FBIM Transactions
DOI 10.12709/fbim.07.07.02.10

ZLOUPOTREBA NOVIH TEHNOLOGIJA I DIGITALNO NASILJE

NEW TECHNOLOGY ABUSE AND DIGITAL VIOLENCE

Zoran Milanović
Kriminalističko-policijski Univerzitet, Beograd, Srbija

JEL Kategorija rada: **L86**

Apstrakt

Super brzi razvoj novih tehnologija doneo je i njihovu nezakonitu primenu u tom obimu da ni napredni korisnici, ni bezbednosni stručnjaci nisu svesni brzine nastajanja digitalnih rizika, niti rešenja za svakodnevne digitalne probleme. Dobra poslovna i korisnička praksa ukazuje da korisnici digitalnih uređaja treba da budu naoružani aktuelnim činjenicama neophodnim za sopstvenu zaštitu, zaštitu svojih porodica, svojih kompanija i svojih zajednica, kako bi se odbranili od novonastalih digitalnih pretnji i rizika. Primarni cilj rada je da se kroz citiranje velikog broja elektronskih naslova, koji opisuju katastrofalne pojave u digitalnom svetu, podigne svest običnih korisnika i promeni njihova percepcija i ponašanje pri korišćenju digitalnih uređaja, jer jedino se praktičnim znanjem može boriti protiv zloupotrebe novih tehnologija i narastajućeg digitalnog nasilja.

Ključne reči: *informaciona bezbednost, zloupotreba novih tehnologija, digitalno nasilje.*

Abstract

The rapid development of new technologies has also led to their unlawful application to the extent that neither advanced users nor security professionals are aware of the rate of formation of digital risks, nor of solutions to everyday digital problems. Good business and customer practice indicate that digital device users should be armed with current facts necessary for their own protection, the protection of their families, their companies and their communities, to defend themselves against emerging digital threats and risks. The primary aim of the paper is to raise the awareness of ordinary users, change their perceptions and behavior when using digital devices by citing a large number of electronic titles describing catastrophic phenomena in the digital world, as only practical knowledge can combat the misuse of new technologies and the growing digital violence.

Keywords: *information security, new technology abuse, digital violence.*

Adresa autora:
Zoran Milanović
zoran.milanovic@kpu.edu.rs

1 UVOD

Kičmu civilizacije poverili smo mašinama i Internetu. Digitalne tehnologije, iako predstavljaju nasušnu potrebu savremenog društva, oduvek su

bile mač sa dve oštrice. Njihovom primenom pružaju nam se mnoge pogodnosti kojima puno dobijamo u svakodnevnom radu i životu, ali i isto toliko gubimo. Naš sveukupni digitalni svet: biznis, zabava, autorsko delo ili neka draga uspomena, mogu biti izgubljeni sa samo nekoliko klikova miša ili hardversko-softverskom greškom. Još mnogo gore od toga, na Internetu nisu ugroženi samo naši lični i poslovni digitalni sistemi i podaci, tu se direktno napadaju i vitalni sistemi civilizacije koji se oslanjaju na nove tehnologije i kojima se upravlja i kontroliše: elektro-energetski, gasovodni i vodni sistemi, avio saobraćaj, policijske, vatrogasne i medicinske službe, vojska, obrazovanje, finansije…

Ne treba da nas brinu samo kriminalci i odmetnički režimi koji za cilj imaju ugrožavanje i zloupotrebu novih tehnologija, već nas često, neverovatno ranjive ostavljaju i velike IT kompanije, proizvođači hardvera, softvera, pružaoci raznih servisa i usluga, kao i organizacije na koje se oslanjamo da nas štite i savetuju, a u stvari i one kontrolišu kod koji upravlja našim životima.

Zato, „što više priključujemo naše uređaje i živote u globalnu informacionu mrežu – bilo preko mobilnih telefona, društvenih mreža, liftova ili autonomnih vozila – to ranjiviji postajemo pred onima koji znaju kako funkcionišu osnove tehnologije i kako se mogu upotrebiti u njihovu korist, a na štetu običnih ljudi. Jednostavno rečeno, kad je sve povezano, svi su ranjivi. Tehnologija koju rutinski unosimo u svoj život sa malo ili nimalo promišljanja ili ispitivanja može sasvim lako da nam se vrati kao bumerang.”(Gudmen, 2017, str. 11)

Korisnici treba da budu svesni, svuda i u svakom trenutku, koje digitalne uređaje (računar, telefon...) nabavljaju i od koga, sa kakvim softverom i podrškom, gde i kako ih povezuju na mrežu, kao i kako ih koriste, a posebno da znaju, da sve što rade na njima, negde se beleži i pre ili kasnije, bez obzira da li postoji veza sa Internetom, biće javno dostupno i nekim drugim osobama ili organizacijama. Takođe, korisnici treba da znaju da skoro da ne postoji nijedan uređaj, nijedno softversko rešenje koje nema neki bezbednosni propust u sistemu, bez obzira da li je svesno napravljen od proizvođača, npr. upis u Firmware (Wodinsky, 2018) ili izvornog programera odn. hakera, npr. Backdoor – otvaranje zadnjih vrata radi ilegalnog pristupa (Stone, 2019), ili problemi i propusti koji nisu ni utvrđeni tokom testiranja proizvoda, npr. greške koje se koriste za Zero-Day – napad nultog dana (Schwartz, 2019).

Na sve navedeno, svakodnevno nas upozoravaju digitalni novinski naslovi, koji iznose puno crne statistike u brojkama (raznim valutama i procentima), puno rezultata stručnih istraživanja i primera iz prakse, koji posebno apostrofiraju digitalno nasilje, najčešće nad decom i mladima.

2 DIGITALNO NASILJE NAD DECOM I MLADIMA

Nedostatak bezbednosne kulture najviše pogađa decu i mlade i to kako zbog njihovog posebnog mesta u sistemu zaštite, tako i zbog njihove naivnosti. Prema Mišelu Sen Lou (2015), direktoru UNICEF-a u Srbiji, „sve više dece koristi digitalne alatke za učenje, društveno angažovanje i druženje. Međutim, putem njih se izlažu i novim rizicima – nasilju, neprikladnom sadržaju, nepoznatim ljudima“.

Naime, mladi imaju probleme koje ne mogu uvek da prepoznaju i objasne, susreću se sa različitim pojavama i pretnjama bez prethodne psihološke zaštite. Probleme uglavnom ne mogu sami da reše i/ili ne znaju kome da se obrate za pomoć.

Opasnosti i pretnje kojima je mlađa populacija korisnika Interneta svakodnevno izložena su brojne i raznovrsne, a posebno sa ekspanzivnim razvojem društvenih mreža i onlajn igrica. One danas predstavljaju sadržaje koji su popularni i kao takvi veoma uticajni na mlađu populaciju korisnika Interneta.

Mladi su najugroženija ciljna grupa većine pojavnih oblika zloupotrebe, a posebno nastajanju, razvoju i širenju dečije pornografije, pedofilije, onlajn igricama, kockanju i klađenju.

Mladi širom sveta, svakodnevno provode sate i sate igrajući onlajn multiplejer video igre. Pozitivna strana onlajn igranja je zabava, sklapanje prijateljstva i razmena iskustva sa ljudima iz raznih delova sveta, otkrivanje novih interesovanja, osećaj pripadnosti društvu i sl. No, postoji i negativna strana korišćenja onlajn gejmerskih servisa koja se ogleda u postojanju brojnih opasnosti koje mogu izuzetno loše uticati

na gejmere (e-igrače). Naime, istraživanje organizacije za ljudska prava Anti-Defamation League (ADL), pokazalo je da se radi o zlostavljanju koje je u onlajn multiplejer igrama doživelo čak 74% osoba koje su učestvovale u ovom istraživanju (Castello, 2019), od čega je 65% njih bilo "ozbiljno zlostavljano" što uključuje i pretnje fizičkim nasiljem i praćenjem. Kao razloge zlostavljanja više od 50% ispitanika navelo je zlostavljanje zasnovano na rasi, etničkoj pripadnosti, religiji i seksualnoj orijentaciji. Skoro 30% tvrdi da su bili doksovani (doxxed – objavljena adresa i broj telefona) u onlajn igri, a skoro četvrtina ispitanika kaže da je bila izložena ideologiji superiornosti bele rase. Takođe, primećeno je da neki gejmeri u toku igranja šire „ekstremističke ideologije“. (Rock, 2019)

Iako rezultati ADL istraživanja nisu definitivni (ispitano oko 1.000 ljudi) gejming zajednica je svesna da onlajn igranje može dovesti do nezdravog ponašanja (Fisher, 2019b). Tako je 24-godišnjak David Katz, posle izgubljenog turnira (ili diskvalifikacije) uzeo pištolj, ubio dvoje ljudi i više njih ranio, a potom i izvršio samoubistvo. Zatim, ubistvo oko 30 ljudi u dve masovne pucnjave u SAD, predsednik Donald Tramp (Donald Trump) je za te tragične događaje, između ostalog, okrivio “stravične i grozne video igre”, što nije prvi put da je uspostavio ovu vezu, niti je jedini koji je to učinio. (Landsverk, 2019)

Još jedan od roditeljskih problema, nakon “Plavog kita” koji se dovodi u vezu sa samoubistvom 130-toro dece u Rusiji (Adejn, 2019), stigao je novi izazov na sajtu YouTube Kids koji tera decu da izvrše samoubistvo. (Dough, 2019)

Takođe, prema studiji sprovedenoj u SAD, a nakon što je prikazivana Netfliks-ova serija "13 razloga zašto", od aprila 2017. godine broj samoubistava među decom od 10 do 17 godina je porastao za jednu trećinu. (Carey, 2019)

Što se tiče crne strane onlajn gejminga, primećeno je, takođe, npr. u igrici Super Mario Odyssey da se preko veoma specifičnih kanala u igru, kroz portrete i specijalne balone, ubacuju slike eksplicitnog pornografskog sadržaja. Kako je u pitanju onlajn deo igre, odnosno novi mod Luigi’s Balloon World, ovo su u svakom trenutku mogla da vide i brojna deca koja igraju Super Mario Odyssey, bez znanja njihovih roditelja, koji očekuju da im deca igraju igru prigodnu njihovom uzrastu. (Keach, 2018)

U najnovijem saslušanju koje je sprovela britanska vlada, otkriveno je da je jedan dečak u igri Runescape putem mikrotransakcija, naneo ogromne finansijske poteškoće svojim roditeljima, potrošivši neverovatnih 62.000 dolara. (Thubron, 2019)

Deca ne samo što su žrtve, mogu biti i napadači. Tako mališani od samo 10 godina pokreću velike kiber napade (DDoS – uskraćivanje usluga), putem besplatnih alata sa Interneta, kako bi dobili ili ostvarili prednost nad protivnicima u onlajn igricama (Fortnite), dok je jedan tinejdžer od 14 godina izveo skoro 500 kiber napada, za samo mesec dana, sa istim ciljem kao i njegov prethodnik. (Stevens, 2019) Deca, iako žive sa roditeljima, nisu svesna da vrše krivično delo, a takođe ni njihovi roditelji. Ovde se posebno upozoravaju roditelji da obrate pažnju na mrežne aktivnosti svoje dece, jer posledice su katastrofalne.

Posebno mesto u ovoj problematici zauzimaju kockanje i klađenje u onlajn varijantama, izuzetno atraktivno za decu i mlade osobe. Prema istraživanju iz 2013. godine, novosadskog centra "Život nije igra" problem patološkog kockanja javlja se već u osnovnoj školi, a ovaj porok sve više uzima maha. Od 790 ispitanika, uzrasta od 11 do 20 godina, skoro polovina igra igre na sreću. Od ukupnog broja ispitanika 48 se patološki kocka, a 20 odsto problematično. Zabrinjava podatak da najmlađi ispitanik koji se patološki kocka ima samo 12 godina (igra sa tatom rulet, a počeo je sa aparatima kad je imao manje od 10 godina uz brata ili tatu). (Život nije igra, 2013)

Komisija za praćenje i nadziranje kockanja u Velikoj Britaniji u svom izveštaju navodi da oko 25.000 dece uzrasta od 11 do 16 godina, pripada kategoriji problematičnih kockara, a mnogi uče da se klade putem računarskih igara tzv. E-sportova (igrice kao što su Counter-Strike, Dota2, Call Of Duty, Overwatch and League of Legends) i društvenih medija. Njih 70% je prve reklame za kockanje i klađenje videlo na društvenim mrežama, 66% na drugim web sajtovima, dok njih oko 10 % prate kompanije za kockanje i klađenje na društvenim mrežama. (Gambling, 2017)

Neočekivano, ispostavilo se da deci i mladima najčešće povrede privatnosti i psiho-fizičko ugrožavanje prete u najbližem okruženju – porodici i vaspitno obrazovnim ustanovama, a najčešće zbog objava na društvenim mrežama. Neodgovorni i nesmotreni roditelji prave probleme deci, kada objavljuju slike na Internetu bez njihovog odobrenja (Lyons, 2019). Oni treba da budu svesni i da čuvaju i zaštite prava deteta, a ne da ugrožavaju njihovu privatnost i da javno dele identitet deteta bez njihovog pristanka. (Hart, 2019) Tako je jedna 18-godišnjakinja iz Južne Australije tužila roditelje zbog objavljivanja njenih fotografija iz detinjstva na Facebooku. (Huggler, 2016)

Koliko je to učestala pojava ili uticaj sve popularnijih društvenih mreža, ukazuje i podatak da roditelji deteta od pet godina u proseku objave 1500 slika o njemu ili njoj na Facebook-u, Tvitter-u, Instagram-u i slično. (Mangan, 2016)

Ono što je posebno alarmantno u Srbiji, svaka treća mlada osoba trpi digitalno nasilje. (PC Press, 2019)

Rešenje i prevenciju za iznete probleme treba tražiti u edukaciji i upozorenju na nivou roditelja koji igraju možda najvažniju ulogu u prevenciji i rešavanju ovog problema. Adekvatna bezbednosna kultura svih korisnika, a naročito mladih, imperativ je savremenog društva.

Decu i mlade treba podsticati da postanu aktivniji, sa većim opsegom znanja, razumevanja i mogućnosti da se suoče sa problemima, kao i da neguju ona ponašanja koja će značajno podići nivo njihove bezbednosne kulture (Ejdus i dr. 2009). Da bi se ovaj cilj postigao neophodno je da informaciono-bezbednosna kultura postane sastavni deo planova i programa svih nivoa obrazovanja i vaspitanja. Prihvatanjem osnovnih načela informaciono-bezbednosne kulture stvorio bi se preduslov za uspostavljanje bezbednog ambijenta u kome bi mladi neometano mogli da koriste sve prednosti i blagodeti informacionih tehnologija i tako ostvare svoja prava na kvalitetno obrazovanje, informisanje i lični razvoj.

3 DRUŠTVENE MREŽE – SERVIS ZA USPEH ILI PROPAST SAVREMENOG DRUŠTVA

Društvene mreže su novi kreatori javnih dosijea, koji prikupljaju sve što je neko podelio, svesno ili ne, sortiraju i skladište, a onda to prodaju oglašivačima, vladama i trećim licima.

Rezultati istraživanja firme Security Baron su, blago rečeno, zastrašujući. Oni ukazuju koliko i kojih podataka velike IT kompanije (Facebook, Google, Microsoft, Amazon, Apple i Twitter) prikupljaju o svojim korisnicima i koliko mnogo zarađuju prodajući te informacije. Sprovedeno istraživanje se odnosi na pregled zvaničnih politika privatnosti navedenih kompanija i tabelarno prikazivanje vrste podataka koje svaka od njih prikuplja o svojim korisnicima. (Turner, 2019) Inače o kolikom bogatstvu se radi najbolje govore podaci dati u Forbsovoj listi za 2019. godinu, gde se među prvih 10, nalaze 4 vlasnika gore navedenih kompanija: 1. Džef Bezos, Amazon, USD 131 milijarda; 2. Bil Gejts, Microsoft, USD 96,5 milijardi; 8. Mark Zuckerberg, Facebook, USD 62.3 milijarde i 10. Leri Pejdž, Google, USD 54 milijardi. (Kroll & Dolan, 2019a)

Iz prethodnih brojki može se zaključiti da naizgled besplatne usluge koje nam nude velike tehnološke kompanije, to zapravo i nisu. Prodaja naših podataka, koje smo im, doduše, sami poklonili, učinila ih je, ne samo najbogatijim, već i najmoćnijim kompanijama na svetu.

Ljudi koji upotrebljavaju društvene mreže treba da budu svesni, da oni nisu korisnici tih servisa već njihov proizvod, koji se prodaje onima koji ponude najvišu cenu. Društvene mreže nisu napravljene da bi ih korisnici upotrebljavali za svoje potrebe, već su osmišljene sa konkretnom namerom da obmanu, zavedu i prevare korisnike, kako bi otkrili što veću količinu podataka o sebi i svom životu. Primeri i brojke o zloupotrebi društvenih mreža i narušavanje privatnosti korisnika gore sve.

- Od nastanka prvih društvenih mreža pa do danas one su prikupljale podatke bez našeg saznanja. Kada je to postalo očigledno, izbijanjem afere o Facebooku i Cambridge Analytice, koji su neovlašćeno prikupljali podatke od oko 87 miliona korisnika bez njihovog pristanka i koristili ih za ciljane oglase i političke kampanje, prešlo se na sledeći nivo tj. korisnicima se plaća za potpuni pristup njihovoj privatnosti.
- Facebook plaća 20 dolara, a Google 25 dolara, tinejdžerima (od 13 godina) da

instaliraju VPN na telefonima, kako bi ih špijunirali (Tech Crunch, 2019b). Facebook interesuje kako mladi koriste telefon i koji sadržaj pregledaju na vebu, a imali su i pristup privatnim porukama, mejlovima itd. Sve to interesuje i Google i mnogo više, kako se koriste njihovi proizvodi, ne samo na pametnim telefonima, već i na ličnim računarima, televiziji, pa čak i pristup ruterima za snimanje šta rade onlajn. Google, takođe interesuje i kako se koriste aplikacije konkurentskih kompanija poput Facebook-a i WhatsApp-a itd.

- Profit Facebook-a raste uprkos skandalima o narušavanju privatnosti, njihova čista dobit dosegla u četvrtom tromesečju 6,88 milijardi dolara, što je 62 odsto više nego godinu dana ranije (Carrie Wong, 2019b). Tako Facebook skandali nisu promenili ni navike korisnika, niti su uticali na promene u podešavanju privatnosti (Lee T., 2018).
- Činjenica da Facebook ugrožava privatnost korisnika više ne predstavlja iznenađenje, njihovo poslednje priznanje odnosi se na snimanje i prisluškivanje glasovnih poruka korisnika u Messenger-u (Hern, 2019).
- Facebook prati i prikuplja podatke korisnika i nakon što deaktiviraju svoje profile i to putem Facebook dugmeta za deljenje sadržaja, koje se nalazi na 275 miliona web stranica, a radi prikupljanja informacija za koje su sadržaje korisnici zainteresovani. Prikupljanje podataka se obalja i kod korisnika koji nisu imali nalog na toj društvenoj mreži, a posetili su stranicu na kojoj se nalazi njihov f-znak (Ng, 2019).
- Studija sa Stanforda i Univerziteta New York otkriva da su korisnici koji su deaktivirali svoj Facebook nalog mnogo srećniji, ali manje informisani (CORDIS, 2019).
- Veliki broj internih dokumenata ukazuje da Facebook-ova surova mašinerija ima informaciju da maloletnici roditeljima troše novac s kartica, ali ipak ništa ne preduzima (Lee D., 2019). A i što bi reagovali, kada je profit iznad svega.
- Bezbednosni stručnjaci su otkrili i osudili, a Facebook priznao da je učitao kontakte 1,5 miliona mejl adresa bez prethodnog znanja i odobrenja korisnika. Facebook je klasičnom fišing prevarom naterao nove korisnike, navodno kako bi potvrdili identitet i uvezli svoje kontakte da se prijave putem e-mail adrese i šifre. Na osnovu ta dva podatka Facebook je “slučajno“ skinuo sve kontakte sa dobijenih e-mail adresa (Porter, 2019c).
- Na Internetu je pronađena Facebook-ova nezaštićena baza podataka koja sadrži više od 419 miliona telefonskih brojeva (Carrie Wong, 2019b), a bezbednosni stručnjak Frank Abagnale tvrdi da bi u 98 odsto slučajeva, datum i mesto rođenja bili dovoljni da hakeri nekome ukradu identitet. Njegova preporuka je da korisnici društvenih mreža, prvenstveno korisnici Facebooka, sklone ove osetljive podatke sa svog profila. (Abagnale, 2019)
- YouTube je kažnjen sa 170 miliona dolara zbog narušavanja privatnosti dece. Oni su nezakonito prikupljali lične podatke dece, bez odobrenja njihovih roditelja (Bartz, 2019). Google je platio i 50 miliona eura francuskoj zbog nepoštovanja GDPR-a (Porter, 2019a), a Facebook kažnjen sa 5 milijardi dolara zbog pronevere privatnosti svojih korisnika (Kelly, 2019). Naravno, ove kazne ih nisu promenile, nastavili su po starom, sa minimalnim kozmetičkim promenama, jer upitanju su velike zarade, a navedeni izuzetno mali troškovi.

U prilog svemu navedenom govori i preporuka bezbednosnog uzbunjivača i stručnjaka Edvarda Snoudena (Edward Snowden) da treba da budemo svesni svaki put kada nešto poželimo da ostavimo ili preuzmemo sa Interneta: „Sve što sada radimo ostaje zapisano zauvek. Ne zato što mi to želimo da zapamtimo, već zato što nam više nije dozvoljeno da zaboravimo" (Sputnik International, 2019). On takođe kaže, „samo zamislite da otvorite računar i pronađete dokument koji niste napisali, a u kojem su svi vaši podaci o životu uredno sačuvani. Vaša matura, vaša fotografija na stadionu, slika sa zabave pre 10 godina u opijenom stanju, detalj poljupca koji ste dali ženi najboljeg prijatelja za koga ste se oboje zakleli da nikada nikome nećete reći. Zatim, lista svih porno snimaka koje ste ikada gledali, mapiranje svakog glupog i seksističkog komentara koji ste ikada napisali ili napravili. Goli

selfiji, fotografije snimljene na rođendanu vaše majke, video snimak u muzeju Louvr, itd. Pa, ovaj dokument postoji, ili bolje rečeno, mogao bi postojati, i nije distopijska fantazija.“ (La Repubblica, 2019)

Koliko istine ima u preporuci Snoudena, pokazuje i primer kako se štite oni koji najviše prikupljaju naše podatke. Tako, vlasnik Facebook-a na svom MacBook Pro ima traku zalepljenu preko web kamere, a da nije jedini, društvo mu pravi i direktor FBI Džejms Komi. S druge strane da i oni nisi svemogući i nedodirljivi i da u digitalnom svetu nema povlašćenih korisnika i apsolutno zaštićenih sistema, podataka, informacija i znanja, potvrđuju naredni primeri.

- Izvršnom direktoru Tvitera Jack Dorsey hakeri su preuzeli nalog i na njemu objavljuju uvredljive i rasističke poruke (Conger, 2019).
- Hakovan mobilni telefon najbogatijeg čoveka na svetu, Džefa Bezosa (Jeff Bezos), šefa kompanije Amazon (Badshah, 2019).
- Bivšem predsedniku SAD, Baraku Obami (Barack Obama, 2014.), ukradena novčana sredstva sa bankovnog računa i blokirana platna kartica (BBC, 2014a).

4 VISOKOTEHNOLOŠKE PRETNJE I HARDVERSKO-SOFTVERSKI BEZBEDNOSNI PROPUSTI

Osnovni razlog zbog koga je teško reagovati i boriti se protiv visokotehnoloških pretnji je postojanje nepoznatih hardversko-softverskih ranjivosti, koje se koriste za tzv. „napad nultog dana”. Velike IT kompanije ulažu mnogo novca kako bi motivisale istraživače da otkrivaju propuste i greške u sistemu, ali ne da bi obični korisnici bili bezbedniji, već da bi zaštitili svoj biznis.

Ono što je posebno važno, problemi sa kojima se susreće informaciona bezbednost daleko je složenija od tehničkih rešenja ili proizvoda. Shodno ovoj konstataciji je i izjava stručnjaka za bezbednost Šnejera (Bruce Schneier) „Ako mislite da tehnologijom možete rešiti vaš bezbednosni problem onda vi ne razumete ni problem ni tehnologiju“ (Schneier, 2015). Sledeći primeri ukazuju da problemi i propusti evidentno postoje.

- Napadi na operativni sistem Microsoft Windows su svakodnevni i učestali. Novo-stari trojanac (iz 2014. godine) RAT (remote access trojan) ugrožava sve verzije i sve uređaje sa ovim operativnim sistemom. Zlonamerni korisnici sa minimalnim tehničkim znanjima mogu da steknu potpunu kontrolu nad Windows uređajima. Svemogući maliciozni program može sa određene udaljenosti da isključi i ponovno pokrene pogođeni Windows uređaj, da pretražuje i pregleda fajlove, pristupi Task Manager-u, Registry Editor-u, i čak preuzme kontrolu nad mišom. Napadač može da otvara web stranice i isključi svetlo koje signalizira da je uključena web kamera, i tako neopaženo snima žrtvu po svojoj volji. Tu je i mogućnost prikupljanja lozinki i akreditiva za prijavljivanje pomoću keylogger-a, i na kraju zaključavanje pogođenog uređaja putem ransomeware. (Winder, 2019b)
- Stručnjaci za informacionu bezbednost iz kompanije Avast objavili su rezultate istraživanja na više od 160 miliona računara iz celog sveta, koja ukazuju da 55% korisnika na svojim ličnim računarima koristi zastareli softver, odnosno programe koji nisu nadograđeni na poslednju verziju, a koja uključuje i bezbednosnu nadogradnju. Tako jedan od 6 korisnika Microsoft Windowsa 7 i jedan od 10 korisnika aktualnog operativnog sistema Windows 10 ne koristi posljednju verziju, što hakerima potencijalno omogućava iskorišćavanje potencijalnih bezbednosnih propusta. (Palmer, 2019)
- Istraživači iz Google-a su otkrili više malicioznih sajtova, koji nakon posete omogućavaju hakerima da pristupe iPhone-u upotrebljavajući set do sada neotkrivenih ranjivosti u iOS-u, verzije od 10 do 12 (Whittaker, 2019). Sa druge strane, za najnoviji Apple operativni sistem iOS 13, bezbednosni stručnjaci i Američko ministarstvo odbrane (DoD) preporučuju da se nikako ne izvrši ažuriranje, jer je puno grešaka i kritičnih ranjivosti (Kelly, 2019).
- Velike probleme širom sveta izaziva specijalna vrsta zlonamernog softvera tzv.

Ransomware, koji uz pomoć enkripcije, ograničava pristup računarskim sistemima i sačuvanim fajlovima, a najčešće od žrtava traži otkup u bitkoinima. Ransomware je paralisao gradske službe u dva grada na Floridi (Ross & Leonard, 2019) koji su platili 1,1 milion dolara za otkup., kao i da je od 2013. godine najmanje 170 državnih i lokalnih samouprava u SAD priznalo da su imali iste probleme. Ransomware napad ostavio je skoro 12 sati bez struje najveći južnoafrički grad i finansijski centar, Johanezburg (Tech Radar, 2019). Takođe, ransomware napad odložio je početak školske godine. (Georg, 2019)

- Bezbednosni Istraživači su otkrili u Google Play prodavnici na desetine lažnih aplikacija za lepotu koje nemaju sopstvenu funkcionalnost, ali reprodukuju reklame na uređajima korisnika, kradu fotografije korisnika aplikacija i preusmeravaju korisnike na zlonamerne veb sajtove koji traže lične podatke (Teiss, 2019a). Takođe tu je pronađeno 15 aplikacija za GPS navigaciju, koje je preuzelo 50 miliona Android korisnika koji su sadržavali adver (softver za oglašavanje). (Teiss, 2019b)
- Više od 500 miliona Android korisnika instaliralo aplikacije sa opasnim malverom (Doffman, 2019).
- Preko 40 sertifikovanih drajvera omogućava instalaciju backdoor-a na Windows računarima (Khandelwal, 2019a).
- Chrome-ove ekstenzije i aplikacije, čak u 85% nemaju pravila o poštovanju privatnosti (Fisher, 2019a).
- Firefox ranjivost koja se eksploatiše čak 17 godina, omogućava krađu lokalnih fajlova i podataka sa računara (Dimitrova, 2019), a WinRAR program koji se često koristi na računarima, za arhiviranje fajlova, je dobio zakrpu za 19 godina star bezbednosni propust (Porter, 2019b).
- U PHP-u (Hypertext preprocessor) najpopularnijem programskom jeziku, koji se koristi u preko 78% servera na Internetu, pronađeni su mnogi nedostaci u izvršenju koda. Ova ranjivost može da omogući daljinski pristup napadačima i da kompromituje ciljani server (Wei, 2019b).
- Naizgled besplatno rešenje za gledanje prenosa sportskih događaja (fudbalske utakmice), uživo putem stream-a, može biti najopasnije i najskuplje, jer na takvim sajtovima postoje brojne skrivene opasnosti, virusi i maliciozni programi koji mogu preuzeti kontrolu nad računarom, ukrasti podatke i naneti veliku štetu (Cuthbertson, 2019).
- Nebezbedni uređaji, IoT (Internet stvari) i drugi digitalni sistemi koji se ne ažuriraju (što zbog proizvođača odn. njihovih korisnika), a povezani su sa Internetom, godinama pomažu različitim vrstama kiber kriminalaca. Najnoviji primer je Smominru, koji predstavlja zloglasni botnet, korišćen za DDoS napade, spam kampanje i ekstra profitabilno rudarenje kriptovaluta. Ovaj računarski virus se toliko brzo širi da mesečno zarazi preko 90.000 računara širom sveta (Khandelwal, 2019e).
- Milijardu mobilnih telefona rizično, zbog novootkrivenog propusta na SIM karticama, gde napadač slanjem SMS poruke može da izvrši ciljani nadzor korisnika (Chaparadza, 2019).
- Pronađeno 125 novih ranjivosti odn. nedostataka na ruterima i uređajima za bežično umrežavanje (ISBuzz News, 2019).
- Višestruke bezbednosne ranjivosti na WiFi ruterima D-Linka i Comba iz kojih cure šifre korisnika u otvorenom tekstu (Khandelwal, 2019b).
- Prevara koju je Google priznao, je da je njihov gadget Nest Secure imao ugrađen mikrofon, a da su “zaboravili” da napomene kupcima za taj dodatak (Bastone, 2019).
- Nedostaci u preko 600.000 nezaštićenih GPS pratilaca, otkrivaju podatke o lokaciji dece, starijih korisnika i kućnih ljubimaca, koji nose te uređaje sa sobom (AVAST, 2019), a aplikacije za fitnes otkrivaju informacije o vojnim bazama (Khandelwal, 2018). Ruska vojska je zabranila korišćenje mobilnih telefona zbog straha od špijunaže i društvenih medija (BBC, 2019b), a na drugoj strani, FBI, CIA i NSA preporučuju da se ne koriste Kineski telefoni marke Huawei (Vincent, 2018b) iz istih razloga.
- Hakeri ukrali lične podatke više od 70% punoletnih građana Bugarske (Wei, 2019).

- Petorica mladih srpskih hakera tvrde da poseduju JMBG gotovo svih građana Srbije (Blic, 2014).

Ipak, i pored svih navedenih primera zloupotrebe novih tehnologija i digitalnog nasilja, primat drži „digitalno crno tržište" na kome se mogu naručiti ubistva (TVC, 2019), trgovati ljudima, prodavati oružje i psihoaktivne supstance, gde cveta pedofilija i pornografija, odn. svo zlo savremenog društva. Nadu da nije baš sve tako crno daje primer uhapšene i privedene pravdi, svetske kriminalne grupe, koja je vodila onlajn prodaju "Wall Street Market" na crnom tržištu. Oni su prodavali sve što je zabranjeno od trgovine ljudima, preko narkotika i hakerskih alata do ilegalnih usluga i ukradenih finansijskih podataka. (New York Post, 2019)

5 INFORMACIONO-NEBEZBEDNA KULTURA KORISNIKA

Bez obzira na sve veći porast bezbednosnih incidenata korisnici ne žele da odustanu od svojih loših navika "zabava po svaku cenu", bahato ponašanje i ugrožavanje sebe, svoje porodice i okruženja, razmišljaju kratkoročno i neodgovorno, ne žele da se upoznaju sa problemima koje donose nove tehnologije. Moćne digitalne uređaje koriste kao pisaće mašine, e-mail kao papirnu poštu, onlajn igrice i društvene mreže, kao druženje na "poljančetu" sa prijateljima, a glavna bezbednosna mera zaštite im je "ma neće to mene, ništa ja ne krijem, nemam šta da štitim, ni da izgubim itd.", a sledeći primeri iz prakse ih demantuju:

- U Srbiji preko 50% kompjuterski nepismenih, izjavila Tatjana Matić, Državni sekretar u Ministarstvu trgovine, turizma i telekomunikacija (Ostojić, 2018b).
- 97% korisnika ne može da identifikuje fišing napade u svom e-mail-u, pokazuje istraživanje bezbednosnih stručnjaka iz kompanije Intel (Paganini, 2015).
- Uprkos rekordnom broju infekcija, korisnici još uvek ne znaju šta je ransomware (Informacija, 2016).
- Antivirusni softver nije svemoguć. Većina korisnika slepo veruje u antivirusni softver bez obzira na to da li je ažuriran ili ne, mada sledeće činjenice potvrđuju nešto sasvim drugo: antivirusni i drugi bezbednosni softveri nas štite samo od do sada poznatih malicioznih kodova (virusa), za novo kreirane zlonamerne kodove su beskorisni, i drugo, poverenje u antivirusne kompanije je narušeno njihovom čestom hakerskom kompromitacijom. Poslednji primer su tri glavne američke bezbednosne kompanije (McAfee, Symantec & Trend Micro) koje su bile ugrožene od elitnih ruskih hakera i čiji se izvorni kod (osnovni antivirusni kod, softver za web zaštitu, model veštačke inteligencije, razvojna dokumentacija kompanije) prodaje na crnom tržištu. (Mathews, 2019; CBR, 2019, Wagenseil, 2019).

6 ZAKLJUČAK

Iznete brojke govore sve. Korisnici novih tehnologija, zbog njih, gube živote, ugrožavaju zdravlje, uništavaju ugled, trpe nasilje, ostaju bez posla i finansija.

Nove tehnologije postale su „Ahilova peta" savremenog informacionog društva, posebno ako se zna da je kiber kriminal produkt i rezultat ljudske aktivnosti. Zasigurno, korisnici su najslabija karika i u situacijama kada je sistem besprekorno implementiran, a jedini pravi uzrok problema leži u njihovom neznanju ili nameri.

Posebnu pažnju treba skrenuti roditeljima da je njihova dobra namera ili povod da podele sa svojim prijateljima neke podatke, fotografije, video i sl. o svojoj deci, često nesmotrena i da lako mogu dovesti svoju decu čak i u životnu opasnost.

Roditelji, takođe, treba da budu svesni da su svojim ponašanjem očigledni primer deci, pa ako oni imaju nalog na društvenim mrežama, igraju onlajn igrice, kockaju se i klade, vrlo je verovatno da će to i njihova deca raditi.

Autor, prevashodno, rešenje vidi u podizanje svesti korisnika novih tehnologija kroz upoznavanje sa velikim brojem bezbednosnih primera iz prakse.

Svest o informacionoj bezbednosti je isto toliko važna, kao i bilo koja bezbednosna tehnika ili procedura koja može biti zloupotrebljena, pogrešno interpretirana ili je krajnji korisnici ne koriste, tako da se gubi njena prava korisnost.

CITIRANA DELA

Abagnale, F. (2019). *Never do these 2 things because 'that's 98% of me stealing your identity'.* https://finance.yahoo.com/news/frank-abagnale-it-only-takes-2-pieces-of-information-to-steal-98-of-your-identity-142210933.html?guccounter=1

Adejn, E. (2019). *Plavi kit: Šta je istina o onlajn „samoubilačkom izazovu“*. https://www.bbc.com/serbian/lat/svet-47672762

Associated Press. (2019). *Germany arrests 3 in the 'Wall Street Market' darknet probe.* https://nypost.com/2019/05/03/germany-arrests-3-in-wall-street-market-darknet-probe/

AVAST. (2019). *Avast Discovers Security Flaws in Widespread GPS Trackers Exposing Locations of Over Half a Million Children and Elderly* https://press.avast.com/avast-discovers-security-flaws-in-widespread-gps-trackers-exposing-locations-of-over-half-a-million-children-and-elderly

Badshah, N. (2019). *Saudis hacked Amazon chief Jeff Bezos's phone, says company's security adviser*. https://www.theguardian.com/technology/2019/mar/31/saudis-hacked-amazons-jeff-bezos-phone-claims-security-chief-jamal-khashoggi-mohammed-bin-salman

Bartz, D. (2019). Google's YouTube to pay $170 million penalty for collecting data on kids https://www.reuters.com/article/us-google-ftc/googles-youtube-to-pay-170-million-penalty-for-collecting-data-on-kids-idUSKCN1VP1RR

Bastone, N. (2019). *Google says the built-in microphone it never told Nest users about was 'never supposed to be a secret'.* https://www.businessinsider.com/nest-microphone-was-never-supposed-to-be-a-secret-2019-2

BBC. (2014.a). *Barack Obama's credit card 'declined'.* http://www.bbc.com/news/world-us-canada-29664831

BBC. (2019.b). *Russia bans smartphones for soldiers over social media fears.* https://www.bbc.com/news/world-europe-47302938

Blic. (2014). *DRŽIMO SRBIJU U ŠACI Hakeri tvrde da su ukrali JMBG "gotovo svih građana"* https://www.blic.rs/vesti/drustvo/drzimo-srbiju-u-saci-hakeri-tvrde-da-su-ukrali-jmbg-gotovo-svih-gradana/j59315x

Carey, B. (2019). *In Month After '13 Reasons Why' Debut on Netflix, Study Finds Teen Suicide Grew.* https://www.nytimes.com/2019/04/29/health/13-reasons-why-teen-suicide.html

Carrie Wong, J. (2019, 01 30). *Facebook posts record profit despite year of scandal.* https://www.theguardian.com/technology/2019/jan/30/facebook-fourth-quarter-profits-revenues-earnings

Carrie Wong, J. (2019b, 09 05). *Facebook confirms 419m phone numbers exposed in latest privacy lapse*. https://www.theguardian.com/technology/2019/sep/04/facebook-users-phone-numbers-privacy-lapse

Castello, J. (2019). *New study finds that 74% have been harassed in online multiplayer games*. https://www.rockpapershotgun.com/2019/07/27/new-study-finds-that-74-have-been-harassed-in-online-multiplayer-games/

CBR. (2019). *Trend Micro Admits it Was Hacked, Symantec Denies Claims of "Fxmsp" Breach.* https://www.cbronline.com/news/trend-micro-symantec-fxmsp

Chaparadza, A. (2019, 09 13). *New SIM Card Flaw Lets Hackers Hijack Any Phone Just By Sending SMS, 1 Billion Phones At Risk.* https://www.techzim.co.zw/2019/09/new-sim-card-flaw-lets-hackers-hijack-any-phone-just-by-sending-sms-1-billion-phones-at-risk/

Conger, K. (2019). *Twitter C.E.O. Jack Dorsey's Account Hacked.* https://www.nytimes.com/2019/08/30/technology/jack-dorsey-twitter-account-hacked.html?smid=tw-nytimes&smtyp=cur

Constine, J. (2019, 07 25). *Facebook pays teens to install VPN that spies on them.* https://www.techradar.com/news/johannesburg-ransomware-attack-leaves-city-without-power?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

CORDIS. (2019). *Study finds users who leave Facebook are happier, but less informed.* https://phys.org/news/2019-02-users-facebook-happier.html

Cuthbertson, A. (2019). *Football live stream: Free Premier League links spreading online could 'wreak havoc'* https://www.independent.co.uk/sport/football/premier-league-live-stream-free-watch-reddit-football-fixtures-a9050316.html

Dimitrova, E. (2019). *17-Year Old Bug in Firefox Allows Local Files Theft Attacks.* https://sensorstechforum.com/17-year-old-bug-firefox-local-files-theft/

Doffman, Z. (2019). *New Android Warning: 500 Million Users Have Installed Apps Hiding Devious Malware—Uninstall Now.* https://www.forbes.com/sites/zakdoffman/2019/09/20/new-android-warning-500m-users-have-installed-apps-hiding-nasty-malwareuninstall-now/?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19#70c4e6c212be

Dough, C. (2019). A mom found videos on YouTube Kids that gave children instructions for suicide https://edition.cnn.com/2019/02/25/tech/youtube-suicide-videos-trnd/index.html

Ejdus, F., Unijat, J., Milošević M. (2009). Istraživanje i podizanje nivoa bezbednosne kulture mladih, http://www.bezbednost.org/Svi-projekti/700/Istrazivanje-i-podizanje-nivoa-bezbednosne.shtml#sthash.IRucHXPn.dpuf

Fisher, C. (2019a). 85 percent of Chrome apps and extensions lack a privacy policy. https://www.engadget.com/2019/02/22/chrome-app-extension-security-flaws/?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Fisher, C. (2019b). *Two-thirds of online gamers in the US experience 'severe' harassment.* https://www.engadget.com/2019/07/25/adl-harassment-online-gaming-survey/?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Gambling. (2017). Young people and gambling 2017. http://live-gamblecom.cloud.contensis.com/PDF/survey-data/Young-People-and-Gambling-2017-Report.pdf

Georg, M. (2019). *NY School Delays Start of Year After Ransomware Attack*. https://www.nbcnewyork.com/news/local/NY-School-Delays-Start-of-Year-After-Ransomware-Attack-559322971.html

Gudmen, M. (2017). *Zločini budućnosti*. Laguna, Beograd

Hart, B. (2019). Consider this before you share your kids' photos on social media without their consent. https://www.abc.net.au/life/sharing-photos-of-your-children-on-social-media-without-consent/10798576

Hern, A. (2019, 08 13). *Facebook admits contractors listened to users' recordings without their knowledge.* https://www.theguardian.com/technology/2019/aug/13/facebook-messenger-user-recordings-contractors-listening

Huggler, J. (2016, 09 14). *Austrian teenager sues parents for 'violating privacy' with childhood Facebook pictures.* https://www.telegraph.co.uk/news/2016/09/14/austrian-teenager-sues-parents-for-violating-privacy-with-childh/

Informacija, 26.5.2016., Uprkos rekordnom broju infekcija, korisnici još uvek ne znaju šta je ransomware. https://www.informacija.rs/Vesti/Uprkos-rekordnom-broju-infekcija-korisnici-jos-uvek-ne-znaju-sta-je-ransomware.html

ISBuzz News. (2019). *125 New Flaws Found In Routers And NAS Devices From Popular Brands.* https://www.informationsecuritybuzz.com/expert-comments/125-new-flaws-found-in-routers-and-nas-devices-from-popular-brands/

Keach, S. (2018). *Super Mario Odyssey porn warning as hackers add smutty pics into Nintendo Switch game.* https://www.thesun.co.uk/tech/6616353/super-mario-odyssey-porn-nintendo-switch-hacker-pictures/

Kelly, G. (2019). Apple iOS 13 Is Full Of Bugs, Reports Warn. https://www.forbes.com/sites/gordonkelly/2019/09/19/apple-ios13-upgrade-problems-iphone-11-pro-max-xs-max-xr-update/#6a23afa322bc

Kelly, M. (2019). *FTC hits Facebook with $5 billion fine and new privacy checks.* https://www.theverge.com/2019/7/24/20707013/ftc-facebook-settlement-data-cambridge-analytica-penalty-privacy-punishment-5-billion

Khandelwal, S. (2018, 01 29). *Heat Map Released by Fitness Tracker Reveals Location of Secret Military Bases.* https://thehackernews.com/2018/01/strava-heatmap-location-tracking.html

Khandelwal, S. (2019a). *Over 40 Drivers Could Let Hackers Install Persistent Backdoor On Windows PCs*. https://thehackernews.com/2019/08/windows-driver-vulnerability.html

Khandelwal, S. (2019b). *Some D-Link and Comba WiFi Routers Leak Their Passwords in Plaintext.* https://thehackernews.com/2019/09/router-password-hacking.html

Khandelwal, S. (2019c). *Smominru Botnet Indiscriminately Hacked Over 90,000 Computers Just Last Month.* https://thehackernews.com/2019/09/smominru-botnet.html

Kroll, L., & Dolan, A. (2019). *BillionaireS*. https://www.forbes.com/billionaires/#73e2013b251c

Landsverk, G. (2019). *Trump says 'gruesome and grisly video games' are to blame for mass violence, but the reality is more complicated.* https://www.insider.com/do-video-games-cause-mass-violence-not-according-to-research-2019-8

Lee, D. (2019). https://www.bbc.com/news/technology-46998055

Lee, T. (2018). *Despite Privacy Uproar, Facebook Users Aren't Changing Their Privacy Settings.* https://www.ubergizmo.com/2018/04/facebook-users-not-changing-privacy-settings/

Leković, J. (2013). *Život nije igra.* http://zivotnijeigra.com/zivotnijeigra/wp-content/uploads/2013/01/REZULTATI-ZA-KONFERENCIJU-NOVINARI-2.pdf

Lo, S., M. (2015). *Prvo razmisli – borba protiv digitalnog nasilja.* http://www.mpn.gov.rs/prvo-razmisli-borba-protiv-digital/

Lyons, K. (2019, 03 29). *Apple Martin tells off mother Gwyneth Paltrow for sharing photo without consent.* https://www.theguardian.com/film/2019/mar/29/apple-martin-tells-mother-gwyneth-paltrow-off-for-sharing-photo-without-consent

Mangan, L. (2016, 09 17). *I don't put pictures of my children on Facebook - and you shouldn't either.* https://www.telegraph.co.uk/family/parenting/i-dont-put-pictures-of-my-children-on-facebook---and-you-shouldn/

Mathews, L. (2019). *Elite Russian Hackers Claim To Have Breached Three Major U.S. Antivirus Makers.* https://www.forbes.com/sites/leemathews/2019/05/09/russian-hackers-breach-antivirus-makers/#7550a2c11db2

Ng, A. (2019). Facebook still tracks you after you deactivate account. https://www.cnet.com/news/facebook-is-still-tracking-you-after-you-deactivate-your-account/?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Ostojić, T. (2018). *U Srbiji preko 50% kompjuterski nepismenih.* https://pcpress.rs/u-srbiji-preko-50-kompjuterski-nepismenih/

Paganini, P. (2015). *New Intel Security study shows that 97% of people can't identify phishing emails*, https://securityaffairs.co/wordpress/36922/cyber-crime/study-phishing-emails-response.html

Palmer, D. (2019). *PC security warning: That out-of-date software is putting you at risk.* https://www.zdnet.com/article/pc-security-warning-that-out-of-date-software-is-putting-you-at-risk/

PC Press. (2019). *Svaka treća mlada osoba u Srbiji trpi digitalno nasilje.* https://pcpress.rs/svaka-treca-mlada-osoba-u-srbiji-trpi-digitalno-nasilje/

Porter, J. (2019a). *Google fined €50 million for GDPR violation in France.* https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil

Porter, J. (2019b, 02 21). *WinRAR patches 19-year-old security vulnerability that put millions at risk*. https://www.theverge.com/2019/2/21/18234448/winrar-winace-19-year-old-vulnerability-patched-version-5-70-beta-1?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Porter, J. (2019c). *Facebook admits harvesting 1.5 million people's email contacts without consent.* https://www.theverge.com/2019/4/18/18485089/facebook-email-password-contacts-upload-1-5-million-security-cybersecurity?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Ross, A. & Leonard, B. (2019, 06 28). *Ransomware attacks put Florida governments on alert.* https://www.tampabay.com/florida-politics/buzz/2019/06/28/ransomware-attacks-put-florida-governments-on-alert/

Saviano, R. (2019). *Roberto Saviano and Edward Snowden: "I'm fighting for the Internet to be free again. Zuckerberg? He'll repent".* https://www.repubblica.it/esteri/2019/09/13/news/roberto_saviano_edward_snowden_intervi ew-235883649/

Schneier, B. (2015). *RM Education*, https://www.rm.com/support/technicalarticle.asp?cref=tec377232

Schwartz, M. (2019). *Apple iPhones Hacked by Websites Exploiting Zero-Day Flaws,* https://www.bankinfosecurity.com/apple-iphones-hacked-by-websites-exploiting-zero-day-flaws-a-13001

Sputnik International. (2019, 09 14) *Go West? Edward Snowden Hopes France's Emmanuel Macron Will Approve His Asylum Application.* https://sputniknews.com/europe/201909141076804460-go-west-edward-snowden-hopes-frances-emmanuel-macron-will-approve-his-asylum-application/

Stevens, K. (2019). *Children as young as 10 are using sophisticated cyber-attacks to take out opponents on online gaming sensation Fortnite.* https://www.dailymail.co.uk/news/article-6738141/NSW-children-young-10-using-sophisticated-cyber-attacks-opponents-Fortnite.html?utm_medium=email&utm_source=flipboard

Stone, J. (2019). *Google's Triada backdoor demonstrates vulnerabilities in the mobile supply chain.* https://www.cyberscoop.com/android-backdoor-triada-mobile-supply-chain/

Tech Crunch, 29.1.2019.b, https://techcrunch.com/2019/01/29/facebook-project-atlas/

Teiss. (2019.b, 01 21). *15 fake navigation apps on Google Play Store enjoyed 50m downloads.* https://www.teiss.co.uk/fake-navigation-apps-play-store/

Teiss. (2019a, 01 31). *Fake beauty apps on Google Play Store enjoyed millions of downloads.* https://www.teiss.co.uk/fake-beauty-apps-play-store/

Thubron, R. (2019, 09 19). *RuneScape player spends $62,000 on microtransactions.* https://www.techspot.com/news/81968-runescape-player-spends-62000-game-microtransactions.html

Turner, G. (2019). *The Data Big Tech Companies Have On You (Or, At Least, What They Admit To).* https://securitybaron.com/blog/the-data-big-tech-companies-have-on-you-or-at-least-what-they-admit-to/

TVC. (2019, 07 16). Ubiystvo sledovatelya Shishkinoy svyazali s delom "darkneta". https://www.tvc.ru/news/show/id/159580

Vincent, J. (2018). *Don't use Huawei phones, say heads of FBI, CIA, and NSA.* https://www.theverge.com/2018/2/14/17011246/huawei-phones-safe-us-intelligence-chief-fears

Wagenseil, T. (2019). *Hackers Say They've Breached Three Antivirus Companies.* https://www.tomsguide.com/us/antivirus-companies-breached,news-30045.html

Wei, W. (2019). *Hacker Stole Data of Over 70% Bulgarian Citizens from Tax Agency Servers.* https://thehackernews.com/2019/07/bulgaria-nra-data-breach.html

Wei, W. (2019b). *Multiple Code Execution Flaws Found In PHP Programming Language.* https://thehackernews.com/2019/09/php-programming-language.html

Whittaker, Z. (2019, 08 29). *Malicious websites were used to secretly hack into iPhones for years, says Google.* https://techcrunch.com/2019/08/29/google-iphone-secretly-hacked/

Winder, D. (2019). *Windows Users Warned To Update Now As 'Complete Control' Hack Attack Confirmed.* https://www.forbes.com/sites/daveywinder/2019/08/24/windows-users-warned-to-update-now-as-complete-control-hack-attack-confirmed/?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19#31d9f5f45bdb

Wodinsky, S. (2018). *Many Android devices ship with firmware vulnerabilities, researchers find.* https://www.theverge.com/2018/8/10/17677206/android-devices-firmware-security-flaws-kryptowire?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Datum prve prijave: 26.08.2019.
Datum prijema korigovanog članka: 07.09.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Milanović, Z. (2019, 10 15). Zloupotreba novih tehnologija i digitalno nasilje. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 86-98. doi:10.12709/fbim.07.07.02.10

Style – Chicago Sixteenth Edition:

Milanović, Zoran. 2019. "Zloupotreba novih tehnologija i digitalno nasilje." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 86-98. doi:10.12709/fbim.07.07.02.10.

Style – GOST Name Sort:

Milanović Zoran Zloupotreba novih tehnologija i digitalno nasilje [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 86-98.

Style – Harvard Anglia:

Milanović, Z., 2019. Zloupotreba novih tehnologija i digitalno nasilje. *FBIM Transactions,* 15 10, 7(2), pp. 86-98.

Style – ISO 690 Numerical Reference:

Zloupotreba novih tehnologija i digitalno nasilje. **Milanović, Zoran.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 86-98.