Hakeri i njihova etika

Vrančić, Ivona

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, University of Zagreb, Faculty of Humanities and Social Sciences / Sveučilište u Zagrebu, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:131:065368

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-20**

Filozofski fakultet
Sveučilišta u Zagrebu

Repository / Repozitorij:

ODRAZ - open repository of the University of Zagreb
Faculty of Humanities and Social Sciences

zir.nsk.hr

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2018./ 2019.

Ivona Petričević

Hakeri i njihova etika

Diplomski rad

Mentor: dr.sc. Kristina Kocijan, doc.

Zagreb 2019.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Ivona Petričević
(potpis)

Sadržaj

Izjava o akademskoj čestitosti ... 2
Sadržaj ... 1
1. Uvod ... 2
2. Početci računala ... 4
2.1. Prva računala ... 4
2.2. Prvi programer - programerka ... 6
3. Hakeri ... 10
3.1. Tko su hakeri ? ... 10
3.1.1. Podjele hakera ... 13
3.1.2. Faze hakerskog napada ... 14
3.1.3. Hakeri u eri velikih podataka ... 15
3.2. Hakeri kroz povijest ... 17
3.2.1. Kriptografija ... 17
3.2.2. Friking ... 19
3.3. Tema hakera u zabavnim sadržajima ... 21
3.3.1. Filmovi ... 21
3.3.2. Serije ... 23
3.3.3. Igrice ... 23
4. Etika ... 25
4.1. Etika informacijskog doba ... 26
4.2. Hakerska etika ... 27
4.2.1. Netika ... 30
4.2.2. Etični hakeri ... 31
5. Računalni kriminal i kako se zaštititi ... 35
5.1. Ciljevi, metode i koraci hakersko napada ... 35
5.1.1. Ciljevi hakerskog napada ... 35
5.1.2. Metode hakerskog napada ... 36
5.1.3. Koraci hakerskog napada ... 37
5.2. Zaštita ... 38
5.2.1. Problemi zaštite ... 38
5.2.2. Načini zaštite ... 40
6. Istraživanje ... 42
6.1. Rezultati ankete ... 42
6.1.1. Prva skupina pitanja ... 42
6.1.2. Druga skupina pitanja ... 50
6.1.3. Treća skupina pitanja ... 52
6.1.4. Četvrta skupina pitanja ... 57
6.1.5. Peta skupina pitanja ... 62
6.2. Analiza rezultata ankete ... 64
7. Zaključak ... 68
8. Literatura ... 70

1. Uvod

Pojam haker u društvu ima prizvuk tajanstvenosti i nepristupačnosti. Biti haker je činjenica koja se skrivala od javnosti. Pojam hakera je mijenjao svoje interpretacije, tako se razumijevanja ovog pojma razlikuju iz godine u godinu, kao i od čovjeka do čovjeka. Teško je pronaći jedinstvenu definiciju hakera, čak i sami hakeri će dati različite odgovore na pitanje: Tko je to haker? Hakeri su sve mlađi, a njihovi postupci sve drskiji. Pitanje privatnosti i velikih podataka je tema u koju hakeri sve više zalaze, ponekad u dobrim, a ponekad u zlim namjerama. U želji za znanjem i zabavom prelaze granicu etičnost, no ipak pokazujem kako postoji i hakerska etika. Unatoč čestim kršenjima društveno priznatih normi, oni pokazuju svoje etičke ciljeve i ideale o kojima ću pisati u ovom radu. Iako većina društva smatra hakere „štetočinama“ informacijskog doba, u ovom radu ću pokazati da uz negativne aspekte postoje i pozitivna djelovanja i mišljenja od strane hakera.

U dvadeset prvom stoljeću raste svijest o postojanju hakera, ali mišljenja o njima su različita. U ovom radu nalaze se odgovori na pitanja poput: Jesu li hakeri isključivo osobe koje čine kriminalne radnje ili postoje i hakeri dobrih namjera? Postoje li različite vrste hakera? Po čemu se razlikuju? Što ih potiče? Za što se zalažu?

Ovaj rad započinjem povijesnim razvojem koji je pogodovao nastanku današnjih hakera, nastavljam mogućim definicijama hakera i njihova viđenja vlastitog djelovanja te se dotičem frikinga kao jedne metode koja predstavlja začetak modernog hakiranja. Objašnjavam povezanost kriptografije i hakiranja, a nakon toga navodim primjere etičkih hakera, njihove namjere, motive i ciljeve. Nakon etičkih hakera definiram računalni kriminal te ga povezujem s hakiranjem. Navodim najčešće ciljeve, metode, korake hakera. S obzirom na to da postoje hakeri zlih namjera na definiram probleme u zaštiti koji olakšavaju hakerske napade te navodim načine zaštite. Provodim anketu kojom želim saznati upućenost društva u temu hakera, koji profil ljudi je hakirao ili je skloniji hakiranju, koje su motivacije i što potiče ispitanike na hakiranje. Hakerski pothvati su nerijetko na rubu moralno prihvatljivog djelovanja, stoga sam odlučila povezati njihovo djelovanje s etičkim teorijama: utilitaristička teorija, teorija dužnosti ili deontološka etika, aretaička

etika ili etika vrlina. Na kraju ankete ispitanike postavljam u hipotetsku situaciju te ih smještam u navedene etičke teorije.

2. Početci računala

Hakiranje u 20. i 21. stoljeću se temelji na računalima i programiranju, a računala su nastala uglavnom za potrebe računanja. Većina hakerskih napada se prvenstveno odvija pomoću računala i zbog podataka koji se nalaze na računalima. Znanja i vještine programiranja uvelike olakšavaju hakerske napade, stoga računala i programiranje predstavljaju dva temelja oko kojih se kreće hakiranje informacijskog doba.

Kako bi smo bolje razumjeli nastanak i razvoj hakera važno je predstaviti razvoj ideje modernih računala i prvih programera, kao i realizaciju te ideje. Snažan interes, želja za napretkom i otkrićem, znanje, umijeće i sposobnosti su karakteristike ljudi koji su kreirali prva računala. Iste karakteristike krase hakere 20. i 21. stoljeća. Osnivači prvih računalnih pomagala, računala, programiranja dijele iste strasti s hakerima, stoga nije na odmet pokazati kako su se izumi i izumitelji razvijali.

2.1. Prva računala

Povijest razvoja računala seže u puno dalju prošlost od 19. stoljeća. Od davnina je ljudima bila potrebna pomoć kako bi olakšali proces računanja. Tako je nastalo jedno od prvih računalnih pomagala Abakus. Vjeruje se da je nastao još u vrijeme Babilona gdje se koristio za brojanje i računanje (Encyclopaedia Britannica, 2016).

Među prva mehanička računala možemo uvrstiti **Pascalinu** i **Leibnizov stroj** za računanje (Freiberger, Swaine, 2019). Karakterizirale su ih mehaničke komponente. Pasacalinu je napravio Blaise Pascal[1] kako bi pomogao svojem ocu porezniku. Oduzimala je i zbrajala brojeve do 9 999 9999. Gottfried Wilhelm Leibniz[2] je napravio stroj za računanje koji je mogao zbrajati, oduzimati, množiti i dijeliti. Nakon Pascala i Leibniza, u 19. stoljeću Charles Babbage[3] radi na univerzalnom stroju za računanje o kojem ćemo više saznati u sljedećem podnaslovu

[1] Blaise Pascal je francuski filozof, matematičar i fizičar koji je živio od 1623. do 1662.
[2] Gottfried Wilhelm Leibniz je njemački filozof, matematičar, fizičar koji je živio od 1646. do 1716.
[3] Charles Babbage je engleski matematičar, filozof, inženjer strojarstva koji je živio od 1791. do 1871.

Zahvaljujući primjeni električne energije nastaju prva elektromehanička računala. Herman Hollerith stvara **stroj za sortiranje** koji se koristi bušenim karticama. Skratio je popisivanje stanovništva s 3 godine na 2 tjedna. 1896. godine je osnovao Tabulathing Machine Company koja kasnije dobiva ime IBM (engl. International Business Machine).

Tommy Flowers vodi stvaranje **Colossusa** 1943., prvog električno, digitalno, djelomično programiranog računala. Imao je preko 2000 elektronskih cijevi, binarni sustav te ga možemo smatrati prethodnikom modernih računala. Potreba za Colossusom je porasla kada su Nijemci počeli kodirati važne njemačke poruke za vrijeme Drugog svijetskog rata. Nakon rata je sva dokumentacija uništena pa se tako ENIAC držalo majkom računala.

1945. godine je napravljeno elektroničko računalo po imenu **ENIAC**, Elektronički Numerički Integrator i Kalkulator (engl. *Electronic Numerical Integrator and Calculator*). John Adam Persper Eckert, John Mauchlay i von Neuman su glavni inženjeri ovog računala koje je koristilo elektronske cijevi..

Pedesetih godina dvadesetog stoljeća nastaje UNIVAC, Univerzalno Automatsko Računalo (engl. *Universal Automatic Computor*) koje započinje trend proizvodnje računala za obradu podataka u profitabilne svrhe.

Razvoj modernih računala težio je širokom repertoaru svrha za što su zaslužni Ada, Babbage i Alan Turing. Turnig je razradio ideju **Turingovog stroja** koji je prema njegovoj zamisli trebao biti u mogućnosti učiniti sve radnje koje bi radili drugi pojedini strojevi. Stvorio je ideju jednog univerzalnog stroja koji može odraditi sve radnje ostalih strojeva. Umjesto pojedinog stroja za pojedinu funkciju, on uvodi ideju jednog univerzalnog stroja koji posjeduje sve potrebne funkcije (Encyclopaedia Britannica, 2019).

Isaacson (2014: 87) je odlično prikazao Turingov doprinos usmjerenju razvoja računala navodeći važan citat iz Alanove knjige Inteligentni strojevi (engl. *Intelligent Machinery)* (1948). Alan Turing je jednom napisao „*Ne moramo imati beskonačno različitih strojeva koji rade različite poslove,*" … "*Jedan će biti dovoljan. Inženjerski problem proizvodnje različitih strojeva za različite poslove zamjenjuje uredski rad programiranja univerzalnog stroja za obavljanje tih poslova*."[4] Njegova vizija će imati

[4] Ovo je slobodni prijevod, Izvorno: engl. "*We do not need to have an infinity of different machines doing different jobs,*" … "*A single one will suffuce. The engineering problem of producing various machines for various jobs is replaced by the office work of programming the universal machine to do these jobs*".

izniman utjecaj na daljnji razvoj računala i njihovu primjenu. Svrha računala, ili bilo kojeg novog uređaja će postati ujedinjenje više uređaj i njegovih upotreba.

Elektroničku obradu Dragičević (2004: 10) dijeli na šest generacija računala u skladu s vremenom nastanka i sastavnim elementima. Prva generacija je trajala od 1951. godine do 1958. godine. Karakterizira ju korištenje elektronskih cijevi[5] i kablovske veze u obradi podataka. U ovu generaciju spadaju prva računala ENIAC i UNIVAC. U drugoj generaciji između 1959. i 1963. godine se koriste tranzistori[6] koji su smanjili fizičke dimenzije računala. TX-0 ili Tixo na MIT-u (engl. *Massachusetts Institute of Technology*) je prema Levyu (1994) prvo računalo koje je koristilo tranzistore. U trećoj generaciji od 1964. do 1970. godine se koriste integrirani krugovi i programski jezici. U četvrtoj generaciji između 1971. i 1987. se koriste integrirani poluvodički sklopovi[7]. U razdoblju između 1989. i 1992. se nalazi peta generacija računala u kojoj se računala baziraju na paralelnoj arhitekturi i arsenid čipovima[8]. Od 1993. godine počinje šesta generacija koja razvija neuronske mreže[9], umjetnu inteligenciju i ekspertne sustave koji oponašaju znanje stručnjaka.

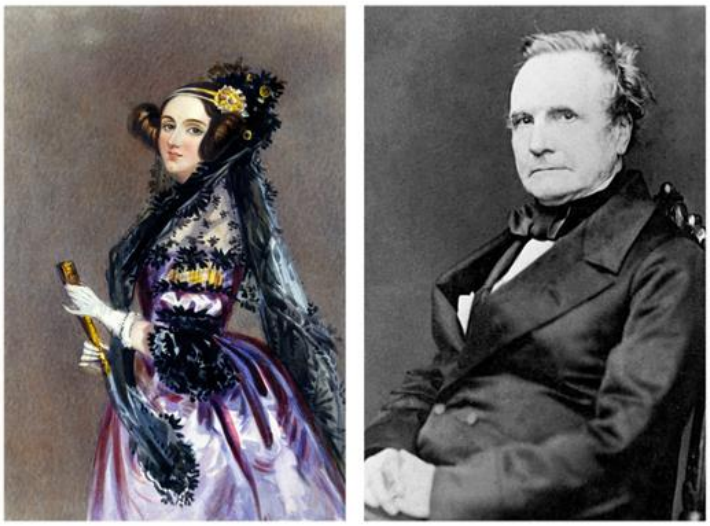
2.2. Prvi programer - programerka

Devetnaesto stoljeće je imalo veliku ulogu u razvoju modernih računala i programiranja. S obzirom na usku povezanost hakiranja i programiranja Walter Isaacson (2014) u tom kontekstu detaljnije opisuje život i postignuća grofice od Lovelacea i Charlesa Babbagea. U 19. stoljeću Augusta Ada King (slika 1 - lijevo), grofica od Lovelacea, kćer pjesnika lorda Byrona je pokazivala veliki interes za Charlesa Babbagea (slika 1 - desno) i njegov rad. Molila ga je za mentorstvo, no Babbage ju je odbio u svrhu očuvanja

[5] Elektronska cijev je elektronički element u kojem se do električne struje dolazi strujanjem elektrona u vakuumu ili sniženom tlaku u cijevi (Hrvatska enciklopedija. Elektronska cijev.).
[6] Tranzistor je aktivni poluvodički elemnt koji se koristi za upravljanje signala (Hrvatska enciklopedija. Tranzistor.).
[7] Integrirani sklop upravlja elektroničkim signalima (Hrvatska enciklopedija. Integrirani sklop.).
[8] Čip se koristi kao nosač elektroničkog elementa ili integriranog sklopa (Hrvatska enciklopedija. Čip.).
[9] Neuronska mreža se sastoji od skupa umjetnih neurona koji su povezani po uzoru na ljudski mozak (Hrvatska enciklopedija. Neuronska mreža.).

prijateljstva i suradnje. Tako je za mentora dobila Augustusa De Morgana, poznatog britanskog matematičara i logičara.

Iako je kćer pjesnika, Ada je uvijek više naginjala znanstvenoj strani. Babbageov rad sa strojevima je privukao je njenu pozornost. Najviše pozornosti zaplijenio je Babbageov rad na strojevima koji su sposobni obavljati ljudske zadatke. Babbage je svoju inspiraciju pronalazio u Pascalu i Leibnizu, upravo ta inspiracija ga je tjerala da nadiđe Pascalinu i Leibnizov kotač. Imajuću u vidu navedeni cilj, radio je na **diferencijalnom stroju** koji je mogao prikazati bilo koju polinomnu funkciju[10] i dati digitalnu metodu za automatsko izračunavanje. Njegov stroj je koristio vertikalne osovine s diskovima koji se mogu okretati u bilo kojem broju. Oni su bili pričvršćeni na zupčanike koji su se mogli napuknuti kako bi se disk dodao na susjednu osovinu. Imao je sposobnost pohranjivanja rezultata na drugu osovinu.



Slika 1. S lijeve strane Ada Lovelace, s desne strane Charles Babbage (H-Wilson, Danielle. Preuzeto s https://digitalblog.coop.co.uk/tag/charles-babbage/)

Britanska vlada je bila impresionirana njegovim radom te mu daje novac kako bi kreirao tablicu brojeva do 10 milijuna. Unatoč poticaju Babbage nije posjedovao mogućnosti za stvaranje funkcionalnog stroja, stoga je počeo raditi na novoj ideji,

[10] Polinomne funkcije su računske operacije poput zbrajanja, oduzimanja, množenja.

analitičkom stroju. Ovaj stroj je imao širu namjenu, mogao je odrađivati različite operacije temeljene na programskim uputama koje bi mu zadali. Mogao je obavljati jedan zadatak, pa se prebaciti na drugi, ili mijenjati obrazac djelovanja. Britanska vlada više nije imala interes za njegov novi naum, no privukao je pozornost mlade Ade. Ona je uvidjela spoj poezije, mehanike i matematike u njegovom izumu. Primijetila je da bi stroj mogao procesuirati simboličke notacije, pa čak muzičke i umjetničke. Odlučila mu je pomoći u traženju podrške i biti njegov publicist (Encyclopaedia Britannica, 2019).

U svojim bilješkama u opisu stroja, postavila je četiri koncepta koji će biti iznimno važni stoljeće nakon, kada nastaje računalo. Bilješka A kaže kako stroj može izvoditi unaprijed definiran zadatak, može se programirati i reprogramirati pomoću probušenih kartica tako da obavlja neograničen i promjenjiv niz zadataka. Drugi koncept izvodi tvrdnju kako je to opće namjenski stroj koji nije ograničen samo na matematiku i brojeve. On može obraditi bilo što što se može izraziti simbolima. Bilo kakav sadržaj, glazba, tekst, mogu biti izraženi u digitalnom formatu kojim stroj može rukovati; tako da znamenke na zupcima mogu predstavljati bilo što osim matematičkih izraza. U trećoj, G bilješci, Ada tvrdi kako bi stroj mogao generirati Bernoullieve brojeve[11]. Tablica kojom je ilustriran proces se može uzeti kao prvi računalni program. U listi su se nalazile kodirane instrukcije koje su bile slične današnjem C++. Zadnji važan koncept u njezinim bilješkama je bilo pitanje: Mogu li strojevi misliti? Ada je ipak bila svjesna kako ovaj stroj može izvršavati samo zadane zadatke na zadani način, te da ne mogu davati ideje niti misliti za sebe. Adine i Babbageove ideje objavljene su u Taylorovoj seriji knjiga Scientific Memoirs 1843 (Science Focus, 2018).

Na posljetku, stroj nisu uspjeli dovršiti. Usprkos neuspjehu u dovršavanju projekta Ada Lovelace je postala feministička ikona u znanosti i povijesti razvoja digitalnog doba. Babbagea se nerijetko naziva ocem modernih računala, a Adu prvom programerkom.

Grace Brewster Murray Hopper je također uvidjela važnost programiranja kao i Ada Lovelace. Hopper je profesorica matematike koja je željela za vrijeme Drugog svjetskog rata biti dio mornarice, završila je u timu koji je radio na Mark I[12]. Pri tome je

[11] Niz racionalnih brojeva koje je otkrio Jacob Bernoulli.
[12] Mark I je računalo sa Sveučilišta Harvard korišteno za svrhe Drugog svjetskog rata.

dobila bilješke Charlesa Babbagea koje su joj pomogle pri pisanju **prvog priručnika za računalno programiranje** (Isaacson, 2014).

3. Hakeri

Blaise Pascal, Gottfried Wilhelm Leibniz, Herman Hollerith, Tommy Flowers, John Adam Persper Eckert, John Mauchlay i von Neuman, Ada Lovelace, Charles Babbage i Alan Turing su samo neki od znanstvenika i izumitelja zaslužni za današnji razvoj tehnologije. Oni, i još mnogi njihovi kolege su utemeljili put budućim izumima. Upravo zbog njih raste strast i želja za znanjem, napretkom i otkrićima na informacijskom području. Iste strasti je naslijedila većina modernih informacijskih znanstvenika, ali i jedne posebne skupine ljudi, hakera. U ovom odlomku ćemo saznati tko su i tko su nekada bili hakeri, kako oni sami sebe doživljavaju, te koje su to njihove strasti, želje i ciljevi. Saznati ćemo zašto su oni važni za naše društvo, te kako mogu pomoći ili odmoći u rukovanju informacijama u 21. stoljeću.

3.1. Tko su hakeri ?

Razvojem računala nastaje potreba za osobnim računalima, istovremeno se počinje vjerovati kako računala mogu služiti za zabavu. Hakeri su se podijelili na one koji su voljeli šalu, programerske trikove, igračke i igre. Drugi su bili pobunjenički nastrojeni, zainteresiraniji za upadanje u sustave. Pedesetih godina dvadesetog stoljeća pojam haker je označavao ljude koji su se odlično razumjeli u računala. To su ljudi koji su se strastveno, sa žarom bavili računalima kao hobijem. Biti haker je značilo poštovanje i ponos. Šezdesetih i sedamdesetih godina dvadesetog stoljeća pojam haker se počinje koristiti za osobe koje bez dozvole pristupaju računalnim mrežama.

Teško je precizno definirati pojam hakera. Postoji više stavova kao odgovor na pitanje: **Tko je haker?**

Prema Eric S. Raymondu (1998) haker (engl. *hacker*) izvorno označava osobu koja izrađuje namještaj sjekirom. Eric daje osam mogućih razumijevanja pojma haker. Definira hakera kao osobu koja uživa istražujući detalje programskog sustava i kako proširiti njegove sposobnosti. Onaj koji entuzijastično, čak i opsesivno programira. Osoba koja cijeni hakerske vrijednosti, brza je u programiranju. Haker može biti ekspert za bilo koji

program ili bilo tko ga često koristi. Haker također može označavati bilo kakvog entuzijastu koji ne mora biti nužno vezan uz računalo. Na primjer haker može biti astronom koji je entuzijastičan oko onoga što radi. Hakeri se mogu definirati i kao osobe koje vole intelektualne izazove i kreativno prelaženje granica. Zadnje definiranje pojma haker je da je on zlonamjerna osoba koja pokušava otkriti osjetljive informacije. Prikladniji naziv za ovo definiranje hakera je **kreker** (engl. *cracker*) koji u prijevodu znači razbijač i provalnik. Dražen Dragičević (2004: 67) kaže „*Hakerstvo se, danas, najčešće svodi na neovlašten pristup informacijskim resursima s namjerom da se kopiraju podaci, prenesu maliciozni programi (virusi, crvi, trojanski konji itd.), promijene ili izbrišu postojeći podaci i/ili programi ili pak onemogući daljnje korištenje sustava*.“.

Anoniman haker u dokumentarnom videu (captjack5169, 2013: 3:45) daje svoje viđenje hakiranja: „*Hakiranje za mene je dobivanje informacija koje želim*.“[13] Za njega zakon ne predstavlja etičku prepreku, jedino važno je dobiti željene informacije. Hakeri u slučaju napada za metu uzimaju uglavnom veće korporacije zbog tajnovitosti podataka i neetičkog poslovanja. Individue postaju meta ako haker ima određeni motiv vezan uz tu metu. Do većine napada dolazi zbog želje za znanjem i iskustvom. Znanje je jedan od najvažnijih motiva koji pokreće hakere. „*Ponekad je potrebno prekršiti zakon da bi dobili potrebne informacije, inače nitko ne bi ništa naučio*.“[14] (captjack5169, 2013: 4:47).

Hakeri većinu svojih vještina nauče sami. Hakiranje ne mora biti nužno vezano uz zlonamjerne aktivnosti, već može biti bezazleno upadanje u neki sustav samo u svrhu istraživanja. Ralph Echemendia je poznati etički haker koji je posjetio Hrvatsku na Danima komunikacija u ožujku 2019. godine. Definira hakere kao ljude koji ne znaju, a djeluju i pri tome uče. Kao ljude koji koriste stvari na načine koje nisu namjeravali koristi ljudi koji su izumili te stvari (Pioneers, 2017: 2:20).

U većini stavova se nalazi i ideja da je hakiranje vezano uz pristupanje informacijama i sustavima za koje nemamo dozvolu, te da je to djelatnost vezana isključivo uz tehnologiju. Mnogo ljudi smatra kako je to aktivnost vezana isključivo uz zle namjere, no važno je imati na umu da postoje i dobri hakeri.

---

[13] Ovo je slobodni prijevod, Izvorno: engl. “*Hacking for me is getting the information that I want*.”.
[14] Ovo je slobodni prijevod. Izvorno: engl. “*Sometimes you have to break the law to get the information you want*.”.

Kevin David Mitnick je najpoznatiji američki haker. Još kao dijete je radio nepodopštine koristeći friking metodu o kojoj piše detaljnije u odlomku pod nazivom Friking. Sa sedamnaest godina je provalio u Sjevernoameričko računalo za zapovjedništvo zrakoplovne obrane. Zbog toga su ga smatrali nacionalnom opasnošću, te je nekoliko puta uhićivan. Prije suđenja je zatvoren na godinu dana u samicu jer je sudac bio uvjeren kako je Mitnick u stanju započeti nuklearni rat zviždanjem pomoću govornice u zatvoru. Intrigiran načinom rada mobilnih i telefonskih uređaja hakirao je mobilne kompanije. Zanimalo ga je kako mobiteli rade pa je hakirao u proizvodnju Nokije i Motorole. Za Mitnicka su to bili samo trofeji, a želja za znanjem i stvaranje nepodopština su ga tjerale da i dalje hakira. Osjetljive podatke je pohranio na serveru sveučilišta u Los Angelesu. Admini su to primijetili i pozvali FBI (engl. *Federal Bureau of Investigation*), Savezni Ured za Istrage koji je obavijestio mobilne kompanije. Važnosti ovog događaja pridaje činjenica da mobilne kompanije nisu bile svjesne hakiranja njihovog sustava sve do trena javljanja FBI-a. Mitnicka su optužili za hakiranje hardvera Digital Equipment Corporation, hardvera tvrtke Pacific Bell i sustava tvrtki kao što su Motorola, NEC i Nokia. Nakon izlaska iz zatvora započinje karijeru kao savjetnik za sigurnost (Silicon Republic, 2018).

Kako bi dobili uvid u uspješnost hakera, Ars Technica je zamolila tri hakera da napadne listu od 16 000 lozinki. Najmanje uspješan haker je u sat vremena identificirao 62% lozinki. Najuspješniji haker je u 20 sati identificirao 90% lozinki. Svoje napade hakeri izvršavaju pomoću liste riječi koje se najčešće pojavljuju u lozinkama. Koriste razne kombinacije i varijacije dok ne dobiju rješenje (Quinn, 2017).

Najveća hakerska konvencija osnovana je 1992. godine pod imenom **DEFCON** u Las Vegasu u obliku zabave na kojoj se pojavilo stotinjak ljudi. Na dvadesetoj DEFCON konferenciji je prisustvovao direktor NSA-e (engl. *National Security Agency*), general Alexander. Pojavilo se je preko 10 000 ljudi iz različitih zemalja. Društvo na konvenciju DEFCON promatra kao anonimni nelegalni skup na kojem se uče nelegalne djelatnosti. Suprotno navedenome, sami polaznici DEFCON-a ga definiraju kao javno financiran privatni party na koji dolaze hakeri kako bi se družili, razmijenili znanja i postignuća (The Documentary Network, 2017).

3.1.1. Podjele hakera

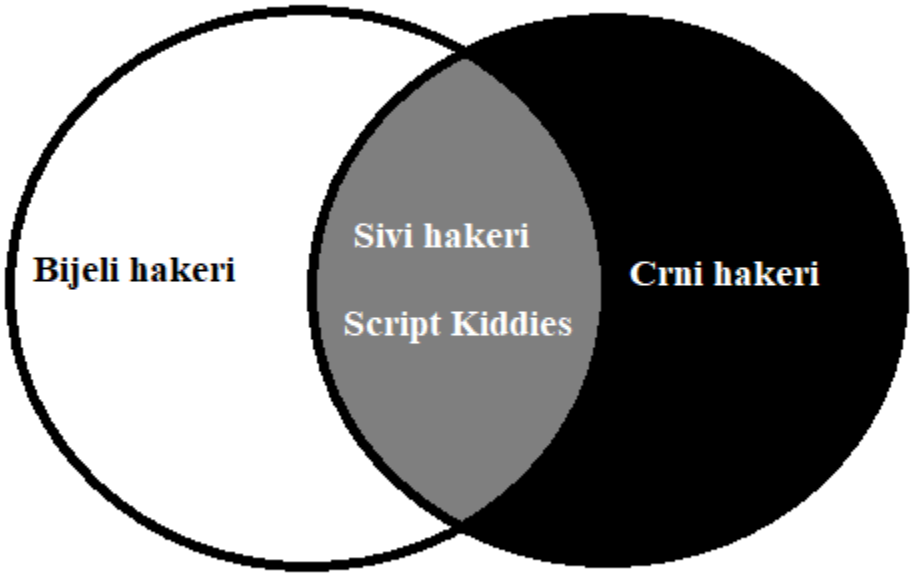
Iako mnogo ljudi na spomen hakera imaju pred očima sliku kriminalca, istina i nije takva. Nisu svi hakeri isti, nemaju svi hakeri iste motive, želje i ciljeve. Postoje dobronamjerni i zlonamjerni hakeri, no postoje i hakeri koji se nalaze između. Vladica Babić (2009) dijeli hakere na **crne** (engl. *black hat hacker*), **bijele** (engl. w*hite hat hacker*) **sive** hakere (engl. *gray hat hacker*) i **Script Kiddie**s. Podjelu vidi na slici 2.

Crni hakeri ili hakeri crnih šešira su karakteristični po svojim zlim namjerama. Kradu osobne podatke, važne informacije, brojeve kartica (Technopedia, Black hat hacker.).

Script Kiddies je pogrdni naziv za sive hakere, pijavice, koji koriste lako nađene gotove alate i programe izrađene od strane drugih hakera. To su najčešće maloljetne osobe s malo iskustva a žele slavu i znanje. Mnogi Script Kiddies hakeri ne razumiju što rade prilikom hakerskog napada pa su zbog toga često ismijavani od strane ostalih hakera.

Bijeli hakeri ili hakeri bijelih šešira svoje znanje koriste kako bi očuvali i poboljšali sigurnost sustava i mreža. Oni su obrana od crnih hakera, legalno zaposleni ljudi koji koriste slične ili iste metode kao i crni hakeri. Dobili su naziv po kaubojskim filmovima u kojima dobri dečki uvijek nose bijeli šešir (Technopedia, White hat hacker.).

Sivi hakeri se ne drže etičkih načela, vrše istu djelatnost kao i crni hakeri, ali bez zle namjere. Ova skupina hakera javno objavljuje slabe točke u sigurnosti sustava, dok bijeli to rade samo unutar tvrtke za koju rade (Technopedia, Grey hat hacker.).



Slika 2. Podjela bijelih, crnih, sivih hakera i Script Kiddies, (Preuzeto iz Babić, V. Kompjuterski kriminal, 115.)

3.1.2. Faze hakerskog napada

Vladica Babić (2009) dijeli faze hakerskog napada na ilegalnu i legalnu koja se sastoji od pripremne i faze planiranja.

Pripremnu fazu karakterizira odabir mete, prikupljanje informacija, inženjering podrška, mrežna podrška, konsolidacija s podzemljem. Haker bira metu o kojoj prikuplja informacije strvinarenjem ili sličnim aktivnostima. Put do mete, softverska i hardverska podrška se uređuje inženjerskom podrškom. Haker bira metodu i tehniku napada te **planira** rezervni plan. Razmišlja o riziku koji sa sobom nosi njihovo djelo te kako će ukloniti dokaze svoje prisutnosti.

Ilegalna faza je faza izvršenja djela

Faza izvršenja se odnosi na instalaciju stražnjih vrata (engl. *back door*) alata pomoću kojeg haker neprimjetno ulazi u računalo, preuzima kontrolu nad njim ili čini bilo što ne legalno. Haker mora brisati datoteke na kojima se vide bilo kakvi

tragovi zločina. Primjer bi bio uklanjanje stražnjih vrata. Takav postupak se zove ubiti (engl. *kill*). Kako bi ga bilo teže pratiti najčešće radi na drugom računalu, na kojem nisu izvršene priprema i planiranje.

3.1.3. Hakeri u eri velikih podataka

Veliki podatci (engl. *Big data*) su najprisutniji kod organizacija u poslovnom sektoru. Velike podatke karakterizira obujam, raznolikost i brzina kojom informacije rastu. Ti podaci su pre veliki da bi se analizirali tradicionalnim bazama podataka, a uz njih javljaju se i etička pitanja vezana uz rukovanje velikim podacima. Pitanje identiteta, privatnosti, vlasništva i reputacije su velika etička pitanja koja se vežu uz etiku velikih podataka. Ciljani marketing, medicina, društvene mreže i mnogi drugi se koriste velikim podacima i nose vezane rizike. Upravo hakeri predstavljaju najveću opasnost zbog svojih sposobnosti krađe ili manipuliranja velikim podatcima. Pred kompanije koje posjeduju i obrađuju velike podatke je stavljena odgovornost očuvanja i etičkog djelovanja tim istim podacima.

Jeroen van den Hoven, Martijn Blaauw, Wolter Pieters, Martijn Warnier (2014) napominju važnost rudarenja velikih podataka. Rudarenje velikih podataka koristi se kako bi se primijetio uzorak u ponašanju korisnika. Na temelju uzoraka koje stručnjaci primijete donose se poslovne odluke vezane za korisnika. Ti podaci mogu procuriti u javnost, pomiješati se i pružiti krivu uslugu što na primjer u medicinskom sektoru može biti kobno. Potrebno je održati balans između rizika i inovacija koje nam veliki podaci omogućuju. Za dobrobit društva nužno je uskladiti etičke vrijednosti s djelovanjem. Tvrtke koje rade s velikim podacima su dužne zaštiti bazu podataka s podacima građana, spriječiti računalnu zloupotrebu, i zaštititi intelektualno vlasništvo. Tehnologija velikih podataka nema vrijednosni okvir, ali ga imaju individualci i tvrtke koje koriste velike podatke. Postaje veliko etičko pitanje kako će oni postupati s našim privatnim podacima. Aktivnosti u kojima se nalaze etički trenuci za donošenje odluka vezanih uz rad s velikim podacima su ispitivanje, analiza, artikulacija, djelovanje. **Ispitivanje** nam pomaže otkriti i razumjeti što vrijednosti jesu.

U ovome kontekstu etičku vrijednost predstavlja **transparentnost** prilikom korištenja velikih podataka. **Analiza** je stupanj provjere kako se trenutačna uporaba velikih podataka slaže s vrijednostima koje smo odabrali. Primjer analize je odluka treba li stvoriti novu značajku proizvoda koristeći velike podatke. **Artikulacija** je trenutak u kojem se pisano izražava podudarnost i razlike između odabranih vrijednosti i prakse. To je trenutak u kojem biramo hoćemo li koristeći tehnologiju velikih podataka podržati ili odbaciti odabrane etičke vrijednosti. **Točka akcije** taktizira kako uskladiti odstupanja koja su se definirala i kako održati tu usklađenost s vremenom. Na odabranom primjeru to znači kako je potrebno upoznati korisnike kako će novi proizvod koristiti osobne podatke. Velike kompanije, koje su česta meta hakera, imaju veliku odgovornost prilikom uporabe i zaštite osobnih podataka. (Davis & Patterson, 2012) Za izvlačenje, transformaciju i analizu podataka dobro je biti pomalo haker, zaključuje Davenport (2014). Znanstvenici koji se bave podacima moraju znati šifrirati ili programirati, razumjeti arhitekturu velikih podataka.

Kada bi haker dobio pristup podacima neke velike tvrtke, na primjer banke, mogao bi izmijeniti poslovne izvještaje kako njemu odgovara što bi moglo dovesti do potpuno drugačijih poslovnih odluka unutar te firme. Konkretno, hakeri bi mogli promijeniti financijske odluke banke, kontrolu nad tehnološkom opremom koja regulira razine vode, tlak plina, željezničke mreže itd., ovisno o tome što ili koga bi uzeo za metu.

Velike agencije koje su zadužene za potrošačke kredite sakupljaju i prodaju podatke o korisnicima. Dobivaju kompletan profil svake osobe, i te informacije se koriste za dobivanje kredita, pronalaženje posla, iznajmljivanje kuće… Podaci postaju novac. J. Sadowski (2017) u britanskim dnevnim novinama The Guardian skreće pažnju na velike podatke koji se sve češće nazivaju novom naftom ili novim kapitalom. Ti svi podaci su mamac za hakere. Equifax je tvrtka za analizu podataka i tehnologija koja djeluje uglavnom u Sjevernoj, Srednjoj i Južnoj Americi, Europi i Aziji. Pomaže organizacijama u donošenju poslovnih i osobnih odluka. 2017. godine se dogodio hakerski napad koji je trajao čak 76 dana bez primjećivanja. Unutar tog vremena hakeri su ukrali imena klijenata, brojeve socijalnog osiguranja, datume rođenja i adrese 147,7 milijuna Amerikanaca. Velike tvrtke poput Equifaxa zarađuju na osobnim podacima, a ne brinu o zaštiti privatnih podataka jer

nema značajnih zakonskih posljedica za firmu. Veliki podaci predstavljaju veliku odgovornost (Alfred Ng, 2018).

Postoje hakeri koji će iskoristiti slabosti i oštetiti milijune ljudi, ali postoje i etički hakeri o kojima će biti riječ u četvrtom poglavlju. Njihova uloga je upravo spriječiti katastrofe poput napada na Equifax.

U svrhu zaštite osobnih podataka na snagu dolaze zakoni i propisi koji reguliraju proces uzimanja, obrade i prodaje podataka. Svaka osoba mora dati osobni pristanak i biti informirana o svrsi obrade njezinih podataka.

3.2.Hakeri kroz povijest

Hakeri su postojali i prije nastanka računala. Jedna od definicija hakera prema Ericu S. Raymondu (1998) je da je on zlonamjerna osoba koja pokušava otkriti osjetljive informacije. U tom razumijevanju, hakeri su postojali od kada postoje ljudi i informacije. Krađa podataka je postojala i prije Babilona, Egipta i Mezopotamije. Uzimajući ovu definiciju u obzir, hakeri su postojali pod imenom kradljivac i lopov. Tek u 20. stoljeću dolazi riječ haker u smislu koii prvenstveno predstavlja osobu sa znanjem i vještinama rukovanja tehnologijom. Nije trebalo puno vremena da se pojam vještine i iskustva ujedini s pojmom kradljivca i lopova u riječi haker. Jedna od važnih vještina koja je pogodovala ovim hakerima je kriptografija.

3.2.1. Kriptografija

Kako je jedno od mišljenje da je hakiranje vezano uz pristupanje informacijama i sustavima za koje nemamo dozvolu, **dešifriranje šifre** stoji kao jedan od najčešćih načina na koji haker želi ući u računalni sustav. U tom kontekstu kriptografiju možemo vezati uz hakiranje. Kriptografija želi sakriti postojanje poruke kao i njezino značenje pomoću enkripcije. Hakeri se često susreću s kriptografijom i šifriranjem kako bi probili sigurnosne sustave, kako bi sakrili svoj identitet prilikom kriminalnih radnji. Kriptografija je grana

kriptologije koja tisućljećima služi za zaštitu podataka. Zaštita podataka postaje relevantna tematika informacijskog doba.

Enkripcija je šifriranje ili kodiranje, dok se šifrirani tekst naziva **šifrat**. **Šifra** predstavlja postupak kojim se šifrirani tekst dešifrira. Pošiljatelj poruke **ključem** šifrira poruku, a primatelj poruke pomoću ključa može dešifrirati poruku. Simon Singh (2002) daje povijest kriptografije i uočava njezinu povezanost s hakiranjem za vrijeme Prvog i Drugog svjetskog rata.

1917. Arthur Zimmermann je bio njemački ministar vanjskih poslova koji je želio sklopiti dogovor s Meksikom protiv SAD-a[15]. U tom dogovoru Zimmermann obećava vraćanje Teksasa i pomoć s novcem i oružjem Meksiku. Tako bi SAD oslabio zbog borbi na više fronti. U to doba komunikacija se odvijala putem telegrafskih kablova. Britanski razbijači šifri su prisluškivali tu komunikaciju. Poruka je bila kodirana. Nigel de Grey i Montgomery, britanski razbijači šifri, dekodiraju njemački pokušaj sporazuma s Meksikom protiv SAD-a. Nakon objave ove tajne namjere SAD objavljuje rat Njemačkoj, a Nigel de Grey ostaje aktivan i u Drugom svjetskom ratu na području dešifriranja tajnih njemačkih poruka.

U Drugom svjetskom ratu u kriptiranju je glavnu riječ imao stroj po imenu Enigma (Slika 3). Nijemci su znali kako radio komunikacija više nije sigurna pa su koristili ovaj stroj kako bi šifrirali poruke koje su si međusobno slali. Poruka unesena preko Enigme strancu izgleda potpuno besmisleno. Tek kada se ta poruka ponovno unese u Enigmu postaje smislena. Ovaj stroj je bio poseban zbog velikog broja kombinacija koje je mogao izvesti. Kako bi druga Enigma mogla dešifrirati poruku trebala je biti postavljena jednako kao i ona s koje je poruka poslana. Dakle, oba stroja su trebala biti jednako postavljena kako bi primatelj razumio pošiljatelja.

Dekodiranja su se odvijala u britanskom centru za dekodiranje Bletchley Parku u Sobi 40. Alan Turing je engleski matematičar i računalni znanstvenik koji je značajno pridonio razbijanju Enigme. Sve aktivnosti vezane uz kriptoanalizu bile su tajne. Tek se 1970-tih objavljuje istina vezana uz Enigmu, a šifrolomci dobivaju priznanje.

[15] Sjedinjene Američke Države.

U 21 stoljeću zaštita informacija dobiva sve veću važnost, a kriptografija nam u toj zaštiti pomaže. Informacije su se nekada slale papirom, no danas prevladavaju informacije u digitalnom obliku. Kriptologija i enkripcija su svoje težište u novo doba prebacile na digitalnu tehnologiju. U Americi su željeli zabraniti enkripciju jer se iza nje često skrivaju kriminalne radnje, dok na drugoj strani velike kompanije žele zaštiti svoje podatke kako ne bi hakeri ušli u računalo i ukrali tajne informacije. Jedan od prvih programa za enkripciju koji se koristio na Internetu je PGP (engl. *Pretty Good Privacy*)[16] Phila Zimmermanna.

Slika 3. Enigma. (Riffe, S. Preuzeto s https://www.cmu.edu/news/stories/archives/2018/february/enigma-machines.html)

3.2.2. Friking

Sedamdesetih godina dvadesetog stoljeća započelo je hakiranje preko telefonskih mreža. Tada su telefonske mreže bile kontrolirane tonovima, pa je bilo lako ući čak pomoću obične igračke. John Draper je otkrio kako je zviždaljka iz pahuljica imala potrebnu frekvenciju. Njezin ton je bio upravo onakav kakav je trebao za pokretanje besplatnog poziva. Osnivači frikinga su većinom bili slijepi. Poznato je kako slijepi ljudi često imaju druga osjetila bolje razvijena što objašnjava pronalazak identičnog zvuka. Izraz friking (engl. p*hreaking*) je složen od engleskih riječi telefon (engl. *phone*), slobodan (engl. *free*) i nakaza (engl. *freak*). Kod kuće se nikada nije frikalo kako ih telefonske kompanije ne bi primijetile. Kako bi olakšali uspostavljanje besplatnih poziva osmislili su plavu kutiju

[16] Prilično Dobra Privatnost.

(engl. *blue box*) (Slika 4), uređaj koji generira određen set tonova, za koje telefonska kompanija misli da dolaze od njihove opreme. Osoba bi saznala da je njena linija korištena tek kada bi bio ispostavljen račun. Tajno društvo se sastajalo na konvencijama na kojima su se nosile maske kako se ne bi otkrio identitet. Frikeri su razvili socijalni inženjering. Ulazili su unutar telefonskih kompanija i razgovarali s ljudima uvjeravajući ih kako su oni radnici te kompanije. Tako su dobivali informacije iz kompanije koje bi im bile potrebne. Zabava i nepodopština je bila jedan od motiva za djelovanja pa su tako obavljali pozive u strane zemlje samo kako bi čuli strani jezik (Chạm Mưa, 2017).

Slika 4. Blue Box. (Ewbank, A. Preuzeto s https://www.atlasobscura.com/articles/capn-crunch-whistle)

Većina frikera nije imala novaca da si priušti obavljanje telefonskih poziva diljem svijeta. Oni koji su i imali novaca, protivili su se politici telefonske kompanije koja je imala u cilju samo zaradu. Frikere je motivirala borba protiv telefonskih kompanija, u kojoj su se zalagali za besplatno telefoniranje.

Kada su ih telefonske kompanije otkrile, započele su velike istrage i uhićenja frikera. Za posjedovanje plave kutije dobivalo se do dvije godine zatvora. Prvi poznati frikeri su bili Joe Enggressia, John Draper, Steve Wozniak i Steve Jobs. Telefonski friking (engl. *phone phreaking*) je bilo učenje kako koristiti tehnologiju, kako ući, iskoristiti i proširiti tehnologiju koja nije bila dostupna široj populaciji (Chạm Mưa, 2017).

U tadašnje vrijeme je bilo nezamislivo imati kućno računalo, sve dok se nije pojavio Altair, računalo koje su ljudi mogli sami sastavljati kod kuće (captjack5169, 2013). Ljudi koji su ga posjedovali su se nalazili u grupama i razmjenjivali probleme i rješenja. Glavno je pitanje bilo što može raditi računalo. Čemu ono služi? Računala su bila zanimljiva jer se

na njima moglo istraživati i učiti. Najviše je otkriveno i naučeno o računalima u kućnoj radinosti zbog nedostatka pravila kojih se moraju pridržavati. Kod kuće je bila prisutna toliko važna sloboda prilikom učenja i istraživanja, kao i razmjena iskustava i znanja s prijateljima. Tako su nastali hakeri 20.stoljeća koji će svoje djelovanje nastaviti u idućem.

3.3.Tema hakera u zabavnim sadržajima

Valja ponovno spomenuti činjenicu da su hakeri prvenstveno bili osobe koje se cijenilo i poštovalo zbog njihova znanja i predanosti. Kroz nekoliko godina taj pojam postaje obavijen isključivo negativnim konotacijama. Haker odjednom za društvo postaje tinejdžer kriminalac koji može učini nezamislive štete.

Toj promjeni shvaćanja pojma haker, uz povremene hakerske napade, najviše su doprinijeli filmovi, serije i igrice. U 20. stoljeću prevladavaju filmovi koji ocrnjuju hakere, no kako se primiče i protječe 21. stoljeće tako tematika hakera u navedenim kategorijama dobiva svjetliju konotaciju.

3.3.1. Filmovi

Mnogo filmova je snimljeno na temu hakera, a ovdje navedeni su jedni od najpoznatijih i najutjecajnijih. Prema sadržaju filma vidimo kako se kroz godine mijenjaju i miješaju konotacije hakera.

Ratne igre, (engl. *War Games*) je film redatelja Badhama J. o hakerima koji je objavljen 1983. Glavnu ulogu ima dječak David Lightman koji upada u vojno superračunalo. Misleći kako je riječ o igri pokreće simulaciju ruskog napada na SAD. Zamalo pokrenuvši treći svjetski rat ovaj film je imao značajan utjecaj na poimanje hakera. Hakeri više nisu oni kojima se ljudi dive, već oni koji **čine štetu**. Haker postaje pojam koji predstavlja tinejdžera koji je u stanju učiniti štetu svjetskih razmjera te pokrenuti treći svjetski rat. Ovaj film je kreirao negativne stavove društva prema hakerima, prikazujući ih uglavnom kao potencijalnu opasnost.

Hakeri (engl. *Hackers*) je film I. Softleeya iz 1995 u kojem glume Jonny Lee Miller i Angelina Jolie, u filmu Dade i Kate. Jonny Lee Miller glumi mladog hakerskog genijalca koji je s11 godina srušio 1507 računalnih sustava. Njegova obitelj je novčano kažnjena, a Dade je dobio zabranu korištenja računala i telefona do svoje 17. godine. Film se nastavlja nakon njegove punoljetnosti gdje Dade upada u hakersko društvo. Jedan od njihovih prijatelja provaljuje u superračunalo velike tvrtke. Dade, Kate i ostatak hakerskog tinejdžerskog društva pomažu spasti prijatelja u nevolji. Ovaj film pokazuje kako postoje i **dobri i zli hakeri**.

Matrica, (engl. *The Matrix*) (1999) je film koji su režisirali Wachowski Lana i Lilly, a ističe se jer je cijelu stvarnost prebacio u matricu. Stvorivši umjetnu inteligenciju ljudima su zavladali strojevi. Ljudi su izgubili bitku sa strojevima, te su ih strojevi odlučili koristiti izvor energije. Ljude su postavili u čahure, a kako bi ih zavarali postavili su um u virtualni svijet dok su tijela bila nesvjesno zarobljena. Thomas Anderson, hakerskog imena Neo je jedan od tih ljudi zarobljen u virtualnom svijetu. Cijeli svoj život osjeća da nešto nije u redu. Nekolicina ljudi koja je uspjela pobjeći iz matrice izvlači i Thomasa te mu pokazuju stvarno stanje izvan virtualnog života. Thomas postaje **heroj** koji može izbjeći pravila koja su zadana unutar matrice, te tako postaje onaj koji bi mogao spasiti čovječanstvo iz nesvjesnog ropstva.

Pronađen (engl. *Trackdown* poznat i kao engl. *Takedown*) je film J. Chapelle napravljen 2000. godine prema knjizi *Takedown* koju su napisali John Markoff i Tsutomu Shimomura. Film i knjiga se temelje na istinitoj priči. Prikazuju **život i hakerske pothvate** poznatog hakera Kevina Mitnicka. Zbog prikazivanja istinitih događaja svrstavam ga među jedne od najvažnijih hakerskih filmova.

Crni haker, (engl. *Blackhat*) iz 2015. godine je film M. Michaela o hakeru koji upada u sustav nuklearne elektrane te uzrokuje eksplozije. SAD pomaže Kini pronaći krivca, pri tome puštaju na slobodu hakera iz zatvora kako bi im pomogao. Ovdje se hakeri dijele na **bijele, crne** i one koji su naknadno postali bijeli. Važno je primijetiti kako se u filmu iz 2015. godine jasno stavlja razlika između crnih i bijelih hakera, dok je u starijim filmovima ta razlika zamućena.

3.3.2. Serije

2015. izlazi serija Gospodin robot, (engl. *Mr. Robot*) u kojoj glavnu ulogu ima Rami Malek, u filmu Elliot Alderson, inženjer za kibernetičku sigurnost. Ova serija ostavlja dojam da su hakeri većinom **ljudi psihičkih poremećaja** poput anksioznosti i depresije. Anderson se pridružuje haktivističkoj grupi *fsociety*, a u seriji se koriste stvarne metode koje hakeri koriste.

Istraga zločina: Cyber (engl. *Crime Scene Investigation: Cyber*) je kriminalistička serija iz 2016. godine koja za glavnu temu ima rješavanje zločina vezanih uz Internet. Glavnim istraživačima pomažu neki od bivših hakera.

3.3.3. Igrice

Igrice i mladež su dva nerazdvojna polja, a čak i mnogi odrasli nikada ne odbace svoju ljubav prema igricama. Igrice predstavljaju bijeg od stvarnosti i ulazak u neki zamišljeni svijet. Upravo svijet hakera se može približiti pomoću igrica. Mnoge igrice simuliraju hakerske pothvate i razvijaju hakerske vještine, pa samim time podižu svijest i interes na navedenu temu. U nastavku navodim neke od igrica koje mladež uvode u svijet hakera.

Hack the Box je online platforma koja pruža izazove kreirane na temelju stvarnih hakerskih scenarija poput testiranja penetracije. Izazovi su rangirani prema težinama, te se tako skupljaju bodovi.

NITE Team 4 uključuje prikupljanje informacija, skeniranje, uzimanje otisaka prstiju, strategije napada… Služi uvježbavanju hakerskih vještina radom u timovima ili samostalno. Igrači sami biraju misije u kojima rješavaju zagonetke koristeći hakerske metode.

Hackmud je tekstualni simulator hakiranja računala. Svaki dobitak se mora zaštititi kodom koji drugi igraći mogu ukrasti. Igra započinje samostalnim igranjem. Kada igrač uspješno izvrši prvu grupu zadataka dobiva priliku kreirati zamke, saveze i alate s ostalim suigračima.

Uplink je hakerska strategijska igra u kojoj je igrač u ulozi agenta. Agent za veliku korporaciju hakira u sustave konkurentskih tvrtki, sabotira ih, krade njihove podatke, pere novce, te na posljetku uklanja dokaze o svojem djelovanju. Uspješnim izvršavanjem zadataka zarađuje se novac kojim se nadograđuju računalni sustavi, kupuju novi softveri i alati.

Hacknet je hakerska igra koja igraću ostavlja upute preminulog hakera. Tijekom igre misterij postaje sve veći, a okolnosti sve sumnjivije (Smith, 2019).

Uz navedene, postoji mnoštvo popularnih igara na temu hakiranja. Ove igre razvijaju hakerske vještine, te podižu razinu svjesnosti o postojanju hakera. Postoji li mogućnost da će upravo iz ovakve igrice nastati budući haker? Postoji li mogućnost da će zbog filma ili serije netko razviti interes prema hakiranju? Zasigurno će zastupljenost teme utjecati na porast interesa baziranog na hakerskoj tematici. Kako će taj interes i stečeno znanje mladi haker upotrijebiti ostaje na njemu, ali i na društvu koje ima popriličan utjecaj.

4. Etika

Kako bismo razumjeli etiku i njenu primjenu u informacijskom dobu potrebno je definirati osnovne pojmove kao što su društvo, moral i etika. **Društvo** je udruženje ljudi koji žive prema određenim pravilima koja imaju za cilj unaprijediti dobro svojih članova. **Moral** čine pravila u ponašanju koja govore ljudima što bi trebali a što ne bi trebali činiti. **Etika** je filozofijska disciplina o moralu. Njezinim se osnivačem smatra grčki filozof Sokrat. Ona se bavi racionalnim propitivanjem ljudskih moralnih uvjerenja i ponašanja (Quinn, 2017).

Dobra etička teorija mora moći pružiti kvalitetne logičke argumente kako bi opravdala svoj stav. Etička pitanja proizlaze iz moralnih dilema. Moralna dilema postaje trenutak u kojem se moralni razlozi sukobljavaju s razlozima izvan moralnog područja. Postoji mnoštvo etičkih teorija, no u ovome radu nas zanimaju utilitarizam koji se svrstava pod konzekvencionalističku teoriju, teorija dužnosti ili deontološka etika i aretaička etika ili etika vrlina. Aretaička, deontološka i konzekvecijalistička etika su verzije normativne etike. Normativna etika je etika prvog reda koja ima za cilj pomoći u donošenju moralnih odluka.

Stipe Kutleša u Filozofskom leksikonu (2012) daje objašnjenje deontološke, aretaičke i konzekvencionalističke etike, dok Berčić (2008) objašnjava etiku vrlina i utilitarizam u istoimenim člancima dostupnim na portalu znanstvenih časopisa Hrčak.

Bentham je osnivač utilitarizma, etičke teorije koja za glavni kriterij moralnog vrednovanja uzima račun sreće. Utilitarizam je konzekvencionalistička teorija koja u obzir uzima posljedice našeg djelovanja. Utilitarizam očekuje djelovanje koje će kao posljedicu inati najveći mogući broj sretnih ljudi. Kako bi neko djelovanje bilo moralno ispravno, posljedica mora biti najveći mogući broj sretnih ljudi. U ovoj teoriji nije važan razlog djelovanja, već posljedica.

Osnivačem deontološke etike se smatra njemački filozof Immanuel Kant. Unutar ove teorije posljedica nema primat u donošenju odluke. Deontološka teorija se temelji na dužnosti i kategoričkom imperativu. Kategorički imperativ predstavlja apriorni moralni zakon koji od nas očekuje da za princip svojeg djelovanja uzmemo ono što može postati

principom svačijeg djelovanja. Čovjeka se nikada ne smije tretirati kao sredstvo, već kao cilj. Namjera djelovanja je dobra samo ako se izvodi iz dužnosti prema gore navedenom moralnom zakonu.

Aretaička etika ili etika vrlina se ne koristi posljedicama ili dužnošću. Najveći doprinos etici vrlina donio je grčki filozof Aristotel. Za ovu etičku teoriju je najvažnije djelovati u skladu s vrlinom. Vrlina je dobra karakterna osobina, suprotna manama koje su loše karakterne osobine. Etika vrlina se ne zamara time što trebamo činiti, već kakvi trebamo biti. Naglasak je na samoj osobi, onome koji djeluje dok su utilitaristička i deontološka usredotočene na djelovanje. Djelovanje u skladu s vrlinom čini čovjeka dobrim.

Istraživanje će nam pokazati kojoj etičkoj teoriji pripadaju naši ispitanici. Rezultati ankete vezani uz etičku teoriju nalaze se u petoj skupini pitanja.

4.1.Etika informacijskog doba

Etika je jedna od najstarijih disciplina koju primjenjujemo u svim segmentima svog života. Nakon industrijskog, informacijsko doba sa sobom donosi novu tehnologiju. 1440. godine Gutembergov tiskarski stroj predstavlja prvi korak informacijske revolucije. Drugi korak je načinjen upotrebom Moresovog telegrafa. Slijede Bellov telefon, televizija i radio, pojava osobnih računala, korištenje računalnih mreža, pojava Interneta. Informacijsko doba karakterizira digitalna revolucija koja upravlja sve većim količinama podatka. Globalizacija omogućuje sve bržu i lakšu razmjenu informacija i dobara. Prostorna udaljenost više ne predstavlja problem. Internet se koristi za prikupljanje, pohranjivanje i dohvaćanje informacija, kao prostor oglašavanja, za komunikaciju, u poslovne svrhe. Sve navedeno je vezano uz razvoj informacijskog doba koje je omogućilo širenje hakera.

Nova tehnologija iziskuje specifične radnje vezane uz nju, otvaraju se nove mogućnosti na području ljudskog djelovanja. Kako se razvija informatička tehnologija tako se broj počinitelja povećava, a počinitelji su sve mlađi. Svako ljudsko djelovanje je korisno pogledati iz etičkog aspekta, pa tako i djelovanja vezana uz tehnologiju. Razvoj informacijske tehnologije donosi nove etičke dileme. Je li hakiranje samo nevina zabava

ili je to nedjelo ravnopravno prevarama i lopovima? U kojem trenu neslana šala i znatiželja postaju kriminalno djelo? Je li zadiranje u privatne informacije zbog znanja moralno ispravno?

4.2. Hakerska etika

Steven Levy (1994:32) vjeruje kako je jedan od osnovnih principa hakerske etike slobodan, tj. neograničen i potpun „*pristup računalima i svemu što vas može naučiti o načinu na koji svijet funkcionira"*[17]. Sama fraza *"Always yield to the Hands-On Imperativ!*" govori u prilog tom principu i vjerovanju da, ako i nešto nema otvoren pristup, zadatak hakera je da se uhvati u koštac s tim izazovom i pronađe rješenje kako bi došao do potrebnih informacija.

Eric S. Raymond (1998: 234) definira hakersku etiku: „*Etička je dužnost hakera razmjenjivati stručno znanje s drugima i pisati slobodni softver kako bi, kad god je moguće, olakšali pristup informacijama i kompjutorima. Vjerovanje da je rušenje sustava za zabavu i istraživanje etički uredu sve dok kreker ne počini nikakvu krađu, vandalizam ili kršenje povjerljivosti*.". Većina hakera se slaže s prvim etičkim principom, no oko drugog principa nastaju neslaganja među njima samima.

Himanen Pekka (2002) navodi tri kategorije naših motivacija koje naziva Linusovim zakonom. Kategorije kroz koje se razvijamo su opstanak, društveni život i razonoda. Svatko od nas ima motivaciju za opstankom, potrebu za društvenim životom i razonodom. Kako bi napredovali potrebno je proći kroz svaku fazu. Upravo taj razvoj možemo primijeniti na hakere. Haker ne koristi računalo radi prve motivacije, opstanka. To znači da njegova osnovna motivacija korištenja računala nije zarada novca za hranu. On računalo koristi zbog društvenog života i razonode. Haker programira jer ga uz to prate osjećaji veselja, uzbuđenja, znatiželje, fascinacije. Linux je nastao kao rezultat razonode,

[17]Ovo je slobodan prijevod. Izvorno engl. "*Access to computers and anything which might teach you something about the way the world works should be unlimited and total. Always yield to the Hands-On Imperative!*".

društvene povezanosti koju oni vole. Linux je nastao tako da su javno pozvani ljudi na sudjelovanje u razvoju.

Himanen (2002) povezuje hakersku radnu etiku s protestantskom radnom etikom. Protestantska etika rad stavlja na prvo mjesto. Rad je potreban i nužan. Protestantsku etiku rada vidimo u ljudskom stavu bilo koje zajednice u trenu kada žale za poslom jer su ostali kod kuće. Osjećaju grižnju savjesti zbog ne dolaska na posao. Pekka primjećuje, nedjelja je postala petak. Rad se je nekada smatrao kaznom, no protestantska radna etika ga pretvara u svrhu. Rad u smislu muke, tlake, kazne postaje svrha. Za hakere njihov rad nije tlaka, muka niti kazna. Za hakere njihov rad ne mora biti niti čista sreća kako bi postigli ono što žele. Tako se hakeri nalaze između pred protestantske etike koja sanja o raju, i protestantske etike koja rad postavlja kao najvišu vrijednost. Hakere karakterizira naporan rad, ali i zabava u tom radu.

Novo doba zahtjeva sve veću brzinu, optimalno korištenje radnog vremena i slobodnog vremena. Slobodno vrijeme mora biti pomno organizirano kako bi se kvalitetno iskoristilo. Nestaje razlika između rada i dokolice. Protestantska etika je postavila rad kao osnovicu prema kojoj ćemo organizirati ostatak života. Dolazak tehnologije je omogućio rad bilo kada i bilo gdje, tako nastaje fleksibilnost radnog vremena. Sada postoji mogućnost sat vremena provesti s djecom u parku, i idućih sat vremena provjeravati poslovni e-mail. Suprotno, postoji mogućnost da vas nazove šef na mobitel i vi morate hitno ići raditi. Nova tehnologija ine u prilog protestantskoj etici. Haker uočava prednosti i iskorištava ih: „*Prema hakerovu mišljenju, upotreba strojeva za optimalno i fleksibilno korištenje vremena trebala bi čovjeku omogućiti život koji manje nalikuje na stroj s manje optimizacije i rutine*“ (Himanen, 2002: 24). Haker želi petak učiniti sličnijim nedjelji. Za protestantsku etiku uz rad je i novac svrha, novac nam treba kako bismo kupili hranu. Novac nam treba za preživljavanje.

Osnovna razlika protestantske etike i hakerske etike je u tome što prva kao prioritet postavlja preživljavanje, dok druga radi kako bi preživjela, ali i kako bi zadovoljila društvene potrebe. Unatoč stavljanju prioriteta na zadovoljavanje društvenih i strastvenih potreba oni su svjesni moći koje novac ima. Znaju ako nemaju novaca, moraju raditi za drugu osobu. U tom slučaju gube slobodu organiziranja vremena. Kapitalistički hakeri su

odlučili postići financijsku neovisnost. To su učinili posjedovanjem dionica ili vođenjem vlastitih tvrtki. Himanen (2002) naglašava još jednu razliku, razliku između kapitalizma i hakerske etike. Kapitalizam je bliži protestantskoj radnoj etici zbog želje za povećanjem kapitala. Ljudi se u konačnici radije odluče za kapitalističku, protestantsku etiku, nego li za hakersku.

Kako bi riješili naveden probleme nastaju nove tvrtke. Njihov softver se razvija prema otvorenom modelu, s otvorenim programskim kodom (engl. *open source*). Otac ovog modela je Richard Stallman. Suprotstavlja se stjecanju novca sprečavanjem pristupa informacijama. Stavlja u pitanje etičnost čuvanja informacija privatnima. Smatra kako nije uredu koristiti tuđe informacije, a svoje zabraniti javnosti. Bori se za slobodno tržište u kojem kontrola informacija ne određuje konkurentnost. Bori se za tržište u kojem svi imaju pravo na sve informacije. Ovo nije komunistička etika, jer komunistička etike podrazumijeva nekakav autoritet. Ova etika se suprotstavlja i komunizmu i kapitalizmu. Otvoreni model po imenu katedrala karakterizira jedna osoba ili manji broj ljudi koji prikazuju samo gotove rezultate svog rada. U drugom otvorenom modelu, bazaru, svi imaju priliku sudjelovati u razvoju, prihvaća se svaka ideja. Akademija je oblik otvorenog modela u kojem se rezultati rada dijele s ostalima koji ih onda mogu koristiti, testirati i razvijati. Ovaj model se pokazao kao najbolji. Zatvoreni model ne dozvoljava dijeljenje informacija i postavljen je hijerarhijski s autoritetom. Samo odabrani imaju pravo rada na projektu. Hakeri su skloniji otvorenom modelu. Mrežna akademija je hakerski model učenja koji je baziran na principu otvorenosti, sličan je Platonovoj akademiji[18]. Prilikom učenja i rada haker djeluje tako da i ostali mogu učiti od njega i nastaviti njegov rad. Kritičko razmišljanje, suradnja i nadograđivanje postojećeg su temelj ovog modela učenja (Himanen, 2002).

[18] 387.g. Platon je osnovao Akademiju, školu koja je od učenika metodom majeutike izvlačila istinu. Ne daje se gotovo znanje. Učitelj pomaže učeniku u promišljanju kako bi sam došao do nove spoznaje.

4.2.1. Netika

Netika je pojam koji označava etiku mreže. „*Taj se pojam odnosi na odnos hakera prema mrežama našeg umreženog društva*„ … „*pravila ponašanja za komunikaciju na Mreži*"… (Himanen, 2002). Netika je pojam koji je osviješten 1990.tih godina kada je osnovana međunarodna nevladina organizacija koja brani slobodu govora, privatnost i prava potrošača korisnika Interneta. Odnosi se na aktivnosti i društvene odgovornosti. Hakeri se protive cenzurama i zabranama koje su bujale 90-tih na teritoriju Jugoslavije. Bilo je zabranjeno emitiranje bilo kakvih ratnih izvješća putem bilo kakvih medija. Želja da Internet bude svima dostupan i da se na njemu može slobodno izražavati je na kraju pobijedila. Urednici radijske postaje B92 su mogli emitirati putem Interneta. Zahvaljujući mogućnosti slanja slika putem Interneta mnogi ratni zločinci su osuđeni. Rat je bio prisutan i na Internetu. Krekeri su napadali u skladu sa svojim uvjerenjima. Iz Srbije izvršen napad na poslužitelja NATO-a. Amerika i, Albanija i Zapadna Europa je vršila napade nad Srbijom.

Vlade imaju tendenciju nadziranja stanovništva, a nadziranje se izvodi tako da se kontroliraju sadržaju poruka, posjećivanja stranica. Web poslužitelji sve češće identificiraju korisnike pomoću cookiesa. Podaci koje uzimaju su sve privatniji. Takvi podaci se na kraju prodaju zbog marketinga. Ako smo pretraživali putovanja, kao reklame će nam se nuditi agencije za putovanja. Mnoge tvrtke prilikom zapošljavanja i nakon zapošljavanja „špijuniraju" elektroničke aktivnosti zaposlenih. Hakeri su svjesni ovog stanja te napominju važnost privatnosti i zaštite. Protive se prikupljanju informacija, ulasku u privatan prostor, te predstavljaju zaštitnike privatnosti na Internetu.

U industriji tipičan slijed događa je takav da čovjek ide u školu i uči. Ono što je naučio primjenjuje na radnom mjestu koje traje fiksno osam sati svaki radni dan. Novo vrijeme dozvoljava da čovjek sam ući, razvija se i prilagođava se sukladno traženim zadacima. Znanja i tehnologije se brzo mijenjaju pa se tako mora i čovjek mijenjati. Pekka kaže čovjek mora naučiti sam sebe programirati, postati sam svoj šef na dane trenutke (Himanen, 2002). Brinu za slobodno vrijeme, ali mu ne pridaju više značenja, nego radu. Hakeri vole stvarati i raditi, ali na kreativan način.

Nisu svi hakeri zlonamjerni, već postoje hakeri koji se brinu za etičnost ponašanja u sklopu današnjeg informacijskog doba. Spremni su opomenuti na nedostatke i pogreške našeg ponašanja u informacijskom dobu.

4.2.2. Etični hakeri

Babić (2009: 121) definira etične hakere kao osobe koje polažu sigurnosni ispit za sprječavanje problema u informatičkoj sigurnosti.

Kevin Mitnick daje sljedeću definiciju etičkog hakiranja: „*Razlika između hakiranja crnih hakera i etičkog hakiranja je jednostavno autorizacija klijenta*." (Silicon Republic, 2018: 4:52)[19].

Crni hakeri često postaju bijeli hakeri, a bijeli hakeri često postaju crni hakeri. Granica je tanka i vrlo lako se prelazi iz etički ispravne u etički neispravno djelovanje što možemo vidjeti iz sljedećih primjera. Kevin Poulsen je hakirao federalnu računalnu mrežu istražujući federalnu istragu filipinskog predsjednika Ferdinanda Marcosa. Marcos je ukrao bilijune Filipinima i imao evidenciju o iskorištavanju ljudskih prava. Objavio je FBI-ova prisluškivanja mafijaša i lokalnih političara. Na kraju je završio u zatvoru zbog namještanja pobjede u nagradnim igrama. Nakon izlaska iz zatvora počinje se baviti novinarstvom. Piše o računalnoj sigurnosti i istovremeno svojim hakerskim vještinama pronalazi pedofile na Internetu.

Adriano Lamo je hakirao razne korporacije kako bi pokazao slabosti u zaštiti. Mnoge njegove žrtve su mu zahvaljivale na ukazanim slabostima. Albert Gonzalez je vodio web stranicu gdje su se prodavali ukradeni osobni podaci koji su mogli poslužiti za krađu ili stvaranje novog identiteta. Nakon uhićenja postaje vladin informator kako ne bi završio u zatvoru. Pomogao je uhititi 28 hakera, ali paralelno se potajno vratio kriminalu. Iz trgovina je krao podatke o kreditnim i debitnim karticama. 2008. godine je osuđen na 20 godina zatvora (The Infographics Show, 2019).

[19] Ovo je slobodan prijevod. Izvorno: engl. „*The difference between, you know, blackhat hacking and ethical hacking is simply authorization from the client.*".

Anonymous je skupina anonimnih hakera koja je velikom brzinom rasla tokom 21. stoljeća. Njihov cilj je u početku bio napraviti jeftinu šalu na 4chanu.[20] S vremenom su postali borci za slobodu korištenja Interneta, slobodu govora na Internetu, a bave se i političkim temama. **Haktivizam** je spoj riječi haker i aktivizam, a označava korištenje digitalne tehnologije za širenje političkih i socijalnih ciljeva. Haktivizam je politički aktivizam gdje se sposobnosti hakiranja koriste protiv velikih institucija, vlada, moćnih tvrtki, države, vjerskih skupina. Upadaju na zaštićene web stranice i baze podataka kako bi objavili tajne informacije u svrhu slobode Interneta i pravde na političkoj sceni. Njihova brojnost je učena na javnim prosvjedima, na kojima se uvijek pojavljuju s maskom kako bi ostali anonimni. Njihov amblem vidimo na slici 5. Najčešća maska (pogledaj sliku 6) je u obliku stiliziranog portreta lica s osmijehom i obrazima, širokim brkovima te tanke i okomite brade, poznata kao Guy Fawkes maska. Anonymousi su se sukobili sa Scijentološkom crkvom. U javnost je izašao interni video s Tom Cruiseom gdje se govorilo o tajnama Scijentologije: Scijentološkoj crkvi to nije odgovaralo pa su stavili autorska prava na taj video kako bi mogli kontrolirati njegove objave. Anonymousi su shvatili to kao pokušaj cenzuriranja Interneta te krenuli u napad na Scijentološku crkvu (Anonymous Official, 2014).

Slika 5. Slika lijevo: amblem Anonymousa. (Anonymous Official. Preuzeto s https://www.youtube.com/user/anonymousworldvoce?sub_confirmation=1)

[20] 4chan je Internetski forum na kojem su se anonimno mogle objavljivati slike.

Slika 6. Slika desno: Maska Anonymousa. (Campbel, R. Preuzeto s https://hacked.com/anonymous-india-reliance-jio-is-sharing-call-data-with-advertisers/)

LulzSec ili Lulz Security su haktivisti koji su se odvojili od Anonymusa 2011. kako bi izvršili osjetljivije napade kao što su napad na Sony i FBI. WikiLeaks je haktivistička grupa koja se bori protiv korupcije društva objavljujući povjerljive informacije na wiki stranicama, što znači da i sami korisnici mogu uređivati dokumente. Haktivističke skupine se često bave medijskim hakiranjem (korištenje elektronskih medija na drugačiji način kako bi prenijeli određenu poruku što većem broju ljudi). Ovakve skupine su pokazale da nije potrebna vojna fizička snaga kako bi bio snažan, kako bi napravio nešto što ima utjecaj i što je važno (Sorell, 2010).

Postoje etički hakeri koji rade za velike kompanije ili privatnike kako bi pomogli očuvati sigurnost. **Ralph Echemendia, Cam Bucannan, Ruben van Vreeland** su primjeri ljudi koji su izgradili karijeru na području etičkog hakiranja. Cam Buchannan je etički haker koji radi kao savjetnik u penetracijskom testiranju. Ruben van Vreeland je samoinicijativno zvao velike tvrtke kako bi im javio da ih je hakirao i koji su im propusti u sigurnosti. Ralph je etički haker koji radi na tome da upozna ljude s digitalnim svijetom i njegovim opasnostima (TEDx Talks, 2019).

Sve popularniji postaju tečajevi etičkog hakiranja ma kojima se stječu sve vještine potrebne za hakiranje. Nakon položenog seminara dobiva se međunarodno priznati Certified Ethical Hacker certifikat, a polaznici potpisuju ugovor kojim se obavezuju kako neće zloupotrijebiti znanje stečeno na seminaru. Obavezuju se na etičko korištenje

stečenog znanja kao i na nadoknadu štete ako je prouzroče (ALGEBRA certifikacijski seminari, Certified Ethical Hacker (CEH)).

Levy (1994) napominje kako se etika hakera sastoji od želje za slobodom svih informacija što omogućava uočavanje i popravak pogrešaka. Otvoreni sustavi omogućuju razmjene informacija i opreme, dok birokracija često koči takvo međudjelovanje. Etični hakeri često hakiraju kako bi ukazali na pogreške u sigurnosti. Ralph Echemendia primjećuje kako zlonamjernim hakerima razlozi hakiranja sve češće postaju financijski, dok im je prije najčešći razlog bio kreiranje nepodopština ili stjecanje znanja (Forbes DACH, 2017). Hakiranje postaje način ilegalne zarade i krađe novaca dok je Mitnickova motivacija bila čista želja za znanjem i uzbuđenjem.

5. Računalni kriminal i kako se zaštititi

Ne znanje pravnih i fizičkih osoba, površna zaštita i informiranost dovode do sve većeg broja hakerskih napada. Ako ne znamo kako se sam napad izvodi onda se ne možemo niti znati obraniti. Djelovanje crnih hakera svrstavamo unutar pojma računalni kriminal. Računalni kriminal je dio života mnogih hakera, stoga je važno definirati što je to računalni kriminal. Iako smo svi podložni djelovanju hakera, ne činimo puno kako bi smo spriječili njihovo zloupotrebljavanje znanja.

Dražen Dragičević (2004: 113) definira računalni kriminal kao „*ukupnost kaznenih djela, učinjenih na određenom području kroz određeno vrijeme, kojima se neovlašteno utječe na korištenje, cjelovitost i dostupnost tehničke, programske ili podatkovne osnovice kompjuterskog sustava ili tajnost digitalnih podataka*.“.

5.1. Ciljevi, metode i koraci hakersko napada

5.1.1. Ciljevi hakerskog napada

Mnogo ljudi na pitanje: Što možeš poduzeti da bi se zaštitio? će pomisliti na karate, judo, taekwondo. Osim svijesti o fizičkoj izloženosti, ljudi postaju sve više svjesni o njihovoj digitalnoj izloženosti. Nova vrsta kriminalaca nema masku na licu i pištolj u ruci, već tipkovnicu i miš kao oružje. Ovi kriminalci ne bježe kombijem, već zločin čine iz svojih fotelja. Dražen Dragičević (2004) razlikuje ciljeve i metode napada na Internetu. Ciljevi mogu biti otkrivanje korisničkih lozinki, podataka i informacija, datoteka s kreditnim i identifikacijskim karticama, računalni programi, Web stranice i News grupe, onemogućavanje korištenja kompjutorskog sustava, materijalni resursi informacijskog sustava. Hakere najviše zanimaju lozinke, podaci i informacije, brojevi kreditnih i identifikacijskih kartica i Web stranice.

Vladica Babić (2009) štetu kompjuterskog kriminala definira kao

Financijsku - cilj kriminalnog djela je financijska korist sebi ili drugome

Nematerijalnu - cilj kriminalnog djela je nedozvoljeno otkrivanje tajnih podataka

Kombiniranu - cilj kriminalnog djela je financijski i nematerijalni.

5.1.2. Metode hakerskog napada

Najčešće hakerske metode su:

- socijalni inženjering(engl. *social engineering*),
- maskiranje ili varanje(engl. *masquerading, deception*),
- spoofing, ispitivanje ili pogađanje (engl. *probe, guessing*),
- pretraživanje (engl. *scanning*),
- prisluškivanje (engl. *wiretapping, eavesdropping*),
- optičko špijuniranje(engl. *optical spying*),
- druženje (engl. *socializing*),
- kompromitiranje (engl. *compromising*),
- programske manipulacije.

Oblici društvenog inženjeringa mogu biti engl. *sholuder surfing* gdje napadač ima direktan uvid prilikom upisivanja lozinke. Engl. *scavenging, dustbin diving, dumpster diving* ili strvinarenje je traženje po tuđem smeću ili bilješkama kako bi se našla lozinka. Maskiranje se odnosi na lažno predstavljanje kako bi se steklo povjerenje. Spoofing se odnosi na bilo koju metodu dolaska do željenih podataka iskorištavajući slabosti IP protokola. Ispitivanje je pogađanje lozinke na slijepo. Pretraživanje označavaju brojni nedozvoljeni pokušaji dolaska do informacija ili sustava pomoću automatiziranog alata. Prisluškivanje je prisluškivanje telefonskih razgovora kako bi napadači došli do željenih podataka. Optičko špijuniranje je promatranje, snimanje ili presretanje elektromagnetskog zračenja s računalnog ekrana. Druženjem sa samim osobom, kompromitacija, podmićivanje i iskorištavanje su metode pomoću kojih počinitelj može dobiti mnogo informacija potrebnih za kriminalnu radnju. Programske manipulacije se odnose na programe kao što su engl. *pocket sniffer* i trojanski konj koji omogućavaju dolazak do lozinki.

Hakeri pokušavaju otkriti korisničke lozinke koristeći navedene metode. Gotovo svi smo bili hakirani samo to ne znamo, svake minute oko tisuću ljudi je hakirano. Velike

korporacije su toga itekako svjesne dok pojedinci slabije. Velike korporacije traže pomoć od hakera.

Crni hakeri se često preobrate u bijele hakere. Njihova svrha postaje zaštita ranjivih. Tako sami hakeri daju savjete za načine zaštite od hakera. Kevin Mitnick (Silicon Republic, 2018: 6:00) ističe izloženost mrežnih usluga, aplikacija, ljudski faktor u korištenju socijalnog inženjeringa kao metode napada na korisnike. Kod testiranja sigurnosti Mitnick obraća pozornost na vanjsku i unutarnju mrežu, bežični Internet, web aplikacije. Kao greške navodi korištenje usluga u oblaku, ostavljanje dostupne baze podataka klijenata s njihovim informacijama, posjedovanje web aplikacija koje nisu testirane na sigurnosne probleme, ne ažuriranje.

5.1.3. Koraci hakerskog napada

Eric Cole (2001: 34) navodi i objašnjava korake hakerskog napada. Neki koraci se mogu ponavljati, a neki i preskočiti.

Pasivno izviđanje. Haker pasivno prikuplja informacije (engl. *information gathering*) o predmetu svog napada. Pasivni napad ne pruža izravan pristup, ali ga može osigurati. Pasivno izviđanje može biti jednostavno promatranje ili razgovor s djelatnicima kroz kojeg se dolazi do relevantnih podataka. Njuškanje (engl. *sniffing*) je još jedna vrsta pasivnog napada koji karakterizira promatranje kompletnog prometa na mreži. Postoje programi koji izvlače i spremaju lozinku.

Aktivno upoznavanje (skeniranje) se odnosi na pokušaj otkrivanja slabosti u samom sustavu. Ako pronađe greške u sigurnosti kreće na sljedeću fazu iskorištavanja sustava.

Iskorištavanje sustava se odvija dobivanjem pristupa tako da napadač sam sebi podigne ovlasti ili korisnicima onemogući pristup resursima. U ovoj fazi se napadač odlučuje hoće li računalo tvrtke A koristiti kao podmetač za napad na računalo tvrtke B: Hakeri tako lakše sakrivaju svoje tragove. U ovoj fazi se događaju napadi na operativni sustav, na aplikacije, skripte, konfiguracije.

Prijenos programa znači da napadač učitava programe u sustav koji mu koristite za povećanje pristupa, kompromis drugih sustava na mreži ili učitati alate koji će se koristiti za kompromis drugih sustava.

Preuzimanje podataka je vrsta napada koja se koristi prilikom špijunaže te se najčešće odnose na Velike podatke.

Održavanje pristupa korištenjem stražnjih vrata. Stražnja vrata može biti dodani račun kroz koji će haker pristupiti sustavu, trojanski konj ili prepisati sistemsku datoteku s verzijom koja ima skrivene značajke (engl. *system file*).

Sakrivanje tragova se odnosi na čišćenje ili isključivanje dnevnika koji sadrži evidenciju o pristupima sustavu.

5.2. Zaštita

Nakon što smo saznali koji su ciljevi i koraci, te kakve su metode hakerskog napada potrebno je znati kako preventivno djelovati da do tog napada ne bi došlo. Ovaj odlomak je posvećen problemima u samoj zaštiti. Ako ne otklonimo slabe točke u samim početcima organiziranja zaštitite ne možemo niti očekivati sigurnost. Sami hakeri često daju najbolja upozorenja kako spriječiti hakerski napad, lako je zaključiti da bijeli hakeri imaju najveću ulogu na području zaštite.

5.2.1. Problemi zaštite

Eric Cole (2001) navodi probleme koji potiču brojnost hakerskih napada:

Internet u sebi sadrži mnoštvo informacija i resursa koji olakšavaju napadačima počinjenje napada. Ako i ne zna kako počiniti napad, haker može mjesecima proučavati metu dok ne uoči slabe točke u zaštiti.

Slaba kontrola Interneta u svrhu zaštite je olakšavajuća okolnost za hakere. Ne postoji Internet policija koja poput kobre na autoputu presreće prijestupnike na Internetu.

Maleni postotak tvrtki prijavljuje hakerske napade. Tako se hakeri ohrabruju na sve brojnije i izazovnije napade. Tvrtke ne prijavljuju napade zbog ne znanja i lošeg publiciteta.

Neznanje kao prvi razlog ne prijavljivanja napada se odnosi na činjenicu da mnoge tvrtke ne znaju da su napadnute. Kada bi tvrtke na vrijeme saznale za napad mogla bi se smanjiti šteta. Isto mjesto se može koristiti kao mjesto za pokretanje drugih napada ako napad nije otkriven. Jedini način da vaša web lokacija bude sigurna je da su sve ostale web lokacije sigurne.

Drugi razlog ne prijavljivanja je strah od lošeg publiciteta za tvrtku koji nastaje prijavom napada. Korisnici te kompanije gube povjerenje i prestaju koristiti njihove usluge.

Uporaba Interneta u poslovne i komercijalne svrhe je rasla bez osvrta na njegove nedostatke i mane. Investiranje u sigurnost ne daje izravnu i opipljivu korist. Korist sigurnosti se vidi tek nakon napada kada tvrtka uvidi koju štetu je izbjegla ili je mogla izbjeći ulaganjem u sigurnost.

Etički haker Ruben van Vreeland je osnivač BitSensora, softvera koji otkriva i prati hakerski napad prije početka napad. Olakšava obranu i identifikaciju napadača. Ralph Echemendia primjećuje problem nedostatka kvalificiranih ljudi na ovom području. Prema američkom časopisu Forbesu svake godine ima 1 milijun cyber sigurnosnih (engl. *cybersecurity*) poslova za kojih nema kvalificiranih radnih snaga. Da bi osoba ili kompanija shvatila da je hakirana u prosjeku prođe 229 dana. Ne zbog nedostatka tehnologije, već zbog nedostatka ljudi.

Dvadeset godina nije osmišljena pristupačna svakodnevna obrambena tehnologija osim antivirusa. Virusi danas više nisu toliko aktualni jer više nije cilj uništiti podatke, već ih ukrasti i unovčiti. Povjerenje koje imamo prema tehnologije je veliko, a mnogo stvari nije zakonski regulirano. Ralph pokazuje kako može hakirati bilo čiji telefon, praviti se kao da je član o obitelji, poslati poruku koja izgleda kao da je poslana od poznanika a ne od nepoznate osobe. Preporučuje korištenje besplatne mobilne aplikacije Seguru Safeware dostupne na App Storeu i Google Playu.

Sljedeći problem je ne razumijevanje načina na koji rade naši uređaji. Posjedujemo mobitele, televizore, računala, ali ne znamo kako se uspostavlja poziv ili kako nastaje slika na ekranima navedenih uređaja. Ralph napominje kako je glavni problem u nama, našem ne znanju i nedostatku želje za znanjem o uređajima kojima se koristimo.

5.2.2. Načini zaštite

Kao siguran način komuniciranja, umjesto e-maila Echemendia predlaže protonmail, besplatnu uslugu poput e-maila koji koristi enkripciju. Javni servisi nisu pouzdani. Oblak označava samo da se informacija nalazi na tuđem serveru. Preporučuje prekrivanje kamera na laptopu.

Dragičević (2004) navodi tehnike zaštite. Dobro je postavljanje alarmnih sustava i fizičke biometrijske zaštite koja pazi na ulazak neovlaštenih ljudi koji se koriste neovlaštenim izvorima. Provjera pristupa se odvija identifikacijom osobe i autorizacijom kojom vidimo koja sve prava i pristup određena osoba ima. Otisak prsta dlana, skeniranje šarenice oka, analiza glasa, magnetski čip, infracrvena kartica su preporučene metode identifikacije. Samo odabranim ljudima dati ključeve. Davanje digitalnog certifikata olakšava utvrđivanje identiteta osobe zbog korištenja kriptografije u ovoj digitalnoj ispravi. Potrebno je imati nadzor nad radom i korištenjem računalnog i mrežnog sustava. Potrebno je provjeravati tko radi, što radi i kako radi. Potrebno je postaviti alate koji traže slabosti u sustavu, koji primjećuju hakerska pristupanja. Kako bi autentičnost poruke bila provjerena dobro je koristiti digitalni potpis. On računa zbroj poruke. Ako je zbroj poruke isti u trenu slanja i u trenutku primanja poruke poruka je vjerodostojna. Važno je postaviti zaštitu od izvanjskih utjecaja kao što nestanak struje. Poželjno je postaviti službu osiguranja. Prijavljivanje ulazaka i izlazaka uz je dobra metoda kontroliranja koja omogućuje informaciju o tome kada je koji pojedinac ušao i izašao. Uz posjetitelje je dobro imati pratnju koja će ih nadzirati. Za što bolju zaštitu potrebno je postavljati što složenije lozinke, često ih mijenjati te koristiti kriptografske metode. Preporučuje da lozinka bude kombinacija velikih i malih slova, brojeva i znakova, duljine veće od 7 znakova. Poželjno je napraviti sigurnosne kopije podataka, izdvojiti važne podatke iz mreže. U slučaju krizne situacije potrebno je imati unaprijed određeni plan djelovanja. Kako bi se znao datum kreiranja i zadnje izmjene dokumenta koristi se digitalni vremenski biljeg. Dragičević preporučuje korištenje steganografije[21] zbog ubacivanja informacija u neiskorištene dijelove informacijskog paketa. Vatreni zid (engl. *Firewall*) štiti računalne mreže od

[21] Steganografija je umijeće i znanje pisanja tajnih poruka.

neovlaštenog pristupa podacima i programima. Eric Cole (2001) kombinaciju ovih sigurnosnih pristupa naziva obranom u dubini (engl. *defense in depth*).

Velike tvrtke trebaju postati mjesto nulte tolerancije na hakerske napade kako bi pokazali ne etičnim hakerima da se njihove aktivnosti neće tolerirati i zataškavati. Edukacija, zaštita, prevencija i detekcija trebaju imati prioritet pred zaradom. Sami zaposlenici moraju biti dio procesa edukacije i osvještavanja.

Testiranje penetracije (engl. *penetration testing*) je jedan od načina testiranja sigurnosti. Cam Buchannan definira ovaj oblik testiranja sigurnosti kao preuzimanje uloge napadača na organizaciju. Uzima se široki raspon alata kojima se procjenjuje ranjivost sustava. Nesigurne točke se pokušavaju iskoristiti. Na kraju se kompaniji kaže koje su slabosti, na koji način se mogu iskoristiti te kako popraviti nedostatke (Vodafone Business, 2014: 1:13).

6. Istraživanje

Kreirala sam anketu putem Google obrazaca kako bih istražila koliko su ljudi upoznati s hakerima, koji profil ljudi je skloniji hakiranju, što potiče ljude na hakiranje, te kako bi ispitanici reagirali u hipotetskoj situaciji. Na anketu su odgovarali ljudi različitih godišta i zanimanja.

Prva skupina pitanja se odnosi na opće podatke ispitanika poput spola, datuma rođenja, županije u kojoj živi, stupanj obrazovanja, naziv srednje škole i fakulteta, način provođenja slobodnog vremena te radno mjesto. Druga skupina pitanja se odnosi na snalaženje u području informatike i znanje programiranja. Treća skupina zadataka istražuje stupanj upoznatosti ispitanika s pojmom hakera. Četvrta skupina pitanja provjerava tko je od ispitanika hakirao, ispituje koji osjećaji i razlozi su ispitanika nagnali na hakiranje ili ne hakiranje. Peta skupina zadataka je postavljena hipotetska situacija. Na temelju donesene odluke svaki ispitanik je smješten u odgovarajuću etičku teoriju. (aretaička, deontološka, utilitaristička etika).

Na anketu je odgovorilo 170 ispitanika. Od 170 ispitanika 39 (23%) se izjasnilo da je hakiralo, a ostalih 131 (77%) da nikada nisu hakirali. Analizirat ću prema svakom pitanju prvo ispitanike koji nikada nisu hakirali, nakon toga ispitanike koji jesu hakirali.

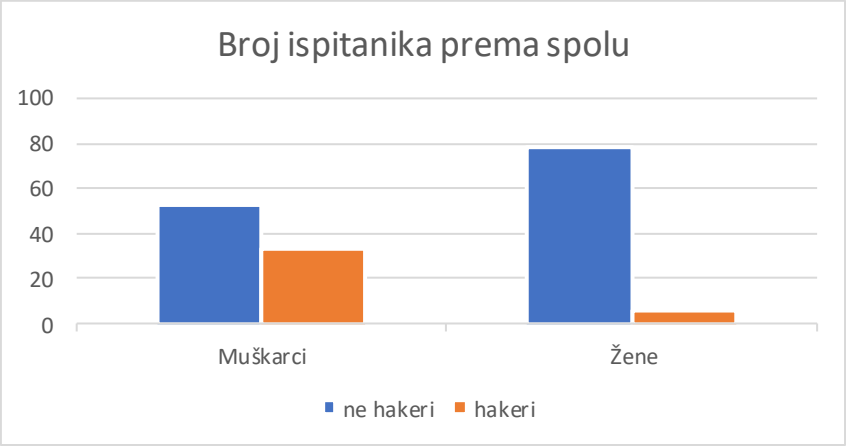
6.1. Rezultati ankete

6.1.1. Prva skupina pitanja

Na anketu su ukupno odgovorile 84 (49.4%) žene i 86 (50.6%) muškarca.

Od 131 ispitanika koji nisu hakirali 78 (59.4%) ispitanica su žene, a 53 (40.6%) ispitanika su muškarci.

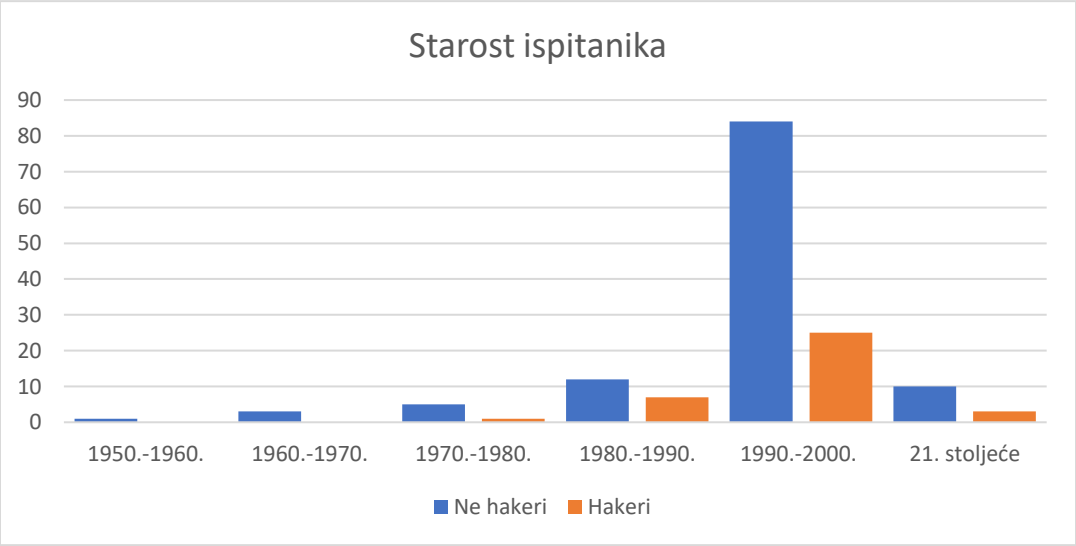
Od 39 ispitanika koji su hakirali, njih samo 6 su žene, a 33 su muškarca što možemo vidjeti na Grafu 1.



Graf 1. Spol ispitanika.

Od 131 ispitanika koji nisu hakirali na pitanje o datumu rođenja 1 ispitanik je odgovorio da je rođen 1950-tih. 3 ispitanika su odgovorila da su rođena 1960-tih, 5 ispitanika je rođeno 1970-tih, 12 ispitanika je rođeno 1980-tih, 84 ispitanika su rođena 1990-tih., 10 ispitanika je rođeno u 21. stoljeću. Od rođenih u 21. stoljeću je 15 ispitanika je greškom odabralo 2019. godinu kao godinu rođenja.

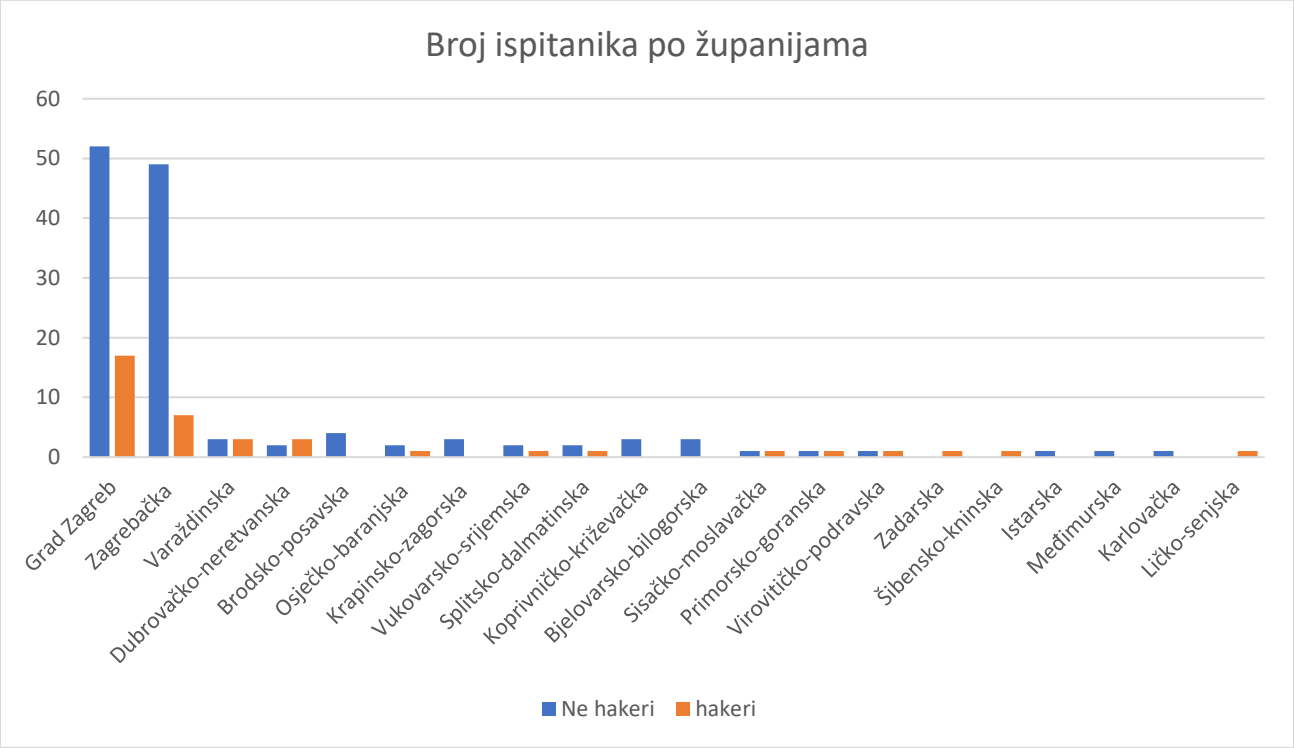
Najstariji ispitanik koji je hakirao je rođen 1970-tih. 7 ispitanika je rođeno 1980-tih. 25. ispitanika je rođeno 1990-tih. Tri ispitanika su rođena u 21. stoljeću. 3 ispitanika su greškom odabrala 2019. godinu kao godinu rođenja. Najmlađi ispitanik koji je hakirao je rođen 2002. godine. Pogledaj graf 2.



Graf 2. Starost ispitanika.

Graf 3 prikazuje gdje ispitanici žive. Od 131 ispitanika koji nije hakirao u gradu Zagrebu živi najviše ispitanika. 52 ispitanika su iz grada Zagreba. 49 ispitanika je iz Zagrebačke županije. 4 ispitanika su iz Brodsko-posavske županije. Po 3 ispitanika su iz Bjelovarsko-bilogorske županije, Koprivničko-križevačke županije, Krapinsko-zagorske županije, Varaždinske županije. Po 2 ispitanika su iz Dubrovačko-neretvanske županije, Osječko-baranjske županije, Splitsko-dalmatinske županije, Vukovarsko-srijemske županije. Po 1 ispitanik je iz Istarske županije, Karlovačke županije, Međimurske županije, Primorsko-goranske županije, Sisačko-moslavačke županije, Virovitičko-podravske županije.

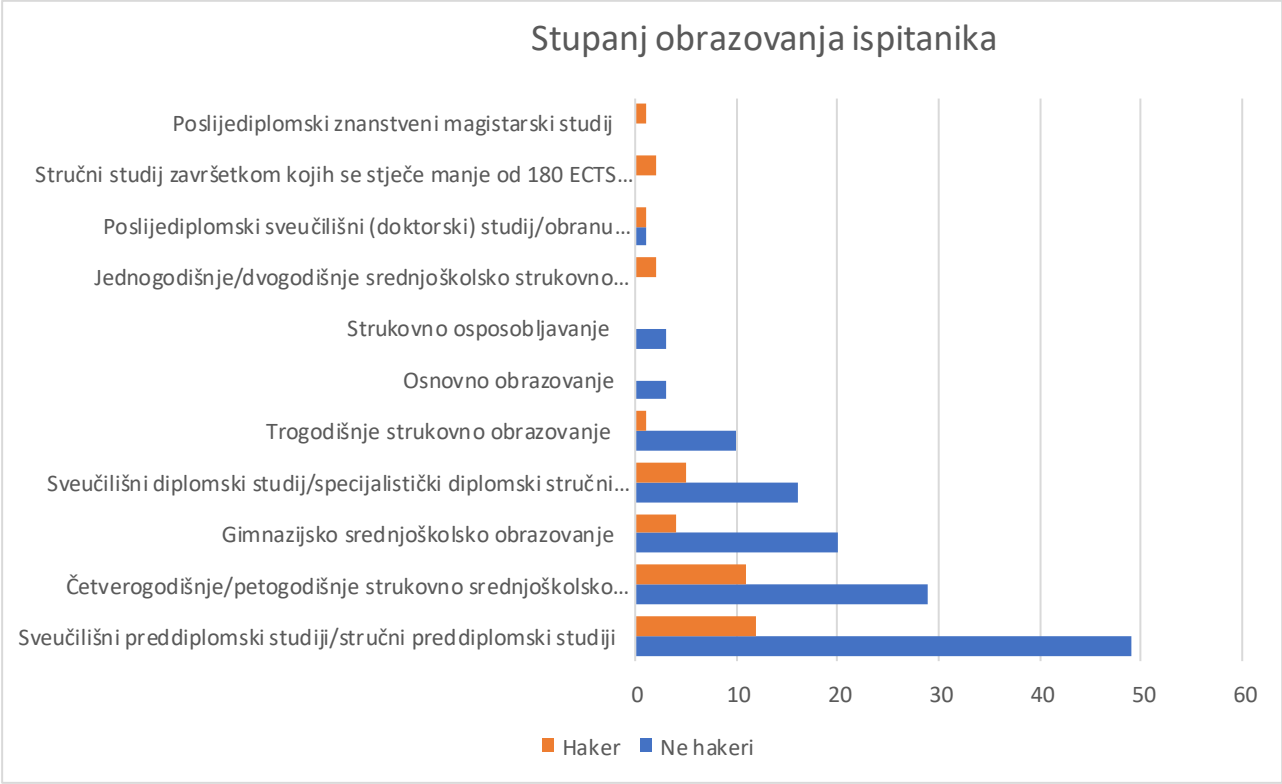
Od 39 ispitanika koji su hakirali u gradu Zagrebu živi 17 ispitanika. Iz Zagrebačke županije je 7 ispitanika. Po 3 ispitanika su iz Dubrovačko-neretvanska županija i Varaždinske županije. Po jedan ispitanik je iz Ličko-senjske županije, Osječko-baranjske županije, Primorsko-goranske županije, Sisačko-moslavačke županije, Splitsko-dalmatinske županije, Šibensko-kninske županije, Virovitičko-podravske županije, Vukovarsko-srijemske županije, Zadarske županije.



Graf 3. Županije u kojima ispitanici žive.

Stupanj obrazovanja ispitanika vidimo na Grafu 4. Od 131 ispitanika koji nije hakirao njih 49 je studiralo sveučilišni preddiplomski studiji/stručni preddiplomski studiji. 29 ispitanika je završilo četverogodišnje/petogodišnje strukovno srednjoškolsko obrazovanje. 20 ispitanika je završilo gimnazijski srednjoškolski program. 16 ispitanika je završilo sveučilišni diplomski studiji/specijalistički diplomski stručni studiji/poslijediplomski specijalistički studiji. 10 ispitanika ima trogodišnje strukovno obrazovanje. 3 ispitanika imaju završeno osnovno obrazovanje, 3 ispitanika imaju strukovno osposobljavanje. 1 ispitanik ima poslijediplomski sveučilišni (doktorski) studij/ obranu doktorske disertacije izvan studija.

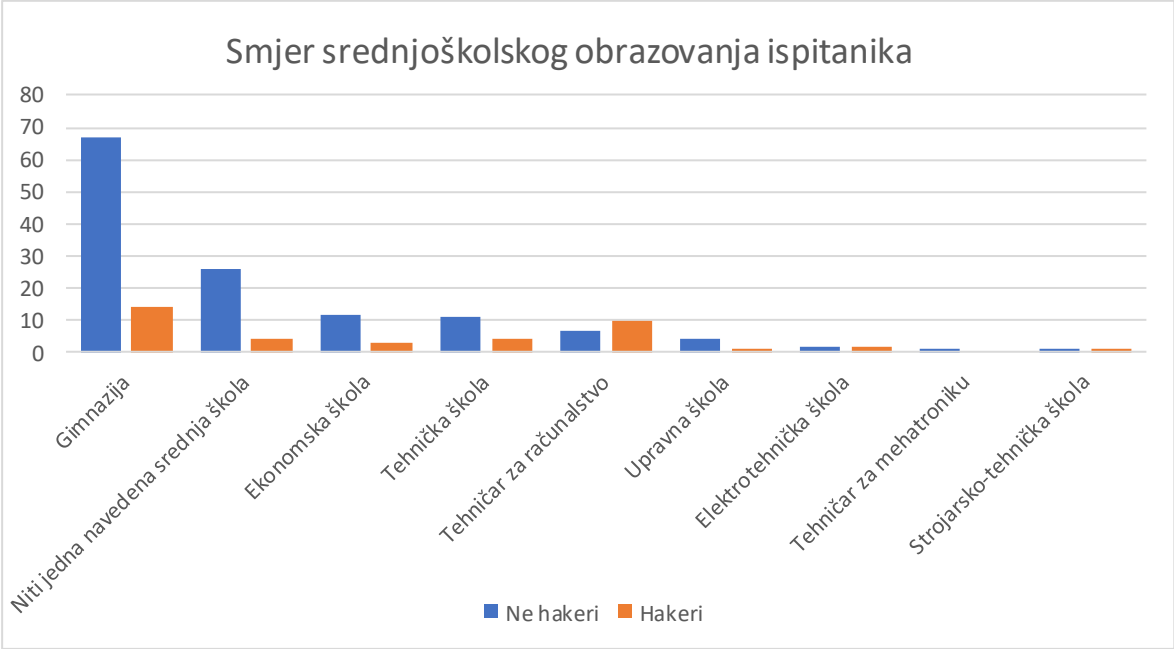
Od 39 ispitanika koji su hakirali 12 ispitanika ima sveučilišni preddiplomski studiji/stručni preddiplomski studiji. 11 ispitanika ima četverogodišnje/petogodišnje strukovno srednjoškolsko obrazovanje. 5 ispitanika ima sveučilišni diplomski studiji/specijalistički diplomski stručni studiji/poslijediplomski specijalistički studiji. 4 ispitanika imaju gimnazijsko srednjoškolsko obrazovanje. 2 ispitanika imaju jednogodišnje/dvogodišnje srednjoškolsko strukovno obrazovanje, 2 ispitanika imaju stručni studiji završetkom kojih se stječe manje od 180 ECTS bodova. Po 1 ispitanik ima poslijediplomski sveučilišni (doktorski) studiji/ obrana doktorske disertacije izvan studija, poslijediplomski znanstveni magistarski studiji, trogodišnje strukovno obrazovanje.



Graf 4. Stupanj obrazovanja ispitanika.

Graf 5 pokazuje smjer srednjoškolskog obrazovanja. Od 131 ispitanika koji nisu hakirali 67 ispitanika je pohađalo gimnaziju. 26 ispitanika nije pohađalo ništa od navedenog. 12 ispitanika je pohađalo ekonomsku školu. 11 ispitanika je pohađalo tehničku školu. 7 ispitanika je pohađalo tehničara za računalstvo. 4 ispitanika su pohađala upravnu školu. 2 ispitanika su pohađala elektrotehničku školu. Po 1 ispitanik je pohađao strojarsko tehničku školu i tehničar za mehatroniku.

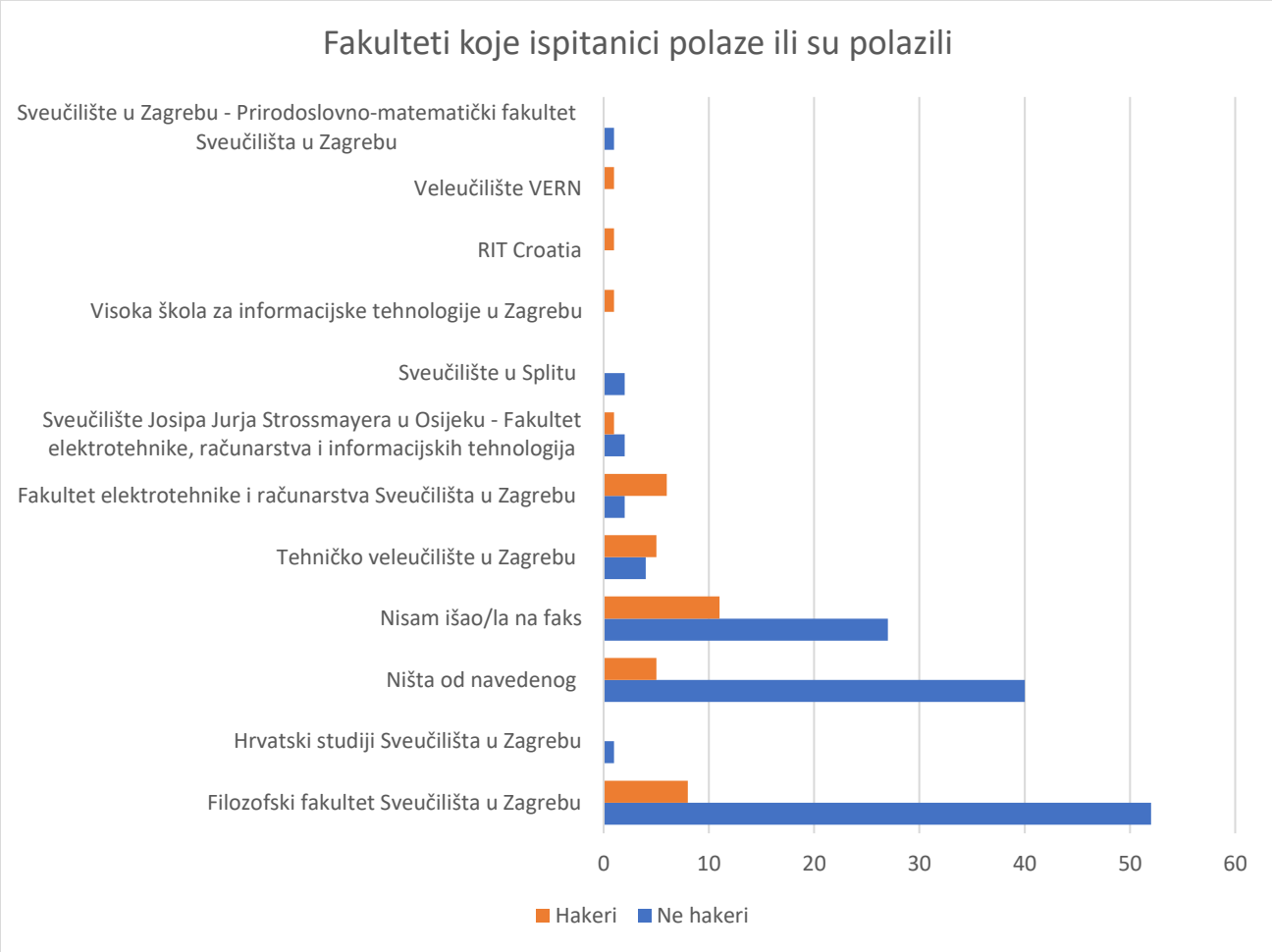
Od 39 ispitanika koji su hakirali 14 ispitanika je pohađalo gimnaziju. 10 ispitanika je išlo u smjer srednje škole tehničar za računalstvo. 4 ispitanika su pohađala srednju tehničku školu. 4 ispitanika nisu pohađali nijednu navedenu srednju školu. 3 ispitanika su pohađala srednju ekonomsku, a 2 srednju elektrotehničku školu. Po jedan ispitanik je pohađao upravnu i strojarsko tehničku srednju školu.



Graf 5. Smjer srednjoškolskog obrazovanja.

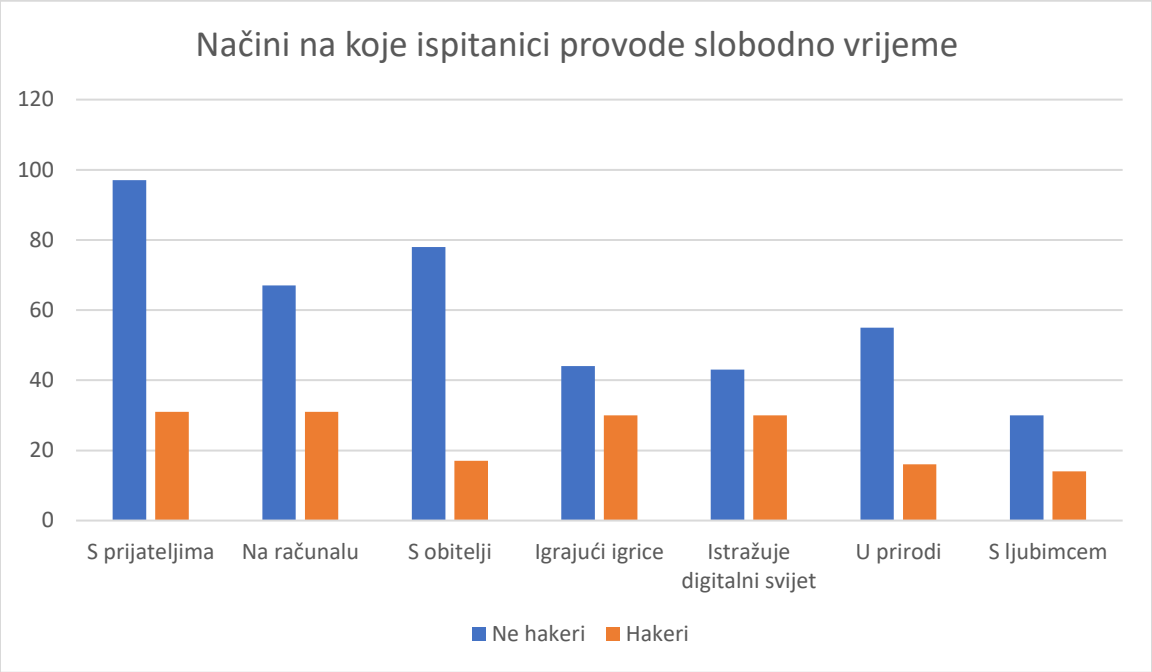
Graf 6 prikazuje koji fakultet pohađaju ili su pohađali ispitanici. Od 131 ispitanika koji nije hakirao 52 ispitanika pohađaju ili su pohađali Filozofski fakultet Sveučilišta u Zagrebu. 40 ispitanika nije išlo niti na jedan navedeni fakultet. 27 ispitanika nije išlo na fakultet. 4 ispitanika pohađaju ili su pohađali Tehničko veleučilište u Zagrebu. Po 2 ispitanika pohađaju ili su pohađala Sveučilište Josipa Jurja Strossmayera u Osijeku - Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Sveučilište u Splitu, Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu. Po 1 ispitanik pohađa ili je pohađao Sveučilište u Zagrebu - Prirodoslovno-matematički fakultet Sveučilišta u Zagrebu, Hrvatske studije Sveučilišta u Zagrebu.

Od 39 ispitanika koji su hakirali čak 11 ispitanika nije išlo na fakultet. 8 ispitanika pohađa ili je Filozofski fakultet Sveučilišta u Zagrebu. 6 ispitanika pohađa ili je pohađalo Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu. 5 ispitanika nije polazilo niti jedan navedeni fakultet. 5 ispitanika pohađa ili je pohađalo Tehničko veleučilište u Zagrebu. Po jedan ispitanik pohađa ili su pohađali RIT Croatia, Veleučilište VERN, Sveučilište Josipa Jurja Strossmayera u Osijeku - Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Visoka škola za informacijske tehnologije u Zagrebu.



Graf 6. Fakulteti koje ispitanici polaze ili su polazili.

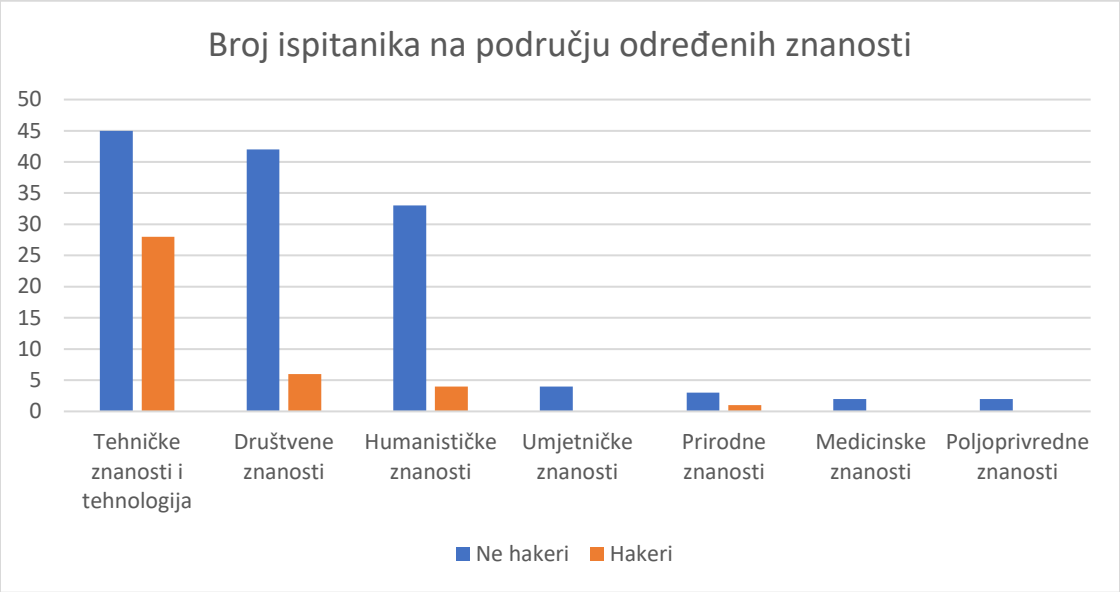
Na Grafu 7. je prikazano kako naši ispitanici provode svoje slobodno vrijeme. Ispitanici su mogli odabrati više odgovora istovremeno. Od 131 ispitanika koji nije hakirao 97 ispitanika provodi svoje slobodno vrijeme s prijateljima, 78 ispitanika s obitelji, 67 ispitanika na računalu. 55 ispitanika provodi slobodno vrijeme u prirodi, 44 ispitanika igrajući igrice, 43 ispitanika istražujući digitalni svijet, 30 ispitanika s ljubimcem. Slobodno vrijeme istražujući digitalni svijet provodi 30 od 39 ispitanika koji su hakirali. 31 ispitanik provodi slobodno vrijeme na računalu. 30 ispitanika provodi slobodno vrijeme igrajući igrice. 31 ispitanik provodi vrijeme s prijateljima. 17 ispitanika provodi slobodno vrijeme s obitelji. 16 ispitanika provodi slobodno vrijeme u prirodi, a njih 14 s ljubimcima.



Graf 7. Načini na koje ispitanici provode slobodno vrijeme.

Graf 8 prikazuje u kojim znanstvenim područjima ispitanici rade ili studiraju. Od 131 ispitanika koji ne hakira 45 ispitanika radi/studira na području tehničkih znanosti i tehnologije, 42 ispitanika na području društvenih znanosti, 33 ispitanika na području humanističkih znanosti. 4 ispitanika radi ili studira na području umjetničkih znanosti, 3 ispitanika na području prirodnih znanosti, po 2 ispitanika na medicinskim i poljoprivrednim znanostima.

Od 39 ispitanika koji su hakirali 28 ispitanika radi ili studira na području tehničkih znanosti i tehnologije. 6 ispitanika radi na području društvenih znanosti. 4 ispitanika rade na području humanističkih znanost. 1 ispitanik radi na području prirodnih znanosti.

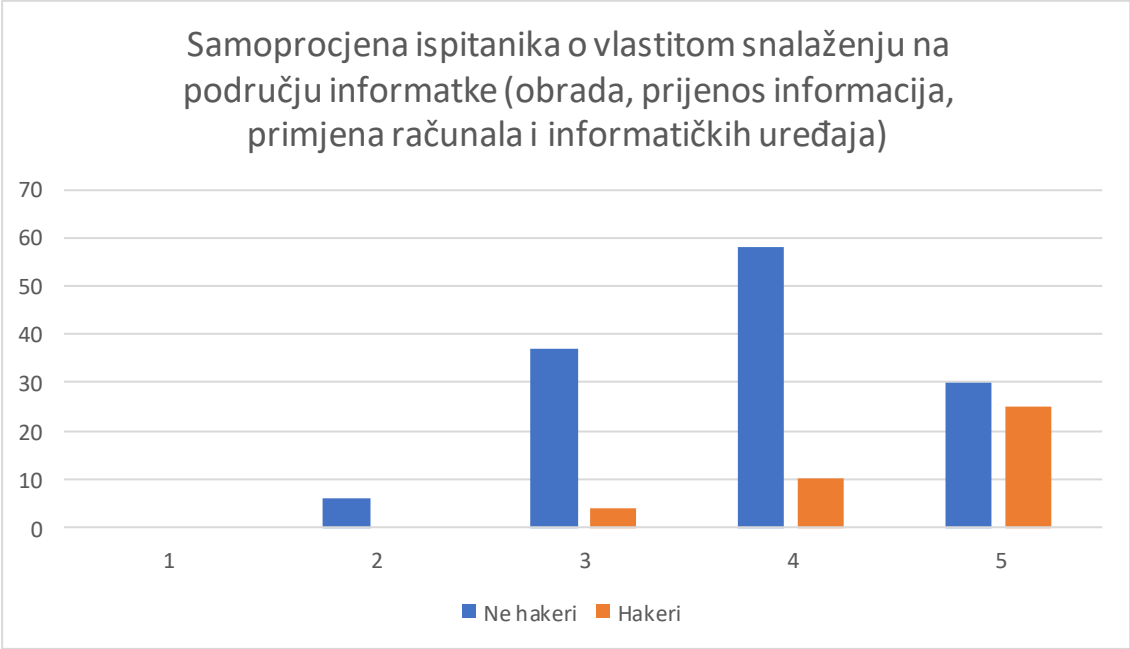


Graf 8. Znanstvena područja u kojima ispitanici rade ili studiraju.

6.1.2. Druga skupina pitanja

Idući zadatak ispitanika bio je procijeniti koliko dobro od 1 do 5 se snalaze na području informatike (obrada, prijenos informacija, primjena računala i informatičkih uređaja). Rezultate prikazuje Graf 9. Od 131 ispitanika koji nije hakirao 58 ispitanika je sebe ocijenilo s 4, 37 ispitanika s 3, 30 ispitanika s 5, 6 ispitanika s 2. Niti jedan ispitanik sebe nije ocijenio s 1.

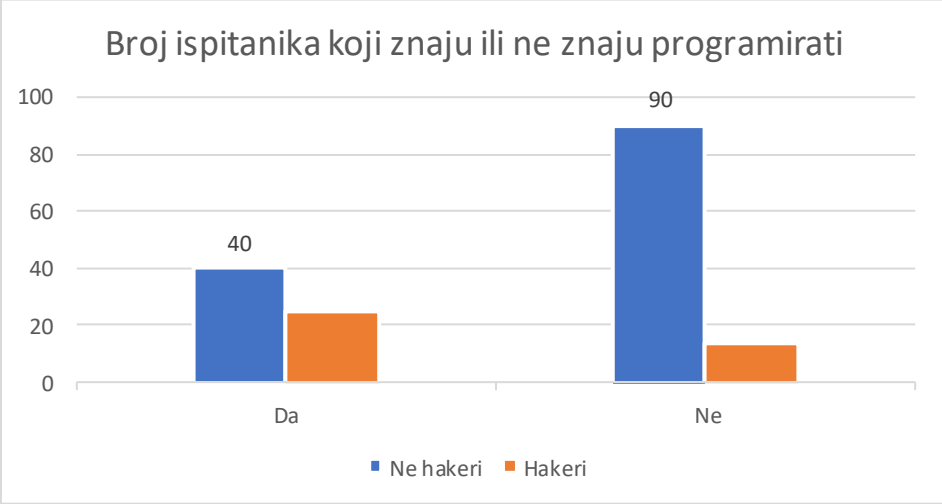
25 od 39 ispitanika koji su hakirali je vlastite sposobnosti snalaženja na području informatike ocijenilo s 5. 10 ispitanika je sebi dalo ocjenu 4, i 4 ispitanika su sebi dala ocjenu 3. Niti jedan ispitanik nije sebe ocijenio s 1 ili 2.



Graf 9. Samoprocjena ispitanika o vlastitom snalaženju na području informatike.

Graf 10 pokazuje koliko ispitanika zna i koliko ne zna programirati. Od 131 ispitanika koji nisu hakirali njih 90 ne zna programirati, a 40 ispitanika zna programirati.

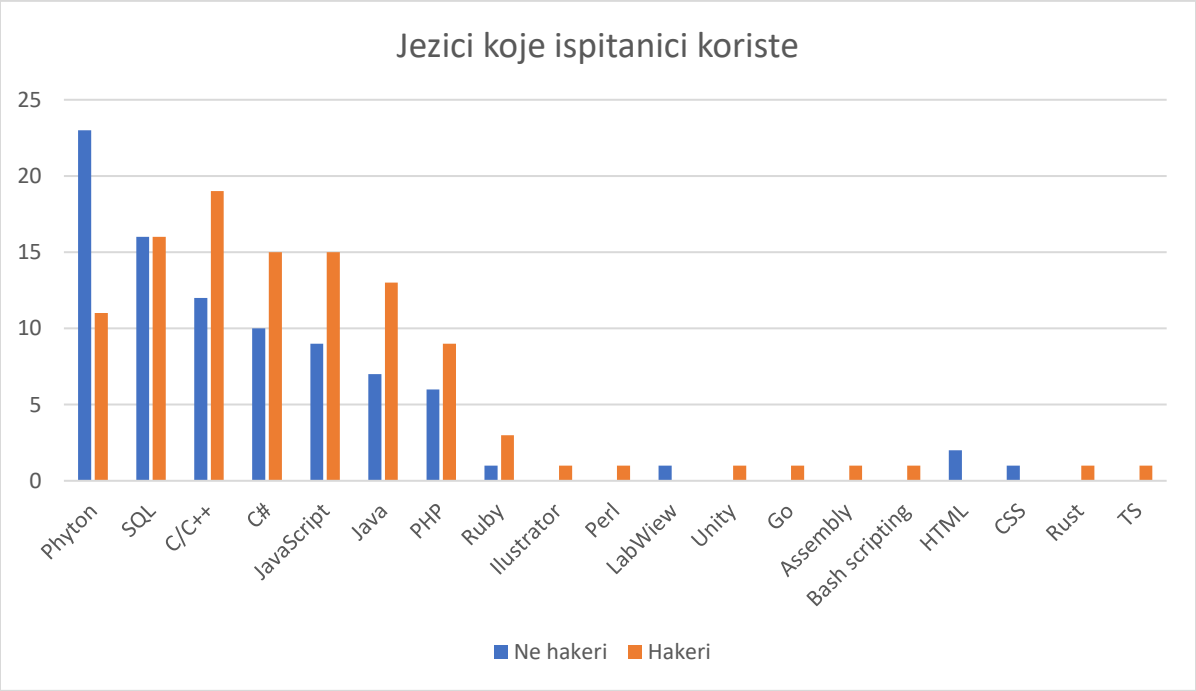
25 od 39 ispitanika se izjasnilo kako zna programirati, a njih 14 se izjasnilo kako ne zna programirati.



Graf 10. Podjela ispitanika na one koji znaju i ne znaju programirati.

Graf 11. prikazuje koje jezike koriste oni koji znaju programirati. Ispitanici su mogli odabrati više jezika ili napisati jezik ako nije ponuđen. Od 40 ispitanika koji znaju programirati, a nisu hakirali, njih 23 koristi Python, 16 ispitanika koristi SQL, 12 ispitanika koristi C/C++, 10 ispitanika koristi C#, 9 ispitanika koristi JavaScript. 7 ispitanika koristi Javu, 6 ispitanika koristi PHP, 2 ispitanika koriste HTML. Po 1 ispitanik koristi Ruby, LabView, CSS

Od 31 ispitanika koji su hakirali, 25 ispitanika se izjasnilo kako zna programirati. 14 ispitanika ne zna programirati. 19 ispitanika koristi C/C++, po 16 ispitanika koristi SQL i C# 15 ispitanika koristi JavaScript, 13 ispitanika koristi Javu, 11 ispitanika koristi Python, 9 ispitanika koristi PHP, 3 ispitanika koriste Ruby. Po 1 ispitanik koristi Ilustrator, Perl, Unity, GO, Assembly, Bash scripting, Rust, TS.



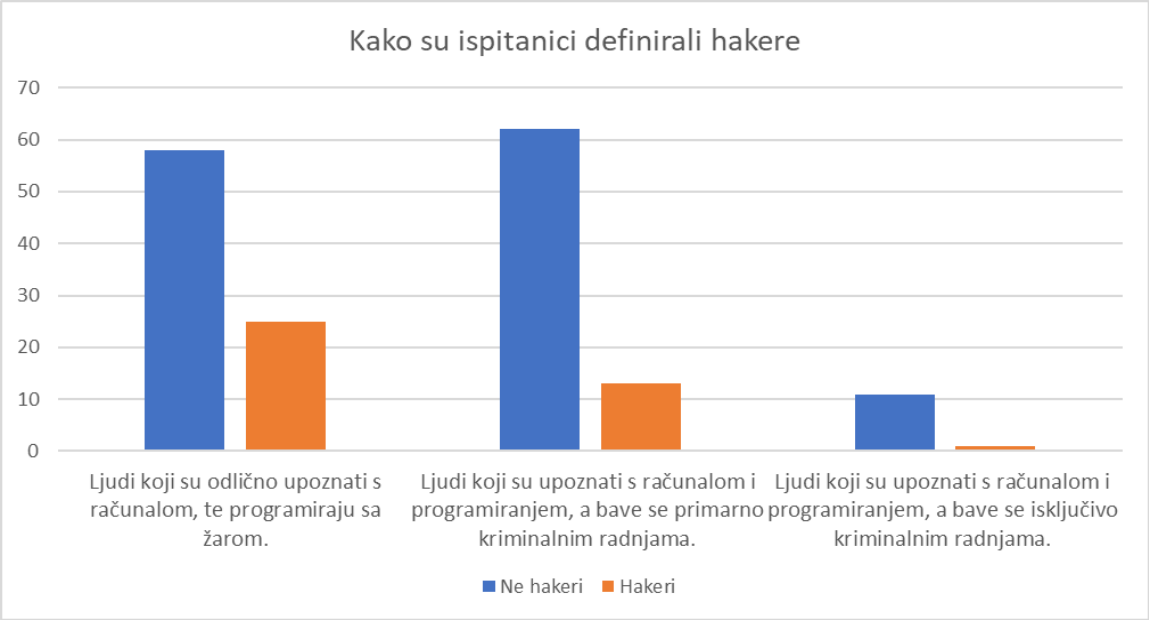
Graf 11. Jezici koje koriste ispitanici koji znaju programirati.

6.1.3. Treća skupina pitanja

U trećoj skupini pitanja ispitanici su morali pokazati svoje znanje o hakerima. Graf 12. prikazuje prvo pitanje iz treće skupine na kojem su ispitanici mogli odabrati jedan od tri ponuđena odgovora. Od 131 ispitanika koji nije hakirao 62 ispitanika su hakere

definirali kao ljude koji su upoznati s računalom i programiranjem, a bave se primarno kriminalnim radnjama. 58 ispitanika je hakere definiralo kao ljude koji su odlično upoznati s računalom, te programiraju sa žarom. 11 ispitanika je hakere definiralo kao ljude koji su upoznati s računalom i programiranjem, a bave se isključivo kriminalnim radnjama.

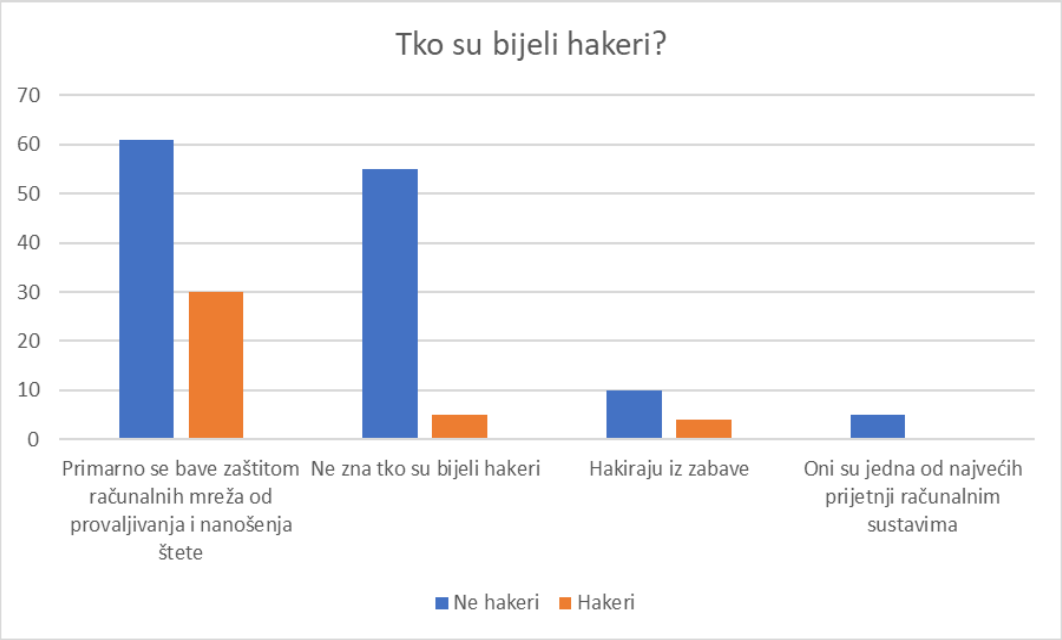
Od 39 ispitanika koji su hakirali 25 ispitanika je odgovorilo da su to ljudi koji su odlično upoznati s računalom, te programiraju sa žarom. 13 ispitanika je odgovorilo da su hakeri ljudi koji su upoznati s računalom i programiranjem, a bave se primarno kriminalnim radnjama. Samo 1 ispitanik je odgovorio da su hakeri ljudi koji su upoznati s računalom i programiranjem, a bave se isključivo kriminalnim radnjama



Graf 12. Ispitanici definiraju hakere.

Graf 13. prikazuje odgovore ispitanika na pitanje vezano uz bijele hakere. Ispitanici su mogli odabrati jedan od četiri ponuđena odgovora. Od 131 ispitanika koji nikada nisu hakirali 61 ispitanik je odgovorio kako se bijeli hakeri primarno bave zaštitom računalnih mreža od provaljivanja i nanošenja štete. 55 ispitanika nije znalo odgovor. 10 ispitanika smatra kako bijeli hakeri hakiraju iz zabave. 5 ispitanika bijele hakere smatra jednom od najvećih prijetnja računalnim sustavima.

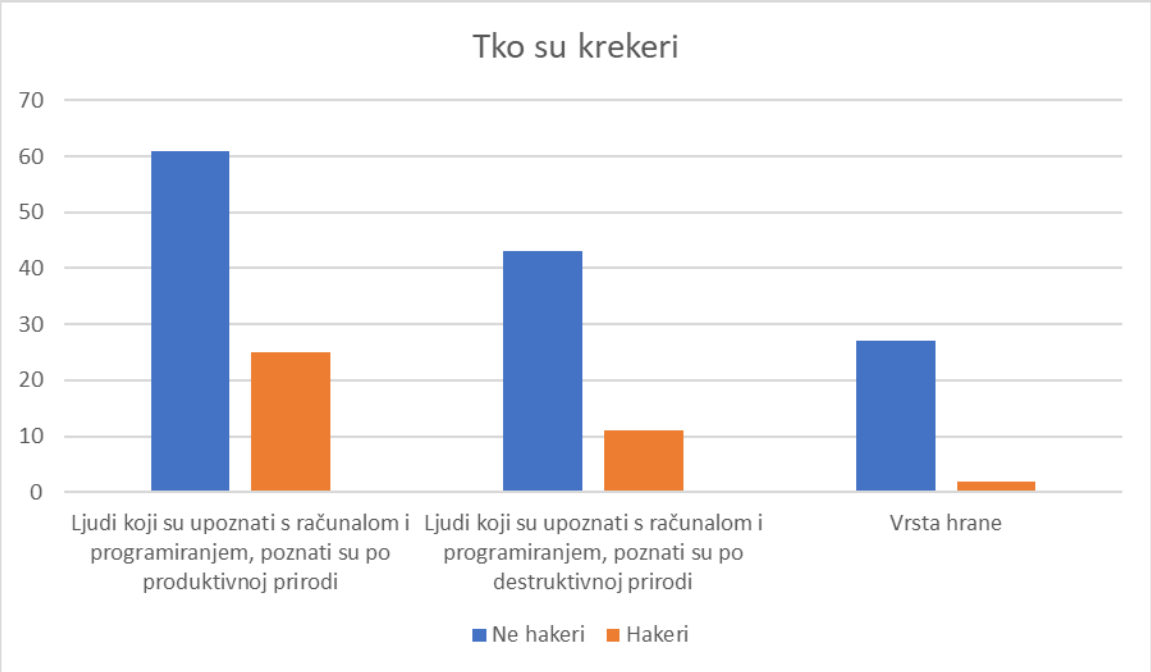
Na pitanje tko su bijeli hakeri 30 od 39 ispitanika je odgovorilo kako se bijeli hakeri primarno bave zaštitom računalnih mreža od provaljivanja i nanošenja štete. 5 ispitanika nije znalo odgovor. 4 ispitanika smatraju da bijeli hakeri hakiraju iz zabave.



Graf 13. Ispitanici definiraju bijele hakere.

Graf 14 pokazuje kako ispitanici definiraju krekere. Ispitanici su mogli odabrati jedan od 3 ponuđena odgovora. Od 131 ispitanika koji nije hakirao 61 ispitanik je krekere definirao kao ljude koji su upoznati s računalom i programiranjem, a poznati su po destruktivnoj prirodi. 43 ispitanika su definirala krekere kao ljude koji su upoznati s računalom i programiranjem, a poznati su po produktivnoj prirodi. 27 ispitanika smatra krekere vrstom hrane.

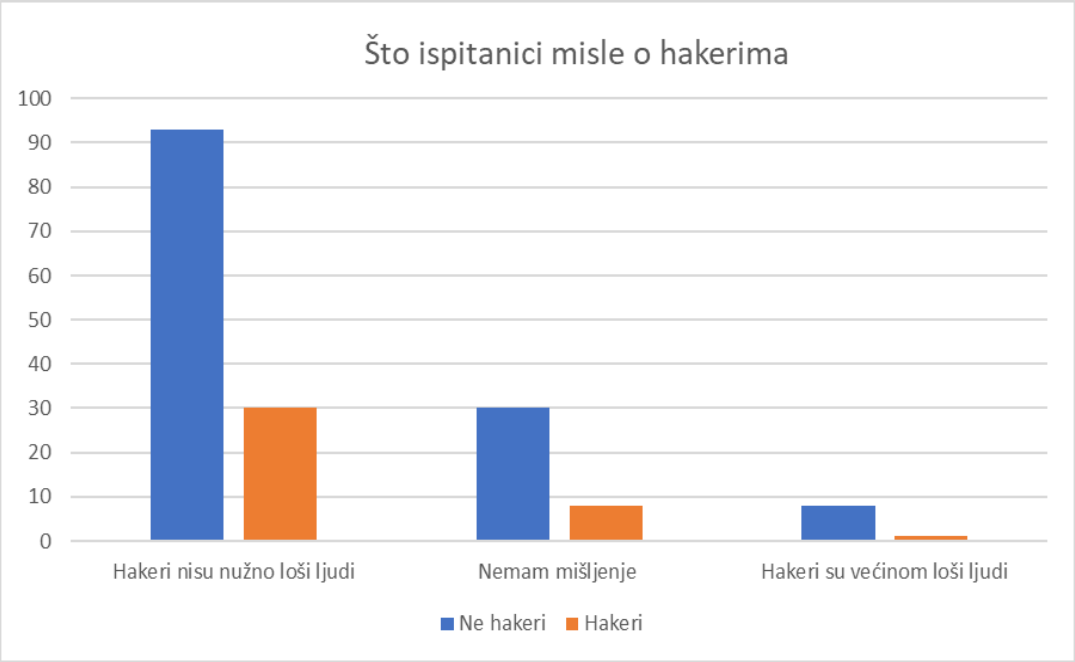
Od 39 ispitanika koji su hakirali 25 ispitanika krekere smatra ljudima koji su upoznati s računalom i programiranjem, a poznati su po destruktivnoj prirodi. 11 ispitanika smatra krekere ljudima koji su upoznati s računalom i programiranjem, a poznati su po produktivnoj prirodi. 3 ispitanika smatraju krekere vrstom hrane.



Graf 14. Tko su krekeri?

Graf 15 prikazuje kakvo mišljenje o hakerima imaju ispitanici. Od 131 ispitanika koji nije hakirao 93 ispitanika ne smatra hakere nužno lošim ljudima. 30 ispitanika nema mišljenje. 8 ispitanika smatra kako su hakeri većinom loši ljudi.

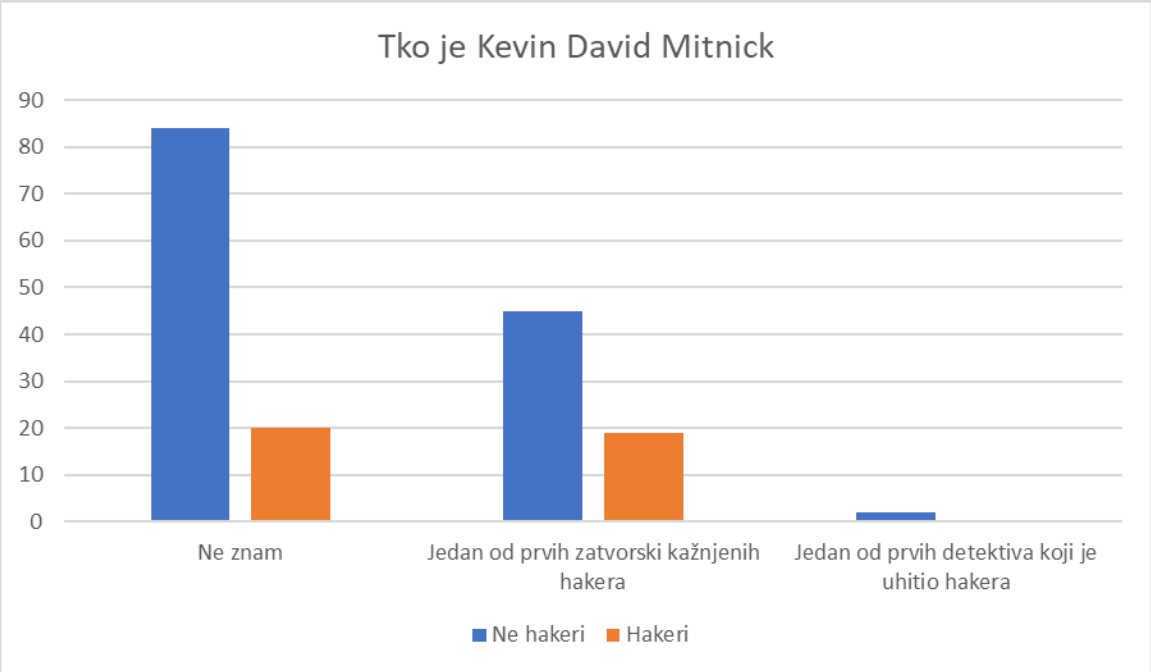
30 od 39 ispitanika koji su hakirali smatra kako hakeri nisu nužno loši ljudi. 8 ispitanika nema mišljenje. 1 ispitanik smatra kako su hakeri većinom loši ljudi.



Graf 15. Mišljenja ispitanika o hakerima.

U Grafu 16 možemo vidjeti što ispitanici znaju o Kevinu David Mitnicku. Od 131 ispitanika koji nije hakirao 84 ispitanika ne znaju tko je Kevin David Mitnick. 45 ispitanika je odgovorilo da je on jedan od prvih zatvorski kažnjenih hakera. 2 ispitanika smatraju kako je on jedan od prvih detektiva koji je uhitio hakera.

20 od 39 ispitanika ne zna tko je Kevin David Mitnick. 19 ispitanika je odgovorilo da je on jedan od prvih zatvorski kažnjenih hakera.



Graf 16. Znanje ispitanika o Kevinu David Mitnicku.

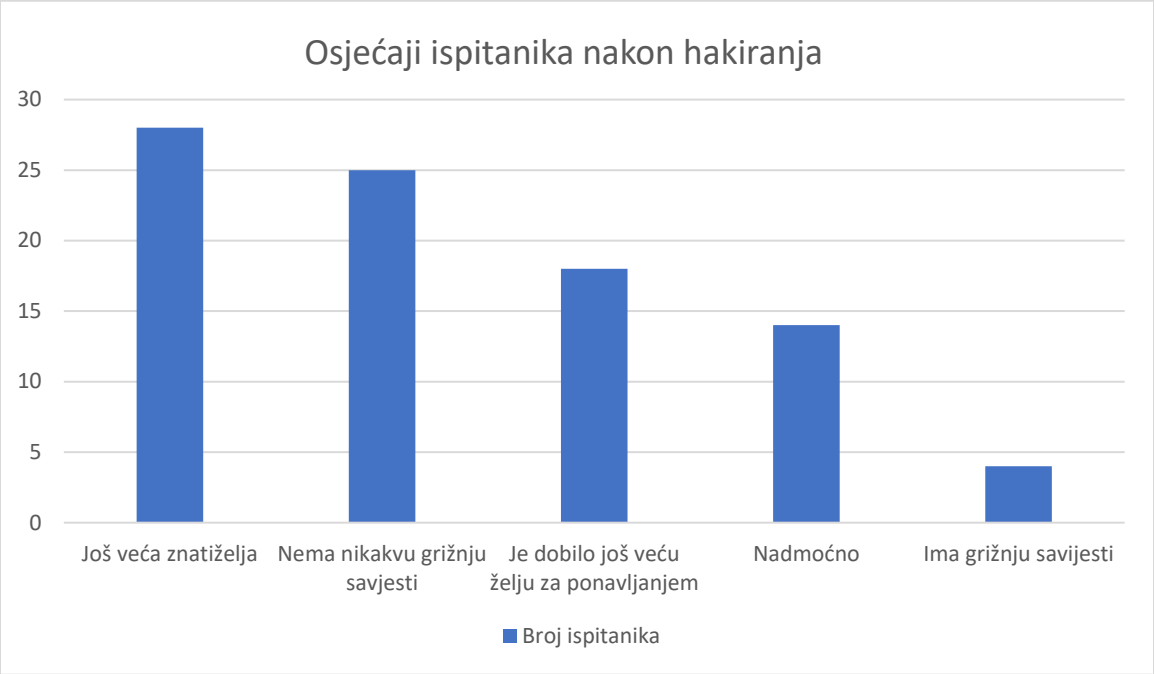
6.1.4. Četvrta skupina pitanja

U četvrtoj skupini pitanja dolazi do podjele ispitanika na one koji su hakirali i one koji nisu. Oni koji su hakirali moraju izraziti svoje osjećaje i razloge vezane uz hakiranje. Ispitanici koji nisu hakirali su morali odabrati razloge zašto nisu hakirali, te što misle kako bi se osjećali da jesu hakirali.

Od 170 ispitanika na Grafu 17 vidimo kako 131 (77.1%) ispitanik nije nikada hakirao, dok 39 (22.9%) ispitanika je hakiralo barem jednom u životu.

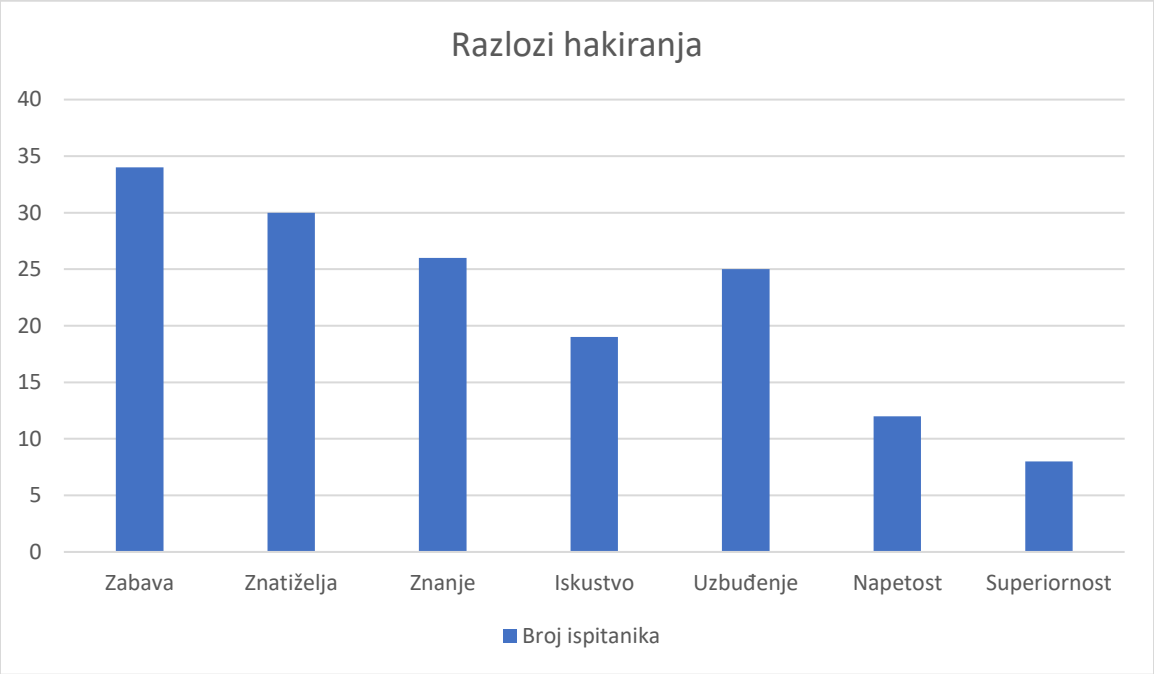
Graf 17. Koliko ispitanika je hakiralo?

39 ispitanika koji su hakirali su potom davali odgovore na pitanja „Kako si se osjećao/la nakon hakiranja ?“ i „Koji je bio razlog hakiranja?“. Ispitanici su mogli odabrati više odgovora istovremeno. Na grafu 18. vidljivo je kako je 28 (71.8%) naših hakera razvilo još veću znatiželju, 25 ispitanika (64.1%) nije imalo nikakvu grižnju savjesti, a njih 18 (46.2%) su dobili želju za ponavljanjem hakerskog čina. 14 (35.9%) ispitanika se osjećalo nadmoćno dok su svega 4 (10.3%) ispitanika koja su hakirala osjećala grižnju savjesti.



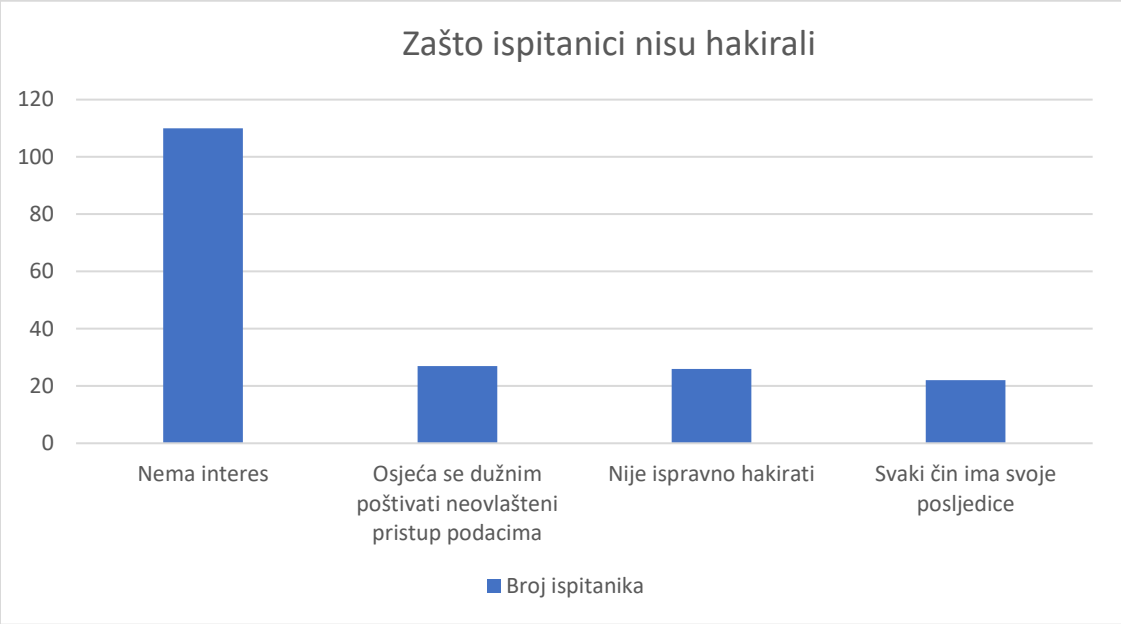
Graf 18. Osjećaji ispitanika nakon hakiranja.

U Grafu 19 vidimo razloge koje naši hakeri navode za hakiranje. 34 (87.2%) od 39 ispitanika je hakiralo zbog zabave, 30 (76.9%) ispitanika zbog znatiželje, a 26 (66.7%) ispitanika zbog stjecanja znanja. 19 (38.7%) ispitanika je željelo steći iskustvo, 25 (38.5%) ispitanika je hakiralo zbog uzbuđenja, 12 (30.8%) ispitanika zbog napetosti, 8 (20.5%) ispitanika zbog osjećaja superiornosti.



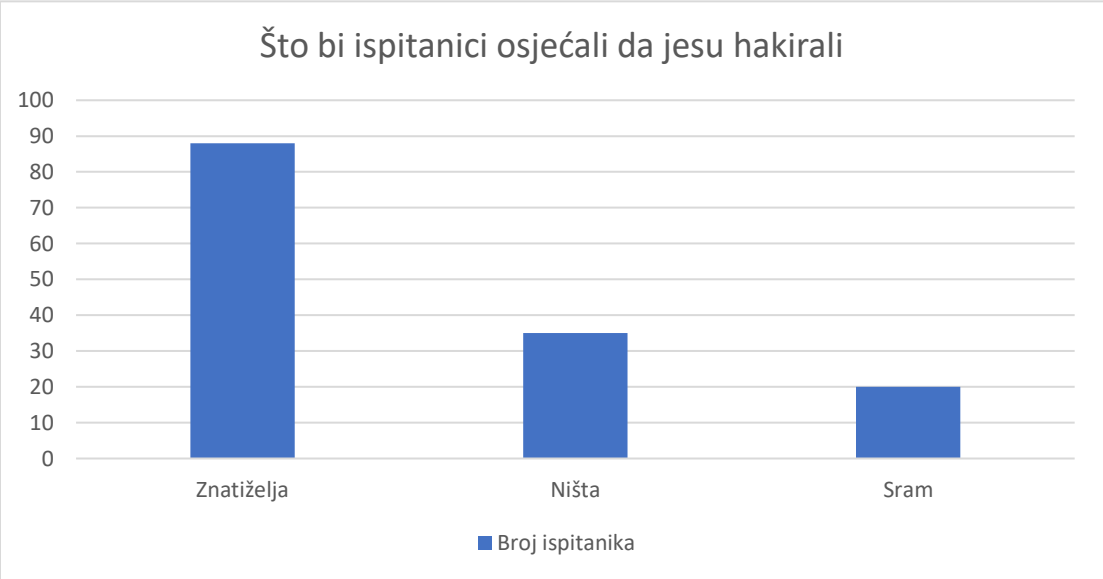
Graf 19. Razlozi hakiranja?

Ispitanici koji nikada nisu hakirali, njih 131, su odgovarali na pitanja „Zašto nikada nisi hakirao/la?“, te su morali pretpostaviti što bi osjećali da jesu hakirali. Ispitanici su mogli istovremeno odabrati više odgovora. Na Grafu 20 vidimo kako je najveći razlog ne hakiranja ne postojanje interesa 110 (84%). Samo 27 (20.6%) ispitanika se osjeća dužnima poštivati neovlašteni pristup podacima, 26 (19.8%) ispitanika smatra kako nije ispravno hakirati, 22 (16.8%) ispitanika misli kako svaki čin ima svoje posljedice.



Graf 20. Razlozi ne hakiranja.

Graf 21 pokazuje što ispitanici koji nisu hakirali misle da bi osjećali nakon hakiranja. Ispitanici su mogli odabrati više odgovora istovremeno. 88 (57.2%) od 131 ispitanika misli da bi osjećalo znatiželju. 35 (26.7%) ispitanika misli da ne bi osjećalo ništa, samo 20 (15.3%) ispitanika misli da bi osjećalo sram.



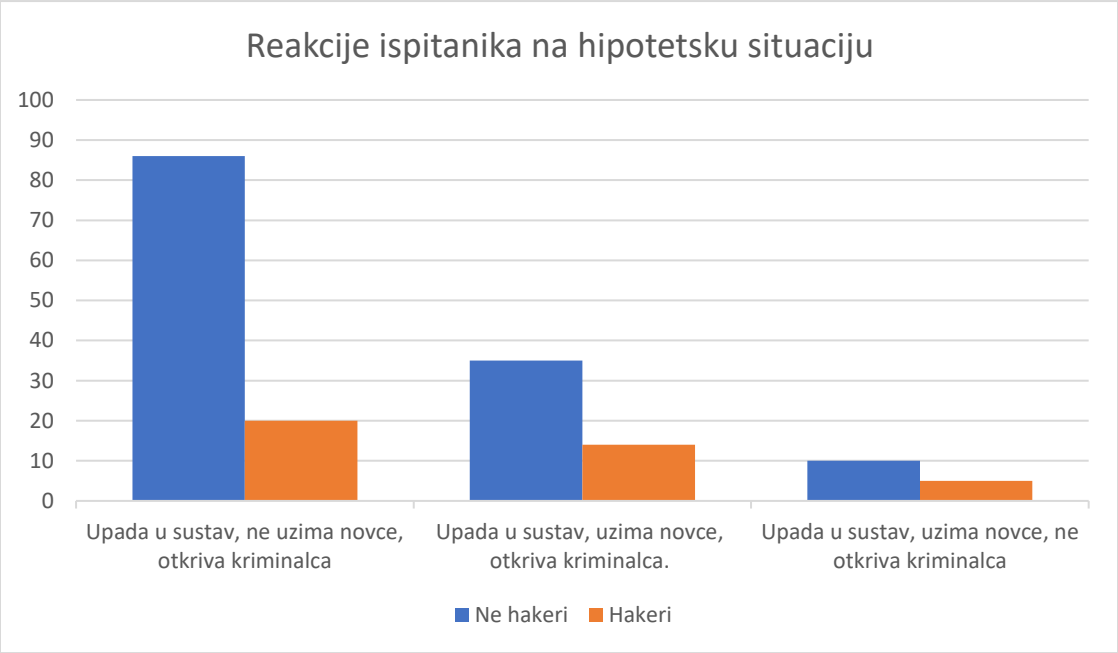
Graf 21. Mišljenja ispitanika što bi osjećali da jesu hakirali?

6.1.5. Peta skupina pitanja

Na zadnju skupinu pitanja odgovaraju svi ispitanici. Predstavljena je hipotetska situacija u kojoj vlasnik banke posjeduje mnogo ne legalno stečenog novca. Banka mu služi samo kao paravan za pranje novca. Ispitanika se stavlja u sljedeću poziciju: ispitanik zna kako bi svojim znanjem i vještinama mogao/la uzeti ne legalno stečeni novac i raskrinkati kriminalca. Uz to postoji sto postotna sigurnost da ispitanikov identitet neće biti otkriven. Ispitanik ima tri ponuđene opcije djelovanja od kojih se može odabrati samo jedna. Pogledaj graf 22.

Od 131 ispitanika koji nije hakirao 86 ispitanika upada u sustav, ne uzima novce i otkriva kriminalca. 35 ispitanika upada u sustav, uzima novce, otkriva kriminalca. 10 ispitanika upada u sustav, uzima novce i ne otkriva kriminalca.

U slučaju hipotetske situacije 20 od 39 ispitanika koji su hakirali upada u sustav, ne uzima novce, otkriva kriminalca. 14 ispitanika upada u sustav, uzima novce, otkriva kriminalca. 5 ispitanika upada u sustav, uzima novce, ne otkriva kriminalca.

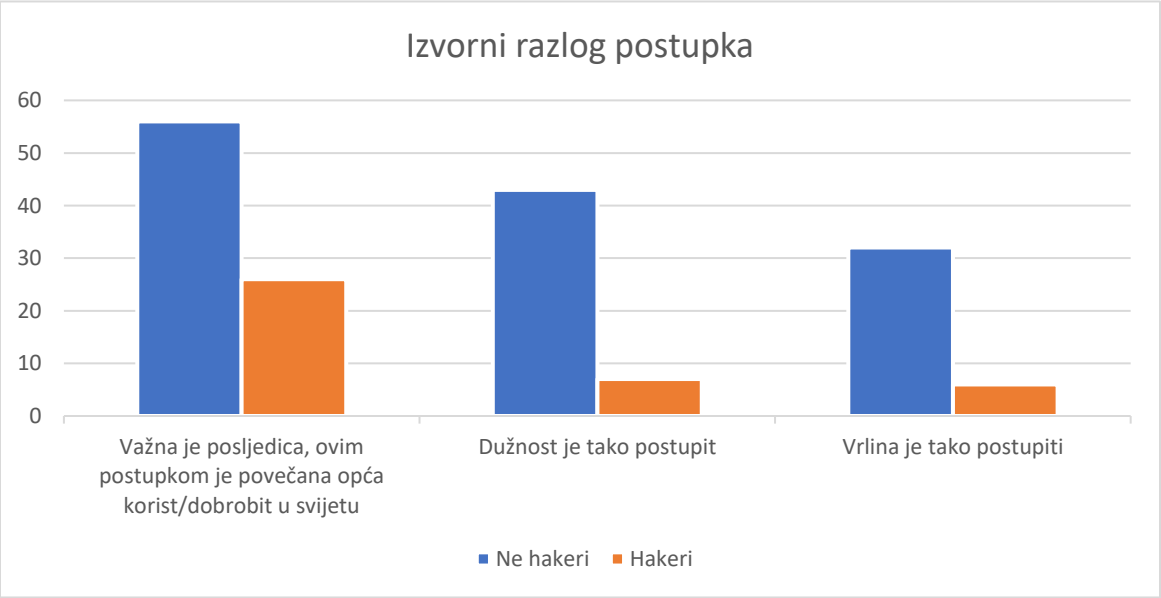


Graf 22. Reakcije ispitanika na hipotetsku situaciju.

Graf 23 prikazuje izvorne razloge ispitanikovih odluka. Svaki ispitanik je mogao odabrati jedan od tri ponuđena razloga. Prema objašnjenim etičkim teorijama u odlomku Etika ispitanike sam smjestila u prikladnu etičku skupinu. Ispitanici koji su odabrali posljedicu spadaju u konzekvencijalističku, preciznije utilitarističku etiku. Ispitanici koji su postupili zbog dužnosti spadaju u deontološku etiku. Ispitanici koji su postupili prema vrlini spadaju u aretaičku etiku ili etiku vrlina.

Od 131 ispitanika 56 ispitanika je postupilo zbog povećavanja opće koristi i dobrobiti u svijetu. 43 ispitanika su osjećala kako su dužni tako postupiti. 32 ispitanika su smatrali vrlinom tako djelovati.

Kao izvorni razlog odluke 26 od 39 ispitanika koji su hakirali je odgovorilo da je važna je posljedica, ovim postupkom povećava opću korist/dobrobit u svijetu. 7 ispitanika je odgovorilo da je njihova dužnost tako postupiti. 6 ispitanika je smatralo da je vrlina tako postupiti.



Graf 23. Izvorni razlog ispitanikovih postupaka.

6.2. Analiza rezultata ankete

Na temelju ankete možemo vidimo kako 131 (77%) ispitanik nije nikada hakirao, dok 39 (23%) ispitanika tvrdi da je barem jednom u životu hakiralo. Iz ankete možemo zaključiti kako su muškarci skloniji hakiranju. 85% ispitanika koji su hakirali su muškarci, a samo 15% ispitanica koje su hakirale su žene. Uzimajući u obzir da je 83% ispitanika rođeno između 1990. i 2000., očekivano je kako 84 ispitanika 64% ispitanika koji su hakirali rođeno u tom desetljeću. Najviše ispitanika, 74% je iz Grada Zagreba i Zagrebačke županije. U skladu s time je najveći broj hakera iz Grada Zagreba, 44% ispitanika. Iz Zagrebačke županije je 18% hakera. Najviše hakera, njih 31 % ima završen sveučilišni preddiplomski studiji/stručni preddiplomski studiji. Čak 28 % hakera ima završeno četverogodišnje/petogodišnje strukovno srednjoškolsko obrazovanje. Najviše hakera, 36% dolazi iz gimnazijskog srednjoškolskog obrazovanja. Najveći broj hakera, 28% nije išao na fakultet. 79% hakera slobodno vrijeme koristi podjednako za prijatelje i na računalo čime se razbija ideja o nesocijaliziranim hakerima sa slabim društvenim sposobnostima. Znanstveno područje na kojima ljudi rade uvelike utječe na njihov razvoj interesa što primjećujemo iz činjenice da 72% hakera radi na području tehničkih znanosti i tehnologije. 64% hakera je svoje snalaženje na području informatike ocijenilo s 5. To pokazuje veliku sigurnost i svjesnost svojih sposobnosti ako uzmemo u obzir da je samo 23% ne hakera ocijenilo svoje sposobnosti s 5. Najviše, čak 64% hakera zna programirati, a 69% ne hakera ne zna programirati. Od jezika hakeri najviše koriste C/C++ 76%, SQL 64%, C# 60%, JavaScript 60%.

Hakeri većinom sebe definiraju kao ljude koji su odlično upoznati s računalom, te programiraju sa žarom. Tako je odgovorilo 64% hakera. Najviše ne hakera je hakere definiralo kao ljude koji su upoznati s računalom i programiranjem, a bave se primarno kriminalnim radnjama. Možemo primijetiti kako društvo više ne gleda na hakere kao ljude koji se bave isključivo kriminalnim radnjama. 77% hakera i 71% ne hakera misle kako hakeri nisu nužno loši ljudi.

Hakeri su pokazali veću upućenost u dane pojmove vezane uz hakiranje. Tako je 64% hakera odgovorilo da su krekeri ljudi koji su upoznati s računalom i programiranjem, poznati su po destruktivnoj prirodi. 47% ne hakera je točno odgovorilo na navedeno

pitanje. 52% hakera ne zna tko je Kevin David Mitnick. 49% hakera je znalo tko je Kevin David Mitnick. Samo 34% ne hakera su odgovorili da je Kevin David Mitnick jedan od prvih zatvorski kažnjenih hakera.

Nakon hakiranja najviše hakera, 72% je dobilo još veću znatiželju. Ne hakeri, njih 67% je također odgovorilo kako bi najvjerojatnije osjetilo znatiželju u slučaju hakiranja. Hakere motivira zabava 87%, znatiželja 77% i znanje 67%. Ne hakeri, 84% nemaju nikakvog interesa veznih uz hakiranje.

U postavljenoj hipotetskoj situaciji najviše ispitanika, hakera 51% i ne hakera 66% se pokazalo dobronamjernim ljudima koji žele pomoći bez iskorištavanja. Većina ispitanika je odabrala upasti u sustav, ne uzeti novce i otkriti kriminalca. Slijedi 27% ne hakera i 36% hakera koji upadaju u sustav, uzimaju novce i otkrivaju kriminalca. Hakeri su prema tome malo skloniji iskoristiti trenutak za svoju dobrobit ako nema posljedica. Svi ispitanici su se u teoretskoj situaciji pokazali najmanje sklonima upasti u sustav, uzeti novce i ne otkriti kriminalca. U ovom odabiru hakeri također imaju malo veći postotak. Hakera koji bi tako postupili ima 13%, dok ne hakera ima 8% .

Ne hakeri 43% i hakeri 67% su najskloniji utilitarističkoj etičkoj teoriji. Najveći utjecaj na donošenje odluke ima posljedica i opća dobrobit svijeta. 33% hakera i 18% ne hakera se pridružuje deontološkoj etičkoj teoriji postupanjem iz dužnosti. U aretaičku etiku smjestilo se 24% ne hakera i 15% hakera uzimajući vrlinu kao izvorni razlog odluke.

Navedene postotke možemo vidjeti na slijedećoj stranici u Tablici 1. Tablica 1 donosi kratak pregled najzastupljenijih odgovora hakera i ne hakera u anketi.

Tablica 1. Popis i postotak najbrojnijih odgovora hakera i ne hakera.

	Hakeri		Ne hakeri	
	23%		77%	
Muškarci **Žene**	85% 15%		40% 60%	
Najviše rođenih	1990.-2000.	64%	1990. -2000.	64%
Županija	Grad Zagreb	44%	Grad Zagreb	40%
Stupanj obrazovanja	Sveučilišni preddiplomski studiji/stručni preddiplomski studiji	31%	Sveučilišni preddiplomski studiji/stručni preddiplomski studiji	37%
Smjer srednjoškolskog obrazovanja	Gimnazija	36%	Gimnazija	51%
Fakultet	Nije išlo na fakultet	28%	Filozofski fakultet Sveučilišta u Zagrebu	40%
Slobodno vrijeme	S prijateljima Na računalu	79%	S prijateljima	74%
Znanstveno područje	Tehničke znanosti i tehnologije	72%	Tehničke znanosti i tehnologije	34%
Samoprocjena	5	64%	4	44%
Znanje programiranja	Da	64%	Ne	69%
Jezici	C/C++	76%	Python	56%
Definiranje hakera	Ljudi koji su upoznati s računalom i programiranjem, te programiraju sa žarom	64%	Ljudi koji su upoznati s računalom i programiranjem, a bave se primarno kriminalnim radnjama	47%
Definiranje bijelih hakera	Primarno se bave zaštitom računalnih mreža od provaljivanja i nanošenja štete	77%	Primarno se bave zaštitom računalnih mreža od provaljivanja i nanošenja štete	47%
Definiranje krekera	Ljudi koji su upoznati s računalom i programiranjem, poznati su po destruktivnoj prirodi	64%	Ljudi koji su upoznati s računalom i programiranjem, poznati su po destruktivnoj prirodi	47%
Mišljenje o hakerima	Oni nisu nužno loši ljudi	77%	Oni nisu nužno loši ljudi	71%
Kevin David Mitnick	Ne znam	51%	Ne znam	64%
Osjećaji hakera nakon hakiranja	Još veća znatiželja	72%	/	/

	Hakeri		Ne hakeri	
Razlozi hakiranja	Zabava Znatiželja	87% 77%	/	/
Razlozi ne hakiranja	/	/	Nema interes	84%
Ne hakeri smatraju da bi u slučaju hakiranja osjećali	/	/	Znatiželju	67%
Reakcija na hipotetsku situaciju	Upada u sustav, ne uzima novce, otkriva kriminalca	51%	Upada u sustav, ne uzima novce, otkrira kriminalca	66%
Izvorni razlog ispitanikovih postupaka	Važna je posljedica, ovim postupkom je povečana opća korist/dobrobit u svijetu	67%	Važna je posljedica, ovim postupkom je povečana opća korist/dobrobit u svijetu	43%

7. Zaključak

Razvoj prvih računala, prvi programer i programerka uvode nas u nastanak hakera 21. stoljeća. Hakeri čine 23% ispitanika što nam govori da čine dobar dio populacije i zato je važno znati tko su oni, kako se obraniti od zlih hakera i kako potaknuti dobre da napreduju. Važno je i da oni sami znaju tko su i tko mogu postati. Upravo sa tom svrhom je napravljen ovaj rad.

Većina naših osobnih podataka nalazi se na Internetu. Datum rođenja, ime i prezime, spol i ostali najintimniji podaci kolaju Internetom. Velike korporacije koriste umrežene sustave, računala, Internet kako bi poslovale. Informacijsko doba u 21. stoljeću pokazuje svoju snagu. Komunikacija, dijeljenje, obrada i pohrana podataka posjeduju nezamislivu moć manipulacije ljudima i njihovim djelovanjima. Onaj tko ima podatak, ima i moć. Hakeri su primijetili moć koju pružaju pristup i manipulacija podatcima. Iako hakere uglavnom prati negativna konotacija, ovaj rad pokazuje kako postoje dobri hakeri koji brinu o našoj privatnost i upozoravaju nas na pogreške koje sami činimo ne brigom o podatcima koje olako puštamo na Internet ili ih bezbrižno dajemo velikim tvrtkama.

Motivi hakiranja mogu biti raznoliki. Kreću se od čiste želje za znanjem, osjećaja uzbuđenja i znatiželje do želje za dokazivanjem nadmoći i izrugivanjem, slanja političkih poruka publiciteta ili krađe novaca i informacija. Iako su hakeri u 21. stoljeću uglavnom smatrani kao zločinci ovaj rad pokazuje da postoje i dobri hakeri koji brinu za dobrobit drugih ljudi. Većina hakera poštuje osnovne etičke norme, a sve više hakera postaju zagovornici slobode i sigurnosti informacijskog doba. Hakeri nisu isključivo zločinci koji su zatvoreni u četiri zida i ne odvajaju se od svojeg računala. Sama anketa je pokazala kako bi najviše hakera, 20 od 39, u hipotetskoj situaciji učinilo najispravniju stvar. Oni bi iskoristili svoje vještine kako bi otkrili kriminalce bez uzimanja novaca. Motivacija koja ih potiče na djelovanje nalazi se u utilitarističkoj etičkoj teoriji. Utilitarizam pokazuje kako uzimaju u obzir druge ljude jednako kao sebe, važne su im posljedice njihovog djelovanja, a sama anketa pokazuje kako većina ispitanika teži najvećoj mogućoj sreći za sve ljude.

Ovaj rad je pokazao kako hakeri cijene osobine kao što su marljivost, predanost, i želja za inovativnošću i samorazvojem. To su osobine koje su naslijedili još od svojih

prethodnika poput B. Pascala, G. W. Leibniza, C. Babbagea, Ade Lovelace, A. Turinga i još mnogih. Hakeri su posebna skupina unutar društva koja odskače svojom strašću i ljubavi. Upravo ta strast i predanost im omogućavaju da postanu novi vladari koji iz pozadine kreiraju svijet. Moć, znanje i vještine koje posjeduju potrebno usmjeriti na dobro, a u tome im mi trebamo pomoći.

8. Literatura

KNJIGE

1. Babić, Vladica: Kompjuterski kriminal, Sarajevo Rabic, 2009.
2. Cole, E. Hackers Beware, New Riders Publishing, 2001., dostupno na https://doc.lagout.org/security/Hackers%20Beware.pdf. Pristupljeno 5.4.2019.
3. Davenport, H., Thomas: Big data @ work, The Human Side of Big Data (85-113). Harvard Business Review Press, Boston, 2014.
4. Davis, Kord; Patterson, Doug: Ethics of big data, O´reilly, 2012.
5. Dragičević, Dražen: Kompjutorski kriminalitet i informacijski sustavi, Informatorov biro sustav, 2004.
6. Isaacson, Walter: The innovators: how a group of hackers, geniuses, and geeks created the digital revolution, A CBS Company, London, 2014.
7. Kutleša, Stipe, Filozofski leksikon, Leksikografski zavod Miroslava Krleže, 2012.
8. Levy, Steven: Hackers: Heroes of the computer revolution, Delta Book, New York, 1994.
9. Pekka, Himanen: Hakerska Etika i duh informacijskog doba, Jesenski i Turk Zagreb, 2002.
10. Quinn, Michael: Ethics for the information age. Introduction to ethics (49-109). InformationPrivacy (227-271). Computer and Network security (321-325), Bosto, Pearson, 2017.
11. Raymond, Eric S | Steele, Guy L. The new hacker's dictionary Cambridge, Mass.; London: The MIT Press, 1996.
12. Singh, Simon: Šifre. Kratka povijest kriptografije, Mozaik knjiga, Zagreb 2003.

ČLANCI

13. Berčić, B. (2008). Etika vrlina. Filozofska istraživanja 28(1), 193–207. Preuzeto s https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=36503
14. Berčić, B. (2008). Utilitarizam. Filozofska istraživanja 28(2), 363–377. Preuzeto s https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=43921

FILMOVI

15. Badham, John. WarGames (1983)
16. Chappelle, Joe. Takedown (2000)
17. Mann, Michael. Blackhat (2015)
18. Softley, Iain. Hackers (1995)
19. Wachowski, Lana i Lilly. The Matrix (1999)

DOKUMENTARNI FILMOVI:

20. Anonymous Official, Anonymous Documentary - How Anonymous Hackers Changed the World Full Documentary, https://www.youtube.com/watch?v=FAECyLvSCHg&t=1228s. Objavljeno: 3.7.2014. Pristupano: 29.3.2019.
21. captjack5169, Hackers & Phreakers Documentary, https://www.youtube.com/watch?v=9-oZa9tkJsw. Objavljeno: 8.2.2013. Pristupano: 21.3.2019.
22. Chạm Mưa, Hacker Documentary - 2001 - Secret History of Hacking, https://www.youtube.com/watch?v=T-aOrz6aobg. Objavljeno: 7.12.2017. Pristupano: 20.3.2019.
23. The Documentary Network, DEFCON - The Full Documentary, https://www.youtube.com/watch?v=3ctQOmjQyYg. Objavljeno: 6.8.2013. Pristupano: 2.4.2019.

YOU TUBE VIDEOZAPISI

24. Forbes DACH, Interview mit Ralph Echemendia Ethical Hacker (Pioneers'17), https://www.youtube.com/watch?v=-sHBajH_gHE. Objavljeno: 27.6. 2017. Pristupano 25.3.2019.
25. Pioneers, Pioneers '17 | Ralph Echemendia: How secure is your Identity? https://www.youtube.com/watch?v=_UkcpbQd8f0. Objavljeno: 17.7.2017. Pristupano: 28.3.2019.

26. Silicon Republic, Interview with renowned hacker Kevin Mitnick, https://www.youtube.com/watch?v=LaypU4qAuYw. Objavljeno: 3.3.2018. Pristupano: 25.3.2019.
27. TEDx Talks, Why I chose to be an ethical hacker | Ruben van Vreeland | TEDxEindhove, https://www.youtube.com/watch?v=CftZnvZdtJw. Objavljeno: 16.1.2018. Pristupano: 1.4.2019.
28. The Infographics Show, How Did These Insanely Smart Hackers Get Caught And Arrested, https://www.youtube.com/watch?v=ZZBnXgiwaR0&feature=youtu.be&fbclid=IwAR3NGYwWwaRXeCgEqXPo_6Wfz5Z1w9yQUH-F0j52ju3qCPn4RTfJXV8mvsQ. Objavljeno: 26.1.2019. Pristupano: 27.3.2019.
29. Vodafone Business, Cyber security: Interview with an ethical hacker [Episode 5], https://www.youtube.com/watch?v=GVDFM9X1prI. Objavljeno: 14.8.2014. Pristupano: 1.4.2019.

INTERNET IZVORI

30. Alfred Ng. (7.9,2018.) How the Equifax hack happened, and what still needs to be done, preuzeto s https://www.cnet.com/news/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/. Pristupano: 29.3.2019.
31. Algebra, Certifikacijski seminari: Certified Ethical Hacker (CEH) Preuzeto s https://www.algebra.hr/certifikacijski-seminari/ec-council/certified-ethical-hacker-ceh/. Pristupano 12.4.2019.
32. Encyclopaedia Britannica. (23.11.2016.) Abacus: Calculating device. Preuzeto s https://www.britannica.com/technology/abacus-calculating-device. Pristupano 3.5.2019.
33. Encyclopaedia Britannica. (30.1.2019.) History of computing. Preuzeto s https://www.britannica.com/technology/computer/History-of-computing. Pristupano 3.5.2019.

34. Hoven van den J., Blaauw M., Pieters W., Warnier M. (20.11.2014.) Privacy and Information Technology. Preuzeto s https://plato.stanford.edu/entries/it-privacy/. Pristupano 8.4.2019.
35. Hrvatska enciklopedija. Čip. Preuzeto s http://www.enciklopedija.hr/natuknica.aspx?id=13410. Pristupano 19.3.2019.
36. Hrvatska enciklopedija. Elektronska cijev. Preuzeto s http://www.enciklopedija.hr/natuknica.aspx?id=17651. Pristupano 5.5.2019.
37. Hrvatska enciklopedija. Integrirani sklop. Preuzeto s http://www.enciklopedija.hr/natuknica.aspx?id=27588. Pristupano 19.3.2019.
38. Hrvatska enciklopedija. Neuronska mreža. Preuzeto s http://www.enciklopedija.hr/Natuknica.aspx?ID=43562. Pristupano 5.5.2019.
39. Hrvatska enciklopedija. Tranzistor. Preuzeto s http://www.enciklopedija.hr/Natuknica.aspx?ID=62073. Pristupano 5.5.2019.
40. Michael R. Swaine Paul A. Freiberger. (26.4. 2019.) Pascaline https://www.britannica.com/technology/Pascaline. Pristupano: 28.4.2019.
41. Ewbank, A. (18.5.2018) Early Hackers Used Whistles From Cap'n Crunch Cereal Boxes. Preuzeto s https://www.atlasobscura.com/articles/capn-crunch-whistle. Pristupano 17.5.2019.
42. H-Wilson, Danielle. (11.10.2016.) Ada Lovelace Day. Preuzeto s https://digitalblog.coop.co.uk/tag/charles-babbage/. Pristupano 17.5.2019.
43. Riffe, S. (27.2.2018.) WWII Enigma Machines Among Computing Treasures Added to University Libraries Collection. Preuzeto s https://www.cmu.edu/news/stories/archives/2018/february/enigma-machines.html. Pristupano: 10.4.2019.
44. Sadowski, J, (8.9.2019) Why do big hacks happen? Preuzeto s https://www.theguardian.com/commentisfree/2017/sep/08/why-do-big-hacks-happen-blame-big-data. Pristupano 20.3.2019.
45. Science Focus (9.10.2018.): How Ada Lovelace's notes on the Analytical Engine created the first computer program. Preuzeto s

https://www.sciencefocus.com/future-technology/how-ada-lovelaces-notes-on-the-analytical-engine-created-the-first-computer-program/. Pristupano 30.4.2019.

46. Smith, J., L. (17.3.2019.) Top Hacking Simulator Games Every Aspiring Hacker Should Play, https://hackwarenews.com/top-hacking-simulator-games-every-aspiring-hacker-should-play-part-1/. Pristupano 13.4.2019.
47. Sorell, T. (22.10.2010.) Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous. Preuzeto s https://academic.oup.com/jhrp/article/7/3/391/2412155. Pristupano 10.3.2019.
48. Technopedia. Black hat hacker. Preuzeto s https://www.techopedia.com/definition/26342/black-hat-hacker. Pristupano 15.3.2019.
49. Technopedia. Gray hat hacker. Preuzeto s https://www.techopedia.com/definition/15450/gray-hat-hacker. Pristupano 15.3.2019.
50. Technopedia. White hat hacker. Preuzeto s https://www.techopedia.com/definition/10349/white-hat-hacker. Pristupano 15.3.2019.