SIGURNOSNI RIZICI KORIŠTENJA DIGITALNIH TEHNOLOGIJA U E-UPRAVI

Stručni rad

Tea Livaić, mag. oec.[1]

dr. sc. **Ivan Livaja**, v. pred.[2]

Marko Pavelić, mag. ing. inf. et comm. techn., pred.[3]

U digitalnoj transformaciji javnih institucija, implementacija e-uprave postaje ključna za unaprjeđenje interakcije građana s vladom. Sustav e-Građani u Hrvatskoj predstavlja središnje mjesto za pružanje informacija i usluga javnog sektora, ali istovremeno je izložen raznim cyber prijetnjama, posebice phishing kampanjama. Ovaj rad analizira prijetnje informacijskoj sigurnosti sustava e-Građani, s naglaskom na phishing, kroz pregled sustava, identifikaciju prijetnji i analizu primjera napada. Nadalje, uspoređuju se primjeri phishinga iz drugih europskih zemalja poput Danske i Finske, ističući globalnu prirodu cyber prijetnji. Kroz analizu tih slučajeva, naglašava se važnost sigurnosnih protokola i edukacije korisnika u zaštiti digitalnih javnih usluga.

Ključne riječi: *e-Građani, e-uprava, informacijska sigurnost, phishing, cyber prijetnje*

[1] Tea Livaić, mag. oec., Veleučilište u Šibeniku, Trg Andrije Hebranga 11, 22000 Šibenik, e-mail: tea.livaic@vus.hr

[2] Dr. sc. Ivan Livaja, v. pred., Veleučilište u Šibeniku, Trg Andrije Hebranga 11, 22000 Šibenik , e-mail: ivan.livaja@vus.hr

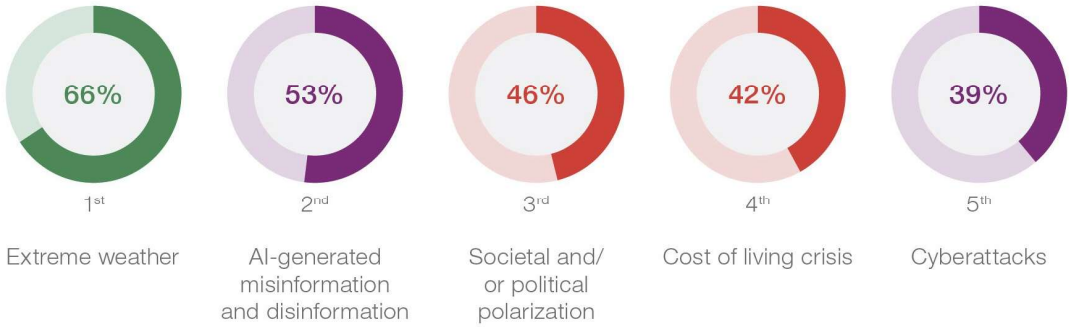
[3] Marko Pavelić, mag. ing. inf. et comm. techn., pred., Veleučilište u Šibeniku, Trg Andrije Hebranga 11, 22000 Šibenik, e-mail: marko.pavelic@vus.hr

1. UVOD

Informacijska sigurnost sustava javnih institucija predstavlja ključan aspekt u digitalnoj transformaciji modernih državnih sustava. U eri digitalizacije i tehnološkog napretka 21. stoljeća, sve više se pažnje posvećuje implementaciji e-uprave kako bi se modernizirale vlade i omogućila bolja interakcija građana s javnim sektorom. Sustav e-Građani, kao integralni dio e-uprave, predstavlja središnje mjesto za sve informacije i usluge javnog sektora u Hrvatskoj (e-Građani, 2024). Kroz pružanje bolje isporuke državnih usluga građanima, unaprijeđenu interakciju s poduzećima te osnaživanje građana putem pristupa informacijama, sustav e-Građani nastoji učiniti interakciju s vladom praktičnijom, transparentnijom i jeftinijom.

Međutim, isto tako važno je naglasiti da se informacijska sigurnost sustava e-Građani nameće kao imperativ u tom procesu. Zaštita privatnosti podataka, prevencija cyber napada i osiguranje pouzdanosti informacijske infrastrukture postaju ključni elementi u održavanju povjerenja građana u sustav e-uprave. Prema istraživanju provedenom u Global Risks Reportu za 2024. godinu ukazuje na informacijsku sigurnost kao ključni faktor u suzbijanju globalnih prijetnji. S obzirom na to da cyber napadi zauzimaju značajno mjesto među pet najvjerojatnijih rizika. Nadalje, kriza troškova života (42%) i cyber napadi (39%) ostaju glavne brige u općem izgledu i pojavljuju se kao jedna od tri najvažnije brige za vladine i privatne sektorske sudionike.

Slika 1. Globalni rizici



Izvor: Global Risks Report 2024, World Economic Forum

Prednosti povezane s e-upravom ogledaju se ne samo u poboljšanoj koordinaciji politika i efikasnijoj dostavi usluga, već i u osiguravanju visokih standarda informacijske sigurnosti. Implementacija sigurnosnih protokola, kontinuirano praćenje ranjivosti sustava te educiranje korisnika postaju neophodni koraci u očuvanju integriteta i pouzdanosti sustava e-Građani.

Cilj ovog rada je istražiti i analizirati prijetnje informacijskoj sigurnosti sustava e-Građani, posebice fokusirajući se na phishing kampanje. Kroz pregled sustava e-Građani, identifikaciju prijetnji te analizu primjera phishing napada u Hrvatskoj i drugim europskim zemljama poput Danske i Finske, cilj je pružiti dublje razumijevanje izazova s kojima se suočavaju javne institucije u digitalnom okruženju. Kroz ovo istraživanje, želimo doprinijeti unapređenju svijesti o cyber prijetnjama te potaknuti daljnje napore u osiguravanju sigurnosti digitalnih platformi javne uprave.

2. PREGLED SUSTAVA E-GRAĐANI

Projekt Vlade RH (Ministarstvo uprave, 2013, str. 3) kojim se želi omogućiti komunikacija građana s javnim sektorom na jednom mjestu na internetu, putem portala koji će objediniti informacije o radu Vlade i ministarstava, informacije o javnim uslugama te omogućiti siguran pristup elektroničkim uslugama

korištenjem elektroničkog identiteta posredstvom jedne ili više prihvatljivih vjerodajnica za elektroničku identifikaciju (npr. Korisničko ime/zaporka, token, digitalni certifikat i sl.). Na portalu e-Građani, 2022. godine bilo je dostupno više od 100 digitalnih javnih usluga. Sustav je u listopadu 2022. imao 1,7 milijuna korisnika što je rast od 30 % u godinu i pol dana. Broj korisnika je porastao zbog redizajna sustava koji je unaprijedio korisničku perspektivu (engl. *user experience*) te korištenje učinio jednostavnijim i intuitivnijim, dok je COVID pandemija primorala sve građane da putem portala e-Građani aktiviraju digitalne COVID propusnice i putne potvrde zbog lakšeg kretanja. Konačno, popisivanje stanovništva u 2021. godine omogućilo je samostalno (digitalno) popisivanje članova kućanstva pa je i to bio motiv za korištenje sustava e-Građana (NN 2/2023).

Portal e-Građani trenutno koristi 1.854.715 građana (Tablica 1.), te su građani od početka rada sustava do danas pristupili više od 97.218.288 puta različitim elektroničkim uslugama od 01.lipnja 2014. do 31 siječnja 2024. godine.

Tablica 1. Korisnici sustava e-Građani po županijama

Naziv Županije	Broj jedinstvenih korisnika[4]	Udjel (%)[5]
Nepoznato	342	0,02%
Ličko-senjska	16.810	0,91%
Požeško-slavonska	23.104	1,25%
Virovitičko-podravska	25.063	1,35%
Bjelovarsko-bilogorska	38.081	2,05%
Šibensko-kninska	38.130	2,06%
Koprivničko-križevačka	41.185	2,22%
Karlovačka	44.325	2,39%
Međimurska	46.837	2,53%
Brodsko-posavska	49.572	2,67%

[4] Broj jedinstvenih korisnika - broj e-Građana koji su se barem jednom autentificirali kroz NIAS na neku od e-usluga, pri čemu se županija određuje prema mjestu prebivališta korisnika.
[5] Udjel (%) - omjer broja korisnika u pojedinoj županiji u odnosu na ukupni broj svih korisnika.

Dubrovačko-neretvanska	51.659	2,79%
Krapinsko-zagorska	54.388	2,93%
Vukovarsko-srijemska	54.730	2,95%
Sisačko-moslavačka	57.575	3,10%
Zadarska	69.337	3,74%
Varaždinska	75.059	4,05%
Istarska	104.030	5,61%
Osječko-baranjska	108.421	5,85%
Zagrebačka	135.186	7,29%
Primorsko-goranska	147.134	7,93%
Splitsko-dalmatinska	192.048	10,35%
Grad Zagreb	481.699	25,97%
UKUPNO	1.854.715	100,00%

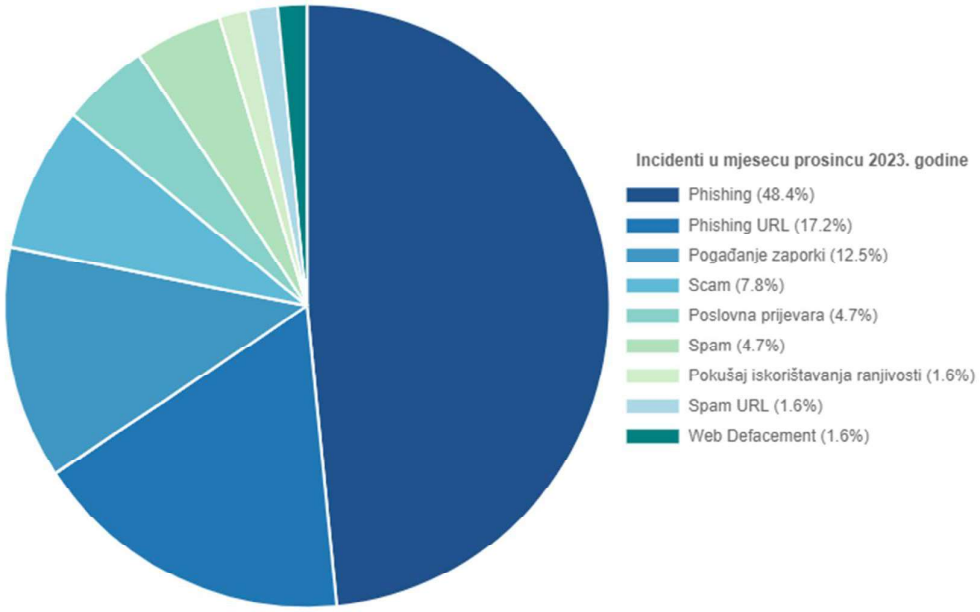
Izvor: Portal otvorenih podataka, https://data.gov.hr/ckan/dataset/e-gradjani-statistika

3. PRIJETNJE INFORMACIJSKOJ SIGURNOSTI U SUSTAVU E-GRAĐANI

Prema izvješću Nacionalnog CERT-a, u veljači 2023. godine primijećene su prijevare putem lažnih e-poruka koje su imitirale sustav e-Građani, s ciljem krađe bankovnih podataka. U tim porukama se obećavala novčana pomoć, a žrtvama se sugeriralo da skeniraju QR kod koji ih je vodio na lažnu stranicu za prijavu bankovnih podataka. Napadači su se predstavljali kao Ministarstvo gospodarstva i održivog razvoja te Hrvatski zavod za zdravstveno osiguranje, nudeći lažne financijske pogodnosti kako bi privukli žrtve. Korištenjem QR koda umjesto izravnih poveznica, imitirali su legitimne institucije i usluge te stvarali privid hitnosti kako bi žrtve brzo reagirale. S obzirom na tu prijetnju, dodatne mjere opreza bile su nužne kako bi se zaštitila informacijska sigurnost e-Građani, uključujući provjeru adresa e-pošte, oprez pri primanju neočekivanih financijskih ponuda, izbjegavanje skeniranja QR kodova iz sumnjivih poruka te pažljivo provjeravanje URL adresa prije unošenja osobnih podataka.-

Mail s adrese info@egradani.com predstavljao se kao službeni mail sustava e-Građani, što nije bilo istinito. Primatelje su upozorili da je riječ o prijevari te da ne otvaraju poruku niti koriste poveznice unutar nje. Lažna poruka nudila je nepostojeću pomoć u stanovanju, navodeći lažne zakone i prava. Uključivala je QR kod koji je vodio na lažnu web stranicu sustava e-Građani s domenom e-gradani.web.app, umjesto službene domene gov.hr. Na toj lažnoj stranici simulirano je sučelje za pristupanje korisničkom računu putem vjerodajnica banaka, s potpisom Ministarstva rada, mirovinskoga sustava, obitelji i socijalne politike (e-Građani, 2023).

Slika 2. Statistika računalno-sigurnosnih incidenata prema CERT-u



Izvor: CERT, https://www.cert.hr/statistika/

Phishing (varijanta engleske riječi za pecanje, *fishing*) je vrsta socijalnog inženjeringa koja se odnosi na prijevare u kojima napadač lažnim predstavljanjem i naizgled legitimnim zahtjevom pokušava potencijalnu žrtvu natjerati da učini nešto u njihovu korist. Riječ je o kriminalnoj aktivnosti. Koristeći razne načine manipulacije, kriminalci od korisnika pokušavaju

prikupiti povjerljive podatke (korisnička imena, lozinke, podaci s kreditnih kartica i sl.) kako bi ostvarili financijsku korist. U pravilu, phishing poruke prenose se putem elektroničke pošte koja navodi korisnika da klikne poveznicu koja ga vodi na stranice zlonamjernog Web poslužitelja (CERT, 2023). Napadi poput phishinga ne samo da prijete sigurnosti pojedinaca već i integritetu javnih sustava, uključujući sustav e-Građani. Stoga je važno ne samo educirati građane o rizicima phishinga, već i osigurati sigurnost samih digitalnih platformi, kao što je naglašeno u Strategiji digitalne Hrvatske za razdoblje do 2032. godine. Osim toga, potrebno je kontinuirano nadograđivati protumjere kako bi se ojačala sigurnost digitalnih javnih usluga i spriječili potencijalni napadi na sustav e-Građani.

Prema Strategiji digitalne Hrvatske za razdoblje do 2032. godine, značajan fokus bit će usmjeren na promociju i osiguranje sigurne upotrebe digitalnih javnih usluga. To uključuje edukaciju građana i poslovnih subjekata putem promidžbenih kampanja, društvenih mreža te edukativnih programa. Poseban naglasak bit će na osposobljavanju službenika za upućivanje korisnika na korištenje digitalnih usluga, posebno starijih građana. Cilj iz Strategije, da barem 80 % građana koristi digitalno identifikacijsko sredstvo, također je prioritet. Poticat će se korištenje elektroničke osobne iskaznice (eID) radi omogućavanja pristupa svim funkcionalnostima sustava e-Građani, te korištenje javnog elektroničkog identiteta za gospodarske aktivnosti.

4. PRIMJERI IZ EUROPSKE UNIJE

Prema globalnom izvještaju Ujedinjenih naroda (eng. *United Nations eGovernment Development Survey 2023*) koji sadrži pregled stanja i usporedno prati razvoj e-uprave u 193 države članice UN, Danska se našla na prvom, a Finska na drugom mjestu (Republika Hrvatska je na 44. mjestu). No, čak se i najrazvijenije e-uprave Finske i Danske suočavaju se s problemom phishing kampanja, što ukazuje na globalnu prirodu ove cyber prijetnje.

Danski slučaj phishinga (Faglige Seniorer, 2023)predstavlja složen i sofisticiran napad na korisnike platforme borger.dk, koja pruža širok spektar usluga i informacija građanima Danske. U ovom slučaju, korisnici su primili lažne e-poruke koje su se pretvarale da su službene poruke s borger.dk, navodeći ih da potvrde osobne podatke kako bi očuvali sigurnost svojih korisničkih računa. E-poruke su bile vrlo uvjerljivo oblikovane, s logotipom borger.dk i jezikom koji je bio vrlo sličan pravim porukama s platforme. Kriminalci su koristili manipulativne tehnike kako bi nagovorili korisnike da kliknu na poveznicu koja ih je vodila na lažnu web stranicu, gdje su tražili osjetljive informacije poput osobnih podataka i bankovnih informacija. Ovakve phishing kampanje predstavljaju ozbiljnu prijetnju sigurnosti osobnih podataka građana, stvarajući rizik od krađe identiteta i financijskih gubitaka.

U finskom slučaju (Suomi, 2023), korisnici su također bili ciljani phishingom putem lažnih poruka koje su se predstavljale kao poruke s platforme Suomi.fi, koja pruža digitalne usluge građanima Finske. U ovom slučaju, korisnici su primili poruke koje su ih pozivale da kliknu na poveznicu radi prijave na lažnu web stranicu koja je imitirala Suomi.fi. Ova kampanja phishinga bila je usmjerena na krađu osobnih podataka korisnika, a poruke su bile dizajnirane tako da izgledaju vrlo slično pravim porukama s platforme Suomi.fi. Kao i u danskom slučaju, kriminalci su pokušali iskoristiti manipulaciju i obmanu kako bi prevarili korisnike da otkriju osjetljive informacije, poput osobnih identifikacijskih brojeva i bankovnih podataka. Ova prijetnja naglašava potrebu za jačanjem sigurnosnih mjera i kontinuiranom edukacijom građana o prepoznavanju i sprječavanju phishing kampanja.

5. ZAKLJUČAK

U današnjem digitalnom dobu, sve češće se susrećemo s prijevarama u kojima prevaranti koriste identitet javnih institucija kako bi ostvarili svoje ciljeve. Primjerice, lažne e-poruke koje se predstavljaju kao poruke Porezne uprave mogu

obavijestiti primatelje o navodno odobrenom povratu poreza, ali za isplatu istog potrebno je kliknuti na sumnjive poveznice ili skenirati QR kod. Slično tome, pojedinci se mogu naći meta prijevare putem e-poruka koje navodno dolaze od tijela javne vlasti poput Ministarstva ili HZZO-a. U tim porukama se građanima obećava isplata pomoći ili povrat troškova, ali je uvjet za ostvarivanje tih prava klik na poveznicu ili skeniranje QR koda, što zapravo može dovesti do gubitka osobnih podataka ili novčanih sredstava. Čak i Policijska uprava nije pošteđena takvih prijevara, gdje se građanima šalju lažne e-poruke optužujući ih za kaznena djela te tražeći njihovo očitovanje putem sumnjivih poveznica ili QR kodova u određenom vremenskom roku.

Primjeri Finske i Danske jasno pokazuju da čak i najrazvijenije e-uprave nisu imune na prijetnje phishing kampanjama. Ovi slučajevi naglašavaju globalnu prirodu cyber prijetnji te potrebu za kontinuiranim unapređenjem sigurnosnih mjera i edukacijom korisnika. Usprkos visokoj razini digitalne zrelosti ovih država, phishing napadi predstavljaju ozbiljan rizik za sigurnost osobnih podataka građana i integritet digitalnih javnih usluga.

Zaključno, ovaj rad doprinosi povećanju svijesti javnosti o zlonamjernim cyber napadima na javne institucije, posebice kroz analizu ranjivosti informacijske sigurnosti sustava e-uprave. Kroz istraživanje primjera prijevara i napada, ističemo važnost kontinuiranog unapređenja sigurnosnih mjera i educiranja korisnika o rizicima i prepoznavanju prijetnji. Uvođenje preventivnih i reaktivnih mjera te suradnja sa stručnjacima iz područja kibernetičke sigurnosti ključni su koraci u zaštiti integriteta sustava e-uprave i osiguravanju povjerenja građana u digitalne javne usluge. Kroz daljnje istraživanje i implementaciju sigurnosnih politika, možemo ojačati otpornost sustava na napade i pridonijeti održivoj digitalnoj transformaciji javnog sektora.

LITERATURA

1. CERT (2023). *E-GRAĐANI SUSTAV SE KORISTI ZA NOVU QR PHISHING KAMPANJU!. Nacionalni CERT* (28. veljače). Dostupno na: https://www.cert.hr/upozorenje-e-gradani-sustav-se-koristi-za-novu-qr-phishing-kampanju/ (pristupljeno 11.02.2024.)
2. CERT (2024). Preuzeto sa: https://www.cert.hr/statistika/ (pristupljeno 11.02.2024.)
3. CERT. Phishing, https://www.cert.hr/phishing/ (pristupljeno 11.02.2024.)
4. e-Građani (2023). *info@egradani.com nije službeni mail sustava e-Građani*. *e-Građani* (16. veljače) Dostupno na: https://gov.hr/hr/info-egradani-com-nije-sluzbeni-mail-sustava-e-gradjani/2479 (pristupljeno 11.02.2024.)
5. *e-Građani* (2024). Dostupno na: https://gov.hr/ (pristupljeno 11.02.2024.)
6. Faglige Seniorer, Dostupno na: https://fagligsenior.dk/2023/07/13/advarsel-falsk-mail-fra-borger-dk-kan-koste-dig-dyrt/ (pristupljeno 13.02.2024.)
7. Ministarstvo uprave (2013). Program razvoja elektroničkih usluga. Dostupno na: https://gov.hr/UserDocsImages/Dokumenti//Program_razvoja_elektronickih_usluga.pdf (pristupljeno 13.02.2024.)
8. *Portal otvorenih podataka* (2023). Dostupno na: https://data.gov.hr/ckan/dataset/e-gradjani-statistika (pristupljeno 11.02.2024.)
9. Strategija digitalne Hrvatske za razdoblje do 2032. godine (Narodne Novine 2/2023). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2023_01_2_17.html (pristupljeno 07.02.2024.)
10. Suomi.fi, Dostupno na: https://www.suomi.fi/news/watch-out-for-scam-messages-pretending-to-be-from-suomi-fi-do-not-click-on-the-links-in-the-message (pristupljeno 13.02.2024.)
11. World Economic Forum (2024). *Global Risks Report*. Dostupno na: https://www.weforum.org/publications/global-risks-report-2024/ (pristupljeno 13.02.2024.)

Summary

SECURITY RISKS OF USING DIGITAL TECHNOLOGIES IN E-GOVERNMENT

Professional paper

In the digital transformation of public institutions, the implementation of e-government becomes crucial for improving citizens' interaction with the government. The e-Građani system in Croatia represents a central hub for providing information and services of the public sector, but it is simultaneously exposed to various cyber threats, particularly phishing campaigns. This paper analyzes the threats to the information security of the e-Građani system, with an emphasis on phishing, through a review of the system, identification of threats, and analysis of example attacks. Furthermore, examples of phishing from other European countries such as Denmark and Finland are compared, highlighting the global nature of cyber threats. Through the analysis of these cases, the importance of security protocols and user education in protecting digital public services is emphasized.

Key words: *e-Građani, e-Government, information security, phishing, cyber threat*