DRŽAVNO SREČANJE MLADIH RAZISKOVALCEV - OSNOVNOŠOLCEV

ZVEZA ZA TEHNIČNO KULTURO SLOVENIJE

VARNA RABA INTERNETA

(raziskovalna naloga)

Panoga:
računalništvo ali tečekomunikacije

Avtorica naloge:
Celeste Sanja Smareglia, 13. let
Osnovna šola Solkan

Mentorica:
mag. Magda Slokar Čevdek

Solkan, 2012

Povzetek

Internet je dandanes zelo pomemben dejavnik v družbi. Uporabljamo ga za komuniciranje, izobraževanje, iskanje spletnih informacij, nekateri za igranje spletnih igric, prenašanje glasbe, filmov in drugo.
V raziskovalni nalogi se ukvarjamo s proučevanjem stanja na področju varne uporabe interneta. Najprej si ogledamo teoretične osnove glede uporabe spleta. Sledi poglavje o metodi, kjer osvetlimo vzorec in merski inštrument ter postopek zbiranja in obdelave podatkov. Nadaljujemo s pregledom rezultatov in ugotovitev raziskave, ki je potekala med učenci OŠ Solkan. Rezultati kažejo, da se učenci večinoma zavedajo potencialnih nevarnosti, najpogostejši varnostni težavi sta neželena pošta in virusi, vendai ne uporabljajo vsi niti osnovnih zaščit. Nekateri posamezniki se spuščajo v veliko nevarnost z objavljanjem osebnih podatkov na spletu in s komuniciranjem s tujci. Nekateri so se srečali tudi s primeri otroške pornografije in spletnim nadlegovanjem. Večina učencev bi se v primeru zlorabe obrnila po pomoč k družinskim članom. Le polovica anketirancev navaja, da je v šoli obravnavala tudi varno uporabo interneta.
Nalogo zaključujemo z razpravo o dobljenih ugotovitvah in predlogi za izboljšanje srednje zadovoljivega stanja. Naša glavna predloga sta, da bi v šoli potekalo osveščanje o varni rabi interneta in da bi učenci uporabljali varen spletni brskalnik.

Ključne besede: varna uporaba interneta, nevarnosti interneta, računalniško piratstvo, škodljive spletne vsebine, nezakonite spletne vsebine, zaščita

Zahvala

Zahvaljujem se mentorici mag. Magdi Slokar Čevdek, učiteljici matematike za vso pomoč, spodbudo, nasvete in čas, ki mi ga je namenila pri nastajanju raziskovalne naloge.

Zahvaljujem se tudi vsem učencem 7., 8. in 9. razreda OŠ Solkan, ki so z reševanjem ankete sodelovali pri raziskavi.

KAZALO VSEBINE

1 UVOD

Internet je virtualno okolje, ki z množico informacij, znanj, storitev in odnosov spreminja družbo (http://www.student.si/preberi-si/aktualno/varna-uporaba-interneta.html). Na spletu je mogoče iskati različne informacije, pošiljati in sprejemati elektronsko pošto, pisati spletne dnevnike, igrati igrice, izmenjavati datoteke z drugimi uporabniki, prenašati glasbo, mogoče je tudi izmenjavati mnenja v spletnih klepetalnicah, prek messengerjev, v forumih in nakupovati preko spleta (http://www.safe.si/). Skoraj vse, kar smo prej morali iskati preko knjig, imenikov, znancev in drugih virov, lahko sedaj najdemo z enim klikom na spletnem brskalniku.

Internet je postal v sodobnem času nujno potrebno sredstvo v družbi, saj ga uporabljamo kot pripomoček v službi, za komuniciranje s prijatelji, nakupovanje, zbiranje informacij, igranje spletnih igric in še marsikaj drugega.

Tudi če internet uporabljamo vsak dan, ne vemo točno, kako deluje in tako se lahko že s klikom na neko nedolžno reklamno okence spustimo v veliko težavo. Težava je v tem, da veliko ljudi izkoristi internetne dobrine v svoje dobro (komercialni nameni) ali pa drugim v slabo (nadlegovanje, kraja gesla, denarja, virusi, ...). Ljudje s svojo neosveščenostjo o internetu so lahek plen za razne hekerje.

Poleg vseh zmogljivosti postaja internet vedno večja grožnja, še posebej mladostnikom, ki zaradi odvisnosti lahko prebedijo celo noč za računalnikom, ki zaradi druženja na spletu postanejo depresivni in postajajo žrtve marketinških prevar. Pogosto obravnavana tema je tudi anonimnost v klepetalnicah, ki jo nekateri izkoristijo v hude namene, kot so zlorabljanje preko spleta, nezaželena pošta in neprimerno obnašanje oziroma žaljenje na internetu.
Na internetu se zaradi raznovrstnih podatkov pogosto pojavljajo tudi nezakonite spletne strani kot so piratski spletni brskalniki ali pa neprimerne vsebine kot na primer pornografske strani, sovražni govor in še marsikaj neprimernega ali škodljivega.

Obravnavani problematiki smo se posvetili, ker so skoraj vsi ali celo vsi mladostniki uporabniki interneta, torej se srečujejo z nevarnostmi, ki prežijo na spletu.

Namen raziskovalne naloge je bil ugotoviti trenutno stanje na področju rabe interneta, ugotovljeno stanje primerjati s teoretičnimi izhodišči in doslej že opravljenimi raziskavami s tega področja ter po potrebi poiskati osnove za izboljšanje stanja.

Z raziskovalno nalogo smo želeli ugotoviti, kako pogosto učenci uporabljajo internet, ali se zavedajo vseh pasti na spletu in ali se znajo obvarovati pred njimi. Zanimalo nas je tudi, koliko učencev si nalaga nezakoniti piratski material, ali so previdni glede objavljanja osebnih podatkov

ter kolikokrat so že sami naleteli na težave. Želeli smo izvedeti, kam bi se učenci obrnili po pomoč v primeru zlorabe preko spleta, ali uporabljajo dovolj varno geslo, ali se pri pouku osredotočajo tudi na varno uporabo interneta, ali vedo, katera so kazniva dejanja ter katero zaščito računalnika uporabljajo. Vprašali smo jih tudi, ali so že kdaj naleteli preko spleta na draženje posameznikov, objavljanje vrstniškega nasilja, otroško pornografijo, sovražni govor in kolikokrat so naleteli na tovrstne primere.

Cilj raziskovalne naloge je bil raziskati ali imajo najstniki res težave z varnostjo na internetu in ali se zavedajo teh nevarnosti ter na osnovi ugotovitev raziskave poiskati predloge za večjo varnost pri delu z internetom. Z ugotovitvami raziskave in predlogi bomo seznanili učence po oddelkih v okviru ur oddelčnih skupnosti oziroma dneva Varne rabe interneta.

Na podlagi teoretičnih izhodišč, predstavljenih v prvem delu raziskovalne naloge, smo postavili naslednje hipoteze:

H1: Vsi anketirani učenci uporabljajo internet, večinoma redno.

H2: Največ anketirancev uporablja računalnik za komuniciranje preko spleta.

H3: Večina učencev sodeluje v socialnih omrežjih (facebook, twiter in drugih).

H4: Učenci se zavedajo potencialnih nevarnosti na internetu. Večina je slišala že za primere kraje identitete, računalniškega piratstva, nadlegovanja preko spleta, nevarnih stikov s tujci, zasvojenosti z internetom, obsedenosti s pornografijo na spletu in podobno.

H5: Med varnostnimi težavami internetnih uporabnikov sta najpogostejši neželena pošta ter virusi.

H6: Nihče od učencev še ni naletel prek interneta na otroško pornografijo.

H7: Za učence je največja varnostna težava kraja gesla oziroma identitete.

H8: Večina učencev je že razkrila svoje ime in spol na spletu.

H9: Večina učencev zaupa svoje geslo še komu drugemu.

H10: Večina učencev uporablja geslo, ki vsebuje njihove osebne podatke.

H11: Anketiranci nimajo dovolj zaščitenih računalnikov.

H12: Večina učencev nalaga nezakonito avdio in video vsebino.

H13: V primeru zlorabe bi učenci rešili težavo sami.

H14: Večina ne bi znala prijaviti sovražnega govora ali otroške pornografije.

Raziskava je bila opravljena med 119 učenci sedmih, osmih in devetih razredov OŠ Solkan. Podatke smo zbrali s spletno anketo ter jih analizirali, računalniško obdelali in interpretirali z informacijsko tehnologijo.

Raziskovalna naloga je nastajala v okviru diferenciranega šolskega dela in domačih zaposlitev nadarjenih učencev pri pouku matematike. Omeniti pa velja, da je takšno delo obsežno in mu je potrebno posvetiti tudi nekaj prostega časa.

2 VARNA RABA INTERNETA - TEORETIČNI DEL

2. 1 Internet

Na spletni strani Varna uporaba interneta (http://www.student.si/preberi-si/aktualno/varna-uporaba-interneta.html) avtorji navajajo, da je internet danes najhitrejši in najcenejši vir podatkov, ki je na voljo.

Internet je virtualno okolje, ki z množico informacij, znanj, storitev in odnosov spreminja družbo. S svojo brezmejnostjo dopušča svobodo in občutek anonimnosti, hkrati pa tudi priložnost za prepovedano. Na spletu je mogoče iskati različne informacije, pošiljati in sprejemati elektronsko pošto, pisati spletne dnevnike, igrati igrice, izmenjevati datoteke z drugimi uporabniki, prenašati glasbo, mogoče je tudi izmenjavati mnenja v spletnih klepetalnicah, prek messengerjev, v forumih in nakupovati preko spleta (http://www.safe.si/).

2.1.1 Raba interneta v Sloveniji

Kovačič idr. (2008) navajajo, da je po podatkih Statističnega urada republike Slovenije za prvo četrtino leta 2007 rednih uporabnikov interneta dobra polovica Slovencev starih med 10 in 74 let, kar 90 % mladih med 10 in 15 let pa internet redno uporablja. Pravijo, da je po podatkih raziskave Eurobarometer 2006 Slovenija po uporabi interneta med otroki kar za 10 % nad evropskim povprečjem ter povprečjem novih članic. Največ slovenskih otrok uporablja internet doma (84 %).
Omenjeni avtorji navajajo izsledke raziskav, na osnovi katerih poročajo, da največ mladih uporablja internet za izmenjavo glasbenih in video datotek. Prav tako popularni so igranje in prenašanje spletnih igric, filmov in glasbe, sledi elektronska pošta in raba interneta za samoizobraževanje ter komuniciranje preko spleta (klepetalnice, forumi).
Nadalje poročajo, da 15 % slovenskih staršev svojim otrokom določa pravila uporabe interneta, skoraj 60 % staršev otrokom časovno omejujejo uporabo interneta, nekaj več kot 40 % jim omejuje dostop do določenih spletnih strani, 40 % staršev pa svojim otrokom ne dovoli nakupovati na spletu. Niti tretjina slovenskih staršev meni, da so njihovi otroci že naleteli na škodljivo spletno stran, skoraj dve tretjini staršev meni, da bi njihovi otroci znali pravilno ravnati v primeru, ko bi naleteli na neprimerno spletno vsebino.

2.2 Nevarnosti interneta

Internet ima številne prednosti, pa tudi pasti. V teoretičnem delu raziskovalne naloge bomo najprej opisali njegove pasti, v nadaljevanju pa se osredotočimo na zaščito pred njegovimi nevarnostmi.

Kot navajajo avtorji priročnika Deskanje po varnih vodah (2008) predstavlja največjo varnostno težavo internetnim uporabnikom prejemanje neželene pošte ter računalniški virusi. Tri četrtine mesečnih uporabnikov interneta je vsaj že slišalo za primere zasvojenosti z internetom, tri petine je vsaj že slišalo za primere obsedenosti s pornografijo na internetu, dobra polovica je vsaj že slišala za primere vdora v tuja gesla za dostop do interneta. Otroci se na splošno dobro zavedajo potencialnih nevarnosti na spletu, kakršna so vprašanja varnosti, virusi, dostop do nezaželenih vsebin, kraje identitete in potencialno nevarni stiki s tujci.

Podatki Statističnega urada Republike Slovenije dokazujejo nevarnost interneta tudi v Sloveniji, saj je leta 2007 varovalo računalnik pred virusi, škodljivimi ter nadležnimi programi le 29 % oseb v starosti od 16 do 74 let. Istega leta je med rednimi uporabniki interneta naletelo na varnostne težave 35 % oseb v istem starostnem obdobju, v EU pa je bilo takih uporabnikov interneta 12 % manj (http://www.stat.si/novica_prikazi.aspx?id=1185).

Na spletni strani Varna uporaba interneta (http://www.student.si/preberi-si/aktualno/varna-uporaba-interneta.html) lahko preberemo, da previdnost ni odveč tudi pri posredovanju elektronskih naslovov, pri razkrivanju osebnih podatkov na spletu in pri presoji kaj objavljati v družbenih omrežjih. Avtor članka v Cosmo naturi (http://matura.cosmopolitan.si/lajf/varna-uporaba-interneta/) navaja sledeče podatke: skoraj petini (17 %) uporabnikov se je že zgodilo, da je njihov bližnji izrabil njihovo zaupanje in na svojem profilu objavil informacije, za katere niso želeli, da bi bile javno objavljene. Med mladimi od 10 do 20 let se je to zgodilo skoraj četrtini (23 %).

Rezultati Eurobarometer kvalitativne raziskave 2007 o varnem internetu za otroke kažejo, da čeprav mladi poznajo nevarnosti in vedo, kako se morajo zavarovati, bi večina poskusila rešiti težave sama ali s svojimi prijatelji in bi se le v skrajni sili zatekla po pomoč ali nasvet k svojim staršem.

2.3 Namerne zlorabe našega računalnika

Kovačič idr. (2008) opisujejo najpogostejše uporabljene zlorabe računalnikov. To so:

a) trojanski konji, virusi, črvi

Avtorji spletne strani Safe (http://www.safe.si/) ugotavljajo, da na splošno obstajajo vsaj trije tipi virusov:

- **Trojanski konji** delujejo tako, da se nam predstavijo kot zanimivi programi, s svojim destruktivnim delom pa se v času delovanja pretihotapijo v naš računalnik, uničujejo datoteke, jih ukradejo, včasih pa s pomočjo njih tretja oseba nadzoruje naš računalnik (s

tem ima dostop do naših gesel in tako naprej). Pri pregledovanju nekaterih spletnih strani lahko uporabniku neko spletno mesto ponudi namestitev posebnega programa ali pa celo izkoristi ranljivosti v operacijskem sistemu ali spletnem brskalniku in tak program namesti brez opozorila in vednosti uporabnika.Trojanski konji samodejno ne »okužijo« drugih računalnikov ali programov, kar je značilno za dve drugi družini škodljivih programskih kod, črve in viruse.

- **Virusi** so ustvarjeni tako, da se pripnejo na program ali datoteko, ki jo uporabljamo in se s pomočjo okužbe širijo. Poleg širjenja tudi poškodujejo programsko, strojno opremo in vse vrste datotek. Nevarnost virusov je prav ta, da nista nobena datoteka ali program imuna nanj. Na viruse pogosto naletimo z nezakonitim nalaganjem avdio in video materiala, običajno pa se prenašajo preko okuženih medijev ali internetnih povezav. Tudi pri klepetalnicah obstaja možnost izmenjevanja virusov, saj se izmenjujejo datoteke-kot pri elektronski pošti.
- **Črvi** se prav tako kot virusi razširjajo samodejno, a s to razliko, da ne okužijo obstoječih datotek ali programov. Ostanejo aktivni v delovnem pomnilniku in se skušajo preko omrežja (interneta) ter avtomatiziranih mehanizmov (na primer razpošiljanje e-pošte) operacijskega sistema razširiti na čim več računalniških sistemov. Večina tega početja je za uporabnika sprva neopazna, kasneje pa se lahko kaže v večji obremenjenosti - počasnosti sistema (zaradi nekontroliranega razpošiljanja črva na veliko število naslovov). Poleg tega večina črvov vsebuje tudi različne prijeme, ki izkoriščajo varnostne luknje v sistemu in s tem omogočijo nadzor nad našim računalnikom s strani tretjih oseb.

b) »Back door« programi in programi, ki omogočajo administriranje na daljavo

Ko so enkrat nameščeni programi za oddaljen nadzor oz. »back door« programi, omogočajo drugim ljudem dostop in kontrolo nad našim računalnikom.

c) DOS napadi

Pri tej obliki napada je na žrtev hkrati poslano toliko zahtev za komunikacijo, da ne more več učinkovito komunicirati s poštenimi klienti.

d) Nezaščitene datoteke operacijskega sistema Windows

Nezaščitene Windows omrežne datoteke lahko napadalci zlorabljajo tako, da namestijo veliko število orodij na računalnike, na katerih delujejo operacijski sistemi Windows in so priključeni na internet. Ker je varnost računalnikov na internetu medsebojno odvisna, ogroženi računalnik ne povzroča težav le svojemu lastniku, temveč je grožnja tudi ostalim subjektom na internetu.

e) Navzkrižno pisanje

Škodljivec lahko na spletni strani pripne škodljivo skripto in ko spletno stran pregledujemo, se škodljiva skripta prenese na naš računalnik.

Svoj spletni brskalnik izpostavljamo škodljivim skriptam z:

- odpiranjem povezav na spletnih straneh in v elektronskih sporočilih, ne da bi vedeli, kakšna je njihova vsebina,
- uporabo komunikacijskih orodij na straneh, ki jim ne zaupamo,
- ogledovanjem forumov, klepetalnic ali drugih dinamično generiranih strani, kjer lahko uporabniki objavljajo tekste s HTML priveski.

f) Prevare z elektronsko pošto

Tarča e-mail spoofing-a postanemo, ko dobimo elektronsko sporočilo od lažnega pošiljatelja. Ta oblika ogrožanja računalnika je poskus prevare uporabnika, s katero napadalci želijo pridobiti pomembne informacije (na primer gesla). Primeri prevar:

- Elektronsko sporočilo, kjer se pošiljatelj izdaja za sistemskega administratorja in zahteva od uporabnika, da svoje geslo zamenja za tistega, ki mu ga določi on in celo grozi s sankcijami, če uporabnik tega ne stori.
- Elektronsko sporočilo, kjer se pošiljatelj izdaja za osebo z avtoriteto in od uporabnika zahteva, da mu pošlje kopijo datotek z gesli ali drugo pomembno informacijo.

g) Virusi, ki se prenašajo preko elektronske pošte

Preden odpremo katerokoli priponko, bodimo prepričani o viru in vsebini priponke. To, da je sporočilo prišlo iz elektronskega naslova, ki ga prepoznamo, še ni zagotovilo. Škodljive kode se lahko prenašajo tudi preko zabavnih in mamljivih programov.

h) Programi za klepetalnice

Programi za internetno klepetanje kot na primer IRC (»Internet Relay Chat«), MSN Messenger, Skype, ICQ in podobni ponujajo mehanizme, s katerimi se informacije prenašajo dvosmerno med računalniki na internetu. »Chat« klienti omogočajo skupinam posameznikom, da si med sabo izmenjujejo dialog, URL povezave in v mnogih primerih tudi datoteke. Ker mnogi »chat«programi omogočajo izmenjavo .exe datotek, predstavljajo podobno grožnjo kot poštni programi. Kot skrbimo za zaščito poštnih programov, bi morali skrbeti tudi za zaščito »chat« programov predvsem z omejevanjem možnosti odpiranja potencialno nevarnih datotek, kot so .vbs in .exe datoteke. Zavedati se moramo tudi morebitnih neprijetnih posledic izmenjave datotek z neznanimi sogovorniki.

Omeniti velja še:

Ribarjenje« (phishing)

Ribarjenje je pogosta oblika kiber kriminala, kjer poskuša kriminalec od nas izvedeti osebne podatke (na primer geslo za e-pošto, občutljive bančne podatke) z namenom, da bi kasneje prevzel našo identiteto. Napadalci postavijo lažno spletno stran oziroma pošljejo prirejeno

elektronsko sporočilo, s katerim poskusijo uporabnika prepričati, da jim posreduje svoje osebne podatke. (Kovačič idr., 2006). Najpogostejša oblika te prevare je, ko elektronsko pismo ali spletna stran od uporabnika zahteva, da vanjo vnese svoje finančne podatke ali gesla. Tako goljufiva spletna stran kot elektronsko pismo sta lahko na pogled popolnoma enaka spletni strani ali pismu legitimnega podjetja (na primer banke), vendar pa bosta pridobljene finančne podatke posredovala tretjim osebam, ki se bodo z njimi okoristile. Takšna pisma in spletne strani so izredno zavajajoče, saj izvirno podjetje posnemajo tako po izgledu kot tudi po funkcionalnosti. Kot primer »ribarjenja« podatkov je bil v Sloveniji odmeven primer ponarejene vstopne strani NLB Klika.

Spam

Z izrazom »spam« označujemo nezaželena oziroma nenaročena elektronska sporočila. Večinoma gre za oglaševanje; pogosto tudi različnih goljufivih ali nezakonitih izdelkov ali storitev (Kovačič idr., 2006). Za spam sporočilo označimo vsako sporočilo, ki je poslano večjemu številu naslovnikov z namenom vsiljevanja vsebine, ki se je naslovniki sami ne bi odločili prejemati. V veliki večini primerov gre za oglaševanje plačljivih storitev ali izdelkov dvomljive kvalitete, velikokrat pa gre za goljufije.

Vohunski programi

So različni programi, ki spremljajo brkljanje uporabnika po internetu, odpirajo različna brskalna okna z reklamami, namenjeni so (prikritemu) zbiranju osebnih podatkov, prikazovanju oglasov, preusmerjanju spletnih brskalnikov in za različne nezakonite dejavnosti (na primer zamenjajo telefonsko številko ponudnika dostopa do interneta v uporabnikovih nastavitvah omrežja na klic z neko plačljivo telefonsko številko, po možnosti v tujini) (Kovačič idr., 2006).

2.4 Računalniško piratstvo

Intelektualna lastnina obsega pravice, ki izhajajo iz intelektualnih aktivnosti (patenti, modeli, blagovne in storitvene znamke, avtorske pravice s področja književnosti, znanosti in umetnosti). Pravo, ki ureja področje intelektualne lastnine, tako avtorju podeli začasen monopol nad komercialnim izkoriščanjem njegove ideje oziroma dela. Za uporabo se šteje zlasti reproduciranje (torej shranjevanje in kopiranje avtorskega dela), pa tudi javno izvajanje, javno prikazovanje in dajanje na voljo javnosti. Pod nekaterimi pogoji je avtorsko delo le mogoče prosto uporabljati: mogoče ga je predelati (na primer v parodijo ali karikaturo), uporabiti za citiranje (seveda pa je pri tem potrebno navesti avtorja), uporabiti (predvajati) za izobraževalne namene in podobno.

Za računalniško piratstvo se šteje vsaka oblika zlorabe avtorsko-pravno zaščitenega dela.

Računalniško piratstvo se uradno deli na pet kategorij:

- ponarejanje - neavtorizirano reproduciranje računalniških programov,

- nalaganje na disk (na primer nalaganje nezakonitih kopij programov na novo kupljene računalnike),
- dajanje računalniških programov v najem oziroma posojo,
- mehko piratstvo: nelegalno reproduciranje ene legalno kupljene kopije na več računalnikov na primer znotraj podjetja,
- internetno piratstvo: neavtorizirana naložitev računalniškega programa na spletno stran, oziroma piratstvo elektronskih oglasnih desk. Ta vrsta piratstva se je v zadnjih letih precej razmahnila, seveda pa ne v obliki nalaganja na spletne strani, pač pa v obliki nezakonite izmenjave datotek in nalaganja novih filmov, še preden se ti predvajajo v kinematografih (pogosto imajo pri tem tudi premoženjsko korist) (Kovačič idr., 2008).

Zakoniti prenosi glasbe in filmov so večinoma plačljivi, zato mladostniki pogosto uporabljajo piratske spletne strani, s katerih si nezakonito prenašajo brezplačno in nekvalitetno avdio in video vsebino. Prenos in prodajanje piratskih materialov sta nezakonita, kazniva in tudi nevarna (zaradi prenašanja virusov) načina varčevanja denarja.
Vsak internetni uporabnik, ki si nezakonito nalaga glasbo, filme, programe, videoigrice in podobno, se mora zavedati naslednjih dejstev (http://www.safe.si/):

- Prenos piratskih programov z interneta je kraja in zato kršitev zakona, prav tako je nezakonita prodaja piratskih programov.
- Piratskih kopij programske opreme ni možno posodabljati, zaradi česar so programi ranljivi za napade in vdore. Prav tako uporabnik ni prepričan o škodljivosti programa, ki ga je prenesel.
- S prenosom datotek se lahko na uporabnikov računalnik prenese tudi virus ali pa pride do izgube ali kraje pomembnih podatkov (kraja gesel, bančnih računov).
- Spletna stran lahko kljub navidezni tehnični dovršenosti pod pretvezo prodaja nelegalen software.

2.5 Škodljive spletne vsebine

Na splošno lahko rečemo, da so škodljive tiste spletne vsebine, ki prizadenejo čustva določenih oseb oz. družbenih skupin (na primer spletne strani o nasilju, umorih, spletna mesta za spodbujanje rasizma, anoreksije ali samomorov). Pogosto sploh ne gre za to, da bi iskali tovrstne teme, ampak veliko strani popolnoma nepovezanih z omenjenimi temami, prikazuje pojavna okna z vsemi vrstami vsebin, še posebej pornografskimi.
Nasilje na internetu obsega nasilne igre, spletno pornografijo, sovražna sporočila, spolne zlorabe in nadlegovanje (Kočevar, 2005).

2.5.1 Računalniške in spletne igrice

Colombain (2009) opozarja, da ima čezmerno igranje videoigric fizične ali celo psihične posledice, zaradi katerih trpi družina in prijatelji poleg uporabnika samega.

Na strani Safe (http://www.safe.si/) si lahko preberemo nekaj pretresljivih dejstev: Igralci v povprečju tedensko porabijo 8 ur za igranje računalniških in spletnih iger. Spletne igre v Evropi igra več kot 60 % otrok med 9 in 12 let in več kot 80 % otrok med 13 in 16 let. Mrežne igre, ki se jih igra skupaj s soigralci, igra polovica fantov med 9. in 16. letom.

Igranje nasilnih računalniških iger slabo vpliva na uporabnika, saj le-te lahko pripomorejo, da igralci postanejo agresivnejši tudi v resničnem življenju.

2.5.2 Nadlegovanje preko interneta

Veliko nasilja se na internetu dogaja na forumih in klepetalnicah, ki jim je skupno, da so namenjeni pogovorom in izražanju mnenj o specifičnih javnih temah, vendar tu lahko na žalost najdemo tudi žaljiva sporočila, zalezovanje in spletno sovraštvo (Kočevar, 2005).

Oblike spletnega nadlegovanja so predvsem naslednje: draženje, norčevanje iz posameznikov, opravljanje, pošiljanje nezaželenih sporočil, pošiljanje prizorov vrstniškega nasilja in podobno.

Med različnimi oblikami nadlegovanja na internetu je prisotno tudi spolno nadlegovanje. Nadlegovanje se lahko dogaja tudi preko elektronske pošte in preko spletnih strani, ne le znotraj klepetalnic.

2.5.3 Zasvojenost z internetom

Kovačič idr. (2008) pravijo, da lahko internetno zasvojenost opišemo kot impulzivno kontrolno motnjo, ki je zelo podobna zasvojenosti z igrami na srečo, motnjam hranjenja ali alkoholizmu. Posameznik preživi preveč časa pred računalnikom in se tem aktivnostim ne more odpovedati. Poznamo pet podtipov zasvojenosti z internetom: s spletno pornografijo, z virtualnimi odnosi, z igrami na srečo na internetu, z informacijami na internetu, s spletnimi igrami. Večji potencial za zasvojenost ima uporaba interneta, ki je usmerjena v navezovanje stikov ali vzpostavljanje (nadomestnih) odnosov; manjšega pa uporaba interneta za iskanje informacij. Youngova (1998; po Kovačič idr, 2008) trdi, da internet lahko zasvoji iz več razlogov. Eden izmed razlogov je ta, da je skupnost resnična in živeča entiteta, ki za zasvojence pomeni drug dom oz. mesto, kjer se vedno čutijo dobrodošle in kamor mislijo, da pripadajo. S pomočjo interneta se zatečeš v nek fantazijski svet, kjer lahko dobiš prijatelje za pogovor ali igranje iger ob katerokoli uri dneva. Na internetu lahko kadarkoli postaneš kdorkoli. Če si v resničnem življenju sramežljiv, lahko preko omrežja postaneš odprt in komunikativen, če si dolgočasen, lahko takoj postaneš duhovit in če si po naravi previden, lahko to previdnost obrneš v tvegano obnašanje, seveda le v kibernetskem prostoru.

Avtorji (2008) navajajo sledeče znake zasvojenosti z internetom:

- prezaposlenost z internetom,

- uporaba interneta ali igranje igric preko vseh časovnih norm (bedenje dolgo v noč)
- nervoza, slaba volja, depresija in razdražljivost, ko je potrebno prekiniti internetno povezavo,
- laganje staršem, prijateljem in ostalim o času, ki ga preživijo »on-line« oz. ob igranju igric,
- poslabšanje šolskega uspeha zaradi pretirane navezanosti na virtualni svet,
- izguba interesa za druženje s prijatelji v »resničnem svetu«,
- ponavljajoči, neuspešen trud za nadzor nad uporabo interneta oz. igranja igric in nezmožnost prenehanja,
- uporaba novih tehnologij kot sredstvo pobega pred problemi ali za sproščanje različnih negativnih občutkov (občutek nemoči, krivde, strahu ali depresije),
- fizične težave: neprespanost, rdeče oči, poslabšanje vida, SMS palec, pomanjkanje gibanja.

Jeričekova v svojem članku Zasvojenost z internetom (2003) povzema vprašalnik, ki ga je pripravila Youngova (1996; po Kovačič 2008) in je prirejen po merilih za zasvojenost s hazardiranjem.

Sestavljen je iz naslednjih vprašanj:

1. *Ali se počutiš preobremenjenega z internetom (misliš na prejšnjo aktivnost ali pričakuješ naslednjo)?*
2. *Ali čutiš potrebo, da bi vedno več časa preživel na internetu, da bi doživel zadovoljitev?*
3. *Kako pogosto si neuspešen pri kontroliranju, zmanjšanju ali prekinitvi uporabe interneta?*
4. *Ali si nemiren, nervozen, depresiven ali razdražljiv, ko zmanjšaš ali prenehaš z uporabo interneta?*
5. *Ali ostaneš na mreži dlje, kot prvotno načrtuješ?*
6. *Si tvegal izgubo pomembnejših odnosov, dela ali izobraževalnih priložnosti zaradi interneta?*
7. *Si se kdaj zlagal prijateljem, staršem ali drugim zato, da bi skril svojo navezanost na internet?*

Pet pritrdilnih odgovorov kaže na zasvojenost z internetom.

Odvisnost od interneta ali pretirana navezanost je namreč predvsem simptom in prvo opozorilo, da se z mladim človekom dogaja nekaj pomembnega v čustvenem in socialnem pogledu. Prekomerna raba novih tehnologij je pogosto znak drugih težav, kot so depresija, jeza in nizka samopodoba. Pomemben je vsakodnevni pogovor z otrokom o njegovih težavah, občutkih in potrebah. Če sumimo, da smo zasvojeni z internetom moramo počasi zmanjševati čas uporabe računalnika, v pridobljenem času pa se moramo zamotiti z drugimi dejavnostmi, ki nas zanimajo. V primeru, da nam tak ukrep ne pomaga, si moramo poiskati pomoč (http://www.safe.si/uploadi/editor/1213086334Deskanje_po_varnih_vodah.pdf).

2. 6 Nezakonite spletne vsebine

V skladu s slovensko zakonodajo med nezakonite sodijo spletne vsebine, ki vsebujejo (Kazenski zakonik RS):

- otroško pornografijo oz. pedofilijo,
- sovražni govor oz. rasistično propagando,
- propagiranje terorizma.

2.6.1 Otroška pornografija

Otroška pornografija naj bi v zadnjih letih na račun interneta in sodobne tehnologije zelo narasla. Od leta 1995 je število spletnih strani z otroško pornografijo naraslo za 1500 %. Otroška pornografija se je razvila v dobičkonosen posel, saj imajo proizvajalci, razpečevalci in uporabniki otroške pornografije na voljo lahko dostopno tehnologijo, predvsem digitalne kamere in fotoaparate ter internet. Policija je postavljena pred zelo težko nalogo predvsem zaradi širjenja materiala preko interneta.
Taylor in Quayle (2003) poudarjata, da ko so fotografije oziroma material z otroško pornografijo enkrat na internetu, jih ni mogoče več nadzorovati (umakniti). Žrtev se mora tako za vedno soočiti z zlorabo. Najnovejše slike imajo v ozadju računalnik in so postavljene v domače okolje. S tem se jasno kaže, da so otroško pornografijo ustvarili ljudje, ki so jim otroci zaupali.

2.6.2 Sovražni govor

Sovražni govor je izražanje mnenj in idej, ki so po svoji naravi diskriminatorne (ksenofobične, rasistične, homofobične in podobno) in uperjene proti različnim manjšinam (etničnim, narodnim, verskim, kulturnim, spolnim in podobno). Temelji na prepričanju, da so nekateri ljudje manjvredni, ker zaradi posamezne osebne okoliščine pripadajo določeni skupini. Te osebne okoliščine so lahko: narodnost, rasa ali etnično poreklo, versko ali drugo prepričanje, spol, zdravstveno stanje, jezik, spolna usmerjenost, invalidnost, starost, gmotno stanje, izobrazba, družbeni položaj in drugo (Kovačič idr., 2008).

2.7 Zaščita

V nadaljevanju bomo proučili možnosti zaščite pred internetnimi nevarnostmi.

2.7.1 Tehnični vidiki zaščite

Avtorji spletne strani Safe (http://www.safe.si/) zagotavljajo, da če želimo obvarovati računalnik pred virusi, je najboljša rešitev antivirusni program, operacijski sistem (oba redno posodabljamo) in požarni zid. Priporočljivo je tudi, da ima naš računalnik nameščen filter za nezaželeno pošto, protivohunski program, program za omejevanje časa na računalniku in filter za neprimerne vsebine, ki blokira nasilne, rasistične in pornografske strani neprimerne za otroke. Na

klepetalnicah je mogoče nastaviti zaščito zasebnosti, le-ta pa omejuje število in vrsto osebnih podatkov, ki jih uporabnikov profil posreduje javnosti. Tistim uporabnikom, ki imajo brezžičen dostop do interneta avtorji spletne strani Safe priporočajo trdno in varno geslo preko katerega sosedje nimajo dostopa do uporabnikovega internetnega računa.

Protivirusni programi

Varnost vsakega uporabnika računalnika zagotavlja dobra zaščita pred virusi. Zaradi hitrega pojavljanja vedno novih virusov, mora uporabnik svoj antivirusni program dopolnjevati z novimi protivirusnimi vzorci oziroma mora posodabljati protivirusni program. Dobri protivirusni programi so največkrat plačljivi, vendar strošek zagotovo odtehta tveganje okužbe z virusom, zmanjša pa se tudi možnost kraje ali izgube podatkov. Podobno kot protivirusni programi delujejo tudi protismetni programi, ki odstranjujejo vohunske programe, očitna razlika pa je, da je večina protismetnih programov na voljo brezplačno (Kovačič idr., 2006). Protivirusni program je potrebno redno posodabljati – vsaj enkrat na mesec, po potrebi pa tudi pogosteje, virusne baze pa naj se posodabljajo vsak dan.

Požarni zid

Požarni zid je poseben vmesnik (program ali strojna oprema), ki omejuje nepooblaščene dostope iz omrežja oziroma v omrežje. Namestitev požarnega zidu je še posebej pomembna za uporabnike, ki so v internet povezani preko ADSL in Kabla, ki jim zagotavlja neprestano povezavo. Računalnik povezan v internet brez ustrezne zaščite izgleda približno tako, kot če bi odšli od doma in pustili vhodna vrata na široko odprta.

Šifriranje

Ena izmed zaščitnih tehnik je tudi kriptografija oz. šifriranje, kjer sporočilo, trdi disk ali datoteko zašifriramo (da bi zaščitili njegovo vsebino) in zavarujemo z geslom ali ključem.

Trajno brisanje podatkov

V primeru prodaje odrabljenega računalnika je priporočljivo, da uporabnik trajno izbriše podatke iz trdega diska in tako tudi uniči elektronske sledi. Trajno brisanje deluje na osnovi prepisovanja podatkov čez stare, vendar kljub temu ni učinkovito na vseh datotečnih sistemih, saj so nekateri datotečni sistemi zasnovani tako, da je uničene podatke mogoče obnoviti.

Filtriranje in blokiranje neprimernih vsebin

Osnovni korak zaščite je, da že v spletnem brskalniku nastavimo stopnjo prepustnosti za določene vsebine, s čimer otrokom preprečimo dostop do nezaželenih spletnih vsebin (na primer pornografije).

Morda na tem mestu ni odveč, če omenimo, da imajo otroci pravico do zasebnosti tudi pred lastnimi starši. Preden starši posežejo po takih metodah, je priporočeno, da se z otrokom

poskušajo pogovoriti in dosežejo medsebojno zaupanje, kjer tovrstne metode sploh ne bodo več potrebne.

Zaščita elektronske pošte
V programu za sprejemanje elektronske pošte je potrebno aktivirati vse možne varnostne mehanizme. S protivirusnim program moramo redno preverjati datoteke na računalniku ter elektronsko pošto.

Uporaba najnovejših operacijskih sistemov
Na računalniku imamo nameščene najnovejše popravke operacijskega sistema (na primer »windows update«) in posodobljen antivirusni program (Kovačič idr., 2008).

2.7.2 Samozaščita

Čeprav se poslužujemo vse tehnične zaščite, ni odveč da smo pri uporabi interneta previdni. V nadaljevanju je podanih nekaj priporočil, ki nam pomagajo, da se izognemo marsikateri nevarnosti na internetu. Najboljša zaščita je pazljivost.

Mlajši otroci ne bi smeli uporabljati družabnih omrežij, saj imajo le-ta v veliki večini omejeno uporabo na starost nad 13 let.
Pomembno je, da varujemo svoje osebne podatke (ime, naslov, telefon). Svojih osebnih informacij (imena, naslova, telefonske številke, e-mail naslova) nikoli ne posredujemo preko interneta. Istega gesla ne uporabljamo za vse spletne skupine, ki se jih udeležujemo, gesla ne zaupamo nikomur in ga vsake toliko zamenjamo. Geslo tudi ne sme vsebovati naših osebnih podatkov, bolje pa je tudi, da je zapleteno. Nikoli ne odgovarjajmo na elektronska pisma, ki od nas zahtevajo osebne in finančne podatke. Nikoli ne odpirajmo ali odgovarjajmo na sporočila, ki nam jih pošiljajo neznanci. Ne objavljamo osebnih podatkov in slik drugih ljudi brez njihovega dovoljenja.
Upoštevajmo spletni bonton. V virtualnem svetu naj veljajo ista pravila kot v realnem svetu. Avtorji spletne strani Safe razlagajo, da tudi na spletu naletimo na pravila, kot na primer spletna etika, ki služi kot osnovna smernica obnašanja na internetu in nam narekuje, naj se do drugih vedemo tako, kot si želimo, da bi se oni do nas ter spoštujemo zasebnost in čas drugih.
Najmanj priporočljiva so osebna srečanja s prijatelji, ki smo jih spoznali prek klepetalnice. V primeru, da smo se vseeno odločili za sestanek s tako osebo, lahko prej malo poizvedujemo o njej, za sam sestanek pa določimo javen kraj podnevi, nanj pa se po možnosti ne odpravimo sami. Otroci naj se ne srečujejo z ljudmi, ki so jih spoznali on-line, vsaj ne brez spremstva.

2.7.3 Omejitve s strani staršev

Priložnosti in koristi interneta daleč presegajo njegove nevarnosti, vendar tehnični pripomočki ne

morejo in ne smejo zamenjati starševskega spremstva ob vstopanju otroka v svet interneta.
Avtorji spletne strani Safe (http://www.safe.si/) poudarjajo, da je pomembno, da:

- vzgoja za internet ne temelji na tehničnih veščinah uporabe, ampak na razvoju kritičnega mišljenja, presoje in odgovornega ravnanja pri uporabi novih tehnologij.
- so starši obveščeni o tem, kaj njihov otrok počne na internetu.
- imajo starši osnovno znanje o internetu in nevarnostih povezanih z njim.
- se cela družina drži pravil o uporabi računalnika, ki so jih starši postavili skupaj z otroci.
- se pogovarjajo z otroki o nevarnostih na internetu.
- vzpostavijo odnos zaupanja in dialoga tako, da prisluhnejo otroku in mu ne vzpostavijo občutka krivde.
- so pozorni na znake, ki kažejo, da je nekaj narobe.
- postavijo časovne omejitve.

Internet lahko postane problem, ko začne negativno vplivati na otrokovo zdravje, šolski uspeh, splošno počutje ter odnose s prijatelji in družino, zato morajo starši nadzorovati čas, ki ga otrok porabi pri računalniku. Starši morajo otroku razložiti tudi posledice prekrška njihove omejitve.

Če obstaja resnični problem, je čas, da se določijo nekatera pravila in meje, kot so na primer:

- Brez mobilnih telefonov ob obrokih (zajtrk, kosilo, večerja) ter v času med 17.30 in 19.00.
- Domača naloga in ostala opravila morajo biti opravljena pred igranjem video igric.
- Prepoved uporabe tehnologije v spalnicah v nočnem času.
- Časovno omejitev igranja video igric, uporabe socialnih omrežij in ostale tehnologije je potrebno vsiliti, če otrok ni sposoben sam nadzorovati uporabe.

Pri uporabi interneta je potrebna zmernost in previdnost. Potrebno je poskrbeti za ustrezno tehnično zaščito, samozaščito pa tudi omejitve staršev niso odveč, če se izkaže, da so potrebne. Vsekakor naj bo internet orodje, vloge resničnega in medosebnih stikov iz oči v oči pa le ne more nadomestiti.

3 METODE

V tem poglavju je opisan vzorec, merski inštrument in prikazan postopek zbiranja in obdelave podatkov.

3.1 Vzorec

V raziskavo smo zajeli 50 moških in 69 žensk, skupaj 119 od 192 učencev od sedmega do devetega razreda na OŠ Solkan, kar predstavlja 62 % populacije.

3.2 Merski instrument

Za zbiranje podatkov smo uporabili vprašalnik izbirnega tipa, ki smo ga na osnovi teoretičnih izhodišč predstavljenih v poglavju »Varna raba interneta - teoretični del« sestavili za potrebe naše raziskave, in je zajemal: vprašanja o spolu, starosti, načinu in pogostosti uporabe interneta, težavah z varnostjo na internetu in o zaščiti pred nevarnostmi na spletu. Anketirani učenci so odgovarjali tudi na vprašanja o tem kakšno geslo uporabljajo, ali so ga že zaupali drugi osebi, ali so že razkrili osebne podatke na spletu in na katere in kolikokrat so že sami naleteli na varnostne težave ter kakšne zaščitne programe uporabljajo. Zanimalo nas je tudi, kam bi se učenci obrnili po pomoč v primeru nadlegovanja prek spleta, ali vedo, kam prijaviti nadlegovanje. Povprašali smo tudi o tem, ali pri pouku in razrednih urah posvečajo pozornost varni rabi interneta. Anketa se je delila na tri dele: na splošna vprašanja glede uporabe interneta, na težave na spletu in na del z vprašanji o zaščiti anketirancev.

3.3 Postopek zbiranja in obdelave podatkov

Za zbiranje podatkov smo uporabili spletno anketo, ki je bila en teden v marcu 2012 objavljena spletni strani www.mojaanketa.si/anketa/213714889. Povezava na anketo je bila učencem dostopna z omrežnega diska v računalniški učilnici ter v učilnici matematike, tako da so učenci lahko izpolnjevali anketo med poukom, med razredno uro ali pa tudi v odmoru po dogovoru z učiteljico matematike. Anketirancem smo zagotovili prostovoljno in anonimno sodelovanje v anketi. Zbrani podatki so bili obdelani, analizirani ter interpretirani s pomočjo informacijske tehnologije.

4 REZULTATI

Z anketnim vprašalnikom smo zbrali mnenja učencev OŠ Solkan glede varne uporabe interneta, slednje podatke pa bomo v nadaljevanju podrobneje predstavili.

4.1 Demografski podatki

V raziskavo smo zajeli 50 moških in 69 žensk. Delež moških in žensk vključenih v raziskavo je prikazan v tabeli 1 ter na diagramu 1. Povprečna starost anketirancev je 13,4 leta. Najmlajši anketiranci so bili stari 12 let, najstarejši pa 15 let.

Tabela 1: Struktura anketirancev po spolu

Spol	Število	%
moški	50	42
ženske	69	57

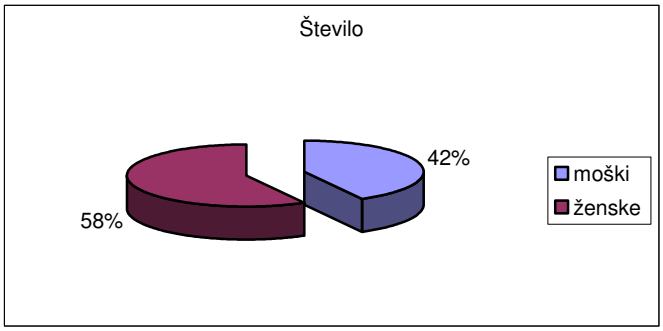

Diagram 1: Struktura anketirancev po spolu

4.2 Uporaba interneta

Vseh 119 učencev (100 %) uporablja internet. Zanimalo nas je tudi, kako pogosto učenci uporabljajo internet. Med 119 udeleženci je bil najbolj pogost odgovor "vsak dan", najmanj pogost odgovor pa "nikoli". Več kot polovica uporablja internet nekajkrat tedensko ali skoraj vsak dan, 41 % pa vsak dan, samo 5 učencev uporablja splet le nekajkrat mesečno. Navedeni podatki so razvidni v tabeli 2. Glede pogostosti uporabe interneta ni bistvenih razlik glede na spol.

Tabela 2: Struktura anketirancev glede na pogostost uporabe interneta

Odgovor	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
nikoli	0	0	0	0	0	0
nekaj krat mesečno	1	2	4	6	5	4
nekaj krat tedensko	14	28	15	22	29	24
skoraj vsak dan	16	32	20	29	36	30
vsak dan	19	38	30	44	49	41

4.3 Namen uporabe interneta

Ko smo anketirance spraševali o namenu uporabe interneta, je bilo možnih več odgovorov. Iz tabele 3 in diagrama 2 lahko razberemo, da največ učencev uporablja računalnik za komuniciranje prek spleta (76 %), najmanj pa za igranje iger na srečo (2,5 %), kar 64 % anketirancev uporablja internet za iskanje informacij, 57 % za prenašanje glasbe, igric in filmov, 52 % za pošiljanje sporočil prek elektronske pošte, 39 % za izmenjavo glasbenih datotek in filmov, enak delež za izobraževanje in 35 % za igranje spletnih igric. 11 % deklet več kot fantov komunicira preko spleta, več kot dvakrat več fantov kot deklet pa igra spletne igrice ter približno petina fantov več kot deklet uporablja internet za izmenjavo glasbenih datotek in filmov ter za prenašanje filmov, glasbe in igric.

Tabela 3: Namen uporabe interneta

Odgovor	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
za izmenjavo glasbenih datotek in filmov	25	50	22	32	47	39
za prenašanje glasbe, filmov in igric	35	70	33	48	68	57
za elektronsko pošto	27	54	35	51	62	52
za izobraževanje	17	34	29	42	46	39
za komuniciranje prek spleta	35	70	56	81	91	**76**
za iskanje informacij	31	62	45	65	76	64
za igranje iger na srečo	1	2	2	3	3	2,5
za igranje spletnih igric	26	52	16	23	42	35

Opomba: Odstotek je izračunan kot število odgovorov za odgovor deljeno s številom anketirancev.

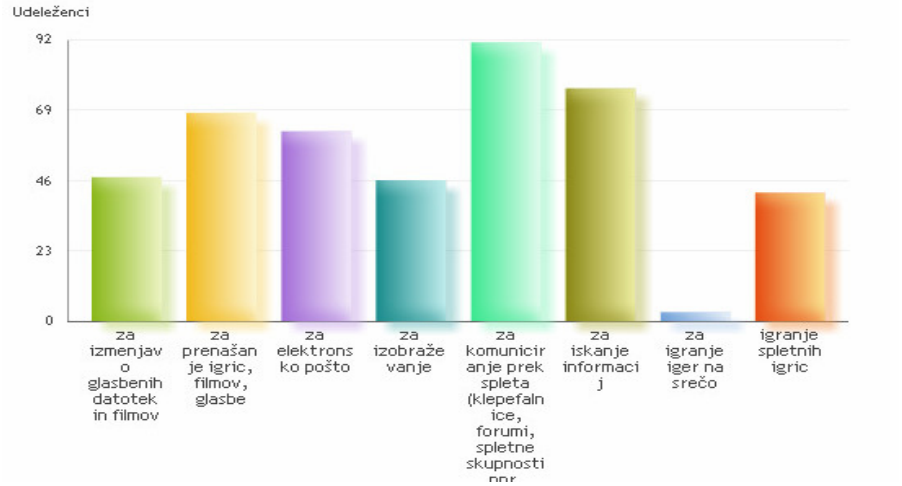

Diagram 2: Namen uporabe interneta

4.4 Sodelovanje v spletnih klepetalnicah, forumih in socialnih omrežjih

Pozanimali smo se, ali anketiranci sodelujejo tudi v spletnih klepetalnicah, forumih in socialnih omrežjih in ugotovili, da spletne klepetalnice obiskuje 19 % učencev, v forumih sodeluje 8 % učencev, v socialnih omrežjih pa klepeta kar 82 %. Fantje sodelujejo v spletnih forumih dvakrat več kot dekleta, dekleta pa v socialnih omrežij 10 % več kot fantje. Bolj podrobne podatke o odgovorih na to vprašanje prikazujejo tabele 4, 5 in 6.

Tabela 4 Sodelovanje v spletnih klepetalnicah

Sodelovanje v spletnih klepetalnicah	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
da	10	20	13	19	23	19
ne	29	58	40	58	69	58
včasih	11	22	16	23	27	23

Tabela 5: Sodelovanje v spletnih forumih

Sodelovanje v spletnih forumih	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
da	6	12	4	6	10	8
ne	30	60	52	75	82	70
včasih	14	28	13	19	14	28

Tabela 6: Sodelovanje v socialnih omrežjih

Sodelovanje v socialnih omrežjih	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
da	36	72	61	88	97	**82**
ne	10	20	7	10	17	14
včasih	4	8	1	1	5	4

4.5 Ocena varnosti interneta

Anketiranci ocenjujejo varnost interneta s povprečno oceno **3,12** na lestvici od 1 do 5. Med fanti je bil povprečen odgovor 3,36, med dekleti pa je bilo povprečje nižje (2,94). Iz povedanega sledi, da je za fantje internet za bolj varen.

4.6 Prepoznava določenih primerov nevarnosti prek interneta

Pri tem vprašanju so učenci navajali, za katere primere nevarnosti na spletu so že slišali. Imeli so možnost navesti več odgovorov. Anketirancem sta najbolj znana primera kraje gesla za dostop do interneta (102 učenca) in zasvojenosti na internetu (103 učenci), največja neznanka pa jim je bil sovražni govor in računalniško piratstvo. Za nevarne stike s tujci ve 75 % učencev, za nadlegovanje preko interneta pa 80 %. Pod odgovorom drugo zasledimo teroristični govor, kar lahko razumemo kot sovražni govor. Natančnejši podatki so predstavljeni na tabeli 7 in diagramu 3.

Tabela 7: Prepoznavanje primerov nevarnosti prek interneta

Primer	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
kraje gesla za dostop do interneta, kraje identitete	40	80	62	90	102	**86**
nadlegovanje preko interneta	36	72	59	86	95	80
nevarnih stikov s tujci	31	62	58	84	89	75
računalniškega piratstva	31	62	38	55	69	58
zasvojenosti z internetom	39	78	64	92	103	**87**
obsedenosti s pornografijo na internetu	29	58	45	65	74	62
sovražnega govora	26	52	40	58	66	55
drugo	1	2	4	6	5	4

Opomba: Odstotek je izračunan kot število odgovorov za odgovor deljeno s številom anketirancev.

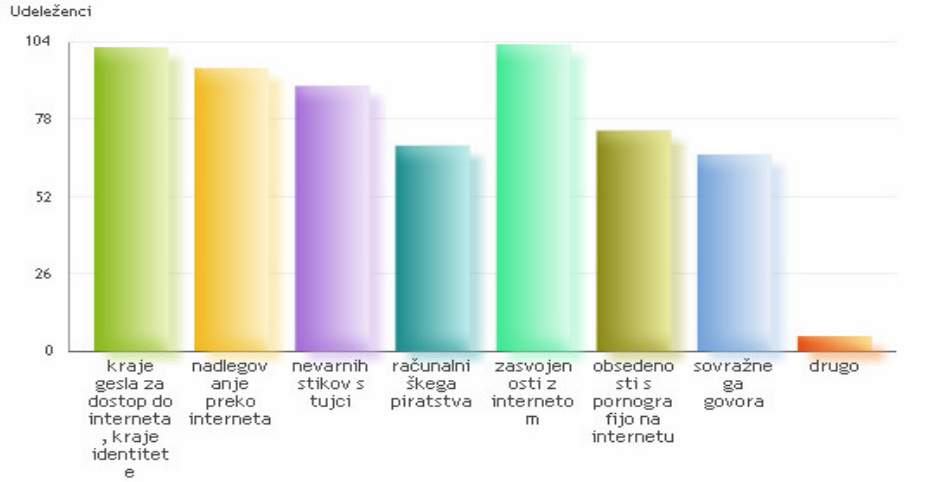

Diagram 3: Prepoznavanje primerov nevarnosti prek interneta

4.7 Soočanje z neprimernimi vsebinami ter varnostnimi težavami na internetu

40 % učencev ne ve, kolikokrat je že naletelo na varnostne težave in neprimerne vsebine prek spleta. Kar 14 % je na take vrste težav naletelo že več kot desetkrat, 24 % pa se je s tem soočilo

le malokrat. Tistih, ki se niso še nikoli soočili z varnostnimi težavami je bolj malo (14 %). Iz spodnjihtavel lahko vidimo tudi, da so fantje večkrat naleteli na težave kot punce.

Tabela 8: Soočanje z neprimernimi vsebinami ter varnostnimi težavami na internetu

Količina	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
1- 4 krat	14	28	15	22	29	24
5- 9 krat	5	10	3	4	8	7
več kot 10 krat	8	16	9	13	17	14
nikoli	7	14	10	15	17	14
ne vem	16	32	31	45	49	40
drugo	0	0	1	1	1	1

4.8 Soočanje z različnimi vrstami varnostnih težav

Ko so anketiranci odgovarjali na vprašanje, s katerimi varnostnimi težavami so se že srečali, so imeli možnost izbire več odgovorov. Varnostna težava, ki se največkrat pojavlja v računalnikih anketirancev so virusi, črvi in trojanski konji (57 % učencev). Zelo pogosta je tudi nezaželena pošta, saj je nanjo naletela tretjina vprašanih (41 učencev). Da bi pa nekdo zlorabil zaupanje učenca in objavil učenčeve podatke, se je pripetilo samo 9 najstnikom (8 %). Nadlegovanje se je zgodilo 6 % učencem, kraja gesla 16 %, nevarnim stikom s tujci je bilo izpostavljeno 10 % vprašanih. Rezultati kažejo, da se dekleta bolj soočajo z več varnostnimi težavami kot fantje. Ostale podatke si lahko ogledamo na tabeli 9.

Tabela 9: Soočanje z različnimi vrstami varnostnih težav na spletu

Primer	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
neželena pošta (spam)	16	32	25	36	41	**34**
virusi, trojanski konj, črvi	30	60	38	55	68	**57**
kraja gesla, identitete, občutljivih podatkov	6	12	13	19	19	16
nevarne stike s tujci	3	6	9	13	12	10
nadlegovanje prek interneta	1	2	6	9	7	6
druga oseba je zlorabila tvoje zaupanje in na internetu objavila tvoje osebne podatke	3	6	6	9	9	8
nobene	13	26	21	30	34	29
drugo	2	4	1	1	3	2,5

Opomba: Odstotek je izračunan kot število odgovorov za odgovor deljeno s številom anketirancev.

4.9 Največje varnostne težave

Največjo težavo učencem predstaljajo virusi, črvi in trojanski konji, najmanjšo pa prejemanje neželene pošte. Kraji gesla oziroma identitete, ki je resen problem, je po mnenju anketirancev pripadlo 3. mesto. Podatki so predstavljeni v tabeli 10.
Rang kaže na pomembnost možnega odgovora; višji kot je rang, bolj pomemben je odgovor. Točke so seštevek vseh odgovorov za ta odgovor. Najbolj pomemben odgovor ima najnižje, najmanj pomemben odgovor pa najvišje število točk.

Tabela 10: Največje varnostne težave na spletu

Primer	Točke	Rang
virusi, trojanski konj, črvi	387	**1**
nevarni stiki s tujci	406	2
kraja gesla, identitete	410	3
nadlegovanje prek interneta	414	4
neželene vsebine	423	5
prejemanje neželene pošte	450	6

4.10 Pogostost varnostnih težav

Skoraj dvema tretjinama učencev so se že kdaj prenesli virusi na računalnik. 52 % anketirancev ni prejelo nezaželene pošte, 83 % ni bilo okradeno identitete in skoraj nihče ni bil okraden denarja prek spleta. Odstotek nadlegovanih je precej velik: 12 %. Iz tabel je tudi razvidno, da so imele anketirane ženske več težav s prenosom virusov, nezaželeno pošto in nadlegovanjem kot fantje. Kar 10 % deklet več kot fantov je že bilo nadlegovanih prek spleta. Te in ostale podatke lahko razberemo s tabel 11, 12 in 13.

Tabela 11: Količina varnostnih težav

	Nikoli		1-5krat		6-10krat		Več kot 10-tkrat	
	število	%	število	%	število	%	število	%
prenos virusov na računalnik	42	35	65	55	3	3	9	8
nezaželena pošta	62	52	35	29	6	5	16	13
kraja gesla, identitete	99	83	16	13	1	1	3	3
kraja denarja	117	98	2	2	0	0	0	0
nadlegovanje prek spleta	105	88	8	7	4	3	2	2

Tabela 12: Količina varnostnih težav - moški

	Nikoli		1-5krat		6-10krat		Več kot 10-krat	
	število	%	število	%	število	%	število	%
prenos virusov na računalnik	22	44	24	48	1	2	3	6
nezaželena pošta	30	60	10	20	2	4	8	16
kraja gesla, identitete	42	84	6	12	1	2	1	2
kraja denarja	49	98	1	2	0	0	0	0
nadlegovanje prek spleta	47	94	1	2	2	4	0	0

Tabela 13: Količina varnostnih težav - ženske

	Nikoli		1-5krat		6-10krat		Več kot 10-tkrat	
	število	%	število	%	število	%	število	%
prenos virusov na računalnik	20	29	41	59	2	3	6	9
nezaželena pošta	32	46	25	36	4	6	8	12
kraja gesla, identitete	57	83	10	15	0	0	2	3
kraja denarja	68	99	1	1	0	0	0	0
nadlegovanje prek spleta	58	84	7	10	2	3	2	3

4.11 Soočanje z neprijetnimi izkušnjami na spletu

Kar 60 % anketiranih je bilo že priča norčevanju iz posameznikov preko interneta, polovica pošiljanju nezaželenih sporočil, najmanj pogost odgovor pa je "spolno nadlegovanje" (8 %). Kar 43 % učencev pa je naletelo na sovražni govor, 39 % se je že soočilo z draženjem, 13 % učencev je tudi že videlo otroško pornografijo preko spleta, kar 18 učencev je potrdilo kroženje prizorov vrstniškega nasilja po spletu. Razvidno je, da navaja večji delež deklet kot fantov, da je naletelo na sovražni govor, draženje in norčevanje iz posameznikov, medtem ko je na pošiljanje nezaželenih sporočil naletelo več fantov kot deklet. V ostalih primerih ni bistvenih razlik med spoloma. Pod odgovor drugo anketiranci navajajo, da se niso srečali z navedenimi težavami. Podatki na to temo so predstavljeni na tabeli 14 in diagramu 4.

Tabela 14: Soočanje z neprijetnimi izkušnjami na spletu

Primer	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
draženje	16	32	31	45	47	39
norčevanje iz posameznikov	27	54	44	64	71	**60**
pošiljanje nezaželenih sporočil	22	44	27	39	49	**49**
pošiljanje prizorov vrstniškega nasilja	7	14	11	16	18	15
spolno nadlegovanje	3	6	6	9	9	8
otroška pornografija	8	16	8	12	16	13
sovražni govor	13	26	38	55	51	43
drugo	6	12	6	9	12	10

Opomba: Odstotek je izračunan kot število odgovorov za odgovor deljeno s številom anketirancev

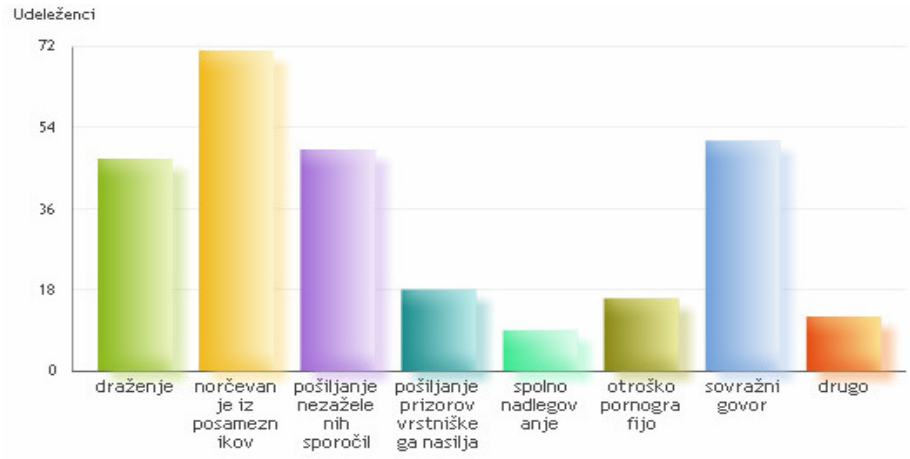

Diagram 4: Soočanje z neprijetnimi izkušnjami na spletu

4.12 Ocena nevarnosti določenih dejanj

V tem primeru se je učencem zdelo, da je najbolj nevarno dejanje razkritja osebnih podatkov neznancem. Najmanj nevarno je po njihovem mnenju pozabiti svoje geslo. Odvisnost, ki je resen in zelo škodljiv problem, je bila po nevarnosti na drugem mestu. Podatke lahko primerjamo v tabeli 15.

Tabela 15: Ocena nevarnosti določenih dejanj

Dejanje	Točke	Rang
razkritje osebnih podatkov neznancem	306	**1**
odvisnost	343	2
kršenje avtorskih pravic	349	3
neprimerno obnašanje na internetu	375	4
pozabiti svoje geslo	402	5

4.13 Razkritje osebnih podatkov prek spleta

Tudi pri vprašanju o osebnih podatkih, ki so jih anketiranci že razkrili preko spleta, so lahko navedli več možnih odgovorov. Večina učencev je razkrila preko spleta svoje ime (85 %), spol (86 %), skoraj 60 % starost, le 5 odstotkov manj elektronski naslov, 12 % učencev je razkrilo svoj naslov bivališča, enak odstotek učencev pa ni razkril nobenega osebnega podatka izmed možnih v anketi. Več deklet kot fantov je razkrilo ime, starost in spol, medtem, ko je13 % fantov več kot deklet razkrilo elektronski naslov ter 4 % več fantov kot deklet razkrilo naslov bivališča. Pod odgovor drugo zasledimo hobije in odgovore, ki so že navedeni prej. Podatki so napisani v tabeli 16 in diagramu 5.

Tabela 16: Razkritje osebnih podatkov prek spleta

Podatek	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
ime	40	80	61	88	101	**85**
spol	42	84	60	87	102	**86**
starost	28	56	42	61	70	59
naslov bivališča	7	14	7	10	14	12
elektronski naslov	31	62	34	49	65	55
nič od tega	5	10	9	13	14	12
drugo	3	6	3	4	6	5

Opomba: Odstotek je izračunan kot število odgovorov za odgovor deljeno s številom anketirancev

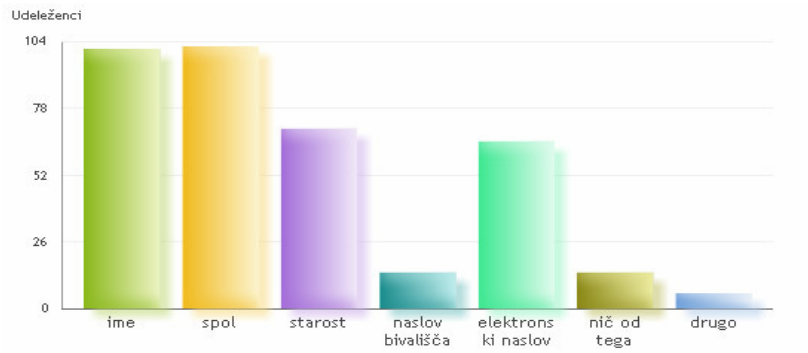

Diagram 5: Razkritje osebnih podatkov prek spleta

4.14 Pogostost nalaganja brezplačnega piratskega materiala

Kar 80 % učencev si nalaga piratsko glasbo, več kot dve tretjini si nalagata filme, več kot polovica piratske programe in več kot tretjina videoigrice na piratski strani. Tovrstni podatki so prikazani v tabeli 17, 18 in 19.

Tabela 17: Pogostost nalaganja brezplačnega piratskega materiala

Primer nalaganja	Nikoli		Redno		Pogosto		Vsak dan	
	število	%	število	%	število	%	število	%
nalaganje glasbe	25	21	37	31	38	32	19	16
nalaganje filmov	65	29	37	31	36	30	11	9
nalaganje videoigric	75	63	26	2	11	9	7	6
nalaganje programov	52	44	37	31	22	19	8	7

Tabela 18: Pogostost nalaganja brezplačnega piratskega materiala - moški

Primer nalaganja	Nikoli		Redno		Pogosto		Vsak dan	
	število	%	število	%	število	%	število	%
nalaganje glasbe	12	24	15	30	14	28	9	18
nalaganje filmov	14	28	17	34	14	28	5	10
nalaganje videoigric	23	49	17	34	6	12	4	8
nalaganje programov	18	36	16	32	16	32	6	12

Tabela 19: Pogostost nalaganja brezplačnega piratskega materiala - ženske

Primer nalaganja	Nikoli		Redno		Pogosto		Vsak dan	
	število	%	število	%	število	%	število	%
nalaganje glasbe	13	19	22	32	24	35	10	15
nalaganje filmov	21	30	20	29	22	32	6	9
nalaganje videoigric	52	75	9	13	5	7	3	4
nalaganje programov	34	49	21	30	12	17	2	3

4.15 Sramovanje dejanj na spletu

Samo 7 % učencev se je odkrito sramovalo svojih dejanj na klepetalnicah in blogih, večina (69 %) se pa ni še nikoli. 24 % je odstotek najstnikov, ki so se svojih dejanj sramovali le nekajkrat. Slednji podatki so prikazani v obliki tabele 20.

Tabela 20: Struktura anketirancev glede na sramovanje dejanj na spletu

Odgovor	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
da	3	6	5	7	8	7
nekajkrat	38	76	44	64	29	24
nikoli	9	18	20	29	82	69

4.16 Zaupanje gesla drugi osebi

Tabela 21 in diagram 6 prikazujeta, da kar 56 % učencev trdi, da ni nikoli zaupalo svojega gesla drugi osebi, 39 % pa ga je. Glede zaupanja gesla drugi osebi ni bistvenih razlik po spolu.

Tabela 21: Zaupanje gesla drugi osebi

	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
da	19	38	27	39	46	39
ne	28	56	38	55	66	56
ne vem	3	6	4	6	7	6

Diagram 6: Zaupanje gesla drugi osebi

4.17 Izgled gesla

Tudi pri tem vprašanju je bilo možnih več odgovorov. Rezultati ankete kažejo, da 40 % učencev uporablja geslo sestavljeno iz črk in številk, 14 % pa geslo, ki vsebuje njihove osebne podatke. 36 % učencev uporablja geslo, ki je njim znana beseda. Zapleteno geslo iz zaporedja majhnih in velikih črk uporablja 12 % anketiranih, geslo ki vsebuje črke, številke in druge znake pa 21 % vprašanih. Dekleta pogosteje uporabljajo geslo z njim znano besedo kakor fantje, medtem ko se fantje raje poslužujejo številskih gesel. Več podatkov lahko vidimo tudi na tabeli 22.

Tabela 22: Izgled gesla

Izgled gesla	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
geslo, ki vsebuje moje osebne podatke	7	14	10	14	17	14
geslo, ki vsebuje meni znano besedo	15	30	28	40	43	36
geslo, ki vsebuje številke	13	26	11	10	24	20
geslo, katerega beseda je sestavljena iz malih in velikih črk	6	12	8	12	14	12
geslo, ki vsebuje črke, številke	18	38	30	43	48	**40**
geslo, ki vsebuje črke, številke in druge znake	12	24	13	19	25	21
ne uporabljam gesla	3	6	4	6	7	6
ne vem	8	16	6	9	14	12

Opomba: Odstotek je izračunan kot število odgovorov za odgovor deljeno s številom anketirancev

4.18 Uporaba zaščitnih programov

Vsak učenec je lahko navedel več različnih zaščit, saj je bilo možnih več odgovorov. Iz tabele 23 lahko razberemo, da nekaj več kot 80 % učencev uporablja redno posodobljen antivirusni program, več kot polovica požarni zid, le četrtina ima v spletnem brskalniku nastavljen filter za neprimerne vsebine. Vse ostale zaščite uporablja skoraj četrtina vprašanih. Najmanj uporabljen je nepiratski operacijski sistem (13 %). 24 % uporablja tudi filter za nezaželeno pošto, ki je po navadi samodejno nastavljen v nastavitvah elektronske pošte in protivohunski program. Enak delež uporablja protivohunske programe. Podatki kažejo tudi na to, da fantje posvečajo večjo pozornost žaščiti računalnika kot dekleta.

Tabela 23: Uporaba zaščitnih programov

Zaščitni program	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
redno posodobljen antivirusni program	41	82	56	81	97	**82**
požarni zid	35	70	33	48	68	57
filter za nezaželeno pošto	12	24	17	25	29	24
protivohunski program	15	30	14	20	29	24
nepiratski operacijski sistem	9	18	7	10	16	**13**
v spletnem brskalniku filter za neprimerne vsebine	14	28	16	23	30	25

4.19 Pomoč v primeru zlorabe

Na vprašanje, kam bi se obrnili po pomoč v primeru zlorabe preko spleta, so učenci večinoma odgovorili k družinskim članom (45 %), samo štirje pa bi prijavili zlorabo imetniku strani. 10 % učencev bi težavo rešilo samo. Le 17 % učencev bi se zaupalo prijateljem, 22 (19 %) pa bi vprašalo za pomoč na spletno stran, ki pomaga v primeru zlorab. Pod odgovor drugo so učenci navajali šolsko psihologinjo, ljudi, ki se na to spoznajo, državne organe.
Dekleta so bolj navezane na družino, saj bi se kar 16 % več deklet kakor fantov zaupalo družinskim članom, medtem ko bi dvakrat več fantov kot deklet reševalo težavo sami. Natančnejši podatki o tovrstni temi so predstavljeni v tabeli 24 in diagramu 7.

Tabela 24: Izbira pomoči v primeru zlorabe

Pomoč	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
k družinskim članom	18	36	36	52	54	45
k prijateljem	7	14	13	19	20	17
na spletno stran, ki pomaga v primeru zlorab	10	20	12	17	22	19
imetniku spletne strani	3	6	1	1	4	3
težavo bi rešil/a sam/a	7	14	5	7	12	10
drugo	5	10	2	3	7	6

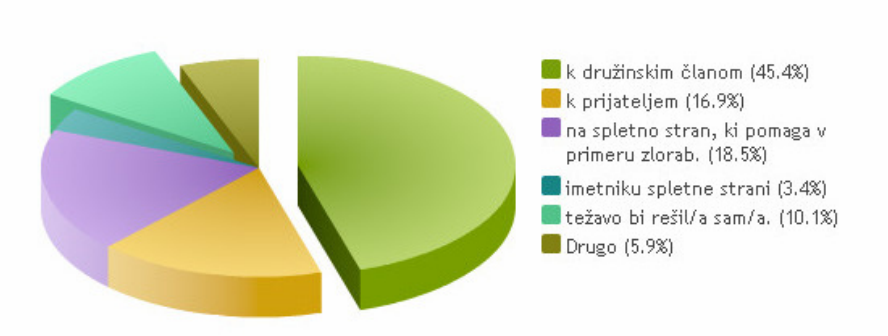

Diagram 7: Izbira pomoči v primeru zlorabe

4.20 Obravnavanje varne uporabe interneta pri pouku oziroma razrednih urah

Na tabeli 25 in diagramu 8 lahko razberemo, da malo več kot polovica učencev trdi, da smo pri pouku obravnavali tudi varno uporabo interneta, 45 % pa trdi nasprotno. Več deklet je bilo priča, da smo pri pouku obravnavali tudi varno rabo interneta.

Tabela 25: Obravnava varne uporabe interneta pri pouku oziroma razrednih urah

	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
da	26	52	40	58	66	56
ne	24	48	29	42	53	45

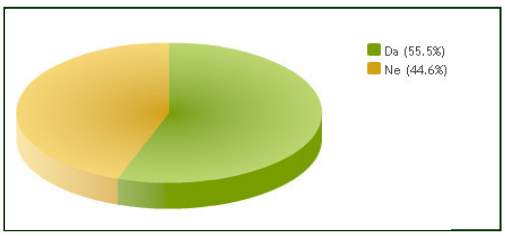

Diagram 8: Obravnava varne uporabe interneta pri pouku oziroma razrednih urah

4.21 Kazniva in nekazniva dejanja

Pri vprašanju, kaj učenci razumejo za kazniva dejanja, so lahko navedli več možnih odgovorov. 80 % učencev je mnenja, da je objavljanje otroške pornografije preko spleta kaznivo dejanje; objava rasističnih komentarjev in neprimerno izražanje preko spleta pa je kot kaznivo dejanje ocenila dobra polovica vprašanih. Prenos glasbe z interneta je nezakonit samo za 11 anketirancev, saj večina učencev nalaga brezplačno piratsko glasbo in noče verjeti dejstvu, da je uporaba piratskih programov (predvsem za komercialne namene) kazniva.
Neprimerno izražanje prek spleta in objavo otroške pornografije je več deklet kakor fantov označilo za kaznivo dejanje, medtem ko pa je objava rasističnih komentarjev bila ocenjena za kaznivo bolj s strani fantov kakor deklet. Slednji podatki so prikazani v tabeli 26.

V odgovoru »navedi še kako nezakonito dejanje prek spleta«, najdemo odgovore: vse mora biti legalno, objavljanje slik drugih brez njihovega dovoljenja, uporaba identitete druge osebe, »hekanje«, nadlegovanje preko interneta »fejkanje slik, videov« in podobno.

Tabela 26. Ločevanje med kaznivimi in nekaznivimi dejanji

Kaznivo/Nekaznivo dejanje	Moški		Ženske		Skupaj	
	število	%	število	%	število	%
prenos glasbe z interneta	7	14	4	6	11	9
kopiranje besedil z elektronskih virov, ki jih navedemo v nalogi	8	16	6	9	14	12
neprimerno izražanje in žaljenje prek spleta	23	46	41	60	64	54
objava otroške pornografije prek spleta	36	72	59	86	95	80
objava rasističnih komentarjev	30	60	34	33	64	54
navedi še kakšno nezakonito dejanje prek spleta	4	8	6	9	10	8

Opomba: Odstotek je izračunan kot število odgovorov za odgovor deljeno s številom anketirancev

5.22 Prijava otroške pornografije in sovražnega govora

Če anketiranci niso vedeli za spletno stran, na katero bi prijavili otroško pornografijo in sovražni govor, so lahko vprašanje preskočili. Tistih, ki so pravilno in resno odgovorili, je bilo le 10 (8 %). Spletne strani, ki so jih navedli so bile: spletno oko, safe.si, facebook, twitter, netlog, myspace, to sem jaz, varna raba interneta in nasvet za net. Najbolj pogost odgovor je bil safe.si.

5 TESTIRANJE HIPOTEZ

Upoštevajoč prikazane rezultate smo preverili postavljene hipoteze v poglavju o metodi:

H1: Vsi anketirani učenci uporabljajo internet, večinoma redno.
Hipotezo **H1 SPREJMEMO**, saj rezultati raziskave kažejo, da vsi anketiranci uporabljajo internet, le 4 % nekajkrat mesečno, vsi ostali bolj pogosto ali celo vsak dan.

H2: Največ anketirancev uporablja računalnik za komuniciranje preko spleta.
Kot vidimo v tabeli 3 največ anketirancev (76 %) uporablja internet za komuniciranje preko spleta, zato hipotezo **H2 SPREJMEMO.**

H3: Večina učencev sodeluje v socialnih omrežjih (facebook, twiter in drugih).
Socialna omrežja so, kot piše tudi v teoretičnem delu te raziskovalne naloge, zelo popularna, predvsem med mladostniki. Prav tako je iz tabele 6 razvidno, da kar 82 % sodeluje v socialnih omrežjih, zato hipotezo **H3 SPREJMEMO**.

H4: Učenci se zavedajo potencialnih nevarnosti na internetu. Večina jih je slišala že za primere kraje identitete, računalniškega piratstva, nadlegovanja preko spleta, nevarnih stikov s tujci, zasvojenosti z internetom, obsedenosti s pornografijoo na spletu in podobno.
Hipotezo **H4 SPREJMEMO**, saj tabela 7 kaže, da je večina učencev že slišala za primere kraje identitete (86 %), računalniškega piratstva (58 %), nadlegovanja preko spleta (80 %), nevarnih stikov s tujci (75 %) in zasvojenosti z internetom (87 %), obsedenosti s pornografijo na spletu (62 %) ter sovražnega govora (55 %).

H5: Med varnostnimi težavami internetnih uporabnikov sta najpogostejši neželena pošta ter virusi.
Iz tabele 9 je možno razbrati, da največ težav anketirancem povzročajo virusi (57 %) in neželena pošta (34 %), hipotezo **H5 SPREJMEMO**.

H6: Nihče od učencev še ni naletel preko interneta na otroško pornografijo.
Na osnovi podatkov iz tabele 14, kjer vidimo, da je že 16 učencev (13 %) že naletelo na otroško pornografijo hipoteze, H6 **NE SPREJMEMO**.

H7: Za učence je največja varnostna težava kraja gesla oziroma identitete.
Ker je na podlagi tabele 10 razvidno, da je kraja identitete oziroma gesla na tretjem mestu po pomembnosti, na prvem pa so virusi, trojanski konji in črvi, hipoteze H7 **NE SPREJMEMO**.

H8: Večina učencev je že razkrila svoje ime in spol na spletu.

Hipotezo H8 **SPREJMEMO**, saj je iz tabele 16 v raziskovali nalogi videti, da je večina učencev že razkrila svoje ime in spol na spletu (85 % oziroma 86 % učencev je razkrilo).

H9: Večina učencev zaupa svoje geslo še komu drugemu.

Hipoteze H9 **NE SPREJMEMO**, saj v tabeli 21 lahko preberemo, da je samo 39 % vprašanih zaupalo svoje geslo drugi osebi, 62 % učencev pa je bolj previdnih oziroma ne vedo, če so ga že nekomu zaupali.

H10: Večina učencev uporablja geslo, ki vsebuje njihove osebne podatke.

Hipoteze H10 prav tako **NE SPREJMEMO**, ker samo 14 % učencev uporablja geslo, ki vsebuje njihove osebne podatke, medtem ko pa večina uporablja geslo sestavljeno iz črk in številk oziroma kako drugače oblikovano geslo (tabela 22).

H11: Anketiranci nimajo dovolj zaščitenih računalnikov.

Ker je iz tabele 23 v raziskovalni nalogi razvidno, da 82 % učencev uporablja antivirusni program (ki je osnova za zaščito računalnika), 57 % učencev pa uporablja požarni zid. Večina ima antivirusni program, veliko pa jih nima filtra za nezaželeno pošto, filtra za neprimerne vsebine, protivohunskega programa ter nepiratskega operacijskega sistema. Hipotezo **H11 DELNO SPREJMEMO.**

H12: Večina učencev nalaga nezakonito avdio video vsebino.

V teoretičnem delu raziskovalne naloge smo zapisali, da veliko mladostnikov nalaga glasbo, filme in drugo na nezakonit način. Prav tako pa lahko v tabeli 17 zasledimo, da manj kot tretjina anketiranih še ni nalagala nedovoljene avidio in video vsebine. 44 % anketirancev ne nalaga piratskih programov, vsi ostali nalagajo nezakonit piratski material. Hipotezo H12 **SPREJMEMO**.

H13: V primeru zlorabe bi učenci rešili težavo sami.

V tabeli 24 lahko vidimo, da bi samo 10 % učencev v primeru zlorabe težavo rešilo samo, večina (45 %) pa bi se obrnila po pomoč k družinskim članom. Zato hipoteze H13 **NE SPREJMEMO.**

H14: Večina ne bi znala prijaviti sovražnega govora ali otroške pornografije.

Iz rezultatov v informativnem polju v anketi je videti, da večina učencev ne bi vedelo, kje prijaviti sovražni govor ali otroško pronografijo, mnogi pa vprašanja niso niti jemljali resno. Hipotezo H14 **SPREJMEMO**.

6 RAZPRAVA IN ZAKLJUČEK

Ugotovitve naše raziskave kažejo, da vsi anketiranci uporabljajo internet, 95 % anketirancev med 12. in 15. letom uporablja internet redno. Ta rezultat potrjuje tudi podatke Statističnega urada RS (1. četrtletje 2007), ki navajajo, da 90 % uporabnikov med 10 in 15 letom redno uporablja internet. Med obema rezultatoma je nekaj razlike morebiti zaradi še večje popularizacije in razvoja interneta.

Večina anketirancev uporablja internet vsak dan, kar je glede na današnjo navezanost na tehnološke pripomočke samoumevno. Nekaj otrok zaradi zunajšolskih aktivnosti ali pa nadzora staršev ne obiskuje vsak dan interneta, ampak skoraj vsak dan (30 %) ali pa nekajkrat tedensko (24 %). Tisti 4 % odstotki, ki uporabljajo internet samo nekajkrat mesečno so verjetno pod strogim starševskim nadzorom ali pa imajo zaradi slabega delovanja računalnika možnost obiskovati računalnik tako malokrat.

Na osnovi rezultata, ki navaja, da 76 % učencev uporablja internet za spletno komuniciranje, smo sprejeli hipotezo, da največ anketirancev uporablja računalnik za komuniciranje preko spleta, medtem ko Kovačič idr. (2008) navajajo, da največ mladih uporablja internet za izmenjavo glasbenih in video datotek, vendar omenja tudi komuniciranje preko spleta za popularno dejavnost mladih. Kar 82 % anketirancev navaja, da sodelujejo v socialnih omrežjih, kar potrjuje hipotezo: ”Večina učencev sodeluje v socialnih omrežjih (facebook, twiter in drugih)”.

Učenci se zavedajo potencialnih nevarnosti na internetu, tako da smo sprejeli četrto hipotezo, saj je večina učencev že slišala za primere kraje identitete (86 %), računalniškega piratstva (58 %), nadlegovanja preko spleta (80 %), nevarnih stikov s tujci (75 %) in zasvojenosti z internetom (87 %), otroške pornografije (62 %) in sovražnega govora (55 %). Ti rezultati potrjujejo navedbe Kovačiča idr. (2008), da se otroci zavedajo potencialnih nevarnosti na internetu. Naši anketiranci ocenjujejo varnost interneta s povprečno oceno 3, 12 na lestvici od 1 do 5, fantje pa smatrajo internet za bolj varen kot dekleta.

Virusi, črvi in trojanski konji predstavljajo učencem največjo varnostno težavo, sledijo jim nevarni stiki s tujci in kraja identitete, anketiranci pa se od težav najpogosteje srečujejo z virusi in nezaželeno pošto. Čeprav se pogosto srečujejo z nezaželeno pošto, jim to ne predstavlja velike varnostne težave.

Potrjena hipoteza, da sta neželena pošta ter virusi najpogostejši varnostni težavi anketirancev (virusi 57 %, neželena pošta 34 %), potrjuje teoretična izhodišča, da predstavljata prejemanje neželene pošte ter računalniški virusi največjo varnostno težavo internetnim uporabnikom.

Dejstvo, da je kar 9 učencev naletelo na spolno nadlegovanje preko spleta je grozljivo in na žalost resnično, saj dandanes najstniki prek socialnih omrežij sprejemajo tuje osebe in brez pomisleka komunicirajo z njimi. Včasih pride do spolnega nadlegovanja, ki najstnike prizadene in zmede, a tega ne prijavijo, temveč osebo samo izbrišejo iz seznama prijateljev. S tem ne rešijo

težave, saj oseba nadaljuje s svojim nadlegovanjem nekje drugje. Velikokrat pride do tega prav zaradi tega, ker najstniki prikrijejo svojo starost in jo povišajo v želeno (nizka samozavest). V večini so to dekleta.
Nevarno je še posebej, če najstniki razkrijejo preko spleta tudi kakšno informacijo, preko katere bi jih lahko dobil nadlegovalec/-ka. Kot primer lahko vzamemo rezultate iz naše raziskovalne naloge, kjer je 14 najstnikov že razkrilo naslov bivališča, 56 (55 %) pa svoj elektronski naslov - kar privede do neželene pošte. Prav tako je večina že razkrila svoje ime (85 %) in spol (86 %) na spletu, kar je tudi osnova za hipotezo H8, ki smo jo sprejeli. Kar 31 % se je že sramovalo svojih dejanj. Anketiranci so na spletu razkrivali svoje osebne podatke kljub temu, da smatrajo razkrivanje osebnih podatkov neznancem za najbolj nevarno dejanje na spletu. 39 % vprašanih je tudi zaupalo svoje geslo drugi osebi.

V nasprotju s podatki Statističnega urada RS (1. četrtletje 2007) je 8 % anketirancem druga oseba izkoristila zaupanje in objavila njihove podatke, medtem ko pa je Statistični urad poročal o tem, da je slednje doživela kar četrtina mladih med 10 in 20 leti. Ob tej primerjavi je vsekakor potrebno upoštevati razliko v letih med raziskavama.

Strašljivo je dejstvo, da je kar 16 učencev (13 %) naletelo na otroško pornografijo na spletu. Nanjo so verjetno naleteli kot pri neželenih vsebinah preko kakšnega brskalnika ali neželene elektronske pošte. Velikokrat nekateri ljudje izkoristijo socialna omrežja (kot na primer facebook) in tam objavijo nezaželene vsebine, ki jih najstniki posredujejo naprej, dokler ne obkrožijo (in pretresejo) večine uporabnikov. Velikokrat izkoristijo socialna omrežja v komercialne namene in sicer tako, da ustvarijo lažni profil popularnega najstnika, ki nato objavlja slike o določenem izdelku, ki ga hoče trgovina promovirati. Socialna omrežja so uporabljena tudi za spodkopavanje samozavesti in spodbujanje najstnikov k skrajnim dejanji.
Na osnovi podatka o tem, da manj kot tretjina anketiranih še ni nalagala nedovoljene avdio in video vsebine, 44 % anketirancev ni nalagala piratskih programov, vsi ostali pa so že nalagali nezakonit piratski material, smo sprejeli hipotezo H12: "Večina učencev nalaga nezakonit piratski material."
Nalaganje glasbe in drugih stvari na nezakonit brezplačen način je dandanes tako pogosto verjetno zaradi tega, ker najstniki poslušajo ogromno glasbe in gledajo veliko filmov, torej bi plačevanje za tovrstne storitve s časom nakopičilo precej denarja, ki ga veliko staršev ne bi rado porabilo za take malenkosti. Verjetno se je v času recesije nalaganje brezplačnega piratskega materiala povečalo.
Zaskrbljujoče je to, da 3 učenci igrajo tudi igre na srečo preko spleta, ki lahko hitro privedejo do hude odvisnosti.

82 % učencev uporablja antivirusni program (ki je osnova za zaščito računalnika), 57 % učencev pa uporablja požarni zid. Večina ima antivirusni program, veliko pa jih nima filtra za nezaželeno

pošto, filtra za neprimerne vsebine, protivohunskega programa ter nepiratskega operacijskega sistema, na varnostne težave pa je naletelo kar 45 % anketirancev. SURS (1. četrtletje 2007) je zbral podatke, da je imelo samo 29 % oseb med 16 in 74 letom zaščiten računalnik, na varnostne težave pa je naletelo samo 35 % oseb istega starostnega obdobja. V H11 smo predpostavljali, da anketiranci nimajo dovolj zaščitenih računalnikov, zato smo hipotezo delno sprejeli. Kar 10 % učencev so že kdaj ukradli geslo in s tem identiteto. Ta podatek nas spet pripelje do socialnih omrežij, kjer učenci vidijo, da je njihov prijatelj objavil zanimiv link. Ko link kliknejo, s tem lahko sprožijo možnost, da tretja oseba prevzame identiteto.
Še posebej bi opozorili na o vprašanje v anketi: "Ali pri pouku oziroma razrednih urah posvečate pozornost varni rabi interneta?" Odgovor je 56 % pozitiven, kar kaže na rahlo neodločenost. Res je, da varne uporabe interneta v šoli nismo nikoli obravnavali kot zelo pomembno dejstvo, ampak samo v sklopu z drugimi življenjskimi težavami.
Glede na to, da 9 % anketirancev uporablja geslo z osebnimi podatki, je 14 učencev razkrilo naslov bivališča preko spleta, je 9 učencev naletelo na spolno nadlegovanje preko interneta, je 40 % zaupalo svoje geslo drugi osebi in je bilo 16 % najstnikov že nadlegovanih preko spleta, a večina učencev ne bi vedela, kje prijaviti sovražni govor ali otroško pornografijo, predlagamo, da bi imeli na šoli vsaj eno osveščanje o varni uporabi interneta. Glede na to, da je internet dandanes glavna atrakcija najstnikov, bi se zlahka dalo pogovarjati z njimi o tej temi in bi jim bila tudi zanimiva.
Glede na to, da je kar 45 % anketirancev naletelo na neprimerno vsebino (tabela 8) in da samo četrtina uporablja filter na spletnem brskalniku za neželene vsebine, bi bilo potrebno tudi sestaviti varen spletni brskalnik z močnimi filtri za neprimerne vsebine, ki bi učencem zagotavljal varno brskanje po spletu. Lahko bi organizirali varno spletno klepetalnico, kjer bi se učenci med seboj pogovarjali o internetnih težavah in jih razreševali. Verjetno bi starejši učenci tako idejo zavračali, a bi spletna klepetalnica za mlajše učence vsekakor delovala pozitivno, saj bi se tako že zgodaj naučila glavnih pravil o zaščiti in razreševanju varnostnih težav.

Lahko pa bi raziskali še nadzor staršev na računalniku, ali učenci vpišejo svojo pravo starost na socialnih omrežjih in ali sprejemajo tudi tujce med prijatelje. Mogoče bi se lahko bolj poglobili v socialna omrežja, saj je tam veliko internetnih pasti. Zanimivo bi bilo tudi proučevanje zasvojenosti z internetom.

Zaključimo lahko, da je naša raziskovalna naloga dosegla svoj namen, proučiti stanje na področju internetnih nevarnosti in zaščite pred temi pastmi med našimi učenci. Z ugotovitvami raziskave bomo seznanili učence po oddelkih v okviru ur oddelčnih skupnosti oziroma dneva Varne rabe interneta, po možnosti tudi učitelje in njihove starše. To bi bil le majhen korak na poti osveščanja v zvezi z obravnavano problematiko, ki ji bo v bodoče potrebno posvetiti več pozornosti.

LITERATURA IN VIRI

Colombain, J.(2009). *Moj računalnik, internet in jaz*. Ljubljana: Tehniška založba Slovenije.

Centrih, E.(17.2.2011). *Varna uporaba interneta*. Cosmo matura. Pridobljeno iz http://matura.cosmopolitan.si/lajf/varna-uporaba-interneta/

Jeriček, H. (2003). Zasvojenost z internetom, *Vzgoja, 19, str.* 42-43.

Kazenski zakonik Republike Slovenije. Uradni list RS, št. 55/2008 z dne 4. 6. 2008. Pridobljeno iz http://www.uradni-list.si/1/objava.jsp?urlurid=20082296

Kočevar, V. (2005). *Verbalno nasilje v internetnih forumih*. Diplomsko delo, Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede. Pridobljeno iz http://dk.fdv.uni-lj.si/dela/Kocevar-Valentina.PDF

Kovačič, M., idr.(2008). *Deskanje po varnih vodah*. Ljubljana. Pridobljeno iz http://www.safe.si/uploadi/editor/1213086334Deskanje_po_varnih_vodah.pdf)

SAFE-SI. Pridobljeno15.12.2011 iz http://www.safe.si/

MojaAnketa.si (3.2.2011). Pridobljeno iz http://www.mojaanketa.si

Varna uporaba interneta (3.2.2011). Študent. Pridobljeno iz http://www.student.si/preberi-si/aktualno/varna-uporaba-interneta.html

Zdešar, P. in Zupan,G.(5.10.2007). *Uporaba interneta v gospodinjstvih*. Statistični urad Republike Slovenije, 1. objava. Pridobljeno iz http://www.stat.si/novica_prikazi.aspx?id=1185

PRILOGE

Priloga 1: Anketni vprašalnik

Varna raba interneta

Sem Celeste Sanja, učenka 8.razreda osnovne šole Solkan. V okviru diferenciranega dela pri matematiki izvajam raziskavo o varni rabi interneta.
Da bi v zvezi z obravnavanim problemom pridobila natančne in objektivne podatke, te prosim, da odgovarjaš iskreno, saj je anketa anonimna.

Vnesite svoje informacije:

Spol ----
Starost ----

1. Ali uporabljaš internet?

- ☐ da
- ☐ ne

2. Kako pogosto uporabljaš internet?

- ☐ nikoli
- ☐ nekajkrat mesečno
- ☐ nekajkrat tedensko
- ☐ skoraj vsak dan
- ☐ vsak dan

3. V kakšne namene uporabljaš internet? (več možnih odgovorov)

- ☐ za izmenjavo glasbenih datotek in filmov
- ☐ za prenašanje igric, filmov, glasbe
- ☐ za elektronsko pošto
- ☐ za izobraževanje
- ☐ za komuniciranje prek spleta (klepefalnice, forumi, spletne skupnosti npr. facebook)
- ☐ za iskanje informacij
- ☐ za igranje iger na srečo
- ☐ igranje spletnih igric

4. Sodeluješ v:

	da	ne	včasih
spletnih klepetalnicah	☐	☐	☐
spletnih forumih	☐	☐	☐
socialnih omrežjih (npr. facebook, twiter,..)	☐	☐	☐

5. Oceni, koliko se ti zdi internet varen:

	1	2	3	4	5	
ni varen	☐	☐	☐	☐	☐	zelo varen

6. Ali si že slišal/a za primere? (več možnih odgovorov)

- ☐ kraje gesla za dostop do interneta, kraje identitete
- ☐ nadlegovanje preko interneta
- ☐ nevarnih stikov s tujci
- ☐ računalniškega piratstva
- ☐ zasvojenosti z internetom
- ☐ obsedenosti s pornografijo na internetu
- ☐ sovražnega govora
- ☐ drugo

7. Kolikokrat si naletel/a na neprimerne spletne vsebine ali varnostne težave na internetu:

- ☐ 1-4krat
- ☐ 5-9krat
- ☐ več kot 10krat
- ☐ nikoli
- ☐ ne vem
- ☐ drugo

8. Na katere varnostne težave si že naletel/a? (več možnih odgovorov)

- ☐ neželena pošta (spam)
- ☐ virusi, trojanski konj, črvi
- ☐ kraja gesla, identitete, občutljivih podatkov
- ☐ nevarne stike s tujci
- ☐ nadlegovanje prek interneta
- ☐ druga oseba je zlorabila tvoje zaupanje in na internetu objavila tvoje osebne podatke
- ☐ nobene
- ☐ drugo

9. Kaj ti predstavlja največjo varnostno težavo? (1 - največja težava; 6 - najmanjša težava)

---	prejemanje neželene pošte
	virusi, trojanski konj, črvi
---	neželene vsebine
	kraja gesla, identitete
---	nadlegovanje prek interneta
	nevarni stiki s tujci

10. Označi kolikokrat si že bil/a prevaran/a prek spleta:

	več kot desetkrat	6-10	1-5	nikoli
prenos virusov na tvoj računalnik	☐	☐	☐	☐
nezaželjena pošta	☐	☐	☐	☐
kraja gesla, identitete	☐	☐	☐	☐
kraja denarja	☐	☐	☐	☐
nadlegovanje prek spleta	☐	☐	☐	☐

11. Si že naletel/a na internetu na: (več možnih odgovorov)

- ☐ draženje
- ☐ norčevanje iz posameznikov
- ☐ pošiljanje nezaželenih sporočil
- ☐ pošiljanje prizorov vrstniškega nasilja
- ☐ spolno nadlegovanje
- ☐ otroško pornografijo
- ☐ sovražni govor
- ☐ drugo

12. Označi, katero dejanje se ti zdi najbolj nevarno (1 - najbolj nevarno; 5- najmanj nevarno):

- --- neprimerno obnašanje na internetu
- kršenje avtorskih pravic
- --- razkritje osebnih podatkov neznancem
- pozabiti svoje geslo
- --- odvisnost

13. Izberi tiste osebne podatke, ki si jih razkril/a na spletu: (več možnih odgovorov)

- ☐ ime
- ☐ spol
- ☐ starost
- ☐ naslov bivališča
- ☐ elektronski naslov
- ☐ nič od tega
- ☐ drugo

14. Označi kako pogosto nalagaš nelegalen brezplačen material z interneta:

	vsak dan	pogosto	redno	nikoli
glasbo	☐	☐	☐	☐
filme	☐	☐	☐	☐
videoigrice	☐	☐	☐	☐
programe	☐	☐	☐	☐

15. Si se že kdaj sramoval/a svojih dejanj na klepetalnicah ali blogih?

- ☐ da
- ☐ nekajkrat
- ☐ nikoli

16. Ali si že kdaj zaupal/a svoje geslo kakšni osebi?

- ☐ da
- ☐ ne
- ☐ ne vem

17. Kakšno geslo uporabljaš? (več možnih odgovorov)

- ☐ geslo, ki vsebuje moje osebne podatke
- ☐ geslo, ki vsebuje meni znano besedo
- ☐ geslo, ki vsebuje številke
- ☐ geslo, katerega beseda je sestavljena iz malih in velikih črk
- ☐ geslo, ki vsebuje črke, številke
- ☐ geslo, ki vsebuje črke, številke in druge znake
- ☐ ne uporabljam gesla
- ☐ ne vem

18. Označi zaščitne programe, ki jih uporabljaš. (več možnih odgovorov)

- ☐ antivirusni program, ga redno posodabljam
- ☐ požarni zid
- ☐ filter za nezaželeno pošto
- ☐ protivohunski program
- ☐ nepiratski operacijski sistem
- ☐ v spletnem brskalniku filter za neprimerne vsebine

19. V primeru zlorabe prek spleta, kam bi se obrnil/a po pomoč?

- ☐ k družinskim članom
- ☐ k prijateljem
- ☐ na spletno stran, ki pomaga v primeru zlorab.
- ☐ imetniku spletne strani
- ☐ težavo bi rešil/a sam/a.
- ☐ Drugo

20. Ali pri pouku oziroma razrednih urah posvečate pozornost varni rabi interneta?

- ☐ Da
- ☐ Ne

21. Označi kaj smatraš za kazniva dejanja: (več možnih odgovorov)

- ☐ prenos glasbe z interneta
- ☐ kopiranje besedil z elektronskih virov, ki jih navedemo v nalogi
- ☐ neprimerno izražanje in žaljenje prek spleta
- ☐ objava otroške pornografije prek spleta
- ☐ objava rasističnih komentarjev
- ☐ navedi še kakšno nezakonito dejanje prek spleta

22. Ali znaš navesti vsaj eno spletno stran, na kateri lahko prijaviš otroško pornografijo in sovražni govor?

Najlepša hvala za sodelovanje.