Stručni rad

# JUICE JACKING

Jasminka Belščak, mag. inf., izvrsna savjetnica, OŠ Petrijanec
mr. sc. Tamara Ređep, izvrsna savjetnica, I. OŠ Varaždin

**Sažetak**

U istraživačkom radu na temu „Juice Jacking – stavovi učenika o korištenju javnih USB stanica za punjenje“ su prikazani rezultati ankete provedene među učenicima 5. do 8. razreda osnovne škole tijekom studenog 2024. godine. Cilj ankete je bio saznati poznaju li učenici cyber napad Juice Jacking (JJ), koriste li i na koji način javne USB stanice za punjenje te jesu li zabrinuti i osviješteni oko sigurnosnih rizika povezivih s uporabom javnih USB stanica za punjenje.

**Ključne riječi:** Juice Jacking (JJ), cyber napad, Universal Serial Bus (USB), istraživanje, anketa, učenici

# 1. Uvod

Pametni telefoni, tablet i prijenosna računala te drugi osobni uređaji koji pripadaju u informacijsko komunikacijske tehnologije (IKT) koriste se svakodnevno ne samo u poslovne svrhe već i kao uređaji za učenje te za privatne potrebe. Ukoliko uređaje koriste djeca, učenici, oni ih najčešće pune kod kuće ili u školi. No, zbog specifičnosti provedbe izvanučioničke i terenske nastave, ali i zbog boravka izvan kuće i van škole, ponekad se može dogoditi da se baterija uređaja isprazni. Upravo je to razlog zašto ponekad postoji potreba za punjenjem uređaja izvan sigurnog, kućnog ili školskog okruženja. Obzirom kako učenici ne nose uvijek punjače svojih uređaja, u situacijama kada se baterija isprazni, postoji mogućnost da će IKT uređaj uključiti u dostupnu javnu Universal Serial Bus (USB) stanicu za punjenje.

USB se ne koristi samo za punjenje IKT uređaja i tzv. gadgeta, već i za komunikaciju. Međutim, prijenos podataka između uređaja putem USB-a sklon je raznim sigurnosnim prijetnjama te je tijekom prijenosa potrebno održavati povjerljivost i osjetljivost podataka kako bi se održao integritet [3]. Upravo zbog jednostavnosti prijenosa podataka putem USB-a, s vremenom je razvijena nova vrsta cyber napada nazvana Juice Jacking (JJ).

Pretraživanjem dostupne literature uočile smo kako o JJ u dostupnim bazama podataka nedostaje stručne literature te kako na području Republike Hrvatske nema istraživanja o sigurnosnim rizicima korištenja javnih USB stanica za punjenje. Uzimajući u obzir ove činjenice, pitanje koje smo istražile je: „Jesu li učenici upoznati s Juice Jacking i sigurnosnim rizicima korištenja javnih USB stanica za punjenje?“

# 2. Teorijska pozadina, metodologija istraživanja i rezultati

## 2.1. Osnovno o JJ

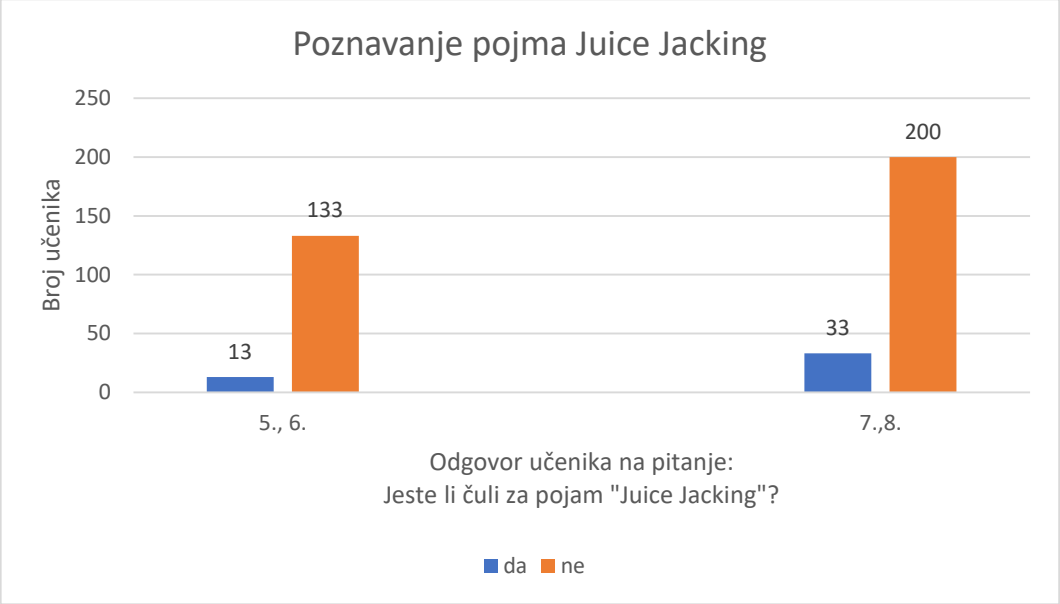
JJ je cyber napad tj. metoda krađe podataka putem USB kabla za punjenje. Ovom metodom napadač jednostavno krade sve podatke s mobilnog telefona ili drugog IKT uređaja spojenog na USB. Ukradeni podatci mogu sadržavati osobne stvari, podatke za kontakt, bankovne podatke, lozinke, kolačiće preglednika i druge važne podatke [2]. Takvi se podatci mogu koristiti u razne nelegalne svrhe poput krađe identiteta, elektroničkog nasilja ili financijskih otuđivanja.

## 2.2. Metodologija istraživanja i dobiveni rezultati

U ovom istraživačkom radu korištena je metoda namjernog uzorka. Prema dostupnim podatcima na eRudniku, osnovnu školu polazi 153492 učenika od 5. do 8. razreda [5]. Istraživanje je provedeno pomoću anonimnog online anketnog upitnika kojem je pristupilo 379 učenika od 5. do 8. razreda osnovnih škola iz Varaždinske, Zadarske i Zagrebačke županije: 54 učenika 5. razreda, 92 učenika 6. razreda, 114 učenika 7. razreda i 119 učenika 8. razreda. Ukoliko je razina pouzdanosti 95% tada je margina greške 5%, a ukoliko je razina pouzdanosti 90% margina greške tada iznosi 4.2%.

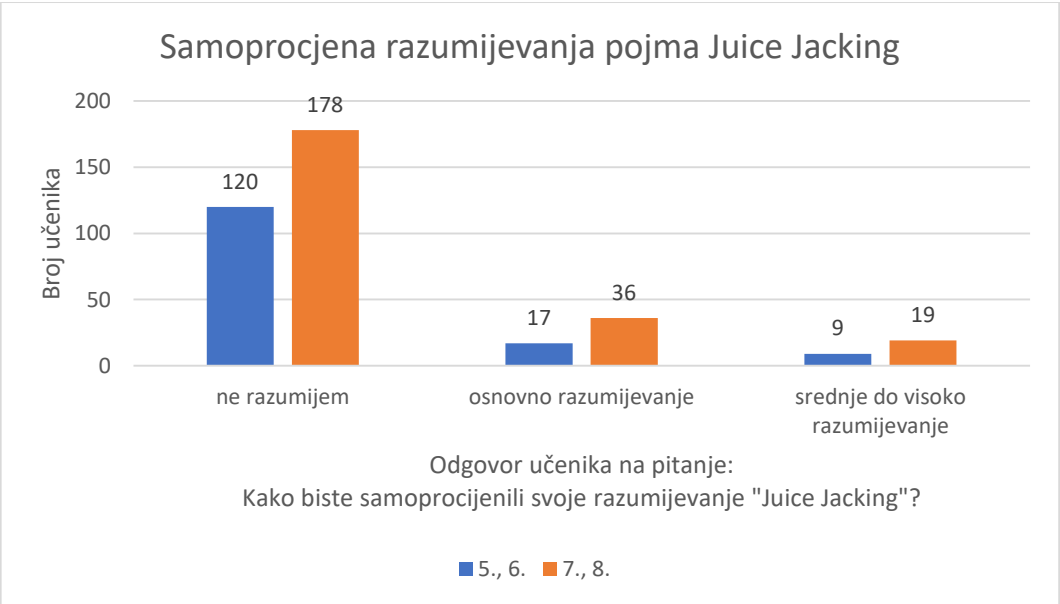
### 2.2.1. Poznavanje pojma JJ

Većini učenika osnovnih škola pojam JJ je nepoznat, no s većim se uzrastom nepoznavanje smanjuje. Slika 1. prikazuje kako je svega 9.77% učenika 5. i 6. razreda osnovne škole čulo za pojam JJ, dok se taj postotak za učenike 7. i 8. razreda povećao na 16.5%.




Slika 1. Poznavanje pojma Juice Jacking

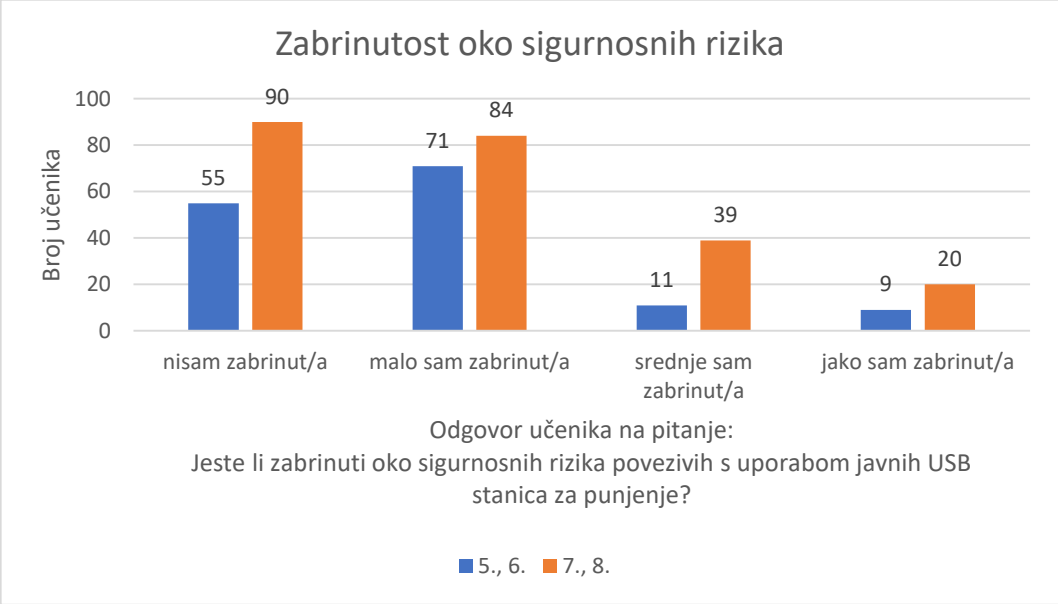
Razumijevanje pojma JJ također se povećava povećanjem uzrasta kao što je prikazano na Slici 2. Zabrinjavajuće je da 78.63% sveukupnog broja učenika predmetne nastave tj. 5.-8. razreda osnovne škole, ne razumije što je JJ. 82.19% učenika 5. i 6. razreda ne razumije pojam, a 7. i 8. razreda 76.39%. Osnovno razumijevanje pojma samoprocijenilo je 11.64% učenika 5. i 6. razreda, a 15.45% učenika 7. i 8. razreda. Srednje i visoko razumijevanje pojma, prema samoprocjeni učenika, iskazalo je 6.16% učenika 5. i 6. razreda te 8.15% učenika 7. i 8. razreda.




Slika 2. Samoprocjena razumijevanja pojma Juice Jacking

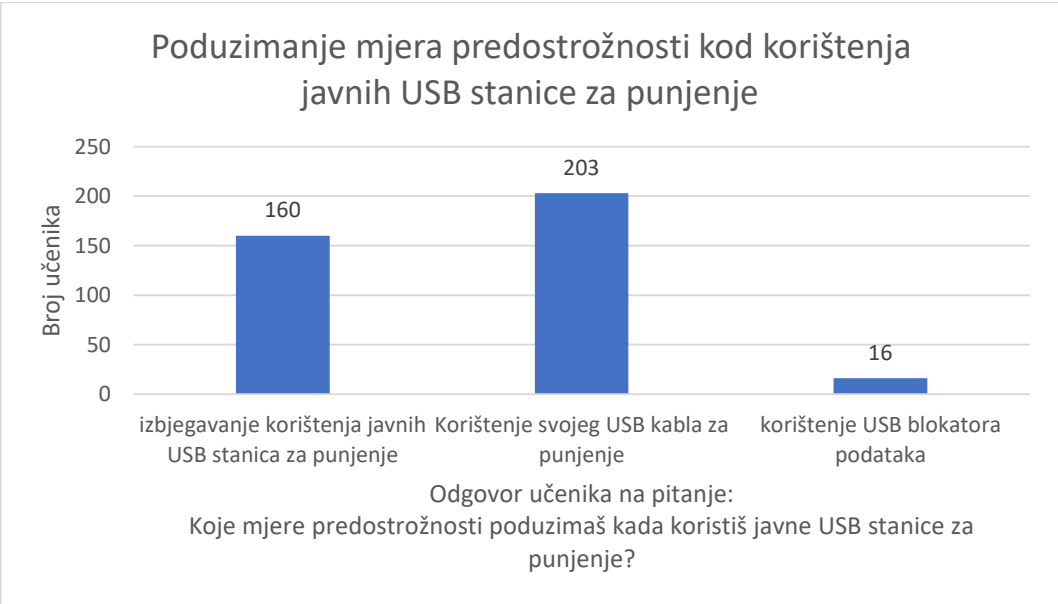
### 2.2.2. Korištenje javnih USB stanica za punjenje

Većina učenika nikada ili jako rijetko koristi javne USB stanice za punjenje, no 13.72% ih koristi često ili gotovo uvijek. Najčešće pune svoje pametne telefone, rjeđe pametne satove, a ponekad i tablet uređaje. Ukupno 86.3% učenika 5. i 6. razreda nije ili je malo zabrinuto oko sigurnosnih rizika povezivih s uporabom javnih USB stanica za punjenje, dok ih je 13.7% srednje do jako zabrinuto. Većim uzrastom povećava se i ova zabrinutost kao što je prikazano na Slici 3. 74.68% učenika 7. i 8. razreda nije ili je malo zabrinuto, dok ih je 25.32% srednje do jako zabrinuto.




Slika 3. Zabrinutost oko sigurnosnih rizika

Iako učenici većinom nisu zabrinuti oko sigurnosnih rizika povezivih s uporabom javnih USB stanica za punjenje, ukoliko ih koriste poduzimaju mjere predostrožnosti te upotrebljavaju svoj USB kabel za punjenje. Svega 4.22% učenika u tim situacijama koristi USB blokator podataka što je vidljivo na Slici 4.



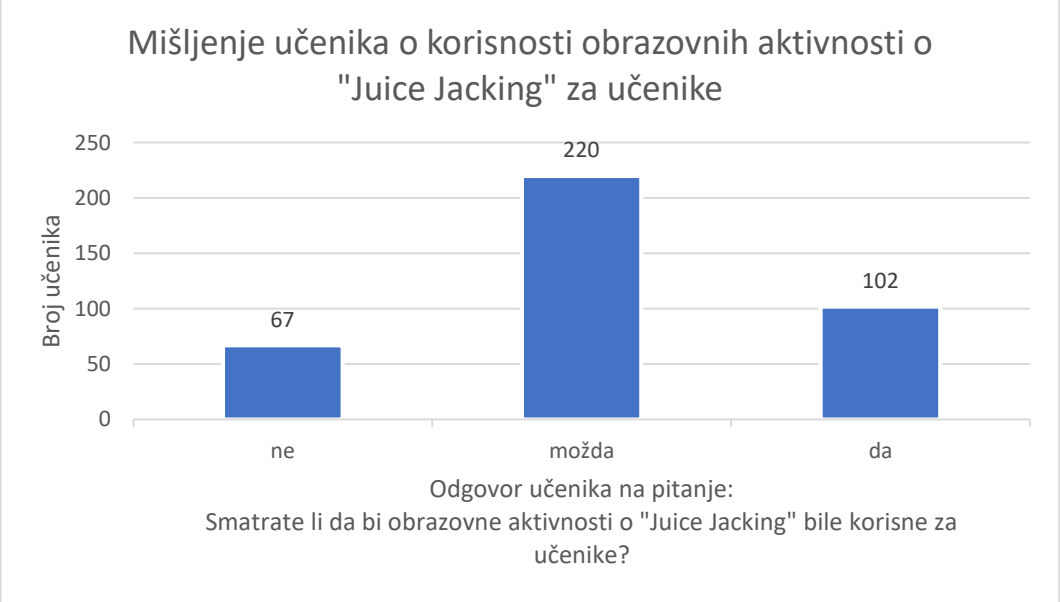

Slika 4. Poduzimanje mjera predostrožnosti

### 2.2.3. Mjere za poboljšanje sigurnosti

U anketnom je upitniku postavljeno pitanje otvorenog tipa „Koje mjere bi, prema Vašem mišljenju, trebalo primijeniti kako bi se poboljšala sigurnost javnih USB stanica za punjenje?“ te su učenici mogli sami predlagati svoje odgovore. Čak 68.3% učenika nije napisalo ni jedan prijedlog, a 31,7% napisalo je svoje prijedloge. Kvalitativnom analizom dolazi se do zaključka kako učenici predlažu ove sigurnosne mjere:

- ukinuti i zabraniti javne USB stanice za punjenje
- izbjegavati takva mjesta
- imati svoj punjač ili svoj kabel
- nositi sa sobom i koristiti svoj Power Bank (prijenosnu bateriju)
- ugraditi vatrozid ili neki drugi sigurnosni program na svoj uređaj

Obzirom kako je dio učenika, 12.14%, čulo za pojam JJ, te da 21.37% učenika samoprocijenjuje svoje razumijevanje pojma JJ na osnovnoj, srednjoj ili visokoj razini, rezultati prikazani na Slici 5. su očekivani. Samo 17.68% učenika smatra kako obrazovne aktivnosti o JJ nisu potrebne i kako ne bi bile korisne za učenike.




Slika 5. Mišljenje učenika o korisnosti obrazovnih aktivnosti o JJ za učenike

## 2.3. Diskusija i ograničenja

Nedostatak literature kao i do sada provedenih istraživanja onemogućuje usporedbu dobivenih rezultata s rezultatima drugih istraživanja. Stoga se predlaže u budućnosti ponoviti istraživanje s učenicima iz drugih županija Republike Hrvatske. Kako bi rezultati bili relevantniji, istraživanje bi se moglo provesti i izvan Republike Hrvatske. Obzirom kako je za ovo istraživanje odabrana metoda namjernog uzorka, preporuča se u budućnosti, zbog objektivnosti prikupljanja rezultata, primjena slučajnog uzorkovanja. Prepoznata je i potreba dublje statističke analize dobivenih rezultata te ujednačenje veličine uzoraka učenika 5.-8. razreda.

# 3. Kako prepoznati JJ i prijedlog sigurnosnih mjera

Korisnik uređaja opažanjem može uočiti osnovne znakove ugroženosti uređaja napadnutog JJ cyber napadom:

- porast povremene uporabe podataka
- brzo tj. neuobičajeno pražnjenje baterije
- primljena upozorenja o krađi identiteta
- postojanje neželjenih aplikacija [1]

Kako bi korisnici uređaja, u ovom primjeru učenici 5.-8. razreda osnovnih škola, bili više zaštićeni od cyber napada JJ, preporuča se uvođenje dodatnih mjera zaštite. Osim tehnološkog ujedno i financijskog ulaganja u USB blokator podataka, prioritet se treba postaviti na obrazovanje i podizanje osviještenosti o postojanju i rizicima koje donosi JJ. Pružanjem jasnih informacija o prepoznavanju pokušaja napada JJ, sigurnim online praksama i prijavljivanjem sumnjivih aktivnosti, korisnici, učenici, učitelji, roditelji, mogu osnažiti te tako imati aktivnu ulogu u zaštiti svojih podataka. Stoga je nužno učenicima pružiti razne obrazovne aktivnosti, predložiti literaturu, prikazati primjere iz prakse kibernetičke sigurnosti. Na taj način bi se učenike educiralo o sigurnosnim mjerama, smanjujući njihov rizik da postanu žrtve prijevara [4].

# 4. Zaključak

Nakon analize provedenog anonimnog upitnika baziranog na istraživačkom pitanju „Jesu li učenici upoznati s Juice Jacking i sigurnosnim rizicima korištenja javnih USB stanica za punjenje?“ mogu se zaključiti ove činjenice:

- većina učenika 5.-8. razreda osnovne škole ne poznaje i ne razumije pojam JJ
- većina učenika 5.-8. razreda osnovne škole nije zabrinuta oko sigurnosnih rizika povezivih s uporabom javnih USB stanica za punjenje
- većina učenika 5.-8. razreda osnovne škole smatra kako su obrazovne aktivnosti o JJ potrebne i korisne za učenike

# 5. Popis literature

[1.] Odey JA, Ola B, Agbonlahor I. (2021). The Cyber Crime of Juice Jacking in Developing Economies: Susceptibilities, Consequences and Control Measures. Eur J Inf Technol Comput Sci. 1(5):1–5.
[2.] Sanwal S, Singh K. (2020). Juice Jacking-A type of Cyber Attack. Cybernomics. 2(1):25–8.
[3.] Singh D, Biswal AK, Samanta D, Singh D, Lee HN. (2022). Juice Jacking: Security Issues and Improvements in USB Technology. Sustain. 14(2):1–17.
[4.] Yoganandham G. (2024). Economic risks in the digital era with special reference to cyber fraud, social media, impersonation, juice jacking , data theft and lottery scams - a theoretical assessment. XIII(X):7–25.
[5.] Školski e-Rudnik. URL: ŠeR - Školski e-Rudnik - gov.hr (28.12.2024.)