows. The public administration is also not lagging behind in it's tehnological progress and provides us whit it's advanced internet services, which includes my study that are electronic taxes or as we call it eDavki. You can define it as a sort of on line registrydocuments forwarded by the taxpayers to the tax authorities of Slovenia trough the internet.
In my thesis i discuss the safety of use e-taxes in Slovenia and about invetion of internet, connection to e-government with internet, danger on internet, solutions and description of Slovenian e-taxes an similarity of e-taxes in Slowenia with other countries.

Key words: Cyber-criminal, internet, e-government, e-taxes, safety, protection, danger

KAZALO VSEBINE

KAZALO PONAZORITEV

KAZALO SLIK

1 UVOD

1.1 OPREDELITEV PODROČJA RAZISKOVANJA IN OPIS PROBLEMA

V diplomskem delu se bom osredinila na varnost elektronskega davčnega poslovanja z vidika fizičnih oseb, ki uporabljajo elektronsko davčno poslovanje, na morebitne spletne prevare in vdore, ki prežijo na uporabnike, na to, na kar morajo biti pozorni in kako se lahko sami zaščitijo pred nevarnostmi.
E-uprava kot nova oblika uprave in upravljanja se vsakodnevno srečuje z novimi izzivi. Večina držav že izvaja različne strategije in akcijske načrte, politiki obljubljajo boljše življenje v novi družbi. Uporabniki ob poslušanju in spoznavanju pričakujejo veliko. Če bodo storitve e-uprave zadovoljile njihove potrebe, jih bodo tudi uporabljali, sicer bo ves trud zaman. Torej je vse odvisno od uporabnikov. Storitve morajo biti učinkovite in hitre ter preproste za uporabo in varne. Uporabniki morajo zaupati v mehanizme, ki storitve podpirajo. Zato mora e-uprava skrbno preučiti in uporabiti najnaprednejše, a hkrati zanesljive varnostne tehnologije, da bi si pridobila zaupanje uporabnikov. Z ozaveščenostjo je mogoče zaznati nevarnost, ko se ta pojavi. S takojšnjim odzivom lahko zmanjšamo učinek in izgube. Z reševanjem problema nevarnost odpravimo in s preprečitvijo omogočimo ponovno kritično situacijo (Curtis v: Vintar in Grad, 2004, str. 222).
In kako se varnosti še lahko lotimo? Pomembna koraka sta ozaveščanje in izobraževanje. V primeru e-uprave to ni samo ozaveščanje zaposlenih v upravi, ampak tudi vseh, ki z njo sodelujejo, torej državljanov in zasebnega sektorja. Za zadnjega je tak korak verjetno odveč, saj je ta v elektronskem poslovanju precej korakov pred upravo. Tako je tudi na področju varnosti. Poudarek, ki se pogosto pozablja, je na državljanih, ki so ali bodo uporabljali storitev e-uprave, kajti uporabniki brez zaupanja teh storitev ne bodo uporabljali (Hange v: Vintar in Grad, 2004, str. 223).
Za razvoj elektronskega poslovanja je treba ustvariti komunikacijsko in informacijsko infrastrukturo, omogočiti njeno uporabo z razumnimi stroški in opredeliti pravno podlago (Popovič,Ž., 2011).
Poleg vsega omenjenega je pomembna tudi uporaba aplikacije e-davki. Najprej potrebujemo ustrezno strojno in programsko opremo ter dostop do interneta, kar večina državljanov že ima.

1.2 OPREDELITEV CILJA IN NAMEN TER ZGRADBA

V diplomskem delu bom skušala odgovoriti na hipoteze, kot so:

- V elektronskem davčnem poslovanju so ogroženi osebni podatki.
- E-davke v Sloveniji uporablja čedalje več ljudi.
- Za e-davke je značilnih več prednosti kot slabosti.

Diplomsko delo je razdeljeno na sedem poglavij, ki so medsebojno povezana in tvorijo zaključeno celoto. Najprej bom predstavila pomemben element, brez katerega e-davki sploh ne bi bili mogoči, to je internet. V drugem delu bom opisala nevarnosti elektronskega poslovanja, ki prežijo na uporabnike interneta, v tretjem način zaščite pred njimi, v četrtem bom opredelila e-davke in njihovo delovanje, v petem prikazala primerjalno analizo Slovenije in Avstralije z vidika spletnih prevar ter v šestem statistične podatke glede uporabe e-davkov.

1.3 UPORABLJENE METODE DELA

Osnovna metoda bo študij domače in tuje literature, internetnih virov, uporaba lastnega znanja, pridobljenega na Fakulteti za upravo, ter primerjalna analiza z uporabo podatkov, pridobljenih v spletu.

2 INTERNET

2.1 DELOVANJE INTERNETA IN MOŽNOSTI, KI JIH PONUJA

Ob prvem srečanju z besedo internet se vsakdo vpraša, za kaj sploh gre. Internet je omrežje vseh omrežij, ki povezuje ljudi po vsem svetu. Ni pomembno, kje ste, pomembno je samo, da ste povezani v internet, in že lahko komunicirate s prijatelji iz katerega koli predela sveta. Internet je torej ogromno omrežje računalnikov, v katero lahko vsakdo priključi svoj računalnik, in je tudi ogromna množica ljudi, ki so povezani v omrežje. Lahko bi rekli, da skoraj ni človeka, ki ne uporablja interneta, bodisi za spletno brskanje bodisi za komuniciranje po elektronski pošti. Ljudje pojem interneta večkrat zamenjujejo s svetovnim spletom (World Wide Web – WWW). Rečejo na primer, da so v internetu, v resnici pa mislijo svetovni splet. Začetek razvoja interneta sega v leto 1969, ko so pri ameriškem obrambnem ministrstvu ustanovili Advanced Research Project Agency (ARPA). Ugotovili so namreč, da potrebujejo omrežje za komuniciranje, če želijo preživeti vojno. Zato so si zastavili cilj izdelati omrežje, ki bo še vedno poslalo sporočilo na cilj, čeprav bo del omrežja odpovedal. Uspešen rezultat je bil ARPAnet, ki so ga leta 1983 razdelili na dva sistema: ARPAnet in Milnet. ARPAnet so uporabili za raziskovanje in civilno uporabo, Milnet pa za vojaške namene. Obe omrežji sta bili povezani tako, da so si uporabniki lahko izmenjevali informacije. To je postalo znano pod imenom internet. Sčasoma so se začela uporabljati tudi druga ločena omrežja. Leta 1986 pa so v National Science Foundation izdelali NSFNET, da bi povezali več računalnikov po državi, predvsem v raziskovalne namene. NSFNET je postal hrbtenica interneta, ARPAnet pa so opustili (Honeycutt, 1998, str. 12–16). Z razvojem in inovacijami internet privablja pod svoje obličje vse več ljudi. V njem je mogočih ogromno storitev. Med najbolj uporabljanimi je svetovni splet. Z njim lahko dostopamo do različnih informacij, opravimo marsikatero storitev, podaljšamo rok izposoje knjig v knjižnici, kupujemo, klepetamo, poslušamo radio, beremo novice, igramo igrice ali pa samo prenašamo datoteke ter pošiljamo in prejemamo elektronsko pošto. Internet nam z vsestranskostjo prihrani marsikateri evro. Kljub naštetim številnim storitvam jih internet omogoča še mnogo več, vedno več pa se nam jih obeta tudi v prihodnosti.

2.2 SLABOSTI INTERNETA

Za delovanje interneta potrebujemo povezavo, ki bo računalnik povezala z njim, ker pa je ta sestavljena iz mnogih delov, ne le računalnika, modema in programov, ampak tudi ponudnikovega strežnika, telefonskega omrežja ter drugih sestavnih delov, se lahko zgodi, da povezava ne bo delovala, kot bi morala. Največkrat se lahko srečamo z naslednjimi slabostmi in težavami interneta:

- z nemožnostjo povezave s ponudnikom internetnih storitev;
- s prepočasno in z nezanesljivo povezavo;
- z nedelovanjem strojne opreme;
- z nezmožnostjo pošiljanja in prejemanja elektronske pošte;

- z nezmožnostjo povezave z želeno spletno stranjo;
- z okužbo računalnika z virusi po internetu;
- z vdorom v računalnik in zbirko podatkov;
- z aplikacijama ActiveX in Java, ki ju z brskalnikom prepišemo iz interneta in lahko v našem računalniku izvajata kar koli;
- z vsebinsko neprimernostjo in osebno nevarnostjo za otroke;
- z nevednostjo pri spletnem nakupovanju.

Zelo veliko je bilo primerov, ko so posamezniki po spletu kupovali mobilne telefone, pri tem pa niso prebrali oziroma niso bili previdni, kaj kupujejo, in so le na podlagi slike, ki je bila pripeta oglasu, kupili telefon, za katerega se je pozneje izkazalo, da je v resnici maketa mobilnega telefona.

2.3 VARNOST INTERNETA

»Ko se računalnik poveže z medmrežjem in začne komunicirati z drugimi računalniki, prevzema tveganje. Internetna varnost zajema zaščito računalniškega internetnega računa in zaščito pred vsiljenimi datotekami neznanega uporabnika« (Wikipedia, 2011). Pred omenjenimi napadi računalnik zaščitimo predvsem tako, da se pri brskanju po svetovnem spletu vedemo pametno. Vsako vprašanje, ki nam ga ponudi brskalnik, pozorno preberemo in o njem razmislimo, preden kliknemo na Yes ali OK. Če želi strežnik zamenjati digitalno potrdilo pri sejah https, se pozanimamo, ali je strežnik resnično zamenjal potrdilo ali pa gre mogoče za potegavščino ali celo napad. Vedno preverimo vir informacij. Če opravljamo spletno nakupovanje, preverimo legitimnost prodajalca, preverimo, ali je v skladu z določenimi standardi zaščite, ali uporablja SSL in kako je z njegovim digitalnim potrdilom. Nikoli ne nameščamo programske opreme, ki je ne poznamo in ki je ni preverila ter odobrila ustrezna služba za informacijsko varnost. Računalnik dodatno zaščitimo z uporabo alternativnega brskalnika, ki sicer ni popoln, vendar pa nam odpusti kako napako« (Pinterič in Svete, 2007, str. 182, 183).

2.4 INOVACIJE IN INTERNET

Dandanes je vedno več inovacij, ki se navezujejo na internet. Vedno več znanja je treba, da najdemo smisel vsega, in iskanje znanja je nujno, če želimo izboljšati svoje sposobnosti, da izboljšamo zastavljene cilje in vizijo. Ne dolgo tega so bile na primer telefonske žice edina stvar, ki je povezovala računalnike in modeme v internet. Te žice so bile edina možnost za povezavo, zdaj pa lahko uporabimo prenosni računalnik in brezžični modem (Wi-Fi), s katerim se lahko sprehajamo po hiši, delovni sobi ali pa ga uporabljamo v službi z velikim udobjem, ko brskamo po najljubših spletnih straneh ali gledamo videe. Uporabniške mreže in brezžični internet ponujajo najpriročnejši širokopasovni internet; brezžični signal je posredovan usmerjevalniku in potem prenosnemu računalniku. Se pa inovacije v internetu ne kažejo samo skozi povezavo interneta do računalnika, ampak lahko tudi s stalno rastjo ter z izboljšavo kakovosti slik in videov ter nadgradnjo aplikacij večino videoposnetkov po internetu spremljamo v HD-tehnologiji, poleg tega je hitrost interneta vedno boljša. Vedno več je naprav, ki dostop do interneta sploh omogočajo – od mobilnega telefona do dlančnika in mini prenosnikov. V bližnji prihodnosti se nam obeta še brskanje po internetu kar po televizijskem sprejemniku ter v ponekod že uveljavljenem BeBooku ali e-bralniku, to je napravi, veliki kot knjiga, ki je namenjena branju elektronskih knjig ter drugih elektronskih vsebin; z BeBookom naj bi nadomestili današnje časopise (Olague, 2010).

3 NEVARNOSTI ELEKTRONSKEGA POSLOVANJA

Virusi

»Virus je najpomembnejša in najpogostejša posebna oblika trojanskega konja, ki se lahko razmnožuje in širi, podobno kot biološki virus. Sprogramiran je tako, da vrine kopijo samega sebe v datoteko, ki z njim še ni okužena. Proces se ponavlja in virus se hitro širi. Seveda pa cilj virusa ni samo razmnoževanje. Ko so izpolnjeni določeni pogoji, virus sproža tudi druge bolj ali manj neprijetne in škodljive dogodke, ki v skrajnosti pripeljejo do uničenja podatkov in programov. Velike možnosti za okužbo oziroma širjenje virusov iz enega v drug računalniški sistem so pri nelegalnem kopiranju programov in pri uporabi interneta. Z elektronsko pošto na primer prav lahko pripotuje virus. Virusi napadajo predvsem osebne računalnike. Večji računalniški sistemi zaradi velikosti omogočajo veliko večjo varnost. Imajo obsežnejše in varnejše operacijske sisteme, ki jih varujejo pred virusi« (Gradišar in Resinovič, 1998, str. 439). Prepoznamo jih po različnih simptomih, kot so npr. počasno delovanje računalnika, samodejni ponovni zagon računalnika, zamrznitev računalnika, nedostopnost do nekaterih programov, nenavadna sporočila o napakah in podobne težave z računalnikom.

Trojanski konji

»Trojanski konj je program, ki je sicer uporaben in koristen, vendar vsebuje skrite ukaze. Ti se izvršijo le, kadar je izpolnjen določen pogoj. Izvršijo se na primer, kadar je v obdelavi zapis z določeno matično številko ali z določenim bančnim računom. Obstajata še dve podvrsti trojanskega konja, in sicer tako imenovana časovna bomba ter logična bomba. Časovna bomba je vrsta trojanskega konja, pri katerem se skriti ukazi izvršijo v določenem trenutku, na primer na določen datum. Časovne bombe so največkrat izraz vandalizma in maščevanja nezadovoljnega delavca. Aktivirajo se, ko je delavec že zapustil organizacijo in se zaposlil drugje. Logična bomba je tudi vrsta trojanskega konja, ki se aktivira ob nekem logičnem pogoju, kot je na primer zagon določenega programa« (Gradišar in Resinovič, 1998, str. 439).

Črvi

»Črv deluje podobno kot logična bomba, le da takrat, ko se aktivira, tvori naključna zaporedja bitov in jih zapisuje na diske, dokler jih popolnoma ne zapolni in s tem povzroči padec sistema« (Gradišar in Resinovič, 1998, str. 439). Simptomi trojanskih konjev in črvov so zelo podobni, na primer samodejno formatiranje trdega diska, programi, ki se zaženejo samodejno in se skrivajo kot priloge v elektronski pošti ali pa so skriti v piratskih datotekah.

Skrivna vrata

»Skrivna vrata so zaporedje ukazov, ki uporabniku omogoča, da preskoči standardni varnostni sistem računalnika. Taka skrivna vrata si pogosto izdelajo sistemski inženirji oziroma zaposleni, ki skrbijo za sistemske programe. Omogočajo jim lažji pristop v varnostni sistem. Storilec, ki najde skrivna vrata, pa jih lahko uporabi za kriminalna dejanja« (Gradišar in Resinovič, 1998, str. 439).

Kraja podatkov

»Storilec lahko ukrade podatke, ki so na fizičnih nosilcih, kot so papir, trakovi, diskete, mikrofilmski listi in zgoščenke. Krajo je težko odkriti, če se podatki le prekopirajo. Podatke je mogoče ukrasti tudi v trenutku, ko potujejo po telekomunikacijskih linijah. Način kraje podatkov s prisluškovanjem telefonskim in radijskim zvezam je tehnično zelo zahteven, ne le zaradi težav pri prestrezanju signalov, ampak tudi zaradi težav pri njihovem dekodiranju. S

prisluškovanjem so na primer poskušali prodreti v mrežo bančnih avtomatov in ukrasti denar« (Gradišar in Resinovič, 1998, str. 438).

Goljufivi podatki

»Vnos goljufivih podatkov je najpreprostejša in najpogostejša metoda kraje z računalnikom. Goljufive podatke lahko posredujejo storilci s poneverjanjem dokumentov, tako da skušajo z organizacijskimi predpisi zaobiti določene procedure ali pa se lažno predstavijo. V teh primerih storilci ne potrebujejo prav mnogo računalniškega znanja. Pomembneje je, da vedo, kako deluje organizacijski sistem« (Gradišar in Resinovič, 1998, str. 437).

Parazitni programi

»Parazitne programe delimo v tri kategorije: Adware, Spyware in prikrita omrežja. Večina teh programov pride v računalnik kot priponka ob nameščanju nekega drugega programa, ki ste ga kupili oziroma prenesli v sistem. V primerjavi z računalniškimi virusi, ki se pripnejo drugim programom in vdrejo v sistem, pa so parazitni programi namerno pripeti programom, s katerimi jih dobite. Najbolj znani so programi adware, ki prikazujejo oglase na različnih spletnih straneh, ki jih obiskujete. Take oglase namerno vstavijo lastniki strani, ki jih obiskujemo. Najpogosteje se nam prikazujejo različna tako imenovana pop-up okna. Če jih kliknemo, se odpre novo okno z oglasno vsebino, miselnimi igricami in različnimi drugimi nadležnimi programi. Razlika med programoma spyware in adware je očitna; medtem ko adware dobi naše podatke s klikom nadležnega oglasa, spyware spremlja naše celotno brskanje po spletu in poroča oglaševalskemu strežniku, kar doseže s pregledovanjem zgodovine spletnega brskanja, kjer tudi dobi seznam strani, po katerih smo brskali. Prikrita omrežja pa so omrežja, ki si delijo datoteke, delujejo po principu »peer to peer«. Datoteke so razpršene po več računalnikih, ki si iskalno zahtevo podajajo med seboj, dokler ne najdejo želene datoteke. Tako delujejo programi, kot so na primer Emule, Kazza in podobni« (4secnet, d. o. o., 2006).

Verižna pisma

Verižna pisma so tista, s katerimi računalniški hekerji pod pretvezo pridobivajo elektronske naslove s tem, ko jih posredujemo naprej. Po navadi so povezani s čustveno in z zdravstveno tematiko in nas napeljujejo, da lahko s pošiljanjem naprej pomagamo obolelim. Znana je tudi druga oblika verižnega pisma, v kateri je sporočilo o tem, kaj vse se lahko zgodi, če pisma ne pošljemo naprej. S pošiljanjem naprej pa tudi pošljemo naslove vseh svojih predhodnikov, ki pridejo do izvornega pošiljatelja, ki pa jih lahko izrabi za škodljive namene. Ne dolgo tega se je nekaj podobnega zgodilo slovenski novinarki, katere prijatelji so dobili njeno poneverjeno sporočilo, da je v Angliji in da nujno potrebuje denar. Ker že podatek o njenem poklicu pove, da ima veliko znancev in prijateljev, je logično sklepanje, da je bilo stikov v njenem elektronskem naslovu veliko. Torej je imela srečo, da ji prijatelji denarja niso poslali, kot je bilo zahtevano v elektronskem sporočilu, in da se je vse srečno končalo. Čeprav je sprva mislila, da gre le za šalo, se je šele pozneje zavedla, da se je vse razpletlo brez posledic. Taka sporočila nam namreč lahko naredijo veliko škode, in to tako materialne kot tudi psihične.

Neželeno oglaševanje po e-pošti ali SPAM

»V splošnem lahko kot SPAM obravnavamo vsako sporočilo, ki je poslano večjemu številu naslovnikov, z namenom vsiljevanja vsebine, ki se je naslovniki sami ne bi odločili prejemati. V veliki večini primerov gre za oglaševanje plačljivih storitev ali izdelkov. Po navadi se s pošto SPAM oglašujejo izdelki ali storitve dvomljive kakovosti, velikokrat pa gre za goljufije (značilen primer je nigerijska prevara, ki prevarantom včasih uspe tudi pri nas). Zaradi razširjenosti in neustrezne slovenske besede, ki bi povzela primeren kontekst za neželeno oglaševanje po elektronski pošti, privzemamo kar pojem iz angleščine. Se pa lahko v

elektronskem poštnem sporočilu skriva tudi kaka priponka s prikritim programom, ki vsebuje trojanskega konja ali črva« (4secnet, d. o. o., 2006).

Zloraba podatkov

»Spletni goljufi želijo z lažnimi spletnimi stranmi in elektronskimi sporočili od vas na tak ali drugačen način izvabiti osebne podatke, kot so številke kreditnih kartic, uporabniška imena in gesla, digitalna potrdila in drugi. Pri tem uporabljajo različne tehnike, ki spadajo v domeno t. i. socialnega inženiringa, s tem da poskušajo od uporabnika na zvit način izvabiti osebne podatke. Praviloma najprej postavijo lažno spletno stran, ki je zelo podobna pravi, nato pa od vas z lažnim elektronskim sporočilom poskušajo izvabiti bodisi obisk te strani ali kar takoj pridobiti vaše podatke z vašim odgovorom na to sporočilo« (Informacijski pooblaščenec Republike Slovenije).

Človeške napake

»Človek je lahko za računalniški sistem največja nevarnost in ga lahko ogrozi na več načinov. Nekateri so nepoučeni in nevešči uporabe računalnika ter tako poškodujejo ali uničijo pomembne podatke, medtem ko jih drugi poškodujejo ali uničijo namerno s kršenjem pravil, tako da izrabljajo sistem v svojo korist« (Bratuša, 2006, str. 316). »Vseeno pa mnogo uporabnikov, zlasti sistemov za avtomatizirano pisarniško poslovanje, ne posveča dovolj pozornosti varnosti ali se zanjo sploh ne meni. Poleg tega so tudi druge omejitve človeka, ki povečujejo ranljivost informacijskega sistema« (Gradišar in Resinovič, 1998, str. 442).

Strojne napake in okvare

»Z razvojem računalniške tehnike postaja strojna računalniška oprema vedno zanesljivejša. Občasno pa do okvar vseeno prihaja. Strojne napake povzročijo dve vrsti posledic, med katerima je pomembna razlika. Običajna posledica strojne okvare je prenehanje delovanja. Zaradi vgrajenega neprestanega preverjanja pravilnosti delovanja računalnik večino strojnih napak odkrije sam in se ustavi. S tem prepreči škodo, ki bi nastala zaradi nepravilnih rezultatov. V izjemno redkih primerih pa računalnik kljub okvari deluje naprej in daje napačne rezultate. Ker te vrste okvar ne pričakujemo, je lahko škoda še večja, vendar je verjetnost tako majhna, da jo lahko zanemarimo« (Gradišar in Resinovič, 1998, str. 430).

4 ZAŠČITA PRED NEVARNOSTMI

»Sodobne komunikacijske rešitve omogočajo, da smo vsak trenutek prisotni kjer koli po svetu. Premalo pa se zavedamo tudi nasprotne smeri; dobaviteljem nekaterih programskih rešitev je veliko do tega, da bi iz našega računalnika prišli podatki do nekoga na drugem koncu sveta« (Toplišek, 1998, str. 107).
Zato je priporočljivo oziroma obvezno, da se zaščitimo z ustrezno tehnologijo, ki je predstavljena v nadaljevanju.

Požarni zid

Postavitev požarnega zidu je zelo učinkovita metoda, s katero napadalcem občutno omejimo možnosti za vdor v sistem, hkrati pa omogoča varno uporabo interneta. Za čim večjo učinkovitost in zaščito mora biti požarni zid konfiguriran, nameščen in vzdrževan z veliko natančnostjo (Bratuša, 2006, str. 321). Njegova namestitev oziroma aktivacija je preprosta. Za primer vzemimo Windows XP. V meniju Start izberemo Nadzorna plošča, kjer pod ikono Sistem in varnost poiščemo požarni zid programa Windows. Kliknemo preverjanje statusa požarnega zidu, da se odpre novo okno, ki pove, ali je požarni zid vklopljen. Če je ikona ščita zelene barve, je požarni zid vklopljen, v primeru rdečega ščita pa je požarni zid izklopljen in ga je priporočljivo vklopiti.

Protivirusni programi

»Za hekerska orodja, viruse in trojanske konje so značilni prepoznavni načini za spreminjanje napadenega sistema. Te značilne spremembe so spremembe določenih datotek, vnosov v register in zaganjanje specifičnih procesov v napadenem računalniku. Vse opisane značilnosti so nekakšni prstni odtisi, ki so dobro znani protivirusnim programom. Tako protivirusni programi zaznajo in preprečijo škodljive dejavnosti« (Bratuša, 2006, str. 327). Protivirusne programe lahko prenesemo iz spleta tudi brezplačno. Gre za programe, ki so označeni kot freeware, vendar pa niso tako kakovostni kot plačljivi programi software, ki omogočajo popolno zaščito računalnika.

Posodobitve operacijskega sistema

Operacijski sistem posodobimo s paketom »service pack« in z zadnjimi popravki iz interneta. Tako bo varnejši in hitrejši. To lahko storimo po istem postopku, kot smo vklopili požarni zid, le da v meniju Sistem in varnost kliknemo posodobitve programa Windows, ki jih lahko nastavimo na samodejno ali pa ročno posodabljanje. Če želimo malo drugače posodobiti sistem Windows, pa se v spletu povežemo z Microsoftovo stranjo, kjer so na voljo vse posodobitve za posamezne različice operacijskega sistema Windows. Opisana posodobitev operacijskega sistema velja zgolj za Windows XP, v primeru drugih operacijskih sistemov pa so posodobitve na voljo na spletni strani proizvajalca.

Elektronski podpis

»Elektronski podpis je nadomestek lastnoročnega podpisa v elektronskem poslovanju in je namenjen preverjanju pristnosti podatkov ter identifikaciji podpisnika. Digitalni podpis omogoča še lažjo razsodbo v primeru, ko podpisnik zanika, da bi bil podpis njegov. Ker je praktično nemogoče določiti zasebni ključ, ki je znan le njegovemu lastniku, takega podpisa ne moremo ponarediti. Identiteto podpisnika lahko popolnoma preverimo vsakič, kadar preverjamo digitalni podpis. Pri lastnoročnih podpisih pa lahko avtentičnost podpisa potrdi le grafolog« (Jerman Blažič, 2001, str. 106, 107).

Digitalna potrdila

»Digitalno potrdilo je digitalno podpisan računalniški zapis, ki vsebuje naslednje podatke: različico formata, enolično številčno oznako, identifikator algoritma, s katerim je bil izdelan digitalni podpis digitalnega potrdila, razločevalno ime agencije, ki je izdala digitalno potrdilo, obdobje veljavnosti digitalnega potrdila, razločevalno ime lastnika javnega ključa in druge podatke. Po svetu je veliko različnih agencij za certificiranje javnih ključev, ki se lahko med seboj logično povezujejo« (Jerman Blažič, 2001, str. 110, 111).

Gesla

»Slabo je, če za geslo izberemo kar uporabniško ime ali kombinacijo imena in priimka (na primer petram/petram ali mejakp/petra). Pri napadih na gesla ne smemo pozabiti na še eno šibko točko sistema. Če ima uporabnik dobro, močno geslo, ki si ga je žal težko zapomniti, si ga je verjetno tudi nekam zapisal. Upajmo, da to ni nalepka na robu računalniškega zaslona ali na spodnji strani tipkovnice. Strokovnjaki za gesla svetujejo, naj si uporabniki izbirajo gesla, ki jih lahko povežejo z realnim svetom in si jih zato lažje zapomnijo; na primer geslo ljubitelja pravljic bi bilo lahko 3prasickiSoSliNaa2gugalnici« (Pinterič in Svete, 2007, str. 186, 187).

Protokol SSL

»Za zaščito transakcij v svetovnem spletu se najpogosteje uporabljajo protokoli SSL (Secure Sockets Layer), TLS (Transport Layer Security) in WTSL (Wireless Transport Layer Security), slednji pri poslovanju na podlagi brezžičnih povezav. Bistvo vseh postopkov je v tem, da vzpostavijo varen kanal med strežnikom in odjemalcem, na primer spletnim brskalnikom. Vsem informacijam, ki potujejo po takem kanalu, so lahko zagotovljene zaupnost, neokrnjenost in avtentičnost izvora. Protokol SSL pogosto uporabljajo banke v elektronskem bančništvu. Uporabnik se najprej prepriča, ali res komunicira s pravim bančnim strežnikom. Hkrati lahko tudi strežnik preveri identiteto stranke, saj mora biti dostop do bančnega računa dovoljen le pooblaščenim osebam. Po vzajemnem overjanju SSL zagotovi neokrnjenost izmenjanih podatkov, na primer vrednost nakazila in zaupnost informacij« (Jerman Blažič, 2001, str. 119).

5 PRIMERJALNA ANALIZA SLOVENIJE Z AVSTRALIJO

5.1 PRIJAVA IN UPORABA E-DAVKOV

»E-davki zagotavljajo davčnim zavezancem udobno, preprosto in varno poslovanje z Davčno upravo Republike Slovenije po spletu. Uporabnik e-davkov lahko postane vsak davčni zavezanec. Za uporabo te storitve potrebuje le računalnik s primerno opremo, dostop do interneta in ustrezno digitalno potrdilo. E-davki so elektronsko vložišče, ki jih davčni zavezanci, bodisi fizične bodisi pravne osebe, oddajajo Davčni upravi Republike Slovenije. Tako pridejo informacije hitreje in ceneje v davčni informacijski sistem« (DURS, 2004, str. 4). Za uporabo e-davkov boste potrebovali najprej digitalno potrdilo, ki ga lahko pridobite na podlagi oddane vloge za digitalno potrdilo. To lahko storite brezplačno pri upravni enoti (SIGEN CA, SIGOV CA), proti plačilu pa ga lahko pridobite tudi pri Novi Ljubljanski banki (AC NLB) za uporabnike storitev Klik in Proklik+, Pošti Slovenije (POŠTARCA) ter družbi Halcom informatika (HALCOM CA) za uporabnike storitev Proklik.
»Digitalno potrdilo, imenovano tudi certifikat, v elektronskem poslovanju nadomešča osebno legitimacijo davčnega zavezanca. S potrdilom in pripadajočim zasebnim ključem vzpostavi davčni zavezanec z e-davki varno komunikacijsko povezavo po spletu« (DURS, 2004, str. 6).
V štirinajstih dneh boste po pošti priporočeno prejeli geslo, s katerim aktivirate oziroma prevzamete digitalno potrdilo, povezavo do njega pa prejmete po elektronski pošti. Sistem vas po korakih vodi do dokončnega prevzema digitalnega potrdila. Ko ste prevzeli digitalno potrdilo, ki je zdaj shranjeno v računalniku, izdelajte varnostno kopijo, jo zaščitite z dodatnim geslom in shranite na disketo. V primeru formatiranja računalnika in nepredvidenih nevšečnosti bo prišla še kako prav. Ob prvem obisku portala eDavki boste morali potrdilo pred vstopom prijaviti, sistem pa vas bo znova vodil skozi postopek. Po vstopu v portal in uspešni prijavi so vsi naši podatki na voljo za vpogled. Portal omogoča shranjevanje izpolnjenih obrazcev, oddajo davčnih obrazcev, vpogled v arhiv že oddanih dokumentov na podlagi sistema e-davki, predizpolnitev določenih podatkov in dve novosti, ki sta na voljo od maja 2010, to sta storitev IREK – informacija o razkritju podatkov o obveznih prispevkih za socialno varnost iz delovnega razmerja, ki omogoča vpogled v te podatke, ter eKartica, pri kateri gre za storitev e-knjigovodske kartice zavezanca za davek, s katero lahko vsak zavezanec za davek sproti preverja stanje na svoji knjigovodski kartici, kar omogoča večjo obveščenost o stanju terjatev in obveznosti. E-davki pa omogočajo preprosto uporabo storitev zgolj uporabnikom Microsoftovih programov, ki uporabljajo le en spletni brskalnik, saj so nekateri uporabniki e-davkov v forumih izrazili nejevoljo zaradi težav, ki jim jih povzroča ta spletna aplikacija v operacijskih sistemih Linux in Mac OS X. Vendar pa, kakor je mogoče razbrati s spletne strani Davčne uprave Republike Slovenije, je tudi ta težava že minimalizirana, zato lahko pričakujemo, da bo tudi kmalu popolnoma izničena.

5.2 PRIMERJAVA PREVAR V AVSTRALIJI IN SLOVENIJI

Glede na podatke, pridobljene v spletu, se v Avstraliji vsako leto pojavljajo spletne prevare, medtem ko o vdorih v davčni sistem ne poročajo. Tako imenovani kibernetski kriminalci so se raje osredinili na lažjo tarčo, tj. davčne zavezance. Glede na rastočo popularnost spletnega

davčnega poslovanja je verjetnost, da bodo spletni uporabniki avstralskega spletnega davčnega poslovanja postali žrtve kibernetskega kriminala, toliko večja. Zaslediti je mogoče več prevar, ki kažejo, da človeška domišljija nima meja. Eden izmed poskusov prevare avstralskih davkoplačevalcev je prevara z elektronsko pošto, ki vsebuje povezavo na spletno stran, na kateri davčne zavezance vabijo, naj jim zaupajo številko kreditne kartice ali podrobnosti o bančnem računu, pod pretvezo, da bo avstralska davčna uprava davčnim zavezancem predčasno izplačala denar. Prav tako se je pojavljala elektronska pošta, ki naj bi pod pretvezo prihajala iz davčne uprave, vendar pa z davčno upravo ni imela nobene povezave. V sporočilu je bila zahteva, naj uporabniki posodobijo digitalno potrdilo. Ti so lahko, misleč, da ravnajo pravilno, v računalnik nevede namestili trojanskega konja.

Slika 1: Primer prevare po elektronski pošti

Example (June 2009)

Subject: Taxation Office - Tax refund - Message ID: XUKRVIZSKG

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $210.75 AUD . Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

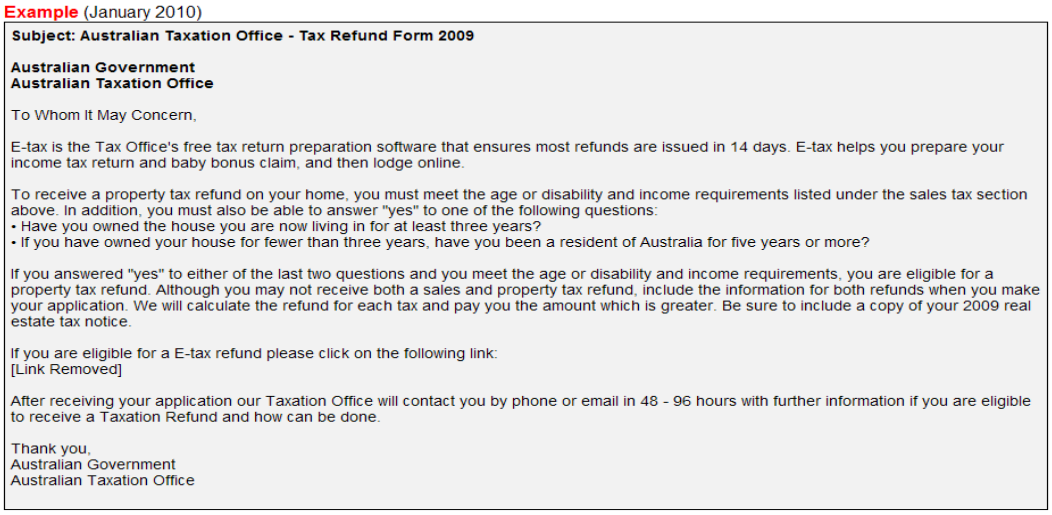
To access the form for your tax refund, please click here

Regards,
Australian Taxation Office

Vir: Christiensen, 2011

Zelo podobne prevare se pojavljajo tudi v Veliki Britaniji, Kanadi in Združenih državah Amerike. Letos pa so se pojavile nove oblike elektronske pošte, s katerimi prevaranti pod pretvezo, da gre za sporočila avstralske davčne uprave, širijo nov način prevarantske pošte. V njej obljubljajo povračilo davkov in vas vabijo, da kliknete navedeno povezavo do spletne strani z obrazcem, v katerega naj bi vpisali osebne podatke, če ste na katero koli vprašanje odgovorili pritrdilno. Vprašanja so na primer taka: Ali ste lastnik hiše, v kateri živite, več kot tri leta? Če ste lastnik hiše manj kot tri leta, ali ste rezident Avstralije pet let ali več? S takim načinom prevare so se prevaranti želeli polastiti osebnih podatkov.

Slika 2: Primer prevare po elektronski pošti (2)



Example (January 2010)

Subject: Australian Taxation Office - Tax Refund Form 2009

Australian Government
Australian Taxation Office

To Whom It May Concern,

E-tax is the Tax Office's free tax return preparation software that ensures most refunds are issued in 14 days. E-tax helps you prepare your income tax return and baby bonus claim, and then lodge online.

To receive a property tax refund on your home, you must meet the age or disability and income requirements listed under the sales tax section above. In addition, you must also be able to answer "yes" to one of the following questions:
• Have you owned the house you are now living in for at least three years?
• If you have owned your house for fewer than three years, have you been a resident of Australia for five years or more?

If you answered "yes" to either of the last two questions and you meet the age or disability and income requirements, you are eligible for a property tax refund. Although you may not receive both a sales and property tax refund, include the information for both refunds when you make your application. We will calculate the refund for each tax and pay you the amount which is greater. Be sure to include a copy of your 2009 real estate tax notice.

If you are eligible for a E-tax refund please click on the following link:
[Link Removed]

After receiving your application our Taxation Office will contact you by phone or email in 48 - 96 hours with further information if you are eligible to receive a Taxation Refund and how can be done.

Thank you,
Australian Government
Australian Taxation Office

Vir: Christiensen, 2011

Pri nas do poskusa vdorov v portal e-davkov domnevno naj ne bi prišlo, prav tako ni zaslediti nobenih prevar po elektronski pošti glede e-davkov. Sem pa zasledila poskus prevare v spletni aplikaciji KLIK Nove Ljubljanske banke, in sicer poskus vstopa z lažno vstopno stranjo v spletno aplikacijo, na kateri pa sta v primerjavi s pravo stranjo še virtualna tipkovnica in ključavnica, ki se pojavi v desnem spodnjem kotu, na izvirni strani je rumena, na lažni pa siva. Na lažni strani se pojavi zahteva, da vpišite svoje geslo in izvozite svoje digitalno potrdilo. Prav tako sem zasledila prevaro, pri kateri gre za izbris digitalnega potrdila iz računalnika, sistem pa ob vstopu v KLIK ponudi novo digitalno potrdilo. V takih primerih se je treba prepričati, ali gre res za pravega izdajatelja digitalnega potrdila, kar povesta serijska številka potrdila in overitelj potrdila, kar bi v tem primeru lahko bil samo AC NLB. Kot pa navaja Janez Zalaznik na spletni strani časnika Dnevnik, so zelo pogosta lažna in zavajajoča elektronska sporočila z zelo podobnih naslovov (na primer info@nlb.tw ali info@n1b.com) (Zalaznik, 2006).

5.3 PRIMERJAVA ZAŠČITE UPORABNIKOV E-DAVKOV V AVSTRALIJI IN SLOVENIJI

Slovenski uporabniki e-davkov uporabljamo tako imenovano digitalno potrdilo, medtem ko so avstralski uporabniki oziroma njihova davčna uprava prešli s sistema digitalnega potrdila na tako imenovani AUSkey. Bistvena razlika med njima je, da je rok uporabe digitalnega potrdila omejen medtem ko je pri AUSkey neomejen, če je uporabljen vsaj enkrat letno. Za AUSkey se lahko uporabnik hitro in preprosto registrira kar po internetu, medtem ko moramo pri digitalnem potrdilu oddati vlogo, AUSkey se lahko uporabi skoraj takoj, medtem ko moramo za digitalno potrdilo čakati približno štirinajst dni, vendar pa je tudi za pridobitev ključa Auskey potrebna nekakšna vrsta identifikacije, torej če še uporabniki nimajo digitalnega potrdila, lahko pridobijo AUSkey podjetniki, ki imajo številko ABN. To je unikatna enajstmestna številka, ki jo uporablja podjetje, ko posluje z drugimi podjetji. Na primer v Avstraliji morajo podjetniki napisati številko ABN na svoje dokumente, ki so v zvezi s prodajo, ki jo podjetje izvede. Če ta številka ni vpisana, ima drugo podjetje po zakonu pravico zadržati 46,5 odstotka kakršnega koli plačila. Za fizične osebe pa ni nikjer omenjena pridobitev ključa

AUSkey, torej se identifikacija opravi na podlagi vložene vloge pri pristojnem upravnem organu. AUSkey omogoča lažjo namestitev na USB-ključ, v osebni računalnik ali oba, medtem ko lahko digitalno potrdilo prevzamemo le prek računalnika z geslom, prejetim po pošti, in ga lahko šele potem izvozimo na prenosni pomnilniški nosilec. Standardni AUSkey je mogoče videti, nadgraditi ali prekiniti kar prek spletne organizacije. Administrator AUSkey, ki je namenjen pravnim osebam in podjetjem, pa lahko v primerjavi s standardnim AUSkey registrira druge ljudi, ki so zaposleni v domnevnem podjetju za AUSkey, in vidi, nadgradi ali prekine kateri koli AUSkey, povezan s svojim podjetjem. AUSkey zaposlenim omogoča dostop do informacij v vladnih organizacijah in s tem do vseh potrebnih podatkov za sklepanje poslov z drugimi podjetji. Zaposleni torej uporabljajo AUSkey pri poslovanju in sklepanju pogodb za podjetje. Pri nas pa poznamo več digitalnih potrdil, in sicer za fizične osebe, za zastopnike pravnih oseb oziroma fizičnih oseb z dejavnostjo, zastopnike državnih ustanov, zaposlene pri pravni osebi oziroma pri fizični osebi z dejavnostjo ter za zaposlene v javni upravi.

5.4 VARNOST V E-DAVKIH

»E-davki so storitev, ki jo slovenska davčna uprava ponuja slovenskim državljanom, in zagotavljajo varno poslovanje z uporabe najsodobnejše tehnologije, zakonskimi določbami in uporabnikovo osebno odgovornostjo. Za varnost podatkov je pri uporabi e-davkov poskrbljeno po najvišjih standardih, ki veljajo v svetu za elektronsko poslovanje po internetu. V spletni storitvi e-davki je varnost zagotovljena z ukrepi, predstavljenimi v nadaljevanju.

Identifikacija uporabnika – Uporabnik sistema se ob vstopu v e-davke identificira z osebnim kvalificiranim elektronskim potrdilom, ki mu določa poslovanje v skladu z njegovimi pooblastili.
Identifikacija strežnika – Prijava uporabnika v sistem preveri tudi identifikacijo strežnika. Tako je uporabnik zavarovan pred pošiljanjem podatkov v goljufivi strežnik.
Zaščitena internetna povezava – Komunikacija med uporabnikovim računalnikom in strežnikom e-davkov je šifrirana, kar preprečuje nepovabljeni vpogled v uporabnikovo poslovanje.
Preverjanje celovitosti podatkov – Strežnik dokument ob prejetju preveri in ga uporabniku ponudi v podpis. S tem je odpravljena možnost, da bi bili zaradi morebitnih tehničnih napak v e-davke vloženi nepopolni dokumenti.
Podpisovanje dokumentov – Ko uporabnik v e-davkih vloži dokument, ga elektronsko podpiše. Postopek podpisovanja vključuje prepisovanje grafično popačene slikovne kode, ki preprečuje vdor samodejnim trojanskim konjem (varnostni sistem, ki je znan tudi kot Captcha).
Časovni žig – Vsi dokumenti v e-davkih se ob podpisu žigosajo s časovnim žigom SIGOV-CA TSA. Z enoličnim določanjem časa oddaje ne glede na lokalne nastavitve strežnika ali uporabnikovega računalnika je onemogočeno ponarejanje časa oddaje dokumenta.
Neizpodbitnost dejanj – Podpis z elektronskim potrdilom in časovni žig na dokumentu pravno zagotavljata neizpodbitnost podpisnika in časa oddaje. Elektronska povratnica, ki jo izda strežnik ob prejetju dokumenta, je za davčnega zavezanca enakovreden pravni dokaz.
Beleženje dogodkov – Vsi dogodki (vpogled v podatke, oddaje dokumentov in spremembe pooblastil) so zabeleženi v dnevniku dogodkov. To velja za vse uporabnike, vključno za poslovne skrbnike – davčne referente.
Varnost strežnikov – Strežniki so pred zunanjim svetom zavarovani z več požarnimi zidovi, ki ščitijo podatke in sistem pred nepooblaščenim vdorom« (DURS).

5.5 VARNOST V E-DAVKIH V AVSTRALIJI

Pri avstralski davčni upravi deluje spletna stran avstralskega poslovnega registra. Obseg varnostnega nadzora se uporablja za zaščito spletnih strani pred nepooblaščenim dostopom, da so informacije zaščitene, medtem ko jih uporabniki zbirajo, hranijo ali podajajo skozi spletno stran avstralskega poslovnega registra. Kljub tem zaščitam pa morajo vedeti, da je svetovni splet nevarno socialno omrežje za potencialne uporabnike, kajti njihove transakcije lahko vidijo, prestrežejo ali spremenijo tretje osebe, datoteke, ki jih uporabnik prenese, pa lahko vsebujejo računalniške viruse, onemogočitvene kode, črve ali druge naprave in napake. Avstralski poslovni register ne prevzema nikakršne odgovornosti za kakršne koli motnje, škodo v uporabnikovem računalniškem sistemu, na programski opremi ali glede podatkov, povezanih s to spletno stranjo. Uporabnike spodbujajo, da sprejmejo ustrezne in

zadostne varnostne ukrepe, z namenom zagotovitve, da je karkoli, kar je izbranega na tej strani, brez virusov ali drugih okužb, ki se lahko vmešajo ali poškodujejo uporabnikov računalniški sistem, programsko opremo ali podatke, kar jim zagotavlja tudi potrjena izjava uporabnika.
Spletna stran avstralskega poslovnega registra (Australian Business Register – ABR) ima dve obliki zaščite:

- šifriranje SSL (Secure Socket Layer), ki zagotavlja varno povezavo med uporabnikom in spletno stranjo ABR;
- PKI (Public Key Infrastructure), tj. digitalno potrdilo, ki se uporablja za preverjanje identitete uporabnika, kar prispeva k zagotovitvi varnosti elektronskih transakcij z ABR.

Uporabniki lahko izberejo ABR AUSkey ali digitalno potrdilo ATO, da se prijavijo na spletno stran avstralske davčne uprave.
Varnostni ukrepi so zagotovljeni tako, da so v pomoč pri zagotovitvi zaupnosti in celovitosti posredovanih podatkov v spletne strežnike ABR in iz njih. Uporabniki so lahko prepričani, da so posredovani podatki vidni le za osebje ABR, ne pa tudi za druge uporabnike. Informacije bodo uporabljene samo za namene, ki jih dovoljuje zakon (Davčna uprava Avstralije).

Pri avstralskem davčnem uradu so ob koncu finančnega leta 2006 prejeli 1.235.000 vlog davčnih zavezancev, kar je 10,8 odstotka davčnih zavezancev, leta 2007 se je število oddanih vlog povečalo na 1.500.000, kar znaša 13 odstotkov, leta 2008 pa jih je že oddalo kar 1.900.000 davčnih zavezancev, to je kar 16,5 odstotka. Podatki za leto 2009 niso na voljo, vendar pa je glede na dani vzorec videti, da število uporabnikov spletnega davčnega poslovanja raste (Miletic, 2008).

Slika 3: Število uporabnikov v Avstraliji

Vir: lasten, 2011

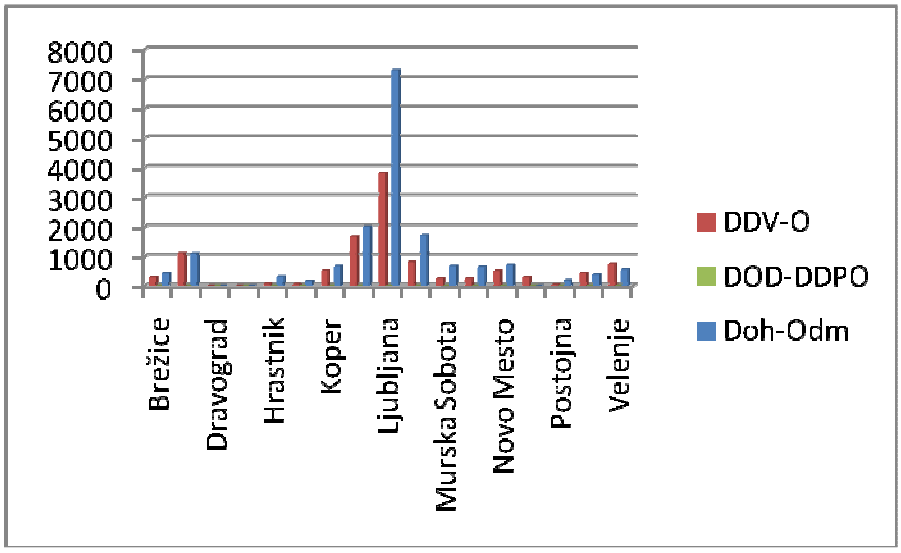
5.6 AUSKEY – NOVOST V E-DAVKIH V AVSTRALIJI

ATO (avstralska davčna uprava) je razvila novi program, ki bo nadomestil v preteklih letih uporabljana digitalna potrdila. Ta potrdila so elektronska varnostna datoteka, ki uporabnikom omogoča dostop do spletnih portalov, v katerih zadržujejo ustrezne informacije o davčnih zavezancih. Uporabniki se lahko prijavijo za svoj AUS-ključ od aprila 2010 kar po spletu. AUS-ključ je lahko nameščen v računalnik, na USB-ključ ali oba. Rok uporabe ključa AUS ne poteče nikoli, če je uporabljen vsaj enkrat letno, medtem ko je rok uporabe digitalnih potrdil potekel vsake tri leta in ga je bilo treba obnoviti. AUS-ključ uporabnikom omogoča dostop do spletnih aplikacij avstralske davčne uprave, avstralskega poslovnega registra ter drugih poslovnih in gospodarskih spletnih aplikacij v prihodnosti (McLoughlin, 2010).

6 STATISTIČNI PODATKI UPORABE E-DAVKOV PO UPRAVNIH ENOTAH

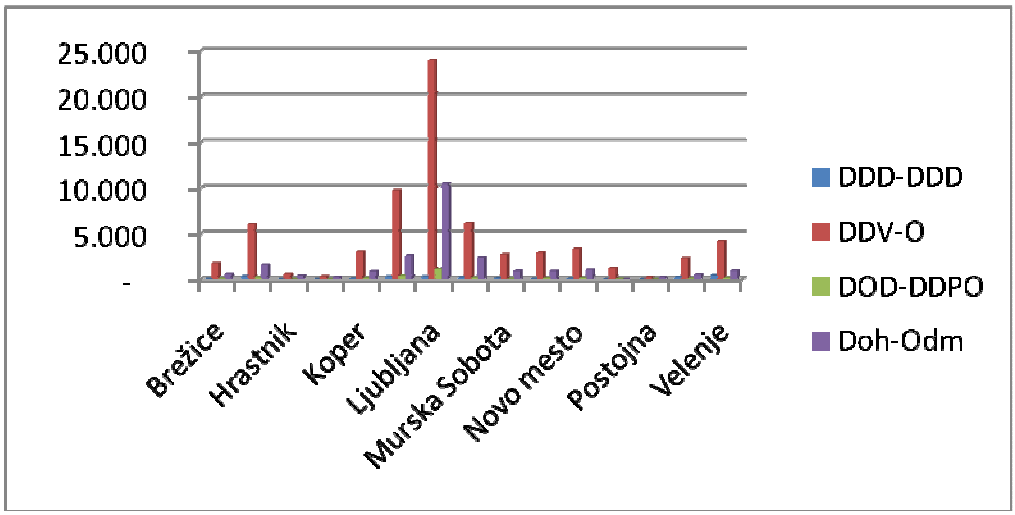
Leta 2004, ko je davčna uprava začela izvajati spletno storitev e-davki, je bilo uporabnikov bolj malo, pa vendar so se prebivalci Slovenije odločali za oddajo obrazca za obračun davka na dodano vrednost (DDV-O) po spletu, ki mu sledi obračun davka od dobička pravnih oseb (DOD-DDPO), medtem ko je oddaja napovedi za odmero dohodnine minimalna (Doh-Odm). Kot kažejo podatki DURS-a, je bilo največ uporabnikov e-davkov z območja Ljubljane in Kranja, medtem ko jih je bilo najmanj z območja Dravograda, od koder ni bilo nobenega uporabnika storitve e-davki, kar pa se je spremenilo že naslednje leto, ko je po številu uporabnikov zadnje mesto zasedla Postojna, Ljubljana in Kranj pa ostajata na vrhu. Od leta 2005 je v e-davkih omogočeno tudi oddajanje novega obrazca, in sicer napovedi za odmero davka od dohodkov iz dejavnosti (DDD-DDD). Leta 2004 je bilo med uporabniki največ fizičnih oseb, medtem ko so bile pravne in fizične osebe, ki opravljajo dejavnost, v manjšini, kar pa se je spremenilo že naslednje leto, saj je oddaja obrazcev za odmero dohodnine močno upadla, kar bi lahko pripisali spremembi zakona, ki davčne zavezance, fizične osebe, odvezuje oddaje obrazca za napoved za odmero dohodnine, medtem ko je oddaja obračuna DDV-ja močno v porastu.

Slika 4: Statistični podatki uporabe po upravnih enotah leta 2004



Vir: lasten, 2011

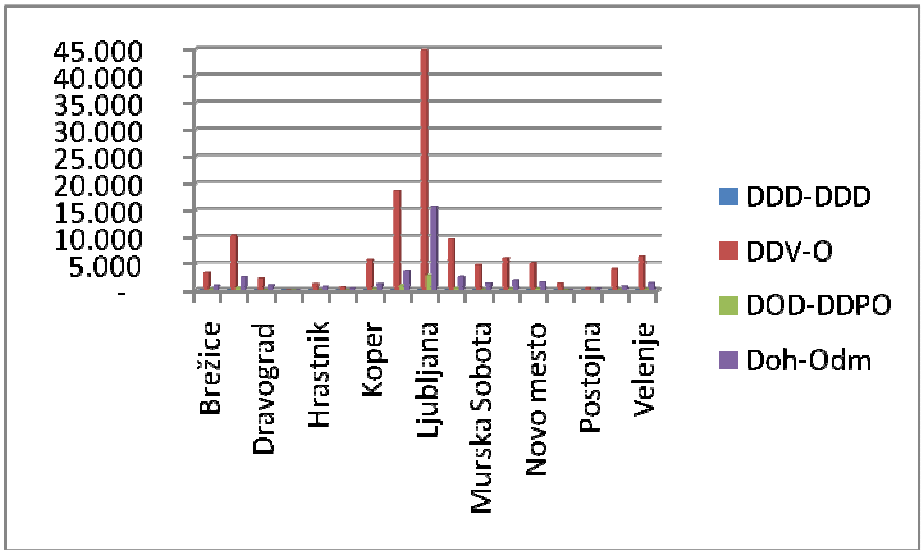
Slika 5: Statistični podatki uporabe po upravnih enotah leta 2005



Vir: lasten, 2011

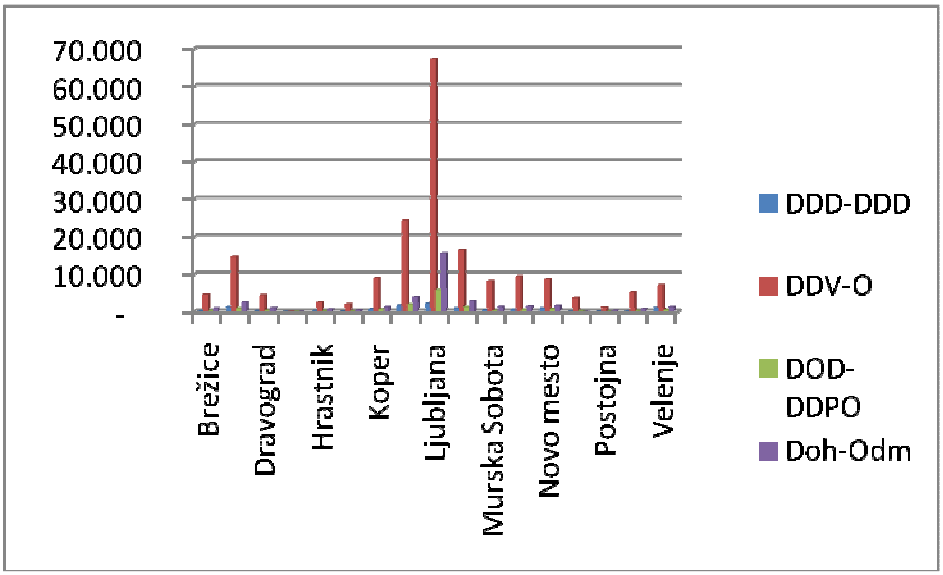
Bistvenih sprememb v letih 2006 in 2007 pri oddaji napovedi dohodnine ni bilo, so pa bile pri oddaji obrazca napovedi za odmero davka od dohodkov iz dejavnosti, ki se je iz leta 2006, ko je obrazec oddal le en uporabnik iz Kranja, povečala na 10.040 skupno oddanih dokumentov po vsej Sloveniji. Zaznati je mogoče porast oddaje obrazca za obračun DDV-ja, in sicer za 64.071 uporabnikov, ter obrazca za obračun davka od dobička od pravnih oseb za 7736 uporabnikov.

Slika 6: Statistični podatki po upravnih enotah leta 2006



Vir: lasten, 2011

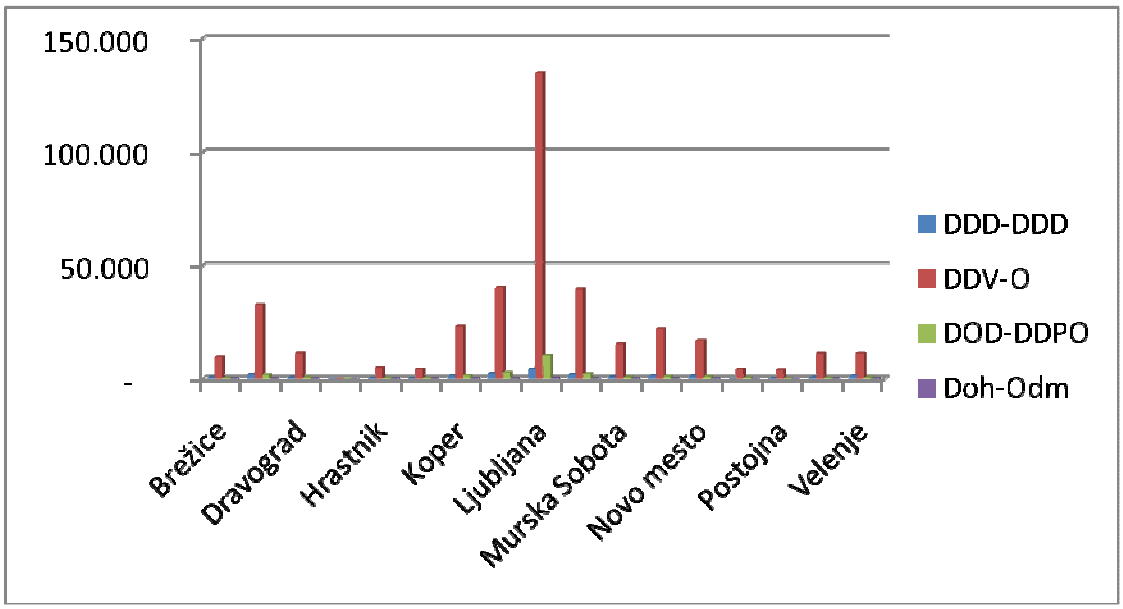
Slika 7: Statistični podatki po upravnih enotah leta 2007



Vir: lasten, 2011

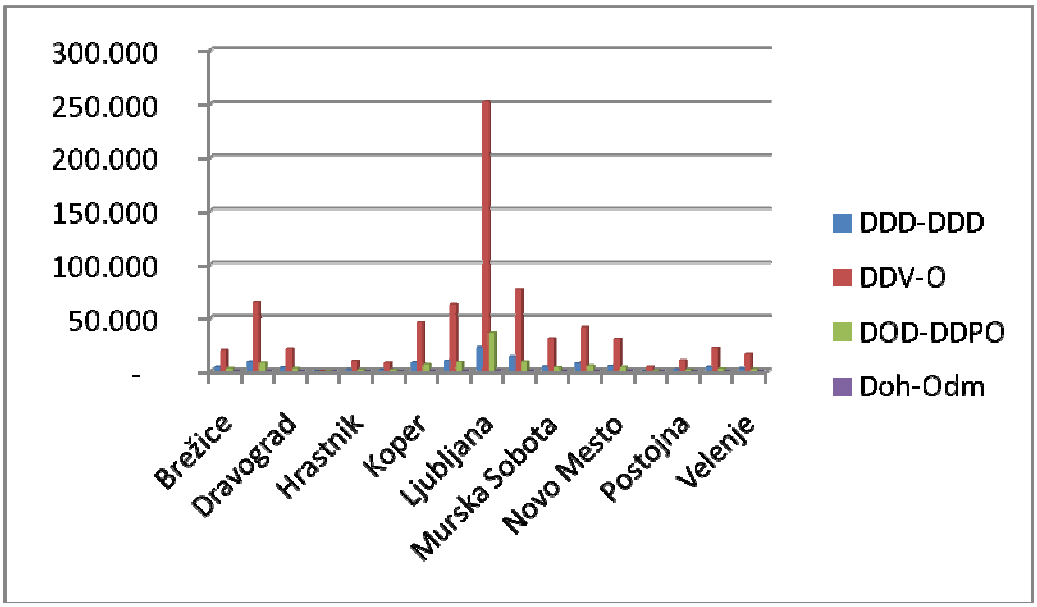
V letih 2008 in 2009 je zelo očiten porast oddaje obrazca napovedi za odmero od dohodkov iz dejavnosti, ki se je iz leta 2008 z 20.147 oddanih dokumentov povečal na kar 98.345 oddanih dokumentov v letu 2009. Porast oddanih dokumentov iz leta 2008 je zaznati še pri oddaji obračuna DDV-ja, in sicer s 386.317 na 712.513, ter pri oddaji obračuna davka od dobička pravnih oseb. Oddaja napovedi za odmero dohodnine pa naglo pada, in sicer z 811 oddanih dokumentov v letu 2008 na 740 oddanih dokumentov v letu 2009. Tudi v letih 2008 in 2009 so največ dokumentov po spletu oddali občani iz Ljubljane, najmanj pa iz občin Postojna v letu 2008 in Kočevje v letu 2009. Leta 2010 ni mogoče primerjati z drugimi statističnimi podatki, ker so pridobljeni le za čas do 21. 6. 2010, in ne kažejo realne slike, vendar je mogoče po do tedaj oddanih dokumentih oceniti, da bosta obrazca za napoved odmere davka od dobička od pravnih oseb in obračun davka od dobička pravnih oseb presegla število oddanih dokumentov iz prejšnjih let razen obrazca napovedi za odmero dohodnine, ki je v polovici letošnjega leta dosegla le 168 oddanih dokumentov. Število oddanih dokumentov napovedi za odmero dohodnine v letošnjem letu torej ne bo preseglo števila 400, kar potrjuje tezo o naglem padcu števila uporabnikov, ki oddajajo ta dokument po spletu.

Slika 8: Statistični podatki po upravnih enotah leta 2008



Vir: lasten, 2011

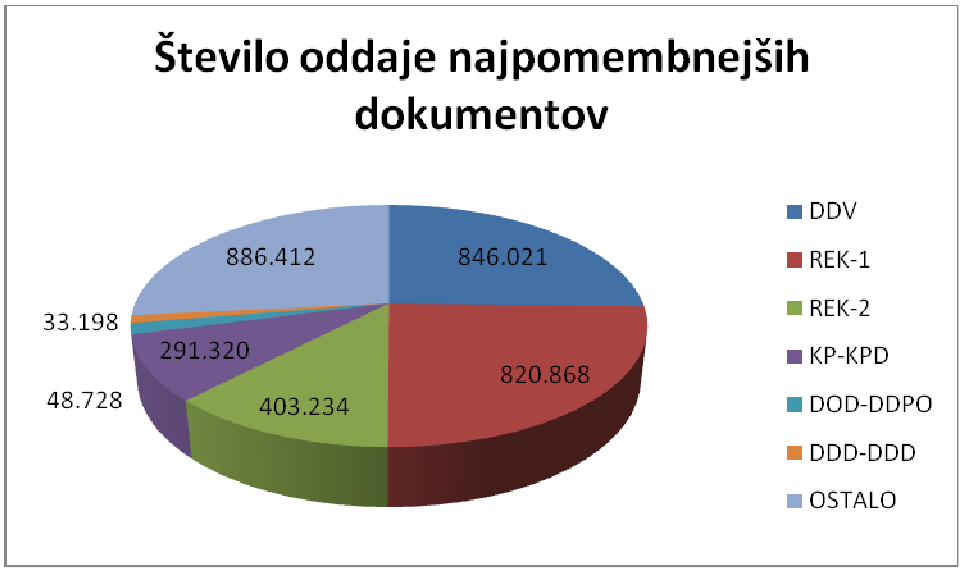
Slika 9: Statistični podatki po upravnih enotah leta 2009



Vir: lasten, 2011

Največ oddaj v e-davkih je za obračun DDV-ja, obračun davčnih odtegljajev od dohodkov iz delovnega razmerja ter obračun davčnih odtegljajev od dohodkov ZDoh-2, ki niso dohodki iz delovnega razmerja. Vsi drugi dokumenti dosegajo skupaj le četrtino vseh oddanih dokumentov.

Slika 10: Število oddaje najpomembnejših dokumentov



Vir: lasten, 2011

7 ELEKTRONSKO POSLAVANJE NEKATERIH DRUGIH DRŽAV

7.1 ELEKTRONSKO DAVČNO POSLOVANJE V AVSTRIJI

Slika 11: Spletna stran e-davkov v Avstriji

Vir: Ministrstvo za finance Avstrije, 2011

Avstrijska spletna stran tako imenovanih e-davkov se v Avstriji imenuje FinanceOnline. Finance oziroma davki po spletu obsegajo elektronsko prenašanje podatkov z metodo avstrijskega finančnega upravljanja, ki temelji na internetni tehnologiji. Ta stran deluje za vse državljane, podjetnike in skupnosti. Dostop do te strani imajo od leta 2003. Prednosti njihove strani so, da je aplikacija na voljo brezplačno 24 ur na dan, da je mogoče urejanje uradne poti z enim klikom iz naslonjača ter da za obisk te spletne strani uporabniki ne potrebujejo posebne programske opreme. Za vsakršno pomoč je vsem na voljo brezplačna telefonska številka. Pri zaščiti spletne strani so se potrudili in avstrijske uporabnike zavarovali z najvišjo ravnjo zaščite, ki so jo izvedli s kodiranjem za zaščito osebnih podatkov in z uporabo najnovejše tehnologije na trgu. Poleg tega pa njihove varnostne ukrepe redno preverjajo tretje osebe. Uporabnik se lahko prijavi v sistem FinanzOnline z uporabniškim imenom (TID), ki je nespremenljivo, z identifikacijo uporabnika (Benid), ki jo lahko izbere sam, in z osebno identifikacijsko številko (PIN), ki jo je prav tako mogoče izbrati (razen Start-PIN), te varnostne kode uporabnik pridobi pri avstrijski davčni upravi (Ministrstvo za finance Avstrije).

7.2 ELEKTRONSKO DAVČNO POSLOVANJE V NEMČIJI

Slika 12: Spletna stran e-davkov v Nemčiji

Vir: Ministrstvo za finance Nemčije, 2011

Nemci za dostop do e-davkov uporabljajo tako imenovano spletno stran ELsterOnline. Za prijavo na spletno stran potrebujejo svojo davčno številko ali davčno številko organizacije, za katero delajo. Na voljo sta jim dve različici spletne strani ELSTER. Za delodajalce je od leta 2009 predpisano varnostno preverjanje pristnosti elektronskih potrdil, na tej strani tudi prejmejo potrdilo v svoj računalnik. Vse, kar morajo narediti, je, da se prijavijo v ElsterOnline. Še večjo varnost uporabniških podatkov zagotavlja ELSTER, kjer v skladu s priporočili zvezne agencije za omrežje ter zveznega urada za informacijsko varnost (BSI) za preverjanje pristnosti in šifriranje uporabljajo algoritme z daljšimi ključi. Uporabniki lahko z ElsterOnline udobno od doma uredijo vsa vprašanja, in to neposredno, brez pošte in obrazcev. Ta storitev je na voljo tako fizičnim osebam kot tudi vsem podjetnikom in davčnim svetovalcem. Za uporabo je treba namestiti program Java Runtime Envronment (JRE). Pri konfiguraciji jim pomaga čarovnik, pri čemer lahko uporabniki preverijo, ali njihov sistem ustreza zahtevam za uporabo ElsterOnline. Prijava v sistem je mogoča na več načinov, in sicer na osnovni načina ElsterBasis z osebnim digitalnim potrdilom v osebnem računalnikom, kot je mogoče tudi pri nas, postopek pa je isti, varnost je visoka, uporaba pa preprosta. Drugi način je tako imenovani ElsterSpecial z osebnim digitalnim potrdilom na USB-ključu, kjer je varnost zelo visoka, uporaba prav tako preprosta, vendar pa je treba za digitalno potrdilo na ključu plačati 41 evrov. Tretji način se imenuje ElsterPlus z osebnim certifikatom na kartici s čipom, ki zagotavlja najvišjo možno raven varnosti, vendar se cena giblje med 50 do 150 evri, uporaba pa je malce zapletenejša (Ministrstvo za finance Nemčije).

7.3 ELEKTRONSKO DAVČNO POSLOVANJE V VELIKI BRITANIJI

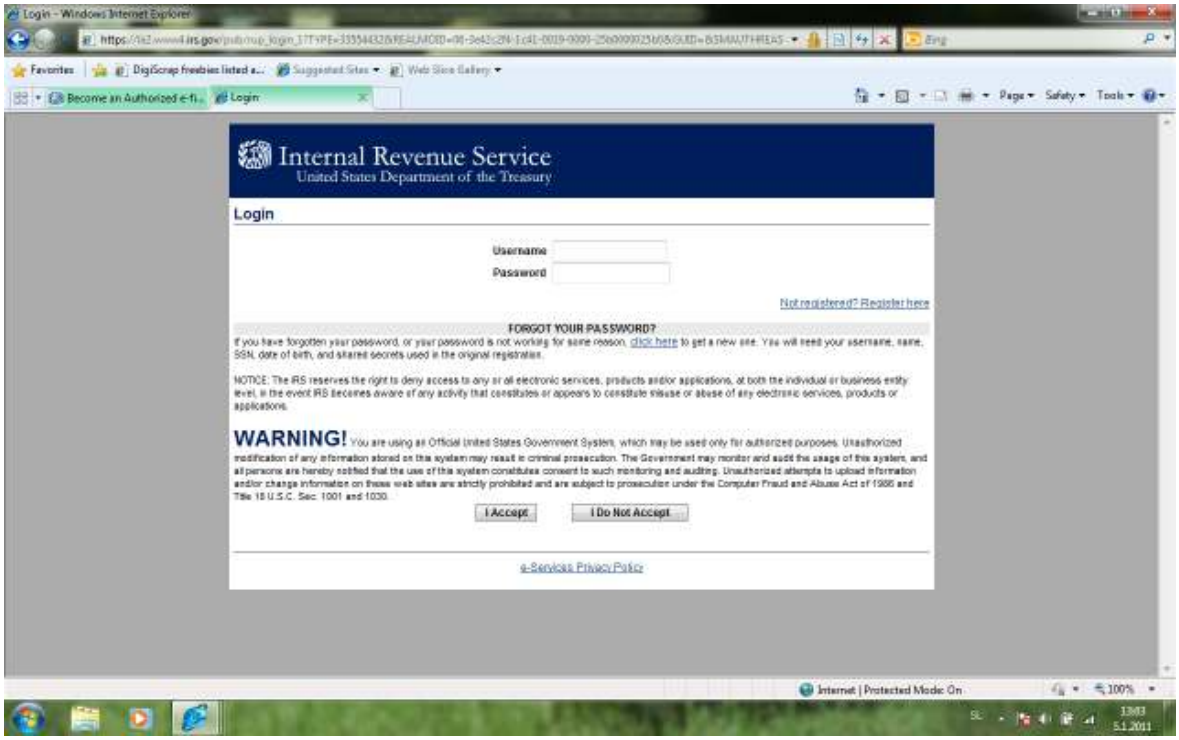
Slika 13: Spletna stran e-davkov v Veliki Britaniji

Vir: Ministrstvo za prihodke Velike Britanije, 2011

V Veliki Britaniji je prav tako omogočena uporaba e-davkov na spletni strani Online Services. Povezava nanjo je navedena pod sliko 13. Za dostop do portala sta potrebna uporabniško ime in geslo, ki ga uporabnik pridobi z registracijo na omenjeni spletni strani ter z digitalnim potrdilom ali s številko PIN, stran pa ga vodi po korakih. Namenjena je prav tako vsem fizičnim in pravnim osebam. Pristojni urad HMRC redno spremlja sistem in vpise v spletni sistem, da bi zagotovil najvišjo varnost osebnih podatkov. Ker se metode zlorabljanja spreminjajo, urad HMC skrbi za redno nadgradnjo glede prevar, za katere se zaveda, da obstajajo. Največje tveganje je povezano s krajo osebnih in vstopnih podatkov, zato morajo njihovi uporabniki narediti vse, kar lahko, da zaščitijo svoja uporabniška imena in gesla ter jih ne posredujejo nikomur. Na spletni strani svoje uporabnike tudi opozarjajo, da jim z njihove strani nikoli ne bodo poslali podatkov glede davkov po elektronski pošti ali pa da bi jih prosili za razkritje kakršnih koli osebnih podatkov in podatkov o plačilu po elektronski pošti. Glede vsake pošte, ki bi vsebovala sumljivo vsebino glede zlorabe iz njihovega urada, morajo sporočiti na elektronski naslov, ki je naveden na omenjeni spletni strani (Ministrstvo za prihodke Velike Britanije).

7.4 ELEKTRONSKO DAVČNO POSLOVANJE V ZDRUŽENIH DRŽAVAH AMERIKE

Slika 14: Spletna stran e-davkov v Združenih državah Amerike



Vir: Ministrstvo za notranje prihodke Združenih držav Amerike, 2011

V ameriško spletno davčno poslovanje uporabnika vodijo podrobna navodila, ki opisujejo postopek prijave v treh korakih. Najprej mora uporabnik izdelati račun IRS e-storitev z vpisom osebnih podatkov, uporabniško ime, geslo, PIN-številko in varnostno vprašanje. Ko po pošti prejme potrditveno kodo, se mora v 28 dneh prijaviti v e-storitve in potrditi registracijo. Drugi korak obsega oddajo prijave, s čimer postane avtorizirani e-uporabnik IRS. V tretjem koraku poda primernost preverjanja. Ko pošlje prijavo in povezane dokumente, IRS izvede primernost preverjanja v podjetju ter vsaki osebi, navedeni ob prijavi, bodisi pri glavnem bodisi pri pristojnem uradniku. Preverjanje lahko vključuje preverjanje kreditov, izpolnjevanja davčnih obveznosti, preteklih kaznivih dejanj in neskladnosti z zahtevami e-dokumentov IRS. Ko je to odobreno, dobijo uporabniki sprejemno pismo IRS z elektronsko podatkovno številko (Electronic Filing Identification Number – EFIN). S tega vidika je varnost ameriškim uporabnikom zagotovljena (Ministrstvo za notranje prihodke Združenih držav Amerike).

7.5 ELEKTRONSKO DAVČNO POSLOVANJE NA HRVAŠKEM

Slika 15: Spletna stran e-davkov na Hrvaškem

Vir: Davčna uprava Republike Hrvaške, 2011

Hrvaški sistem e-davkov, imenovan e-Porezna, omogoča vsem davčnim zavezancem v Republiki Hrvaški preprosto in varno dostavljanje podatkov o mesečnem obračunu DDV-ja za določeno obračunsko obdobje. Pred uporabo sistema mora uporabnik izpolniti določene uporabniške predpogoje, od katerih sta najpomembnejša uporabniško ime in digitalno potrdilo, ki ga izda ministrstvo za finance. Ministrstvo za finance izdaja digitalna potrdila na tako imenovanih pametnih karticah z vgrajenim čipom, zato je treba tudi imeti čitalnik teh kartic. Vso programsko opremo, ki jo uporabniki potrebujejo za izpolnjevanje obrazcev, njihovo digitalno podpisovanje, enkripcijo, pošiljanje v servis davčne uprave in podobno, zagotavlja davčna uprava. Imeti morajo le predpisane operacijske sisteme, ki jih navajajo na svoji spletni strani. Sistem je zelo podoben našemu, le da na Hrvaškem izdajajo digitalna potrdila na pametni kartici, prav tako morajo hrvaški uporabniki program za oddajo obrazcev namestiti v računalnik, šele nato se lahko prijavijo kot uporabniki sistema e-Porezna. Za vse tehnične informacije so na njihovi spletni strani naslovi in telefonske številke za pomoč uporabnikom. Varnost strani je, tako kot pri nas, velika in zagotovljena z že omenjeno pametno kartico, ki jo morajo uporabniki skrbno hraniti (Davčna uprava Republike Hrvaške).

8 PRAVNA UREDITEV E-POSLOVANJA V SLOVENIJI

Pravno ureditev elektronskega poslovanja v Sloveniji ureja Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP), ki ga je sprejel Državni zbor Republike Slovenije 23. junija 2000 in je bil tudi objavljen v Uradnem listu RS, št. 57/2000. Veljati je začel 22. avgusta leta 2000. Sestavljen je iz petih poglavij. Prvo poglavje z naslovom splošne določbe vsebuje štiri člene. Prvi člen določa področje uporabe in opisuje njegovo vsebino. V drugem členu so opredeljeni posamezni izrazi, uporabljeni v zakonu, ter njihov pomen. Tretji in četrti člen pa določata razmerja pri obdelavi elektronskih sporočil ter njihovo veljavnost, kar pomeni, da je vrednost podatkov v elektronski obliki enaka kot v primeru podatkov v pisni obliki. Drugo poglavje z naslovom Elektronsko poslovanje sestavljata dva razdelka, ki podrobno predstavljata elektronsko sporočilo, podatke v elektronski obliki in njihovo hrambo. Tretje poglavje z naslovom Elektronski podpis sestavlja osem razdelkov, ki opredeljujejo splošne določbe, potrdila in overitelje, ki jih izdajajo, kvalificirana potrdila in overitelje, ki jih izdajajo, tehnične zahteve za varno elektronsko poslovanje, odgovornost overiteljev, nadzor, prostovoljno akreditacijo ter veljavnost tujih potrdil. V četrtem poglavju so zapisane kazenske določbe, ki določajo sankcije v primeru kršitev ter njihovo denarno in materialno vrednost. ZEPEP overitelju nalaga številne obveznosti, katerih kršitev pomeni prekršek. V zvezi s tem ZEPEP določa zakonske obveznosti zanesljive določitve identitete, točno določeno vsebino kvalificiranega potrdila, našteva primere, ko mora overitelj nemudoma preklicati potrdilo, da mora biti v tem preklicu točno določen čas preklica potrdila, da mora overitelj prosilca potrdila obvestiti o vseh pomembnih podatkih, mora voditi dokumentacijo o varnostnih ukrepih ter inšpektorju omogočiti pregled dokumentacije in aktov, ki se nanašajo na poslovanje overiteljev, pregled prostorov, kjer se overitve opravljajo, ter dovoliti preverbo ukrepov in postopkov overitelja. Prav tako mora overitelj, preden začne opravljati svojo dejavnost, njen začetek prijaviti ministrstvu, zagotoviti vodenje registra preklicanih potrdil ter uporabljati zanesljive sisteme in opremo. Inšpektor lahko overitelju z odločbo časovno in vsebinsko prepove opravljanje dejavnosti. Do uporabe oznake akreditiranega overitelja so upravičeni overitelji, ki so vpisani v register akreditiranih overiteljev. Kazensko pa ne odgovarja le overitelj, ampak tudi imetnik potrdila oziroma njegova odgovorna oseba, če gre za pravno osebo, če ne zahteva preklica potrdila ali kvalificiranega potrdila ali če uporablja podatke in sredstva za elektronsko podpisovanje v nasprotju s tem zakonom. Denarno kaznovan je lahko tudi posameznik, ki brez vednosti podpisnika ali imetnika potrdila uporabi njegove podatke ali sredstva za elektronsko poslovanje. Ta zakon se konča s petim poglavjem, v katerem so zapisane prehodne in končne določbe. K temu zakonu sta dodana še uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje ter pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji.

Overitelj je lahko fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi. Kdor želi postati overitelj, mora najprej oddati vlogo za prijavo v register, ki jo direkciji dostavi overitelj, lahko pa tudi njegov pooblaščeni zastopnik. Vloga mora biti v elektronski ali papirnati obliki na predpisanem obrazcu. Na podlagi vloge in izpolnjevanja pogojev overitelja direktor direkcije odloči v osmih dneh od vložitve popolne vloge o vpisu overitelja v register. O kakršni koli spremembi podatkov je treba sporočiti takoj. Direkcija vodi register v elektronski obliki in ga podpiše z varnim elektronskim podpisom, overjenim s kvalificiranim potrdilom, in ga objavi v Uradnem listu Republike Slovenije (ZEPEP, 2001; Pavliha in drugi, 2002).

9 ZAKLJUČEK

Z uporabo interneta lahko marsikaj opravimo hitreje in celo privarčujemo. Za tako se je izkazala spletna aplikacija e-davki (eDavki). Po prvi v diplomskem delu postavljeni hipotezi so v e-davkih ogroženi osebni podatki. DURS je hipotezo ovrgel, saj je aplikacija e-davki dovolj zaščitena. Nevarnost ogroženosti osebnih podatkov ter njihova kraja je v rokah uporabnikov in imetnikov digitalnih potrdil in njihove hrambe. Čeprav kibernetski kriminalci pri vdorih napredujejo in je samo še vprašanje časa, kdaj bo DURS zabeležil kak vdor, lahko tudi na njihovi strani pričakujemo nadgradnje in izboljšave celotnega sistema. Podobno kot v sistemih drugih držav, ki so predstavljeni v diplomskem delu, lahko tudi pri nas pričakujemo varnostne kartice ali celo kak boljši način zagotavljanja avtentikacije uporabnika in daljšo enkripcijo ključev. Po drugi hipotezi e-davke uporablja čedalje več ljudi. Hipoteza je potrjena glede na statistične podatke, pridobljene pri Davčni upravi Republike Slovenije, kajti aplikacijo uporablja vedno več ljudi, povečanje števila uporabnikov pa je vidno še posebej pri pravnih osebah in fizičnih osebah s pridobitno dejavnostjo, medtem ko je število fizičnih oseb, ki uporabljajo to aplikacijo, nekoliko upadlo.
Po tretji hipotezi je prednosti e-davkov več kot slabosti. Ta hipoteza je potrjena, saj uporaba e-davkov prinaša veliko ugodnosti, med katerimi so prihranek časa in denarja, vpogled v osebne podatke in zagotavljanje najvišje varnosti aplikacije. Slabosti e-davkov so, da za uporabo potrebujemo računalnik, internet ter ustrezno strojno in programsko opremo, vključno z digitalnim potrdilom, kar pa je na voljo že skoraj vsakomur, zato v zvezi s tem ni toliko ovir, pa tudi cenovno so čedalje dostopnejši. E-davke velikokrat nadgrajujejo in dopolnjujejo, tako je večkrat na voljo beta različica aplikacije, kar pomeni, da je ta aplikacija še v preizkušanju, vendar lahko DURS le tako vsako leto omogoča večjo varnost in manjšo možnost zlorabe osebnih podatkov oziroma jo lahko skoraj izniči. E-davki omogočajo preprosto uporabo storitev zgolj uporabnikom Microsoftovih programov, ki uporabljajo le en spletni brskalnik, vendar pa so tudi v zvezi s tem že vidni rezultati in lahko pričakujemo izboljšave z vidika uporabnikov Linuxa ter operacijskega sistema Mac OS X, čeprav jim včasih povzročajo še malce težav.

LITERATURA

COOPER, Brian in drugi. Internet. Založba Pasadena, Ljubljana, 1997.
GRADIŠAR, Miro in RESINOVIČ, Gortan. Informatika v organizaciji. Moderna organizacija, Kranj, 1998.
TOPLIŠEK, Janez. Elektronsko poslovanje. Založba Atlantis, Ljubljana, 1998.
BRATUŠA, Tomaž. Hekerski vdori in zaščita. Založba Pasadena, Ljubljana, 2006.
JERMAN BLAŽIČ, Borka. Elektronsko poslovanje na internetu. Gospodarski vestnik, Ljubljana, 2001.
PINTERIČ, Uroš in SVETE, Uroš. Elektronsko upravljanje in poslovanje v službi uporabnika. E-governance and E-business at the service of customer. Fakulteta za družbene vede, Ljubljana, 2007.
VINTAR, Mirko in GRAD, Janez. E-uprava: Izbrane razvojne perspektive. Fakulteta za upravo, Ljubljana, 2004.
PAVLIHA, Marko in drugi. Zakon o elektronskem poslovanju in podpisu s komentarjem. GV Založba, Ljubljana, 2002.

VIRI

Olague, T. New Internet innovations.
URL="http;//ezinearticles.com/?New-Internet-Innovations&id=3895694".
4secnet, d. o. o., Kaj je parazitni program?
URL="http://www.secpoint.si/url_Kaj_je_parazitni_program".
4secnet, d. o. o., Kaj je nezaželena pošta?
URL="http://www.secpoint.si/url_Kaj_je_nezazelena_posta".
O'Neill, N. Varstvo osebnih podatkov na internetu.
URL="http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/".
Sistem24, d. o. o., Posodobitev operacijskega sistema.
URL="http://www.sistem24.si/racunalniska-pomoc-storitve/namestitev-in-vzdrzevanje-racunalniske-opreme.php".
Christiensen, B. M. Australian tax refund scam email.
URL= "http://www.hoax-slayer.com/australian-tax-refund-scam.shtml".
Miletic, B. Lodging eTax can be hazardous says F-secure.
URL="http://www.smarthouse.com.au/Home_Office/Security_And_Support/B3M2V5Q9".
Zalaznik, J. NLB žrtev spletne prevare.
URL="http://www.dnevnik.si/poslovni_dnevnik/210820".
DURS, Varnost v E-davkih.
URL="http://edavki.durs.si/OpenPortal/Pages/Introduction/Safety.aspx".
McLoughlin, L. AUSkey.
URL="http://yourbasagent.com.au/2010/04/auskey/".
Delišimunovič, R. Elektronsko davčno poslovanje.
URL"http://www.gzdbk.si/media/pdf/sekcije/racunovodje/posvet2009/eDavkiOtocec_RobertaDelisimunovic.pdf".
Popovič, Ž. E-poslovanjem do veče konkurentnosti.
URL="www.ericsson.com/hr/etk/novine/kom0507/17.pdf".
Klun, M. in Dečman, M. E-public services: The case of E-taxation in Slovenia.
URL= "http://ideas.repec.org/a/ipf/finteo/v30y2006i3p233-252.html".
Franz Lu, D. Dursovi eDavki delujejo brezhibno le v Microsoftovih oknih z raziskovalcem.
URL="http://www.dnevnik.si/novice/znanost/319557".
Davčna uprava Avstralije – Australian taxation office, Coming soon – changes to our online security system.
URL="http://www.ato.gov.au/onlineservices/content.asp?doc=/content/00235460.htm".
Davčna uprava Avstralije – Australian taxation office, Register for an Australian Business Number (ABN).
URL="http://www.business.gov.au/BusinessTopics/Registrationandlicences/Registeroftaxation/RegisterforanAustralianBusinessNumber(ABN).aspx".
Davčna uprava Avstralije – Australian taxation office, ABR security policy.
URL="http://help.abr.gov.au/content.asp?doc=/Content/17865.htm&placement=ABH/SEC/SYS&usertype=BC".
Ministrstvo za finance Avstrije – Bundesministerium für finanzen, FinanceOnline.
URL="http;//www.bmf.gv.at/government/finanzonline/".
URL="http://bmf.gv.at/EGovernment/FINANZOnline/HufiggestellteFragenFAQ/_start.htm".
Ministrstvo za finance Nemčije, Bayerisches Landesamt für Steuern, ElsterOnline.
URL="https://www.elsteronline.de/eportal/Authentisiere.tax".

Ministrstvo za prihodke Velike Britanije – HM Revenue & Customs, Security advice HMRC.
URL="http://www.hmrc.gov.uk/security/index.htm".
Ministrstvo za notranje prihodke Velike Britanije – IRS, Become an Authorised e-file Provider.
URL="http://www.irs.gov/taxpros/providers/article/0,,id=222533.html".
Davčna uprava Republike Hrvaške – Porezna uprava Republike Hrvatske, O aplikaciji ePorezna.
URL="http://www.porezna-uprava.hr/e-Porezna/e-PoreznaApp?id=b03d4".
Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji, Uradni list RS, št. 99/2001.
URL=" http://www.uradni-list.si/1/content?id=33791".