Upoznatost studenata s metodama zaštite podataka

Ivančić, Martin

SVEUČILIŠTE U ZAGREBU

FILOZOFSKI FAKULTET

ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

Ak. god. 2018./ 2019.

Martin Ivančić

UPOZNATOST STUDENATA S METODAMA ZAŠTITE PODATAKA

Završni rad

Mentor: dr. sc. Vjera Lopina

Zagreb, 2019.

Sadržaj

1. Uvod 1
2. Maliciozni računalni programi (engl. *malware*) 4
2.1. Virusi, trojanci i crvi 5
2.1.1. Virusi 5
2.1.2. Trojanci 5
2.1.3. Crvi 6
2.2. Ostale vrste malwarea 7
2.2.1. Spyware 7
2.2.2. Ransomware 7
2.2.3. Adware 8
3. Sigurno ponašanje na internetu 8
4. Antivirusni alati, firewall i obrana od virusa/malicioznih programa 10
5. Javne Wi-Fi mreže (engl. public wi-fi networks) 12
6. Lančane poruke i spam 14
7. Anketno istraživanje 16
7.1. Rezultati ankete 17
8. Zaključak 42
9. Literatura 43

1. Uvod

U današnje vrijeme za koje možemo reći da je digitalno doba, suočavamo se s jednom posve drugačijom vrstom opasnosti. Kriminal više ne uključuje samo oružane pljačke, provale u stanove ili krađe automobila nego se on proširio kako bi uključio jednu posve novu vrstu kriminala. Ova vrsta kriminala dobila je vlastitu kategoriju pod nazivom kibernetički kriminal (engl. *cyber crime*). U knjizi pod naslovom *The Defender's Dilemma*, napisano je kako su brige oko sigurnosti na internetu započele 1988. godine, u studenom, s nastankom Morrisovog crva (Libicki, Ablon and Webb 23).[1] Kao posljedica toga javlja se želja i zanimanje o zaštiti protiv ovakve vrste opasnosti. Internetska sigurnost i zaštita od zlonamjernih pojedinaca i programa (engl. *software*) nešto je što mnogi korisnici uzimaju zdravo za gotovo, pogotovo ako su nešto manje zainteresirani kad su u pitanju računala ili ako su nedovoljno informatički opismenjeni. S 21. stoljećem, broj prijetnji za samo računalo i korisnika dosegao je nepredviđenu razinu, uglavnom zbog nezaustavljivog napretka tehnologije koji je doveo do nikad veće raznovrsnosti i dostupnosti raznih alata, opcija i mogućnosti. Ovaj razvoj događaja opisan je u knjizi *Hackers wanted* koja govori o porastu potražnje za računalnim ekspertima. Govori kako je jedan od razloga za porast potražnje upravo razvoj računala i povezanosti. Više podataka se pohranjuje i više procesa je kontrolirano na način koji omogućava pristup osobama koje pristup ne bi smjele imati. Zbog ove činjenice, broj mogućnosti za zlodjela je doživio drastičan porast kao i visina samog rizika zbog spremanja velikog broja informacija o velikom broju korisnika (Libicki, Senty and Pollak 5).[2] Kad spojimo ovakvu količinu podataka s određenim pojedincima čija kreativnost i želja za izazivanjem kaosa, novcem, slavom ili bilo čim drugim nadmašuju prosjek tada dolazimo da opasnih situacija koje su okarakterizirane prijetnjama u raznim oblicima. Ako se analiziraju metode koje se koriste za zlonamjerne ciljeve i ako ih se usporedi sa sličnim pokušajima u prošlosti, može se vidjeti kako su same metode napredovale zajedno s pojedincima

[1] https://www.jstor.org/stable/pdf/10.7249/j.ctt15r3x78.11.pdf?ab_segments=0%2Fdefault-2%2Fcontrol&refreqid=search%3A9a740349b32632c5c8b11e28836358d9

[2] https://www.jstor.org/stable/pdf/10.7249/j.ctt7zvzmj.9.pdf?ab_segments=0%2Fdefault-2%2Fcontrol&refreqid=search%3A9a740349b32632c5c8b11e28836358d9

i njihovim znanjem te napretkom tehnologije. Pojedinci koji su bili posvećeni ovom području upsjeli su određene metode usavršiti do zavidne razine. Neke metode kojima se korisnike pokušava navesti da otkriju neke privatne podatke ili da izlože svoje računalo su toliko sofisticirane da je ponekad čak i iskusnom korisniku teško raspoznati nešto stvarno (engl. *legit*) od neke vrste prevare (engl. *scam*). Baš zbog ovog razloga, cyber kriminal je problem koji treba shvatiti vrlo ozbiljno i definirati ga kao jedan od velikih i vodećih problema s kojim se moramo nositi u digitalnom dobu 21. stoljeća.

Agencija Ipsos, zajedno s agencijom ICJS, nedavno je provela istraživanje o cyber kriminalu kako bi odredili koliki je postotak organizacija bio zahvaćen nekom vrstom cyber kriminala. Ovo istraživanje služilo je kao nastavak na istraživanja provedena prethodnih godina te je pokazalo da još uvijek postoji konstantna prijetnja od cyber napada. Gotovo trećina organizacija (32%) i petina humanitarnih organizacija (22%) bile su žrtve kibernetičkih napada u posljednjih 12 mjeseci.[3] Ako promotrimo Hrvatsku, iz istraživanja iz 2018. godine koje je provela tvrtka PwC, vidljivo je da je gotovo polovica (47%) hrvatskih ispitanika izjavila kako su im kibernetički napadi ozbiljno naštetili i poremetili poslovne planove. Iako se dosta njih izjasnilo o problemima s kibernetičkim napadima, samo 53% ispitanika istaknulo je kako bi podijelili informacije o pretrpljenim napadima s državnim tijelima.[4] Ovdje se susrećemo s problemom gdje pojedine organizacije često zataje određeni napad ili probleme kako to ne bi imalo utjecaja na njihovu reputaciju i kako ne bi izgubili svoje korisnike i njihovo povjerenje. Ovakva vrsta ponašanja zapravo otežava samu situaciju i usporava borbu s kibernetičkim kriminalom. Prešućivanje prijetnji i napada naposljetku može rezultirati još lošijom situacijom za pojedinu tvrtku, a ponajprije za same korisnike neke usluge.

Zbog svega navedenog, važno je naučiti kako se sigurno ponašati na internetu u što ranijoj dobi, budući da gotovo svi koriste internet na dnevnoj bazi, bilo poslovno ili privatno. Za potrebe ovog rada provedeno je istraživanje u obliku ankete. Htjelo se istražiti koliko su studenti upoznati sa sigurnim načinom korištenja interneta. Anketu su ispunjavali studenti preddiplomskog i diplomskog studija informacijskih znanosti kao i studenti s drugih smjerova na Filozofskom

[3] https://www.ipsos.com/ipsos-mori/en-uk/cyber-security-breaches-survey-2019

[4] http://www.poslovni.hr/hrvatska/u-2-godine-vise-od-pola-hrvatskih-organizacija-bile-su-zrtve-prijevare-i-kriminala-345047

fakultetu te također studenti s drugih fakulteta. Sama anketa služi ispitivanju opće informiranosti studenata o sigurnosti na internetu. Ispitat će se korisničke navike korištenja računala odnosno interneta, poznavanje raznih opasnosti, prijašnja pozitivna ili negativna iskustva itd. Vidjet će se koliki je postotak studenata ponekad postupio na način koji bi se mogao opisati kao rizično ponašanje. Studenti će također moći ocijeniti stupanj vlastitog znanja o internetskoj sigurnosti. Rezultati će biti analizirani na razini pitanja i svako anketno pitanje bit će komentirano za sebe. Svako će pitanje također imati vizualnu reprezentaciju odgovora u obliku grafa, bilo da se radi o grafu preuzetom iz same ankete ili posebno izrađenom zbog nekih restrikcija. Prije same analize rezultata ankete, bit će definirani neki općeniti pojmovi koji su bitni za samu temu. Definirat će se maliciozni programi i opisati same podvrste kao što su npr. virusi. Bit će nabrojani najčešći načini zaraze računala kao i najrizičnije vrste ponašanja na internetu. Nakon toga bit će prikazani načini zaštite od ovakvih napada kao i koraci koje korisnik može poduzeti kako bi smanjio sveukupni rizik i prilagodio svoje ponašanje nekim sigurnosnim pravilima i savjetima. Na samom kraju, nakon analize ankete, cijeli rad će biti sažet i zaključen uz pomoć rezultata same ankete.

2. Maliciozni računalni programi (engl. *malware*)

Ljudi koji rade s računalima, često se susreću s pojmom virus. Neki pojedinci ponekad koriste ovaj termin kako bi opisali nešto što uopće ne spada u skupinu virusa i tako zbunjuju i druge koji nisu sigurni u samu definiciju. Što je zapravo virus? Pojam virusa definirao je dr. Frederick Cohen napisavši kako je virus program koji ima sposobnost inficiranja drugih programa na način da ih modificira kako bi uključili kopiju njega samog. Ta kopija, po potrebi, može također biti modificirana.[5] Prema ovome se može zaključiti da su ovi programi dobili naziv virusi zbog sličnosti s biološkim virusima jer imaju funkciju odnosno sposobnost zaraze. Ono što se često dogodi, kako je već bilo napomenuto, je da neki ljudi zamijene neki drugi maliciozni program s virusom. Ovo se lako može pripisati činjenici da ti ljudi jednostavno nisu dovoljno informatički pismeni da bi znali određene razlike između ovih programa pa stoga sve stavljaju u istu kategoriju.

Maliciozni programi se zapravo dijele na nekoliko različitih podvrsta pa tako imamo već spomenute viruse, trojanske konje (trojance) i crve. Do zaraze malicioznim programima najčešće dolazi na nekoliko tipičnih načina: tijekom pretraživanja interneta i preuzimanja neprovjerenih datoteka, tijekom slanja i primanja e-mailova ili preko spojenih uređaja (npr. usb).[6] Također postoji još nekoliko vrsta zloćudnih programa, a u njih se ubrajaju ransomware, adware, spyware itd. Sva ova imena zapravo daju nagovještaj o kakvom se tipu programa radi.[7]

[5] https://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html
[6] https://www.britannica.com/technology/malware
[7] https://www.uscybersecurity.net/malware/

2.1. Virusi, trojanci i crvi

2.1.1. Virusi

Već je spomenuto kako su virusi programi koji inficiraju računalo tako da umnažaju sami sebe bez znanja korisnika. Kako bi se dočarala brzina kojom je broj virusa rastao, može se pogledati informacija o 1988. godini koju je plasirala tvrtka CVIA (The Computer Virus Industry Association). Naime, govore kako je 1988. bilo poznato samo 5 virusa u svijetu. Kroz tu godinu u prosjeku se pojavljivao jedan novi virus svaka dva mjeseca. Već 1990. godine, pojavljivala su se otprilike 2 nova virusa svakih tjedan dana. U siječnju 1988. bilo je 3100 prijavljenih infekcija virusom, dok je u prosincu iste godine taj broj narastao na 176.000 (Azarmsa 26).[8]

Virus se sastoji od 3 dijela, a oni uključuju:

1) Zarazni dio (engl. *self-propagating component*)
2) Nosivu komponentu (engl. *mission component*)
3) Funkciju za okidanje (engl. *trigger component*)[9]

2.1.2. Trojanci

Naziv trojanski konj dolazi iz epa o Trojanskom ratu gdje su grci „maskirali“ svoje vojnike unutar drvenog konja koji je predstavljen kao dar Trojancima. Kada su ga Trojanci uveli u grad, vojnici su preko noći izašli iz drvenog konja i osvojili Troju. Baš po uzoru na ovu priču

[8] https://www.jstor.org/stable/pdf/44425719.pdf?ab_segments=0%2Fdefault-2%2Fcontrol&refreqid=search%3A1249aa51debc0ba40ef26a3ccea1a09b

[9] https://books.google.hr/books?id=mK2QhS11JtsC&pg=PA194&lpg=PA194&dq=mission,+trigger+and+self+propagation+component&source=bl&ots=j1u1aS-n8z&sig=ACfU3U3fUVetXQ9FnrhTWKgyE6S-I3982A&hl=en&sa=X&ved=2ahUKEwiCpvH82PjjAhX3QhUIHfsYCHgQ6AEwDXoECAcQAQ#v=onepage&q=mission%2C%20trigger%20and%20self%20propagation%20component&f=false

funkcionira i sam malware zvan trojanac. On će se pretvarati da je neki korisni program ili aplikacija te vas navesti da ga pokrenete. Budući da se zapravo radi o prikrivenom malwareu, jednom kada ga pokrenete on izvršava svoju zlonamjernu funkciju, bilo da se radi o šteti prema računalu, krađi podataka ili nećem trećem.

Razlika koju je potrebno istaknuti između trojanca i virusa je ta da trojanca aktivira sam korisnik, dok se virus može aktivirati sam te također može umnažati samog sebe.[10]

2.1.3. Crvi

Računalni crv je vrsta malwarea koja širi svoje kopije preko internetske mreže s računala na računalo. Crv se može replicirati bez ikakve ljudske interakcije te se također ne mora prikačiti na program (engl. *software*) kako bi izazvao štetu. Crvi mogu modificirati ili brisati datoteke te čak i dodati dodatni maliciozni software na računalo. Ponekad im je cilj samo trošenje računalnih resursa tako da se repliciraju puno puta, a mogu i krasti podatke kao i instalirati stražnja vrata (engl. *backdoor*) i omogućiti hakerima pristup računalu.[11]

[10] https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html
[11] https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

2.2. Ostale vrste malwarea

2.2.1. Spyware

Kao što mu i samo ime govori, ovaj software služi za špijuniranje odnosno prikupljanje informacija o korisniku ili nekoj organizaciji bez znanja samog korisnika ili organizacije. Te informacije se nakon toga šalju nekoj trećoj strani te također mogu omogućiti pristup povjerljivim podatcima na uređaju bez znanja korisnika.[12]

2.2.2. Ransomware

Ovo je još jedan malware kojemu ime donekle otkriva o čemu se radi. Ransomware će zaključati vaše podatke i zaprijetiti njihovim objavljivanjem ili će vam samo blokirati pristup dok ne platite određeni iznos odnosno otkupninu (engl. *ransom*). Postoje jednostavniji oblici ovog malwarea koje nije problem zaobići no kod nekih složenijih oblika podaci bivaju enkriptirani i ne može im se pristupiti bez plaćanja otkupnine.[13]

[12] www.cisco.com/c/en/us/about/security-center/virus-differences.html
[13] 12

2.2.3. Adware

Posljednja vrsta malwarea u ovoj kategoriji je adware. Ovaj malware stvarat će prihod za svog kreatora na temelju reklama (engl. *advertisement*, skraćeno – *ad*) koje će „iskakati“ tijekom korištenja računala. Kreator može biti plaćen na temelju broja prikazanih reklama ili na temelju broja klikova na pojedinu reklamu.[14]

3. Sigurno ponašanje na internetu

Uz ovakav porast malwarea i straha od krađe i zlouporabe podataka, nije veliko iznenađenje da se ljudi žele dodatno informirati o tome kako ostati siguran na internetu. Često se održavaju razna predavanja na tu temu i problem kibernetičkog kriminala sve se ozbiljnije shvaća diljem svijeta.

Sigurnost na internetu zapravo ima dvije svrhe. Prva je sačuvati povjerljivost/tajnost podataka, a druga je sačuvati cjelovitost (engl. *integrity*) podataka (Hamilton 50).[15]

Sigurno ponašanje na internetu na razini pojedinca zapravo se svodi na dvije stvari:

1) pravovremeno poznavanje internetske sigurnosti kako bismo mogli izbjeći potencijalne zamke i prepoznati što ulazi pod rizično ponašanje
2) adekvatni programi za zaštitu samog računala (firewall, antivirusni program...)

Ovo na prvi pogled ne djeluje previše komplicirano, ali trenutak neopreznosti i brzopletosti kod korisnika može rezultirati jako lošim posljedicama. Ako korisnik nije siguran u istinitost ili sigurnost neke stranice, ponude ili bilo čega drugog, najbolje je osloniti se na instinkt; ako nešto

[14] 12
[15] https://www.jstor.org/stable/pdf/23288059.pdf?ab_segments=0%2Fdefault-2%2Fcontrol&refreqid=search%3A65f6cbd1b8dc25272f29618ca8f13b0dcea1a0

djeluje predobro da bi bilo istinito, najčešće to i je. Ovo je jedan od čestih načina na koji sigurnost računala postane kompromitirana jer se zloćudni programi i njihovi kreatori često oslanjaju na ljudsku naivnost i znatiželju ili neke druge karakterne osobine kako bi zadobili povjerenje i samim time pristup računalu.

Kad biste informatičara upitali kako biti posve siguran od bilo kakve vrste malwarea, njegov odgovor bi vjerojatno bio: „ne spajajte se na internet“. U toj situaciji, vjerojatno biste mu uputili zbunjen pogled i pitali se kako on to misli da se računalo može koristiti bez pristupa internetu. Istina je da u današnje vrijeme koristimo internet gotovo svakodnevno i za puno različitih stvari. Trebate recept za neki kolač? Internet će vam pružiti stotine prijedloga. Trebate platiti račune, ali ne da vam se izaći iz kuće i otići do banke? Internetsko bankarstvo je odgovor. Želite javiti profesoru da vam nije upisao ocjenu, ali ne možete iz nekog razloga doći na konzultacije? I u ovom slučaju vam, još jednom, internet pristiže u pomoć nudeći vam opciju slanja digitalne pošte odnosno e-maila. Ako ikad sagledate svoje korištenje interneta, gotovo je nemoguće zamisliti kako bi vaš svakodnevni život izgledao bez njega. Upravo zato je ovaj odgovor toliko začuđujuć iako je to zapravo jedini potpuno djelotvoran način da se zaštitite od malwarea.

Sve ostalo, uključujući čak i obično pregledavanje web stranica, nosi sa sobom neku vrstu rizika baš kao što je napisao Peter Neumann u svom članku rekavši da je spajanje računala na internet jednako pozivnici za ulazak u sustav cijelom svijetu (51).[16]

Neki od najčešćih načina infekcije računala malwareom su:

1) dodatni programi (engl. *software*) koji dolazi s nekim besplatnim programom skinutim s interneta
2) peer-to-peer programi (npr. torrenti)
3) tuđi USB stickovi, DVD-ovi, eksterni diskovi itd. (mogu sadržavati malware koji se onda prenosi dalje)
4) malwarei koji su maskirani kao programi za internetsku sigurnost
5) ne korištenje programa za internetsku sigurnost[17]

[16] https://www.jstor.org/stable/pdf/43310933.pdf?ab_segments=0%252Fdefault-2%252Fcontrol&refreqid=excelsior%3A070defc9bc6812ec0378224

4. Antivirusni alati, firewall i obrana od virusa/malicioznih programa

Kad se radi o obrani od malwarea, posao nikad nije jednostavan. Kako tehnologija napreduje svakim novim danom tako se i sami virusi mijenjaju i napreduju, postaju opasniji i teži za uočavanje i iskorijenjivanje. Upravo iz ovog razloga, važno je pravilno i pravovremeno zaštititi računalo kako bi spriječili ili barem drastično smanjili mogućnost infekcije ili napada na računalo. Ono što je nužno za sigurnost računala, uz opreznost samog korisnika, su postavljeni firewall koji će blokirati neautorizirani promet i instalirani antivirusni program. Mnogo kvalitetnih antivirusnih programa pripada grupi softwarea koju je potrebno kupiti, no postoji također isto toliko kvalitetnih besplatnih ili djelomično besplatnih verzija tih programa koji će biti dovoljni za prosječnog korisnika.

Svake godine, stranice koje se bave internetskom sigurnošću sastave popis top 10 najboljih besplatnih antivirusnih alata te se tako u 2019. može odabrati između programa kao što su: Avast, Avira, AVG, Malwarebytes, Kaspersky, Norton, McAfee ili nekog drugog na popisu. Za svaki od ovih programa navedene su glavne karakteristike kao i prednosti i mane te to čini izbor lakšim, ovisno o prioritetima i željama korisnika.[18]

Ove programe također treba držati na najnovijoj verziji (engl. *up to date*) odnosno nadograditi kad izađe novi update jer će on najčešće popraviti neke greške i ponuditi poboljšanu razinu sigurnosti. Uz nadogradnju antivirusnog programa, također bi bio dobar savjet nadograditi sam windows operacijski sustav ukoliko on donosi sigurnosne zakrpe za neke ranije poznate probleme.

Antivirusni alati djeluju tako da skeniraju programe i datoteke instalirane na računalu i potom ih uspoređuju s poznatim vrstama malwarea. Ako se podatci poklapaju, znači da je datoteka inficirana. Na ovu definiciju, svatko bi se zapitao: „A što je s virusima čiji se potpis ne nalazi u bazi podataka? Prema ovome se da zaključiti da što je veća baza podataka i što je uključivija, to

[17] https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-simple-attacks.html
[18] https://www.antivirussoftwareguide.com/free-malware-protection

je antivirusni program bolji i moći će „uhvatiti“ više virusa. Antivirusni programi također nude mogućnost nadogradnje svojih virusnih baza podataka i tako postaju sigurniji i sveobuhvatniji.

Kad se radi o novim virusima čiji potpisi se ne nalaze u bazi, antivirusni program se koristi heurističkom detekcijom. Ovo znači da program traži neke karakteristične osobine virusa odnosno znakove ponašanja kako bi probao otkriti radi li se o virusu budući da te načine ponašanja može povezati s virusima koji se nalaze u bazi.[19]

Kako bi korisnik mogao biti sigurniji na mreži, najbolje bi bilo da slijedi određene savjete ponašanja i da je upoznat s visinom rizika određenih radnji. Ne preporučuje se otvarati e-mailove nepoznatih pošiljatelja, a korisnik pogotovo ne bi smio otvarati privitke koji se nalaze u njima jer se gotovo uvijek radi o nečemu zlonamjernom. Također, korisnik bi trebao izbjegavati komunikaciju s nepoznatim osobama, a pogotovo bilo kakvo dijeljenje datoteka s nekom nepoznatom osobom. Prije nego što nešto skine (engl. *download*) s interneta, korisnik bi trebao provjeriti radi li se o pouzdanoj i provjerenoj stranici koja ima dobru reputaciju. U protivnom, korisnik riskira puno po pitanju sigurnosti jer nepouzdane stranice često u svojim programima skrivaju malware ili dodatne programe koje korisnik ne želi.

U današnje vrijeme internet je pun raznih pop-up prozora i reklama koje nas zatrpavaju na svakom koraku. Najbolje je takve stranice odmah zatvoriti bez klikanja na njih, a jedna od najboljih opcija uključuje preuzimanje ekstenzije za naš web preglednik koja će nakon kratkog postavljanja moći efektno blokirati reklame. Korisniku se također savjetuje da barem jednom do dvaput godišnje promijeni lozinke za svoje internetske račune kako ne bi došlo do proboja zaštite.

[19] https://www.geeksonsite.com/computer-security/what-does-virus-scan-do-how-antivirus-softw

5. Javne Wi-Fi mreže (engl. public wi-fi networks)

Danas svi vlasnici pametnih telefona koriste Wi-Fi mogućnosti spajanja na internet. Međutim, malo njih pridaje značaj spajanju na javne mreže. Javne mreže su danas posvuda uključujući prodavaonice, kafiće, gradske trgove itd. Većini ljudi postala je navika da nakon što sjednu negdje u grad, pretraže Wi-Fi mreže na koje bi se mogli spojiti. Ovo se sve događa automatski bez puno razmišljanja iako nije tako sigurno kao što bi većina ljudi pomislila te zapravo može biti veoma opasno. Ono što čini ovakvu vrstu veze privlačnom za korisnike, također ju čini privlačnom za napadače koji mogu iskoristiti ranjivost korisnika na mreži koje ne zahtijeva nikakvu autentifikaciju.

Dennis Kennedy napisao je kratak članak na ovu temu gdje je sažeo 5 najbitnijih savjeta za sigurnost kod korištenja javnih Wi-Fi mreža. Prvi savjet bio je da saznamo koliko je točno naše računalo ranjivo tako da možemo razumjeti cijeli problem u potpunosti kao i što možemo učiniti kako bismo poboljšali stanje. Za ovaj dio, Kennedy u svom članku predlaže Shields Up, internetsko testiranje sustava koje skenira računalo i nakon toga pokazuje njegove slabosti. Kennedy također napominje kako sama stranica nudi mnoštvo edukacijskih materijala o temi sigurnosti sa savjetima koje korisnik može primijeniti. Drugi savjet odnosi se na firewall. Iako windows OS dolazi s već instaliranim firewallom, mnogi stručnjaci kritiziraju i nemaju povjerenja u tu besplatnu verziju te preporučuju neke kvalitetnije koje se plaćaju. Firewall ne samo da blokira načine na koje vanjski korisnici mogu pristupiti našem računalu nego neke verzije čak i sprječavaju malware koji pokušava odaslati podatke s našeg računala. Kennedy predlaže da nakon instalacije firewalla ponovno testiramo naše računalo sa Shields Up. Treći savjet je da isključimo file-sharing odnosno djeljenje podataka. Ističe kako je jedna od najranjivijih stvari kod windows OS-a kada korisnici imaju osjetljive podatke u folderima za koje je uključeno dijeljenje podataka (engl. *file-sharing*). Netko tko ostvari pristup našem računalu bi u tom trenutku imao pristup svim datotekama u tim folderima. File-sharing može se isključivati na bazi foldera, a dobra ideja je imati samo jedan public folder u kojem se nalaze datoteke za dijeljenje. Četvrti savjet se odnosi na problem malicioznog softwarea i njegovog sprječavanja. Uz firewall, potrebno je također imati dobar program za sprječavanje malwarea.

Kennedy napominje kako je dobra praksa testirati računalo na malware nakon što smo bili povezani na javnu Wi-Fi mrežu. Peti i posljednji savjet odnosi se na nešto što Kennedy naziva „sigurnosna higijena“. Drugim riječima, trebamo koristiti zdrav razum i koncentrirati se na dobre sigurnosne rutine. Jedna od njih je korištenje VPN-a (Virtual Private Network). Također bi trebalo izbjegavati skidanje (engl. *download*) osjetljivih datoteka na javim Wi-Fi mrežama kao i usluge npr. internetskog bankarstva. Preporuča se korištenje jakih zaporki kao i aktivacija sigurnosnih zaštita za račune na društvenim mrežama. Treba pravovremeno nadograđivati programe, biti svjestan trenutnih problema koji postoje kao i pratiti provjerene savjete stručnjaka. Treba zapamtiti da je sigurnost proces, a ne trenutni događaj kojem se posvetimo samo jednom i nikad više (31).[20]

[20] https://www.jstor.org/stable/pdf/23034127.pdf?ab_segments=0%2Fdefault-2%2Fcontrol&refreqid=search%3A9a740349b32632c5c8b11e28836358d9

6. Lančane poruke i spam

Svi smo dobro upoznati s ovakvom vrstom e-mailova. Ponekad spam može biti opasan ukoliko sadržava privitke koji najčešće sadržavaju malware. Iako su ovi e-mailovi u većini slučajeva bezopasni, uvijek sa sobom nose neželjeni trošak internetskog prometa te trošak vremena potrebnog za uklanjanje. Također, oni zatrpavaju poštanski pretinac (engl. *inbox*) te ga čine manje preglednim i jednostavno su naporni za korisnika i ometaju ga u svakodnevnom radu. Ovakve poruke masovne prirode su najčešće razni oglasi i ponude raznih tvrtki kao i pokušaji prevare u obliku klasične priče o nigerijskom princu koji nam želi ostaviti zlato/novac ako mu prvo uplatimo određenu svotu novca za troškove.

Kako bi se prikazalo koliko doista veliki problem predstavlja spam u današnje doba te koliko je raširen pojam, mogu se pogledati podatci grupe Talos. Talos grupa bavi se internetskim problemima i opasnostima za informacije te također sažimaju podatke u statistiku. Istraživanje za srpanj ove godine pokazuje da spam sačinjava čak 85% od ukupne količine e-mail prometa, dok legitimni e-mailovi zauzimaju svega 15%. Kad uzmemo u obzir da je ukupna količina prometa za sedmi mjesec bila 520 milijardi e-mailova, tek tada možemo vidjeti koliko je zapravo spam sveprisutan. Iako je količina spam e-mailova doživjela pad od 8% u odnosu na mjesec prije (lipanj) to ne mijenja situaciju budući da je i sveukupni e-mail promet pao za 8.4%.[21]

Na sreću svih korisnika, rješavanje problema spam poruka, barem na osobnoj razini, nije ni približno toliko teško koliko sprječavanje malwarea. Postoji veliki broj informacija na internetu i brojne informatičke stranice nude sjajne savjete kako pobijediti i spriječiti spam poruke.

Jedna od takvih stranica je TapSmart koja je pretkraj prošle godine sažela informacije i napravila listu s 8 savjeta kako se nositi sa spamom u svom e-mail sandučiću. Savjeti uključuju stvari poput poništavanja pretplata (engl. *subscription*) na raznim stranicama i za razne novosti (engl. *newsletter*) kako više ne bismo primali neželjene e-mailove. Također se savjetuje da korisnici budu pažljiviji kod prihvaćanja raznih stvari na internetu i da naročito čitaju instalacijske upute i

[21] https://www.talosintelligence.com/reputation_center/email_rep

što im određena instalacija nudi jer one često pokušavaju korisnika pretplatiti na određeni newsletter. Također savjetuju standardni postupak koji uključuje izbjegavanje interakcije sa spam porukom i premještanje iste u pretinac za smeće (engl. *junk*). Još jedan koristan savjet koji se može pronaći na stranici govori o kreiranju takozvane throwaway odnosno sekundarne e-mail adrese koja će služiti kao e-mail adresa za razna sumnjiva mjesta i nepoznate stvari kao i za forume te društvene mreže. Na ovaj način možemo biti sigurni kako će naša primarna adresa biti slobodna od spam poruka. Na kraju, ako ništa od ovoga ne uspije, a svejedno nam pristižu neželjene poruke, možemo ili blokirati pošiljatelja ili jednostavno napraviti potpuno novu e-mail adresu ako se ne možemo nositi sa spamom.[22]

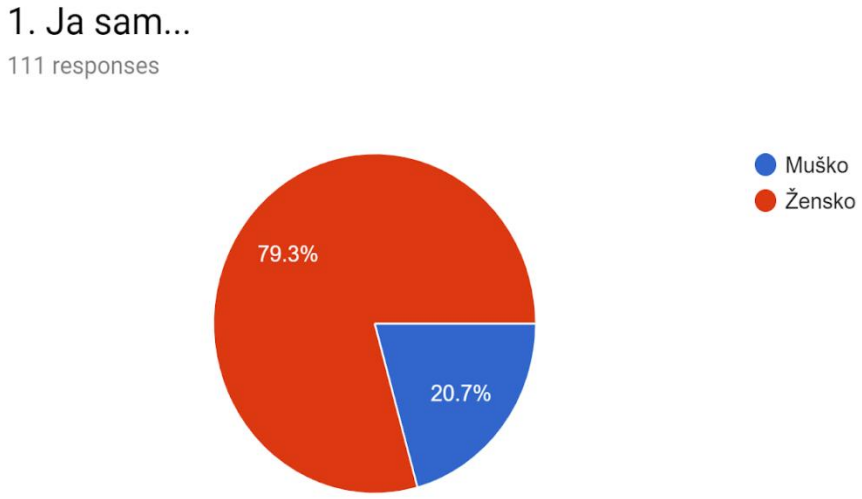
[22] http://www.tapsmart.com/tips-and-tricks/dealing-spam-reduce-junk-email/

7. Anketno istraživanje

Kao što je već navedeno u uvodu, ova anketa težila je ispitati studentsko poznavanje sigurnosti na internetu. Anketa je bila sastavljena i provedena online, putem Google obrazaca. Anketa se sastoji od 20 pitanja od kojih većina spada u kategoriju višestrukog izbora. Prvih nekoliko pitanja služilo je kako bi se stekla slika o anketnom uzorku. Od ispitanika se tražilo da navedu spol, studijski smjer i godinu studija. Nakon toga se od ispitanika tražilo da navedu pojedine statistike o korištenju interneta, koliko vremena dnevno provedu na internetu, koriste li mobitel za pristup internetu kao i specifične stranice, odnosno usluge koje koriste na internetu. U nastavku ankete, ispitanici su upitani o vlastitim iskustvima na internetu te o nekim navikama povezanim sa sigurnošću (npr. promjene zaporki). Ispitanici su također morali procijeniti vlastitu razinu znanja kad je u pitanju internetska sigurnost. Pred sam kraj ankete, ispitanici su bili upitani da vlastitim riječima napišu nekoliko stvari za koje smatraju da su bitne kad je u pitanju internetska sigurnost kao i da napišu što po njihovom mišljenju predstavlja najveću opasnost za računalo.

7.1. Rezultati ankete

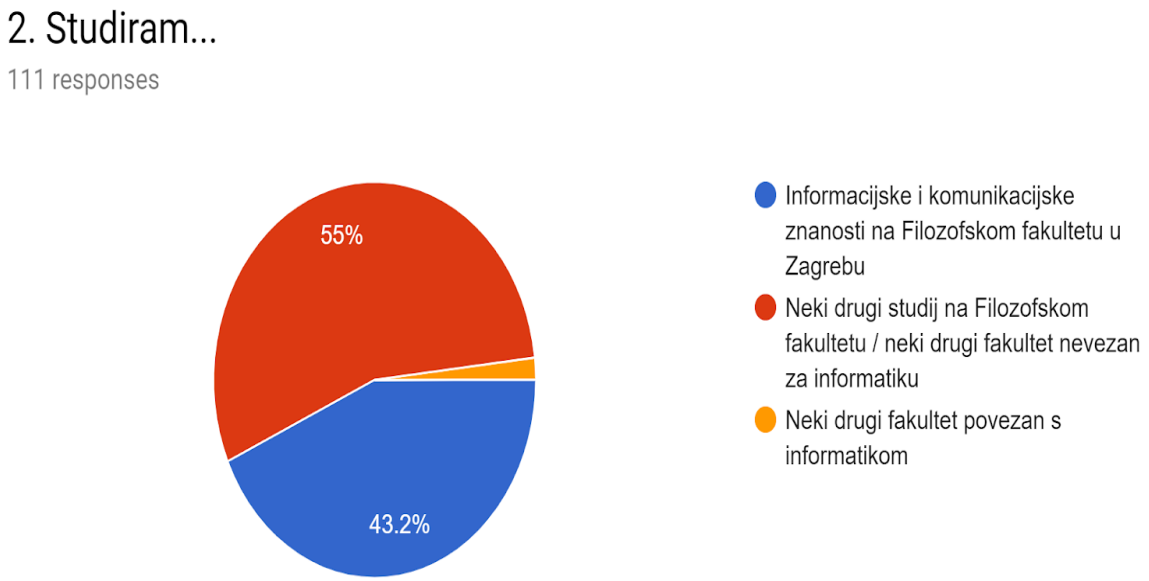
1. Anketu je ukupno ispunilo 111 studenata od kojih je 79,3 % bilo ženskog spola, što je 88 ispitanika, a 20,7 % muškog spola, što je 23 ispitanika.



Graf 1 - Spol kandidata

Kao što se može vidjeti, broj ispitanika ženskog spola uvelike prelazi broj ispitanika muškog spola, toliko da je omjer ispitanika ženskog spola naspram muškog 4:1.

2. U drugom pitanju, ispitanici su morali odabrati svoj studijski smjer odnosno odgovor koji opisuje njihov smjer. Ponuđene su ukupno 3 opcije.



Graf 2 - Smjer/fakultet ispitanika

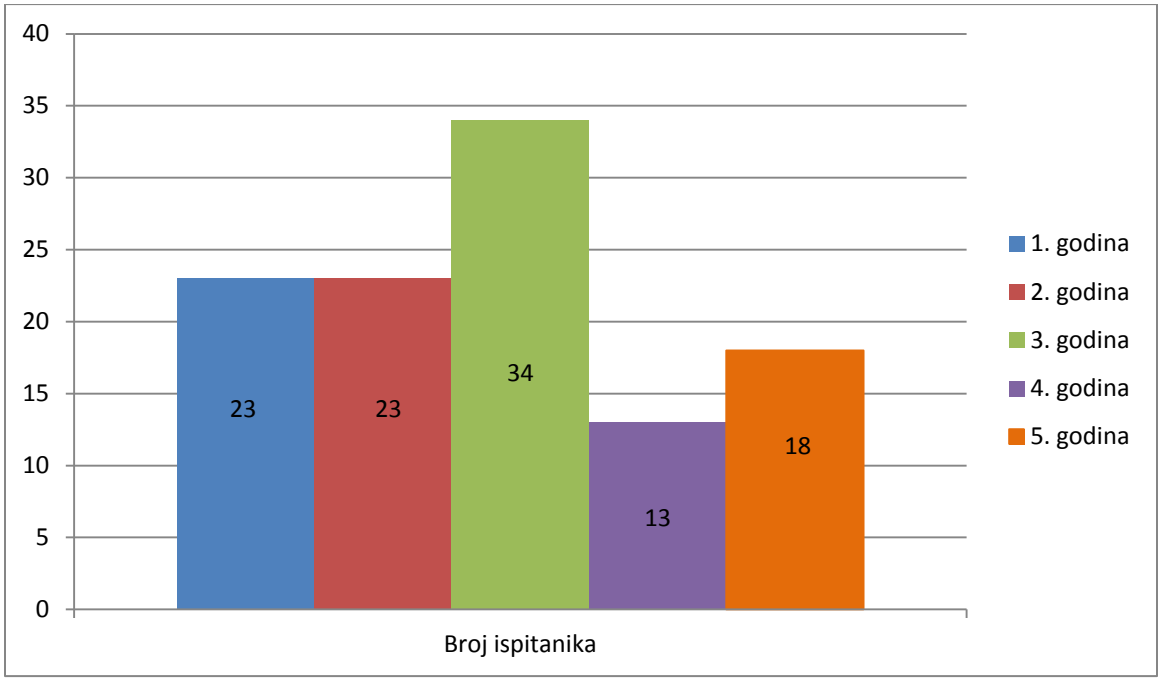
Kao što se može vidjeti iz priloženog grafa, broj ispitanika koji studiraju na nekom drugom fakultetu koji je povezan s informatikom je svega 1,8 % što je ukupno dvoje ispitanika. Broj ispitanika koji studiraju informacijske i komunikacijske znanosti je 48, a broj ispitanika koji studiraju neki smjer nepovezan s informatikom, bilo da je na Filozofskom fakultetu ili nekom drugom fakultetu je 61.

3. Treće pitanje bilo je opcionalno; samo ispitanici koji studiraju informacijske i komunikacijske znanosti bili su obavezni ponuditi odgovor. Pitanje je bilo vezano uz osobno iskustvo tijekom studija, odnosno, misle li ispitanici da se njihovo znanje o internetskoj sigurnosti unaprijedilo kao rezultat samog studija.

Graf 3 - Mišljenje o napretku vlastitog znanja kod ispitanika

Rezultati su bili veoma zanimljivi budući da su bili podijeljeni na dvije jednake grupe. 24 ispitanika odgovorila su da im je studij pomogao unaprijediti znanje o internetskoj sigurnosti dok je druga polovica, također 24 ispitanika, odgovorila suprotno odnosno kako studij nije imao utjecaja na njihovo poznavanje internetske sigurnosti.

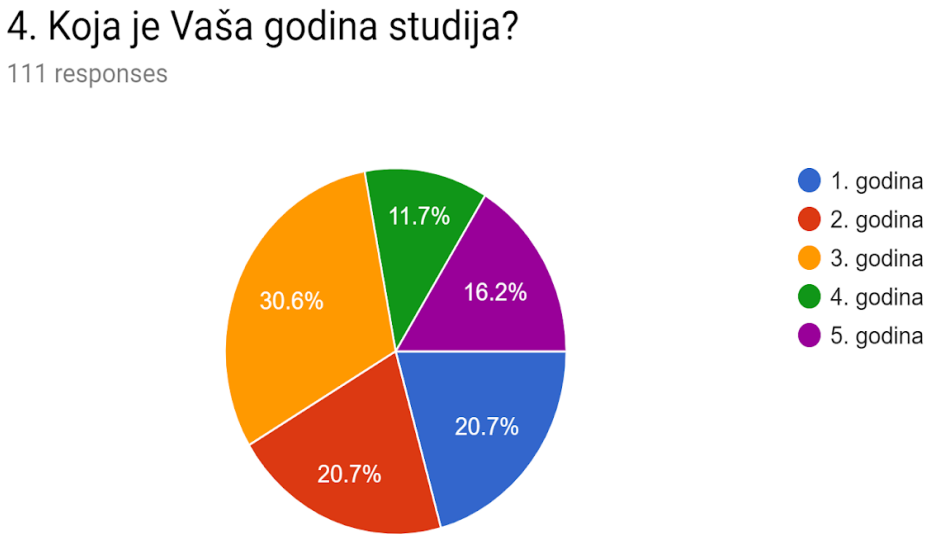
4. Četvrto pitanje bilo je posljednje u skupini pitanja koja su služila za stvaranje slike o anketnom uzorku. Ispitanici su zamoljeni da odaberu godinu svog studija, neovisno o kojem studiju se radi.



Graf 4 – Broj ispitanika po godini studija

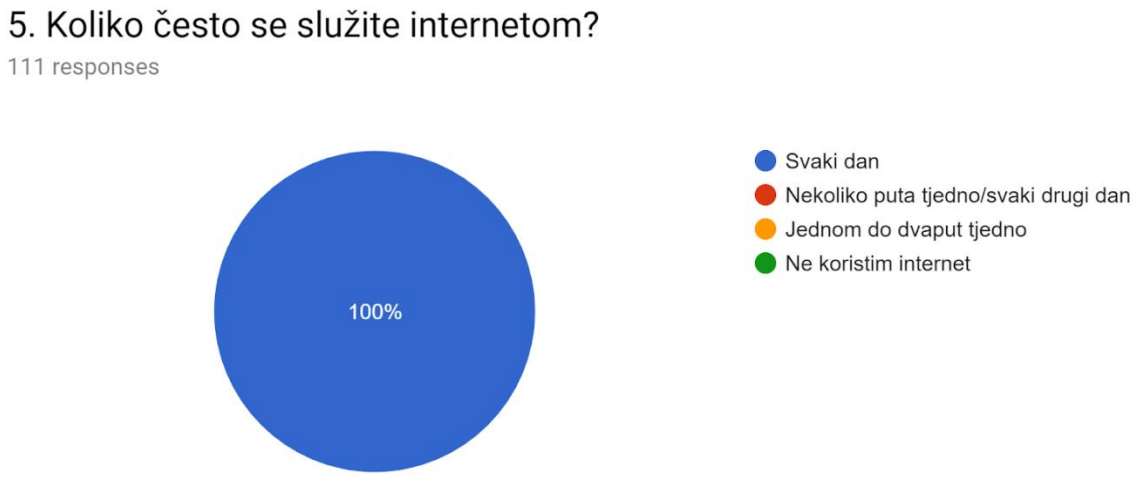
Iz rezultata je vidljivo kako najveći broj ispitanika pripada 3. godini studija, gotovo trostruko više nego na 4. godini. Najmanji broj ispitanika nalazi se na 4. godini, svega 13 (11,7 %). Ostale godine su zastupljenje u otprilike podjednakom broju s izuzetkom 5. godine kojoj pripada 18 (16,2 %) ispitanika.

Sljedeći graf preuzet je direktno iz google docs ankete i prikazuje zastupljenost svake godine u postocima.



Graf 5 - Postotak ispitanika po godini studija

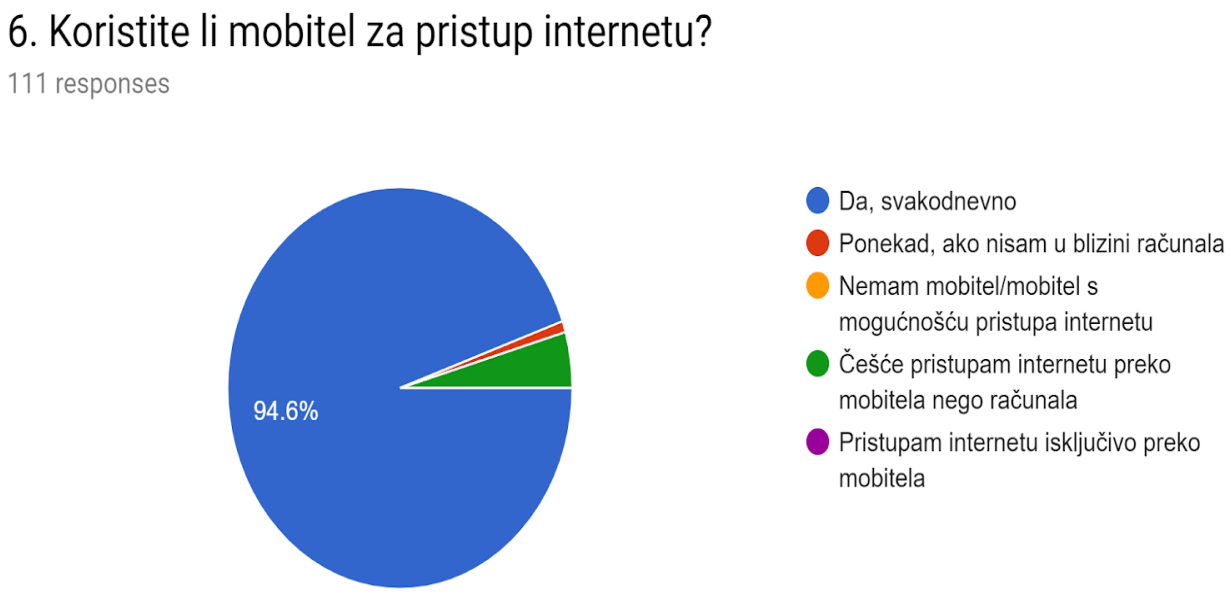
5. Odgovor na peto pitanje je zapravo bio očekivan jer danas svaki student koristi internet bilo da se radi o komunikaciji s profesorom, prijavljivanju ispitnih rokova ili o pristupu nekim ispitnim sadržajima i zadacima. Internet je postao neizostavna sastavnica fakultetskog obrazovanja, a ne samo alat koji nam olakšava studiranje.



Graf 6 - Učestalost korištenja interneta

Svih 111 ispitanika odgovorilo je kako internet koristi svaki dan, bez iznimke.

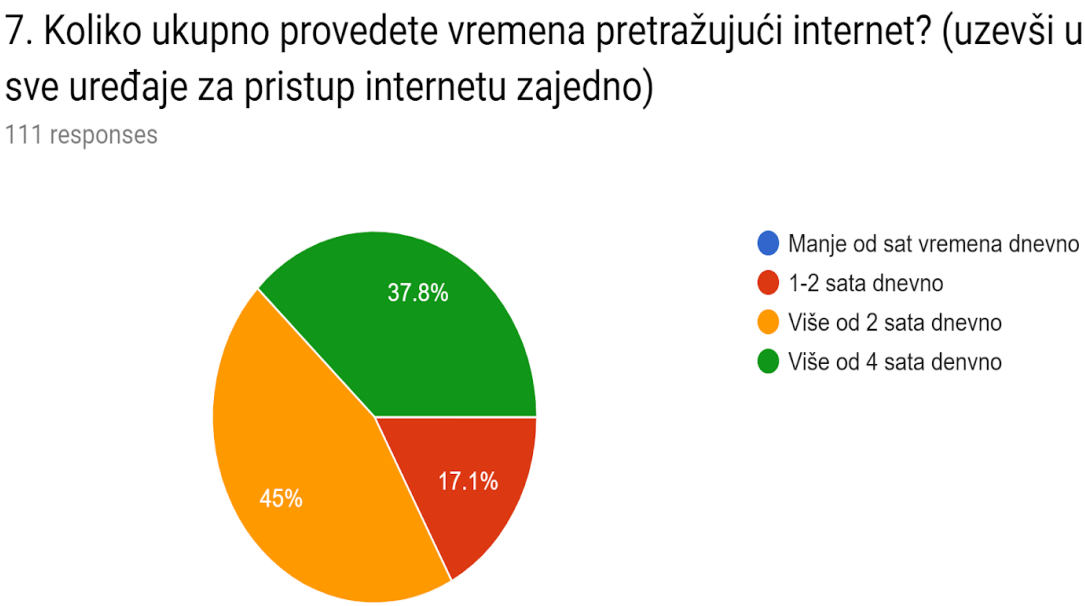
6. Iduće pitanje se odnosilo na pristup internetu putem mobilnog uređaja. Pitanje je služilo kako bi se utvrdile navike pristupa internetu i način na koji studenti to biraju činiti. Iako je prijašnji odgovor bio posve očekivan, kad se radi o mobilnim uređajima cijela situacija može izgledati malo drugačije. Odgovori su ponovo bili očekivani, ali pitanje je svejedno bitno kako bi se stvorio opis studenata i njihovih navika u digitalnom dobu 21. stoljeća.



Graf 7 - Učestalost korištenja mobitela za pristup internetu

Rezultati pokazuju da svih 111 ispitanika posjeduje mobitel s mogućnošću pristupa internetu, a čak 95 % koristi mobitel kao uređaj za svakodnevni pristup inernetu. Ovo je malo promjena u odnosu na pristup internetu putem računala. 4.5 %, odnosno 5 ispitanika koristi mobitel češće nego računalo za pristup internetu, a samo jedan ispitanik koristi mobitel ako nije u blizini računala kako bi pristupio internetu. Bilo kako bilo, nijedan od ispitanika se ne oslanja isključivo na mobitel kao uređaj za pristup internetu.

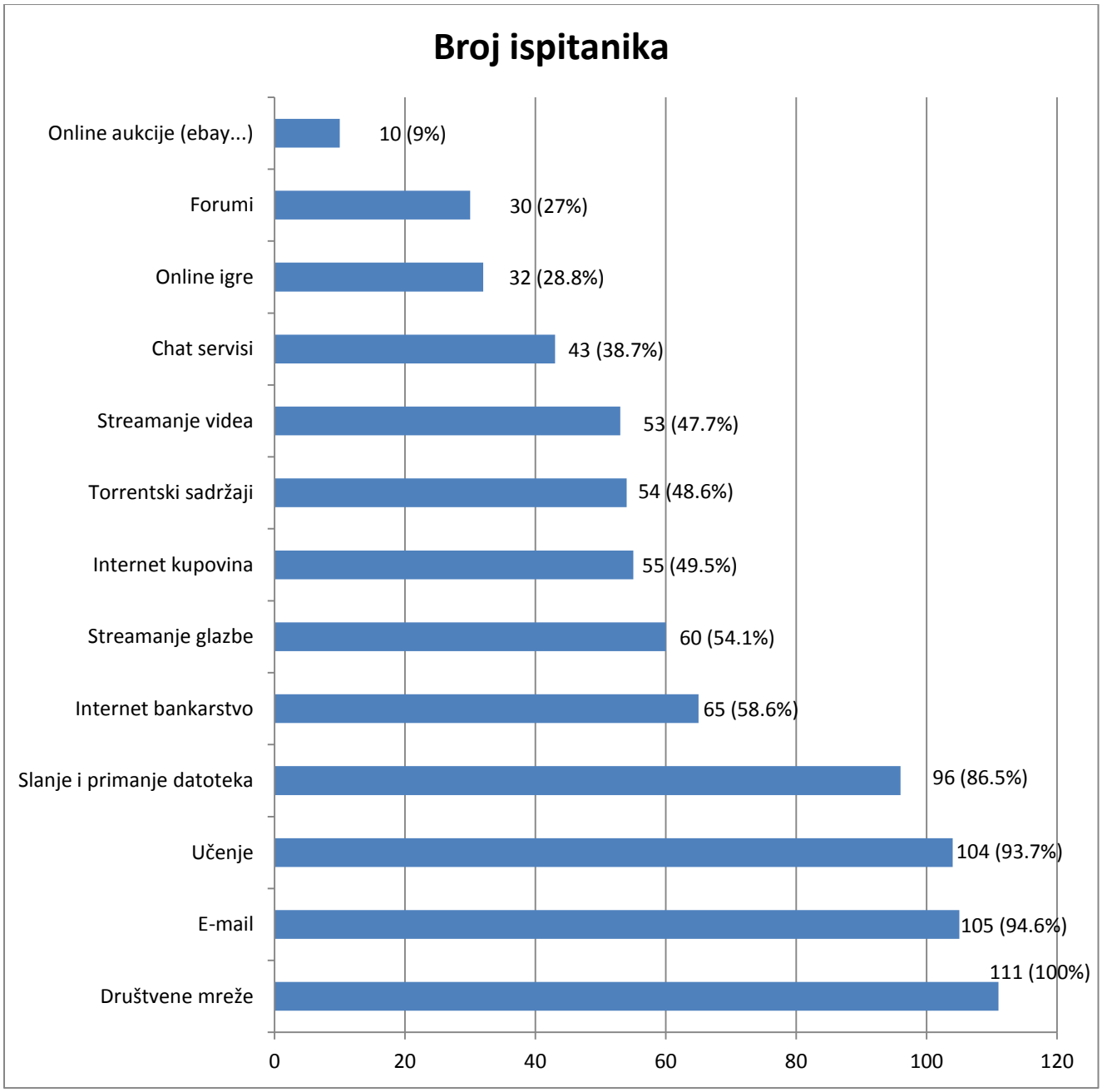
7. Sedmo po redu pitanje služilo je produbljivanju slike o studentskim navikama korištenja interneta. Od ispitanika se tražilo da procijene koliko vremenski dnevno provedu na internetu (uključujući sve uređaje koje koriste za pristup internetu zajedno).



Graf 8 - Ukupnost vremena provedenog na internetu dnevno

Anketa je pokazala da nijedan od ispitanika ne provodi manje od sat vremena dnevno na internetu, što je razumljivo u današnje doba. Manjina ispitanika (17,1 %) provodi od 1 do 2 sata dnevno na internetu dok preko 80 % provodi na internetu preko 2 sata dnevno, a njih 37,8 % čak više od 4 sata. Ako pretpostavimo da prosječan ispitanik provede 8 sati spavajući, 4 sata koje provede na internetu čine 25% od preostalih 16 sati koje ispitanik provede u budnom stanju, što je ogromna količina vremena. Također, budući da je odgovor definiran kao više od 4 sata dnevno, ne možemo znati o kolikoj količini vremena se točno radi. Pravi rezultat bi mogao biti još veći. Vrlo je vidljivo kako je internet ogroman dio svakodnevnog života velikog broja studenata, a ne samo neka popratna i povremena aktivnost ili pripomoć.

8. Ovo pitanje bilo je veoma specifično po pitanju navika na internetu. Od ispitanika se tražilo da odaberu sve tvrdnje koje se odnose na njih odnosno da odaberu sve internetske usluge koje koriste/posjećuju. Naveden je velik broj mogućih opcija, a same opcije su poredane od najmanjeg broja korisnika prema najvećem. Pored svake od opcija naveden je broj ispitanika i njihov postotak u odnosu na ukupni broj ispitanika (111).

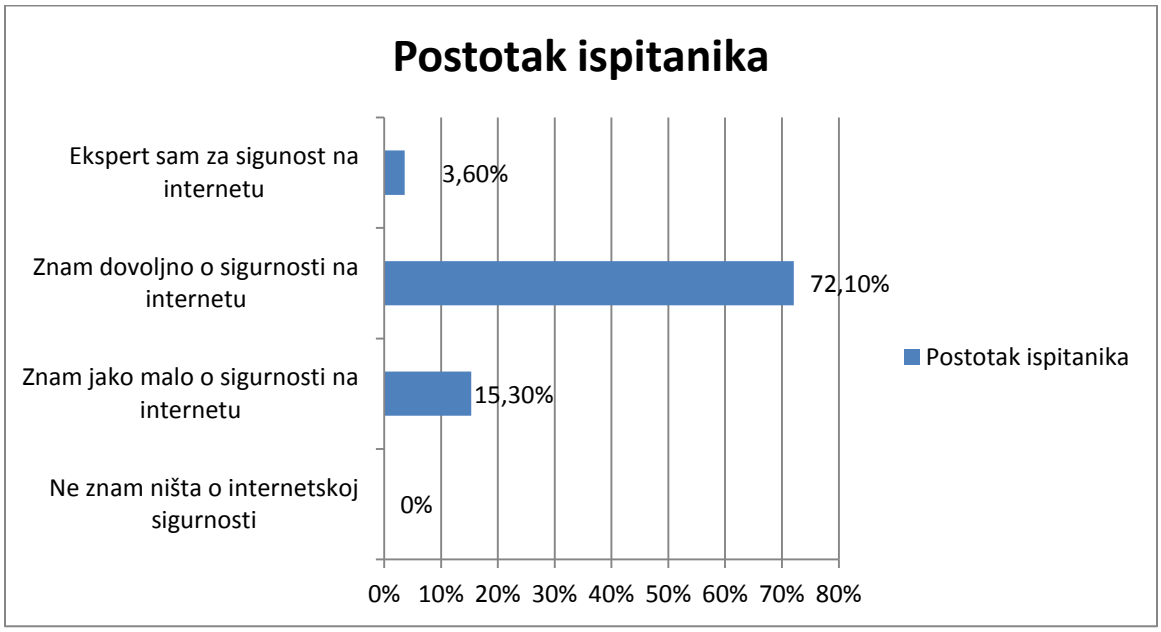


Graf 9 - Zastupljenost korištenja internetskih usluga kod ispitanika

Iz grafikona je vidljivo da svih 111 ispitanika koristi internet za društvene mreže što i nije toliko iznenađujuće budući da puno osoba starije dobi također koristi društvene mreže, a ovdje se radi o studentima kojima je najvažnije ostati povezan s ostalima i biti pravovremeno informiran o raznim novostima. Sljedeći po redu su e-mail usluge i učenje, odnosno, pronalazak materijala, skripti i informacija koji imaju gotovo identičan broj ispitanika koji su se izjasnili o korištenju ovih usluga. Nešto niži broj ispitanika koristi internet za slanje datoteka, ali svejedno se radi o

većini studenata. Broj ispitanika drastično pada kad se radi o internet bankarstvu gdje nešto više od polovice studenata koristi ove usluge. Nakon toga slijede streamanje glazbe, internet kupovina, torrentski sadržaji, streamanje videa, chat servisi, online igre, forumi, a na samom dnu smjestile su se online aukcije poput eBaya. Prema ovim rezultatima možemo zaključiti da studenti najviše internet koriste za učenje i povezanost s prijateljima i ostatkom svijeta putem društvenih mreža.

9. Deveto pitanje odnosilo se na procjenu vlastitog znanja o internetskoj sigurnosti. Ispitanici su bili zamoljeni da označe sve tvrdnje koje se odnose na njih/njihovo iskustvo.

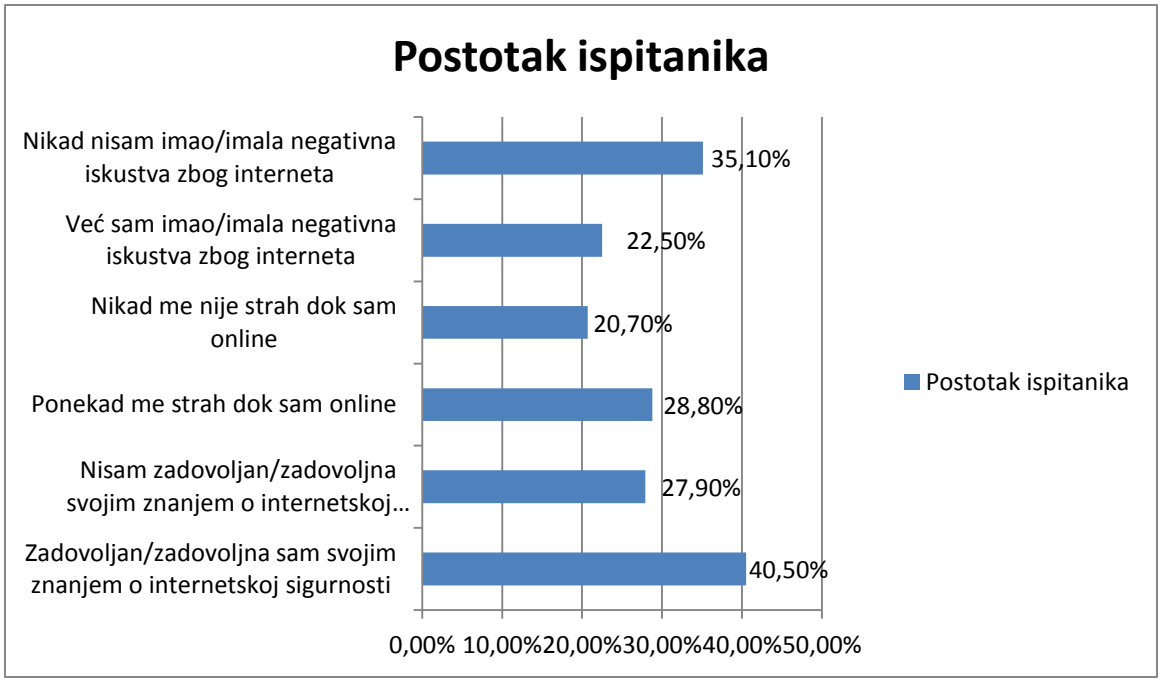


Graf 10 - Procjena vlastitog znanja o internetskoj sigurnosti

Prvi dio pitanja odnosio se na procjenu znanja. Svaki od ispitanika trebao je odabrati tvrdnju koja najbolje opisuje njegovo znanje o internetskoj sigurnosti. Nijedan od ispitanika nije se izjasnio za kompletno nepoznavanje internetske sigurnosti, što je bilo i za očekivati s obzirom na današnje vrijeme u kojem morate znati barem nešto kako biste mogli uspješno koristiti računalo i ostati sigurni. Nešto više od 15 % ispitanika opisalo je svoje znanje kao površno, odnosno izjavili su

kako znaju jako malo o samoj sigurnosti na internetu. Najveći dio ispitanika, njih čak 72,1 %, izjavilo je kako misli da znaju dovoljno o internetskoj sigurnosti. Svega 3,6 % ispitanika izjavilo je kako se smatraju ekspertima za internetsku sigurnost. Rezultati ovog pitanja su zapravo veoma dobri budući da 3 od 4 studenta smatraju kako je njihovo poznavanje sigurnosti dovoljno ili čak bolje od toga. Ako zbrojimo postotke svih odgovora, možemo vidjeti da oni sačinjavaju tek nešto više od 90 %. Razlog za to je da se neki studenti nisu izjasnili odnosno nisu odabrali nijednu od ove 4 opcije pa su vjerojatno odabrali neku drugu iz kategorija koje slijede.

U drugom dijelu pitanja, bilo je potrebno naznačiti zadovoljstvo ili nezadovoljstvo vlastitim znanjem, postojanje negativnih iskustava kao i postojanje straha tijekom vremena koje ispitanik provodi na internetu.

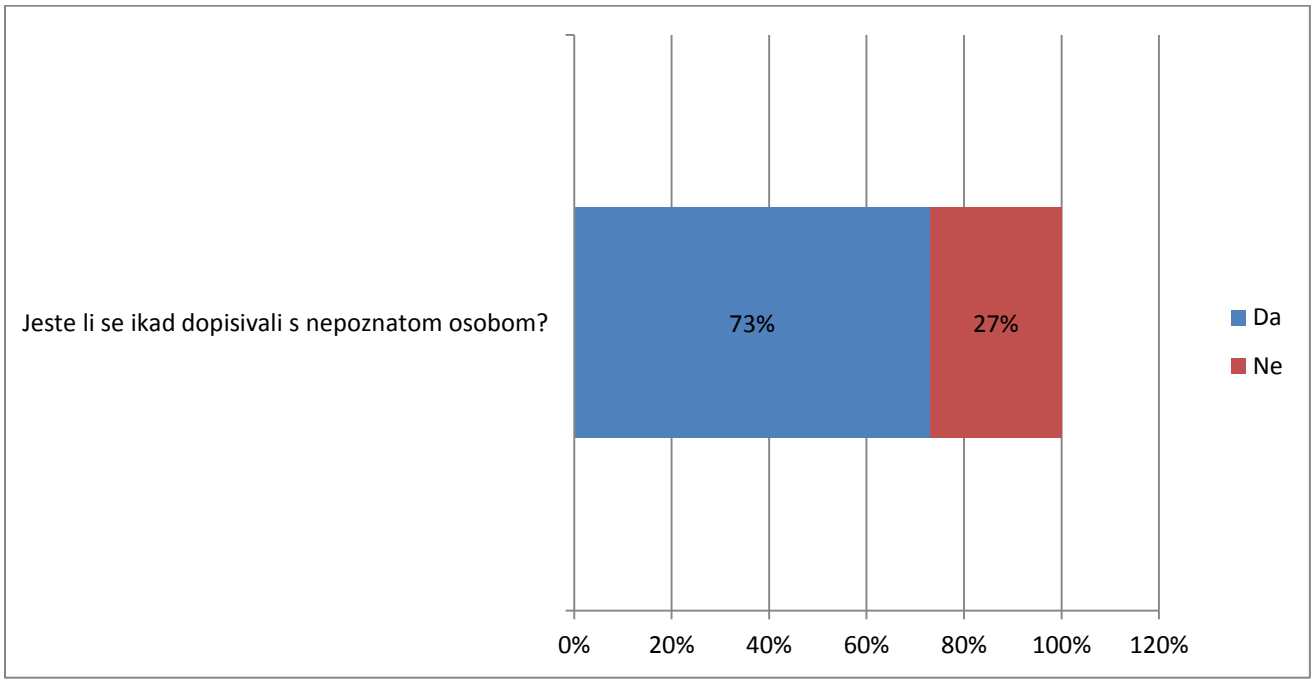


Graf 11 - Osobna iskustva ispitanika u vezi interneta

Kao što je vidljivo iz priloženog grafa, neki se ispitanici ponovo nisu izjasnili za određene tvrdnje, ali svejedno se može uočiti određeni omjer kod odgovora ostatka ispitanika. Tako je recimo nešto više od 35 % ispitanika izjavilo kako nikad nije imalo negativnih iskustava zbog

interneta, što je 39 studenata, a 22,5 % ispitanika izjavilo je suprotno odnosno kako su već doživjeli određena negativna iskustva. 22,5 % je ukupno 25 ispitanika. Nadalje, 20,7 % ispitanika (23) izjavilo je kako ih nikad nije strah dok pregledavaju internet dok je njih 28,8 % (32) izjavilo kako su ponekad osjetili strah u nekom trenutku pregledavanja interneta. Kad se radi o zadovoljstvu vlastitim znanjem, 27,9 % ispitanika (31) izrazilo je nezadovoljstvo vlastitim znanjem o internetskoj sigurnsti, a 40,5 % (45) ispitanika izrazilo je zadovoljstvo svojim znanjem.

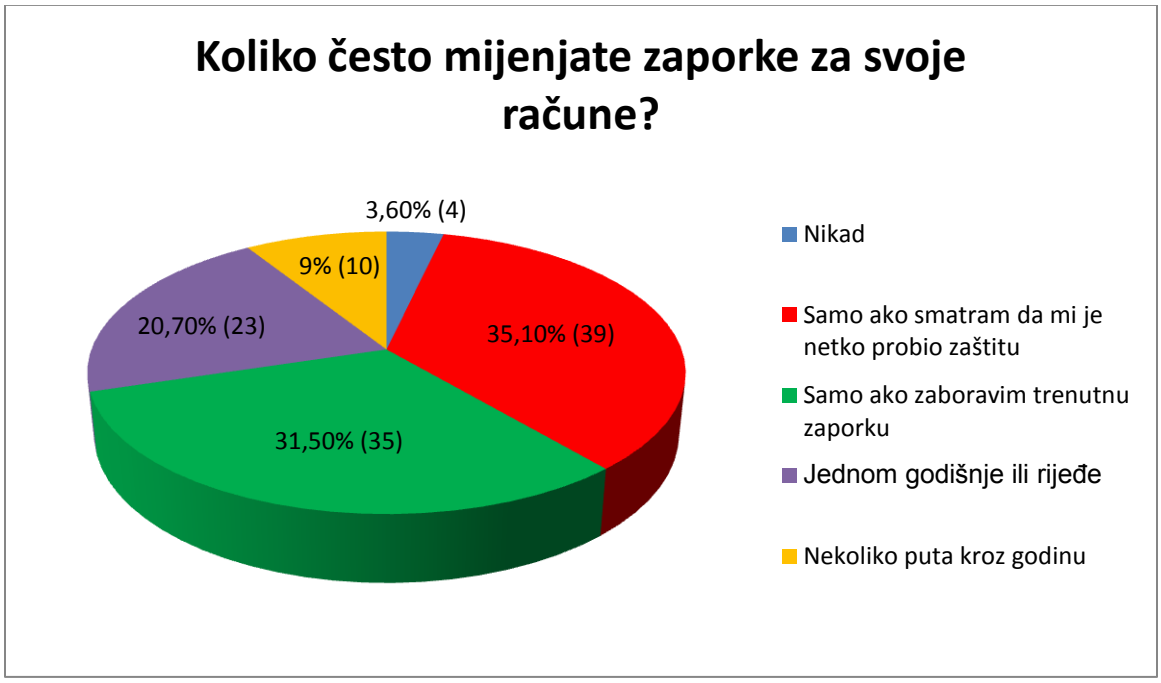
10. Deseto pitanje je ponovno zahtijevalo da/ne odgovor. Od ispitanika se tražilo da se izjasne po pitanju dopisivanja s nepoznatom osobom i rezultati su dosta iznenađujući.



Graf 12 - Postotak ispitanika koji se dopisivao s nepoznatom osobom

Kao što je vidljivo iz priloženog grafikona, omjer ispitanika je gotovo 3:1 u korist onih koji su se dopisivali s nekom nepoznatom osobom. Ovo uvijek za sobom nosi određenu dozu rizika, no ako se ne razmjenjuju datoteke, rizik bi trebao biti minimalan.

11. U jedanaestom pitanju, studenti su bili upitani koliko često mijenjaju zaporke za svoje račune te je ponuđeno više mogućih odgovora i situacija.



Graf 13 - Učestalost mijenjanja zaporki

Jako mali udio ispitanika izjasnio se kako nikad ne mijenjaju zaporke. Gotovo 70 % ispitanika mijenja zaporke samo ako uoče da im je zaštita probijena ili ako zaborave vlastitu zaporku odnosno tek kad su prisiljenji promijeniti zaporku. Nešto više od 20 % ispitanika mijenja zaporke jednom godišnje ili rjeđe, a samo svaki 11 ispitanik (9 %) mijenja zaporke redovito i to

nekoliko puta kroz godinu. Redovita promjena zaporki je važna sigurnosna praksa, a kao što se iz rezultata može vidjeti, studenti baš nemaju tu naviku. Ovo se može pripisati nepoznavanju internetske sigurnosti, ali i ljudskoj lijenosti.

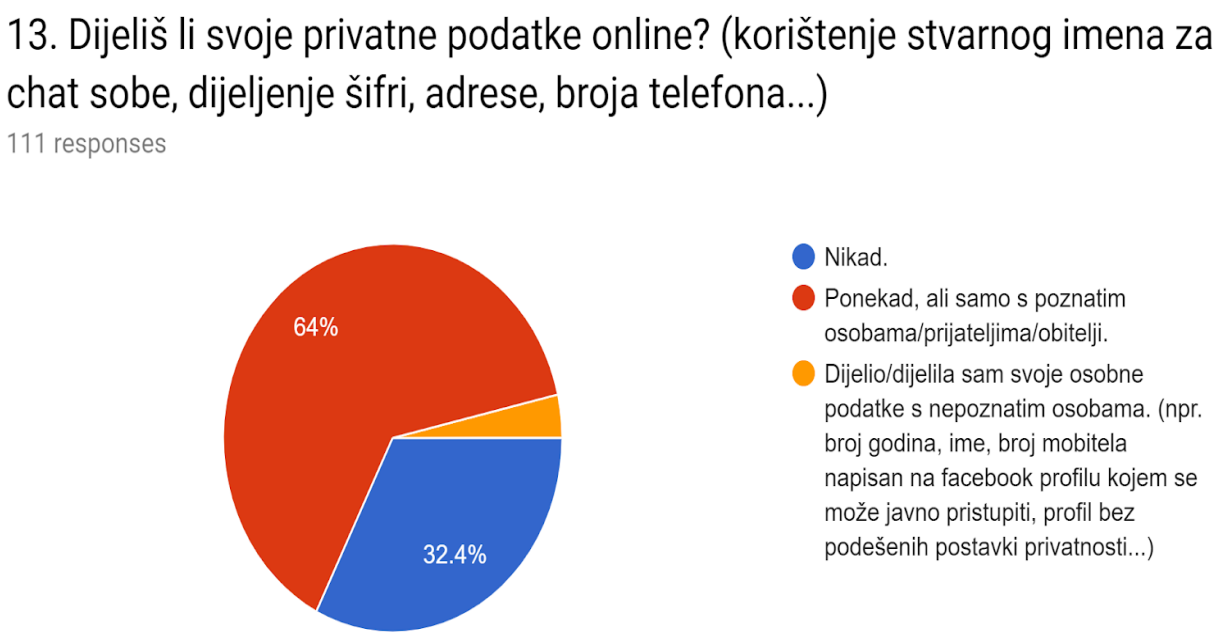
12. Dvanaesto po redu pitanje služilo je kako bi se dobio odgovor na pitanje koje je izuzetno bitno za sigurnost na internetu. Ovo pitanje ja također povezano s prethodnim jer se nastavlja na pitanja o lozinkama. Pitanje je glasilo: „Koristite li identične zaporke za više računa?“. Odgovori su ponovo bili iznenađujući i to ne u pozitivnom smislu.

Graf 14 - Postotak ispitanika koji koriste istu zaporku za više računa

Kao i kod pitanja o dopisivanju s nepoznatim osobama, omjer je ponovno bio 3:1 budući da se čak 73.9 % kandidata izjasnilo kako koristi identičnu zaporku za više različitih računa što je

ukupno 82 ispitanika. Samo 29 ispitanika (26,1 %) izjasnilo se kako nikad ne koriste identičnu zaporku na više računa. Identične zaporke se nikad ne bi smjele koristiti za više različitih računa budući da to uvelike olakšava posao osobama koje možda nemaju najbolje namjere. Ako npr. osoba ima identičnu zaporku za neku društvenu mrežu kao i za e-mail, počinitelj lako može promijeniti tu zaporku jer će nakon što sazna jednu zaporku moći pristupiti i profilu kao i glavnom e-mailu koji je vezan za profil. Baš zbog ovog razloga potrebno je koristiti različite zaporke i redovito ih osvježavati tako da ih promijenimo. Ispitanici su u ovom slučaju ponovno pokazali nepoznavanje nekih bitnih dijelova sigurnosti iako se može raditi o nemarnosti ili nemogućnosti pamćenja velikog broja različitih zaporki. U svakom slučaju, uvijek je bolje zapisati zaporke na neki papir i zapamtiti ih s vremenom nego koristiti identičnu zaporku za više računa.

13. Ovim pitanjem htjele su se ispitati studentske navike kad su u pitanju osobni podatci odnosno privatnost.



Graf 15 - Navike dijeljenja privatnih podataka kod ispitanika

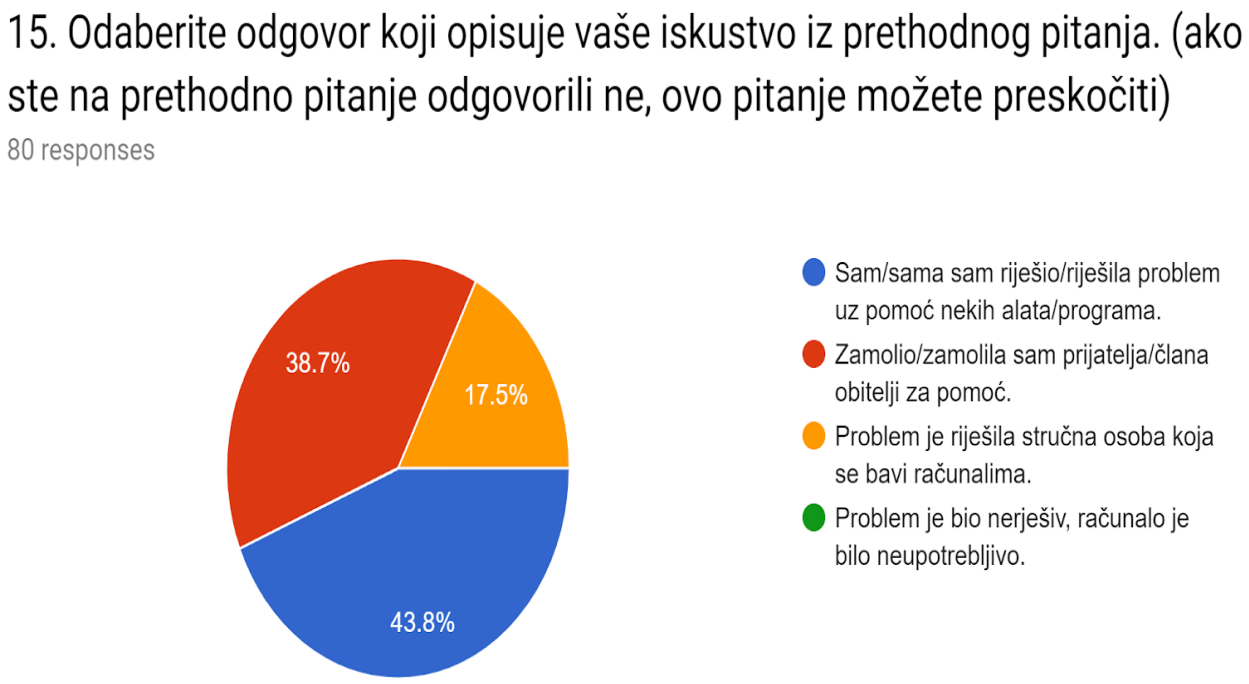
Trećina od ukupnog broja ispitanika (36) izjavila je kako nikad ne dijeli privatne podatke neovisno o poznavanju osobe. Skoro dvostruko više ispitanika (71) izjavilo je kako ponekad dijeli osobne podatke, ali samo s poznatim osobama koje uključuju prijatelje ili obitelj. Vrlo mali postotak ispitanika, točnije 3,6 % (4), izjavio je kako su dijelili svoje privatne podatke s nepoznatim osobama. Ovo je dobar rezultat koji pokazuje da ispitanici brinu o svojoj privatnosti, a ako ju i odluče dijeliti, onda ju dijele samo s osobama kojima vjeruju.

14. Četrnaestim pitanjem htjelo se doznati koliki se postotak ispitanika u nekom trenutku susreo s računalnim virusom. Pretpostavka je da je većina studenata imala susret s nekom vrstom virusa budući da su sami virusi u današnje vrijeme toliko rašireni da lako može doći do zaraze računala, pogotovo ako je korisnik neiskusan i/ili neoprezan.

Graf 16 - Postotak ispitanika koji je imao virus na svom računalu

Odgovori su pokazali da svaki 4 ispitanik (27,9 %) nije imao iskustvo s virusom na svom računalu, ali većina ispitanika (72,1 %) susrela se s virusom u nekom obliku što je potvrdilo prethodnu pretpostavku.

15. Ovo pitanje služilo je kao nastavak na prethodno pitanje i bilo je opcionalno. Od ispitanika koji su na prethodno pitanje o susretu s virusom odgovorili potvrdno, tražilo se da odaberu tvrdnju koja najtočnije opisuje njihovo rješenje za nastalu situaciju. Ukupno je odgovaralo 80 ispitanika.



Graf 17 - Opis iskustva s virusom kod ispitanika

Odmah se može vidjeti da nijedan od ispitanika nije doživio susret s virusom toliko ozbiljnim da bi učinio računalo neupotrebljivim. Najviše ispitanika (35) izjasnilo se za prvu opciju, rekavši kako su uspjeli sami riješiti problem. Približno jednak broj ispitanika (31) izjasnio se za drugu opciju koja je uključivala pomoć člana obitelji ili prijatelja. Preostalih 17,5 % (14) ispitanika, što je otprilike svaki šesti ispitanik, izjavilo je kako su pomoć potražili kod stručne osobe.

16. Ovo pitanje bilo je prvo pitanje u kojem se od ispitanika tražio vlastiti odgovor. Studentima je ponuđena mogućnost dugačkog odgovora, a tražilo se da navedu 3 stvari za koje smatraju da su najvažnije kad je u pitanju internetska sigurnost.

Ispitanici su uglavnom ponudili dobro informirane odgovore (Odgovori ispitanika većinom su pokazali njihovu dobru informiranost), a najčešće su spominjali ne posjećivanje sumnjivih stranica, ne otvaranje sumnjivih e-mailova i privitaka, mijenjanje zaporki kao i dobar antivirusni program. Također su istaknuli informiranost, sumnjičavost i brigu o vlastitoj privatnosti kao bitne dijelove internetske sigurnosti.

Slika 1 - Postavke sigurnosti

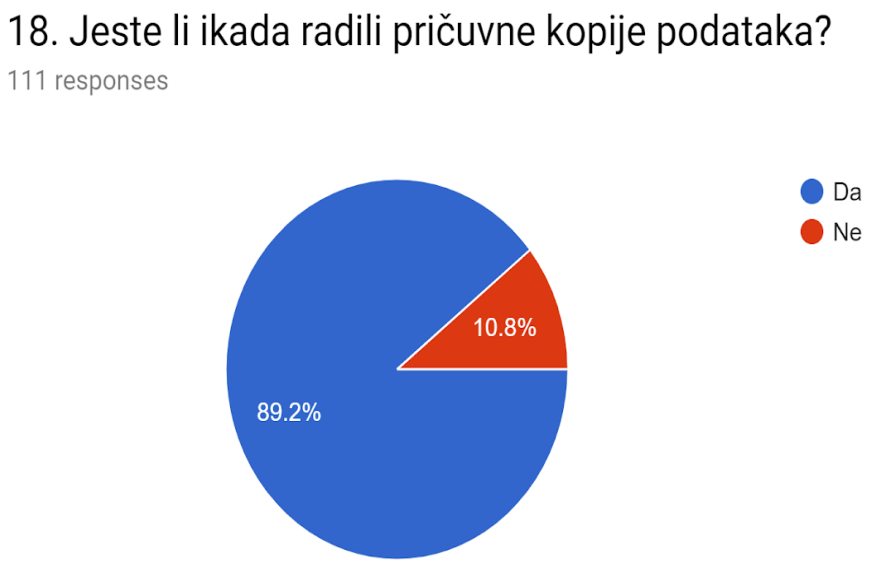
17. Ovo pitanje odnosilo se na jedan od najlakših načina zaraze računala u današnje vrijeme, a radi se o sumnjivim e-mailovima koji sadržavaju privitak (engl. attachment). Najčešće se radi o e-mailu koji nismo očekivali i koji dolazi s nepoznate adrese. Sadržaj je obično nešto što bi nas potaklo da kliknemo i otvorimo privitak i nakon toga bi naše računalo bilo zaraženo. Pitanjem su se htjela ispitati iskustva studenata koji su se susreli s ovakvom vrstom prijetnje. Od ukupnog broja ispitanika, njih 88 ponudilo je odgovor na ovo pitanje što znači da je njih 79 % u nekom trenutku primilo ovakav e-mail.

Graf 18 - Postotak ispitanika koji su primili e-mail nepoznatog pošiljatelja

Ispitanici koji su se susreli s ovakvim e-mailom, imali su ponuđene 4 opcije od kojih su morali odabrati onu koja najbolje opisuje način na koji su postupili. Ovo pitanje ponudilo je izuzetno pozitivne rezultate budući da se nitko od ispitanika nije izjasnio za opciju otvaranja e-maila i privitka. Nešto više od pola ispitanika (46) izjasnilo se za opciju brisanja e-maila bez otvaranja i čitanja što je najbolji način postupanja kad se radi o ovakvim e-mailovima. 40,9 % ispitanika (36) reklo je kako su jednostavno ignorirali e-mail u potpunosti. Preostalih 6,8 % ispitanika (6) izjasnilo se kako su otvorili e-mail kako bi vidjeli o čemu se radi, pri tome ne otvarajući privitak. Ovo također može biti veoma opasno jer neki e-mailovi mogu sadržavati kod koji se pokreće čim se e-mail otvori. Rezultati su dosta dobri i pokazuju da veliki dio ispitanika prepoznaje opasnost u ovakvim situacijama, iako postoji mali dio njih koji je demonstrirao rizično ponašanje.

Graf 19 - Postupak ispitanika u vezi s e-mailom nepoznatog pošiljatelja

18. Osamnaesto pitanje bilo je povezano s očuvanjem podataka. Htjelo se vidjeti koliko studenata je pripremljeno za slučaj da dođe do gubitka podataka, odnosno koliko njih poduzme „mjere“ prije nego do opasnosti uopće dođe.



Graf 20 - Postotak ispitanika koji su radili pričuvne kopije podataka

Rezultati su ponovno bili veoma dobri jer se može vidjeti da čak 9 od 10 studenata sprema podatke za slučaj neke opasnosti koja bi uzrokovala njihov gubitak. Back up (spremanje) podataka izuzetno je bitan kad se radi o internetskoj sigurnosti.

19. Ovo pitanje bilo je još jedno pitanje samostalnog odgovora. Ispitanici su bili zamoljeni da napišu što, po njihovom mišljenju, predstavlja najveću opasnost za računalo.

Najveći broj ispitanika odlučio se za viruse, što je bilo za očekivati s obzirom da se ta tema provlači kroz cijelu anketu. Neki od ispitanika su se odlučili za ljudske karakteristike kao što su neodgovornost, neopreznost i naivnost. Veliki dio njih također je istaknuo samog korisnika kao najveću prijetnju za računalo. Pojedini ispitanici su odlučili odgovoriti malo specifičnije pa su nudili odgovore koji točno definiraju određenu radnju, npr. klikanje na razne reklame i pop-up prozore, posjećivanje sumnjivih internetskih stranica te preuzimanje datoteka s istih, otvaranje e-mailova nepoznatih pošiljatelja itd.

Slika 2 - Zaraženo računalo

20. Dvadeseto i ujedno i posljednje pitanje referiralo se na samu anketu. Od korisnika se tražilo da se izjasne je li ih ova anketa potakla na razmišljanje o internetskoj sigurnosti i na razmišljanje o njihovom znanju o toj temi.

Graf 21 - Postotak ispitanika koje je anketa potakla na ramišljanje

Odgovori su ponovno bili dosta dobri i može se vidjeti da su se čak 3 od 4 ispitanika zamislila o internetskoj sigurnost nakon ispunjavanja ove ankete, što je ujedno bio i jedan od ciljeva ankete.

8. Zaključak

U današnje vrijeme, sigurnost je postala veoma upitna. Ranijim razvojem tehnologije i napretkom čovječanstva došlo je do potpuno novih oblika kriminala koje smo prije običavali gledati samo u filmovima. Neprilagođeni sustav isprva se mučio i nije znao kako se nositi s novim opasnostima koje su se odjednom pojavile i počele nekontrolirano rasti. Postavljalo se pitanje što učiniti s ovim problemom. S vremenom, razvile su se nove tehnologije i zaposlili novi stručnjaci te se stanje počelo popravljati. Ljudi su bili informirani i naučeni kako reagirati na određene prijetnje i kako zaštititi sebe i svoju privatnost. Međutim, broj malicioznih programa i osoba zlih namjera raste svakim danom te se stvaraju sve sofisticiranije metode prevare, stvaranja štete itd. Samo pitanje sigurnosti na internetu kao takvo vjerojatno nikad neće biti razriješeno budući da će uvijek postojati dvije strane. Jedna strana koja brine o sigurnosti i ekvilibriju korisnika i interneta i druga koja želi iskoristiti internet za svoje zle namjere i ciljeve odnosno neku vrstu vlastite koristi. Baš zbog ovog razloga je važno nastaviti borbu protiv kibernetičkog kriminala te nastaviti programe i radionice za informiranje građanstva o koristima kao i opasnostima interneta. Pravovremeno obrazovanje te opreznost i sumnjičavost samog korisnika kod korištenja interneta pomoći će smanjiti crne statistike o broju žrtava kibernetičkog kriminala, a povjerenje i suradnja između organizacija, građana i stručnjaka za internetsku sigurnost će rezultirati općenitim poboljšanjima kod mjera zaštite. Provedena anketa je pokazala pozitivne rezultate kad se radi o poznavanju internetske sigurnosti kod studenata te je također pokazala da su studenti željni naučiti više i poboljšati svoje znanje. Upravo ova želja je ono što nas treba voditi u budućnosti, želja da poboljšamo sami sebe kroz proširivanje našeg znanja te istovremeno želja da unaprijedimo čovječanstvo općenito, kroz međusobnu pomoć. Na ovaj način, postotak kibernetičkog kriminala počet će padati, a zamijenit će ga pozitivne statistike.

9. Literatura

1. "8 Different Types of Malware." *United States Cybersecurity Magazine*, 3 Aug. 2018, www.uscybersecurity.net/malware/.

2. Azarmsa, Reza. "Computer Viruses and Safe Educational Practices." *Educational Technology*, vol. 31, no. 11, 1991, pp. 26–32. *JSTOR*, www.jstor.org/stable/44425719

3. "Computer Viruses - Theory and Experiments." *EECS Department*, https://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html.

4. "Cyber Security Breaches Survey 2019." *Ipsos MORI*, www.ipsos.com/ipsos-mori/en-uk/cyber-security-breaches-survey-2019.

5. "Dictionary of Information Security." *Google Books*, Google, https://books.google.hr/books?id=mK2QhS11JtsC&pg=PA194&lpg=PA194&dq=mission,+trigger+and+self+propagation+component&source=bl&ots=j1u1aS-n8z&sig=ACfU3U3fUVetXQ9FnrhTWKgyE6S-I3982A&hl=en&sa=X&ved=2ahUKEwiCpvH82PjjAhX3QhUIHfsYCHgQ6AEwDXoECAcQAQ#v=onepage&q=mission%2C%20trigger%20and%20self%20propagation%20component&f=false.

6. Geeks on Site. "What Is Antivirus Software and How Does It Work?" *Geeks on Site*, 25 Oct. 2017, www.geeksonsite.com/computer-security/what-does-virus-scan-do-how-antivirus-softw.

7. Grannell, Craig. “Dealing with Spam: Reduce the Junk in Your Email.” *TapSmart*, 31 Oct. 2018, www.tapsmart.com/tips-and-tricks/dealing-spam-reduce-junk-email/.

8. HAMILTON, MELISSA. “The Dark Side of the Computer Age: Protecting a Client Company's Precious Asset: Information.” *Business Law Today*, vol. 3, no. 2, 1993, pp. 50–53. *JSTOR*, www.jstor.org/stable/23288059.

9. Hosch, William L. “Malware.” *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., www.britannica.com/technology/malware.

10. Kennedy, Dennis. “TIE DOWN THAT WI-FI: Security in Public Requires Vigilance.” *ABA Journal*, vol. 97, no. 10, 2011, pp. 31–31. *JSTOR*, www.jstor.org/stable/23034127.

11. “Malware 101: How Do I Get Malware? Simple Attacks.” *Malware 101: How Do I Get Malware? Simple Attacks*, https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-simple-attacks.html.

12. NEUMANN, PETER G. “Computer Insecurity.” *Issues in Science and Technology*, vol. 11, no. 1, 1994, pp. 50–54. *JSTOR*, www.jstor.org/stable/43310933.

13. “The Efficacy of Security Systems.” *The Defender’s Dilemma: Charting a Course Toward Cybersecurity*, by Martin C. Libicki et al., RAND Corporation, Santa Monica, Calif., 2015, pp. 23–40. *JSTOR*, www.jstor.org/stable/10.7249/j.ctt15r3x78.11.

14. "Top 10 Best Free Anti-Malware Software 2019." *The Best 10 Free Malware Protection Software 2019 - Best Free Malware Protection*, www.antivirussoftwareguide.com/free-malware-protection.

15. "U 2 Godine Više Od Pola Hrvatskih Organizacija Bile Su Žrtve Prijevare i Kriminala." *Povratak Na Naslovnicu Poslovnog Dnevnika*, www.poslovni.hr/hrvatska/u-2-godine-vise-od-pola-hrvatskih-organizacija-bile-su-zrtve-prijevare-i-kriminala-345047.

16. "Vulnerability Information." *Email and Spam Data || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence*, www.talosintelligence.com/reputation_center/email_rep.

17. "What Is a Computer Worm and How Does It Work?" *What Is a Computer Worm and How Does It Work?*, https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html.

18. "What Is a Trojan? Is It a Virus or Is It Malware?" *What Is a Trojan? Is It Virus or Malware? How It Works.*, https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html.

19. "What Is the Difference: Viruses, Worms, Trojans, and Bots?" *Cisco*, 24 May 2019, www.cisco.com/c/en/us/about/security-center/virus-differences.html.

20. “Why Has Demand Risen Sharply?” *Hackers Wanted: An Examination of the Cybersecurity Labor Market*, by MARTIN C. LIBICKI et al., RAND Corporation, 2014, pp. 5–12. *JSTOR*, www.jstor.org/stable/10.7249/j.ctt7zvzmj.9.

Prilozi

Anketa - Upoznatost studenata s metodama zaštite podataka

Link:
https://docs.google.com/forms/d/e/1FAIpQLScQf3MozpMMHSJxUI6ek6yK5vGT3N6wNeCsVJ7GBj9GhCnfJw/viewform?usp=sf_link

Sažetak

U 21. stoljeću razvija se problem kibernetičkog kriminala. Sam je problem jako raširen te uključuje velike tvrtke, kao i pojedince. Kako bi se obranilo od ovakve vrste prijetnji, potrebno je ne samo znanje nego i vlastita procjena opasnosti i zdrav razum. Vrlo je bitno da se znanje o ovim opasnostima stekne pravovremeno, da informacije budu provjerene, a savjeti primjenjivi. Zbog ovog razloga je provedena anketa koju su ispunjavali studenti kako bi se vidjelo koliko oni znaju o internetskoj sigurnosti i kako bi se procijenilo koliko je rizično njihovo ponašanje u određenim slučajevima. Budući da su studenti uglavnom djeca 21. stoljeća, oni su bili savršeni anketni uzorak za ovu temu. Prije same ankete, također su definirani i komentirani neki važni pojmovi poput malicioznih programa i njihove podjele. Opisano je sigurno ponašanje na internetu kao i ponašanje koje predstavlja rizik. Također su opisani načini za zaustavljanje prijetnji poput vatrozida i antivirusnih programa. Na kraju su također dotaknuta područja problema spam e-mailova kao i internetska sigurnost u javnosti, odnosno na javnim Wi-Fi mrežama.

Ključne riječi: kibernetički kriminal, prijetnja, informacije, sigurnost, antivirus

Abstract

In the 21st century, the problem of cyber crime was developing. The problem itself is widely spread and includes not only big companies but also individuals. In order for one to defend themselves from these sorts of threats it takes not only knowledge and common sense but also one's own ability to anticipate danger. It is very important to acquire the knowledge of these dangers ahead of time, for information to be verified and for advice to be applicable. For this

reason, a survey was conducted among students in order to see how much they know about safety on the internet and also to gauge how risky their behaviour is when it comes to certain situations. Since most students are 21st century children, they constitute a perfect survey sample. Before delving into the survey results, some important notions and ideas had to be defined and commented on. Safe online behaviour was described as well as behaviour that poses a threat to the user. Different ways to put a stop to these threats, like antivirus software and firewalls, were also described. At the end, problems like e-mail spam and public online security when it comes to connecting to public Wi-Fi networks were also mentioned.

Key words: cyber crime, threat, information, safety, antivirus