UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo

VARNA UPORABA INTERNETA: ORGANIZACIJE IN ODNOS ŠTUDENTOV

Lucija Jelen

Ljubljana, september 2012

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

DIPLOMSKO DELO

VARNA UPORABA INTERNETA: ORGANIZACIJE IN ODNOS ŠTUDENTOV

Kandidatka: Lucija Jelen
Vpisna številka: 04037623
Študijski program: Univerzitetni študijski program Uprava prva stopnja

Mentor: izr. prof. dr. Ljupčo Todorovski

Ljubljana, september 2012

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Lucija Jelen, študentka Univerzitetnega študijskega programa Uprava prva stopnja, z vpisno številko 04037623, sem avtorica diplomskega dela z naslovom: Varna uporaba interneta: organizacije in odnos študentov.

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 v 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 avtorstvu in sorodnih pravicah, Ur. list RS, št. 21/95), 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 ter soglašam z objavo dela v zbirki »Dela FU«.

Diplomsko delo je lektorirala: Bernarda Jelen, prof. slo

Ljubljana, september 2012

Podpis avtorice:

POVZETEK

Diplomsko delo obravnava definicijo varnosti na internetu z različnih aspektov organizacij, ki skrbijo za varnost na internetu. Informacijska varnost je proces, ki nas ščiti pred naraščajočim in vedno bolj nevarnim kibernetskim kriminalom. Nevarnost spletnega kriminala se skriva predvsem v tem, da so ti napadi izvršeni iz kateregakoli računalnika po svetu, hkrati pa v nekaj minutah ali urah povzročijo škodo na vseh kontinentih sveta.

Internetnemu kriminalu se vse večkrat po robu postavljajo različne spletne organizacije, katerih glavna naloga je zavarovati uporabnike pred nezakonito spletno vsebino. Preučili smo slovenske in mednarodne projekte in organizacije za varnost na internetu. V mednarodnem okolju deluje združenje spletnih prijavnih točk INHOPE, v Sloveniji je tej prijavni točki enako Spletno oko. Poleg njiju delujejo še SAFE-SI, slovenska nacionalna točka osveščanja in s krovno organizacijo INSAFE, katerih glavna naloga je promocija varne in odgovorne rabe interneta in mobilnih tehnologij in SI-CERT, slovenski center za posredovanje pri internetnih incidentih.

V nadaljevanju smo z anketo analizirali poznavanje področja varnosti med študenti. Rezultati so pokazali, da se študentje ne zavedajo nevarnosti interneta in tudi ne poznajo slovenskih ali mednarodnih organizacij za varnejši internet. Pozitivna ugotovitev je, da vedo za razliko med zakonito in nezakonito spletno vsebino in bi v primeru srečanja s slednjo znali in predvsem želeli ukrepati.

Ključne besede: varnost, internet, SAFE-SI, Spletno oko, SI-CERT, INHOPE, INSAFE

SUMMARY

SAFE USE OF INTERNET: ORGANIZATIONS AND STUDENT ATTITUDES.

This thesis deals with the definition of safe use of the internet, with various aspects of the organizations which are responsible for safety on the internet. Data protection is a process that protects us from increasingly dangerous cyber crime. Risk of cyber crime lies primarily in the fact, that those attacks can be executed from any computer in the world but also in a few minutes or hours can cause damage on all continents around the globe.

Different online organizations, whose main task is to protect users from illegal online content, are increasingly working against internet crime. We studied the Slovenian and international projects and organizations for internet safety. INHOPE is the International Association of Internet Hotlines, which Slovenian project Spletno oko is part of. There are also organizations like INSAFE, which is a European network of Awareness Center, and Slovenian national Awareness Centre SAFE-SI promoting safe, responsible use of the Internet and mobile devices to young people. We must not forget Si-CERT, Slovenian computer emergency response team for intervening in internet incidents.

In addition, we analyzed survey data of safe use of internet among students. The results showed that students are not aware of dangers of the internet and do not know the Slovenian or international organizations for safer internet. However, it is positive, that they know the difference between legal and illegal content and if they encounter such content, they would know how to act against it.

Key words: safety, internet, SAFE-SI, Spletno oko, SI-CERT, INHOPE, INSAFE

KAZALO

KAZALO PONAZORITEV

KAZALO GRAFIKONOV

KAZALO SLIK

KAZALO TABEL

KAZALO PRILOG

SEZNAM UPORABLJENIH KRATIC IN OKRAJŠAV

ARNES	Akademska in raziskovalna mreža Slovenije
IT	**I**nformacijske **T**ehnologije
KZ	**K**azenski **z**akonik
ZASP	**Z**akon o **a**vtorskih **p**ravicah
ZEKom	**Z**akon o **e**lektronskih **kom**unikacijah

SEZNAM PREVODOV TUJIH IZRAZOV

CDA	**C**ommunication **D**ecency **A**ct = Zakon o spodobnosti pri komuniciranju
CERT	**C**omputer **E**mergency **R**esponse **T**eam = Center za posredovanje pri internetnih incidentih
DARPA	**D**efense **A**dvanced **R**esearch **P**roject **A**gency = Agencija za znanost in razvoj
ENISA	**E**uropean **N**etworking and **I**nformation **S**ecurity **A**gency = Evropska agencija za varnost omrežij in informacij
INHOPE	**In**ternational Association of Internet **Ho**tline **P**rovid**e**rs = Mednarodno združenje internetnih prijavnih točk
IP	**I**nternet **P**rotocol = internetni protokol
NAC	Safe **N**etwork **A**ccess **C**ontrol = varen omrežni dostop
WWW	**W**orld **W**ide **W**eb = svetovni splet

1 UVOD

Internet je virtualno okolje, ki z množico informacij, znanj, storitev in odnosov spreminja družbo. S svojo brezmejnostjo dopušča svobodo in anonimnost, hkrati pa tudi priložnosti za »prepovedano« (Spletno oko, 2009).

Na ulici popolnemu neznancu verjetno ne bi zaupali svoje denarnice, kajne? Zavedate se, da obstaja možnost, da vam jo ukrade. Lahko zlorabi vaše osebne podatke, bančno kartico ali kako drugače škoduje vaši integriteti. Kako pa varujete svoje podatke na spletu? Ste prepričani, da na prvi pogled nedolžne informacije, kot so hišni naslov, telefonska številka, e-naslov in slike, ki jih objavite na spletu, ne bodo prišle v napačne roke?

Za varnost v virtualnem svetu lahko največ storimo sami, seveda pa nam pri tem pomaga kar nekaj organizacij. V mednarodnem prostoru za osveščanje uporabnikov pred nevarnostmi interneta najbolje skrbita organizaciji INHOPE in INSAFE, slovenskim uporabnikom pa to pomoč nudijo projekt SAFE-SI, ki ponuja informacije za varno in odgovorno rabo interneta, SI-CERT center za posredovanje pri omrežnih incidentih in spletna prijavna točka Spletno oko, pri kateri lahko podamo anonimno prijavo otroške pornografije in sovražnega govora.

Vsaka od organizacij tako zagotavlja neko vrsto varnosti; javno, zasebno ali pravno varnost. Zato želimo raziskati, kako nas različne organizacije skušajo varovati pred neprimerno ali celo nezakonito vsebino, ki jo je na svetovnem spletu vse več.

Pri tem je v prvi vrsti potrebna pomoč uporabnikov, da si vzamejo čas in vsebino, ki se jim zdi neprimerna ali nezakonita tudi prijavijo. Ker je sedaj največ spletnih uporabnikov mladostnikov in tistih v zgodnji odraslosti, želimo preveriti, ali ti sploh znajo ukrepati zoper neprimerno vsebino ali jo zgolj prezrejo. S pravilnim ukrepanjem bomo tako lahko nekoč brez skrbi, zase in za druge, brskali po spletu.

Namen diplomskega dela je teoretično preučiti tako slovenske kot mednarodne organizacije, ki se ukvarjajo s problematiko varnosti na internetu. Z empiričnim delom pa izvedeti, ali študentje poznajo te organizacije in pojme, varnost, neprimernost, nezakonitost.

Cilji diplomskega dela so:

- preučiti in primerjati definicije varnosti na internetu, ki jih ponujajo različne organizacije za varnejši internet,
- podrobneje preučiti slovenske organizacije za varen internet SAFE-SI, Spletno oko in SI-CERT ter mednarodni organizaciji INHOPE in INSAFE,
- izvesti intervju z organizacijami SAFE-SI, SI-CERT, Spletno oko in INHOPE,

- s pomočjo rezultatov ankete analizirati poznavanje področja varnosti na internetu med študenti.

Hipoteze, ki smo si jih zastavili so naslednje:
H1: Različne organizacije, ki skrbijo za varnejši internet, ponujajo različne definicije pojma varnost na internetu.
H2: Študentje različno razumejo pojem varnost na internetu.
H3: Večina študentov ne pozna razlike med zakonitostjo in nezakonitostjo spletnih komentarjev.
H4: Večina študentov ne pozna slovenskih in mednarodnih organizacij za varen internet.
H5: Študentje na spletnih forumih praviloma ne prijavljajo nezakonite vsebine zaradi nepoznavanja sistema delovanja.

Za pisanje naloge bomo uporabili naslednje metode:
- metodo deskripcije, s katero bomo opisali teorijo, pojme in ugotovljena dejstva,
- metodo kompilacije, kjer bomo s povzemanjem stališč drugih avtorjev v zvezi z izbranim raziskovalnim problemom oblikovali svoja stališča in
- statistično metodo, s katero bomo obdelali in analizirali podatke pridobljene s posebej pripravljenim anketnim vprašalnikom.

Veliko predhodnih raziskav je omejenih zgolj na eno področje varnosti pred internetno kriminaliteto. Kot na primer raziskava o varnosti elektronske izmenjave podatkov (Ljubisavljević, 2006), raziskava o varnostnih mehanizmih elektronskega poslovanja (Verbič, 2012), bančnega poslovanja (Prah, 2012) ali davčnega poslovanja (Škarlin, 2011). Prav tako so že narejene raziskave o varnosti spletnih brskalnikov (Urbanija, 2012), o vdorih v informacijske sisteme (Martinis, 2012) in pravnih vidikih takšnih kaznivih dejanj (Ostanek, 2007). Največ raziskav najdemo na področju varovanja osebnih podatkov (Kozole, 2012), v socialnih omrežjih (Zver, 2011), kot je Facebook (Klanjšek, 2012) ki jih vede ali nevede pustimo v internetnem prostoru. Le peščica raziskav omenja slovenske organizacije, ki se ukvarjajo z varnostjo na internetu kot sta Spletno oko (Borštnar, 2011) in SAFE.SI (Živkovič, 2008). Organizacij SI-CERT, INHOPE in INSAFE pa ne omenja nobena iz med njih, zato smo se odločili, da bomo vse naštete organizacije zbrali na enem mestu in opisali njihove naloge pri varovanju uporabnikov na spletu.

Z diplomskim delom želimo predstaviti organizacije in projekte, katerih glavni cilj je izobraziti in s tem preprečiti neodgovorno ravnanje na internetu ter pomagati, ko je škoda že narejena. Končni rezultati naše raziskave bodo objavljeni na različnih spletnih portalih, ki se ukvarjajo z varnostjo na internetu. S tem bomo pripomogli k boljšemu zavedanju internetne kriminalitete, saj jo naša nevednost le še razpihuje.

Predstavljena bodo tri večja poglavja. V prvem delu bomo preverili različne definicije varnosti na internetu, preučili v katerih pogledih se razlikujejo in kakšne so oblike zlorab interneta, ki jih definicije opisujejo. Ker bomo preučili nezakonito internetno vsebino,

bomo pregledali tudi zakonsko podlago pravne informatike. V drugem delu bomo predstavili slovenske in mednarodne organizacije ter projekte, katerih glavna naloga je poskrbeti za varnost na internetu. Opisali bomo njihov namen ustanovitve, cilje, ki jih želijo doseči in orodja oziroma aktivnosti, s katerimi izpolnjujejo svoje poslanstvo. Zadnji del bo namenjen empirični raziskavi med študenti o varnosti interneta. Zanima nas, ali se študentje zavedajo nevarnosti, ki jim preti ob nepravilni uporabi (osebnih) podatkov.

2 VARNOST NA INTERNETU

Internet je svetovno računalniško omrežje, v katerem najdemo več vrst računalnikov, kot so npr: osebni računalniki, prenosni računalniki, tablični računalnik in številni drugi. Mnogi so le del manjših krajevnih omrežij, ki so tudi zelo različna. Internet sloni na skupnem jeziku oz. protokolih, ki omogočajo sporazumevanje med vsemi tako zelo različnimi računalniki. Internet je računalniško omrežje, ki nima svojega središča, prek katerega bi bile speljane vse povezave. To pomeni, da se omrežje nikoli ne ustavi, tudi če pride do izpada kakega njegovega pomembnega dela. Podatki preprosto najdejo drugo pot in tako obidejo neuporaben del omrežja. (Kjaer, 2000, str. 5)

World Wide Web ali svetovni splet deluje kot skladišče spletnih strani, ki so shranjene na strežnikih po celem svetu. Spletne strani večinoma vsebujejo besedila, slike, animacije ter zvočne in slikovne posnetke (Kjaer, 2000, str. 8).

Če želimo uporabljati svetovni splet, moramo imeti nameščen spletni brskalnik. Ta poskrbi, da se strani, ki si jih želimo ogledati prenesejo s strežnika in prikažejo na zaslonu. Najbolj razširjeni brskalniki spletnih strani so Microsoft Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera, Safari in Lynx.

V omrežju internet je danes več kot 350 milijonov spletnih strani, ki so shranjene na več sto tisočih strežnikih po celem svetu. Vsebina nekaterih strani se le redko spreminja, medtem ko se druge nenehno spreminjajo ali se celo samodejno prilagajajo posameznim uporabnikom (O'Dell, 2011).

Spletno mesto je torej zbirka spletnih strani, ki opisujejo neko temo, podjetje, ustanovo, storitev ali posameznika. Na spletnem mestu je lahko le nekaj strani, večja mesta pa vsebujejo celo nekaj tisoč spletnih strani. Vse te strani so običajno na istem strežniku in na njem je vedno tudi začetna stran, ki služi kot izhodišče za obiskovalce.

2.1 DEFINICIJA VARNOSTI

Po elektronski pošti smo izvedli tri intervjuje s slovenskimi organizacijami, ki skrbijo za varnost na internetu, saj smo želeli izvedeti kako posamezna organizacija opredeljuje pojem varnost na spletu. Za SAFE-SI je na vprašanja v Prilogi 1, odgovorila koordinatorka projekta Tanja Šterk. V Prilogi 2 smo s pomočjo koordinatorke Lije Mihelič spoznali prijavno točko Spletno oko. V Prilogi 3 pa je za center za posredovanje pri internetnih incidentih SI-CERT na vprašanja odgovarjala koordinatorka nacionalnega programa ozaveščanja o informacijski varnosti Jasmina Mešić.

Varnost na internetu je zelo širok pojem in bi ga težko opredelili le v enem stavku, saj zajema različne oblike varnosti na različnih nivojih: lahko govorimo o varnosti strojne

opreme, ki procesira naše podatke, o omrežni varnosti, vse do končnega spletnega uporabnika in varnosti njegove spletne identitete. (Mešić, osebna komunikacija, 2012)

Po Šterk (osebna komunikacija, 2012) je pomembno, da se na internetu vedemo odgovorno, da skrbimo za zaščito svoje spletne zasebnosti in objavljamo le tisto, za kar nam je vseeno, če kdorkoli vidi. Namreč, ko nekaj objavimo na spletu tega ne moremo dokončno izbrisati in tako se nezadržno širi med uporabniki.

Varnost na internetu pa je z vidika projekta Spletno oko vsako stanje oziroma vedenje posameznika, ki privede do tega, da se posameznik – uporabnik spleta – izogne nevarnostim na spletu. Hkrati navaja definicijo iz spletne stran Wikipedia: Internetna varnost ali varnost na spletu je varnost ljudi in njihovih informacij pri uporabi interneta. (Mihelič, osebna komunikacija, 2012)

Za varno uporabo interneta je potrebno zagotoviti varnost dostopa do virov v omrežju, varnost prenosa podatkov preko omrežja in neovrgljivost izvorov informacij. Prvo dosežemo z gesli in filtri, drugo s šifriranjem podatkov, tretje pa z elektronskimi podpisi. Ena prvih nalog, ki jih moramo opraviti ob vključitvi lokalnega omrežja v omrežje interneta, je zagotoviti varnost našega omrežja. (Pagon, 1997, str. 33)

Eden iz med splošnih problemov, ki se pojavlja, je tudi ta, da puščamo svoje elektronske prstne odtise povsod, kamorkoli se odpravljamo. Vsakokrat, ko se povežemo z nekim strežnikom, lahko ta preveri, katero vrsto spletnega brskalnika uporabljamo, katero spletno stran smo nazadnje obiskali, poleg tega pa pozna tudi naš naslov IP.

Varnostno tveganje je povezano tudi z majhno datoteko cookies.txt, ki je vključena v nekatere spletne brskalnike. Ko se povežemo s spletnim strežnikom, vanjo zapiše nekatere podatke. Navadno se ta datoteka uporablja za shranjevanje sprememb in prilagoditev, ki smo jih opravili na neki spletni strani, tako, da se te nastavitve uporabijo ob vsakem naslednjem obisku iste spletne strani. Seveda pa nihče ne more jamčiti, kaj se v resnici zapiše v to datoteko. Morda so to osebni podatki, ki ste jih nepremišljeno izdali in se lahko uporabijo v propagandne namene. Zato je potrebno biti previden pri izdajanju osebnih podatkov, ko izpolnjujemo obrazce na spletnih straneh. (Kjaer, 2000, str. 57)

Ena največjih prednosti interneta – poleg številnih drugih možnosti – je prav v tem, da omogoča in vzpodbuja sodelovanje tudi med policijsko-varnostnimi strokovnjaki in organizacijami s celega sveta, s čimer ustvarja virtualne skupnosti, ki doslej zaradi razdalje ter časovnih in finančnih omejitev niso mogle obstajati. Ob oceni varnosti interneta se morate zavedati, da v trenutku, ko je lokalno omrežje vključeno v internet, je dostopno množici potencialnih vlomilcev iz vsega sveta, pred katerimi se je potrebno ščititi.

S sistematični spremljanjem različnih aktivnosti na internetu lahko policijske organizacije zasledijo vrsto nezakonitih aktivnosti oziroma informacij o njih. Tu imamo v mislih

predvsem odprte in javno dostopne informacije na internetu, kot so domače strani posameznikov ali organizacij (na primer anarhistične skupine), razprave v diskusijskih skupinah, ponudbe nelegalnih izdelkov, navodila za izdelavo eksplozivnih teles, pisemskih bomb ipd. Preiskovalci, ki se ukvarjajo z računalniško kriminaliteto in preiskujejo vdore v računalniške sisteme, mnogo uporabnih informacij dobijo tudi s spremljanjem diskusij na diskusijskih in novičarskih skupinah. (Pagon, 1997, str. 203)

2.2 ZAKONSKA PODLAGA

O internetu lahko s pravnega stališča razmišljamo bodisi kot o predmetu pravnega urejanja bodisi kot o orodju za pravnike. V slednjem primeru govorimo o pravni informatiki. To področje se pogosto neutemeljeno zamenjuje s predmetom internetnega prava oziroma prava in interneta, čeprav je skupna točka internetnega prava in pravne informatike izključno tehnologija, ne pa tudi cilj, zaradi katerega jo preučujeta. (Makarovič et al., 2007, str. 27)

Ker internet ni okolje zunaj jurisdikcije držav, lahko najprej ugotovimo, da moramo uporabljati celo vrsto predpisov, ki urejajo ravnanje posameznikov in pravnih oseb tudi zunaj njega.

Zaradi globalne narave kibernetskega kriminala se je že v začetku 90. let 20. stoletja pojavila potreba po mednarodnem urejanju. Tako je leta 1995 Svet ministrov Sveta Evrope sprejel Priporočilo št. R(95) 13 o problemih kazenskega postopka, povezanih z informacijsko tehnologijo, 22. novembra 2001 pa je bila v okviru Sveta Evrope sprejeta Konvencija o kibernetski kriminaliteti (Convention on CyberCrime). Omenjena konvencija je prvi in še vedno najpomembnejši mednarodni akt s tega področja na svetu. Leta 2003 je bil sprejet še Dodatni protokol h konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih.

Oba dokumenta je Slovenija ratificirala leta 2004, kar je imelo za posledico tudi pomembne izboljšave nekaterih inkriminacij kibernetskega kriminala v slovenskem KZ.

Tako utegne na primer študent, ki je objavil žaljive trditve o svojem profesorju na spletnem forumu, kazensko odgovarjati po Kazenskem zakoniku (KZ). Prav tako fotograf, katerega fotografije s potovanja je njegova sopotnica brez dovoljenja objavila na spletni strani, lahko zahteva umik fotografij s spletne strani na podlagi Zakona o avtorskih pravicah (ZASP). Potrebno je omeniti še Zakon o elektronskih komunikacijah (ZEKom), ki posebej ureja vprašanja varstva zasebnosti in osebnih podatkov v zvezi s svetovnim spletom in elektronsko pošto. (Makarovič et al., 2007, str. 33)

2.3 AVTONOMNI VIRI INTERNETNEGA PRAVA

V sodobnih okoljih pojav avtonomnih virov prava ni nič nenavadnega: udeleženci določenega foruma, predstavniki industrije ali uporabniki storitev se lahko dogovorijo za specifična pravila ravnanja v medsebojnih odnosih, kolikor ta pravila niso v nasprotju z obveznimi (kogentnimi) normami, ki jih postavlja zakonodajalec.

Internet je okolje, za katerega so značilni izredna razsežnost, globalna razširjenost in posledično ignoriranje državnih meja ter visoka stopnja anonimnosti. Glede na te lastnosti je obstoj avtonomnih virov lahko omejen na ožje skupine znotraj interneta, kamor sodijo na primer nacionalni kodeksi ravnanja e-trgovcev, lahko pa gre za vire, katerih priznavanja in vsebina utegneta biti vprašljiva. Tak vir je že imenovana netika. (Makarovič et al., 2007, str. 38)

2.3.1 NETIKA

Netika (ang. netiquette) so pravila lepega vedenja v internetu. Tovrstna pravila so navadno precej ohlapna in njihove vsebine ni mogoče vedno natančno določiti. Netika na primer prepoveduje zasipavanje z nenaročenimi e-poštnimi sporočili.

O splošno priznani kodificirani netiki ne moremo govoriti, pravna veljavnost netike pa je vprašljiva iz več razlogov. Prvič, da bi bila netika pravno obvezna, bi se morala stranka bodisi izrecno zavezati bodisi bi morala netika pri določenih transakcijah predstavljati pravno zavezujoč običaj. In drugič, ker ni univerzalno kodificirane netike, je vsebina pravil pogosto vprašljiva (Makarovič et al., 2007, str. 38).

2.3.2 SAMOREGULACIJA INTERNETA

Od začetka razvoja storitev informacijske družbe je ključno vlogo poleg državne prisilne regulacije imela tudi samoregulacija. Gre za pristop, pri katerem ponudniki sami sprejmejo določene zaveze glede načina in oblike ponudbe storitev ali opredelitev dolžnih ravnanj ali pa sprejmejo določene omejitve ponudbe.

Eno prvih oblik samoregulacije je bilo mogoče zaslediti na strani ISP (Internet Service Provider) na področju zaščite mladoletnikov na internetu. Ta ima dve komponenti: na eni strani od ponudnikov zahteva omogočanje ustreznih filtracijskih storitev, ki mladoletnim omejujejo dostop do nekaterih tipskih vsebin, na drugi strani pa ima samoregulacija na področju zaščite mladoletnikov tudi pomen preprečevanja otroške pornografije in drugih škodljivih vsebin na internetu. Za spodbujanje samoregulacije in v podporo ustreznih ukrepov je Evropska komisija posebej oblikovala program *Safer internet* (Makarovič et al., 2007, str. 39).

2.3.3 KODEKSI RAVNANJA

Kodeksi ravnanja v internetu se od netike ločijo predvsem po tem, da so kodificirani, torej je mogoče njihovo vsebino nesporno ugotoviti iz zapisanega dokumenta. Kodekse ravnanja lahko sprejemajo e-trgovci ali njihova združenja, lahko pa tudi nevladne, na primer potrošniške organizacije. Kodeksi lahko določijo standarde poslovanja s potrošniki, ki so višji od standardov, kakršne kot obvezni minimum določa zakon(Makarovič et al., 2007, str. 40).

2.4 OBLIKE ZLORAB INTERNETA

Razvoj informacijske in komunikacijske tehnologije in njena široka vsakodnevna uporaba za javne, gospodarske in zasebne namene imata tudi svojo temnejšo plat – razcvet kibernetskega kriminala. Določene oblike kriminalitete, kot so na primer raznovrstne goljufije in ponarejanja, kraje identitet, zlorabe avtorskih pravic, sovražni govor in zloraba nelegalne, predvsem otroške pornografije, brez interneta verjetno ne bi obstajale v obsegu, kot ga poznamo danes. Informacijski sistemi so namreč vse pogosteje tarča vdorov, prestrezanja in uničenja podatkov, informacijskega vandalizma, razširjanja različnih virusov in drugih zlonamernih programov. Vse to danes imenujemo kibernetski kriminal. Enotne definicije ni, lahko pa kibernetski kriminal opredelimo kot kriminaliteto, povezano z računalniki, pri kateri je v najširšem smislu zajeta vsaka oblika kriminala, pri kateri je uporabljena računalniška oziroma informacijska tehnologija.

Šalamon (1998, str. 104-105) opisuje najbolj razširjene oblike zlorab interneta.

- Neupravičeno prilaščanje avtorskega dela oziroma intelektualne lastnine. Besedila, slike, zvok ali video, ki so v omrežju namenjeni javni rabi, prenesemo na svoj računalnik in jih poljubno uporabljamo.
- Pornografija. Širjenje pornografskega gradiva, ki je v večini držav prepovedano, posebej kritično je razširjanje gradiva za pedofile oziroma pornografske vsebine z mladoletnimi osebami.
- Elektronska trgovina. Vsaka uporaba komercialnih storitev v omrežju pusti digitalne sledi, še posebej kritična je uporaba kreditnih kartic.
- Banke podatkov o državljanih. Tajnost osebnih podatkov, kakršni so v bazah zdravstvenih ustanov, gospodarstva ali državne uprave, je izpostavljena nevarnosti vdorov v sistem.
- Politična propaganda skrajnežev. Anarhizem spodbuja in napeljuje k stanju družbenega kaosa.
- Terorizem. Spodbujanje k mednarodnemu terorizmu in terorističnim skupinam.
- Verski ekstremizem. Razpošiljanje žaljivih mnenj o posameznih verskih skupnostih in voditeljih.
- Rasni ekstremizem in nestrpnost. Ekstremistične skupine netijo sovraštvo, razširjajo antisemitistične ideje, rasizem in ostalo.
- Žalitve in obrekovanja. Žalitvam in obrekovanju so izpostavljene predvsem različne javne osebnosti.

- Napeljevanja k nasilnim dejanjem. Napeljevanja so uperjena zoper posameznika, manjšine ali skupine.
- Napeljevanja h kaznivim dejanjem. Možno je napeljevanje k uživanju drog in drugim nesprejemljivih dejavnosti.
- Organiziran kriminal. Internet predstavlja novo obliko komunikacijskega sredstva za organiziran kriminal, še posebej elektronske pošte.
- Zloraba elektronske pošte. Možnost izsiljevanje, grožnje, žalitve.
- Računalniški virusi. Preko interneta se razširjajo računalniški virusi z namenom, da se onemogoči delovanje sistemov in naprav.
- Vdori v sisteme. Vdori v računalniške sisteme in omrežja, ki lahko omogočijo pridobitev protipravne premoženjske koristi.

Temelje za pregon različnih oblik kibernetskega kriminala je nudil že prvi Kazenski zakonik (KZ) samostojne Slovenije iz leta 1995, vendar so bile mnoge definicije okorele in v praksi težko uporabljive. Novela KZ iz leta 2004 pa je slovensko kazensko zakonodajo uskladila z zahtevami Konvencije o kibernetski kriminaliteti.

Kibernetska kriminaliteta se z vidika kazenskega prava deli na tri področja:

- najbolj tipična dejanja kibernetske kriminalitete predstavljajo kazniva dejanja, pri katerih je računalnik oziroma informacijski sistem **tarča protipravnega dejanja,** (na primer vdori v informacijski sistem, oviranje delovanja informacijskega sistema, neupravičen prenos, uničenje, kopiranje podatkov iz informacijskega sistema ali v informacijski sistem itd.);

- naslednji sklop so dejanja, pri katerih računalnik oziroma informacijski sistem predstavlja bistveno **orodje izvršitve** sicer klasičnega kaznivega dejanja, ki je inkriminirano tako v fizičnem kot virtualnem svetu (prestrezanje podatkov, zlorabe plačilnih kartic, goljufije, prevare, ponarejanje listin itd.);

- zadnji sklop predstavljajo dejanja, povezana z **vsebino na računalniških ali informacijskih sistemih,** ki so sicer kazniva tudi v fizičnem svetu. Mednje uvrščamo predvsem tri kategorije ravnanj, ki so po svoji naravi različna in ogrožajo različne kazenskopravne varovane dobrine, imajo pa skupno lastnost in prav internet predstavlja prostor njihovega razcveta: to so kazniva dejanja, povezana s kršitvijo avtorskih pravic, nelegalno pornografijo in sovražnim govorom.

Danes so v KZ kot kazniva dejanja, ki bi jih lahko šteli med različne oblike kibernetskega kriminala, opredeljena naslednja ravnanja:

- neupravičen vstop v informacijski sistem (225. člen KZ);
- vdor v informacijski sistem (242. člen KZ);
- izdelovanje in pridobivanje orožja in pripomočkov, namenjenih izvršitvi kaznivega dejanja (309. člen KZ);
- kršitev tajnosti občil (150. člen KZ);
- neupravičeno prisluškovanje in zvočno snemanje (148. člen KZ);

- nedovoljena objava zasebnih pisanj (151. člen KZ);
- zloraba osebnih podatkov (154. člen KZ);
- kršitev avtorske pravice (158. člen KZ);
- neupravičeno izkoriščanje avtorskega dela (159. člen KZ);
- kršitev avtorski sorodnih pravic (160. člen KZ);
- goljufija in poslovna goljufija (217. člen in 234. a člen KZ);
- prikazovanje in izdelava pornografskega materiala (187. člen KZ);
- zbujanje sovraštva, razdora ali nestrpnosti, ki temelji na kršitvi načela enakosti (300. člen KZ);
- ponarejanje listin, ponareditev ali uničenje poslovnih listin, posebni primeri ponarejanja listin in overovitev lažne vsebine (256., 240., 257. in 258. člen KZ).

3 ORGANIZACIJE ZA VAREN INTERNET

Do leta 1995 so se uporabniki interneta, internetni ponudniki, državne vlade in organi pregona že zavedali, da je internet postal tudi prostor pedofilov, ki ga izrabljajo za objavo in izmenjavo slik z otroško pornografijo. Prav tako so zasledili druge nezakonite dejavnosti, kot so objave z rasističnim gradivom.

Leta 1996 je bila sprejeta prva omejitev uporabe interneta po svetu. V Združenih državah Amerike so sprejeli Communication Decency Act, ki je omejeval razpečevanje pornografije po omrežju. (Šalamon, 1998, str. 5)

Različne nacionalne pobude je tako združil interes, da razmislijo, kako preprečiti nezakonite dejavnosti. V Nemčiji je bilo več ločenih skupin, ki so prve začele z razpravo o primerih pedofilije v parlamentu. Obenem je bila ustanovljena neprofitna, mednarodna organizacija Childnet Internacional s sedežem v Veliki Britaniji, z nalogo za »*spodbujanje otrokovih interesov v mednarodnih komunikacijah*«.

V Sloveniji se z varnostjo na internetu in v okviru preventive ukvarja predvsem točka osveščanja SAFE.SI, medtem ko Spletno oko in SI-CERT nastopita s svojo vlogo takrat, ko smo že soočeni z nevarnostjo na internetu.

3.1 SAFE-SI

SAFE-SI od leta 2005 deluje kot slovenska nacionalna točka osveščanja (www.safe.si), katere poslanstvo je informiranje uporabnikov interneta, kako se lahko zaščitijo pred nevarnostmi, ki jih prinašajo nove interaktivne tehnologije, kot sta internet in mobilni telefon. Namenjena je spodbujanju zaščite in izobraževanju otrok ter najstnikov, ki uporabljajo internet in nove spletne tehnologije. Ob ustanovitvi je bil projekt deležen takojšnjega in vsesplošno pozitivnega odziva tako s strani različnih deležnikov kot tudi splošne javnosti.

V obdobju 2007 do 2009 so izvajali informacijsko kampanjo, s katero so želeli starše in mladostnike še bolj direktno vključiti v aktivnosti projekta. V letu 2009 je s svojim delovanjem pričela tudi telefonska linija Nasvet za net, ki je namenjena svetovanju (preko telefona ali elektronske pošte) otrokom in mladostnikom, ki so naleteli na neprimerno ali škodljivo spletno vsebino, stike, postali žrtev spletnega nadlegovanja, kraje identitete ali bi se radi pogovorili o drugih vprašanjih in dilemah, povezanih s spletom (SAFE-SI, 2012).

Namen projekta je informiranje ciljne skupine (učitelji, starši, otroci in najstniki) o prednostih in nevarnostih uporabe IKT s skrbno zasnovano kampanjo osveščanja. V tesnem sodelovanju z nacionalnimi deležniki pripravljajo informativna gradiva, organizirajo

dogodke, kakršen je Dan varne rabe interneta, izobraževanja v obliki delavnic in seminarjev za starše, otroke in učitelje ter vzdržujejo informativno spletno stran.

Aktivnosti in orodja osveščanja

Za večjo prepoznavnost in osveščanje uporabnikov o varni rabi interneta in mobilnih telefonov, so pri SAFE-SI pripravili različna orodja in aktivnosti osveščanja, ki jih vsako leto dopolnjujejo in širijo. Te aktivnosti in orodja osveščanja so (SAFE-SI, 2009):

a) orodja za osveščanje,
b) online in offline izobraževalna gradiva,
c) kampanja za širjenje osveščanja,
d) izobraževanje za ciljne skupine,
e) panel mladih,
f) SAFE-SI v medijih.

a) ORODJA ZA OSVEŠČANJE

Spletna stran SAFE-SI nudi specifične in podrobne informacije ter nasvete o varnejši rabi interneta in mobilnih telefonov, ki so namenjeni določenim ciljnim skupinam - staršem, učiteljem, otrokom in najstnikom. Preko njihove spletne strani lahko obiskovalci dostopajo tudi do slovenske prijavne točke Spletno oko in telefonske svetovalne linije Nasvet za net. Poleg tega spletna stran obiskovalcem omogoča gledanje video posnetkov in poslušanje avdio gradiv, dostop do elektronskih verzij promocijskih in izobraževalnih gradiv, ki so nastala v okviru SAFE-SI, udeležbo pri različnih igrah, testih in kvizih, pošiljanje razglednic ter podpisovanje zaobljube proti spletnemu nadlegovanju, itn. Spletna stran obiskovalcem omogoča, da si preko aplikacij, kot so Facebook, Twitter, Delicious, Google, StumbleUpon, s prijatelji, otroki, starši in drugimi izmenjujejo uporabne ali zanimive informacije, ki jih najdejo na strani (SAFE-SI, 2009).

Spletna stran SAFE-SI je postala ključna referenčna točka, ki jo v veliki meri uporabljajo ciljne skupine, da bi našle informacije ter navodila za varno uporabo interneta. V iskalnikih za ustrezne ključne besede je postavljena zelo visoko, saj zaseda prvo mesto.

b) ONLINE IN OFFLINE IZOBRAŽEVALNA GRADIVA

V okviru projekta so pripravili številna uporabna, izobraževalna in promocijska gradiva za mladostnike, starše in učitelje.

Online izobraževalna gradiva

V skladu s pogodbo, sklenjeno z največjim slovenskim spletnim iskalnikom Najdi.si, imajo na njihovi spletni strani na voljo brezplačen prostor za oglase in relevantne prikaze vsebin, glede na ključne besede, povezane z varno rabo interneta, ki jih v iskalnik vtipka uporabnik. Leta 2009 so sklenili sponzorski dogovor za brezplačno promocijo spletne strani projekta v Httpool premium omrežju, v katerega so vključene različne spletne strani, kot so Otroci.org, Kolosej.si, Kulinarika.net, ipd. (SAFE-SI, 2009).

Poleg tega se je SAFE-SI vključil v priljubljena spletna socialna omrežja Facebook, Twitter, Youtube in RSS. Na Facebooku so ustanovili skupino proti spletnemu nadlegovanju, člane povabili na dogodek Dan varne rabe interneta 2011, in jim omogočili postati oboževalec spletne strani SAFE-SI. Vse našteto prispeva k boljši prepoznavnosti. Na spletni strani navedenega socialnega omrežja so objavili oglasno pasico, s katero so najstnike pozvali, da preverijo svojo stopnjo odvisnosti od interneta. Prav tako ima SAFE-SI otroško igrišče. Vključene so vse igre, primerne za mlajše otroke, njihova tema je internetna varnost.

Offline izobraževalna gradiva

SAFE-SI je za povečanje prepoznavnosti svoje spletne strani sklenil tudi nekaj pomembnih dogovorov o oglaševanju s slovenskimi tiskanimi mediji. Od novembra 2008 je oglas projekta SAFE-SI redno prisoten v mesečniku Otrok in družina, ki je namenjen staršem. Dva oglasa SAFE-SI sta bila vključena tudi v stenski koledar revije National Geographic Junior, ki je izšel v 10.000 izvodih skupaj z decembrsko izdajo omenjene revije.

V letu 2011 so s pričetkom novega šolskega leta (1. september 2011), razdelili več kot 21.000 kopij periodnih sistemov z mislijo »Pomisli, preden objaviš!« vsem dijakom prvih letnikov srednjih šol.

Prav tako SAFE-SI sodeluje na različnih prireditvah: sejmih, konferencah in festivalih. Glavni namen udeležbe je seveda osveščanje in izobraževanje.

c) KAMPANJA ZA ŠIRJENJE OSVEŠČANJA

Vseevropska kampanja proti spletnem nadlegovanju 2009

Slovenska točka osveščanja je leta 2009 v celoti podprla vseevropsko komunikacijsko kampanjo proti spletnemu nadlegovanju in se aktivno vključila v posredovanje njenega sporočila ciljni skupini najstnikov, starih od 12 do 17 let. SAFE-SI je preko nacionalnih televizijskih postaj, spletnih strani in priljubljenih socialnih omrežij, Facebook, Frendi in flirt, Mojvideo ter GenSpot, uspešno promoviral televizijsko in spletno različico vseevropskega videa »Ustavimo spletno nadlegovanje« (SAFE-SI, 2009).

Tudi aktivnosti točke osveščanja na nacionalni ravni so bile ob Dnevu varne rabe interneta usmerjene v boj proti spletnemu nadlegovanju. Osrednje sporočilo kampanje se je glasilo: »Spletno nadlegovanje ni zabavno. Ustavimo ga!« Za najstnike so izdelali plakate in zloženke o spletnem nadlegovanju, ki so jih februarja posredovali slovenskim osnovnim in srednjim šolam. Ekipa SAFE-SI je sestavila spletno zaobljubo, ki jo mladi lahko podpišejo in s tem obljubijo, da spletnega nadlegovanja ne bodo dopuščali. Zaobljuba kroži tako na spletni strani SAFE-SI kot tudi po drugih straneh s spletnimi storitvami, ki jih večinoma uporabljajo mladi.

Dan varne rabe interneta 2011 in 2012

Dan varne rabe interneta je vsakoletni mednarodni dogodek, ki spodbuja varnejšo in odgovornejšo rabo spletnih tehnologij in mobilnih telefonov, ki ga organizirata mednarodna organizacija INSAFE in nacionalna točka osveščanja SAFE-SI.

V letu 2011 je projektna skupina SAFE-SI prvič organizirala ne le dan, ampak tudi *»Mesec varne rabe interneta«*. Tako so februarja potekale različne aktivnosti in dogodki. Zaradi pozitivnih izkušenj je bil enak koncept uporabljen tudi v letu 2012.

d) IZOBRAŽEVANJE ZA CILJNE SKUPINE

Velik interes je v slovenskih šolah izkazan izobraževanju mladostnikov in staršev. SAFE-SI tako nudi pomoč pri izobraževanju staršev, učiteljev in otrok o nevarnostih interneta že od leta 2007. Novembra 2011 so se odločili še za korak naprej in ponudili možnost izobraževanja delavcem v nevladnih organizacijah in socialnim delavcem, da bi jih opremili z osnovnimi informacijami spletne varnosti, saj jih potrebujejo v vsakdanjem poklicem življenju. Program usposabljanja je primeren za različne svetovalce in delavce, ki delajo z mladimi, prostovoljce, terapevte, strokovnjake, ki delajo na telefonih za pomoč in za druge organizacije, ki skrbijo za dobro počutje otrok. Osredotočili so se na podajanje ustreznih informacij, preučili praktične primere, kako varno uporabljati mobilne telefone, obravnavali so spletno zasvojenost in preučevali rezultate nacionalnih spletnih primerov zlorabe otrok.

e) PANEL ZA MLADE

V Sloveniji nimamo stalnega panela za mlade, vendar so organizirane različne diskusijske skupine z otroci iz različnih delov države – tistih iz mesta pa tudi s podeželja, saj želijo, da bi čim več mladih spregovorilo o izkušnjah na spletu, le tako bi lahko dvignili zavedanje vseh slovenskih otrok. V obdobju od septembra 2010 do februarja 2012 so organizirali pet panelov za mlade.

f) SAFE-SI V MEDIJIH

V zadnjih dveh letih je bil NAC (Safe Network Access Control – Varen omrežni dostop) vedno uspešen pri ustvarjanju tiska in medijev. SAFE-SI je uspešno vzpostavil močno povezanost z mediji in tako dosegel kontinuirano izdajo informacij o ozaveščanju. S tem je SAFE-SI postal referenčna točka za vse novinarje, ki pripravljajo članke/zgodbe o internetni varnosti.

3.2 SPLETNO OKO

Spletno oko je slovenska spletna prijavna točka, kjer lahko anonimno prijavimo otroško pornografijo in sovražni govor na internetu (www.spletno-oko.si). Projekt deluje v okviru komunitarnega programa Varnejši internet plus in organizacije INHOPE. Kot člani svetovalnega telesa pri projektu sodelujejo tudi Vrhovno državno tožilstvo Slovenije in policija ter predstavniki medijev in ostalih organizacij, ki aktivno delujejo na področju varovanja pravic otrok.

Glavna naloga prijavne točke Spletno oko je zbiranje anonimnih prijav otroške pornografije in sovražnega govora na internetu ter njihovo posredovanje pooblaščenim

organom pregona. Anonimno prijavo lahko poda vsak uporabnik interneta, če meni, da je na internetu naletel na otroško pornografijo ali sovražni govor.

Prijavna točka Spletno oko je del širšega evropskega združenja za učinkovito zmanjševanje nezakonitih vsebin na internetu. V različnih državah trenutno deluje 42 prijavnih centrov, ki so združeni v okvir krovne organizacije INHOPE.
V Sloveniji projekt izvajajo:

- Univerza v Ljubljani, Fakulteta za družbene vede kot koordinatorka projekta,
- ARNES, Akademska in raziskovalna mreža Slovenije in
- Zveza potrošnikov Slovenije kot partnerka pri projektu.

Projekt izvajajo v sodelovanju s slovensko policijo in drugimi deležniki na projektu, kot so mediji, nevladne organizacije, podjetja in nacionalni projekti.

V pogledu sovražnega govora Spletno oko obravnava **izključno** prijave domnevno **kaznivega sovražnega govora** kot je opredeljeno v 297. členu Kazenskega zakonika KZ-1, ki se nanaša na sovražni govor, povezan s pozivanjem k ogrožanju določenih skupin. Kaznivi sovražni govor predstavlja zelo majhen delež komunikacije, ki se v javnosti sicer označujejo kot sovražni govor. Podobne omejitve javne komunikacije v primeru sovražnega govora poznajo praktično vse države in temu je zelo težko oporekati. Gre za zelo resna kazniva dejanja, podobno kot v primeru **otroške pornografije**, ki je drugo področje, kjer Spletno oko sprejema prijave (Spletno oko, 2012).

V navedenih dveh primerih Spletno oko nastopa kot točka civilne družbe, ki omogoča uporabnikom interneta, da prijavijo nelegalne vsebine na alternativen način mimo organov pregona.

V primeru otroške pornografije in kaznivega sovražnega govora se Spletno oko vsekakor zavzema, da se tovrstne vsebine čim prej odstranijo s spleta. Lahko bi rekli, da se Spletno oko zavzema za cenzuro teh vsebin, vendar je treba takoj dodati:

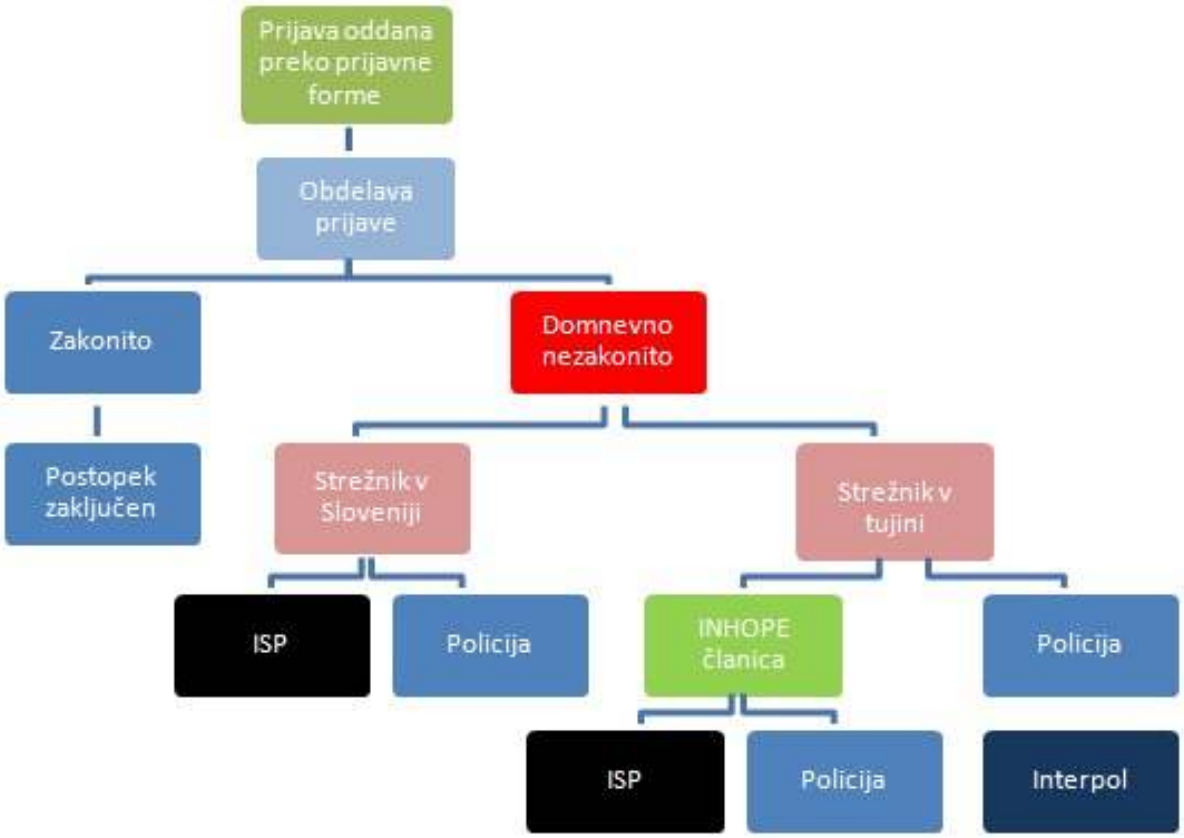
- ni države, ki ne bi cenzurirala,
- ni resnih argumentov, ki bi nasprotovali omejevanju tovrstnih ekstremnih vsebin,
- o tovrstnih omejitvah obstaja – tako v slovenski kot v evropski družbi – tako visoko soglasje kot o redkokateri drugi zadevi (Spletno oko, 2012).

Postopek prijave domnevno nezakonite vsebine

Kot prikazuje Slika 1, mora prijavitelj najprej izpolniti kratek prijavni obrazec. Ključna informacija v obrazcu je naslov spletne strani, na kateri se domnevno nezakonita vsebina nahaja. Usposobljeni pregledovalci prijavne točke Spletno oko prijavo pregledajo in jo, če ocenijo, da gre za domnevno nezakonito vsebino, posredujejo organom pregona. V primeru, da je prijavljena stran na slovenskem strežniku, le-to obravnava policija, hkrati pa prijavna točka, po navodilih policije o obstoju nezakonite vsebine na strežniku, obvesti tudi ponudnika gostiteljstva.

V primeru, da gre za prijavo strani na tujem strežniku, se le-ta preko slovenske policije posreduje tudi Interpolu, in če obstaja, še prijavni točki pod okriljem INHOPE-a v državi, kjer gostuje strežnik z domnevno nezakonito vsebino. Pregledovalci prejete prijave obravnavajo v najkrajšem možnem času, najkasneje v dveh dneh od prejetja prijave (Spletno oko, 2012).

Slika 1: Postopek prijave domnevno nezakonite vsebine



Vir: Spletno oko, 2012

V celotnem postopku (od prijave nezakonitih spletnih vsebin do ustreznega ukrepanja) se prijavna točka in policija ukvarjata izključno z vsebino prijave. Podatki o prijavitelju se ne hranijo, saj prijava po spletnem obrazcu ne omogoča razkritja identitete prijavitelja. Podatki, ki so posredovani na pristojne inštitucije, se nanašajo zgolj na vsebino prijave. Prijavna točka ne beleži podatkov o prijavitelju in jih torej tudi ne posreduje tretjim osebam. V primeru, da prijavitelj v prijavni obrazec sam namenoma vnese svoje podatke (na primer svoj elektronski naslov v polje namenjeno komentiranju prijave), so ti podatki pred posredovanjem prijave pristojnim inštitucijam odstranjeni. Prijaviteljevi podatki v nobenem primeru niso uporabljeni pri nadaljnjem obravnavanju prijave.

3.3 SI-CERT

SI-CERT (Slovenian Computer Emergency Response Team) je center za posredovanje pri internetnih incidentih, ki koordinira obveščanje in reševanje varnostnih problemov v računalniških omrežjih v Sloveniji (www.cert.si). SI-CERT obravnava varnostne incidente, obvestila o zlorabah, okužbah in vdorih v računalniške sisteme. Predstavlja kontaktno točko, ki opravlja posredniško in svetovalno vlogo. SI-CERT je bil ustanovljen leta 1995 in deluje v okviru Arnesa (Akademske in raziskovalne mreže Slovenije), vendar sprejema prijave varnostnih incidentov za vsa računalniška omrežja v Sloveniji.

Po nekajletnih dogovarjanjih je Arnes spomladi 2010, na pobudo Direktorata za informacijsko družbo Ministrstva za visoko šolstvo, znanost in tehnologijo, pričel z dejavnostmi programa osveščanja, ki poteka pod imenom Varni na internetu.

Kaj je CERT?
Prvi CERT je bil ustanovljen leta 1988 v ZDA kot odgovor na prvi večji internetni incident - širjenje prvega črva, kasneje imenovanega kar "The Internet Worm". CERT je bil ustanovljen s strani DARPA (Defense Advanced Research Projects Agency, US Department of Defense), nato pa je prešel v upravljanje Carnegie Mellon University. S širitvijo interneta po svetu so se postopoma začele podobne organizacije in servisi pojavljati tudi izven ZDA, prvotni CERT se je preimenoval v CERT Coordination Center (CERT/CC) (SI-CERT, 2012).

Poslanstvo
Glavni cilj je odzivanje na omrežne incidente in osveščanje spletnih uporabnikov o spletnih tveganjih. SI-CERT obravnava varnostne incidente, obvestila o zlorabah, okužbah in vdorih v računalniške sisteme. Predstavlja kontaktno točko, ki opravlja posredniško in svetovalno vlogo. Poleg odzivanja na varnostne incidente je velikega pomena tudi osveščanje uporabnikov omrežja o tveganjih in s tem povezanimi ukrepi, ki zmanjšajo verjetnost neljubega dogodka.

Program osveščanja Varni na internetu naslavlja dve ciljni skupini: odrasle, domače uporabnike in mala podjetja oz. samostojne podjetnike. Prvim nudi nasvete s področja spletnega bančništva in spletnih nakupov, drugim pomaga pri vprašanjih, ki so povezana z IT vidikom poslovanja podjetja. Obema skupinama je predstavljen sklop spletnih goljufij in prevar.

Sodelovanje s slovenskimi in tujimi organizacijami
SI-CERT je z novim programom osveščanja Varni na internetu razvil sodelovanje z drugimi organizacijami, ki skrbijo za varnejši internet. Te lahko razdelimo v tri sklope (Mešić, osebna komunikacija, 2012):

1. Sodelovanje z ARNES-om in SAFE-SI

Arnes je že od leta 1999 (takrat na pobudo MŠŠ), v okviru mednarodne projektne koordinacije European Schoolnet, partner pri izvajanju projektov Evropske komisije iz akcijskega načrta Varnejši internet (Safer Internet Action Plan – Safer Internet Plus), ki promovira varnejšo uporabo interneta za otroke in mladostnike. Gre za koordinirane aktivnosti v vseh državah članicah EU, sofinancira ga Evropska komisija (Grant Agreement No SI-2009-SIC-123905). V Sloveniji projekte podpira Direktorat za informacijsko družbo na Ministrstvu za visoko šolstvo, znanost in tehnologijo. V okviru tega akcijskega načrta Arnes od leta 2005 aktivno sooblikuje SAFE-SI, nacionalni center osveščanja o varnejši rabi interneta.

Mednarodno sodelovanje poteka skozi omrežje INSAFE, ki povezuje nacionalne centre osveščanja.

2. SI-CERT in sodelovanje s slovenskimi organizacijami

SI-CERT lahko deluje le ob dobri povezanosti z različnimi deležniki na področju omrežne in informacijske varnosti. Ob obravnavi sodelujemo z internetnimi operaterji (individualno in v okviru združenja Sispa) in ponudniki storitev na spletu, kot tudi z Agencijo za pošto in elektronske komunikacije. V letu 2010 smo na sestankih pri Informacijskem pooblaščencu RS obravnavali vprašanja s področja osebnih podatkov, prometnih podatkov in omrežne komunikacije s stališča Zakona o varstvu osebnih podatkov in Zakona o elektronskih komunikacijah. Z Zvezo potrošnikov Slovenije (oz. njihovim Evropskim potrošniškim centrom) smo sodelovali pri posameznih incidentih lažnih nakupov ali prodaje.

3. Sodelovanje SI-CERT-a v mednarodnih organizacijah

SI-CERT je aktiven član Terenine delovne skupine evropskih centrov za posredovanje pri internetnih incidentih, TF-CSIRT in svetovnega združenja FIRST (Forum of Incident Response and Security Teams). TF-CSIRT združuje vse evropske varnostne centre, tako iz raziskovalno-izobraževalne kot tudi iz komercialne in vladne sfere. SI-CERT je aktiven član evropske agencije ENISA (European Networking and Information Security Agency), program Varni na internetu pa bo zastopal Slovenijo v prihajajočem »mesecu spletne varnosti«, ki ga oktobra 2012 organizira ENISA.

Sporočanje incidenta SI-CERT

Najbolj pomembna podatka pri vsakem prijavljanju kakršnekoli omrežne zlorabe ali varnostnega incidenta sta:

- datum in točen čas dogodka in
- IP številka oz. naslov izvora.

Zgornja dva podatka sta praviloma vedno prisotna v sistemskih zapisih, ki beležijo aktivnosti na sistemu ("log files" oz. "audit files"). V elektronski pošti sta ta podatka vidna v glavi sporočila, ki pa se ne prikaže v polni obliki v vseh programih za elektronsko pošto, zato morate najti način prikaza polne glave sporočila (večkrat se možnost nahaja v meniju programa kot "full headers", ali pa možnost "view as source") (SI-CERT, 2012).

Varnostne grožnje

Uporaba omrežja nam olajša komunikacijo in zabriše zemljepisne omejitve. Ravno zaradi tega smo na omrežju tudi bolj izpostavljeni različnim grožnjam. Z izkoriščanjem varnostnih lukenj, ranljivosti v programski opremi ali v naših vedenjskih vzorcih lahko tujci pridobijo nadzor nad našo opremo, podatki in denarjem. Spodaj izpostavljamo nekaj tipičnih varnostnih groženj (SI-CERT, 2012):

- **phishing;** lažna spletna mesta, namenjena kraji gesel,
- **kraja identitete;** izguba osebnih podatkov, gesla za elektronsko pošto in dostop do storitev na omrežju,
- **spletne goljufije;** goljufi preko lažnih oglasov za prodajo, ponudbami za nakup in potvorjenimi sporočili poskušajo do vašega denarja,
- **vdor;** priprave na vdor, zlorabe preko ranljivosti spletnih aplikacij ali šibkih gesel.
- **okužbe;** računalniški virusi, črvi in trojanski konji,
- **spam**; neželena elektronska pošta vseh oblik, od reklam do zadetkov na loterijah.

3.4 MEDNARODNA POVEZANOST ORGANIZACIJ ZA VAREN INTERNET

Junija 1996 je bila ustanovljena prva internetna prijavna točka s sedežem na Nizozemskem, ki je osebe, povezane z razpečevanjem nelegalnega materiala, iskala s pomočjo policije. Temu zgledu so hitro sledile Norveška, Belgija in Velika Britanija leta 1996. Kasneje so načrte za internetne prijavne točke uresničili še v Avstriji, na Irskem, Finskem, v Španiji in Franciji.

Organizacija Childnet Internacional je leta 1997 predlagala, da bi prijavne točke po vsem svetu pričele s tesnejšim sodelovanjem. Evropska komisija je v okviru programa Daphne zagotovila finančna sredstva za oblikovanje foruma, za vse evropske prijavne točke, da se lahko srečajo in razpravljajo o perečih skupnih vprašanjih. Sprejeli so Statut združenja in 23. novembra 1999 je osem prijavnih točk uradno ustanovilo organizacijo INHOPE.

3.4.1 INHOPE

INHOPE (International Association of Internet Hotline Providers) je mednarodno združenje internetnih prijavnih točk (www.inhope.org). Naloga organizacije je usklajevanje mreže internetnih prijavnih točk po vsem svetu, jim nuditi podporo pri odzivanju na prijave o nezakonitih vsebinah z namenom, da bi internet bil varnejši.

Zgodovina

Do leta 1995 so se uporabniki interneta, internetni ponudniki, državne vlade in organi pregona že zavedali, da je internet postal tudi prostor pedofilov, ki ga izrabljajo za objavo in izmenjavo slik z otroško pornografijo. Prav tako so zasledili druge nezakonite dejavnosti, kot so objave z rasističnim gradivom.

Različne nacionalne pobude je tako združil interes, da razmislijo, kako preprečiti te nezakonite dejavnosti, zlasti otroško pornografijo. V Nemčiji je bilo več ločenih skupin, ki

so prve začele z razpravo o primerih pedofilije v parlamentu. Obenem je bila ustanovljena neprofitna, mednarodna organizacija Childnet Internacional s sedežem v Veliki Britaniji, z nalogo spodbujati otrokove interese v mednarodnih komunikacijah (INHOPE, 2010).

Junija 1996 je bila ustanovljena prva internetna prijavna točka s sedežem na Nizozemskem, ki je osebe, povezane z razpečevanjem nelegalnega materiala iskala s pomočjo policije. Temu zgledu so hitro sledile tudi Norveška, Belgija in Velika Britanija leta 1996. Kasneje so načrte za internetne prijavne točke uresničili še v Avstriji, na Irskem, Finskem, v Španiji in Franciji.

Naslednje leto, 1997 je organizacija Childnet Internacional predlagala, da bi prijavne točke po svetu pričele s tesnejšim sodelovanjem. Evropska komisija je v okviru programa Daphne zagotovila finančna sredstva za oblikovanje foruma, za vse evropske prijavne točke, ki se na ta način srečajo in razpravljajo o perečih skupnih vprašanjih. Sprejeli so Statut združenja in 23. novembra 1999 je osem prijavnih točk uradno ustanovilo organizacijo INHOPE, registrirano na Nizozemskem. Urejena je s Statutom in Kodeksom ravnanja.

Danes so INHOPE prijavne točke zrasle v omrežje dvainštiridesetih prijavnih točk v sedemintridesetih državah po vsem svetu; v Evropi, Aziji, Severni Ameriki in Avstraliji. Še vedno se financirajo s podporo Evropske komisije v okviru programa Varnejši internet in so urejene s Statutom in Kodeksom ravnanja. Imajo redne skupščine, kjer izmenjujejo izkušnje in način dela. INHOPE in njene članice se borijo proti nezakonitim spletnim vsebinam, zlasti proti otroški pornografiji (INHOPE, 2012).

Kaj je prijavna točka?

INHOPE »Hotline« ali prijavna točka, je možnost anonimne, internetne prijave internetnega gradiva, za katerega uporabniki menijo, da vsebuje otroško pornografijo ali drugo nezakonito vsebino. Prijavna točka mora zagotoviti preiskavo in če je ugotovljeno, da je le-ta nezakonita, mora podatke posredovati ustreznemu organu pregona, kot tudi ponudniku internetnih storitev, ki gosti vsebino. Vse države, ki so članice združenja INHOPE prijavnih točk, morajo ravnati v skladu z najboljšo prakso, saj jih zavezuje Kodeks ravnanja. Slovenska prijavna točka je Spletno oko.

Poslanstvo

»Podpirati in krepiti delovanje internetnih prijavnih točk po vsem svetu, zagotoviti hiter odziv in ukrepanje na prijave o nezakonitih vsebinah ter zagotoviti, da bo internet postal varnejši.« Za doseganje tega poslanstva INHOPE upošteva pet posebnih ciljev (INHOPE, 2012):

- oblikovanje politike in standardov najboljše prakse za prijavne točke in spodbujanje izmenjave znanja med članicami z dobrim delovnim odnosom in zaupanjem;

- zagotavljanje hitrega in učinkovitega odziva na nezakonite vsebine po vsem svetu, z razvojem doslednih, učinkovitih in varnih mehanizmov za izmenjavo poročil med prijavnimi točkami na mednarodni ravni in s tem zagotoviti usklajen pristop;
- širitev INHOPE mreže prijavnih točk po svetu in zagotovitev podpore novim prijavnim točkam ter usposabljanje za doseganje standardov dobre prakse;
- promoviranje dela prijavnih točk političnemu svetu na mednarodni ravni, državnim vladam, organom pregona in drugim podobnim institucijam, da bi dosegli boljše mednarodno sodelovanje;
- povečanje ozaveščenosti o organizaciji INHOPE in njenih članicah pri ključnih interesnih skupinah kot tudi širši javnosti, za boljše globalno sodelovanje pri prijavah nezakonite vsebine, še posebej pri otroški pornografiji.

Ključne naloge organizacije so:
- izmenjava znanja,
- podpora tako starim kot novim prijavnim točkam,
- izmenjava poročil,
- koordinacija s sorodnimi organizacijami,
- izobraževanje in obveščanje političnega sveta na mednarodni ravni.

Vrednote, ki jih cenijo v organizaciji INHOPE:
- svoboda interneta,
- zavezanost k pozitivni uporabi interneta,
- skupna odgovornost za zaščito mladih ljudi s strani vlade, vzgojiteljev, staršev in internetnih ponudnikov.

Cilji organizacije INHOPE:
- vzpostavitev in vzdrževanje učinkovite podpore nacionalnim prijavnim točkam,
- izobrazba in podpora novim prijavnim točkam,
- spodbujanje trajno ozaveščanje in izobraževanje o internetni varnosti,
- vzpostavitev učinkovitih postopkov za sprejem in obdelavo prijav.

Mobilni INHOPE

Mobilni INHOPE je orodje, s katerim želijo vključiti sodelovanje javnosti v poročanje o otroški pedofiliji na internetu. Na voljo je za Windows Phone 7, Android, iPhone in Blackberry. Z uporabo preprostega vmesnika omogoča uporabniku, da pošlje anonimno prijavo preko mobilne naprave za katerokoli spletno vsebino, ki vsebuje nelegalno vsebino (INHOPE, 2011).

3.4.2 INSAFE

INSAFE je evropsko omrežje točk osveščanja, ki mladim po vsej Evropi promovira varno in odgovorno rabo interneta in mobilnih telefonov (www.saferinternet.org).

INSAFE skuša zagotoviti visoko stopnjo osveščenosti vsakega posameznika glede varne uporabe informacijsko-komunikacijskih tehnologij, prav tako pa tudi poudariti pozitiven vidik novih IKT tehnologij.

Točke ozaveščanja

Nacionalne točke ozaveščanja pomagajo odgovoriti na vprašanja in skrbi mladih, povezanih z njihovimi spletnimi izkušnjami pri stiku s škodljivo ali nezakonito spletno vsebino. V Sloveniji je točka ozaveščanja imenovana SAFE.SI.

V omrežje so vključene posamezne nacionalne točke osveščanja (od 1.3.2005 tudi Slovenija). Posamezne točke osveščanja v okviru INSAFE omrežja medsebojno sodelujejo, si izmenjujejo znanja in izkušnje, načrtujejo skupne aktivnosti (npr. priprava aktivnosti ob Dnevu varne rabe interneta).

Poslanstvo

Poslanstvo omrežne organizacije INSAFE je predstaviti uporabnikom interneta in drugih spletnih tehnologij vsako spletno izkušnjo kot pozitivno, varno in učinkovito. Mreža poziva k skupni odgovornosti za zaščito pravic in potreb državljanov, še posebej otrok in mladostnikov s strani države, izobraževalnih institucij, staršev, medijev in drugih pomembnih akterjev (INSAFE, 2012).

INSAFE točke osveščanja tesno sodelujejo pri izmenjavi najboljših praks, informacij in sredstev. Najtesneje sodelujejo s šolami in družinami s ciljem, da izobrazijo ljudi in jim omogočijo premostiti digitalni razkorak med domom, šolo in generacijo.

Skupaj s partnerji INSAFE spremlja nastajajoče trende in si tako prizadeva okrepiti svoj prostor na spletu kot mesto, kjer se lahko izobrazimo o varnosti na internetu in razvijamo računalniško pismenost. Uporabnike želijo ozavestiti o škodljivih in nezakonitih vsebinah ali drugih storitvah.

Centri za osveščanje

Vsaka država v omrežju INSAFE ima svoj nacionalni center osveščanja, ki je odgovoren za izvajanje kampanj, usklajevanje dejavnosti, razvoj sinergije na nacionalni ravni in je v tesnem sodelovanju z vsemi pomembnimi akterji na evropski, regionalni in lokalni ravni.

Omrežje INSAFE organizira Dar varne rabe interneta, ki poteka v mesecu februarju že od leta 2004 in vključuje tudi države izven Evrope.

Program za varnejši internet

V zadnjih letih je Evropska unija uskladila in podprla prizadevanja, da bi internet postal varnejši še posebej za otroke. Ta prizadevanja so v teku, v 5-letnem projektu (2009-2013), pod okriljem programa za varnejši internet. Za boj proti nezakonitim vsebinam in škodljivemu vedenju na internetu bo namenjenih 55 milijonov evrov.

Program Varnejši internet zajema Web 2.0 komunikacijske storitve, kot je socialno mreženje, hkrati pa sofinancira projekte za (INSAFE, 2012):

- zagotavljanje ozaveščenosti otrok, staršev in učiteljev o tem, kako ostati varen na spletu,
- zagotovljanje nacionalne kontaktne točke državljanom za prijavo nezakonitih in škodljivih vsebin in vedenja, zlasti v zvezi s spolno zlorabo otrok,
- spodbujanje samoregulativnih pobud na tem področju,
- spodbujanje otrok k sodelovanju pri ustvarjanju varnejšega spletnega okolja,
- vzpostavljanje baze znanja o uporabi novih tehnologij in s tem povezanih tveganj, ki združuje raziskovalce, na področju spletne varnosti otrok na evropski ravni.

Od 55 milijonov evrov proračuna skoraj polovica (48 odstotkov), služi za dvig javne zavesti, 34 odstotkov za boj proti nezakonitim vsebinam in škodljivemu obnašanju na spletu, 10 odstotkov za spodbujanje varnejšega spletnega okolja in 8 odstotkov za vzpostavitev baze izobraževanja (INSAFE, 2012).

Program ima štiri glavne ukrepe:

- boj proti nezakonitim vsebinam,
- boj proti škodljivi vsebini,
- spodbujanje varnejšega okolja in
- ozaveščanje.

Tabela 1: Primerjalna tabela organizacij

	Obseg	Poslanstvo	Ciljne skupine	Sodelovanje z organi pregona
SAFE-SI	Slovenska nacionalna točka osveščanja.	Promocija varne in odgovorne rabe interneta ter mobilnih tehnologij.	Otroci, najstniki, starši in učitelji.	Ne.
Spletno oko	Slovenska spletna prijavna točka.	Zmanjšanje posnetkov spolnih zlorab otrok in sovražnega govora na spletu.	Vsi.	Da.
SI-CERT	Slovenski center za posredovanje pri internetnih incidentih.	Odzivanje na omrežne incidente in osveščanje spletnih uporabnikov o spletnih tveganjih.	Vsi.	Posredniki.
INHOPE	Mednarodno združenje spletnih prijavnih točk.	Usklajevanje mreže internetnih prijavnih točk po vsem svetu, podpora pri odzivanju na prijave o nezakonitih vsebinah.	Vsi.	Da.
INSAFE	Evropsko omrežje točk osveščanja.	Promocija varne in odgovorne rabe interneta ter mobilnih tehnologij.	Mladostniki.	Ne.

Vir: lasten

4 EMPIRIČNA RAZISKAVA ODNOSA ŠTUDENTOV DO VARNOSTI NA INTERNETU

V začetku meseca avgusta 2012 sem opravila empirično raziskavo s pomočjo anketnega vprašalnika. Za izvajanje ankete sem uporabila spletno orodje MojaAnketa.si (www.mojaanketa.si). Namen empirične raziskave je bil preučiti odnos študentov do varnosti na internetu, ki se izkazuje skozi poznavanje organizacij in osveščenostjo za neprimerno ali nezakonito vsebine, ki jo najdemo na spletu. Pripravila sem tematsko ustrezen anketni vprašalnik s šestimi vprašanji, od tega sta dve o varnosti interneta, dve o organizacijah in dve o (ne)primernosti ali nezakonitosti spletnih vsebin. Anketni vprašalnik je podan v prilogi 5.

Anketa je bila namenjena zgolj študentom, zato smo s prvo točko vprašalnika preverili ali imajo anketiranci status študenta. Če je bil odgovor na vprašanje pritrdilen, so lahko nadaljevali z anketo, če ne, jih je anketni vprašalnik popeljal na konec. S tem smo izločili ostalo populacijo.

Pri izbiri anketirancev sem se omejila na študentsko populacijo, ki uporabljala internet, saj se je raziskava navezovala na varnost na internetu. Povezavo do anketnega vprašalnika sem objavila na različnih študentskih forumih, Facebook skupinah in razposlala tudi preko elektronske pošte. Odzvali so se številni anketiranci, vendar vsi niso izpolnjevali osnovnega kriterija za izbiro – biti študent.

Skupno je bilo oddanih 156 anket, od tega je 100 anket izpolnjevalo osnovni kriterij. Vse ankete so bile izpolnjene pravilno, zato sem lahko iz pridobljenih podatkov naredila empirično raziskavo o varnosti interneta med študenti, ki sledi v nadaljevanju. Ker je število odgovorov enako 100, so ti rezultati enaki odstotkom.

4.1 OSNOVNI PODATKI O ANKETIRANCIH

1. Spol:

Tabela 2: Struktura anketirancev glede na spol

SPOL	Št. odgovorov
Ženske	67
Moški	33
SKUPAJ	100

Vir: lasten

Večina sodelujočih pri anketi (Tabela 2) je bilo žensk in sicer 67%, za tretjino manj je bilo moških, kar je 33%.

2. Starost anketirancev:

Kot kaže Tabela 3, je največ anketirancev starih 22 ali 23 let, teh je kar 52. Sledijo anketiranci v starosti med 24. in 28. letom, ki jih je 32. Polovico manj jih je v starosti med 18. in 21. letom.

Tabela 3: Struktura anketirancev glede na starost

STAROST	Št. odgovorov
18 do 21 let	16
22 do 23 let	52
24 do 28 let	32
SKUPAJ	100

Vir: lasten

4.2 ODGOVORI NA VSEBINSKA VPRAŠANJA

1. Splošna opredelitev varnosti na internetu

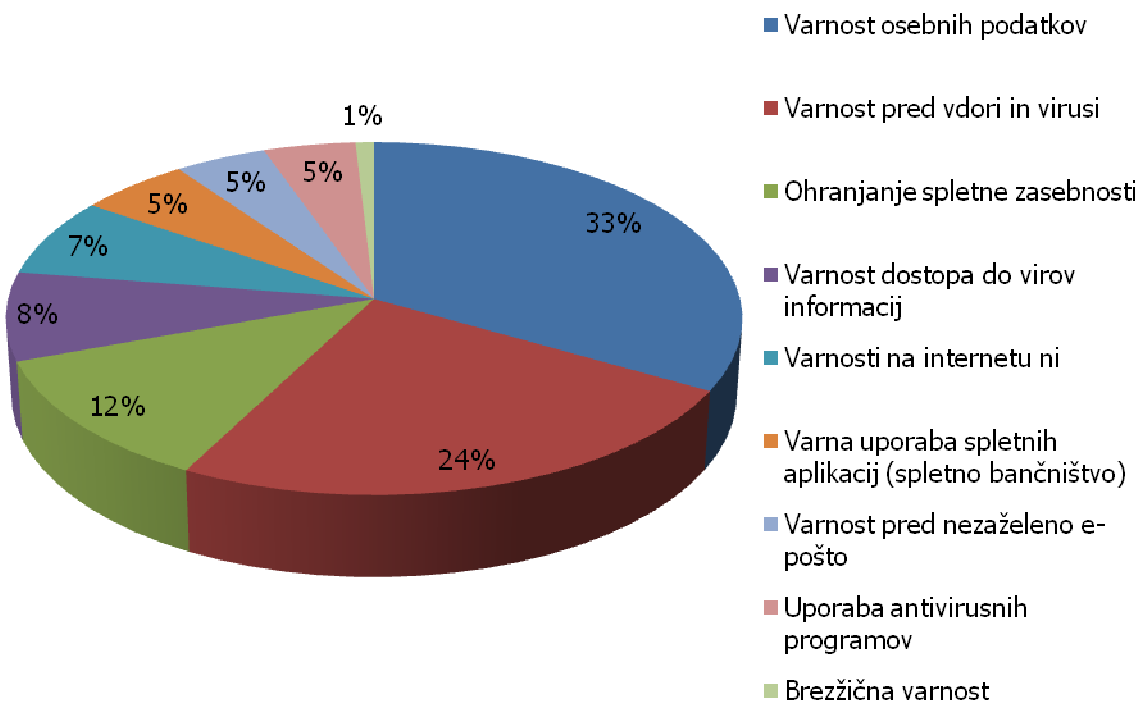
Prvo vprašanje je bilo odprtega tipa, kar pomeni, da so anketiranci nanj odgovorili brez vnaprej ponujenih odgovorov. Nekateri anketiranci so navedli več pomenov varnosti, zato je skupno število večje od 100, saj je vsak zabeležen posebej.

Tabela 4: Opredelitev varnosti na internetu

OPREDELITVE	Št. odgovorov	Odstotek
Varnost osebnih podatkov	37	33
Varnost pred vdori in virusi	27	24
Ohranjanje spletne zasebnosti	13	12
Varnost dostopa do virov informacij	9	8
Varnosti na internetu ni	8	7
Varna uporaba spletnih aplikacij (spletno bančništvo)	6	5
Varnost pred nezaželeno e-pošto	5	5
Uporaba antivirusnih programov	5	5
Brezžična varnost	1	1
SKUPAJ	111	100

Vir: lasten

Grafikon 1: Opredelitev varnosti na internetu (v %)



Vir: lasten, tabela 4

Od skupno stotih odgovorov (Grafikon 1), so bili največkrat omenjeni varnost osebnih podatkov (37-krat), varnost pred vdori (27-krat) in ohranjanje spletne zasebnosti (13-krat). Manj pogoste so bile opredelitve varnosti na internetu kot varnost dostopa do informacij (9-krat), varna uporaba spletnih aplikacij (6-krat), varnost pred nezaželeno e-pošto in uporaba antivirusnih programov 5-krat ter enkrat brezžična varnost.

Zanimivo je, da je osem anketirancev zapisalo, da varnosti na internetu ni. V trenutku, ko podatek javno objavimo na internetu, je le-ta dostopen množici ljudi in ga lahko zlorabijo.

2. Pomembnost varnosti na internetu

Pri drugem vprašanju so morali anketiranci razvrstiti naštete vrste varnosti na internetu, od najbolj do najmanj pomembne z ustreznim točkovanjem, kjer dobi najbolj pomembna vrsta varnosti 1 točko, najmanj pomembna pa 10. V Tabeli 5 so razvrščene vrste varnosti po pomembnosti, kot so jo ocenili anketiranci. Na prvem mestu je najbolj pomembna vrsta (tista, ki je dobila najmanjše skupno število točk od vseh anketirancev), na zadnjem pa najmanj pomembna vrsta (tista, ki je dobila največje skupno število točk od vseh anketirancev). V stolpcu »Razlika« je razlika v točkah med predhodno in tekočo vrsto varnosti.

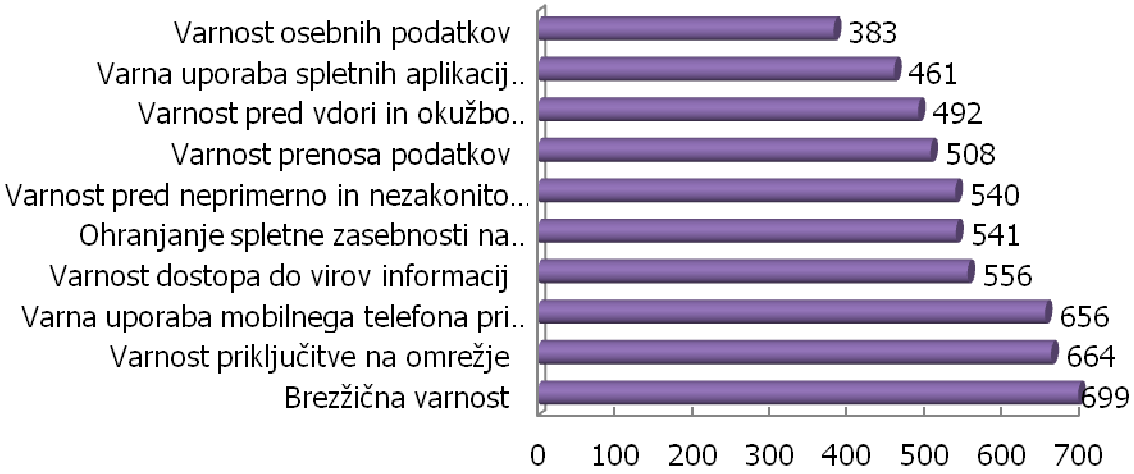
Tabela 5: Pomembnost varnosti na internetu

OPREDELITVE	Mesto	Točke	Razlika
Varnost osebnih podatkov	1	383	/
Varna uporaba spletnih aplikacij (spletno bančništvo, spletno nakupovanje)	2	461	78
Varnost pred vdori in okužbo operacijskega sistema	3	492	31
Varnost prenosa podatkov	4	508	16
Varnost pred neprimerno in nezakonito vsebino (sovražni govor, otroška pornografija, nezaželena e-pošta)	5	540	32
Ohranjanje spletne zasebnosti na socialnih omrežjih	6	541	1
Varnost dostopa do virov informacij	7	556	15
Varna uporaba mobilnega telefona pri spletni uporabi	8	656	100
Varnost priključitve na omrežje	9	664	8
Brezžična varnost	10	699	35

Vir: lasten

Iz danih rezultatov v Tabeli 5 lahko vrste varnosti razdelimo v tri kategorije, saj se med naštetimi vrstami varnosti pojavita dva večja preskoka. V prvi je za anketirance daleč najbolj pomembna varnost osebnih podatkov s 383 točkami. V drugi varna uporaba spletnih aplikacij s 461 točkami, le 31 več jih ima varnost pred vdori in okužbo operacijskega sistema, nato varnost prenosa podatkov, ki ima 508 točk, 32 točk več varnost pred neprimerno in nezakonito vsebino ter še eno točko več ohranjanje spletne zasebnosti na socialnih omrežjih. Zadnjo, tretjo kategorijo zasedajo varnost dostopa do virov informacij s 556 točkami, varna uporaba mobilnega telefona pri spletni uporabi s 656 točkami, varnost priključitve na omrežje s 664 točkami in na zadnjem mestu brezžična varnost s 699 točkami.

Grafikon 2: Pomembnost varnosti na internetu



Vir: lasten, tabela 5

3. Slovenske in mednarodne organizacije za varnost na internetu

Pri vprašanjih tri in štiri smo preverili ali študentje poznajo slovenske in mednarodne organizacije, ki se ukvarjajo z varnostjo na internetu. Nekatere izmed naštetih smo opisali tudi v diplomski nalogi.

Tabela 6: Slovenske organizacije za varnost na internetu

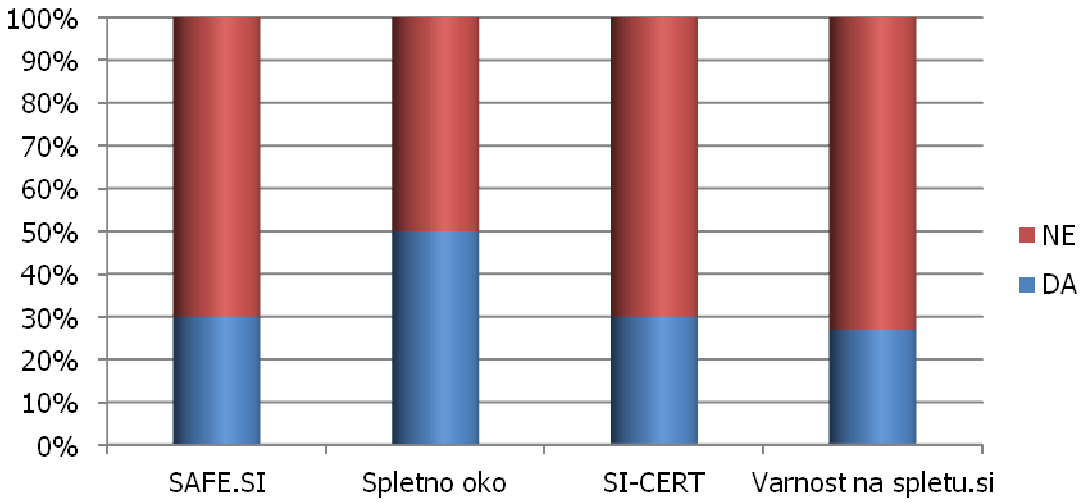
Slovenske organizacije	Št. odgovorov	
	DA	NE
SAFE.SI	30	70
Spletno oko	50	50
SI-CERT	30	70
Varnost na spletu .si	27	73
POVPREČNO (v %)	34	66

Vir: lasten

Rezultati v Tabeli 6 so pokazali, da polovica študentov ne pozna projekta Spletno oko. Več kot dve tretjini pa ne pozna organizacij SAFE.SI in SI-CERT, še več jih ne pozna projekta Varnost na spletu .si.

S povprečno oceno smo želeli ugotoviti, koliko študentov povprečno naj bi vedelo za vse izmed naštetih organizacij; teh je tretjino oziroma 34%, kar pomeni, da 66% ne pozna niti ene izmed naštetih organizacij.

Grafikon 3: Slovenske organizacije za varnost na internetu (v %)



Vir: lasten, tabela 6

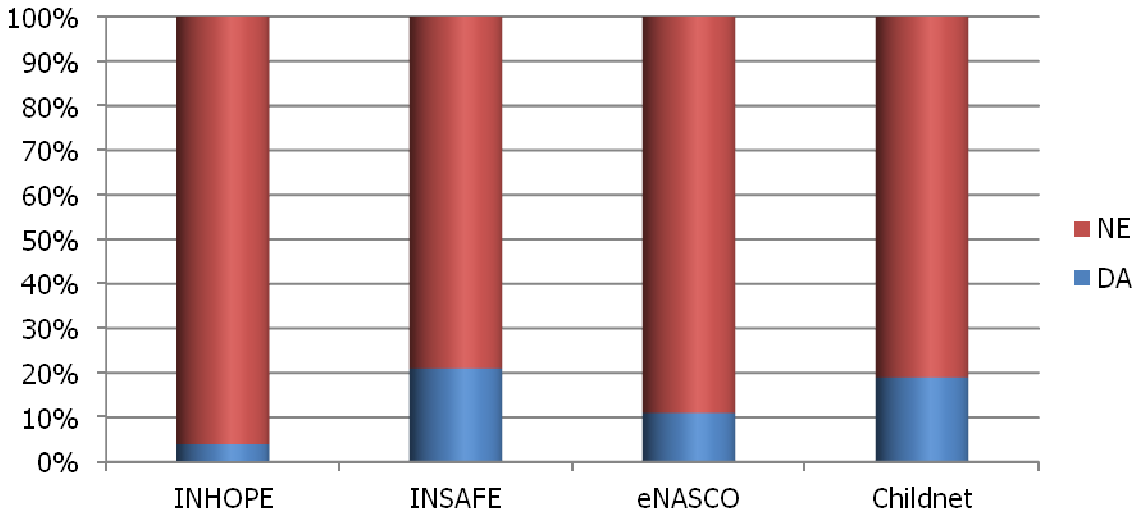
Tabela 7: Mednarodne organizacije za varnost na internetu

Mednarodne organizacije	Št. odgovorov	
	DA	NE
INHOPE	4	96
INSAFE	21	79
eNASCO	11	89
Childnet	19	81
POVPREČNO	14	86

Vir: lasten

Iz danih rezultatov v Tabeli 7 lahko ugotovimo, da povprečno 86% anketiranih ne pozna mednarodnih organizacij za varnost na internetu. Najbolj poznana sta INSAFE z 21% in Childnet z 19%, najmanj pa eNASCO z 11% in INHOPE z le 4%.

Grafikon 4: Mednarodne organizacije za varnost na internetu (v %)



Vir: lasten, tabela 7

4. Prijava neprimerne ali nezakonite vsebine

S petim vprašanjem smo preverjali ali so anketiranci na internetnih forumih zasledili neprimerno, nezakonito vsebino in jo prijavili s pomočjo spletnega obrazca ali kateri izmed organizacij, ki skrbijo za varnost na internetu. Zanimali so nas tako razlogi prijave kot razlogi za neukrepanje.

Tabela 8: Prijava neprimerne ali nezakonite vsebine

Možni odgovori	Št. odgovorov
DA	17
NE	83

SKUPAJ	100

Vir: lasten

Iz Tabele 8 je razvidno, da kar 83% študentov meni, da na internetu ni zasledilo neprimernih ali nezakonitih vsebin, ki bi jih bili dolžni prijaviti eni izmed organizacij za varnost na internetu. Ostalih 17% meni, da je že prišlo v stik z neprimerno in nezakonito vsebino, ki so jo tudi prijavili v pregled organizacijam.

a) Odgovor DA

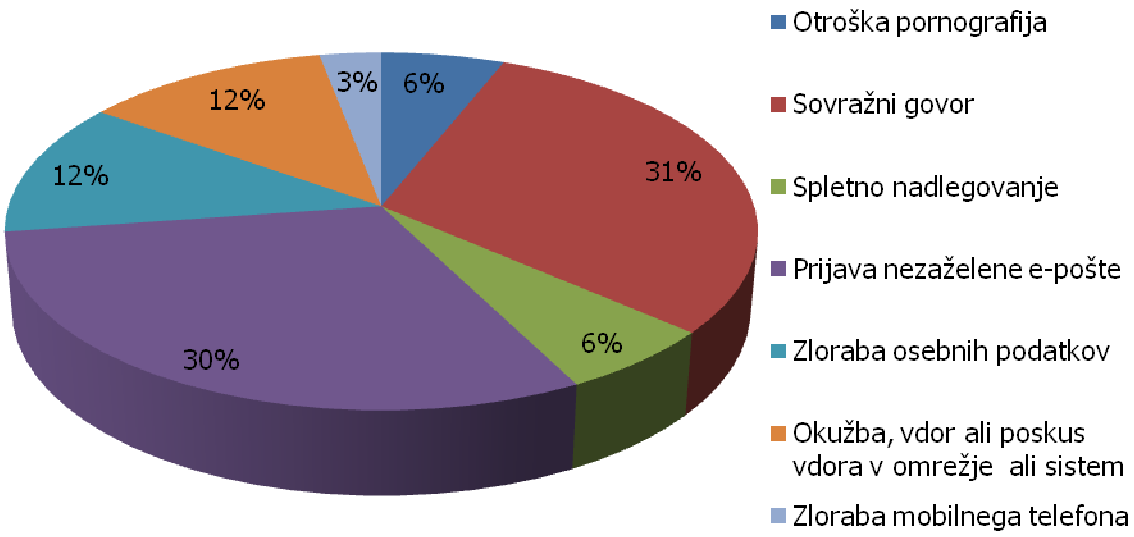
Tabela 9: Razlog prijave neprimerne ali nezakonite vsebine

Možni odgovori	Št. odgovorov	Odstotek
Otroška pornografija	2	6
Sovražni govor	10	31
Spletno nadlegovanje	2	6
Prijava nezaželene e-pošte	10	30
Zloraba osebnih podatkov	4	12
Okužba, vdor ali poskus vdora v omrežje ali sistem	4	12
Zloraba mobilnega telefona	1	3
SKUPAJ	33	100

Vir: lasten

Anketiranci, ki so na vprašanje o prijavi neprimerne ali nezakonite vsebine odgovorili pritrdilno, teh je bilo 17, so morali pri naslednjem vprašanju opredeliti razlog prijave. Iz Tabele 9 je razvidno, da so nekateri izmed anketiranih prijave podali večkrat in z različnimi razlogi, zato je tudi skupno število prijav večje, kar znaša 33 prijav. Če to vzamemo za povprečje, sta na vsakega prijavitelja povprečno dve prijavi.

Grafikon 5: Razlog prijave neprimerne ali nezakonite vsebine (v %)



Vir: lasten, tabela 9

Iz Grafikona 5 je razvidno, da je največ prijav (31%) zaradi sovražnega govora, sledijo prijave nezaželene e-pošte s 30%, zloraba osebnih podatkov in okužba ali vdor v sistem (oba z 12%). Otroško pornografijo in spletno nadlegovanje je prijavilo 6% anketiranih, zlorabo mobilnega telefona pa 3%.

b) Odgovor NE

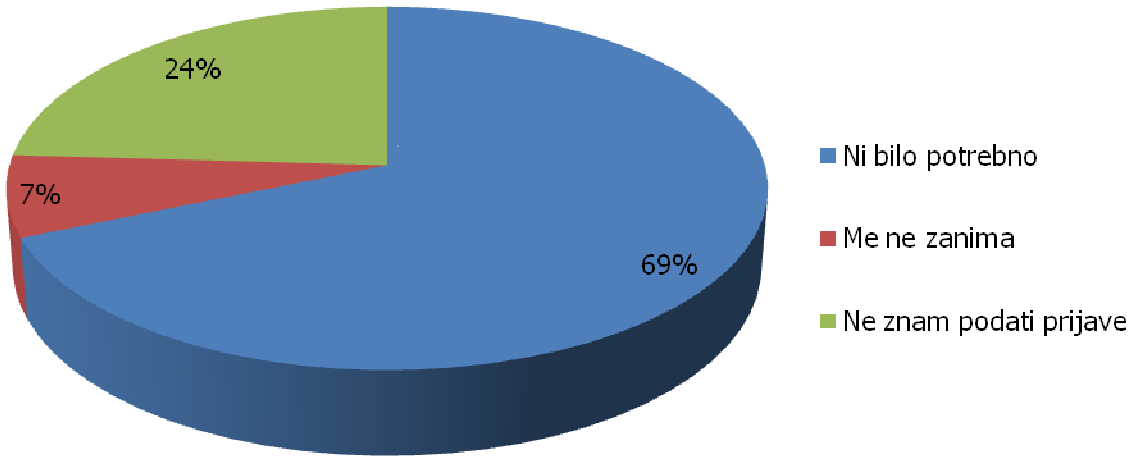
Tabela 10: Razlog neprijave neprimerne ali nezakonite vsebine

Možni odgovori	Št. odgovorov	Odstotek
Ni bilo potrebno	57	69
Me ne zanima	6	7
Ne znam podati prijave	20	24
SKUPAJ	83	100

Vir: lasten

Iz podatkov v Tabeli 10 je razvidno, da je večina od 83-ih anketirancev, kar 69%, navedla kot razlog neprijave dejstvo, da se z neprimerno ali nezakonito vsebino še niso srečali in ukrepanje ni bilo potrebno. 24% anketiranih prijave nezakonite vsebine ne zna ali ne ve komu podati, 7% anketiranih pa prijavljanje nezakonite vsebine tudi ne zanima.

Grafikon 6: Razlog neprijave neprimerne ali nezakonite vsebine (v %)



Vir: lasten, tabela 10

5. Zakonit ali nezakonit spletni govor?

Pri zadnjem vprašanju smo preverjali ali anketirani študentje poznajo razliko med zakonito in nezakonito spletno vsebino in kje postavijo mejo neprimernemu obnašanju. Navedli smo petnajst primerov spletnih komentarjev, ki bi jih našli na javnem forumu.
Po pogovoru s predstavnico Spletnega očesa je izmed naštetih situacij sovražni govor le v dveh primerih. In sicer: *»Peder! Ko te najdem te bom ubil!«*, pod številko 5 in *»Hitlerja bi rabili! Vse cigane pobit!«*, pod številko 10. Vsi ostali komentarji so zakoniti. Opciji »primerno in neprimerno« sta subjektivni, saj se lahko posamezniku zdi neprimerno vse, kar je zanj žaljivo.

Rezultate anketirancev (Tabela 11) smo razdelili v tri skupine. V prvi sta komentarja s sovražnim govorom, ki sta nezakonita. V drugo skupino spadajo komentarji, ki so bili pravilno označeni za zakonite in v tretjo, tisti, ki so bili nepravilno označeni za nezakonite. Za mejo pravilnega odgovora smo vzeli dvo-tretjinsko večino oziroma 67%.

Spletna komentarja (Tabela 11) *»Peder! Ko te najdem te bom ubil!«*, pod številko 5 in *»Hitlerja bi rabili! Vse cigane pobit!«*, pod številko 10 sta nezakonita. Študentje so v veliki večini, prvega s kar 90%, drugega pa s 86% pravilno označili za nezakonita.

Anketiranci so za zakonite pravilno označili (Tabela 11) naslednje komentarje: *»Prasec!«* (št. 1) in *»Tu se govori slovensko, ne bosansko.«* (št. 6) s 70%, z 71% *»Ukradla si mi punco, ti pocestnica!«* (št. 11) in *»Ti bodi tiho, ko imaš samo sedem razredov osnovne šole.«* (št. 12) z 72%. Komentarja pod številko 8 *»Makaronarji pa res ne znajo igrat nogometa.«* in številko 15 *»Hipohonder…«* sta dobila 82% pravilnih odgovorov, komentar pod številko 7 *»Kako si ti butasta!«* pa 87%. Največji odstotek pravilnih odgovorov sta dobila komentarja *»Kakšne kokoši ste!«* (št. 2) z 91% in *»Kako ste bedasti.«* s kar 94%.

V zadnji skupini so komentarji, ki so zakoniti, a so jih študentje označili nepravilno, torej za nezakonite (Tabela 11). Prvi takšen komentar je pod številko 3 *»Hrvati sami hrčki!«*, ki je bil za zakonitega označen z 53%. Naslednja komentarja *»Kaj boš ti govoril, ko si pravi invalid.«* (št. 9) z 49% in *»Jebem ti mater!«* z 41%. Najmanjši odstotek pravilnih odgovorov je dobil komentar *»Ha, ha, ha muslimani zdaj ste ga najebal.«* pod številko 14, ki je dobil le 37% pravilnih odgovorov.

Tabela 11: Zakonitost spletnih komentarjev

Št.	Vrste spletnih komentarjev	Št. odgovorov			Odstotek	
		Primerno	Neprimerno, a ni sovražni govor	Nezakonito, je sovražni govor	Zakonito (Primerno + Neprimerno)	Nezakonito
1	Prasec!	5	65	30	70	30
2	Kakšne kokoši ste!	21	70	9	91	9
3	Hrvati sami hrčki!	8	45	47	53	47
4	Jebem ti mater!	3	39	58	42	58
5	Peder! Ko te najdem, te bom ubil!	0	10	**90**	10	**90**
6	Tu se govori slovensko, ne bosansko.	25	45	30	70	30
7	Kako si ti butasta!	14	73	13	87	13
8	Makaronarji pa res ne znajo igrat nogometa.	21	61	18	82	18
9	Kaj boš ti govoril, ko si pravi invalid.	3	46	51	49	51
10	Hitlerja bi rabili, vse cigane pobit!	2	12	**86**	14	**86**
11	Ukradla si mi punco, ti pocestnica!	12	59	29	71	29
12	Ti bodi tiho, ko imaš samo sedem razredov osnovne šole.	11	61	28	72	28
13	Kako ste bedasti.	24	70	6	94	6
14	Ha, ha, ha muslimani zdaj ste ga najebal.	2	35	63	37	63
15	Hipohonder…	29	53	18	82	18

Vir: lasten

4.3 RAZPRAVA

Pred začetkom izdelave diplomskega dela smo zastavili hipoteze, ki smo jih želeli preveriti z empirično raziskavo. V tem poglavju pa bomo pogledali, ali rezultati ankete hipoteze zavržejo ali potrdijo.

H1: Različne organizacije, ki skrbijo za varnejši internet, ponujajo različne definicije pojma varnost na internetu.
Prva hipoteza je bila preučena v drugem poglavju diplomske naloge. Najširša in najsplošnejša opredelitev varnosti na internetu je podala Mešić (SI-CERT), ki pravi, da je varnost potrebno opredeliti na različnih nivojih, saj lahko govorimo o varnosti strojne opreme, ki procesira naše podatke, o omrežni varnosti, vse do končnega spletnega uporabnika in varnosti njegove spletne identitete. Tanja Šterk (SAFE.SI) navaja, da je pomembno, da se na internetu vedemo odgovorno, da skrbimo za zaščito svoje spletne zasebnosti in objavljamo le tisto, za kar nam je vseeno, če kdorkoli vidi. Ko nekaj objavimo na spletu, tega ne moremo dokončno izbrisati in tako se nezadržno širi med uporabniki. Ta definicija je opredeljena natančneje in se nanaša zgolj na uporabnika, njegovo zaščito, zaščito osebnih in drugih podatkov. Varnost na internetu je z vidika projekta Spletno oko vsako stanje oziroma vedenje posameznika, ki privede do tega, da se posameznik – uporabnik spleta – izogne nevarnostim na spletu (Mihelič, osebna komunikacija, 2012). Tudi zadnja definicija se delno nanaša na uporabnika in na nevarnosti, ki so prisotne v svetu interneta. Lahko bi zaključili, da različne organizacije, ki skrbijo za varnejši internet, resnično ponujajo drugačne definicije pojma varnosti na internetu in s tem smo hipotezo tudi potrdili

H2: Študentje različno razumejo pojem varnost na internetu.
Od sto študentov smo dobili devet različnih opredelitev varnosti (Tabela 3). Nihče ni navedel tri ali več vrst varnosti na internetu, največ eno ali dve. Polovica je varnost opredelila kot varnost osebnih podatkov in varnost pred vdori in virusi (Grafikon 2). Druga polovica je pojmovala varnost kot ohranjanje spletne zasebnosti, varnost dostopa do informacij in uporabe spletnih aplikacij. Nekaj jih tudi meni, da varnosti na internetu ni, neglede na varovalke, ki jih imamo z antivirusnimi programi. Menim, da je hipoteza potrjena, saj se študentje ne zavedajo nevarnosti interneta in tudi sam pojem varnosti ne znajo širše opredeliti.

H3: Večina študentov ne pozna razlike med zakonitostjo in nezakonitostjo spletnih komentarjev.
Če želimo preveriti to hipotezo je najprej potrebna razlaga, kakšna je razlika med zakonito in nezakonito vsebino spletnih komentarjev. Če velja nek komentar za nezakonitega, pomeni, da zagotovo obstaja pravna podlaga za pregon in morebitno obsodbo. Zaradi subjektivnih mnenj je lahko kakšen komentar sporen, a še vedno zakonit, čeprav bralcu neprimeren. Tako so tudi anketiranci po prebiranju spletnih komentarjev morali odločati ali so navedeni komentarji zakoniti ali nezakoniti. Izmed petnajstih komentarjev (Tabela 10), sta bila dva nezakonita in študentje so ju, v veliki večini, tudi označili za takšna. Od

ostalih trinajstih komentarjev, ki so bili zakoniti, jih je bilo devet označenih pravilno, štirje pa napačno. Skupno je bilo torej pravilno označenih več kot dve tretjini komentarjev, zato moramo hipotezo zavrniti.

H4: Večina študentov ne pozna slovenskih in mednarodnih organizacij za varen internet.
Internetna kriminaliteta je v današnjem času zelo razširjena, pred njo nas, kar se da učinkovito, želijo zaščititi različne organizacije za varnost na internetu. Seveda pa je pomembno, da vemo h komu pristopiti, ko potrebujemo pomoč. Žal so rezultati ankete pokazali (Grafikon 4), da polovica študentov ne pozna projekta Spletno oko, več kot dve tretjini anketiranih ne ve za delovanje organizacij in projektov SAFE-SI, SI-CERT in Varnost na spletu .si. Pri poznavanju mednarodnih organizacij (Grafikon 5), so rezultati še slabši, saj 86% študentov ne pozna naštetih organizacij – INHOPE, INSAFE, eNASCO in Childnet. Iz danih rezultatov lahko potrdimo našo hipotezo, saj anketirani študentje resnično ne poznajo slovenskih in mednarodnih organizacij za varen internet.

H5: Študentje na spletnih forumih praviloma ne prijavljajo nezakonite vsebine zaradi nepoznavanja sistema delovanja.
Organizacije, projekti, Facebook skupine in drugi akterji, ki nudijo pomoč pri varovanju pred nezakonito spletno vsebino so nemočni, če jim pri tem ne pomagajo tudi uporabniki sami. Z zadnjo hipotezo smo želeli preveriti, ali študentje ukrepajo, ko zasledijo domnevno nezakonito vsebino in kakšni so razlogi za neukrepanje. Od sto študentov jih je sedemnajst že prijavilo nezakonito vsebino (Tabela 17), ko so prišli v stik z njo. Če sklepamo (Hipoteza 3), da študentje poznajo razliko med zakonito in nezakonito spletno vsebino, jih 57 trdi (Tabela 9), da prijave še ni bilo potrebno podati, bi jo pa, če bi jo zasledili. Ostalih 26 anketirancev pa ne saj jih 6 ne zanima, 20 pa ne ve kako podati prijavo. Če povzamemo, lahko rečemo, da le petina ali 20% študentov prijave nezakonite vsebine ne ve kako ali komu bi jo podalo, zato hipotezo zavrnemo.

5 ZAKLJUČEK

Tudi v virtualnem svetu obstajajo zakoni in pravila lepega vedenja. Če jih ne upoštevamo smo lahko kaznovani, hujše kršitve pa nas pripeljejo tudi v zapor. Za varnost na spletu lahko največ naredimo sami, seveda nam pri tem pomagajo tudi razne spletne organizacije in vsaka od njih skrbi za varnost na različnem nivoju.

Varnost na internetu je zelo širok pojem, ki ga ne moremo opisati le z enim stavkom. Če pričnemo na začetku, še preden se vklopimo na internet, moramo zagotoviti varnost strojne opreme, ki procesira naše podatke in omrežno varnost, ki skrbi za nemoten dostop do interneta. Še večjo previdnost moramo nameniti času, ko smo dejansko na internetu. Varnostno tveganje se poveča, če brskamo po nepreverjenih spletnih straneh, prenašamo na računalnik nepreverjene datoteke ali kako drugače izpostavimo naš informacijski sistem internetnemu kriminalu. Varnost se nanaša tudi na nezakonito spletno vsebino, ki jo zasledimo na internetu. Naša dolžnost je, da sovražni govor, otroško pornografijo ali drugo nezakonito vsebino prijavimo spletnim organizacijam.

Prva v vrsti slovenskih organizacij, ki skrbijo za varnost na internetu je SAFE-SI, ki deluje kot slovenska nacionalna točka osveščanja otrok, najstnikov, staršev in učiteljev. Njihova glavna naloga je informiranje uporabnikov interneta, kako se zaščititi pred nevarnostmi, ki jih prinašata uporaba interneta in mobilnih telefonov. Za večjo prepoznavnost in osveščenost uporabnikov vsako leto pripravijo različne aktivnosti in orodja osveščanja, kot so izobraževalna gradiva, kampanje proti spletnemu nadlegovanju, mednarodni dogodek Dan varne rabe interneta, ki so ga razširili na celoten mesec februar ter različne diskusijske skupine za mlade.

Slovenska spletna prijavna točka se imenuje Spletno oko, pri kateri lahko podamo anonimno prijavo otroške pornografije in sovražnega govora na internetu. Prijavna točka Spletno oko je del širšega evropskega združenja za učinkovito zmanjšanje nezakonitih vsebin na internetu, ki so del krovne organizacije INHOPE. Pomembna značilnost projekta je tudi sodelovanje s policijo in Vrhovnim državnim tožilstvom Slovenije.

Pri varnosti na internetu nam v Sloveniji nudi pomoč tudi center za posredovanje pri internetnih incidentih imenovan SI-CERT. Prednostno poslanstvo centra je odzivanje na omrežne incidente in osveščanje spletnih uporabnikov o spletnih tveganjih, kot so kraja identitete, spletne goljufije, spam, okužbe in vdori v računalniške sisteme. SI-CERT je razvil sodelovanje tudi z drugimi organizacijami, ki skrbijo za varnejši internet – Arnes, SAFE-SI, SISPA, FIRST, ENISA in druge.

V evropskem prostoru skrbi za promocijo varne in odgovorne rabe interneta in mobilnih tehnologij organizacija INSAFE. Je krovna organizacija vsem nacionalnim točkam osveščanja, v Sloveniji se ta imenuje SAFE-SI. Osredotočena je predvsem na mlade, ponuja pa pomoč in informacije tudi otrokom, staršem in učiteljem. Njihova želja je

predstaviti uporabnikom interneta in drugih spletnih tehnologij vsako izkušnjo kot pozitivno in varno.

Zadnja izmed organizacij je INHOPE, ki predstavlja mednarodno združenje spletnih prijavnih točk. Njeno poslanstvo je usklajevanje mreže internetnih prijavnih točk po vsem svetu in podpora pri odzivanju na prijave o nezakonitih vsebinah, kot sta otroška pornografija in sovražni govor. Tako kot v Sloveniji s policijo sodeluje Spletno oko, tako v mednarodnem okviru INHOPE sodeluje z Interpolom. V okviru združenja INHOPE je trenutno v omrežju 42 prijavnih točk v sedemintridesetih različnih državah po vsem svetu.

V nadaljevanju smo z anketo želeli analizirati poznavanje področja varnosti med študenti. Najprej smo želeli pridobiti vpogled v razumevanje pojma varnosti med študenti. Rezultati so pokazali, da se študentje ne zavedajo nevarnosti interneta, saj pojem varnosti v večini opredeljujejo enoznačno, kot varnost osebnih podatkov in ohranjanje spletne zasebnosti ali kot varnost pred vdori in virusi ter varno uporabo spletnih aplikacij. Prav tako smo ugotovili, da ne poznajo slovenskih in mednarodnih organizacij, ki skrbijo za varen internet, kar je zaskrbljujoče. Z internetno kriminaliteto se je potrebno spoznati preden je prepozno, da se lahko pravilno zavarujemo in ne potem, ko je škoda že bila narejena. Same organizacije bi torej morale delati več na področju promocije in seznanjanja uporabnikov o spletnih nevarnostih.

Pozitivno je, da študentje poznajo razliko med zakonito, neprimerno in nezakonito spletno vsebino. Zanimivo pa, da so nekatere zakonite komentarje smatrali tudi za nezakonite. Lahko bi sklepali, da je Kazenski zakonik premalo občutljiv za nekatere spletne komentarje in vsebine. Preseneča tudi dejstvo, da bi več kot dve tretjini študentov podalo prijavo o domnevno nezakoniti vsebini, če bi na spletu prišli v stik z njo. Če je temu tako, se lahko med brskanjem po spletu resnično počutimo varnejše, saj skrbimo drug za drugega.

Nadaljnje raziskave bi lahko bile usmerjene na celotno populacijo in njeno zavedanje varnosti na internetu. Prav tako bi lahko razširili znanje in dodali opise še drugih organizacij in projektov za varen internet. Lahko bi se posvetili zakonodaji, ki ureja (ne)zakonitost spletnih vsebin in njeno »prizanesljivost« do spletnih komentarjev. Zanimivo bi bilo vpeljati možnost direktne prijave, preko spletnega obrazca, domnevno nezakonite vsebine, tako kot to sedaj omogoča Spletno oko na nekaterih forumih. S tem bi se lahko posvetili vprašanju, zakaj nekateri popularni javni forumi ne uporabljajo možnosti spletnega obrazca za prijavo sovražnega govora med komentarji.

Zaključujem z željo in namenom vzpodbuditi zavedanje vsakega uporabnika spleta, da je del širše virtualne skupnosti, ki ima tako svetlo kot temno plat. Z osveščenostjo o nezakonitih spletnih vsebinah in njihovo preprečitvijo lahko le-ta postane varnejša, svetlejša.

LITERATURA IN VIRI

LITERATURA

1. BERČIČ, Boštjan, BOJANEC Anton, KRKOČ Peter, MRHAR Peter, PATRU Primož, ŠINIGOJ Aleksander, VALENČIČ Iztok (2003). *Ukrepi v primeru informacijskih nesreč.* Inštitut IZIV, Šempeter pri Gorici.
2. BOGATAJ, Jančič Maja, KLEMENČIČ Goran, MAKAROVIČ Boštjan, TIČAR Klemen, TOPLIŠEK Janez (2007). *Pravni vodnik po internetu.* GV Založba, Ljubljana.
3. BORŠTNAR, Vesna (2011). *Otroška pornografija v Sloveniji*. Pravna fakulteta, Ljubljana.
4. ERJAVEC, Jožica (2009). *Otroška pornografija na spletu in boj zoper njo*. Fakulteta za varnostne vede, Ljubljana.
5. KJAER, Torben (2003). *Začnimo z internetom: naj ostane preprosto!* Flamingo, Šempeter pri Gorici.
6. KLANJŠEK, Bojana (2012). *Varnost uporabe Facebooka med mladimi.* Fakulteta za družbene vede, Ljubljana.
7. KOVAČIČ, Matej (2009). *Deskanje po varnih vodah: priročnik*. Fakulteta za družbene vede, Center za metodologijo in informatiko, Ljubljana.
8. KOZOLE, Aleš (2012). *Načini varovanja identitete v spletu.* Fakulteta za varnostne vede, Ljubljana.
9. KREVL, Matej (2006). *Osnovni koncepti varnega obnašanja na internetu*. Fakulteta za računalništvo in informatiko, Ljubljana.
10. LJUBISAVLJEVIĆ, Milomirka (2006). *Varnost elektronske izmenjave podatkov.* Visoka šola za upravljanje in poslovanje, Novo mesto.
11. MARTINIS, Klemen (2012). *Vdor in neupravičen vstop v informacijski sistem.* Fakulteta za varnostne vede, Ljubljana.
12. OSTANEK, Bojan (2007). *Neupravičen vstop v informacijski sistem in vdor v informacijski sistem kot kaznivi dejanji.* Fakulteta za varnostne vede, Ljubljana.
13. PAGON, Milan, JANJAC Ivica, BELIČ Igor (1997). *Modri internet.* Gnosis-Quatro, Ljubljana.
14. PRAH, Benjamin (2012). *Primerjalna analiza varnosti elektronskega poslovanja v slovenskih bankah.* Ekonomsko-poslovna fakulteta, Maribor.
15. ŠALAMON, Brane (1998). *Internet za otroke in družino.* Moj mikro, Ljubljana.
16. ŠKARLIN, Urška (2011). *Varnost elektronskega davčnega poslovanja v Sloveniji.* Fakulteta za upravo, Ljubljana.
17. URBANIJA, Aljaž (2012). *Varnost in zasebnost spletnih brskalnikov.* Fakulteta za elektrotehniko, Ljubljana.
18. VERBIČ, Andreja (2012). *Varnostni mehanizmi elektronskega poslovanja.* Fakulteta za varnostne vede, Ljubljana.
19. ZVER, Denis (2011). *Varnost in zasebnost v socialnih omrežjih.* Fakulteta za varnostne vede, Ljubljana.
20. ŽIVKOVIČ, Sara (2008). *Računalniška tehnologija v očeh mladih uporabnikov: analiza spletnega mesta safe.si*. Fakulteta za družbene vede, Ljubljana.

INTERNETNI VIRI

1. INHOPE (2010). *Annual report*. Dostopno 18. 4. 2012 na: inhope.org/Libraries/Annual_reports/2009_INHOPE_Annual_Report.sflb.ashx?download=true.
2. INHOPE (2011). *Annual report*. Dostopno 18. 4. 2012 na: inhope.org/Libraries/Annual_reports/2010_Annual_report.sflb.ashx?download=true
3. INHOPE (2012). *About INHOPE*. Dostopno 18. 4. 2012 na: http://inhope.org/gns/about-us/about-inhope.aspx
4. INSAFE (2012). *Online safety.* Dostopno 13. 4. 2012 na: http://www.saferinternet.org/web/guest/safety-issues.
5. O'DELL, Jolie (2011). *How big is the web and how fast is it growing?* Dostopno: 9. 6. 2012 na: http://mashable.com/2011/06/19/how-many-websites/#17199How-Big-Is-the-Web
6. Spletno oko (2009). *Poročilo 2007 – 2009*. Dostopno 20. 4. 2012 na: https://www.spletno-oko.si/uploadi/editor/1239375991spletno_oko_slo.pdf.
7. Spletno oko (2012). *Pogosta vprašanja – FAQ.* Dostopno 26. 8. 2012 na: https://www.spletno-oko.si/c/780/FAQ/.
8. Varni na internetu (2011). *Hitri vodnik abc varnosti na spletu*. Dostopno 14. 4. 2012 na: http://www.varninainternetu.si/content/uploads/2011/11/Varni_hitriVodnik_splet_kakovostna.pdf.

PREDPISI

1. (1994). Kazenski zakonik Republike Slovenije (KZ). Ur. list RS, št. 23/99, 60/99, 226/95, 40/04, 95/04, 37/05, 17/06, 55/08, 89/08, 5/09.

PRILOGE

Priloga 1: Intervju s SAFE-SI

Po elektronski pošti smo izvedli tri intervjuje s slovenskimi organizacijami SAFE-SI, Spletno oko in SI-CERT ter enega z mednarodno organizacijo INHOPE. Vse naštete organizacije skrbijo za varnost na internetu. Vprašanja smo razdelili v tri sklope. V prvem smo želeli pridobiti splošne informacije o organizacijah, v drugem kako posamezna organizacija opredeljuje varnost na internetu in ali sodeluje z drugimi organizacijami, v zadnjem pa smo želeli izvedeti ali zbirajo podatke o prijavah in kakšni so zbrani podatki.

Splošne informacije

1. *Najprej Vas, prosim, da se predstavite in poveste, kakšno je vaše mesto pri projektu SAFE-SI?*

Sem Tanja Šterk in že od leta 2005, ko smo v okviru Fakultete za družbene vede pričeli izvajati ta projekt, le-tega koordiniram.

2. *Na kratko, prosim, podajte nekaj osnovnih informacij o projektu.*

SAFE-SI ni organizacija, temveč je projekt v okviru Fakultete za družbene vede v Ljubljani, ki ga izvajamo v sodelovanju z javnim zavodom ARNES, Zvezo prijateljev mladine Slovenije ter Zavodom MISSS (Mladinsko informativno svetovalno središče Slovenije), financirata pa ga Generalni direktorat Connect pri Evropski komisiji in Ministrstvo za izobraževanje, znanost, kulturo in šport, že od leta 2007.
SAFE-SI predstavlja eno iz med treh komponent Centra za varnejši internet, preostali dve sta še SPLETNO OKO - točka za anonimno prijavo nelegalnih spletnih vsebin; otroške pornografije in sovražnega govora in TOM TELEFON - telefonska linija za pomoč mladim in njihovim staršem, ki se znajdejo v težavah, povezanih z uporabo interneta.

3. *Kakšen je vaš glavni cilj – poslanstvo?*

Naš glavni cilj je promocija varne in odgovorne rabe interneta ter mobilnih tehnologij med izbranimi ciljnimi skupinami otrok, najstnikov, staršev in učiteljev. Z različnimi aktivnostmi, ki jih izvajamo, želimo dvigniti stopnjo ozaveščenosti o teh temah. Ključne aktivnosti pri projektu so tako sledeče:

- vzdrževanje osrednje spletne strani (www.safe.si) kot baze znanja in pomoči za otroke, najstnike, starše in učitelje;
- izobraževanje učiteljev in drugih strokovnih delavcev za poučevanje in prenos vsebin varne rabe interneta;
- priprava in distribucija izobraževalnih tiskanih in spletnih gradiv (zloženk, brošur, didaktičnih iger ipd.) za vse ciljne skupine;
- promocija projekta skozi socialna omrežja – predvsem Facebook, kjer imamo vzpostavljeni dve skupini - za starše SAFE-SI (www.facebook.com/safe.si) in za najstnike Deskam varno (www.facebook.com/deskamvarno);
- izvedba delavnic za otroke in mladostnike, predavanj za starše, natečajev za šole;
- zagotavljanje medijske prisotnosti, priprava člankov in prispevkov za različne medije;

- organizacija in izvedba dogodkov in aktivnosti ob svetovnem dnevu varne rabe interneta (vsako leto drugi torek v februarju).

Varnost na internetu

4. Kako bi opredelili pojem »varnost« na internetu?

Varnost na internetu je zelo širok pojem in bi ga zelo težko opredelili le v enem stavku. Pomembno je, da se na internetu vedemo odgovorno, da skrbimo za zaščito svoje spletne zasebnosti, ter da na spletu objavljamo le tisto, za kar nam je vseeno, če kdorkoli vidi. Ko nekaj objavimo na spletu, ne moremo tega dokončno izbrisati in tako se lahko nezadržno širi med uporabniki.

5. Ali sodelujete z drugimi slovenskimi in tujimi organizacijami, ki skrbijo za varnost na internetu? (Kot so npr.: Spletno oko, Varni na internetu, SI-CERT, INSAFE, INHOPE,…)

SAFE-SI kot samostojna komponenta in kot del Centra za varnejši internet sodeluje s številnimi domačimi in tujimi organizacijami s tega področja. Pomembne so skupne aktivnosti, izmenjava medsebojnih mnenj in izkušenj. Če nastopamo skupaj, lahko dosežemo večjo prepoznavnost te tematike in v končni fazi prispevamo k večji zaščiti otrok, pa tudi vseh ostalih uporabnikov interneta.

6. Ali vaše delovanje zahteva sodelovanje z organi pregona?

SAFE-SI z organi pregona neposredno ne sodeluje, ker je to naloga Spletnega očesa.

7. Menite, da so študentje dovolj osveščeni o varni rabi interneta? Zakaj ja/ne?

Podam lahko le svoje, laično mnenje, ker se neposredno s študentsko populacijo v okviru projekta ne ukvarjamo. Zagotovo se študentje zavedajo določenih pasti uporabe interneta, ampak še vedno se, tako kot ostali uporabniki, premalo zavedajo pasti razkrivanja svoje zasebnosti in intimne na spletu.

Statistika

8. Ali spremljate število prijav, ki jih dobite mesečno/letno?

Ne. Prijave podrobneje spremljajo pri Spletnem očesu.

9. Ali lahko ocenite, v kateri starostni skupini so ljudje, ki se največkrat obrnejo po vašo pomoč? (Otroci, mladostniki, študentje, starši, stari starši.)

Na SAFE-SI se, na nas s svojimi vprašanji in težavami, največkrat obrnejo učitelji, kadar se v šoli pojavijo kakšne resne težave v povezavi z uporabo interneta oz. mobilnih telefonov. Žal je tako, da se šole na nas največkrat obrnejo šele, ko se je določena težava že zgodila, saj bi lahko skozi naše delavnice, ki jih izvajamo za učence in predavanja za starše, posredovali znanja in informacije, kako preprečiti, da bi se zloraba sploh zgodila oz. ko se zgodi, kako najhitreje in najučinkoviteje ukrepati.

Največ vprašanj je v povezavi z zlorabami na Facebooku, npr. izdelava lažnih profilov, ter primerov žaljenja in nadlegovanja. Zanimivo je, da se otroci oz. najstniki res le izjemoma obrnejo na nas s kakšno težavo. Očitno svoje težave bolj ali manj uspešno raje rešujejo v družbi svojih vrstnikov.

Priloga 2: Intervju s Spletno oko

Splošne informacije

1. *Najprej Vas, prosim, da se predstavite in poveste, kakšno je vaše mesto v organizaciji Spletno oko?*

Sem Lija Mihelič, po izobrazbi univerzitetna diplomirana varstvoslovka. Po diplomi leta 2008 sem svojo poklicno pot začela na Fakulteti za družbene vede, sprva kot asistentka koordinatorja prijavne točke Spletno oko, od marca 2009 dalje pa opravljam delo koordinatorja prijavne točke Spletno oko.

2. *Na kratko, prosim, podajte nekaj osnovnih informacij o organizaciji.*

Spletno oko je prijavna točka, ki predstavlja eno izmed treh komponent Centra za varnejši internet Slovenija. Deluje od marca 2007, in sicer v okviru programa Evropske komisije Varnejši internet (Safer Internet Programme), torej gre za projekt, ki je sofinanciran s strani Evropske komisije. Spletno oko deluje na Univerzi v Ljubljani, na Fakulteti za družbene vede, v partnerstvu z ARNES-om, Zvezo prijateljev mladine, in Mladinskim informacijskim središčem Slovenije. Delovanje Spletnega očesa je financirano s strani Generalnega direktorata za informacijsko družbo in medije pri Evropski komisiji in Ministrstva za izobraževanje, znanost, kulturo in šport.
Vsebinsko na prijavni točki delujemo štirje ljudje, od teh sta dva pregledovalca prijav. Imamo pa seveda v okviru Fakultete na voljo še druge ljudi, ki nam pomagajo, ko je to potrebno.

3. *Kakšen je vaš glavni cilj – poslanstvo?*

Naše glavno poslanstvo je zmanjšanje posnetkov spolnih zlorab otrok in sovražnega govora na spletu. Prioriteta so predvsem posnetki spolnih zlorab otrok.

Varnost na internetu

4. *Kako bi opredelili pojem »varnost« na internetu?*

Besedna zveza »varnost na internetu« je tako obsežna, da je zelo težko podati neko splošno definicijo. Tudi sicer se z varnostjo na internetu kot tako v okviru preventive ukvarja predvsem točka osveščanja safe.si, medtem ko Spletno oko nastopi svojo vlogo takrat, ko smo že soočeni z nevarnostjo na internetu (torej ne več 'varnostjo' na internetu). Sama bi tako iz strokovnega vidika in vidika projekta, ki obravnava predvsem problematiko nezakonitih vsebin na spletu, veliko lažje opredelila nevarnost na internetu.
Varnost na internetu pa je z vidika projekta Spletno oko vsako stanje oziroma vedenje posameznika, ki privede do tega, da se posameznik – uporabnik spleta - izogne nevarnostim na spletu. Dobra opredelitev se mi zdi tudi sledeča: Internetna varnost ali varnost na spletu je varnost ljudi in njihovih informacij pri uporabi interneta (Wikipedia).

5. *Ali sodelujete z drugimi slovenskimi in tujimi organizacijami, ki skrbijo za varnost na internetu? (Kot so npr.: Safe.si, Varni na internetu, SI-CERT, INSAFE, INHOPE,…)*

Spletno oko je v stalnem tesnem sodelovanju s policijo, kateri posredujemo prijave, ki jih ocenimo kot domnevno nezakonite. Spletno oko pri obravnavi prijav sodeluje tudi z

drugimi slovenskimi organizacijami predvsem v obliki posredovanja prijav, ki jih obravnava določena organizacija (v taki obliki največ sodelujemo s SI-CERT-om).

Na drugi strani je Safe.si del Centra za varnejši internet (tako kot Spletno oko), tako da je sodelovanje z njimi še posebej intenzivno, predvsem na področju osveščanja o prijavni točki in problematiki nezakonitih vsebin na spletu.

Spletno oko je tudi član INHOPE organizacije, kar pomeni, da sodelujemo tudi z njimi in z ostalimi prijavnimi točkami, ki so članice INHOPE organizacije, in sicer predvsem v obliki posredovanja prijav posnetkov spolnih zlorab otrok na strežnikih v tujih državah. Poleg tega sodelujemo tudi z drugimi nacionalnimi vladnimi in nevladnimi organizacijami, ko se za določeno sodelovanje pojavi priložnost in potreba.

6. Ali vaše delovanje zahteva sodelovanje z organi pregona?
Da. Naše sodelovanje z organi pregona je predvsem v obliki posredovanja prijav, pa tudi v obliki organiziranja raznih strokovnih dogodkov, oblikovanja smernic dela in izobraževanja.

7. Menite, da so študentje dovolj osveščeni o varni rabi interneta? Zakaj ja/ne?
Safe.si, točka osveščanja o varni rabi interneta, intenzivno deluje na področju osveščanja o varni rabi interneta tako osnovnošolcev kot tudi srednješolcev. Informacij o tej problematiki je tako po mojem mnenju na voljo dovolj, kako resno jih kdo vzame 'za svoje', pa je seveda odvisno od vsakega posameznika.

Statistika

8. Ali spremljate število prijav, ki jih dobite mesečno/letno?
Da.

9. Menite, da število prijav narašča ali upada?
Število prijav narašča.

10. Ali lahko ocenite, v kateri starostni skupini so ljudje, ki se največkrat obrnejo po vašo pomoč? (Otroci, mladostniki, študentje, starši, stari starši.)
Tega ne moremo oceniti, ker teh informacij ne zbiramo.

Priloga 3: Intervju s SI-CERT

Splošne informacije

1. *Najprej Vas, prosim, da se predstavite in poveste, kakšno je vaše mesto v organizaciji SI-CERT?*

Jasmina Mešić, zaposlena v SI-CERT, koordinatorka nacionalnega programa ozaveščanja o informacijski varnosti - Varni na internetu.

2. *Na kratko, prosim, podajte nekaj osnovnih informacij o organizaciji.*

SI-CERT (Slovenian Computer Emergency Response Team) je center za posredovanje pri internetnih incidentih, ki koordinira obveščanje in reševanje varnostnih problemov v računalniških omrežjih v Sloveniji. Na podlagi sklepa Vlade Republike Slovenije št. 38600-3/2009/21 z dne 8.4.2010, SI-CERT opravlja tudi naloge centra za obravnavo incidentov v sistemih državne in javne uprave.
Po nekajletnih dogovarjanjih je Arnes spomladi 2010 na pobudo Direktorata za informacijsko družbo Ministrstva za visoko šolstvo, znanost in tehnologijo pričel z dejavnostmi programa osveščanja, ki poteka pod imenom *Varni na internetu*.
SI-CERT je bil ustanovljen leta 1995 in deluje v okviru Arnesa (Akademske in raziskovalne mreže Slovenije), vendar sprejema prijave varnostnih incidentov za vsa računalniška omrežja v Sloveniji.
Redno zaposlene so 4 osebe, vodja SI-CERT je Gorazd Božič.

3. *Kakšen je vaš glavni cilj – poslanstvo?*

Glavni cilj je odzivanje na omrežne incidente in osveščanje spletnih uporabnikov o spletnih tveganjih.
SI-CERT obravnava *varnostne incidente*, tj. obvestila o zlorabah, okužbah in vdorih v računalniške sisteme. Predstavlja kontaktno točko, ki opravlja posredniško in svetovalno vlogo.
Poleg odzivanja na varnostne incidente je velikega pomena tudi osveščanje uporabnikov omrežja o tveganjih in s tem povezanimi ukrepi, ki zmanjšajo verjetnost neljubega dogodka.
Program osveščanja *Varni na internetu* naslavlja dve ciljni skupini: odrasle, domače uporabnike in mala podjetja oz. samostojne podjetnike. Prvim nudi nasvete s področja spletnega bančništva in spletnih nakupov, drugim pa pomaga pri vprašanjih, ki so povezana z IT vidikom poslovanja podjetja. Obema skupinama pa je predstavljen sklop spletnih goljufij in prevar.

Varnost na internetu

4. *Kako bi opredelili pojem »varnost« na internetu?*

Tu gre za zelo širok pojem, ki zajema različne oblike varnosti na različnih nivojih: lahko govorimo o varnosti strojne opreme, ki procesira naše podatke, o omrežni varnosti, vse do končnega spletnega uporabnika in varnosti njegove spletne identitete. Lahko pa posplošimo, saj je ravno spletni uporabnik ponavadi najbolj kritičen del celotne verige.

5. *Ali sodelujete z drugimi slovenskimi in tujimi organizacijami, ki skrbijo za varnost na internetu?*

a) Sodelovanje ARNES in SAFE-SI

Arnes je že od leta 1999 (takrat na pobudo MŠŠ), v okviru mednarodne projektne koordinacije European Schoolnet, partner v projektih Evropske komisije iz akcijskega načrta *Varnejši internet (Safer Internet Action Plan – Safer Internet Plus)*, ki promovira varnejšo uporabo interneta za otroke in mladostnike. Gre za koordinirane aktivnosti v vseh državah članicah EU, sofinancira ga Evropska komisija (Grant Agreement No SI-2009-SIC-123905), v Sloveniji projekte podpira Direktorat za informacijsko družbo na Ministrstvu za visoko šolstvo, znanost in tehnologijo. *V okviru tega akcijskega načrta Arnes od leta 2005 aktivno sooblikuje SAFE-SI, nacionalni center osveščanja o varnejši rabi interneta.*

Mednarodno sodelovanje pa poteka skozi *omrežje INSAFE*, ki povezuje nacionalne centre osveščanja.

b) SI-CERT sodelovanje s slovenskimi organizacijami

SI-CERT lahko deluje le ob dobri povezanosti z različnimi deležniki na področju omrežne in informacijske varnosti. Ob obravnavi sodelujemo z internetnimi operaterji (individualno in v okviru združenja Sispa) in ponudniki storitev na spletu, kot tudi z Agencijo za pošto in elektronske komunikacije. V letu 2010 smo na sestankih pri Informacijskem pooblaščencu RS obravnavali vprašanja s področja osebnih podatkov, prometnih podatkov in omrežne komunikacije s stališča Zakona o varstvu osebnih podatkov in Zakona o elektronskih komunikacijah. Z Zvezo potrošnikov Slovenije (oz. njihovim Evropskim potrošniškim centrom) smo sodelovali pri posameznih incidentih lažnih nakupov ali prodaje.

c) Sodelovanje SI-CERT v mednarodnih organizacijah

SI-CERT je aktiven član Terenine delovne skupine evropskih centrov za posredovanje pri internetnih incidentih, TF-CSIRT in svetovnega združenja FIRST (Forum of Incident Response and Security Teams). TF-CSIRT združuje vse evropske varnostne centre, tako iz raziskovalno-izobraževalne kot tudi iz komercialne in vladne sfere. Prav tako je SI-CERT član evropske agencije ENISA (European Networking and Information Security Agency), program Varni na internetu pa bo zastopal Slovenijo v prihajajočem »mesecu spletne varnosti«, ki ga oktobra organizira ENISA.

6. Ali vaše delovanje zahteva sodelovanje z organi pregona?

Naše delovanje je posredno seveda povezano tudi z organi pregona. Sicer tu ne gre za neke formalne postopke, ampak bolj za neformalno sodelovanje: organom pregona prijavljamo hujše lokalne incidente, nanje napotujemo žrtve zlorab, včasih se različni organi pregona na nas obrnejo glede kakšnega tehničnega vprašanja, z našimi predavanji pa aktivno sodelujemo tudi pri njihovem izobraževanju glede informacijske varnosti.

7. Menite, da so študentje dovolj osveščeni o varni rabi interneta? Zakaj ja/ne?

Ker so prijave, ki jih prejemamo anonimne in nimamo vpogleda v demografijo, zelo težko ocenjujemo, kako osveščena je študentska populacija v Sloveniji (prav tako nismo seznanjeni, da bi bila opravljena kakšna bolj poglobljena raziskava pri tej populaciji). Čisto splošna ocena bi bila, da je ta populacija bolj računalniško pismena (uporablja storitve e-bančništva, e-nakupovanja, storitve e-uprave) vendar se premalo zaveda pomena varstva osebne identitete in osebnih podatkov na družabnih omrežjih.

Statistika

8. Ali spremljate število prijav, ki jih dobite mesečno/letno?

Da.

9. Menite, da število prijav narašča ali upada?

Vse dosedanje letne statistike kažejo, da število prijav incidentov narašča. Več statističnih podatkov je na voljo v letnih poročilih:

10. Ali lahko ocenite, v kateri starostni skupini so ljudje, ki se največkrat obrnejo po vašo pomoč? (Otroci, mladostniki, študentje, starši, stari starši.)

Vpogleda v demografijo nimamo, saj so vse prijave anonimne oz. ne zahtevamo podatkov o prijaviteljih. Gotovo prevladujejo odrasli spletni uporabniki (približna ocena bi bila nad 24 let), ki že uporabljajo storitve spletnega nakupovanja in bančništva.

Priloga 4: Intervju z INHOPE

General information

1. *First, please, introduce yourself and explain what your work assignment in organization is.*

My name is Denton Howard and I am Training & Services Coordinator for INHOPE.

2. *Please, briefly provide some background information on the organization.*

Founded in 1999 with 6 Hotlines that came together to try and work against online Child Sexual Abuse Material (including child pornography).
Hotlines offer the public a way of anonymously reporting Internet material including child sexual abuse material they suspect to be illegal.
INHOPE now has 42 Hotlines. INHOPE is the coordinator of Hotlines – it does not run Hotlines.

3. *What is your main goal - mission?*

To support and enhance the performance of Internet Hotlines around the World; ensuring swift action is taken in responding to reports of illegal content making the internet a safer place.

Safety on the Internet

4. *How would you define the term »safety« on the Internet?*

INHOPE Hotlines deal with reports of potential illegal content as in child abuse and hate speech.

5. *Do you collaborate with other foreign organizations, which provide safety on the Internet?*

Yes. The most of our time we work with INSAFE, they are our consortium partner.

6. *Does your work operation require cooperation with law enforcement authorities?*

Yes.

7. *Do you think that students are sufficiently informed about the safe use of the Internet? Why yes / no?*

This relates to awareness and I would refer you to INSAFE on this issue.

Statistics

8. *Do you monitor the number of reports you get (monthly / yearly)?*

We coordinate real-time statistics via an online system that Hotline participates in. These are not public information. The accumulated information is published via the INHOPE website.

9. *Do you think that the number of reports is growing or declining?*

The answer to that is yes it is, but that is due to many factors because there are more Hotlines, a greater awareness of Hotlines and there are more people accessing the internet, thus there will be more reports.

10. *Can you estimate in which age group are people who usually turn to for your help? (Children, youth, students, parents, grandparents.)*

We do not collect that information.

Priloga 5: Anketni vprašalnik

ANKETNI VPRAŠALNIK

Sem Lucija Jelen, študentka na Fakulteti za upravo, Ljubljana. V okviru diplomske naloge preučujem poznavanje varnosti na internetu med študenti. V ta namen sem izdelala vprašalnik, ki bo izhodišče empiričnega dela. Podatki, ki jih bom pridobila z anketnim vprašalnikom bodo namenjeni izključno le izdelavi naloge.

Navodila: Pri večini vprašanj obkrožite ali dopišite le EN odgovor.

SPOL: M Ž
STAROST: _____
ŠTUDENT: DA NE *Anketa je namenjena izključno študentski populaciji

Varnost na internetu

1. Kako bi opredelili pojem »varnost« na internetu?
2. Z 1 do 10 označite, kaj je najpomembneje za varnostjo na internetu?
   (1 je najmanj pomembno in 10 najbolj pomembno)
   - varnost priključitve na omrežje
   - brezžična varnost
   - varnost pred vdori in okužbo operacijskega sistema
   - varnost dostopa do virov informacij
   - varnost prenosa podatkov
   - varnost osebnih podatkov
   - varna uporaba spletnih aplikacij (spletno bančništvo, spletno nakupovanje)
   - ohranjanje spletne zasebnosti na socialnih omrežjih
   - varnost pred neprimerno in nezakonito vsebino (sovražni govor, otroška pornografija, nezaželena e-pošta)
   - varna uporaba mobilnega telefona pri spletni uporabi

3. Ali poznate naslednje slovenske organizacije, ki se ukvarjajo z varnostjo na internetu?
   a) SAFE.SI DA NE
   b) Spletno oko DA NE
   c) SI-CERT DA NE
   d) Varnost na spletu .si DA NE

4. Ali poznate naslednje mednarodne organizacije, ki se ukvarjajo z varnostjo na internetu?
   a) INHOPE DA NE
   b) INSAFE DA NE
   c) eNASCO DA NE
   d) Childnet DA NE

5. Ali ste že kdaj na spletnih forumih uporabili spletni obrazec ali kako drugače podali prijavo neprimerne ali nezakonite vsebine?
   DA NE

   Zakaj DA? (Več možnih odgovorov.)
   a) Otroška pornografija.
   b) Sovražni govor.
   c) Spletno nadlegovanje.
   d) Prijava nezaželene e-pošte.
   e) Zloraba osebnih podatkov.
   f) Okužba, vdor ali poskus vdora v omrežje ali računalniški sistem.
   g) Zloraba mobilnega telefona.

   Zakaj NE?
   a) Ni bilo potrebno.
   b) Me ne zanima.
   c) Ne znam podati prijave.

6. Predstavljajte si, da ste na javnem forumu in berete komentarje uporabnikov. Med naštetimi izberite tiste, za katere menite da so oblika sovražnega govora. Nato opredelite ali je le-ta neprimeren ali nezakonit.

	Primerno.	Neprimerno, a ni sovražni govor.	Nezakonito, je sovražni govor.
1.	Prasec!		
2.	Kakšne kokoši ste!!		
3.	Hrvati sami hrčki!		
4.	Jebem ti mater!		
5.	Peder! Ko te najdem te bom ubil!		
6.	Tu se govori slovensko, ne bosansko.		
7.	Kako si ti butasta!		
8.	Makaronarji pa res ne znajo igrat nogometa.		
9.	Kaj boš ti govoril, ko si pravi invalid.		
10.	Hitlerja bi rabili! Vse cigane pobit!		
11.	Ukradla si mi punco, ti pocestnica!		
12.	Ti bodi tiho, ko imaš samo sedem razredov osnovne šole!		
13.	Kako ste bedasti.		
14.	Ha,ha,ha muslimani zdaj ste ga najebal.		
15.	Hipohonder...		

Najlepše se zahvaljujem za sodelovanje v anketi!