Prijevare putem digitalne tehnologije

Dobrica, Nikolina

Sveučilište u Zagrebu

Ekonomski fakultet

Preddiplomski sveučilišni studij „Poslovna ekonomija“

PRIJEVARE PUTEM DIGITALNE TEHNOLOGIJE

ZAVRŠNI RAD

Studentica: Nikolina Dobrica

JMBAG: 0067498463

Kolegij: Informatika

Mentorica: prof. dr. sc. Mirjana Pejić Bach

Zagreb, rujan 2019.

Nikolina Dobrica

Ime i prezime studenta/ice

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad

(vrsta rada)

isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. 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. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student/ica:

U Zagrebu, 23. 9. 2019.

Nikolina Dobrica

(potpis)

SADRŽAJ

SAŽETAK 5
SUMMARY 6
1. UVOD 1
1.1. Predmet i cilj rada 1
1.2. Izvori podataka i metode prikupljanja podataka 1
1.3. Sadržaj i struktura rada 2
2. DIGITALNA TEHNOLOGIJA 3
2.1. Pojam digitalne tehnologije 3
2.2. Važnost i utjecaj digitalne tehnologije 5
2.3. Digitalna kultura 6
3. KRIMINALITET U KIBERNETIČKOM PROSTORU 7
3.1. Pojam kriminaliteta u kibernetičkom prostoru 7
3.1.1. Digitalna forenzika 8
3.2. Pravna regulativa kriminaliteta u kibernetičkom prostoru Republike Hrvatske 8
3.2.1. Ostala dodirna kaznena djela 8
3.2.1.1. Kaznena djela protiv časti i ugleda 9
3.2.1.2. Kaznena djela spolnog zlostavljanja i iskorištavanja djeteta 9
3.2.1.3. Kaznena djela protiv intelektualnog vlasništva 9
3.2.1.4. Kaznena djela protiv javnog reda 10
3.3. Nedozvoljena ponašanja u kibernetičkom prostoru 10
3.3.1. Hakiranje 10
3.3.2. Računalna sabotaža 11
3.3.3. Sabotaža računalnih sustava i podataka 11
3.3.4. Računalna špijunaža 11
3.3.5. Računalno piratstvo 12
3.3.6. Računalna prijevara 12
3.3.7. Zloporaba naprava 12
3.4. Nacionalna strategija kibernetičke sigurnosti 12
3.4.1. Statistički podaci o kibernetičkom kriminalu u Republici Hrvatskoj 13
4. PRIMJERI PRIJEVARA PUTEM DIGITALNE TEHNOLOGIJE 16
4.1. Prijevare s osobnim podacima 17

4.2. Nigerijske prijevare 18
4.3. Nagradne igre i lutrije 19
4.4. Prijevare sa zapošljavanjem 20
4.5. Prijevare lijekovima 22
4.6. Prijevare kreditnim karticama 22
4.7. Klik prijevare 23
4.8. Lažne recenzije i stranice 24
4.9. Digitalno krivotvorenje 26
4.10. Lažne vijesti 27
4.11. Ostale opasnosti 28
4.12. Osnovna online zaštita 29
5. ZAKLJUČAK 30
LITERATURA 31
POPIS NAVODA I IZVORA PODATAKA 33
POPIS SLIKA 34

SAŽETAK

Ovaj završni rad na temelju sekundarnih izvora podataka objašnjava pojam i kratki povijesni pregled digitalne tehnologije, te njezinu važnost i utjecaj, kao i pojam digitalne kulture. Također, definiran je i pojam kriminaliteta u kibernetičkom prostoru, te su navedena kaznena djela i nedozvoljena ponašanja, nakon čega slijedi objašnjenje nacionalne strategije kibernetičke sigurnosti. Nadalje, opisani su brojni primjeri prijevara u digitalnoj tehnologiji kako bi se što bolje prikazali mogući načini zlouporabe podataka.

Digitalna tehnologija je dovela do Treće revolucije, a uvela je svijet i u Četvrtu. Neosporiva je njezina važnost i utjecaj na čovječanstvo, te ona sa sobom donosi nova znanja ali i prijetnje. Razvojem Interneta, pametnih telefona, fotografije i sl., razvijaju se i negativni načini iskorištavanja istih. U Republici Hrvatskoj, kao i u svijetu, postoji pravna regulativa kriminaliteta u kibernetičkom prostoru, točnije propisana kaznena djela i nedozvoljena ponašanja, a statistika pokazuje da bi se opširnost regulative mogla i povećati budući da broj korisnika Interneta i digitalne tehnologije konstantno raste, a time i broj kriminalaca. Isto tako, zabilježeni su brojni primjeri prijevara putem digitalne tehnologije, te svaki od njih ima svoje karakteristike i načine otuđivanja digitalnih podataka. Međutim, svaki od njih ima i svoje nedostatke, te se već i uz samu informiranost mogu izbjeći. Ovo je aktualna tema koja se svakim danom proširuje i mijenja, baš kao što je i razvoj tehnologije nezaustavljiv.

Ključne riječi: digitalna tehnologija, kibernetički kriminal, kaznena djela, nedozvoljena ponašanja, prijevare

SUMMARY

On the basis of secondary data sources this final work explains the concept and brief historical overviews of digital technology, its importance and impact, as well as the concept of digital culture. Cybercrime is also explained, and criminal offenses and misconduct are listed, which are followed by the national cyber security strategy. Furthermore, numerous examples of digital fraud have been described in order to present all the possible ways of misusing data.

Digital technology led to the Third Revolution, and it introduced the world to the Fourth. Its importance and influence on humanity is indisputable, it carries new knowledge, but also many threats. With the development of the Internet, smartphones, photography, etc., there are also negative ways of exploiting them. In the Republic of Croatia, as in the world, there is a legal regulation of cybercrime, precisely prescribed criminal offenses and illegal behavior, and statistics show that the prolixity of these regulations could be bigger due to the fact the number of Internet and digital users constantly grows, and therby the number of criminals, too. Likewise, numerous examples of digital frauds are recorded, and each has its own characteristics and ways of alienating digital data. However, each of them also has its drawbacks, and they can be avoided even with only regular information. This is a topic that expands and changes every day, just like the development of technology is unstoppable.

Keywords: digital technology, cybercrime, criminal offenses, illicit behavior, fraud

1. UVOD

Digitalna tehnologija je iznimno bitan faktor današnjeg načina života. Od njezinog početka pa do danas je utjecala je gotovo na sve ljude. Koliko je to dobro, toliko donosi sa sobom i loše strane, te se, kao i u svakom području, i ovdje razvija kriminalitet. Za razliku od ostalih kaznenih djela, ona u digitalnoj tehnologiji se teško dokazuju zbog opširnosti i anonimnosti koje pruža Internet. Pravne regulative su nužne i potrebno ih je ozbiljno shvatiti. Od kaznenih djela protiv časti i ugleda, do kaznenih djela protiv javnog reda, uz nedozvoljena ponašanja kao što je hakiranje, piratstvo i špijunaža, neporeciva je statistika njihovog rasta u modernom društvu Republike Hrvatske, kao i u svijetu. Broj i raznolikost prijevara, te njihova ponekad zapanjujuća inovativnost i efikasnost, je realnost s kojom se svaki korisnik može susresti koristeći digitalnu tehnologiju. Navedeni primjeri, poput *phishinga*, nigerijskih i klik prijevara, lažnih recenzija itd., samo su dio informativnog znanja potrebnog da se one i izbjegnu, uz osnovnu online zaštitu.

1.1. Predmet i cilj rada

Predmet ovog rada je opisati utjecaj digitalne tehnologije, te zatim objasniti kriminalitet i prijevare putem digitalne tehnogije. Cilj rada je obrazovati čitatelje o pojmovima kibernetičkog kriminala, kao i upozoriti na moguće različite prijevare koje im prijete kao digitalnim korisnicima.

1.2. Izvori podataka i metode prikupljanja podataka

U radu su korišteni sekundarni izvori podataka kako bi se objasnili osnovni pojmovi vezani uz temu. Proučena je domaća i strana stručna i znanstvena literatura. Relevantni internetski izvori su u najvećoj mjeri poslužili za istraživanje teme budući da se radi o samom Internetu i informacijama koje se konstantno mijenjaju i ažuriraju, te nisu sve dostupne u knjigama. Što se tiče metode prikupljanja podataka, u radu je primjenjena metoda istraživanja za stolom, tzv. *desk research*.

1.3. Sadržaj i struktura rada

Rad je podijeljen u 5 cjelina. Nakon Uvoda, u drugoj cjelini je objašnjen pojam i važnost digitalne tehnologije kao ključnog elementa rada, a uz koju je definirana i digitalna kultura. U trećoj cjelini definiran je kibernetički kriminal, te su, po pravnoj regulativi, detaljno nabrojena kaznena djela i nedozvoljena ponašanja u kibernetičkom prostoru, iza čega slijedi nacionalna strategija kibernetičke sigurnosti. Četvrta cjelina je u cijelosti posvećena primjerima prijevare putem digitalne tehnologije. Na kraju rada, kao peta cjelina, donesen je Zaključak na temelju prikupljenog znanja o temi.

2. DIGITALNA TEHNOLOGIJA

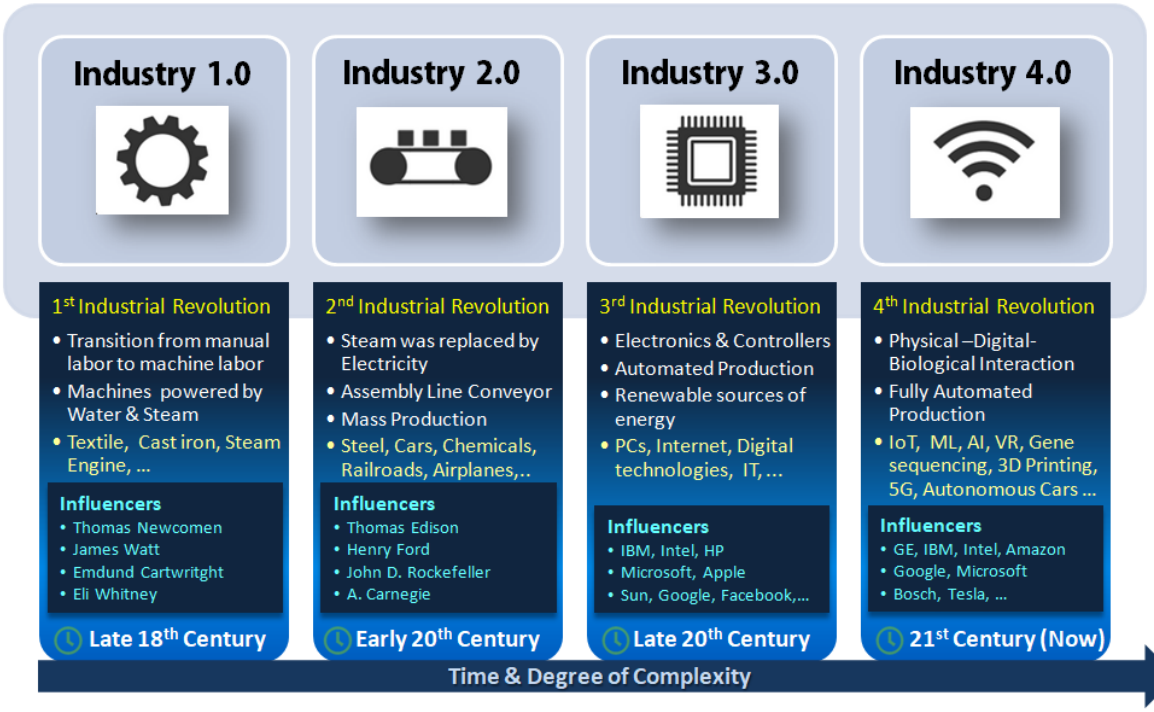
Konvergencija telekomunikacija, medija i računarstva promijenila je način na koji radimo i živimo. Jedno za drugim, sve je povezano. Informacije prolaze kroz mreže s većim intenzitetom i mijenjaju sve. Tržišta nestaju i zamjenjuju se mrežama informacija s kupcem u srži. Snaga je prešla na potrošača koji se ponaša kao aktivni element mreže, a ne kao pasivni cilj tržišta. Sve se kreće brže – trendovi, novosti, novi proizvodi, tržišta… Tržišta i svijet sada su složeniji, internetski orijentirani, prilagodljivi sustavi.[1]

2.1. Pojam digitalne tehnologije

Digitalna tehnologija je usko povezana s digitalnom revolucijom. Prema Sinčić (2018) „digitalna je revolucija, također poznata i kao Treća industrijska revolucija, a odnosi se na napredak tehnologije iz analognih elektroničkih i mehaničkih uređaja na digitalnu tehnologiju dostupnu danas. Digitalna revolucija također označava početak razdoblja informacija. Središte ove revolucije je masovna proizvodnja i raširena upotreba digitalnih inovacija uključujući računalo, digitalni mobilni telefon i internet.“

Digitalna je tehnologija započela svoj razvoj krajem 20. stoljeća te nas je u 21. stoljeću iz Treće industrijske revolucije uvela u Četvrtu revoluciju, tj. doba umjetne inteligencije, autonomnih vozila kao što je npr. Tesla, virtualne realnosti, 3D printanja, itd. Razlike između industrijskih revolucija objašnjene su na Slici 1.

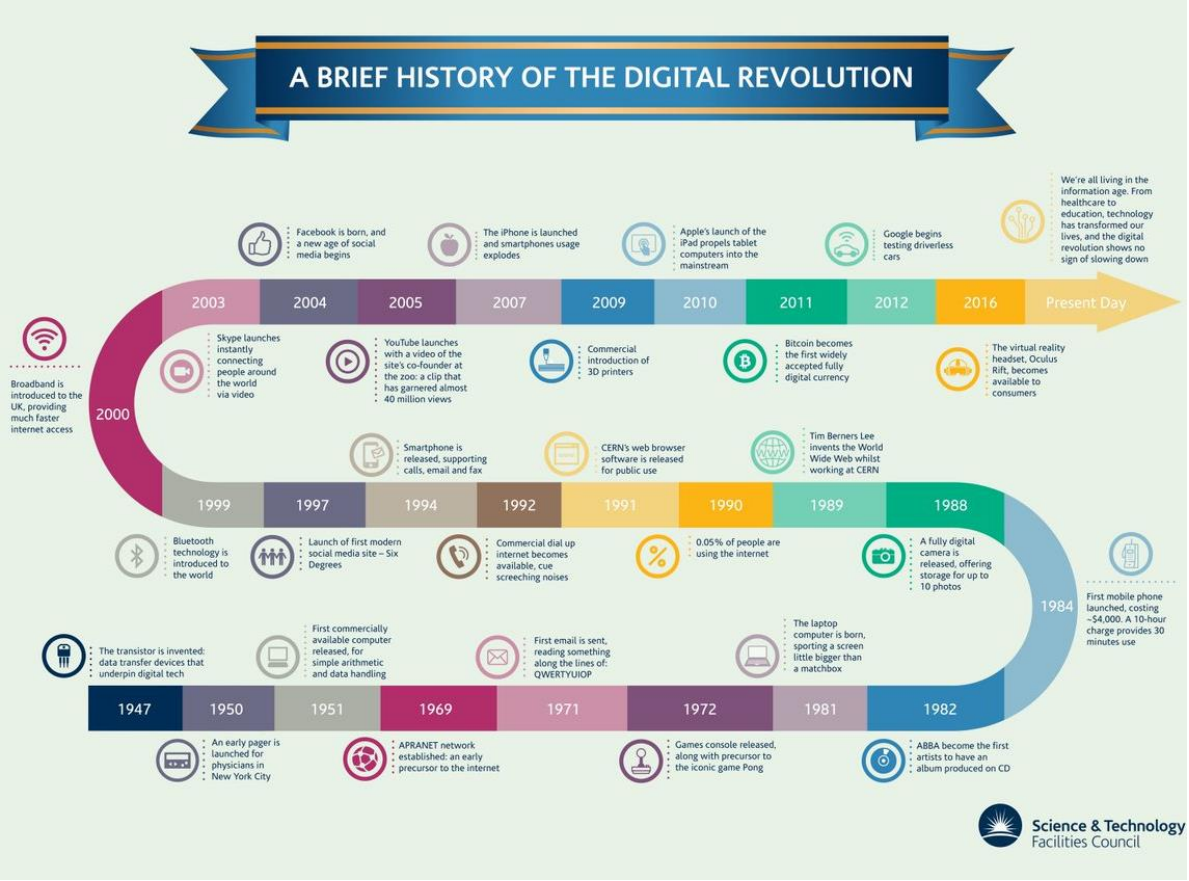
[1] Izvor: https://economictimes.indiatimes.com/blogs/et-commentary/changing-in-a-world-of-digital-revolution/ (10.08.2019.)



Slika 1 – Četiri industrijske revolucije

Izvor: https://blog.innovxminds.com/2019/01/02/timeline-of-industrial-revolution/ (10.08.2019.)

Razvoj digitalne tehnologije obilježili su događaji poput izuma prvog tranzistora 1947. i prvog računala 1951., mobilnog telefona 1984., digitalne kamere 1988., pojave World Wide Weba 1989., pametnog telefona 1994., bluetooth tehnologije 1999., pa sve do Facebooka 2004. i iPhonea 2007. godine. Danas se npr. susrećemo s Bitcoinima i virtualnom realnošću, te svjedočimo kontinuiranom digitalnom razvoju i tehnološkim novitetima. Detaljan povijesni pregled digitalne tehnologije, odnosno revolucije vidljiv je na Slici 2.



Slika 2 – Povijesni pregled digitalne revolucije

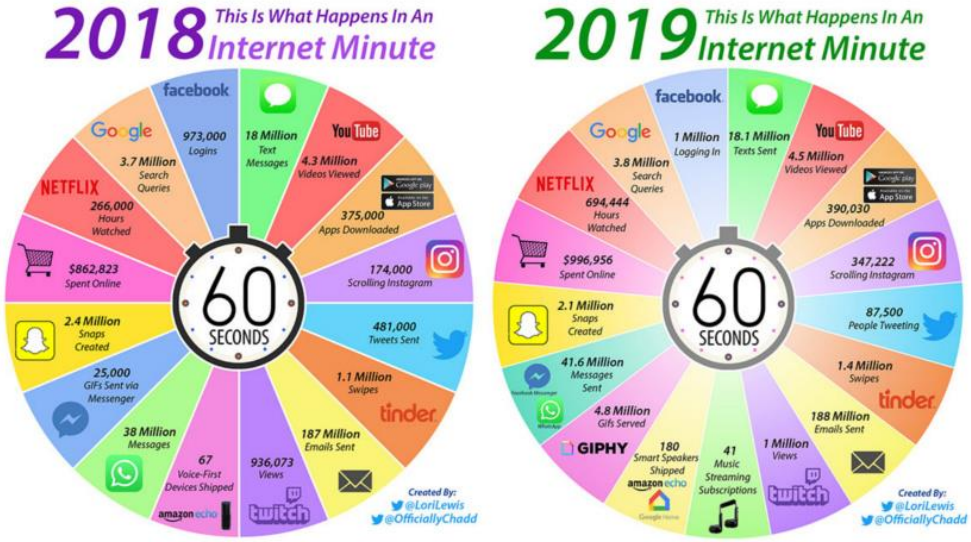
Izvor: https://stfc.ukri.org/news-events-and-publications/features/rise-of-the-machines/ (10.08.2019.)

2.2. Važnost i utjecaj digitalne tehnologije

Upotreba digitalne tehnologije neizostavan je dio današnjeg života. Ona pruža 1. socijalnu povezanost, 2. brzo i jednostavnu komunikaciju i prenošenje informacija, 3. mobilnost zaposlenicima, npr. rad kod kuće, 4. mogućnost učenja i obrazovanja, pogotovo nepokretnim osobama, 5. automatizaciju u industriji ali i kućanstvu, 6. pohranu velikih količina podataka, 7. lakše i jeftinije uređivanje tekstova, videa, fotografija i sl., 8. lako kopiranje i razmjena podataka, kao i 3D printanje, 9. GPS i online mape, 10. brža putovanja s digitaliziranim prometnim sustavom, 11. jeftinije ili besplatne usluge poput oglašavanja na Instagramu, 12. različite vrste zabava, od gledanja filmova i serija na Netflixu do igranja online igrica, 13. dostupnost vijestima, 14. ratovanje izdaleka s manjim brojem žrtava, 15. brže bankovne usluge, te 16. male i praktične uređaje.[2]

[2] Izvor: https://turbofuture.com/computers/Advantages-of-Digital-Technology (10.08.2019.)

Internet je dinamično mjesto, gdje se stalno javljaju novi zanimljivi sadržaji, ali gdje i oni stariji gube na popularnosti. Koliko je velik utjecaj i konstantan rast digitalizacije može se uočiti usporedbom korištenja Interneta 2018. i 2019. godine na Slici 3.



Slika 3 – Jedna minuta na Internetu

Izvor: https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/ (10.08.2019.)

2.3. Digitalna kultura

Bushati i Lezha (2017) navode „pojam *digitalna kultura* označava suvremenu fazu komunikacijskih tehnologija, onu koja prati kulturu tiska 19. stoljeća i elektroničku kulturu emitiranja 20. stoljeća, a koja je naglašena i ubrzana popularnošću umreženih računala, personaliziranih tehnologija i digitalnih slika. Nastanak digitalne kulture obično je povezan sa skupom praksi utemeljenih na sve intenzivnijoj upotrebi komunikacijskih tehnologija. Točnije, digitalna kultura izražava prije svega promjene koje su nastale pojavom digitalnih, umreženih i personaliziranih medija u našem društvu, te prelazak iz faza komunikacije usredotočene na tiskane i emitirane medije, na personaliziranije i umreženije medije koji koriste digitalno komprimiranje i kapacitete za obradu u svojoj srži. Posljedice takvih procesa preko kojih medijske tehnologije transformiraju naše načine interakcije društvenom smislu, su ono što nazivamo *digitalnom kulturom*. Također slični izrazi koji se često koriste su *cyber kultura, računalna kultura ili internetska kultura*.“ Gilles Deleuze (1977), navedeno u Bushati i Lezha (2017), tvrdi: „Stroj je uvijek društven prije nego što je tehnički. Uvijek postoji društveni stroj koji bira ili dodjeljuje korištene tehničke elemente.“

3. KRIMINALITET U KIBERNETIČKOM PROSTORU

Dragičević (2005), kako je navedeno u radu Protrka (2018), objašnjava da „suvremeno društvo uvelike ovisi o neometanom funkcioniranju informacijskih i komunikacijskih sustava uz pomoć kojih se upravlja svim bitnim sustavima kao što su policija, vojska, promet, opskrba i druge službe, kao i kritična nacionalna infrastruktura, te uobičajena dnevna komunikacija. Kako se svi ti sustavi međusobno sve više povezuju, tako postoji i sve veća opasnost napada na takve sustave. Široka dostupnost tehnologije omogućuje sve veću automatizaciju napada i korištenja sofisticiranih alata za napade. Razvoj informacijsko-komunikacijske tehnologije, uz sve svoje pozitivne strane, nažalost ima i svoju negativnu stranu - kibernetički kriminal, odnosno kiberkriminal."

3.1. Pojam kriminaliteta u kibernetičkom prostoru

Dvije definicije kriminaliteta u kibernatičkom prostoru su:

1) „Kibernetički kriminal je općeniti pojam kojim se označavaju sva kriminalna djela u kojima je kao cilj ili sredstvo bilo uključeno računalo ili računalna mreža, dok valja istaknuti kako se računalni kriminal smatra dijelom kibernetičkog kriminala. U prvu kategoriju uključena su kaznena djela u kojima je računalo objekt kriminala, kada je kriminal bio povezan sa samim računalima (poput krađe računala ili njegovih komponenti ili uništenje računala i slično). Druga kategorija opisuje računalo kao cilj, odnosno "subjekt" kriminala, kada računalo predstavlja okolinu u kojoj je kriminal počinjen (poput krađe podataka, provale u računalo i slično). U treću kategoriju uvrštena su kaznena djela u kojima je računalo alat ili instrument za izvođenje ili planiranje kriminala (kada se npr. računalo koristi za provalu u drugo računalo). Četvrta kategorija opisuje sva kaznena djela u kojima se računalo slučajno pojavljuje u drugima kriminalnim djelima ili se jednostavno koristi kao simbol za zastrašivanje (poput pedofilije, pranja novca i slično)." (Bača, 2004, navedeno u Protrka, 2018)

2) „Ukupnost kaznenih djela koja su kroz određeno vrijeme počinjena unutar kibernetičkog prostora ili uz njegovu pomoć korištenjem ili zlorabljenjem resursa ili servisa kibernetičkog prostora ili usluga uz pomoć informacijskih tehnologija koje čine njegovu infrastrukturu. Kako do danas ne postoji opće prihvaćena definicija pojma, tako je bitno naglasiti da termin cyber, kao prvi element riječi, u većini rječnika označava nešto vezano uz svijet prividne stvarnosti koji nastaje uporabom računala." (Dragičević, 2004, navedeno u Protrka, 2018)

3.1.1. Digitalna forenzika

Prasanthi et al. (2017) objašnjavaju pojam digitalne forenzike koji je usko povezan s kriminalitetom u kibernetičkom prostoru: „digitalna forenzika je ogromno je područje forenzičke znanosti koja uključuje istraživanje cyber napada podataka koji se pohranjuju u elektroničkom obliku“. Nadalje pojašnjavaju: „Internet iz dana u dan raste, a eksplozija tehnologije zahtijeva veliko spremanje podataka i informacija. Svaki pojedinac posjeduje pametne telefone i računala, te su kao takvi pod udarom osoba s lažnim identitetom što dovodi do dramatičnog porasta cyber zločina. Digitalna forenzika i cyber forenzika velika su područja za istraživanje takvih zločina koji uključuju hakiranje, bankarske prevare, neželjenu poštu putem e-pošte itd.“ (Prasanthi et al., 2017)

3.2. Pravna regulativa kriminaliteta u kibernetičkom prostoru Republike Hrvatske

Prema Protrka (2018) iako sve razvijene zemlje prate suvremene pravne tokove koji se odnose na kiberkriminal, brzina kojom se ta vrsta kriminala razvija je ponekad ispred zakonskih rješenja. Republika Hrvatska je Kaznenim zakonom iz 2011. godine, uvela sveobuhvatnu Glavu zakona posvećenu *kaznenim djelima protiv računalnih sustava, programa i podataka* (Protrka, 2018). Protrka (2018) nadalje objašnjava da Kazneni zakon propisuje sljedeća kaznena djela koja tvore računalni kriminalitet: neovlašteni pristup (članak 266.), ometanje rada računalnog sustava (članak 267.), oštećenje računalnih podataka (članak 268.), neovlašteno presretanje računalnih podataka (članak 269.), računalno krivotvorenje (članak 270.), računalna prijevara (članak 271.), zloporaba naprava (članak 272.), teška kaznena djela protiv računalnih sustava, programa i podataka (članak 273.).

3.2.1. Ostala dodirna kaznena djela

Prema Protrka (2018) „postoje i druga kaznena djela u čijem se opisu spominje računalo kao sredstvo napada ili objekt napada. Takvih kaznenih djela u postojećem Kaznenom zakonu ima nekoliko, a u budućnosti se može očekivati sve više. U skupinu kaznenih djela protiv privatnosti ulazi i kazneno djelo nedozvoljene uporabe osobnih podataka. Iz perspektive Ministarstva unutarnjih poslova, djelatnici policije su korisnici sigurno najveće zbirke osobnih podataka u Republici Hrvatskoj. Sukladno ovlastima i potrebama, svaki djelatnik je osobno odgovoran za etičko korištenje povjerene mu ovlasti korištenja osobnih podataka u službenim evidencijama. U posljednje vrijeme svjedoci smo

događanja mnogih društvenih pojava koje u širokom spektru prikupljaju osobne podatke. Jedno od kaznenih djela koje na nedozvoljen način prikuplja naše osobne podatke naziva se phishing, ili mrežna krađa identiteta.“

3.2.1.1. Kaznena djela protiv časti i ugleda

„Kod kaznenih djela protiv časti i ugleda postoje sljedeća kaznena djela: uvreda, sramoćenje i kleveta. Čast se može definirati kao subjektivno pravo svakog čovjeka na osobni osjećaj vrijednosti, a ugled je pravo na priznanje te vrijednosti od strane drugih pripadnika zajednice. Preuzimanje odgovornosti za javno izrečeno i napisano korištenjem foruma i društvenih mreža, te ostavljanje komentara na portalima donosi sa sobom i razinu odgovornosti budući da su uvrede, sramoćenje i klevete putem računalnog sustava ili mreže tretirane kao kazneno djela za koje su predviđene novčane kazne.“ (Protrka, 2018)

3.2.1.2. Kaznena djela spolnog zlostavljanja i iskorištavanja djeteta

Protrka (2018) navodi da gledanje sadržaja koji prikazuju seksualno zlostavljanje djece na internetu, spremanje istih u memoriju računala ili na bilo koji drugi medij za pohranu podataka, predstavlja radnju kaznenog djela. U ovu vrstu kaznenih djela spada iskorištavanje djece za pornografiju, iskorištavanje djece za pornografske predstave, te upoznavanje djece s pornografijom (Protrka, 2018).

3.2.1.3. Kaznena djela protiv intelektualnog vlasništva

Sukladno Zakonu o autorskom i srodnim pravima, autorska prava sadržavaju imovinska prava, koja obuhvaćaju: pravo reproduciranja (pravo umnožavanja), pravo distribucije (pravo stavljanja u promet), pravo priopćavanja autorskog djela javnosti, pravo prerade (Protrka, 2018). Slijedom toga, kaznena djela iz ove domene su povreda osobnih prava autora ili umjetnika izvođača (softversko piratstvo) i nedozvoljena uporaba autorskog djela (Protrka, 2018).

3.2.1.4. Kaznena djela protiv javnog reda

Kaznena djela protiv javnog reda u globalnosti karakterizira heterogenost, napadaju se različiti društveni odnosi, a tu spada i kazneno djelo javnog poticanja na nasilje i mržnju (Protrka, 2018).

3.3. Nedozvoljena ponašanja u kibernetičkom prostoru

„U većini slučajeva kibernetičkog kriminaliteta počinjenje kaznenih djela se odvija u više zemalja, što zahtijeva niz koordiniranih operacija od strane većeg broja međunarodnih tijela koja su nadležna i kompetentna za rješavanje, odnosno realizaciju operacija u svrhu zaustavljanja počinjenja i hvatanja počinitelja kaznenih djela u domeni kibernetičkog kriminaliteta.“ (Hughes, 2010, navedeno u Protrka, 2018)

Kuehl (2009), navedeno u radu Protrka (2018), tvrdi: „treba priznati da zakonodavstvo kasni s prepoznavanjem i definiranjem novih vrsta kaznenih djela počinjenih preko računalne mreže i računalnih sustava, a ni policija još uvijek ne reagira adekvatno na ubrzani tehnološki razvoj, što za posljedicu ima veliki broj kaznenih djela koja nisu zakonski definirana ili su u tamnoj brojci jer ih policija i državno odvjetništvo ne prepoznaju kao kaznena djela ili se uopće ne bave razrješavanjem takvih kaznenih djela.“

3.3.1. Hakiranje

Prema autorima Larry i Lars (2012), citiranih u Protrka (2018), hakiranje je objašnjeno na sljedeći način: „kada jedna osoba koristi identitet druge osobe kako bi na taj način pristupila računalnoj infrastrukturi, govorimo o lažnom predstavljanju ili maskiranju. Sigurnosne metode koje koriste sustavi zaštite računalne infrastrukture moraju biti dovoljno aktivne kako bi otkrili i spriječili lažno predstavljanje. Kada se govori o lažnom predstavljanju, moramo razlikovati fizičku i elektroničku formu lažnog predstavljanja. O fizičkom predstavljanju govorimo kada počinitelj koristi ovlašteni korisnički identitet ili pristupnu karticu kako bi pristupio povjerljivim područjima i stekao pristup računalnoj infrastrukturi i podacima. Za lažno predstavljanje kažemo da je elektroničko kada počinitelj, u stvari, koristi legalni korisnički identifikacijski broj ili zaporku kako bi se prijavio u računalni sustav te na taj način nelegalno došao u posjed podataka i informacija.“

3.3.2. Računalna sabotaža

Protrka (2018) navodi da „računalni podaci u današnje vrijeme predstavljaju iznimno vrijednu imovinu i često se ogodi slučaj u praksi, a pogotovo u IT sektoru, da je vrijednost računalnih podataka mnogo veća nego u fizičkom obliku. Za primjer možemo navesti poredbu da vrijednost programa, aplikacije ili izvornog koda može biti veća od zgrade u kojoj se ti podaci nalaze. Još 2013. godine analitičari su predviđali porast vrijednosti internetskih društvenih mrežnih stranica kao novi način financijskog bogaćenja.“

3.3.3. Sabotaža računalnih sustava i podataka

Dokazne radnje kojima se može ustanoviti sabotaža računalnih sustava ovise primarno o korištenom softveru i hardveru, te mjestu u arhitekturi računalnog sustava gdje se ometanje događa (Protrka, 2018). Potrebno je ustanoviti koja funkcija računalnog sustava je ometana i na koji način, koji je uzrok ometanja te tko je prouzročio ometanje (Protrka, 2018).

S druge strane, po Protrka (2018) možda još i teže ustanovljiva situacija, je oštećenje računalnih podataka koja zahtijeva otkrivanje promjena na podacima. Protrka (2018) navodi da tom smislu istraživanje mora otkriti je li se dogodila promjena na podacima, na koji se način dogodila, te tko ju je uzrokovao i s kojom namjerom.

3.3.4. Računalna špijunaža

Protrka (2018) objašnjava: „istraživanja kojima je moguće ustanoviti neovlašteno presretanje računalnih podataka su izuzetno kompleksna, što je razlog da se vrlo teško može ustanoviti situacija presretanja podataka. U najvećem dijelu slučajeva radi se o otkrivanju kopija podataka dobivenih presretanjem, a radnje na osnovu tih pronađenih podataka moraju dokazati da je došlo do presretanja podataka. Uz same kopije podataka mogu se pronaći i alati tzv. napadački alati. Postojanje alata nije jednoznačan dokaz budući su vrlo često u uporabi kao pomoćna sredstva za administraciju računalnih sustava, pogotovo bežičnih računalnih mreža.“

3.3.5. Računalno piratstvo

„Piratstvo programske podrške predstavlja neovlašteno kopiranje i distribuiranje programa koji su zakonski zaštićeni od kopiranja. Sam čin piratizacije programske podrške moguće je promatrati sa aspekta omogućavanja korištenja i kopiranja nelegalne programske podrške svjesnim kopiranjem zaštićene programske podrške i njezinim distribuiranjem, te sa aspekta instaliranja prethodno piratizirane programske podrške na računalo. Piratizacija programske podrške može se izvesti na nekoliko načina od kojih su najčešći: kopiranje krajnjeg korisnika, kloniranje tvrdog diska, *skidanje* softvera s interneta, slanje putem elektroničke pošte, krivotvorina, korištenje programske podrške sa poslužitelja, kopiranje posuđene programske podrške.“ (Protrka, 2018)

3.3.6. Računalna prijevara

O ovom nedozvoljenom kibernetičkom ponašanju Protrka (2018) piše: „računalna prijevara obuhvaća razne vrste manipulacija na podacima, a najčešće financijskim. Do takvih manipulacija može doći tijekom unosa, obrade, pohranjivanja, distribucije podataka i informacija, kao i pri razmjeni podataka unutar računalne mreže ili putem telefonskih i drugih komunikacijskih kanala. Pri tome se podaci mogu nalaziti na bilo kojem digitalnom mediju.“

3.3.7. Zloporaba naprava

Prema Protrki (2018) za počinjenje kaznenih djela računalnog kriminalitet potreban je ili određeni hardver ili određeni softver ili spoj hardvera i softvera, odnosno računalna oprema.

3.4. Nacionalna strategija kibernetičke sigurnosti

„Spoznajom o pojavljivanju nove kibernetičke dimenzije društva, kao i pojave novih prijetnji za fizičke i pravne osobe te javna i državna tijela, Vlada Republike Hrvatske uvidjela je potrebu za donošenjem Nacionalne strategije kibernetičke sigurnosti, a sve u cilju zaštite kibernetičkog prostora. To je sveobuhvatna strategija zaštite kibernetičkog prostora koja je obuhvatila sve zakonske i podzakonske akte, kao i sve segmente društva nužne za provođenje sigurnosti na kibernetičkom planu. Kao opće ciljeve strategije postavljeni su: sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog

okvira; provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora; uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima; jačanje svijesti o sigurnosti kibernetičkog prostora; poticanje razvoja usklađenih obrazovnih programa; poticanje razvoja e-usluga; poticanje istraživanja i razvoja rada akademskog, gospodarskog i javnog sektora; sustavni pristup međunarodnoj suradnji. Za ostvarivanje kibernetičke sigurnosti postavljeni su specifični ciljevi za svaku od sljedećih poveznica: zaštita podataka, tehnička koordinacija u obradi računalnih sigurnosnih incidenata, međunarodna suradnja, te obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru.“ (Protrka, 2018)

Posebno je važna zaštita podataka, a Sinčić (2018) u svom radu objašnjava: „GDPR (General Data Protection Regulation) je Opća uredba o zaštiti podataka koja se primjenjuje od 25. svibnja 2018. godine. Omogućuje građanima Europske unije da bolje kontroliraju svoje osobne podatke. Pod osobne podatke se smatraju svi podaci koji se odnose na osobu koja se može izravno ili neizravno identificirati. Ova definicija omogućuje širok raspon osobnih identifikatora uključujući ime, identifikacijski broj, podatke o lokaciji ili on-line identifikator, što odražava promjene u tehnologiji i na način na koji organizacije prikupljaju informacije o ljudima. Također modernizira i ujedinjuje pravila koja omogućuju tvrtkama smanjenje birokracije i pridonosi većem povjerenju potrošača. Opća uredba o zaštiti podataka dio je paketa EU za reformu podataka, zajedno s direktivom o zaštiti podataka za policijske i kriminalističke vlasti.“

3.4.1. Statistički podaci o kibernetičkom kriminalu u Republici Hrvatskoj

Na stranicama Ministarstva unutarnjih poslova dostupni su statistički podaci s obzirom na vrstu kriminala. Slika 4 prikazuje usporedni prikaz kaznenih djela kibernetičkog kriminala iz 2017. i 2018. godine, te se može zaključiti kako je većina ove vrsta kriminala u porastu u Republici Hrvatskoj.

Kaznena djela	Prijavljena			Razriješena			Naknadno otkrivena		
	Broj djela		+ - %	Broj djela		+ - %	Broj djela		+ - %
	2017.	**2018.**		2017.	**2018.**		2017.	**2018.**	
Iskorištavanje djece za pornografiju	140	**55**	-60,7	139	**55**	-60,4	103	**40**	-61,2
Krivotvorenje lijekova i medicinskih proizvoda	2	**2**	0,0	2	**2**	0,0	2	**2**	0,0
Neovlašteni pristup	7	**16**	+128,6	5	**13**	+160,0	3	**12**	+300,0
Ometanje rada računalnog sustava	11	**1**	-90,9	10	**1**	-90,0	9		
Oštećenje računalnih podataka	7			7			1		
Neovlašteno presretanje računalnih podataka	1								
Računalno krivotvorenje	37	**32**	-13,5	35	**39**	+11,4	35	**37**	+5,7
Računalna prijevara	1.114	**1.310**	+17,6	915	**1.162**	+27,0	901	**1.144**	+27,0
Zlouporaba naprava	9	**17**	+88,9	7	**17**	+142,9	5	**16**	+220,0
Nedozvoljena uporaba autorskog djela ili izvedbe umjetnika izvođača	2	**1**	-50,0	2	**1**	-50,0	2	**1**	-50,0
Povreda žiga	80	**130**	+62,5	80	**130**	+62,5	78	**90**	+15,4
UKUPNO	**1.410**	**1.564**	+10,9	**1.202**	**1.420**	+18,1	**1.139**	**1.342**	+17,8

Slika 4 – Usporedni prikaz kaznenih djela kibernetičkog kriminala

Izvor:

https://mup.gov.hr/UserDocsImages/statistika/2018/Statisticki%20pregled%20temeljnih%20sigurnosnih%20pokazatelja%20i%20rezultata%20rada%20u%202018.%20godini.pdf (10.08.2019.)

Kada se uzmu u obzir sve vrste komunikacijskih tehnologija, što uključuje društvene mreže, aplikacije za razmjenu digitalnih sadržaja, mrežne usluge, SMS i MMS, te Darknet, dolazi se do puno većeg broja kaznenih djela, kao što je prikazano na Slici 5.

Članak/ /Glava KZ-a	Naziv kaznenog djela	UKUPNO KAZNENIH DJELA	UKUPNO kaznenih djela korištenjem komunikacijskih tehnologija	Društvene mreže	Aplikacije za razmjenu digitalnih sadržaja	Mrežna usluga (online)	SMS i MMS	DARKNET
IX.	**Kaznena djela protiv čovječnosti i ljudskog dostojanstva**	**45**	1	1				
106.	Trgovanje ljudima	**12**	1	1				
XIII.	**Kaznena djela protiv osobne slobode**	**4.260**	122	32	20	3	67	
138.	Prisila	**5**	1	1				
139.	Prijetnja	**3.868**	93	26	18	3	46	
140.	Nametljivo ponašanje	**333**	28	5	2		21	
XIV.	**Kaznena djela protiv privatnosti**	**298**	15	13	2			
144.	Neovlašteno slikovno snimanje	**14**	1		1			
146.	Nedozvoljena uporaba osobnih podataka	**228**	14	13	1			
XVI.	**Kaznena djela protiv spolne slobode**	**321**	15	13	1		1	
156.	Spolno uznemiravanje	**49**	4	2	1		1	
157.	Prostitucija	**28**	11	11				
XXVII.	**Kaznena djela spolnog zlostavljanja i iskorištavanja djeteta**	**543**	121	100	7	2	12	
158.	Spolna zlouporaba djeteta mlađeg od petnaest godina	**232**	4	3			1	
160.	Zadovoljenje pohote pred djetetom mlađim od petnaest godina	**48**	10	7	1		2	
161.	Mamljenje djece za zadovoljenje spolnih potreba	**14**	6	3	1		2	
163.	Iskorištavanje djece za pornografiju	**120**	48	41	4	1	2	
164.	Iskorištavanje djece za pornografske predstave	**4**	4	4				
165.	Upoznavanje djece s pornografijom	**107**	49	42	1	1	5	
XVIII.	**Kaznena djela protiv braka, obitelji i djece**	**2.340**	5	1	1	1	2	
177.	Povreda djetetovih prava	**1.096**	2				2	
178.	Povreda privatnosti djeteta	**17**	3	1	1	1		
XIX.	**Kaznena djela protiv zdravlja ljudi**	**2.279**	4					4
190.	Neovlaštena proizvodnja i promet drogama	**1.880**	4					4
XXIII.	**Kaznena djela protiv imovine**	**27.997**	**45**	**16**	**13**	**12**	**4**	
236.	Prijevara	**1.677**	35	14	9	11	1	
243.	Iznuda	**181**	10	2	4	1	3	
XXV.	**Kaznena djela protiv računalnih sustava, programa i podataka**	**1.376**	26	5	2	16	3	
266.	Neovlašteni pristup	**16**	4	3		1		
267.	Ometanje rada računalnog sustava	**1**	1			1		
271.	Računalna prijevara	**1.310**	20	2	1	14	3	
272.	Zlouporaba naprava	**17**	1		1			
XXIX.	**Kaznena djela protiv pravosuđa**	**216**	1	1				
306.	Sprječavanje dokazivanja	**19**	1	1				
XXX.	**Kaznena djela protiv javnog reda**	**1.596**	7	6		1		
325.	Javno poticanje na nasilje i mržnju	**19**	7	6		1		
UKUPNO		**51.287**	**362**	**188**	**46**	**35**	**89**	**4**

Slika 5 – Kaznena djela počinjena putem komunikacijske tehnologije

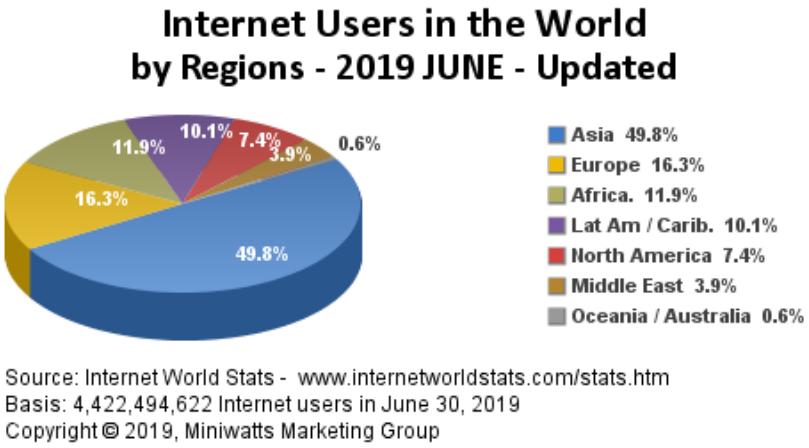
Izvor:

https://mup.gov.hr/UserDocsImages/statistika/2018/Statisticki%20pregled%20temeljnih%20sigurnosnih%20pokazatelja%20i%20rezultata%20rada%20u%202018.%20godini.pdf (10.08.2019.)

4. PRIMJERI PRIJEVARA PUTEM DIGITALNE TEHNOLOGIJE

„Činjenica koja se ne može osporiti je da za Internetom konstantno raste zaluđenost. Svaki dan novi korisnici po prvi put usvajaju Internet. Globalna internetska populacija (od 2012.) predstavlja nešto više od 2,4 milijarde ljudi u odnosu na 360 milijuna krajem 2000. Paralelno s ovim rastom korisnika, sadržaj na Internetu se također proširuje svake minute. Nažalost, uz svaki popularni fenomen dolazi i do povećanja njegovog iskorištavanja." (Lötter et al., 2014)

Danas je broj korisnika naravno još veći, i broji oko 4.5 milijarde ljudi, kao što pokazuje Slika 6, dok su najčešće prijevare s kojima se korisnici digitalne tehnologije susreću prikazani na Slici 7.



Slika 6 – Globalna internetska populacija

Izvor: https://internetworldstats.com/stats.htm (10.08.2019.)

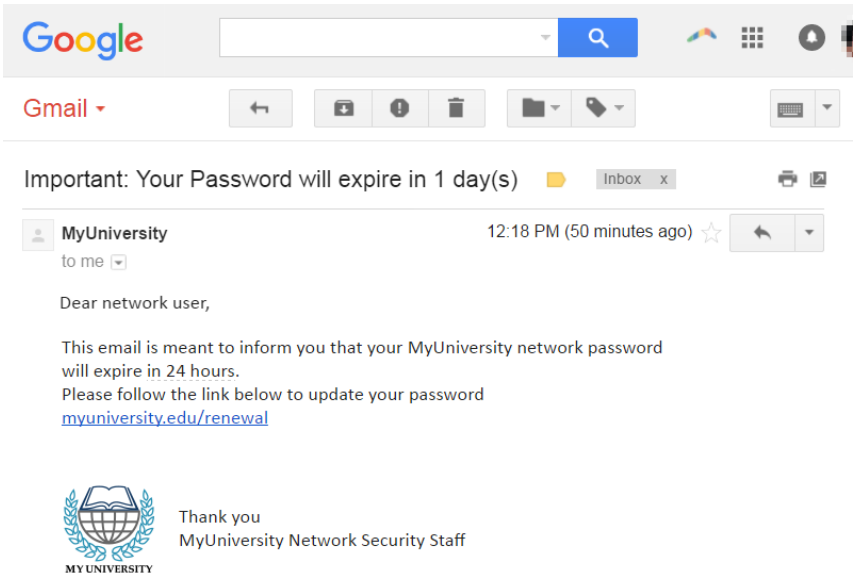
Slika 7 – Najčešće Internet prijevare

Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)

4.1. Prijevare s osobnim podacima

Phishing je vrsta društvenog napada koji se često koristi za krađu podataka o korisnicima, uključujući lozinke za prijavu i brojeve kreditnih kartica. To se događa kada napadač, koji se maskira kao povjerljiv subjekt, obmanjuje žrtvu u otvaranju e-pošte, instant poruke ili SMS poruke. Tada se primatelj upućuje na klik zloćudne veze, što može dovesti do instalacije zlonamjernog softvera, zamrzavanja sustava ili otkrivanja povjerljivih podataka. Napad može rezultirati neovlaštenom kupovinom, krađom sredstava ili krađom cijelog identiteta, te takvi napadi mogu biti i veći, na korporacije ili vlade.[3]

Na Slici 8 primjer je *phishing* napada, gdje su napadači koristili legitimnu instituciju, tj. sveučilište kako bi doveli žrtvu do ažuriranja ili samo provjere podataka.

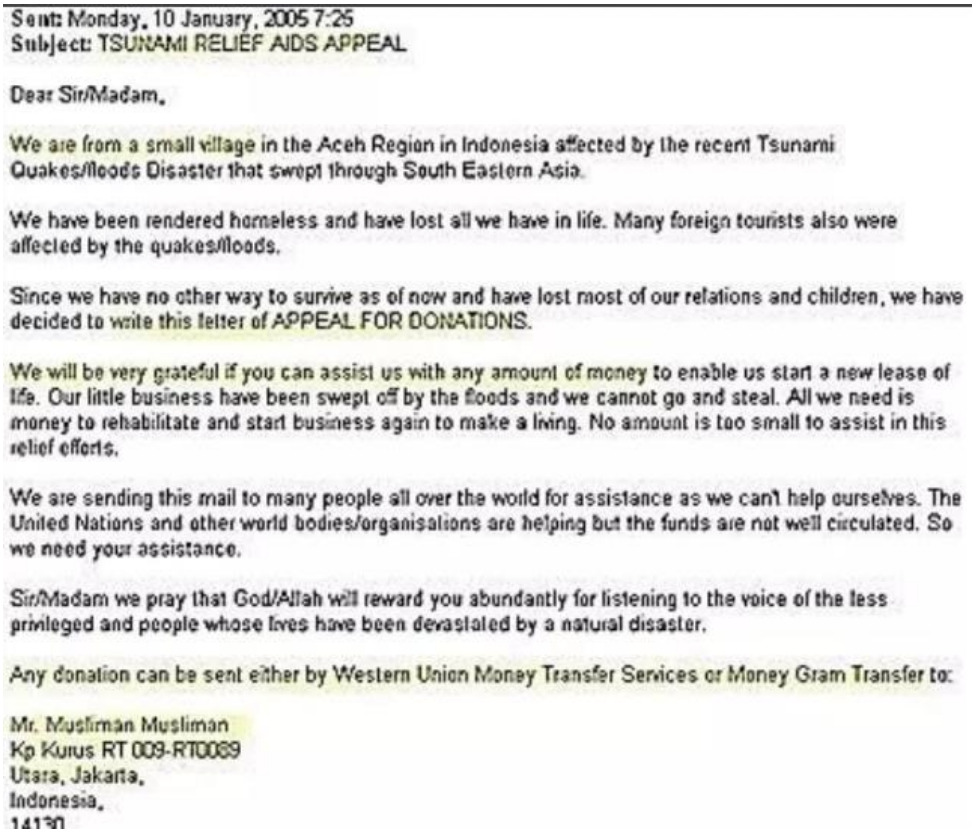


Slika 8 – *Phishing* napad: lažno sveučilište

Izvor: https://www.imperva.com/learn/application-security/phishing-attack-scam/ (10.08.2019.)

Postoji mnogo različitih primjera za ovakve vrste napada, a jedan od njih je i krađa novčanih sredstava putem lažnih dobrovoljnih udruga, pogotovo u slučaju neke katastrofe. Slika 9 je e-poruka takve organizacije.

[3] Izvor: https://www.imperva.com/learn/application-security/phishing-attack-scam/ (10.08.2019.)



Sent: Monday, 10 January, 2005 7:25
Subject: TSUNAMI RELIEF AIDS APPEAL

Dear Sir/Madam,

We are from a small village in the Aceh Region in Indonesia affected by the recent Tsunami Quakes/floods Disaster that swept through South Eastern Asia.

We have been rendered homeless and have lost all we have in life. Many foreign tourists also were affected by the quakes/floods.

Since we have no other way to survive as of now and have lost most of our relations and children, we have decided to write this letter of APPEAL FOR DONATIONS.

We will be very grateful if you can assist us with any amount of money to enable us start a new lease of life. Our little business have been swept off by the floods and we cannot go and steal. All we need is money to rehabilitate and start business again to make a living. No amount is too small to assist in this relief efforts.

We are sending this mail to many people all over the world for assistance as we can't help ourselves. The United Nations and other world bodies/organisations are helping but the funds are not well circulated. So we need your assistance.

Sir/Madam we pray that God/Allah will reward you abundantly for listening to the voice of the less privileged and people whose lives have been devastated by a natural disaster.

Any donation can be sent either by Western Union Money Transfer Services or Money Gram Transfer to:

Mr. Muslimah Muslimah
Kp Kurus RT 009-RT0089
Utara, Jakarta,
Indonesia,
14130

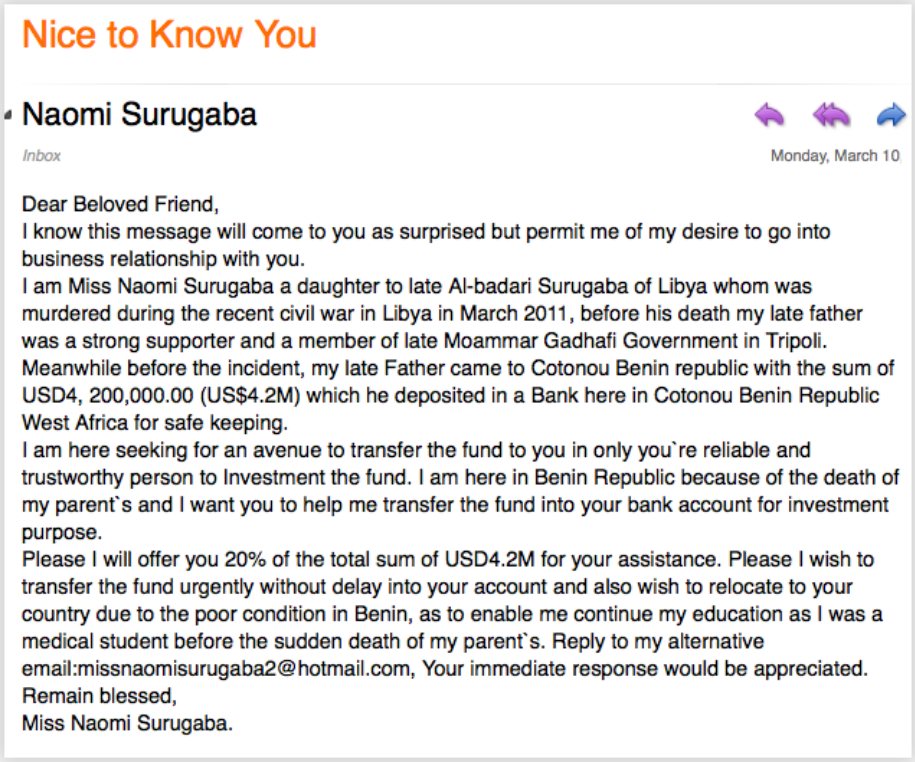
Slika 9 – *Phishing* napad: lažna dobrotvorna organizacija

Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)

4.2. Nigerijske prijevare

Isacenkova et al. (2014) objašnjavaju: „Nigerijska prijevara, koja se u nigerijskom kaznenom zakonu naziva i *419 prijevara*, poznati je problem već nekoliko desetljeća. Naziv obuhvaća mnogo varijacija, poput prijevare s unaprijed plaćenim naknadama, lažne lutrije, prijevare s crnim novcem itd. Prijevara se temelji na tome da prevarant zatraži određeni iznos novca pod obećanjima buduće, veće isplate. Progon takvih zločinačkih aktivnosti složen je i zločinci ga često mogu izbjeći. Kao rezultat toga, izvještaji o takvom zločinu i dalje se pojavljuju na društvenim medijima i mrežnim zajednicama, te npr. stranica 419scam.org postoji kako bi se umanjio rizik i pomoglo korisnicima da prepoznaju prijevare."

U nekim varijacijama, e-poruke kći ili sin ubijenog službenika traže novac od žrtve, primjer čega je Slika 10, a može se dogoditi da prevarant obećava i znatnu količinu novca žrtvi koja je, kako tvrdi, jedini živući nasljednik.



Nice to Know You

Naomi Surugaba

Inbox

Monday, March 10

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

Slika 10 – *Phishing* napad: lažni službenik

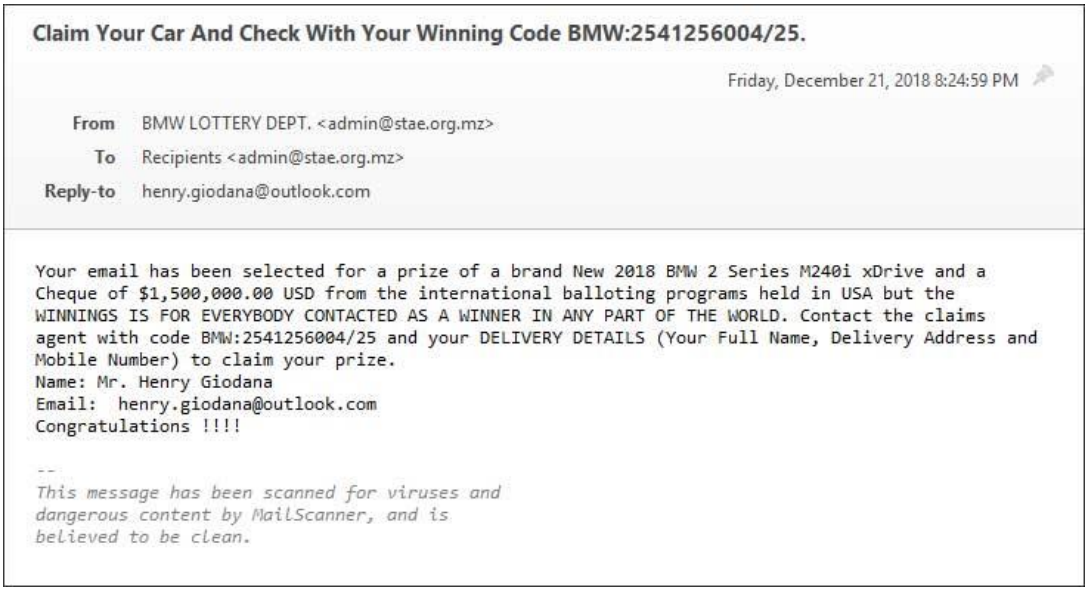
Izvor: yahoo.com: 9 internet scams we're still falling for in 2018 (10.08.2019.)

4.3. Nagradne igre i lutrije

Iako su sve vrste prijevara uglavnom predobre da bi bile istinite, te se poigravaju ljudskim osjećajima i slabostima, osvojiti lutriju je nešto što svaka osoba bar jednom pomisli. Ova prijevara također obično dolazi u obliku uobičajene poruke e-pošte te obavještava da ste osvojili milijune dolara s uzastopnim čestitkama. više puta vam laska čestitkama. Međutim, prije nego što možete pokupiti svoj dobitak, morate platiti naknadu za obradu koja može biti veća od nekoliko tisuća dolara.[4]

Slika 11 je primjer prijevare nagradnom igrom, točnije osvajanje automobila, a još jedna popularna prijevara je i lažno nagradno putovanje.

[4] Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)



Claim Your Car And Check With Your Winning Code BMW:2541256004/25.

Friday, December 21, 2018 8:24:59 PM

From BMW LOTTERY DEPT. <admin@stae.org.mz>
To Recipients <admin@stae.org.mz>
Reply-to henry.giodana@outlook.com

Your email has been selected for a prize of a brand New 2018 BMW 2 Series M240i xDrive and a Cheque of $1,500,000.00 USD from the international balloting programs held in USA but the WINNINGS IS FOR EVERYBODY CONTACTED AS A WINNER IN ANY PART OF THE WORLD. Contact the claims agent with code BMW:2541256004/25 and your DELIVERY DETAILS (Your Full Name, Delivery Address and Mobile Number) to claim your prize.
Name: Mr. Henry Giodana
Email: henry.giodana@outlook.com
Congratulations !!!!

--
This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.

Slika 11 – Prijevara nagradnom igrom

Izvor: https://www.bleepingcomputer.com/news/security/beware-of-bmw-lottery-email-scam-stating-you-won-a-bmw-m240i/ (10.08.2019.)

Također, može se dogoditi i prijevara vezana uz oglas. Prevarant za predmet koji se prodaje, npr. automobil, e-poštom ponudi platiti puno više od tražene cijene, što objašnjava međunarodnim naknadama za otpremu automobila u inozemstvo. Zauzvrat, žrtva mu treba poslati automobil i novac za razliku.[5]

4.4. Prijevare sa zapošljavanjem

Ova prijevara usmjerena je osobama koje su objavile svoj životopis na zakonitom mjestu zapošljavanja, s barem nekim osobnim podacima kojima bi mogli pristupiti potencijalni poslodavci. Zatim se može dobiti ponuda za posao, npr. za financijskog predstavnika inozemne tvrtke, a koja ima problema s prihvaćanjem novca od određenih kupaca i potrebna im je osoba za upravljanje tim plaćanjima. Ta tvrtka će platiti postotak provizije po transakciji, te ako se žrtva prijavi, tj. pošalje podatake o bankovnom računu kako bi mogla biti plaćena, nasjedne na prijevaru.[6] Slika 12 prikazuje jednu takvu lažnu poslovnu ponudu.

[5] Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)
[6] Ibid.

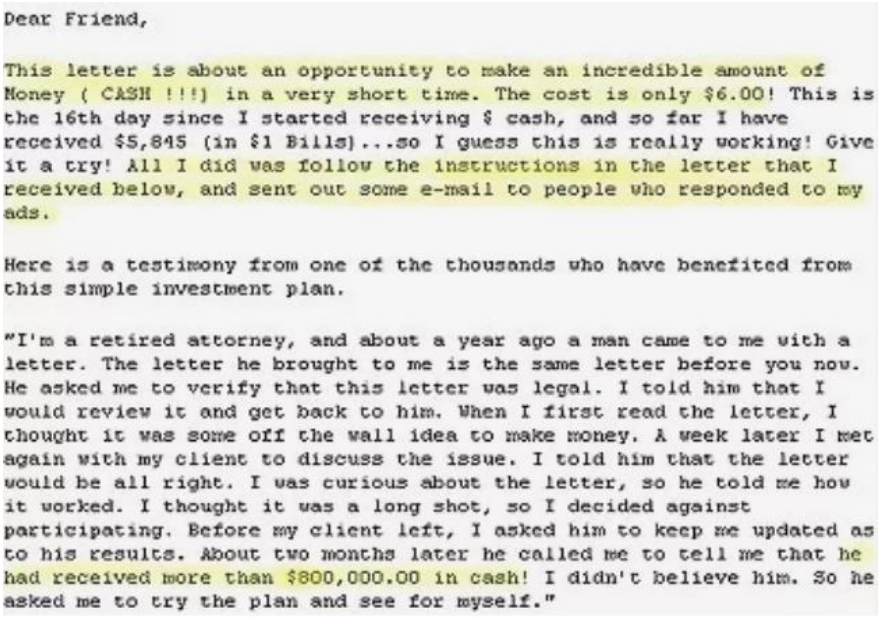
Slika 12 – Lažno zapošljavanje

Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)

Slično tome, mogu nuditi i jednostavan rad od kuće. „Brz put do zaradite puno novca od kuće, a da pritom nemate kvalifikacija, vještina ili stručnosti. Žrtva prije početka bilo kakvog posla mora uplatiti novac unaprijed, za registraciju ili za kupnju robe. Nakon što je taj novac uplaćen žrtva ili utvrdi da nema posla koji obavlja ili neće biti plaćena za napravljeni posao." (Drew, 2011)

Kao jedan oblik lažnog zapošljavanja je i *Multilevel marketing plan* (MLM) ili višerazinski marketinški planovi prodaje robe ili usluga putem distributera. Ti planovi obično obećavaju da ako se prijavite kao distributer, dobijete provizije i za vlastitu prodaju i za one druge koje zaposlite kao distributere. Većina država zabranjuje ovu praksu, koja je poznata i kao piramidalna shema, jer se mogu plaćati provizije za prodaju ali ne i za zapošljavanje budući da to nije osigurano i većina ljudi gubi novac.[7] Slika 13 prikazuje e-poruku, koja je dio *chain-maila*, gdje se nudi brza zarada.

[7] Izvor: https://kb.iu.edu/d/afvn (10.08.2019.)



Dear Friend,

This letter is about an opportunity to make an incredible amount of Money (CASH !!!) in a very short time. The cost is only $6.00! This is the 16th day since I started receiving $ cash, and so far I have received $5,845 (in $1 Bills)...so I guess this is really working! Give it a try! All I did was follow the instructions in the letter that I received below, and sent out some e-mail to people who responded to my ads.

Here is a testimony from one of the thousands who have benefited from this simple investment plan.

"I'm a retired attorney, and about a year ago a man came to me with a letter. The letter he brought to me is the same letter before you now. He asked me to verify that this letter was legal. I told him that I would review it and get back to him. When I first read the letter, I thought it was some off the wall idea to make money. A week later I met again with my client to discuss the issue. I told him that the letter would be all right. I was curious about the letter, so he told me how it worked. I thought it was a long shot, so I decided against participating. Before my client left, I asked him to keep me updated as to his results. About two months later he called me to tell me that he had received more than $800,000.00 in cash! I didn't believe him. So he asked me to try the plan and see for myself."

Slika 13 – Prijevara s brzom zaradom

Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)

4.5. Prijevare lijekovima

Potrošači primaju e-poštu koja obećava čudesno ozdravljenje. Nude se pilule, losioni, kreme i drugi proizvodi koji će navodno izliječiti ćelavost, artritis, reumu, srčane bolesti, multiplu sklerozu, Parkinsonovu bolest, rak, pretilost, impotenciju i sl. Mogu se obećati i sredstva za lako mršavljenje bez potrebe za dijetom ili vježbanjem. Najčešće ponuđeni proizvodi nisu ni pravilno testirani ili dokazano medicinski učinkoviti, pa mogu biti čak i opasni. Oglašavanje često uključuje lažne izjave zadovoljnih kupaca, neosnovane tvrdnje o učinkovitosti proizvoda te da je klinički dokazan, kao i jamstvo vraćanja novca (Drew, 2011)

4.6. Prijevare kreditnim karticama

Prijevare kreditnim karticama se događaju na različite načine, od već navedenog *phishing* do *skimminga*. „Skimming je oblik krivotvorine kod kojeg je magnetni zapis ukraden s jedne originalne kartice uređajem koji se naziva skimmer (engl. to skim= obrati, letimice lagano dotaći, preletjeti očima). Skimmer je mali kompleksni uređaj veličine kutije šibica koji optički čita i pohranjuje podatke s magnetnog zapisa.“ (Jelenski et al., 2013)

Također, postoji i varijanta u kojoj je osobi unaprijed odobren kredit ili kreditna kartica, ali za koje se unaprijed naplaćuje naknada, što zapravo nijedna banka ne radi. Žrtve s novčanim problemima nasjedaju na ovakav oblik prijevare, iako je samo po sebi sumnjivo i kako bi netko uopće znao financijsku situaciju pojedinca toliko dobro.[8] Slika 14 je primjer ovakve lažne ponude.

Slika 14 – Prijevara kreditnim karticama

Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)

4.7. Klik prijevare

Wilbur (2009) objašnjava: „Klik prijevara je praksa lažnog klika na oglase s namjerom povećanja prihoda trećim osobama. Oglašivači su prisiljeni vjerovati da sigurnosni programi otkrivaju i sprečavaju klik prijevare iako se ti programi moraju platiti i za svaki neotkriveni lažni klik."

Primjer za to su poklon kartice ili vaučeri (Slika 15) koje možete dobiti klikom na ponudu, dijeljenjem iste uz pozitivan komentar na Facebooku. Ono što se događa je da prevaranti koji stoje iza toga dobivaju izravan promet na web stranice koje se bave mrežnim anketama, što će im zauzvrat zaraditi partnersku proviziju.[9]

[8] Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)
[9] Izvor: https://www.scam-detector.com/article/free-gift-card (10.08.2019.)

Slika 15 – Klik prijevara: poklon kartice

Izvor: https://www.scam-detector.com/article/free-gift-card (10.08.2019.)

Slično lažnom zapošljavanju, i klik prijevare navode do brze zarade, kao na Slici 16.

Slika 16 – Klik prijevara: brza zarada

Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)

4.8. Lažne recenzije i stranice

Na Internetu postoji mnogo lažnih stranica, vrlo sličnih originalnima. Legitimna URL adresa veze počinje s https://, dok lažni identiteti često imaju samo http://, bez slova s. Također, puno puta URL nije ni u domeni službene web stranice institucije.[10]

[10] Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)

Slacktivizam je izraz koji kombinira riječi *klevetnik* i *aktivizam*, a odnosi se na lažne statuse, informacije i recenzije na društvenim medijima u svrhu promicanja marketinške svijesti.[11]

Goswami et al. (2017) objašnjavaju: „Online recenzije potrošača postale su osnovica za nove potrošače da isprobaju novu marku ili proizvod. One omogućuju brzi uvid u primjenu i iskustvo korištenja. Međutim, neke tvrtke to iskorištavaju za širenje lažnih informacija koje mogu promovirati relativno prosječan proizvod ili utjecati na konkurenciju.“

Slika 17 prikazuje lažne komentare na stranici Amazon. Takvi komentari su uglavnom pisani na isti datum, profesionalnim rječnikom, s prevelikim entuzijazmom, ocijenjuju s 5/5 zvjezdica i slično.

Slika 17 – Lažne recenzije

Izvor: https://www.lenwilson.com/latest-news-nowhere-else-what-to-do-in-lafayette-indiana/2018/09/15/review-that-fake-review-poster-sent-to-jail (10.08.2019.)

[11] Izvor: https://www.techopedia.com/definition/28252/slacktivism (10.08.2019.)

Razvoj marketinga na društvenim platformama povećao je vrijednost preporuka poznanika, a to je dovelo vodeće marke da iskoriste inkluzivnu prirodu Instagrama za zapošljavanje slavnih, poznatih blogera ili influencera, kao prijenosnike marketinške poruke (Thornton, 2018). Jedna od takvih marketing strategija bila je i za Fyre festival 2017, te kako opisuje Burrough (2017), navedeno u Thornton (2018), Fyre je najveća prijevara 2017. godine. „Prvi dan festivala nije ni započeo, a društvene mreže su eksplodirale nezadovoljstvom. Umjesto egzotičnog, ekskluzivnog glazbenog iskustva, festival je opisan kao da se distopija susreće sa histerijom. Luksuzne kabine zamijenili su šatori namjenjeni za katastrofe, a ni oni nisu bili potpuno izgrađeni. Raskošna kuhinja su bili loši sendviči. Uz to, gosti su izgubili prtljagu između prekomjerno rezerviranih letova i nasukani su na nepoznatom otoku. Bio je to prizor neispunjenih, a plaćenih obećanja, od kojih je profitirao glavni i sada osuđeni organizator Billy McFarland. Između osobnih izvještaja o događaju i tužbi koje su izbijale na površinu, novinari su sudjelovali na svojim platformama, optužujući inluencere i slavne osobe za krivo navođenje, malo spominjajući organizatore. Ovaj događaj je skoro uništio kredibilitet influecera i slavnih koji nešto sponzoriraju.“ (Thornton, 2018)

4.9. Digitalno krivotvorenje

„Danas je izmjenjivanje digitalnih slika putem intuitivnog softvera jednostavnost s vrlo niskim troškovima; na taj način svaki pojedinac može sintetizirati lažnu sliku. Na široko dostupnom Internetu, lažne se informacije šire vrlo brzo. Kao posljedica toga, činjenice mogu biti iskrivljene i utjecati na javnost, što dovodi do negativnog društvenog utjecaja. Istina može biti još gora kada se slike prikažu kao dokaz. Zbog toga je velika potražnja za valjanom i učinkovitom metodom provjere autentičnosti da bi se utvrdilo je li slika originalna ili ne.“ (Liu et al., 2014)

„Na Internetu su-egzistiraju različite vrste informacija (tekst, slika, video i audio zapis, multimedija), a velika količina sadržaja postavlja problem kako efikasno pronaći traženu informaciju, jednako kao i kako osigurati arhiviranje i dostup on-line sadržaju, s obzirom na njegovu dinamičku strukturu i promjenjivost sadržaja. Ta i druga pitanja povezana su i s pravom na slobodu informiranja, stvaralačkom slobodom, slobodom govora i s drugim političkim pitanjima.“ (Uzelac, 2004)

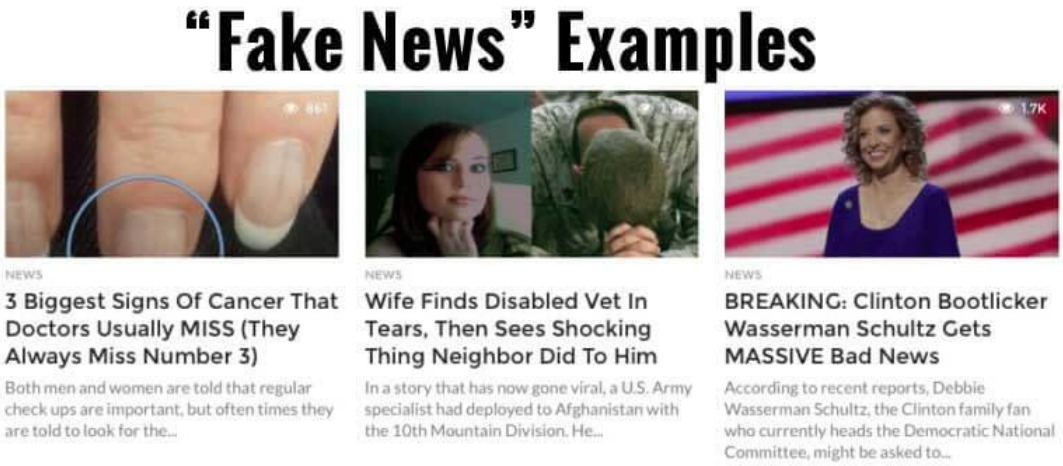
4.10. Lažne vijesti

„Lažne vijesti (popularnim imenom *fake news*) imaju izravno ili uobičajeno razumljivo značenje. To je zato što *vijest*i označavaju provjerljive informacije u javnosti i informacije koje ne zadovoljavaju te standarde ne zaslužuju oznaku vijesti. U tom smislu, tada su *lažne vijesti* oksimoron koji je podložan potkopavanju vjerodostojnosti informacije, te prelaze prag provjerljivosti i javnog interesa, tj. stvarne vijesti.“ (UNESCO, 2018)

„U današnjem kontekstu dezinformacija i misinformacija krajnja opasnost nije nepravilno reguliranje novinarstva, već to što javnost može početi sumnjati u sve sadržaje - uključujući i novinarstvo. U tom slučaju ljudi bi, s druge strane, smatrali vjerodostojnima bilo koje sadržaje koji su na njihovim društvenim mrežama, te u koje vjeruju po osjećaju, a ne promišljajući. Već možemo vidjeti negativni utjecaj toga na mišljenje javnosti o zdravstvu, znanosti i obrazovanju, te razumijevanju multikulturalnosti. Taj se utjecaj na javnost posebno tiče i izbora vlasti, i same ideje demokracije kao ljudskog prava. Isto tako pitanja migracija, klimatskih promjena i sl. mogu biti pod velikim utjecajem nevjerice proizišle iz dezinformacija.“ (UNESCO, 2018)

„Dezinformacije narušavaju povjerenje u institucije, te u digitalne i tradicionalne medije, čime štete našoj demokraciji ometajući sposobnost građana da donose informirane odluke. Mogu polarizirati rasprave, stvoriti ili produbiti napetosti u društvu i potkopati izborni sustav, te imati širok utjecaj na europsku sigurnost. Umanjuje slobodu mišljenja i izražavanja, temeljno pravo sadržano u Povelji o temeljnim pravima Europske unije. Borba protiv dezinformacija u eri društvenih medija i mrežnih platformi mora biti koordiniran napor koji uključuje sve relevantne aktere, od institucija do društvenih platformi, od novina do pojedinih korisnika.“ (Europska komisija, 2019.)

Osim potpuno izmišljenim vijestima, na Internetu se pregledi članaka skupljaju i naslovom koji privlači, tj. mami veliku pažnju i zainteresira korisnika da klikne i pročita o čemu se radi. Takav *clickbait* prikazuje Slika 18.



Slika 18 – Lažne vijesti: *clickbait*

Izvor: https://marketingland.com/first-thought-brand-dollars-safe-happened-200793 (10.08.2019.)

4.11. Ostale opasnosti

„Pojavila su se mnoga pitanja u vezi praćenja potrošača preko njihove upotrebe Interneta ili aplikacija za mobilne telefone, obično poznate kao *apps*. Općenito govoreći, zabrinutosti leži u tome je li praćenje ispravno objašnjeno potrošačima ili bi oni uopće imali razloga znati je li praćena i pohranjena njihova upotreba podataka, a ponekad i lokacija. Svrha je praćenja obično omogućiti ciljanje reklama na potrošače na temelju njihove trenutne lokacije ili njihove povijesti pregledavanja." (Martin et al., 2018)

Darknet se odnosi na sadržaje koji nisu dostupni u tražilicama kao što su Google, Yahoo ili Bing. To je mreža koja je dostupna određenoj grupi ljudi, ne široj internetskoj javnosti, a dostupna je samo putem autorizacije, specifičnog softvera i konfiguracija. Darkweb uključuje bezopasnije sadržaje, poput akademskih baza podataka i korporativnih web stranica, ali i one strože kažnjive sadržaje, kao što su crna tržišta, fetiš zajednice, hakiranje i piratstvo. Korisnici Darkneta su anonimni, a upravo je ta anonimnost privukla zločinački element. Na njemu je slobodno voditi ilegalni posao i izražavati se bez straha od posljedica. Postao je utočište za kriminalce koji prodaju drogu i oružje, pa čak i trguju ljudima.[12]

[12] Izvor: https://www.techopedia.com/definition/2395/darknet (10.08.2019.)

4.12. Osnovna online zaštita

Iako za svaku pojedinačnu prijavaru treba individualna opreznost i zaštita, postoje određene osnovne upute kako povećati svoju online sigurnost. Četiri najbolje stvari koje korisnici mogu učiniti kako bi zaštitili svoje računalo su: održavati i ažurirati trenutni softver, prakticirati načelo najmanje privilegije (eliminirajući nepotrebne privilegije koje mogu rezultirati mrežnim iskorištavanjima), koristiti sigurnosni softver, te često izrađivati sigurnosnu kopiju važnih dokumenata i datoteka. Tu su i dodatni koraci u zaštiti kao npr.: ne dijeliti lozinke, prijaviti se za upozorenja o stranoj prijavi, ne klikati na sumnjive veze, provjeriti web lokacije koje traže korisničko ime i zaporku, ignorirati e-poruke nepoznatih osoba, ne preuzimati nepoznate dokumente ili softvere s Interneta, ne širiti lančane e-poruke, odjavljivati se sa svog računala, ukloniti nepotrebne programe itd.[13]

[13] Izvor: https://kb.iu.edu/d/akln#digitalsign (10.08.2019.)

5. ZAKLJUČAK

Digitalna tehnologija je do sad najbitniji i najveći čimbenik u razvoju ljudi, bez koje ne bi došlo do Treće i Četvrte industrijske revolucije. Tehnologijom je obuhvaćena većina područja, od kulturog, poslovnog, zabavnog, do znanstvenog itd., te je neizostavan dio današnjice. Time raste njezina uloga i važnost, jer bez nje moderni svijet ne bi dosegnuo dostignuća koja je i koja će tek postići. Digitalna kultura i obrazovanje je neizbježno, svaka osoba se susreće s barem nekom tehnološkom granom. Budući da se čovjek razvija tehnologijom, a tehnologija zbog čovjeka, oni su u konstantnoj simbiozi napredka. Međutim, iako je većina stvari povezana uz nju pozitivna, upravo zbog tog čovjekovog udjela, normalno je da se razvijaju i one negativne. Tako su kriminalitet u kibernetičkom prostoru, kao i npr. digitalna forenzika, relativno novi, ali nezaobilazni pojmovi kad se govori o digitalnoj tehnologiji. Nove prilike za razvoj potiču i nove prilike za iskorištavanje tog razvoja, te se tu pojavljuju internetski prevaranti i kriminalci. Kako u svijetu, tako i u Republici Hrvatskoj, donesena je pravna regulativa da se spriječe takvi pothvati loše namjere. Kaznena djela protiv časti i ugleda, spolnog zlostavljanja i iskorištavanja djeteta, protiv intelektualnog vlasništva i protiv javnog reda, su od pojave Interneta sve više prisutna i u digitalnoj realnosti. Uz to, nedozvoljena ponašanja poput hakiranja i piratstva, računalne sabotaže i prijevara, sabotaže računalnih sustava i podataka, špijunaže i zloporabe naprava, su također praćena i kažnjiva. Nediskutabilna je primjena nacionalne strategije kibernetičke sigurnosti budući da je Internet globalna, ali zato i ranjiva platforma, jer činjenica je da su osobe s druge strane tih zakona u većini slučajeva dva koraka ispred zbog anonimnosti koja im je dostupna u virtualnom svijetu. Zato je važno ne samo djelovati na razini zakona, nego i na razini sprječavanja, tj. informirati obične građane koje im opasnosti prijete.

Informiranost o prijevarama putem digitalne tehnologije bitna je za sigurnije korištenje Internetom, ali i ostalom tehnologijom. Prevaranti zarađuju upravo na osobama koje su neupućene, ili se nikad prije nisu susrele sa sumnjivom e-porukom. Nigerijske prijevare, koje uključuju krađu osobnih podataka i novčanih sredstava, poznate su još od 1920.-ih u drugačijim oblicima, stoga je upitno hoće li se uopće ikada iskorijeniti do kraja. Osim toga, prevaranti su sve inovativniji, pa i oni iskusni mogu upasti u zamku neke nove prijevare. Potrebno je osvijestiti korisnike digitalne tehnologije kako bi pozornije obratili pažnju na sadržaj koji im se prezentira, bez obzira koliko bezopasno nešto izgledalo. Lažne vijesti i recenzije, lažni lijekovi i kreditne kartice, sve to i više, unazaduje digitalni razvoj, te je na svakom pojedinačnom korisniku da prosudi u kojem će on smjeru krenuti.

LITERATURA

1) Bushati, J.; Lezha, E.: About digital culture and education, 2017., https://hrcak.srce.hr/184275 (10.08.2019.)

2) Drew, J. M.: Assessing the Magnitude of Mass Marketing Fraud, 2011., https://search.proquest.com/docview/920647031?pq-origsite=summon (10.08.2019.)

3) European Commission: Fake news and online disinformation, 2018., https://ec.europa.eu/digital-single-market/en/fake-news-disinformation (10.08.2019.)

4) Goswami, K.; Park, Y.; Song, C.: Impact of reviewer social interaction on online consumer review fraud detection, 2017., https://search.proquest.com/docview/1987890006?pq-origsite=summon (10.08.2019.)

5) Isacenkova, J.; Thonnard, O.; Costin, A.; Francillon, A.; Balzarotti D.: Inside the scam jungle: a closer look at 419 scam email operations, 2014., https://link.springer.com/article/10.1186%2F1687-417X-2014-4 (10.08.2019.)

6) Jelenski, M.; Šuperina, M.; Budiša, J.: Kriminalitet platnim karticama (krađa identiteta, krivotvorenje i zlouporaba platne kartice), 2013., https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=177889 (10.08.2019.)

7) Liu B.; Pun C-M.; Yuan X-C.: Digital Image Forgery Detection Using JPEG Features and Local Noise Discrepancies, 2014., https://www.hindawi.com/journals/tswj/2014/230425/ (10.08.2019.)

8) Lötter, A.; Futcher, L.: A framework to assist email users in the identification of phishing attacks, 2015., https://search.proquest.com/docview/2093316524?pq-origsite=summon (10.08.2019.)

9) Martin, A. R.; Sarkar, R.: Developments in Advertising and Consumer Protection in Cyberspace, 2018., https://search.proquest.com/docview/2049984545?accountid=132154&pq-origsite=summon (10.08.2019.)

10) Prasanthi, B. V.; Kanakam, P.; Hussain, M.: Cyber Forensic Science to Diagnose Digital Crimes- A study, 2017., http://www.ijcttjournal.org/2017/Volume50/number-2/IJCTT-V50P119.pdf (10.08.2019.)

11) Protrka, N.: Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru, doktorski rad, 2018., https://repozitorij.unizd.hr/islandora/object/unizd:2333 (10.08.2019.)

12) Sinčić, P.: Digitalna revolucija, diplomski rad, 2018., https://repository.inf.uniri.hr/islandora/object/infri%3A358/datastream/PDF/view (10.08.2019.)

13) Thornton, C. E.: Intimacy issues: a content analysis of intimacy levels and engagement rates between celebrities and influencers, 2018., https://baylor-ir.tdl.org/handle/2104/10382 (10.08.2019.)

14) UNESCO: Journalism, 'Fake News' & Disinformation, 2018., https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf (10.08.2019.)

15) Uzelac, A.: Digitalna kulturna dobra u informacijskom društvu između javne domene i privatnog vlasništva, 2004., https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=36250 (10.08.2019.)

16) Wilbur, K. C.; Zhu, Y.: Click Fraud, 2009., https://search.proquest.com/econlit/docview/57022911/1D9B7F4B075A47DBPQ/8?accountid=168605 (10.08.2019.)

POPIS NAVODA I IZVORA PODATAKA

[1] Izvor: https://economictimes.indiatimes.com/blogs/et-commentary/changing-in-a-world-of-digital-revolution/ (10.08.2019.)

[2] Izvor: https://turbofuture.com/computers/Advantages-of-Digital-Technology (10.08.2019.)

[3] Izvor: https://www.imperva.com/learn/application-security/phishing-attack-scam/ (10.08.2019.)

[4] Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)

[5] Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)

[6] Ibid.

[7] Izvor: https://kb.iu.edu/d/afvn (10.08.2019.)

[8] Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)

[9] Izvor: https://www.scam-detector.com/article/free-gift-card (10.08.2019.)

[10] Izvor: https://www.lifewire.com/top-internet-email-scams-2483614 (10.08.2019.)

[11] Izvor: https://www.techopedia.com/definition/28252/slacktivism (10.08.2019.)

[12] Izvor: https://www.techopedia.com/definition/2395/darknet (10.08.2019.)

[13] Izvor: https://kb.iu.edu/d/akln#digitalsign (10.08.2019.)

POPIS SLIKA

Slika 1 – Četiri industrijske revolucije 4
Slika 2 – Povijesni pregled digitalne revolucije 5
Slika 3 – Jedna minuta na Internetu 6
Slika 4 – Usporedni prikaz kaznenih djela kibernetičkog kriminala 14
Slika 5 – Kaznena djela počinjena putem komunikacijske tehnologije 15
Slika 6 – Globalna internetska populacija 16
Slika 7 – Najčešće Internet prijevare 16
Slika 8 – *Phishing* napad: lažno sveučilište 17
Slika 9 – *Phishing* napad: lažna dobrotvorna organizacija 18
Slika 10 – *Phishing* napad: lažni službenik 19
Slika 11 – Prijevara nagradnom igrom 20
Slika 12 – Lažno zapošljavanje 21
Slika 13 – Prijevara s brzom zaradom 22
Slika 14 – Prijevara kreditnim karticama 23
Slika 15 – Klik prijevara: poklon kartice 24
Slika 16 – Klik prijevara: brza zarada 24
Slika 17 – Lažne recenzije 25
Slika 18 – Lažne vijesti: *clickbait* 28